TECHNICAL
DOCUMENTATION

Getting Started with the Illumio Console

Welcome to the Illumio Console. The Illumio Console is the integration of the Illumio Core and CloudSecure products into the same platform. With the right user permissions, you can access features of two Illumio products in one unified user interface.

Table of Contents

What's New and Release Notes

Review these release notes to learn about new features and for a list of new and resolved issues.

Published: May 2025

Illumio Console What's New and Release Notes 25.21

Learn about new features in version 25.21 and review the known and resolved issues in this release.

What's New in 25.21 [5]

New APIs in 25.21 [13]

Resolved Issues in 25.21 [21]

What's New in 25.21

Before you upgrade to Illumio Console 25.21, familiarize yourself with new features in this release.

Hybrid Policy Support

After hybrid policies are enabled, your on-premises and applicable cloud networks assume to use non-overlapping private IP subnets. Any policies between on-premises and cloud workloads are distributed to the appropriate on-premises workloads and cloud resources. Within each cloud, Illumio Console determines the network segregation with VPC peering detected. Currently, supported clouds are AWS and Azure.

Hybrid policy support is available only to applicable customers. For details, contact your Illumio representative.

Rule-Based Labeling Enhancements

For details about Rule-Based Labeling, see Rule-Based Labeling.

This release introduces the following enhancements to the Rule-Based Labeling feature:

Support for Regular Expressions and NOT operators

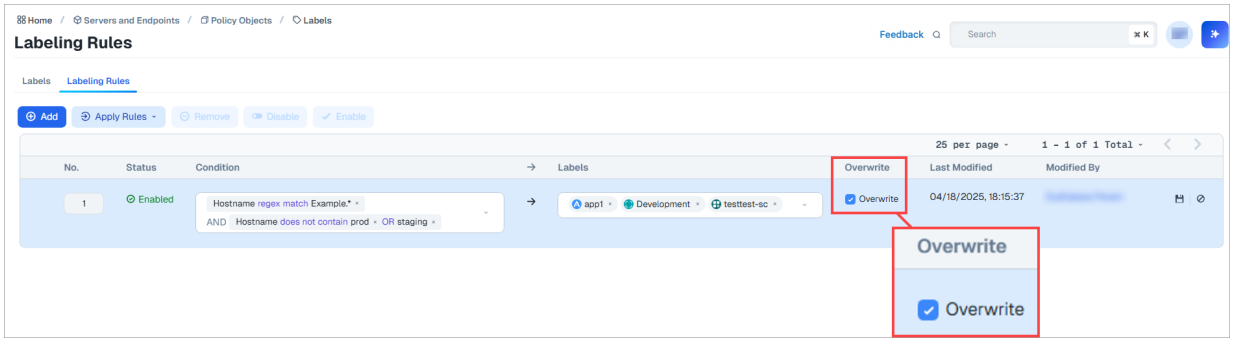
- **Regular Expressions**

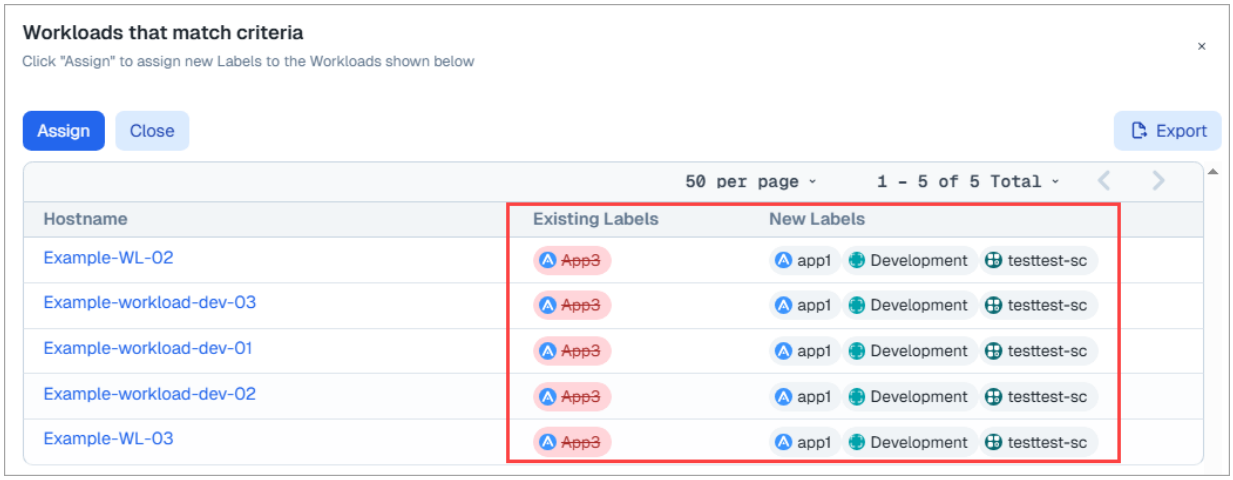
  Regular Expressions (regex) allow you to define complex patterns to precisely match workloads in your environment. This precision is particularly useful when you're trying to find and label workloads that have multiple attributes.
- **NOT Operators**

  NOT operators allow you to refine search queries by excluding certain values. You can combine NOT operators with other search operators (like AND, OR) to create complex queries that precisely target the desired information while excluding irrelevant data.

Support for Overwriting Existing Labels

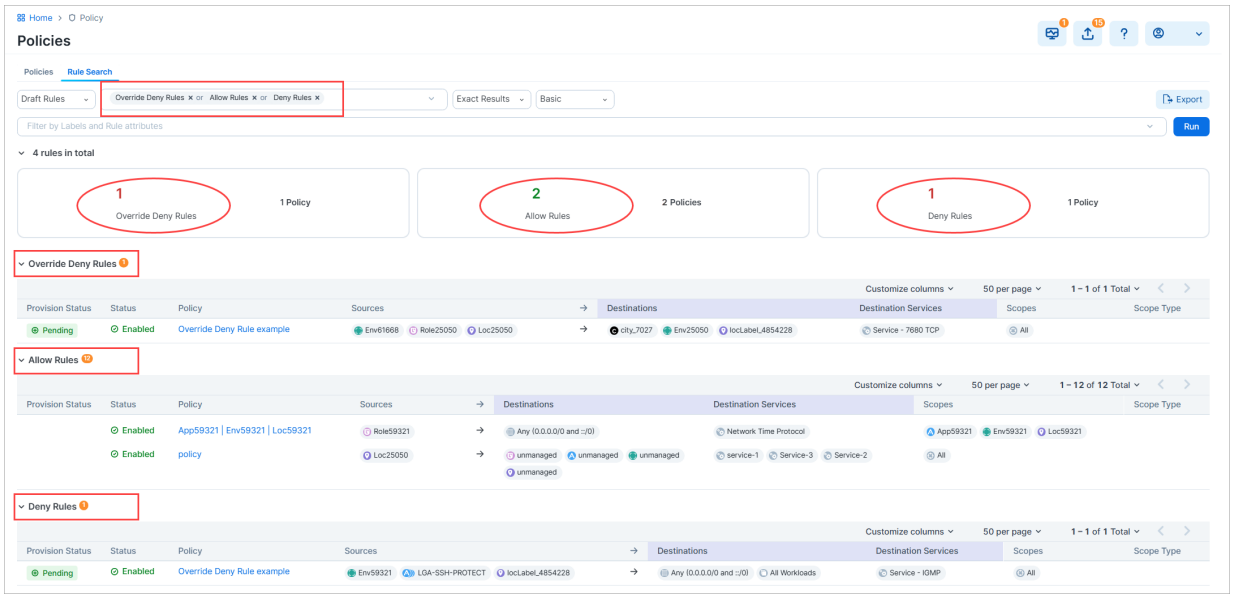
The Overwrite option allows you to replace labels already assigned to workloads with new labels of the same type. For example, if your labeling rule is set to assign an Application label to matching workloads, selecting this option ensures that any Application label already assigned to these workloads is overwritten by the new Application label when you click Assign.





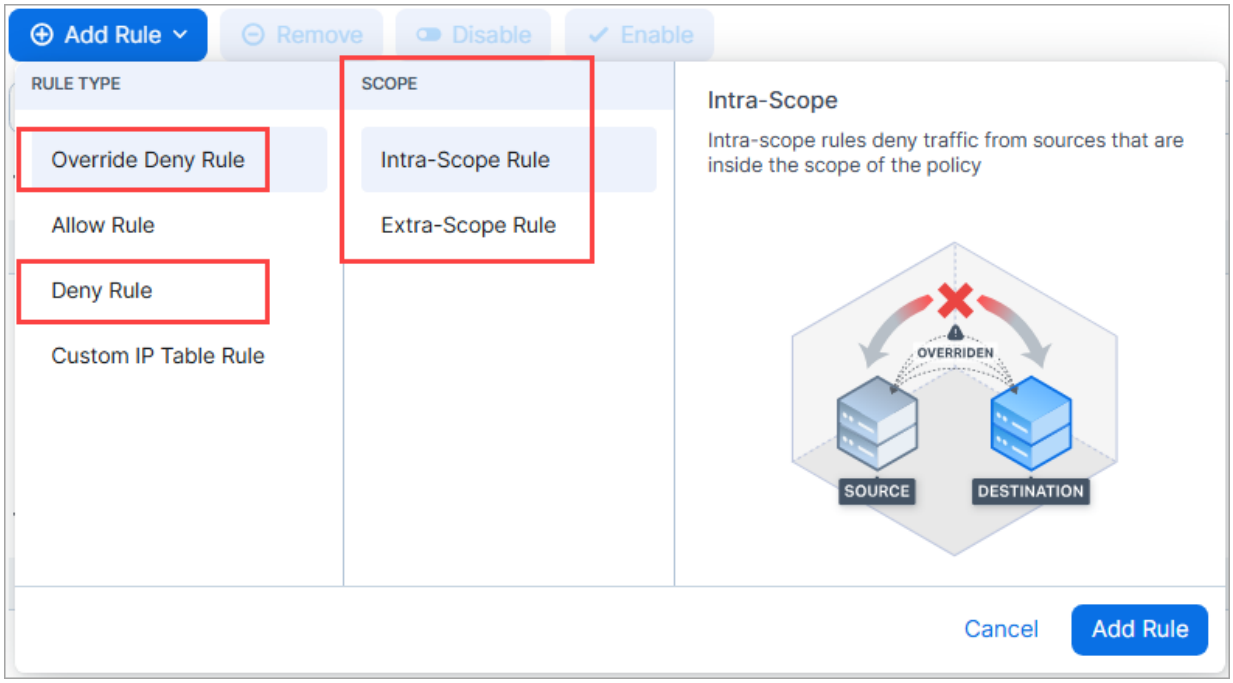
Rule Search now supports Deny and Override Deny rules

You can now search for any combination of Allow, Deny, and Override Deny rules from the **Policies > Rule Search** tab. Previously, Rule Search was limited to Allow rules. Also, the total number of each rule type is prominently displayed just below the search filter.



Deny and Override Deny rules now support Intra- and Extra-Scopes

You can now specify an Intra-Scope or Extra-Scope scope when you add Deny and Override Deny rules. Previously, this was only possible for Allow rules.



Rule IDs now included in Syslog

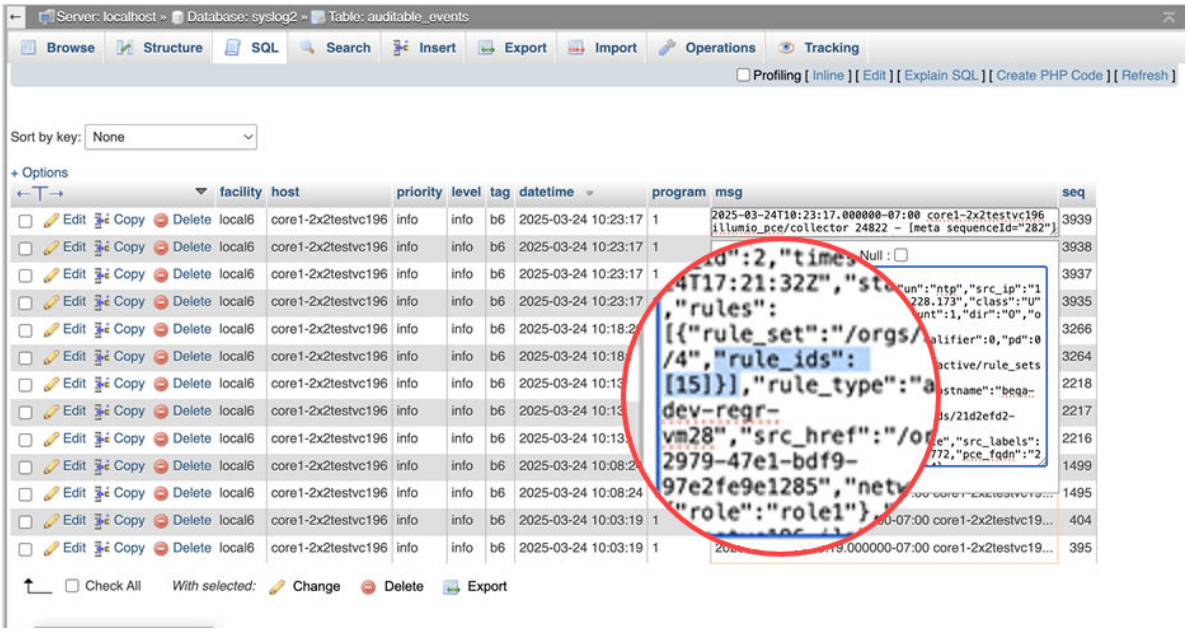
To help you trace and investigate traffic flows, each traffic flow entry in Syslog now includes the rule ID associated with the policy decision of the flow. This provides an explicit reference to the rule that affected the flow's policy state.

CAUTION

For large customers with 10K+ messages per second, adding rule IDs to the syslog events will make the recorded data significantly larger.

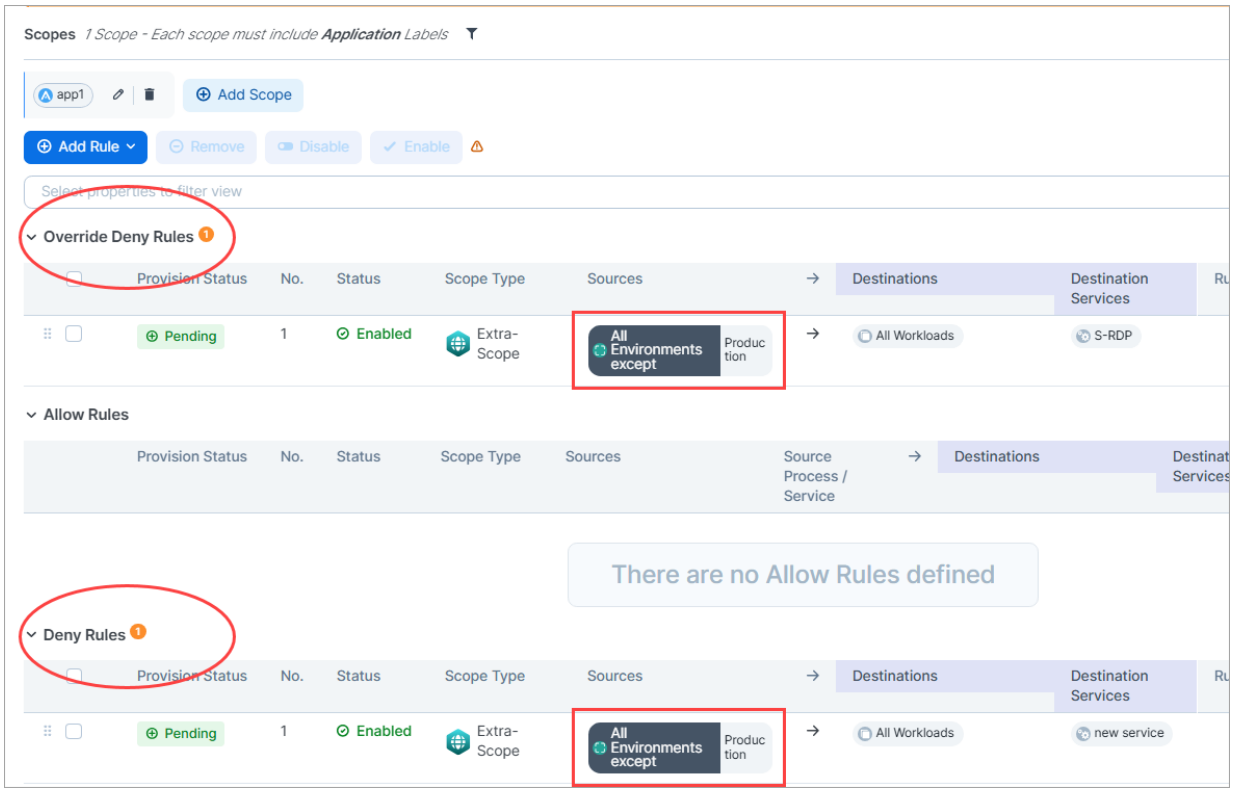
To use this feature, perform these steps:

1. Enable Rule Hit Count on the PCE and the VEN.
   - Enable Rule Hit Count on a VEN
   - Enable Rule Hit Count on a PCE
2. Enable the Rule ID feature as described in Showing Rule ID in Syslog in the Illumio REST API Guide.
3. Find the rule IDs in your syslog.



Label Exclusion now available for Deny and Override Deny rules

The ability to use an "all labels except. . ." approach when selecting labels for your rules is now available for Override Deny and Deny Rules. Previously, this feature was only available for Allow rules.

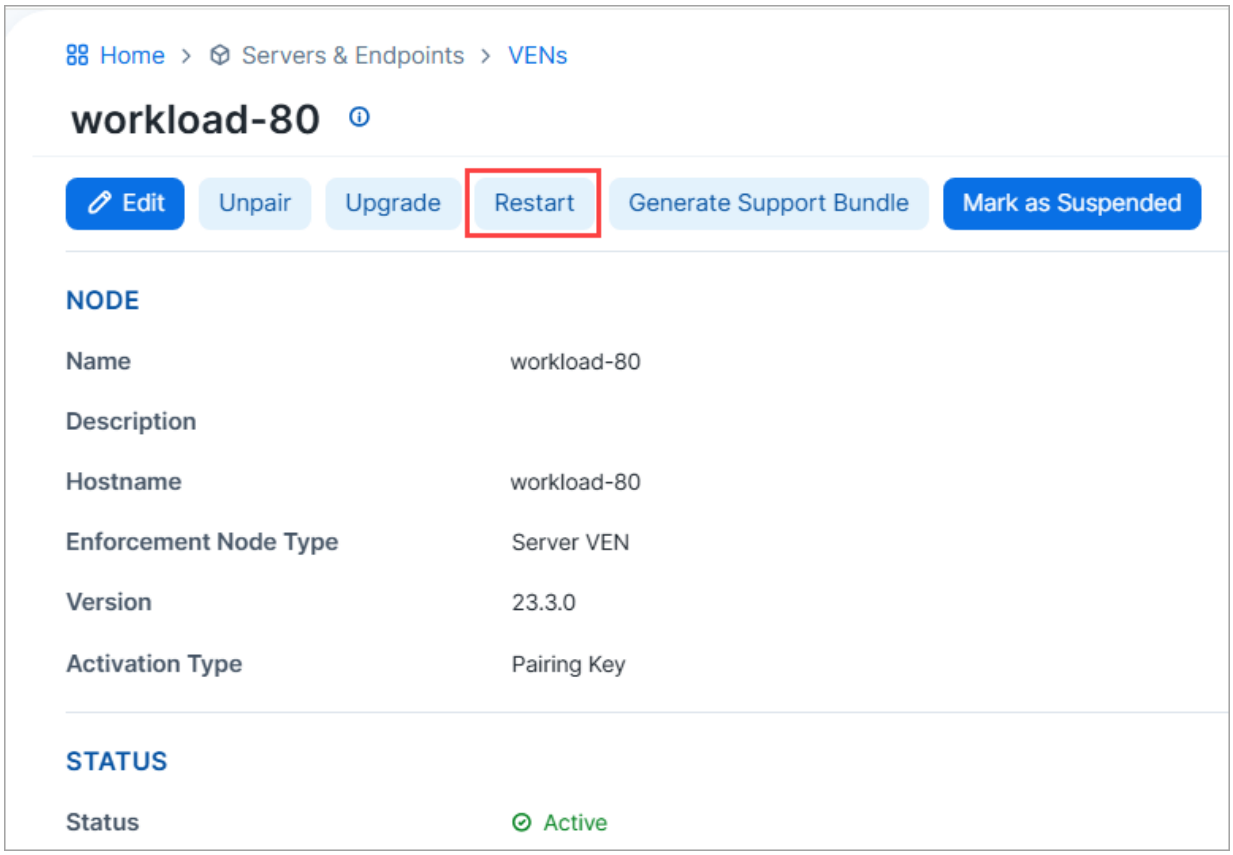


VEN Remote Restart

You can now restart a VEN directly from the PCE without physical access to the workload. Remote Restart is similar to other VEN operations that you can initiate from the PCE, such as unpairing and upgrading. For details, see Remote VEN Restart.

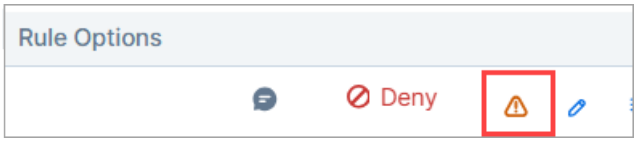
NOTE

The Restart button is grayed out if the VEN is Suspended or Offline.



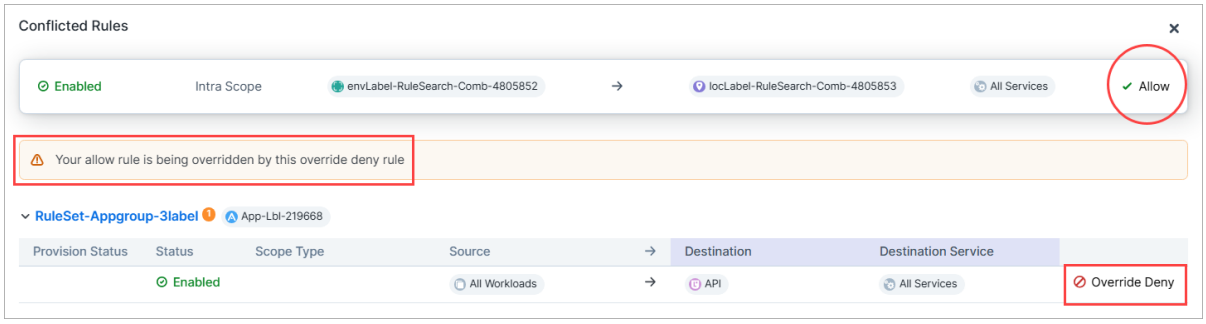
Conflicted Rules panel

You are now alerted when rules are in conflict with one or more other rules in the same or another policy in your organization. Click the yellow icon to display a panel with the conflict details and use the information to perform housekeeping on your policy or troubleshoot unexpected policy behavior.

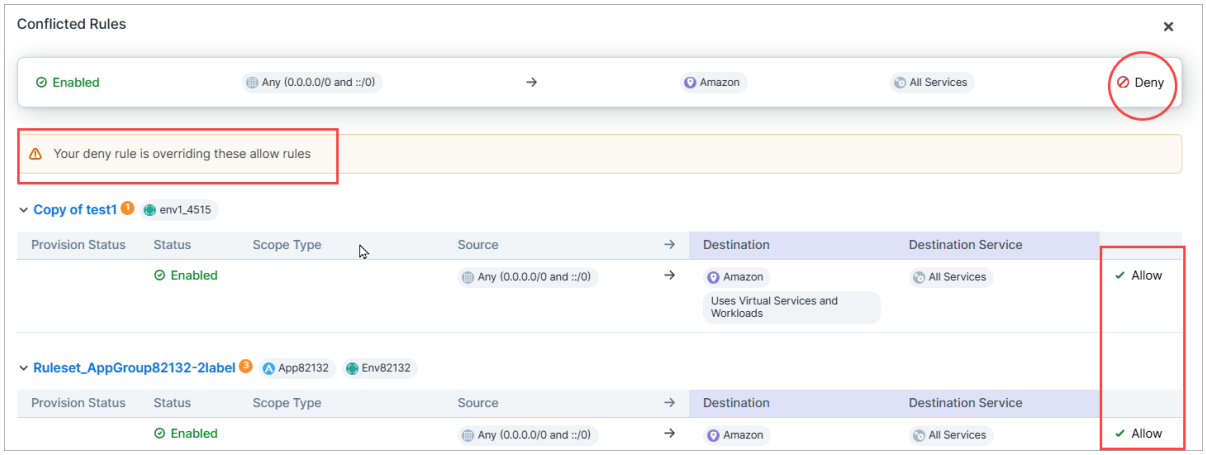


Rules are in conflict when:

- Traffic allowed by an Allow rule in your policy is overridden by an Override Deny rule in the same or another policy in your organization. Result: traffic is **denied**, which you may or may not have intended.



- Traffic denied by a Deny rule in your policy is overridden by an Allow rule in the same or another policy in your organization. Result: traffic is **allowed**, which you may or may not have intended.

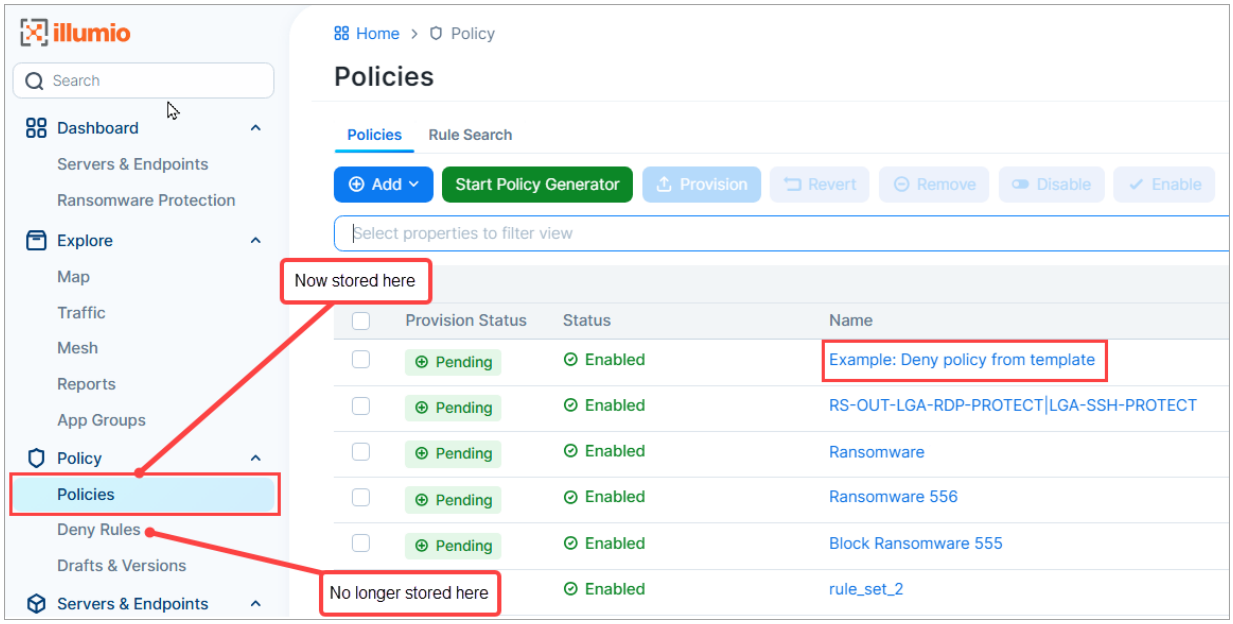


Deny Rules created from a Template now appear in the Policies page

When you add a deny rule from a template, it's now placed in the Policies list page, not the Deny Rules page as before.

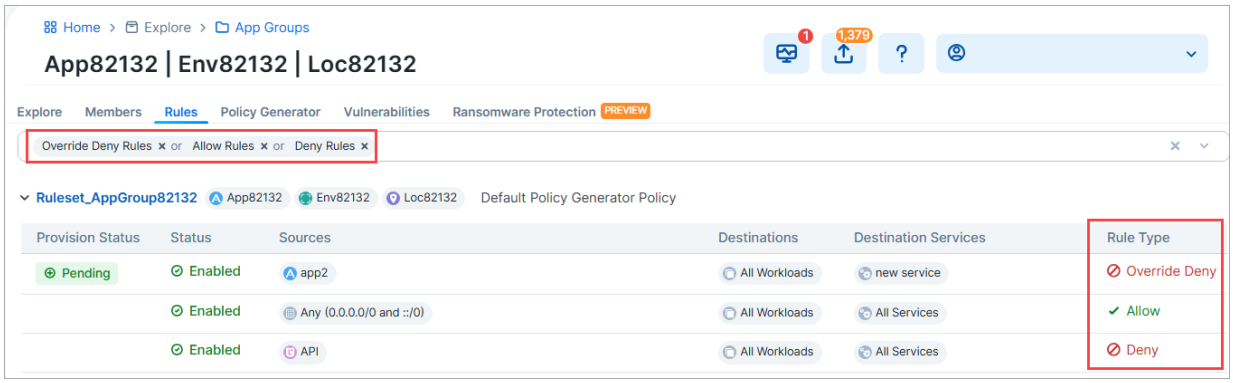
NOTE

Although the stand-alone Deny Rules page still appears in the left navigation, Illumio plans to deprecate it in a future release. If your Core instance was upgraded to release 25.2.10 or later, Illumio recommends that you migrate your Deny rules from the Deny Rules page to the Policies page and add and manage Deny Rules from the Policies page from now on.



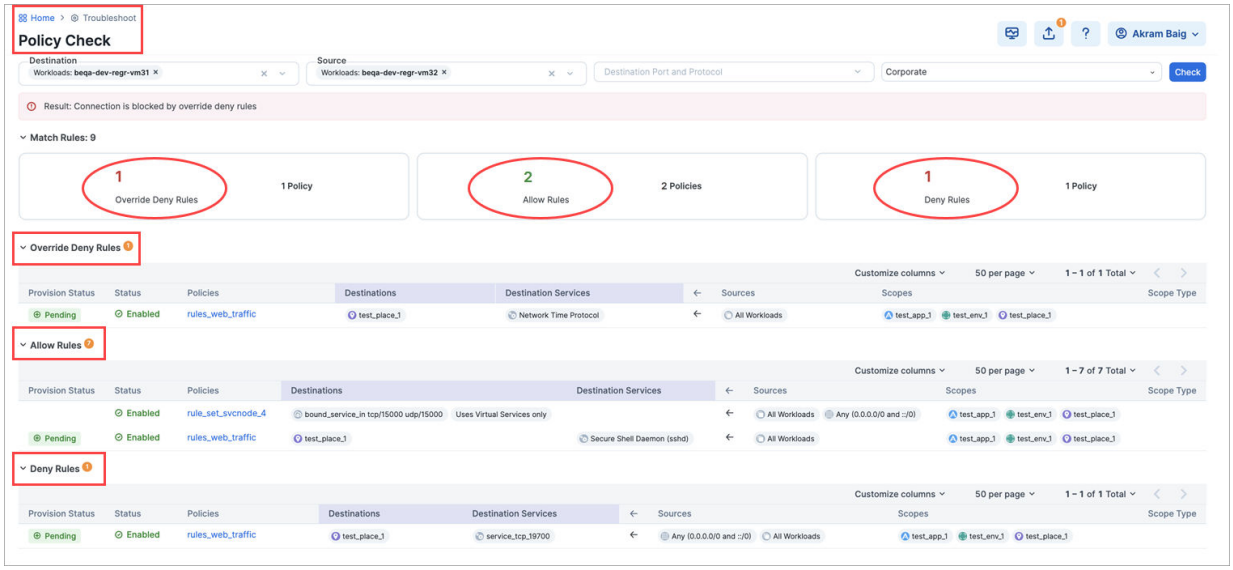
Support for searching App Groups by Deny and Override Deny rules

You can now search for Deny and Override Deny rules from an App Group's details page. Previously, you could only search for App Groups containing Allow rules from this page.



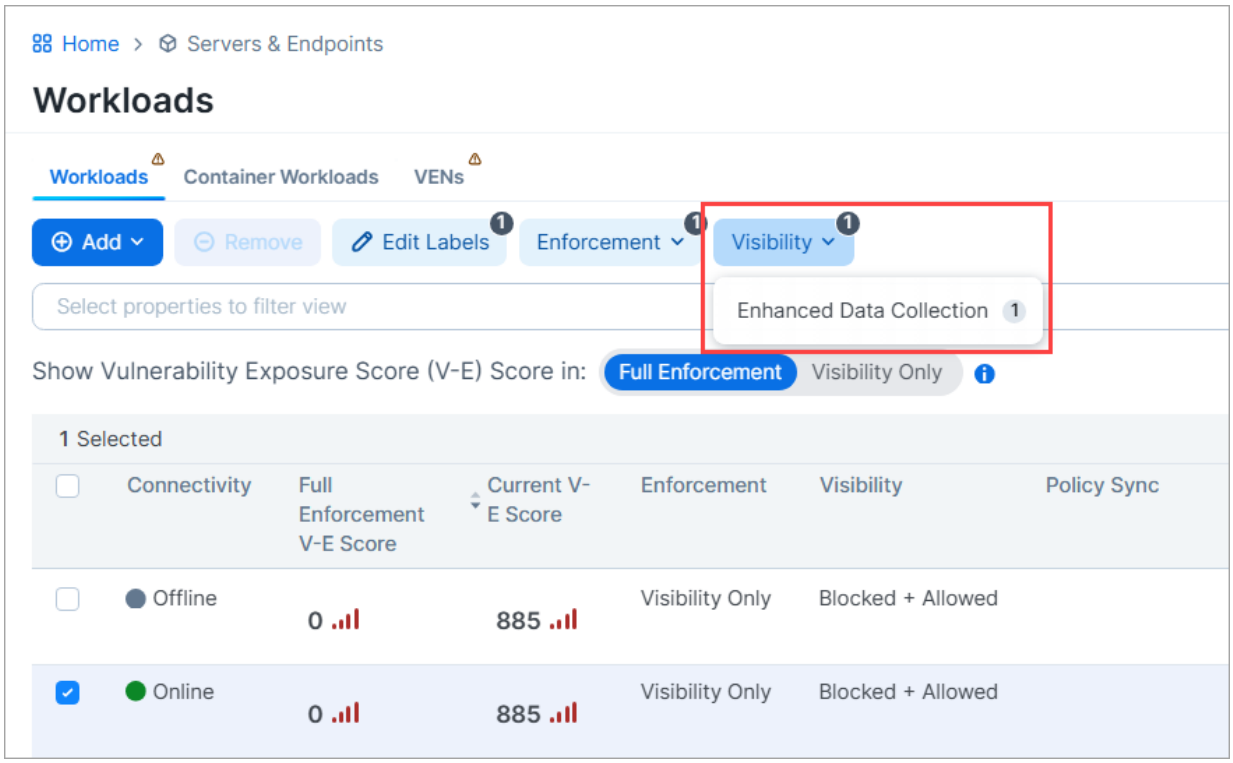
Support for checking policy by Deny and Override Deny rules

Beginning with this release, the policy check feature (**Troubleshooting > Policy Check**) checks for policies that include Deny and Override Deny rules. Previously, this featured only checked policies containing Allow rules.



Support for Enhanced Data Collection in all enforcement modes

You can now enable the Enhanced Data Collection option in any enforcement mode, not just Full Enforcement as before. Enhanced Data Collection allows the VEN to log byte counts and connection details for Allowed, Blocked, and Potentially Blocked traffic.



New APIs in 25.21

New Common Schemas

- **common deny_rule_actor**: The Enforcement Boundary Actor schema describes the actors as workloads and defines the exclusions.

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "description": "Enforcement boundary actor",
  "type": "array",
  "minItems": 1,
  "items": {
    "type": "object",
    "additionalProperties": false,
    "properties": {
      "actors": {
        "description": "Rule actors are all workloads ('ams')",
        "type": "string",
        "enum": ["ams"]
      },
      "exclusion": {
        "description": "Boolean to specify whether or not the actor is an
exclusion - only for labels and label groups",
        "type": "boolean",
        "expose_to": ["end_user_experimental"],
        "default": false
      },
      "label": {
        "$ref": "href_object.schema.json"
      },
      "label_group": {
```

```
        "$ref": "href_object.schema.json"
      },
      "ip_list": {
        "$ref": "href_object.schema.json"
      },
      "workload": {
        "expose_to": ["end_user_private_perm"],
        "$ref": "href_object.schema.json"
      }
    }
  }
}
```

- **common deny_rules_get**: For deny_rules, this gets the timestamps when the Enforcement Boundary was created, updated, and deleted. It also defines the users who originally created, updated, and deleted the boundary.

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "description": "Enforcement boundary",
  "type": "object",
  "required": ["href", "providers", "destinations", "ingress_services"],
  "expose_to": ["end_user_private_perm"],
  "_comment": "Don't set additionalProperties:false here as it collides
with usage in allOf, set that in the schema that references this one
instead.",
  "properties": {
    "created_at": {
      "description": "Timestamp when this Enforcement Boundary was first
created",
      "type": "string",
      "format": "date-time"
    },
    "updated_at": {
      "description": "Timestamp when this Enforcement Boundary was last
updated",
      "type": "string",
      "format": "date-time"
    },
    "deleted_at": {
      "description": "Timestamp when this Enforcement Boundary was
deleted",
      "type": ["string", "null"],
      "format": "date-time"
    },
    "created_by": {
      "type": ["object", "null"],
      "required": ["href"],
      "properties": {
        "href": {
          "description": "User who originally created this Enforcement
Boundary",
          "type": "string"
        }
      }
    },
    "updated_by": {
```

```
      "type": ["object", "null"],
      "required": ["href"],
      "properties": {
        "href": {
          "description": "User who last updated this Enforcement
Boundary",
          "type": "string"
        }
      }
    },
    "deleted_by": {
      "type": ["object", "null"],
      "required": ["href"],
      "properties": {
        "href": {
          "description": "User who deleted this Enforcement Boundary",
          "type": "string"
        }
      }
    },
    "update_type": {
      "$ref": "../common/sec_policy_update_type.schema.json"
    },
    "href": {
      "description": "The job URI.",
      "type": "string"
    },
    "providers": { "$ref": "deny_rule_actor.schema.json" },
    "destinations": { "$ref": "deny_rule_actor.schema.json" },
    "ingress_services": {
      "$ref": "sec_rule_ingress_services.schema.json"
    },
    "egress_services": {
      "$ref": "sec_rule_egress_services.schema.json"
    },
    "caps": {
      "$ref": "../common/entity_caps.schema.json"
    },
    "enabled": {
      "description": "Enabled flag",
      "type": "boolean"
    },
    "description": {
      "description": "Description",
      "type": ["string", "null"]
    },
    "network_type": {
      "$ref": "../common/rule_network_type.schema.json"
    },
    "override": {
      "description": "When true, the deny rule will override and take
precedence over other user defined allow rules.",
      "default": false,
      "type": "boolean"
    },
```

```
    "unscoped_destinations": {
      "description": "Set the scope for rule destinations to All",
      "type": "boolean"
    }
  }
}
```

- **common rule_set**: Parent Rule Set of a Rule.

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "description": "Enforcement boundary",
  "type": "object",
  "required": ["href", "providers", "destinations", "ingress_services"],
  "expose_to": ["end_user_private_perm"],
  "_comment": "Don't set additionalProperties:false here as it collides
with usage in allOf, set that in the schema that references this one
instead.",
  "properties": {
    "created_at": {
      "description": "Timestamp when this Enforcement Boundary was first
created",
      "type": "string",
      "format": "date-time"
    },
    "updated_at": {
      "description": "Timestamp when this Enforcement Boundary was last
updated",
      "type": "string",
      "format": "date-time"
    },
    "deleted_at": {
      "description": "Timestamp when this Enforcement Boundary was
deleted",
      "type": ["string", "null"],
      "format": "date-time"
    },
    "created_by": {
      "type": ["object", "null"],
      "required": ["href"],
      "properties": {
        "href": {
          "description": "User who originally created this Enforcement
Boundary",
          "type": "string"
        }
      }
    },
    "updated_by": {
      "type": ["object", "null"],
      "required": ["href"],
      "properties": {
        "href": {
          "description": "User who last updated this Enforcement
Boundary",
          "type": "string"
        }
```

```
        }
      },
      "deleted_by": {
        "type": ["object", "null"],
        "required": ["href"],
        "properties": {
          "href": {
            "description": "User who deleted this Enforcement Boundary",
            "type": "string"
          }
        }
      },
      "update_type": {
        "$ref": "../common/sec_policy_update_type.schema.json"
      },
      "href": {
        "description": "The job URI.",
        "type": "string"
      },
      "providers": { "$ref": "deny_rule_actor.schema.json" },
      "destinations": { "$ref": "deny_rule_actor.schema.json" },
      "ingress_services": {
        "$ref": "sec_rule_ingress_services.schema.json"
      },
      "egress_services": {
        "$ref": "sec_rule_egress_services.schema.json"
      },
      "caps": {
        "$ref": "../common/entity_caps.schema.json"
      },
      "enabled": {
        "description": "Enabled flag",
        "type": "boolean"
      },
      "description": {
        "description": "Description",
        "type": ["string", "null"]
      },
      "network_type": {
        "$ref": "../common/rule_network_type.schema.json"
      },
      "override": {
        "description": "When true, the deny rule will override and take
  precedence over other user defined allow rules.",
        "default": false,
        "type": "boolean"
      },
      "unscoped_destinations": {
        "description": "Set the scope for rule destinations to All",
        "type": "boolean"
      }
    }
  }
```

- **common sec_rule_egress_services**: Array of objects.

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "description": "Array of objects",
  "type": "array",
  "items": {
    "type": "object",
    "$ref": "../common/href_object.schema.json"
  }
}
```

- **common sec_rules_get**: For sec_rules, this gets the timestamps when the Enforcement Boundary was created, updated, and deleted. It also defines the users who originally created, updated, and deleted the boundary.

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "description": "Enforcement boundary",
  "type": "object",
  "required": ["href", "providers", "destinations", "ingress_services"],
  "expose_to": ["end_user_private_perm"],
  "_comment": "Don't set additionalProperties:false here as it collides
with usage in allOf, set that in the schema  that references this one
instead.",
  "properties": {
    "created_at": {
      "description": "Timestamp when record was first created",
      "type": "string",
      "format": "date-time"
    },
    "updated_at": {
      "description": "Timestamp when record was last updated",
      "type": "string",
      "format": "date-time"
    },
    "deleted_at": {
      "description": "Timestamp when record was deleted",
      "type": ["string", "null"],
      "format": "date-time"
    },
    "created_by": {
      "type": "object",
      "properties": {
        "username": {
          "description": "The username which created this record",
          "type": "string"
        }
      }
    },
    "updated_by": {
      "type": "object",
      "properties": {
        "username": {
          "description": "The username which last updated this record",
          "type": "string"
        }
      }
    },
```

```
    "deleted_by": {
      "type": ["object", "null" ],
      "properties": {
        "username": {
          "description": "The username which deleted this record",
          "type": "string"
        }
      }
    },
    "update_type": {
      "description": "Type of update",
      "oneOf": [
        {
          "type": "null"
        },
        {
          "type": "string",
          "enum": ["create", "update", "delete"]
        }
      ]
    },
    "update_label": {
      "description": "Type of update",
      "oneOf": [
        {
          "type": "null"
        },
        {
          "type": "string",
          "enum": ["create", "update", "delete"]
        }
      ]
    },
    "href": {
      "description": "URI of object",
      "type": "string"
    },
    "enabled": {
      "description": "Enabled flag",
      "type": "boolean"
    },
    "description": {
      "description": "Description",
      "type": ["string", "null"]
    },
    "ingress_services": { "$ref":
"sec_rule_ingress_services.schema.json" },
    "egress_services": { "$ref": "sec_rule_egress_services.schema.json" },
    "resolve_labels_as": { "$ref":
"sec_rule_resolve_labels_as.schema.json" },
    "sec_connect": {
      "description": "Whether a secure connection is established",
      "type": "boolean"
    },
    "stateless": {
```

```
      "expose_to": ["end_user_experimental"],
      "description": "Whether packet filtering is stateless for the rule",
      "type": "boolean"
    },
    "machine_auth": {
      "expose_to": ["end_user_experimental"],
      "description": "Whether machine authentication is enabled",
      "type": "boolean"
    },
    "providers": { "$ref":
"sec_policy_rule_sets_sec_rules_providers_get.schema.json" },
    "destinations": { "$ref":
"sec_policy_rule_sets_sec_rules_destinations_get.schema.json" },
    "consuming_security_principals": { "$ref":
"consuming_security_principals_get.schema.json" },
    "unscoped_destinations": {
      "description": "Set the scope for rule destinations to All",
      "type": "boolean"
    },
    "use_workload_subnets": {
      "$ref": "sec_rule_use_workload_subnets.schema.json"
    },
    "rule_set": { "$ref": "../common/rule_set.schema.json" },
    "log_flow": {
      "description": "If false, the VEN will not log any traffic that
matches this flow.",
      "type": "boolean",
      "expose_to": ["end_user_private_transitional"]
    },
    "network_type": { "$ref": "../common/rule_network_type.schema.json" }
  }
}
```

Resolved Issues in 25.21

Issue	Fix Description
E-127134	**Enable editing the label of namespace under Container Workload Profile** You can now edit the labels of a Container Workload Profile by clicking **Edit Labels** at the Container Workload Profiles page.
E-126725	**Unavailable Save button following virtual services update is now available** In some cases with a NEN managing a Server Load Balancer (SLB), after updating the SLB's associated virtual servers through the PCE UI, it wasn't possible to save those changes because the **Save** button remained grayed-out.
E-126227	**Conflict with the "All services" rule is now properly reported** When a user defined a rule to overlap another rule (do the opposite of the other rule), this rule was: • Reported as in conflict with the 'All services' rule when the rule was defined using port + proto (which is correct). • Not reported as in conflict with the 'All Services' rule when the rule was defined using a service (which is wrong). After the fix, the rule is reported as in conflict with the 'All services' rule when using a service.
E-126207	**Custom Time Range query issue is resolved** On the Blocked Traffic tab of a Workload's details page, filtering the Blocked Traffic list by a custom date range failed because the query always began no more than 24 hours previously, regardless of the start date specified in the date selector.
E- 126122	**Fixed public API flows failures while automating policy creation** When attempting to automate policy creation and pull flows across various applications and ports/protocols, these queries failed multiple times before completing.
E- 126120	**Fixed asynchronous traffic query in Core Service Detection** Fixed the asynchronous traffic query that caused an incorrect **No Traffic to Display** message to appear after a user clicked the Information icon for a recommended endpoint in Core Services Detector.
E- 125803	**Conflicted rules alert message is now correct** An alert message in the PCE UI about conflicting rules misstated the details of the conflict.
E- 125150	**Improved PCE performance by streamlining C-VEN and Kubelink API queries** Streamlined C-VEN and Kubelink API queries to improve PCE performance, which was sometimes noticed in large clusters.
E- 124960	**Azure Cloud Objects now properly displayed in the Explore Map** When customers attempted to view the Explore Map grouped by "Service Categories" and "Service Roles", the Azure objects were displayed as **No Service Category** despite having these labels.
E-124809	**Issues seen in Draft View are fixed**

Issue	Fix Description
	In the Unified Console, the Traffic table appeared in Draft View with several issues, including missing or erroneous information and anomalous behavior of some global filters. These issues have been fixed.
E-124060	**Fixed the formatting when adding a service to the "Service is not" field** A small formatting misalignment that sometimes occurred when filtering traffic is now fixed when adding an additional service to a list of services in the **Service is not** field.
E-122808	**Fixed issues with exporting core events on scp41** Customers experienced issues with filtering core events. Once events have been filtered, users couldn't export filtered events or all events.
E-118620	**Reverting the IP List from its detail page is fixed** Users can now properly revert an IP List from its details page without the page loading forever.
E-117295	**Issue with Rule Search results resolved** Fixed an issue in **Rule Search** in which, when running a query to find rules that contained at least one of several individual ports ("or" logic), the search returned only rules that had all of the ports ("and" logic).
E-112195	**Fixed hidden Create menu option when creating label or label group** Fixed a UI issue when clicking the label or label group in the selector menu that caused the **Create** menu option to be hidden.

Resolved Issues in 25.21.12

The following issues have been resolved in release 25.21.12

Resolved Issues

Issue	Fix Description
E-127873	**Kubernetes Workloads not displayed** Kubernetes Workloads were not displayed on the Container Cluster Details page, specifically in the "Kubernetes Workloads" tab.
E-127812	**Essential service rules are now displayed on the Workloads Rules tab.** Essential service rules were not displayed on the Workloads Rules tab. This issue is fixed.
E-127763	**Label rules are now case-insensitive and will apply labels.** The hostname used in 25.21.0 is case-sensitive, but it was case-insensitive in prior releases. The behavior has been reverted to its original state.

What's New and Release Notes for Illumio Console 25.11

April 2025

What's New in Illumio Console 25.11.1

This release includes quality improvements.

What's New in Illumio Console 25.11.0

Here's a summary of the new and enhanced features in this release.

Rule-based labeling enabled by default

Rule-based labeling is now enabled for all organizations by default. For more information on rule-based labeling, see the Security Policy Guide.

Release Notes for Illumio Console 25.11

These release notes describe the new features, enhancements, resolved issues, and known issues for the Illumio Console 25.11.*x* releases.

Resolved Issue in Release 25.11.1

This release includes quality improvements.

Resolved Issues in Release 25.11.0

Issue	Description
E-123410	**Load balancer Save button no longer remains greyed out** The **Save** button is no longer greyed out when attempting to create a NEN F5 entry at the Server Load Balancer page (**Infrastructure** > **Load Balancers**).
E-123267	**Policy Settings are now persistent** The UI column order for Destination and Source on the **Policy Settings** page now remain as last set. Changes to these values can be made (and Saved) as expected.
E-123184	**Core Traffic Map now loads** The traffic map now appears as expected in the UI.
E-123059	**Reports Email feature fixed** The reporting feature sends emails as expected when the option "**Email me a copy of the report**" is enabled.
E-123026	**User can no longer add duplicate filters** After a filter is added manually, the same filter can no longer be added again by using the contextual menu.

Known Issues in Release 25.11.0

Issue	Description	Status
E-122945	**Mesh: Clicking on Resource Type or Public Address Ticks in Mesh produces JavaScript errors** Clicking on Resource Type or Public Address values in a Mesh view causes JavaScript errors. In some cases, it can cause the view to become unresponsive and hang.	Unresolved

Illumio Console 24.34 What's New and Release Notes

February 2025

What's New in Illumio Console 24.34

Learn about new features, enhancements, and resolved issues for this release.

- **Map shows partial data if some data is unavailable**
  The unified map now shows partial data even if one region is temporarily down, without waiting for all region data to be available. A message indicates which regions data are missing from the map.

Release Notes for Illumio Console 24.34

These release notes describe the resolved issues in this release.

Resolved Issues

Issue	Description
E-122444	**Unable to load results from an existing query** Attempts to **Load Results** of an existing query failed to show any results.
E-121200	**Add new scope taking time to reflect on side panel** When adding a new scope to a rule, saving the new scope (by clicking the **Save** icon) at the **Policy Details** panel took several seconds before the new scope appeared in the list of Scopes.
E-120904	**Existing macOS workloads not found by Labeling Rule** A Label Rule designed to apply a label to macOS workloads failed because it didn't identify existing macOS workloads in the customer's network.
E-120650	**User is able to add same service to service filters more than once** After a service was already added directly in the **Service** query field, the same service could be added by hovering over that service in the results table and selecting it from there to be added to the filter, causing the service to be listed twice in the field.
E-112003	**Core Services side navigation menu item disappears after browser reloads** After enabling Core Services Detection and Scanner Detection (at **Settings** > **Core Service Settings**), the menu item for accessing the **Core Services** page appeared as expected under the **Infrastructure** menu. But after refreshing the browser, the **Core Services** menu item disappeared from under the **Infrastructure** menu.

Illumio Console 24.33 What's New and Release Notes

These release notes describe the new features, resolved issues, limitations, and known issues for Illumio Console 24.33.

Published: January 2025

What's New in Illumio Console 24.33

Release 24.33.1 provides performance improvement of traffic flow visualization in draft mode on the Unified Map.

Release Notes for Illumio Console 24.33

Resolved Issues in Illumio Console 24.33.1

- **Allow Port Ranges for Cloud Flow Queries** (E-121798)
  Previously, cloud flows did not support port ranges. This limitation has been removed.
- **Unexpected "401 unauthorized" error** (E-121576)
  Sometimes after a long period of use, the UI displayed a "401 unauthorized" error message.
- **Allowed quick filter in Draft view is not working** (C-7516)
  When unchecking the **Allowed** quick filter to a Draft View at the Traffic page, the system incorrectly found no traffic, and displayed a "No Traffic available for selected filters" message. This filter error also occurred at the Map page.

Illumio Console 24.32 What's New and Release Notes

These release notes describe the new features, resolved issues, limitations, and known issues for 24.32.

Published: December 2024

What's New in Illumio Console 24.32.0

The following sections describe the new features that were added in Illumio Console 24.32.0.

Risky Ports Insight

Illumio Platform now provides insights into Risky Ports across your network. The Risky Ports insight helps network administrators easily identify and analyze traffic flows that have been detected on risky ports between IP Lists on the network. Use these insights to proactively manage and mitigate potential security risks by having detailed visibility into the source, destination, traffic volume, and other details of these ports.

To launch:

1. From **Home**, click **Insights**.
2. From the carousel, click the **Traffic on Risky Ports** tile.
   Risky port traffic is shown in a summary table .

The risky ports table summarizes an aggregate of active risky ports, initially sorted by amount of traffic flow that changed over the time period or periods shown next to the table heading. Aggregated flows are based on IP Lists, which can include any lists defined by you.

For more information, see the topic "Insights into Risky Ports."

Policy Scopes and Options Improvements

You can add scopes to an application policy by clicking **Manage Scopes** in the header for that policy's detail page, which launches a panel where you can add, edit or delete scopes. You can also change the name and description for the policy.

You can also add scopes to an organization policy by clicking **Policy Options** and choosing **Edit Details**. From the Policy Details pane, click **Add Scopes**.

Release Notes for Illumio Console 24.32.0

Resolved Issues in Illumio Console 24.32.0

- **Unified Map doesn't load when expanding Servers group** (E-120924)
  In a Map set to group by "Data Center Type," when right-clicking to expand the **Servers** group, the Map would not load.
- **Virtual Services: Unable to bind workloads because 'Save' button is disabled** (E-120515)
  When trying to bind a workload to a virtual service at the Virtual Services details page, the **Bind** button was disabled, which prevented the action from being completed.
- **Delete workload right-click option shows 'Add Rule', but clicking on it results in navigation error** (E-118591)
  The **Add Rule** and **Double-click to expand** options were not working when right-clicking on deleted workloads.

Known Issues in Illumio Console 24.32.0

- **Allowed quick filter in Draft view is not working** (C-7516)
  When unchecking the "**Allowed**" quick filter to a Draft View at the **Traffic** page, the system incorrectly finds no traffic, and displays a "No Traffic available for selected filters" message. This filter error also occurs at the **Map** page.
  Workaround: None.
- **Sometimes selected navigation links disappear** (E-121598)
  Sometimes after a long period of use, the side navigation pane stops showing links to the pages associated with the unified map/policy, as well as to the **Server and Endpoints** menu.
  Workaround: Log out, and then log in again.
- **Mesh: Drill down on Workload is not working** (E-121580)
  In the Mesh view, after applying a filter and clicking on the **Workload** option along the **Source/Destination** axis, expected changes were not appearing in the UI. At other times, clicking on Workloads
  Workaround: Refresh the browser page.
- **Unexpected "401 unauthorized" error** (E-121576)
  Sometimes after a long period of use, the UI displays a "401 unauthorized" error message.
  Workaround: Log out, and then log in again.

Limitations in Illumio Console 24.32.0

- Existing flows seen before this upgrade are still shown occurring from servers and endpoints to an IP address, or from cloud resources to an IP address. New flows occurring after this upgrade to 24.32 are shown flowing between servers and endpoints and cloud accounts.

Security Changes in Illumio Console 24.32.0

- **d3-color is upgraded to version 3.1.0**
  The d3-color module has been upgraded to version 3.1.0 to address GHSA-36jr-mh4h-2g58.

Illumio Console 24.31.0+UI2-PCE What's New and Release Notes

What's New in Illumio Console 24.31.0+UI2-PCE

Illumio Console 24.31.0+UI2-PCE Maintenance Release

Illumio Console 24.31.0+UI2-PCE includes an updated version of the PCE software.

Illumio provides regular maintenance updates for reported bugs and security issues, as well as to add support for new operating system versions. As a maintenance release, Illumio Console 24.31.0+UI2-PCE solved software issues for the PCE to improve its reliability and performance.

For the complete list of improvements to the PCE for this release, see Release Notes for Illumio Console 24.31.0+UI2-PCE [28].

Release Notes for Illumio Console 24.31.0+UI2-PCE

This section provides a list of resolved issues for this release.

Resolved Issue in Illumio Console 24.31.0+UI2-PCE

Issue	Description
E-122843	**Traffic queries in the Map resulted in a blank screen** In some circumstances, querying the Map to view traffic intermittently resulted in a blank screen.

Illumio Console 24.31 What's New and Release Notes

Published: October, 2024

What's New in Illumio Console 24.31

Illumio Console is the integration of the Illumio Core and Cloud products into the same platform. Now, with the right user permissions, you can access features of two Illumio products in one unified UI. The features of Cloud are available in the Cloud menu, and the features of Core are available in the Servers & Endpoints menu.

The following sections describe the new features that were added in Illumio Console 24.31.

Overview of Conflicted Rules

Within **All Policies > Application Polices** and the **Cloud > Application > Policy** tab, Illumio Console now indicates if a rule in a policy has a conflict with another rule in the policy. If

there is a conflict, a warning information icon displays at the end of the row for that rule. A conflicted rule means that there are rules for your application that contradict each other. For example, someone else may have written an Allow rule that will permit traffic that you do not want to allow, and this rule is overriding the Deny rule that you want to enforce.

When you click the icon, the **Conflicted Rules** pane displays the reference rule that you clicked at the top of the pane, and provides more information about the rule conflicts for the application:

- For **Override Deny** rules, the pane shows the **Allow** rules that are overriding the subject rule.
- For **Allow** rules, the pane shows the **Override Deny** rules that are overriding the subject rule.
- For **Deny** rules, the pane shows the **Allow** rules that are overriding the subject rule.

View Inherited Rules

A new **View Inherited Rules** button has been added to Illumio Console. This feature allows you to see organization policies and application policies rules that apply to the application you are viewing. If an application has inherited rules, a **View Inherited Rules** button displays in the top-right corner of the **Application Policies** page for that application, with a badge that displays the number of inherited rules. This feature allows you to see other applications that have written rules that allow them to communicate with your application. For example, the **Inherited Rules** page for your CRM application could show you that the Finance application has an outbound rule that allows it to communicate to your CRM application.

To view inherited rules:

1. Navigate to **Policies > Application Policies** or **Policies > All Policies** and drill down on an application.
2. Click the **View Inherited Rules** button in the top-right corner of the **Application Policies** page.
3. Within the **Inherited Rules** detail page for the application, click the **Organization Policies** or **Application Policies** tabs to view details about the inherited rules.
4. If the application has inherited multiple rules for **Override Deny Rules**, **Allow Rules**, and **Deny Rules**, expand the pane to view the details for each rule.
5. Click the **Go to Policy** button to return to the details page for the application.

Note that if users do not have the appropriate role to view inherited rules, when they click the **View Inherited Rules** button, the application will display the Cloud Dashboard page.

View Provisioning Errors

The **Provisioning errors** button is available in the **All Policies**, **Organization Policies**, and **Application Policies** tabs. If you attempted to provision a policy but the policy did not successfully provision, click **Provisioning errors** to display the **Provisioning errors** page. This page provides more information about the application and organization policies that didn't provision and displays the cloud, the name and ID, the status, and the modification date for the policies that failed to provision.

Cloud Resources Displayed in Map View

Illumio Console now allows you to view Illumio Cloud and Illumio Core resources on the map regardless of whether or not these resources have traffic. Hover over the button in the interaction panel to switch between the display modes.

Context Menu Filters for Cloud Resources

Illumio Console now allows you to hover over a resource and add filter criteria from the context menu. This feature is available on the **Traffic** page and on the **Traffic** tab within the Map page. For example, within the **Traffic** table, if you want to search for traffic that uses TCP 443 as the service, hover over 443 TCP to select Port and/or Protocol as the type. Next, select **Service is** from the context menu to add 443 TCP to the **Service** field as a filter. If you want to add to your query so that it excludes traffic from the uswest2 region, hover over a Cloud resource in the **Destination** column, hover over uswest2, and then select **Source is not** from the context menu to exclude traffic from that region from your search.

The context menu filters function similarly within the **Map** page except that you would click a traffic link between Cloud resources and then hover over the resource in the **Traffic** tab to begin adding values to include or exclude from your query.

The query filters that display in the context menu depend on which operators you select from the **More** menu and whether or not you select **Show Exclusion Filters**.

You can filter by the Account ID, Resource Type, Region, and Cloud/Data Center categories.

Saved Settings Persist Across Sessions

User preferences and settings are now maintained across sessions within Illumio Console. Previously, when users logged out of the application, their settings were lost, but the information is now stored on the server side in k-v pairs.

Limitations in Illumio Console 24.31

- In the Map page, the Show Members with Traffic button only displays if you have 500 workloads and 500 Cloud resources.
- The Map page only displays resources in the Compute category, such as EC2 or VM instances.
- Exclusion filters do not work on multiple port ranges.

Known Issues in the Illumio Console 24.31 Release

- Within the Labeling Rules page, trying to schedule label assignment throws a JS error that breaks the page. (E-119321)

Resolved Issues in Illumio Console 24.31

Issue	Description
E-119339	**Editing a label created by Cloud service account throws a 401 error** When users try to edit a label created by the Cloud service account, a 401 error occurs and the user is logged out.
E-119313	**Filtering a label in Map or Traffic view is slow** When users filter for the Payment label in the Map or Traffic view, the query performs slowly and does not complete.

Release Notes for Illumio Console 24.31

These release notes describe the new features and known limitations for the Illumio Console 24.31 release.

Illumio Console 24.31 is available for Illumio Platform customers.

Illumio Core release numbering uses the following format: “a.b.c-d+e”.

- “a.b”: Standard or LTS release number, for example, “2.2”
- “.c”: Maintenance release number, for example, “.1”
- “-d”: Optional descriptor for pre-release versions, for example, “preview2”

Illumio Console 24.22 What's New and Release Notes

Release Notes for Illumio Console 24.22

These release notes describe the new features, resolved issues, limitations, and known issues for Illumio 24.22.x releases.

- Illumio Console 24.22.0+UI3 is available for Illumio Cloud customers only.

Document Last Revised: October 2024

Document ID: 14000-100-24.22.0+UI3-PCE

Product Version

PCE Version: 24.22.0+UI3 (Illumio Cloud customers only)

Illumio Core release numbering uses the following format: “a.b.c-d+e”.

- “a.b”: Standard or LTS release number, for example, “2.2”
- “.c”: Maintenance release number, for example, “.1”
- “-d”: Optional descriptor for pre-release versions, for example, “preview2”

What's New in This Release (24.22.0)

Illumio Console is the integration of Illumio's Core product into the Illumio Console UI. A companion Illumio product, Cloud, is also available in the Console. Now, with the right user permissions, you can access features of two Illumio products in one unified UI. The features of Cloud are available in the **Cloud** menu, and the features of Core are available in the **Servers & Endpoints** menu.

The following new features were added in Illumio Console 24.22.0:

- New **Explore** and **Policies** menu items have been added to the left navigation, which provide unified visualization (**Map**, **Traffic**, and **Mesh**) and unified policy writing and enforcement (**Policies**) across both Cloud workloads and Servers and Endpoints workloads.

  The unified Map shows workloads on Servers and Endpoints with a square icon.

  The unified Map view can group by Data Center Type -- Servers, Endpoints, AWS, and Azure.
- Illumio Console now lets you achieve unified visibility with the Map:
  - You can view the traffic between resources
  - You can right-click on a resource to write policy
  - You can distinguish between AWS, Azure, and server and endpoint datacenter types
  - You can query the cloud resources using the Cloud metadata Account ID, Region, Resource Type, VPC/VNET ID, Subnet ID, and Cloud/Data Center
- Policy can now be authored and enforced for all Servers and Endpoints and Cloud workloads. Illumio Console allows or denies traffic between applications using policies that you write. In order to write application policies, you must create rules for the policy.

- Policy is a new section in the left navigation

  The **Policy** section replaces **Rules & Rulesets** in the left navigation. The **Policies** page differs from **Rulesets and Rules** in the following ways:
  - Rule types appear in a list when you click **Add Rule**.
  - All rule types can now be added from a single page.
  - You can add and view Override Deny rules (see Override Deny Rules).
  - Rule types are listed in the order of their precedence.
  - Scope types are listed in a **Scope** category when you choose **Allow Rule**.
- Override Deny Rules

  NOTE
  - Override Deny rules require VEN release 22.3.0 or later.
  - Deny and Override Deny rules are implicitly Intra-Scope rules. Extra-Scope deny rules are not supported currently.

  This release introduces Override Deny rules. These are "without exception" deny rules that have precedence over all other types of rules and can't be overridden. Use Override Deny rules to block communication that should always be blocked. For example, if an administrator in your organization creates an Allow rule that would permit communication that should always be denied, having an Override Deny rule in place denying that communication serves as a safeguard.

  Override Deny Rules:

- Provide an additional type of granular control for blocking network traffic, helping to ensure that only explicitly authorized communications are permitted.
- Block traffic with a type of Deny rule that can't be overridden.
- Can be used in scoped and un-scoped rulesets.
- Impact the calculation of ransomware protection coverage and V-E scores.
- Support the Rule Hit Count
- Support compliance with stringent regulatory requirements by enforcing the principle of least privileged access.

Example

Suppose you want to block all traffic between your Production and Development environments except over splunk-data (9997 TCP) (existing capability). Additionally, you want to block all traffic between all workloads over SSH with no exceptions possible (highest precedence; new capability with this release).

1. Add a Deny rule specifying Production as the source and Development as the destination, blocking all services.
2. Add an Allow rule specifying the same source and destination, permitting traffic over splunk-data (9997 TCP).
3. Add an Override Deny rule blocking all traffic between all workloads over SSH. Because this role has the highest precedence, it can't be overridden by an Allow rule.

Appearance in Visualization tools

When Override Deny rules block or potentially block traffic in your environment, the policy decision is indicated in the Map and Traffic views in the Illumio Console.

Impact on key security measurements

Adding Override Deny rules to your security policy affects the calculation of the following security measurements:

- Ransomware protection coverage
- V-E score

- UI Updates for Extra-Scope and Intra-Scope rules
  - The separate tabs that contained Intra-Scope and Extra-Scope options in previous releases are removed and a new column called **Scope Type** appears in the **Allow Rules** section of the **Policies** page.
  - Extra-Scope and Intra-Scope rules occupy different sections within **Allow Rules**, separated by a gray line.
  - You can move rules up or down but only within their respective section.
  - Extra-Scope rules are now distinguished by an icon.
- "**Allow Rules Only**" is listed on some pages

  The badge "**Allow Rules Only**" appears in the following areas of the Illumio Console where only Allow Rules are listed. Illumio plans to list other rule types in those pages in a future release.
  - **Troubleshoot** > **Policy Check**
  - **App Groups** details page > **Rules** tab
  - **Policy** > **Policies** > **Rule Search** tab
- Get faster query results by turning off Aggregate Explorer Results

  If it's taking too long for query results to appear in the Map or the Traffic table, you can now try to speed things up by turning off **Aggregate Explorer Results** (which is on by default) through the **More** menu. Be aware that turning off aggregation means you may see more duplicate flows, which can result in a slight loss of fidelity in data reporting.

  1. Click **More**.
  2. Click **Aggregate Explorer Results** on the menu to turn it off/on.
  3. Click **Run**.
- Rule Hit Count

Beginning with this release, the Rule Hit Count feature is now available. Rule Hit Count is available only on Server and Endpoint workloads, and requires VEN 23.2.30 or later.

NOTE

Flows going to or coming from Cloud resources are not collected by the Rule Hit Count.

You can add a Rule Hit Count Report through the Illumio Console or through the Illumio REST API.

The Rule Hit Count Report provides the following:

- **Policy Compliance**: Generate a Rule Hit Count Report to provide evidence that security controls are in place and working effectively, demonstrating compliance to auditors.
- **Redundancy Removal**: Identify unused or less-used rules so you can remove or modify them to reduce redundancy and clutter in your implementation.
- **Troubleshooting**: When network issues arise, identify the rules that were in effect during the relevant traffic flow, allowing you to resolve problems faster and more efficiently.

Both Console and VENs require enablement through the Illumio REST API. For details and limitations, see About Reports.

Limitations in Release 24.22.x

- In the unified Map, label groups, IP lists, and CIDR blocks are not supported as Cloud flow filters.
- The number of Cloud flows is limited to 10,000 in addition to the number of Server and Endpoints configured in the Results Setting.
- Cross-datacenter flows between Cloud and Server & Endpoint workloads are subject to a scaled limit. Flows that are hybrid over that limit sometimes do not fully translate the IP address back into the workload or Cloud resources. So **Resource** > **IP Address** in Cloud flow and a Server flow with the same **IP address** > **Server workload** does not get mapped as **Cloud resource** > **Server workload**.
- Only label-based rules can be written for Cloud resources.
- Show Impact in Policies only supports Cloud resources.
- Unified Visibility and Policy are only available for organizations created on or after the 24.22 release. Organizations created before this release will be migrated in the future.

Resolved Issue in 24.22.0+UI3

- **Unable to run a traffic query to completion** (E-120198)

  During the “Loading” phase of running a traffic query, the page would become blank.

Resolved Issue in 24.22.0+UI2

- **Explore query does not complete** (E-119527)

  In some situations, running a query in Map or Traffic view failed to complete. The "**Run**" button would remain yellow (animated).

Known Issues in Release 24.22.0

- **Sometimes reverting the IP List from the details page keeps the page loading forever** (E-118620)

  Workaround: None
- **Right-clicking on the deleted workload group shows the ‘Add rule’ option while clicking on the Add Rule option getting navigation error** (E-118591)

The '**Add Rule**' and '**Expand Group**' options are not applicable when right clicking on '**Deleted workloads**.'

Workaround: None

- **Rules proposed for server to cloud flows not correct when writing rule entity to entity** (E-117893)

  Rules cannot be written directly for cloud resources. So when '**Allow selected connections**' is selected for cloud resources without labels, rules will not be written correctly. Only label-based rules can be written for cloud resources.

  Workaround: None

Illumio Console 24.21 What's New and Release Notes

Release Notes for Illumio Console 24.21

These release notes describe the new features and known limitations for Illumio 24.21.x releases.

NOTE

Illumio Console 24.21.0 is available for Illumio Cloud customers only.

Product Version

PCE Version: 24.21.0 (Illumio Cloud customers only)

Illumio Core release numbering uses the following format: “a.b.c-d+e”.

- “a.b”: Standard or LTS release number, for example, “2.2”
- “.c”: Maintenance release number, for example, “.1”
- “-d”: Optional descriptor for pre-release versions, for example, “preview2”

What's New in This Release

Illumio Console is the integration of the Illumio Core and Cloud products into the same platform. Now, with the right user permissions, you can access features of two Illumio products in one unified UI. The features of Cloud are available in the Cloud menu, and the features of Core are available in the Servers & Endpoints menu.

The following new features were added in Illumio Console 24.21.0:

Rule Hit Count for Illumio Core SaaS

Beginning with this release, the Rule Hit Count feature is now available for Illumio Core SaaS customers. (Requires VEN 23.2.30 or later).

You can add a Rule Hit Count Report through the Console UI or through the Illumio REST API.

The Rule Hit Count Report provides the following:

- Policy Compliance: Generate a Rule Hit Count Report to provide evidence that security controls are in place and working effectively, demonstrating compliance to auditors.
- Redundancy Removal: Identify unused or less-used rules so you can remove or modify them to reduce redundancy and clutter in your implementation.
- Troubleshooting: When network issues arise, identify the rules that were in effect during the relevant traffic flow, allowing you to resolve problems faster and more efficiently.

The PCE and VENs require enablement through the Illumio REST API. For details and limitations, see Rule Hit Count Report.

Policy is a new section in the left navigation

The **Policy** section replaces Rules & Rulesets in the left navigation.

NOTE

For now, the stand-alone Deny Rules page still appears in the left navigation but it's slated to be deprecated in a future release. If your Core instance was upgraded to release 24.2.x, Illumio recommends that you migrate your Deny rules from the Deny Rules page to the Policies page and add Deny Rules from the Policies page from now on.

The Policies page differs from Rulesets and Rules in the following ways:

- Rule types appear in a list when you click Add Rule.
- All rule types can now be added from a single page.
- You can add and view Override Deny rules (see Override Deny Rules).
- Rule types are listed in the order of their precedence.
- Scope types are listed in a Scope category when you choose Allow Rule.

Override Deny Rules

NOTE

- Override Deny rules require VEN release 22.3.0 or later.
- Deny and Override Deny rules are implicitly Intra-Scope rules. Extra-Scope deny rules are not supported currently.

This release introduces Override Deny rules. These are "without exception" deny rules that have precedence over all other types of rules and can't be overridden. Use Override Deny rules to block communication that should always be blocked. For example, if an administrator in your organization creates an Allow rule that would permit communication that should always be denied, having an Override Deny rule in place denying that communication serves as a safeguard. Override Deny rules:

- Provide an additional type of granular control for blocking network traffic, helping to ensure that only explicitly authorized communications are permitted.
- Block traffic with a type of Deny rule that can't be overridden.

Known Issues in Release 24.21.0

These known issues were reported previously in 24.12:

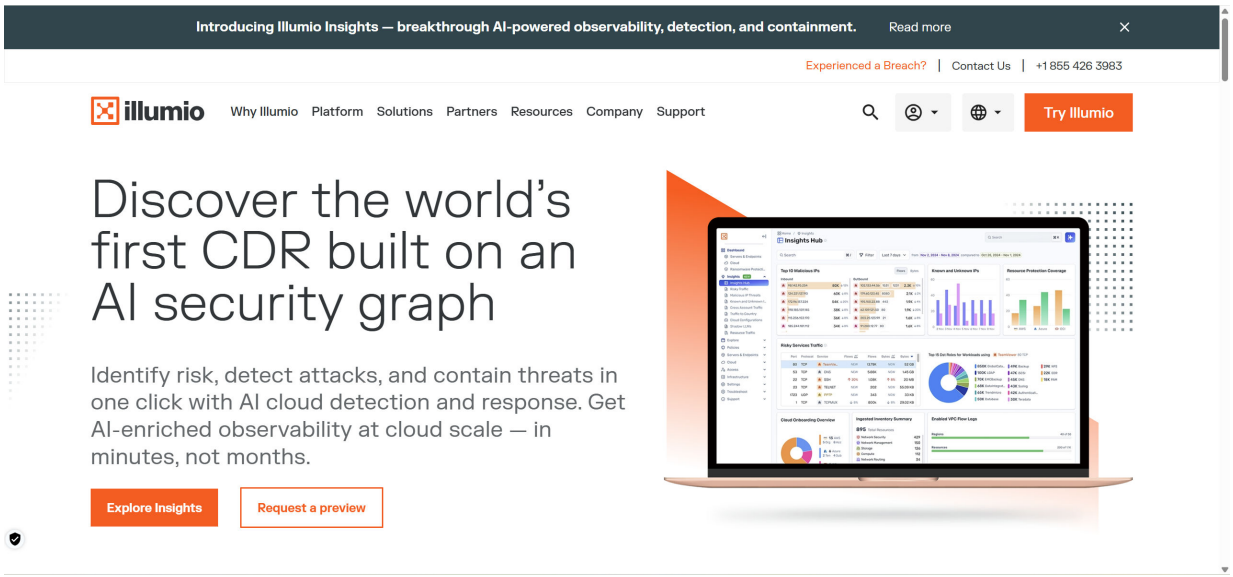
- Refused to connect to the support portal with segmentation templates > sign in (E-113084)
  Clicking on segmentation templates -> sign in the support portal returns an error.Workaround: none.
- Standalone PCE not starting up after service_discovery_encryption_key change (E-104880)
  Workaround: none
- Removal of inactive accounts ignores API use (E-103316)
  User accounts that have been inactive for more than 90 days are removed automatically. However, the active status is determined based only on whether the account has logged in to the web console UI. If the account is used only to issue API requests, it is counted as inactive and removed after 90 days.
- Updating max results in Illumination Plus (10K) updates the Explorer max results (E-102742)
  The maximum connection number in Explorer gets updated to the same maximum number as the update in Illumination Plus. However, the maximum number in Illumination Plus is 10,000, while in Explorer, it is 100,000.
  Workaround: Update the max results setting in Explorer to get more than 10K results.
- Secure Connect only logs the "E" on the destination (E-101229)
  Works as designed. There is no way to tell whether Secure Connect is in the egress path.
- Windows 11 shows as Windows 10 on the workload/VEN page (E-100844)
  Workaround: none.
- Flow timestamp incorrect in Explore Map for inbound-only or outbound-only reported flows (E-96595)
  The flow timestamp shown in the Explore Map for Servers and Endpoints is unreliable for ingress- or egress-only reported flows.
  Workaround: None

Introducing the Illumio Console

Illumio Console is the integration of the Illumio Core and Cloud products into the same platform. Now, with the right user permissions, you can access features of two Illumio products in one unified UI. The features of Cloud are available in the Cloud menu, and the features of Core are available in the Servers & Endpoints menu.

Set Up Illumio Console Account

To obtain an Illumio Console account, visit illumio.com and click the **Try Illumio** link.



Authenticating Users with OIDC

Users with the Owner role can add external users from identity providers (IdPs) that conform to the OpenID Connect (OIDC) protocol. Although you can authenticate with any OIDC-compliant IdP, Illumio has validated the following well-known OIDC applications:

- MS Entra ID (Azure AD)
- Amazon Cognito
- AuthO
- Okta
- SecureAuth

Integration with an OIDC-compliant application is your responsibility.

CAUTION

If you have multiple tenants, Illumio recommends that you use unique email domains to access each tenant on Illumio Console. Tie each tenant to a unique domain -- for example, to `example.com` for production and `test.example.com` for testing. Also, users must have their email addresses tied to these unique domains. This configuration lets Illumio Console correctly route authentication requests to the appropriate tenant based on the user's email address.

Customers using multiple tenants mapped to the same domain are advised to follow the these steps:

- Use OIDC configuration on one tenant to automatically redirect SSO requests to the Identity Providers.
- For additional tenants, either add them as local users or use unique email domains for them.

Configure external user authentication through an OIDC IdP

1. Go to **Access > Authentication**.
2. At the Authentication page, click the **OpenID Connect (OIDC)** tile.
3. On the OIDC page, several well-known identity providers are shown. Alternatively, you can use a different OIDC-compliant provider not listed here. Click the provider tile to see configuration information from that provider's documentation set.

   Alternatively, you can follow Illumio-specific configuration guidelines for these IdPs in the following topics:
   - Configuring Microsoft Entra ID (Azure AD) [40]
   - Configuring Amazon Cognito as an IdP [42]
   - Configuring AuthO as an IdP [42]
   - Configuring SecureAuth as an IdP [43]
   - Configuring Okta as an IdP [44]
4. Follow the configuration steps for your selected provider, either by following the information in the Illumio-specific topics or from the general information in that provider's documentation. Make sure to retain the Client ID and Issuer URL generated by whichever procedure you follow.
5. After you finish the external configuration at the OIDC-compliant IdP, enter the **Client ID** and **Issuer URL** provided by the IdP during your configuration procedure.

   Some IdPs use terms that are not obvious matches to the parameters you enter at the Illumio Console OIDC page. The following table matches the configuration terms used by some popular IdPs with their equivalent Illumio OIDC parameter settings.

IdP Provider	Client ID Equivalent	Issuer URL Equivalent
MS Entra ID	Application (client) ID	Directory (tenant) ID, used in: `https://login.microsoftonline.com/<tenant_id>/v2.0`
Amazon Cognito	Client ID	Token signing key URL, minus trailing `/.well-known/jwks.json`
AuthO	Client ID	The **Domain** value prepended with "`https://`" and appended with "`.us.auth0.com`"
SecureAuth	Client ID	Issuer URL
Okta	Client ID	Issuer ID value prepended with "`https://`"

6. Click **Enable IdP Logout** if you want users to be also logged out of their identity provider when they log out of Illumio Console.
7. Click **Save**.

Configuring Microsoft Entra ID (Azure AD)

Follow these steps to configure Microsoft Entra ID (formerly known as Microsoft Azure Active Directory) as an external identity provider (IdP) in the Illumio Console's Okta instance via OIDC protocol.

Prerequisites

Ensure that you have entered an email, first name, and last name in your user profile in your Azure AD instance. These fields cannot be empty.

Register Illumio as an application

1. Log into Entra ID (Azure AD).
2. In the Azure left navigation panel, click **App registrations**.
3. At the App Registrations page, click **New registration**.
4. At the Register an application page:
   a. In the Name field, enter a name for your Illumio Console instance. For example, "MyCorp on Illumio".
   b. For Supported account types, select **Accounts in this organizational directory only (Single tenant)** .
   c. Under Redirect URI, choose **Single-page application (SPA)** and enter the URI to Illumio Console: **https://console.illum.io**.
5. Click **Register**.

Additional configuration

After you have registered your Illumio Console application as an Entra application, you can see it listed when you click **App registrations**, then **All applications**.

1. At the **App registrations** page, click your application name (for example,"MyCorp on Illumio") to see more details.
2. At your application details page, click **Authentication**.
3. Confirm that you have entered the proper Redirect URI, and correct it if needed.

4. Under **Implicit grant and hybrid flows**, you must enable the **ID tokens** setting.

Save Configuration Parameters

1. At the details page for your Illumio Console application, click **Settings**.
2. Copy the Client ID setting shown there. You will use this as the **Client ID** setting when completing your OIDC authentication in the Illumio Console.
3. Copy the **Directory (tenant) ID** shown here. This ID will be used as the basis for the **Issuer URL** setting when completing your OIDC authentication in the Illumio Console, where you will enter the URL in the form: **https://-login.microsoftonline.com/*tenant_ID*/v2.0**.
4. Click **Manifest**, and at this page use the editor to update the following JSON entries to these values:

   ```
   "acceptMappedClaims": true
   "accessTokenAcceptedVersion": 2
   ```

   Instead of `accessTokenAcceptedVersion` you might see `requestedAccessTokenVersion`. Whichever entry is in your manifest, ensure that this entry is set to 2.

Configure tokens

1. Click **Token configuration**. At this page:
   a. Select **ID Token**.
   b. Click **Add optional claim**. Enable **email** and **upn** in the list of claims. If available, also enable the option to **Turn on Microsoft Graph email permission**.
   c. Click Add.
2. At the Token configuration page, confirm that both email and upn are listed under the Claim column, and they are Token type of ID.
3. Click **API permissions**.
   When you enabled Microsoft Graph earlier, API permissions should be turned on for email and profile.
4. Click **Microsoft Graph** under the API/Permissions name column, and enable the **openid** permission.
   The email and profile permissions should be enabled already.
5. Click **Add**.

Custom Claims Mapping

1. Go to your Entra ID Home, and click **Enterprise applications**.
2. From the list of your applications, click the name of your new Illumio Console application (for example, "MyCorp on Illumio").
3. At the details page for your Illumio Console application, click **Properties**. Ensure that the **Assignment required?** option is set to **Yes**. This setting ensures that when a user logs in, the user is assigned to the target Entra ID application.
4. Click **Single sign-on** from the left navigation. At the OIDC-based Sign-on page, under the Attributes and Claims section, click **Edit**.
5. On the Manage claim page, enter new claims for firstName and lastName:
   a. Enter the Name (for example, **firstName**).
   b. Set Source to **Attribute**.
   c. In Source attribute, choose the menu item **user.givenname** for thefirstName claim, and **user.surname** for the lastName claim.
   d. Leave all other options at default values or unspecified.
   e. Click **Save** after completing each claim.
6. The next time you log into the Illumio Console, a Microsoft window requests you grant permission. Click **Accept**.

Configuring Amazon Cognito as an IdP

Follow these steps to configure Amazon Cognito as an external identity provider (IdP) in the Illumio Console's Okta instance via OIDC protocol.

1. Go to the Amazon Cognito console (`https://console.aws.amazon.com/cognito/home`). If prompted, enter your AWS credentials.
2. Create a user pool by clicking **Create user pool**. You might need to select **User Pools** from the left navigation pane to reveal this option.
3. In Configure sign-in experience, under Cognito user pool sign-in options, select **Email** only, and click **Next**.
4. In Configure security requirements:
   a. Under Multi-factor authentication, choose **No MFA**.
   b. Under User account recovery:
      i. Select **Enable self-service account recovery**.
      ii. Select **Email only** for Delivery method for user account recovery messages.
   c. Click **Next**.
5. In Configure sign-up experience, determine how a new user verifies their identity when signing up.

   Under Required attributes, confirm that **email** is specified, and from the Additional required attributes menu, select **family_name** (surname) and **given_name** (first name).
6. In Configure message delivery, choose the settings you prefer. Note the prerequisites for sending email with Amazon SES.
7. On Integrate your app:
   a. Enter a name in **user pool name**.
   b. Under Initial app client, confirm that App type is set to **Public client**.
   c. Enter a name in **App client name**.
   d. Under Client secret, you can choose whether you want to generate a client secret or not.
   e. Expand **Advanced app client settings**, and under this section set up various client app authentication flows:
      i. For Authentication flows, choose **ALLOW_USER_SRP_AUTH**.
      ii. Choose a session duration and the various token expirations as you wish.
      iii. Under the optional Advanced security configurations, we recommend **Enable token revocation** and **Prevent user existence errors**.
   f. Click **Next**.
8. At Review and Create, review your user pool details, and when satisfied click **Create user pool**.

Configuring Auth0 as an IdP

You can use Auth0 as an external Identity Provider (IdP) through the OIDC protocol support provided in Illumio Console.

Auth0 configuration

1. Log in to your Auth0 account.
2. In the left navigation pane, click **Applications > Applications**.
3. Click **Create Application**.
4. In the Create application window:

   a. Enter a **Name** for your Illumio instance.
   b. For Choose an application type, click **Single Page Web Applications**.
   c. Click **Create**.
5. At the wizard page that asks What technology are you using for your web app? click **React**.
6. At the wizard Settings tab for your new application, under the Basic Information section copy the **Client ID** and **Domain** values generated for your Illumio app. (The Domain value is the basis for your Issuer ID.)
7. Scroll down to the Application URIs section, and enter the correct callback URL in the **Allowed Callback URLs** field.
8. Click **Save** at the bottom of the page.

Finishing configuration at Illumio Console

After generating and copying the Client ID and Domain at the Auth0 website, return to the OIDC page in the Illumio Console, and complete the IdP configuration as described in Authenticating Users with OIDC [38].

1. In **Client ID**, enter (or paste) the **Client ID** generated when configuring your web app on Auth0.
2. In **Issuer URL**, enter (or paste) the **Domain** value that you also generated at Auth0, and prepend the value with "`https://`" and append the value with "`.us.auth0.com`".

   For example, a **Domain** value of `my-1a2b3c4d5e6f7g` is entered as **https://my-1a2b3c4d5e6f7g.us.auth0.com** in the **Issuer URL** field.

Configuring SecureAuth as an IdP

Follow these steps to configure SecureAuth as an external identity provider (IdP) via OIDC in your Illumio Console instance.

NOTE

Review SecureAuth documentation here: OpenID Connect and OAuth 2.0 configuration.

1. Log into your SecureAuth account.
2. Click **Applications** > **Clients** in the left navigation pane.
3. Click **Create Client** in the `Client Applications` page.
4. At the `Create Application` page:
   a. Enter **Application Name** (such as `Illumio Console for MyCorp`).
   b. Enter your application URL (`https://console.illum.io/`).
      This field can be left blank if mentioned as Optional in the SecureAuth console.
   c. Select **Single Page** for **Application Type**.
   d. Click **Create**.

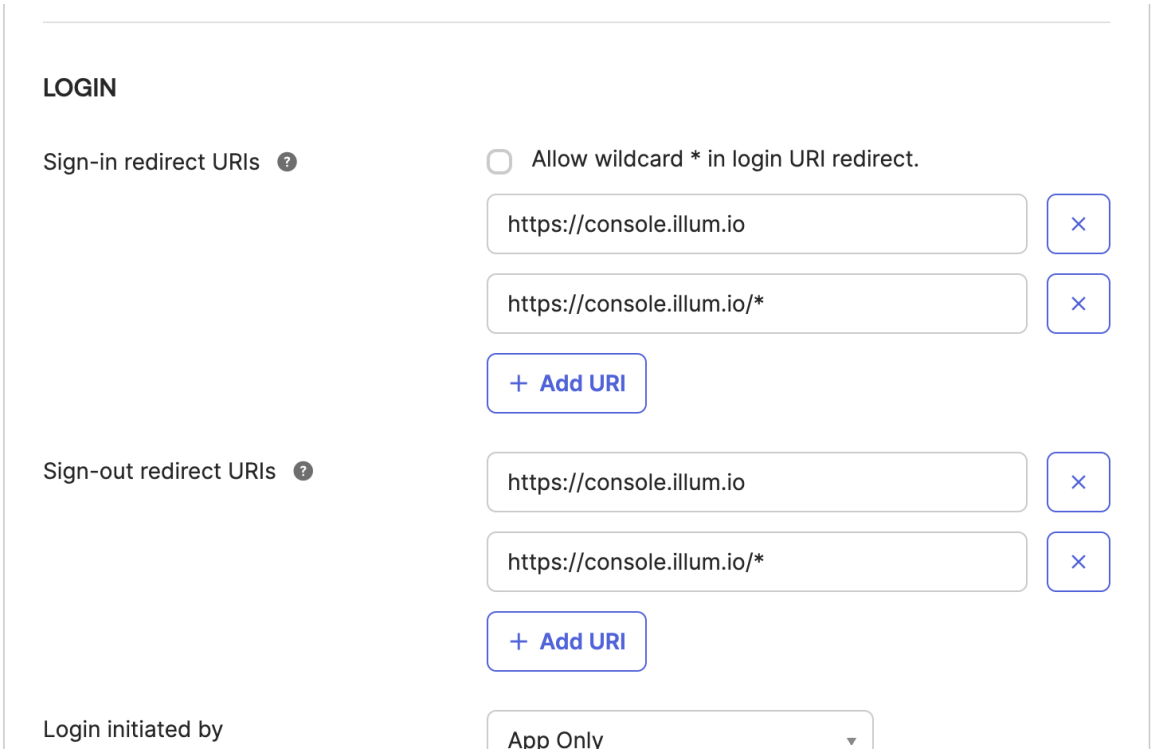
   SecureAuth shows your assigned Client ID and Issuer URL.
5. Enter in both **Redirect URI** and in **Post-Logout Redirect URIs** the URL to Illumio Console, `https://console.illum.io`, and **Save** each entry.
6. Click **Claims** in the left navigation pane.

7. Click **Add Claim** at the `Claims` page.
8. Add the email claim at the `Add claim` dialog:
   a. In **Name**, enter `email`.
   b. In **Source type**, choose **AuthN Context**.
   c. In **Source path**, choose **Email**.
      The **Scopes** field shows the `email` claim.
   d. Click **Add** to finish.

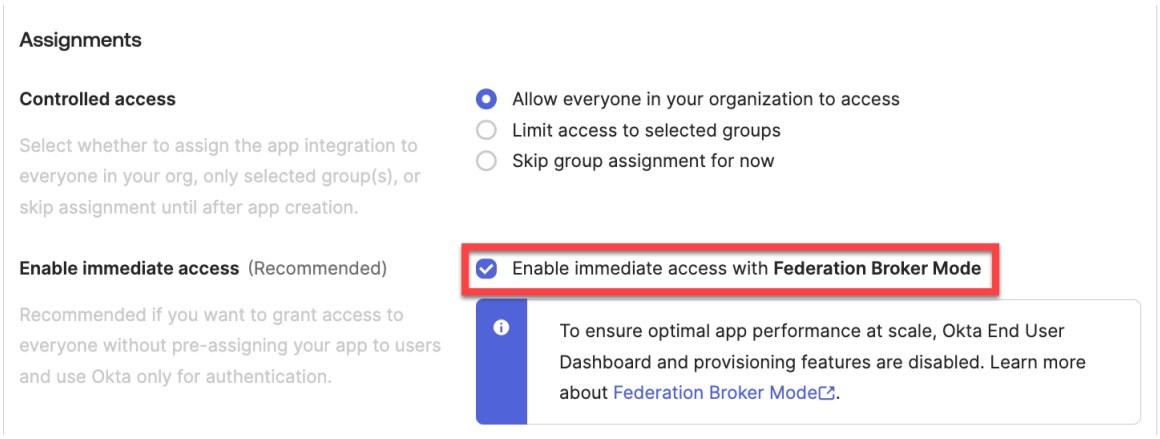
Configuring Okta as an IdP

Follow these steps to configure Okta as an external identity provider (IdP) via OIDC in your Illumio Console instance. Okta can be used as an IdP for both local users and external groups in Illumio Console.

1. Log into your Okta account.
2. From the left navigation pane, click **Applications** > **Applications**.
3. At the Applications page, click **Create App Integration**.
4. In the **Create a new app integration** popup:
   a. For **Sign-in method**, choose **OIDC - OpenID Connection**.
   b. For **Application type**, choose **Single-Page Application**.
   Click **Next**.
5. Under the **Login** section, click **Add URI**, and enter the **Sign-in redirect URI** as `https://console.illum.io/*`, making sure to append the asterisk wildcard.

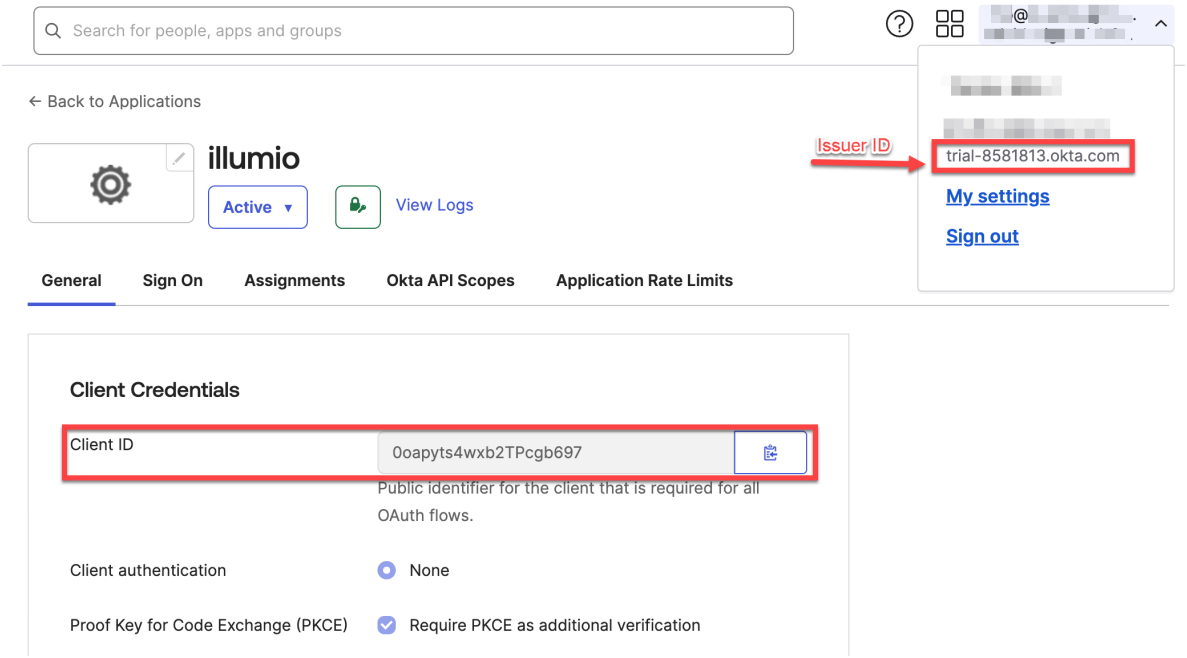


   This value is used by Okta to allow a browser redirect from the Illumio application to Okta.
6. Select your Granted Access.
7. Click **Save**.
8. Scroll to the bottom of the page, and under the **Assignments** section, disable **Federation Broker Mode** by clearing the checkbox.



Click **Continue** at the **Disable Federation Broker Mode?** confirmation popup.

9. Click **Save** at the bottom of the page to save your authorization application.
10. On the details page for your new application, the General tab now shows the **Client ID** and **Issuer ID** values for the application. The *Issuer URI* consists of the Issuer ID with "`https://`" added in front of it. In the example shown below, the Issuer URI is **https://trial-8581813.okta.com**.



Copy the Client ID and Issuer URI values because you must enter them when you finish configuring the authentication at the Illumio Console OIDC page (**Access** > **Authentication**). See Authenticating Users with OIDC [38]. You will also use the Client ID when you update the Authorization Server [46] for this application, later in this procedure.

Additional information about your OIDC Application (or assigning users to your Okta IdP App for Illumio Console)

After creating and configuring an Okta App to serve as an IdP for your Illumio Console instance, you can assign People and Groups to the app. These appear in Illumio Console as external users and external groups, respectively.

1. At your Okta application details page (**Applications** > **Applications**), click **Assignments**.
2. List people to add. Either click **People** under the **Filters** heading , or click the **Search** field, Choose **People** from pull-down menu and enter a specific name in **Search**.

3. Assign the **Everyone** group to your Okta app.
   You must assign the Everyone group, to ensure the People type of Individual can properly access the application, and therefore access the Illumio Console it is configured to.

Update Authorization Server

1. In left navigation pane, go to **Security** > **API**.
2. Click **Authorization Servers** tab.
3. Click **Add Authorization Server**.
4. Click the pencil icon to edit the default API.
5. On the details page for the `default` API, at the **Settings** tab, enter in the **Audience** field the **Client ID** value of your OIDC application you created earlier.
6. Click **Save**.
7. Click **Claims** tab, to add the following claims to the ID token:
   a. Add **groupNames** claim, with value type **Groups**.
   b. Add **firstName** claim, with value type **Expression**, and value **user.firstName**.
   c. Add **lastName** claim, with value type **Expression**, and value **user.lastName**.

Add a Trusted Origin

1. In left navigation pane, go to **Security** > **API**.
2. Click **Trusted Origins** tab.
3. Under **Filters**, choose **Redirect**.
4. At the **Add Origin** popup, complete the following entries:
   a. **Origin Name** -- of your Okta app
   b. **Origin URL** -- https//www.illium.io
   c. **Cross-Origin Resource Sharing** (CORS) -- Enable
   d. **Redirect** -- Enable
5. Click **Save**.

Using MS Entra ID to Add External Groups

You can use Microsoft Entra ID as an OIDC-compliant Identification Provider (IdP) for external groups in your Illumio Console instance. (Note that Azure Active Directory (AD) is now named Microsoft Entra ID.) You can then add the group and its members to Illumio Console. What are called *users* in an Ilumio Console group are called *members* of an Entra ID group.

First create a new group in the Entra ID application that you have previously created for your Illumio Console instance, add owners and members (users) for the group, and then set some basic configuration values.

Prerequisite: You have an Entra ID account, and have set up an Enterprise application on it to serve as the IdP for your Illumio Console instance.

Add Roles and Groups to an Entra ID Application

Create a role for your Entra ID Enterprise application that maps to a user role in Illumio Console,

1. Log in to the Entra ID (Azure) account for your Enterprise application.
2. From **Home** on the left navigation pane, go to the application page of your enterprise application for Illumio Console.
3. Under **Manage**, click **App roles**.
4. At the **App roles** page, click the **Create app role** link (near the plus sign).
5. At the **Create app role** pane, enter:
   a. **Display name**
   b. For **Allowed member types**, select **Users/Groups**
   c. **Value**
      Remember this value, because this is also entered as the Claim value when adding the external group in Illumio Console.
   d. **Description**

   Also enable the checkbox for **Do you want to enable this app role?**

Adding a New External Group and Users in Entra ID

1. Log in to the Entra ID (Azure) account for your Enterprise application.
2. Go to the **All Groups** page: Either in left navigation pane follow **Access** > **Users and Groups** > **Groups** > **All Groups**, or `Search` for "groups" using the search bar, and click the "Groups" results with the icon next to it.
3. Click **New Group**.
4. At the **New Group** page, enter the following:
   a. Group type - Use **Security**.
   b. Group name
   c. Optional Group description
   d. **Owners** of the new group by clicking the link:
      i. At the **Add Owners** page, use **Search** to find Entra ID users.
      ii. Select the checkbox for one or more users to be assigned as an owner of this group.
      iii. Click **Select** when satisfied with the users listed on the far right panel as group owners.
   e. **Members** of the new group by clicking the link:
      i. At the **Add members** page, use **Search** to find Entra ID users.
      ii. Select the checkbox for one or more users to be assigned as members of this group.
      iii. Click **Select** when satisfied with the users listed on the far right panel as group members.

   After selecting Owners and selecting Members, click **Create**.
5. Go to your Enterprise application for Illumio Console.
6. In the left navigation pane, under **Manage** , click **Users and groups**.
7. At the **Users and groups** page, click **Add user/group**.
8. At **Add Assignment**, click **Users and groups**.
9. At **Users and Groups** page, click the **Groups** tab to see all groups, or use **Search** to find a specific group, like the one you just added.
10. Select the checkbox for each group to be assigned to your organization application.
11. Click **Select** when satisfied with the group or groups listed on the far right panel.
12. Click **Assign**.

    The **Users and groups** page lists the group or groups you assigned (that is, *added*) to your application.
13. At the **Users and groups** page, click **Add user/group**.

14. Search for your group name, and select it.
15. At the **Edit Assignment** page, click Select a role.
16. In the **Select a role** pane, click on the app role you create earlier, and click **Select**.

    At the **Users and groups** page for your application, the new group is listed as a Group object type, and has the role you just assigned to it. Users in this group will inherit access to this OIDC application.
17. In the left navigation pane, under **Manage** click **Single sign-on**.
18. In the **Attributes & Claims** section, click Edit.
19. Add a new claim at the **Manage claim** page, by entering:
    a. **Name**: groupNames
    b. **Source**: Attribute
    c. **Source attribute**: user.assignedroles

Add Permissions to an Entra ID External Group

1. Log in to the Entra ID (Azure) account for your Enterprise application.
2. Click **Security** > **Permissions** in the left navigation pane.
3. At the **Permissions** page, click **Grant admin consent for <*your_ilo_org*>**, where <*your_ilo_org*> is the name of your Illumio Console organization.
4. At the sign in prompt, enter your login credentials.
5. At the **Permissions** page, click the **Application registration** link.
6. At the **API permissions** page, under the **Configured permissions** heading you should see a green checkmark next to "**Grant admin consent for <*your_ilo_org*>**," which confirms the admin consent was activated.

Using Okta to Add External Groups

Prerequisites: Create an account on Okta, and create an authorization application there for your Illumio Console instance. For details, see Configuring Okta as an IdP [44].

NOTE

When you create your Okta authorization application for your Illumio Console instance, make sure to copy and save the Client ID and Issuer URL values that are generated for your Okta application.

When you add an authorization server to your Okta application, make sure to add the following claims to its ID token (at **Security** > **API** > **Add Authorization Server** under the **Claims** tab):

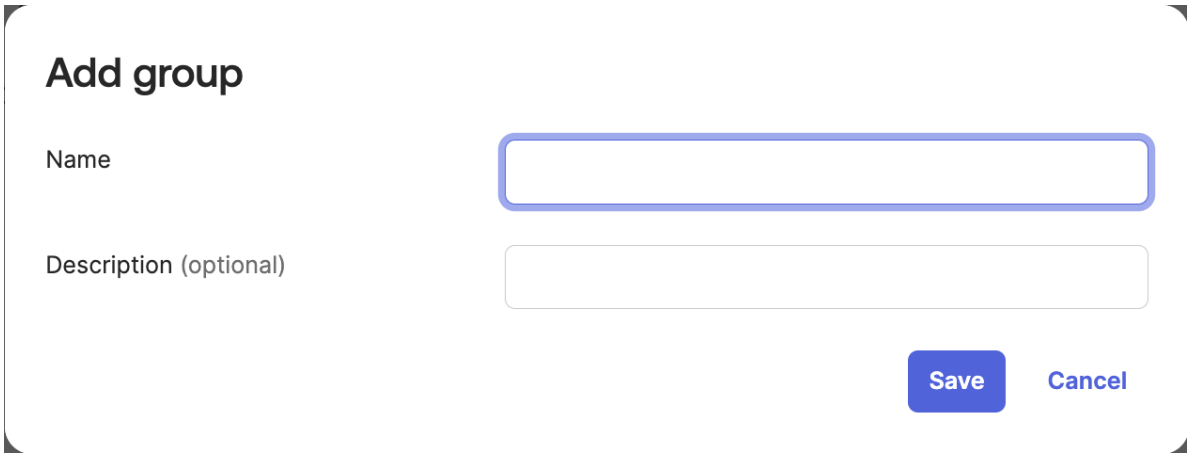
- **groupNames** (with value type `Groups`)
- **firstName** (with value type `Expression`, and value `user.firstName`)
- **lastName** (with value type `Expression`, and value `user.lastName`)

Follow this workflow to configure Okta as the IdP for your external groups:

1. Create a group in Okta [49]
2. Add a user and assign the user to a group [49]
3. Assign the application to the group [50]
4. Configure OIDC in the Illumio Console authentication settings [50]
5. Add the new external group and specify the claim [51]

Create a Group in Okta

1. Log into your Okta application
2. Go to **Directory** > **Groups**.
3. Click **Add Group**.
4. Enter a **Name** and an optional **Description**.



   Use this Okta application group Name when you add this external group to your Illumio Console [51].
5. Click **Save**.

Add a User and Assign the User to an Okta Group

Log into your Okta application and add users into your Okta group.

1. Go to **Directory** > **People**.
2. Click **Add Person**.
3. At the Add Person popup, enter the user details, and click **Save**.
   You can continue to add users by clicking **Save and Add Another**.
4. Click **Directory** > **Groups**.
5. Click the new group you just created in Create a Group in Okta [49].
6. Click the **People** tab, and assign people.
7. Use Search to find the new user or users you created and click **Assign people** to assign them to this group.

Assign the Application to an Okta group

IMPORTANT

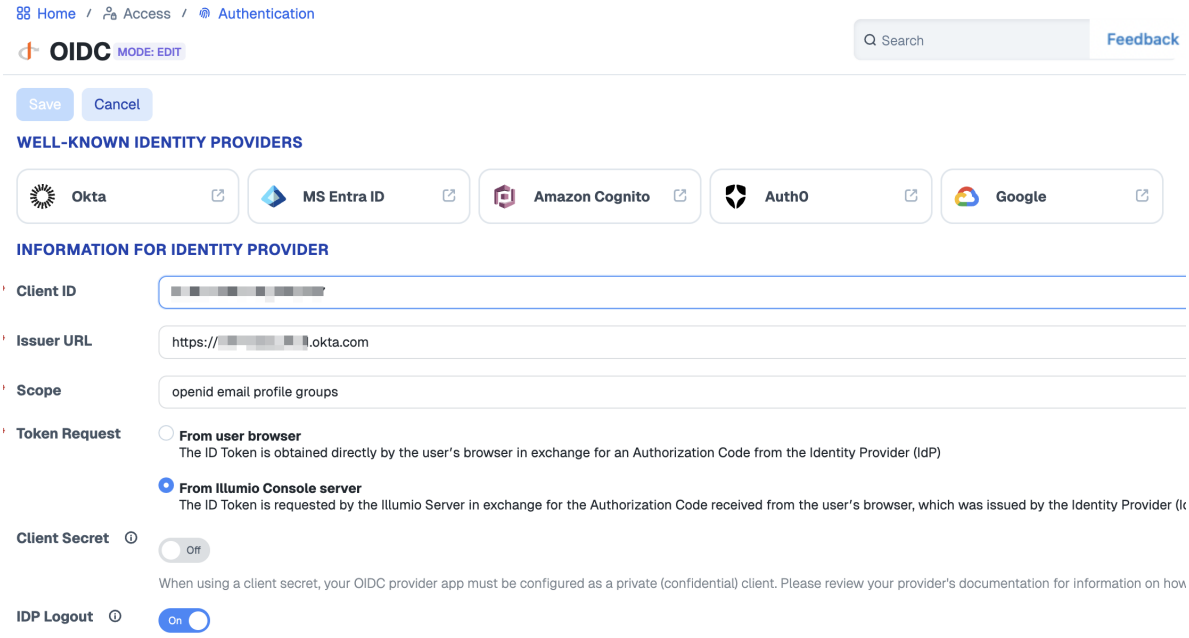
Prerequisite: Make sure you have already created an enterprise application in Okta for your Illumio Console instance.

1. Click **Directory** > **Groups**.
2. Click the group that you created in Create a Group in Okta [49].
3. Click the **Applications** tab.
4. Click **Assign Applications**.
5. Use **Search** to find your application and click **Assign applications**.
6. Click **Done**.

Configure OIDC in the Illumio Console Authentication Settings

The first action at Illumio Console is to configure the Console for Okta as an OIDC-compliant IdP.

1. Log into Illumio Console.
2. Click **Access** > **Authentication**.
3. Click **OIDC Authentication**.
4. In **Identity source**, choose **Okta**.
5. Under **Information for Identity Providers**, enter details for this Okta configuration:



a. **Client ID** - Enter the Client ID generated by Okta when you created your Okta Application for Illumio Console.
b. **Issuer URL** Enter the Issuer ID generated by Okta when you created your Okta Application for Illumio Console.

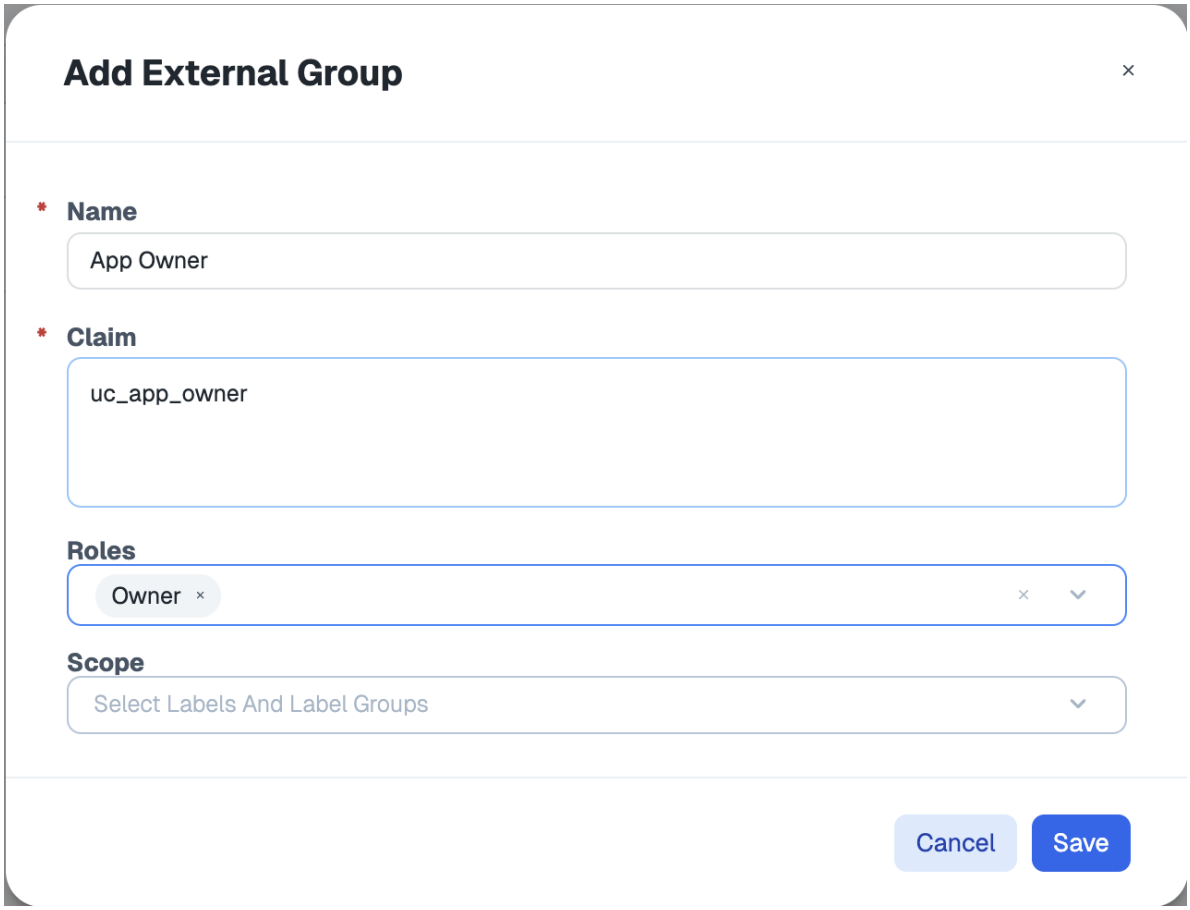
c. **Scope** - You must enter **openid email profile groups**.
d. **Token request** - Choose **From Illumio Console server**.
e. **Client secret**
f. **IdP Logout**

6. Click **Save**.

Add an External Group to Illumio Console and Specify Claims

Next, add the specific Okta group as a Console external group.

1. Log into Illumio Console.
2. Click **Access** > **External Groups**.
3. Click **Add**.
4. Enter the external user group details.



a. **Name** - Enter a name for this external group as it will appear in your Illumio Console. This is *not* the name you gave the group in Okta.
b. **Claim** - Enter the group Name you entered when adding the group to your Okta application [49].
c. **Roles** (optional)
d. **Scope** (optional)
e. Click **Save**.

Insights into Risky Ports

Illumio Platform now provides insights into Risky Ports across your network. The Risky Ports insight helps network administrators easily identify and analyze traffic flows that have been detected on risky ports between IP Lists on the network. Use these insights to proactively manage and mitigate potential security risks by having detailed visibility into the source, destination, traffic volume, and other details of these ports.

Launching Risky Ports Insights

1. From **Home**, click **Insights**.
2. From the carousel, click the **Traffic on Risky Ports** tile.
   Risky port traffic is shown in a summary table .

Risky Ports Summary Table

The risky ports table summarizes an aggregate of active risky ports, initially sorted by amount of traffic flow that changed over the time period or periods shown next to the table heading. Aggregated flows are based on IP Lists, which can include any lists defined by you.

New customers will have default IP Lists of "Corporate Network" (as defined in RFC 1918) and “Multicast.” These default IP Lists provide quick time-to-value by capturing any traffic on Risky Ports, even if a new customer has not defined any custom IP Lists yet.

By default, traffic is collected over the most recent seven-day period, aggregated, analyzed, and then characterized by risk.

You can also compare traffic that was analyzed between two timeframes. For example, compare traffic observed during a Aug 4 - Aug 10 timeframe with traffic observed during a July 28 - August 3 timeframe. The change in traffic between the two timeframes is shown as a percentage next to the aggregated amounts.

Change timeframes by clicking on a date range shown next to the table heading, and in the popup menu select the desired timeframe. Also use this menu to filter results by other characteristics, such as Traffic Type, Source, Destination, or Port/Protocol.

Traffic is shown in table columns:

- **Traffic Type** - Shows status of the aggregated traffic: Allowed, Blocked, or Mixed
- **Source** - Based on defined IPlist
- **Destination** - Based on defined IP List
- **Services** - Risky ports and protocols listed here are those defined under the Policies menu, which are also used by the Ransomware dashboard.

- **Flows** - Total count of flows, both in and out between Source and Destination. If two time-frames are defined, the percentage change that occurred over the specified time periods is also shown here.
- **Bytes** - Total count of bytes, both in and out between Source and Destination, If two time-frames are defined, the percentage change that occurred over the specified time periods is also shown here.

By default, traffic is sorted by Flow amount (most to least), which you can change. Alternatively, you can sort by Traffic Type or Bytes.

Caveats

- "No Rule" ports are shown in this Insight as an "Allowed" Traffic Type.

Cloud Resources Displayed in Map View

Illumio Console now allows you to view Illumio Cloud and Illumio Core resources on the map regardless of whether or not these resources have traffic. Hover over the button in the interaction panel to switch between the display modes.

Context Menu Filters for Cloud Resources

Illumio Console now allows you to hover over a resource and add filter criteria from the context menu. This feature is available on the **Traffic** page and on the **Traffic** tab within the Map page. For example, within the **Traffic** table, if you want to search for traffic that uses TCP 443 as the service, hover over 443 TCP to select Port and/or Protocol as the type. Next, select **Service is** from the context menu to add 443 TCP to the **Service** field as a filter. If you want to add to your query so that it excludes traffic from the uswest2 region, hover over a Cloud resource in the **Destination** column, hover over uswest2, and then select **Source is not** from the context menu to exclude traffic from that region from your search.

The context menu filters function similarly within the **Map** page except that you would click a traffic link between Cloud resources and then hover over the resource in the **Traffic** tab to begin adding values to include or exclude from your query.

The query filters that display in the context menu depend on which operators you select from the **More** menu and whether or not you select **Show Exclusion Filters**.

You can filter by the Account ID, Resource Type, Region, and Cloud/Data Center categories.

About the Illumio Virtual Advisor

Illumio Virtual Advisor (IVA) helps you understand your risk exposure by using natural language questions to generate quick answers and actions to reduce your risk.

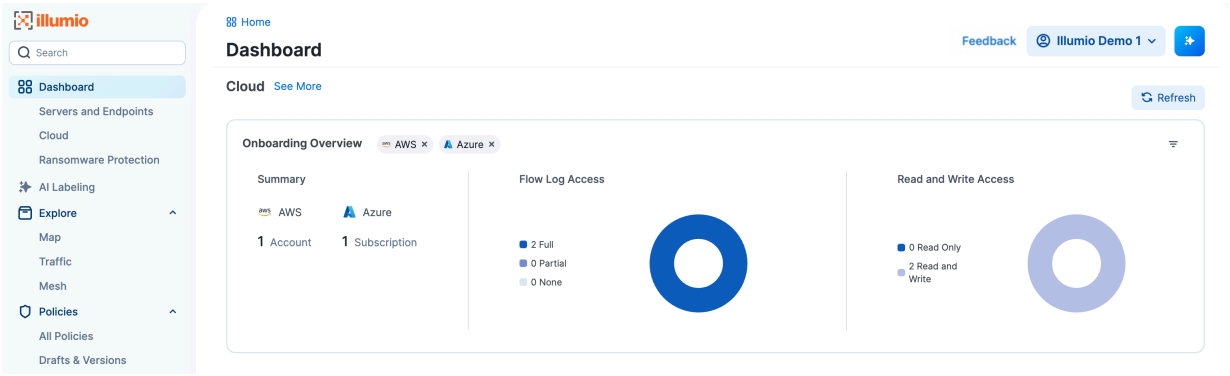
- Use IVA to visualize all traffic from a compromised server so you can take quick action to stop the risk. You can also use IVA to see all traffic from risky ports so you can preempt and prevent breaches.

- Illumio's AI-powered zero trust segmentation helps enhance workload visibility and ensure more proactive segmentation controls so you can stop attacks before they happen
  - Illumio does this with actionable guidance, automated labeling, and robust policy recommendations.
  - By reducing the time and effort required to operate a Zero Trust Segmentation platform, Illumio empowers organizations to respond to the threat of AI-powered attacks by containing spread and getting insights faster.
- Illumio's AI-powered segmentation strengthens cyber resilience by minimizing the attack surface
  - Complex tasks like labeling and policy creation are automated so that you can receive actionable guidance to ensure continuous protection. The internal attack surface is minimized with segments and policies that are identified automatically to protect against threats.

IVA can answer questions related to Illumio products and provide best practices recommendations to improve security based on feedback and questions generated from Illumio support.

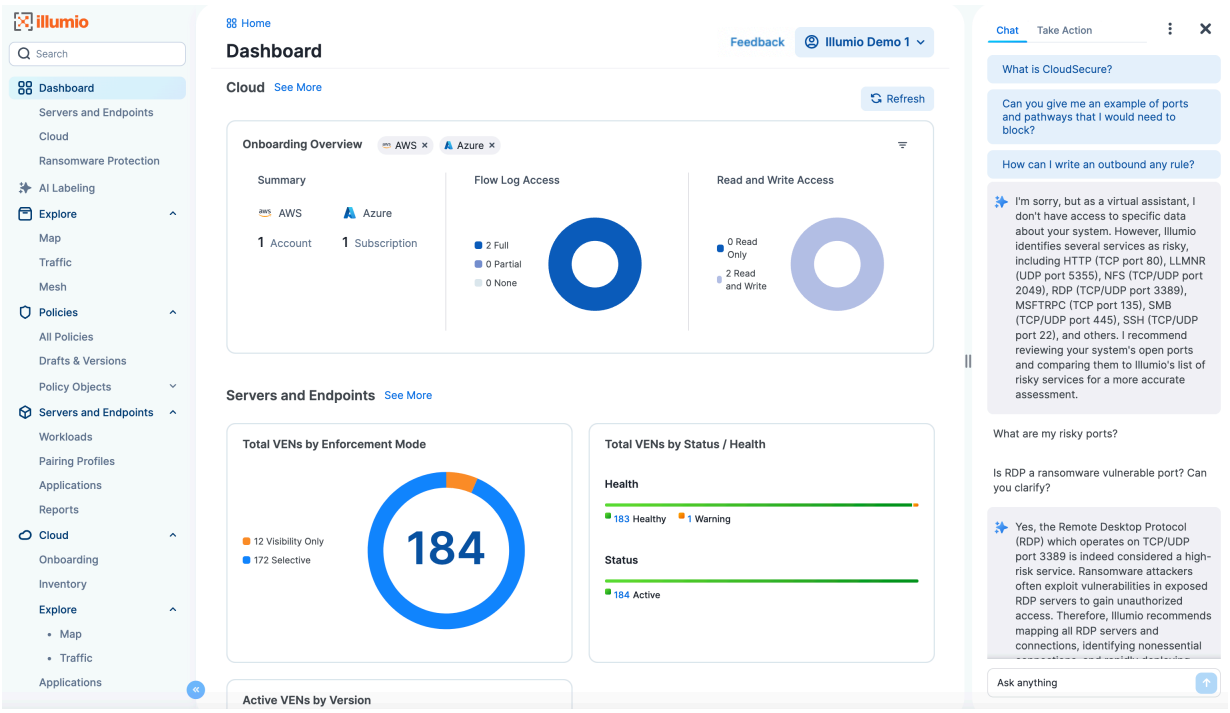
Use IVA

1. Click the IVA located next to your name on the top, right side.
2. Ask general questions in the Chat tab, or ask specific questions about maps and web traffic in the Take Action tab.

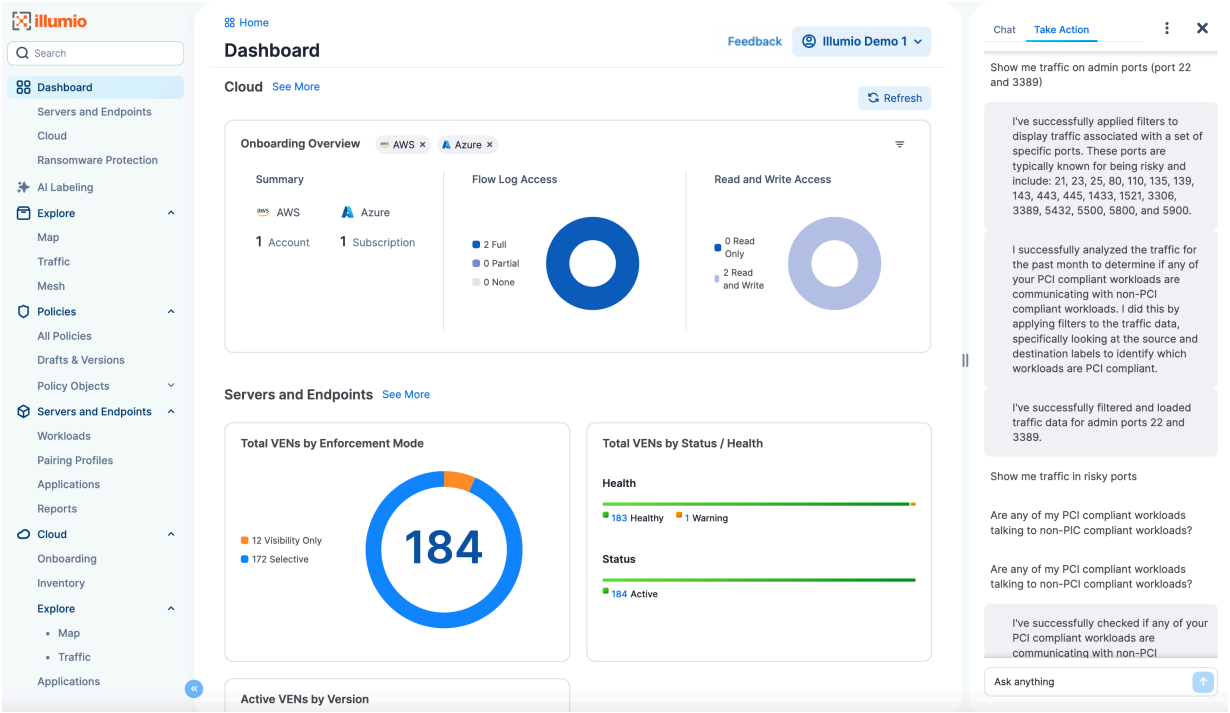


You can view information in two tabs:

- Chat view: Ask general questions and IVA provides an answer using natural language processing.



- Take Action view: This applies to questions related to Maps and Traffic only. For example, "Show me all web traffic in my production environment for the past week." Based on your input, IVA will set appropriate filters such as specific ports and generate web traffic data.



Best Practices

- Ask questions in the Support tab, not in the Take Action tab, and vice versa
- Ask questions related to Illumio or information security

- Ask questions related to the feature you have active in the UI. Asking Core-related questions while you are in a Servers and Endpoints feature will give you inaccurate answers.
- Use the Take Action tab for things related to the feature you have active in the UI. For Servers and Endpoints, the Take Action tab is available on the Map and Traffic pages. For Core, the Take action tab is available on the Cloud Map and Traffic pages.
- Ask questions that are 50 words or fewer in length
- Ask no more than seven questions per minute, per tenant, for best performance
- Filters support AND with the following terms:
  - Cloud Map and Cloud Traffic:
    - Cloud
    - Regions
    - Account ID
    - Resource Type
  - Maps and Traffic (Servers and Endpoint):
    - Source: labels
    - Destination: labels
    - Service port and protocol
    - Time Range

NOTE

Transparency Notice: Illumio confirms that Customer Data processed through the Illumio Virtual Advisor feature (IVA) will not be commingled with the data of other customers. It will remain logically separated to ensure data integrity and confidentiality and will not be used to train a large language model.

Customer Data will only be used within the bounds of the customer's instance and strictly for the purpose of the Company providing the IVA feature to Customer. This includes the operation, maintenance, support, and improvement of IVA, but does not include use for any other purposes without Customer's explicit consent.

The Customer agrees that any output of IVA is merely a suggestion or recommendation to be taken under advisement by the Customer and must be independently reviewed, verified, and assessed for accuracy by the Customer.

Saved Settings Persist Across Sessions

User preferences and settings are now maintained across sessions within Illumio Console. Previously, when users logged out of the application, their settings were lost, but the information is now stored on the server side in k-v pairs.

View Inherited Rules

A new **View Inherited Rules** button has been added to Illumio Console. This feature allows you to see organization policies and application policies rules that apply to the application you are viewing. If an application has inherited rules, a **View Inherited Rules** button displays

in the top-right corner of the **Application Policies** page for that application, with a badge that displays the number of inherited rules. This feature allows you to see other applications that have written rules that allow them to communicate with your application. For example, the **Inherited Rules** page for your CRM application could show you that the Finance application has an outbound rule that allows it to communicate to your CRM application.

To view inherited rules:

1. Navigate to **Policies > Application Policies** or **Policies > All Policies** and drill down on an application.
2. Click the **View Inherited Rules** button in the top-right corner of the **Application Policies** page.
3. Within the **Inherited Rules** detail page for the application, click the **Organization Policies** or **Application Policies** tabs to view details about the inherited rules.
4. If the application has inherited multiple rules for **Override Deny Rules**, **Allow Rules**, and **Deny Rules**, expand the pane to view the details for each rule.
5. Click the **Go to Policy** button to return to the details page for the application.

Note that if users do not have the appropriate role to view inherited rules, when they click the **View Inherited Rules** button, the application will display the Cloud Dashboard page.

View Provisioning Errors

The **Provisioning errors** button is available in the **All Policies**, **Organization Policies**, and **Application Policies** tabs. If you attempted to provision a policy but the policy did not successfully provision, click **Provisioning errors** to display the **Provisioning errors** page. This page provides more information about the application and organization policies that didn't provision and displays the cloud, the name and ID, the status, and the modification date for the policies that failed to provision.

Scopes

Illumio Console includes several roles that grant users access to perform operations. Scoped roles allow users to perform operations within a defined scope. You can add users (local and external) and groups to all roles.

Roles with Global Scopes

These Global Roles use the scope All Applications, All Environments, and All Locations. You cannot change the scope for these roles. The roles have the following capabilities in Illumio Console.

Role	Granted Access
Owner	Perform all actions: add, edit, or delete any resource, security settings, or user account.
Viewer	View any resource or organization setting. Viewers can perform only view operations.
Provisioner	Provision policy objects, such as IP lists, services, and label groups. They cannot provision policies, virtual services, or virtual servers. Neither can they add, modify, or delete existing policy items. View all other resources.

Roles with Custom Scopes

You can apply the following roles to specific scopes. These roles are called *Scoped Roles*.

Role	Granted Access
Ruleset Manager	• Add, edit, and delete all policies (rulesets) within the specified scope. • Add, edit, and delete rules when the destination matches the specified scope. The rule source can match any scope.
Limited Ruleset Manager	• Add, edit, and delete all policies (rulesets) within the specified scope. • Add, edit, and delete rules when the destination and source match the specified scope. • Ruleset Managers with limited privileges cannot manage rules that use IP lists, custom iptables rules, user groups, label groups, iptables rules as sources, or have internet connectivity.
Ruleset Provisioner	Provision policies (rulesets) within the specified scope.
Ruleset Viewer	Read-only access to policies (rulesets) within the specified scope. Cannot edit policies or rules.
Workload Manager	Manage workloads and pairing profiles within the specified scope. Read-only access provided to all other resources.

Example Scoped Role Use Cases

Consider the following use cases for two of the scoped roles described in the Roles with Custom Scopes topic -- the Workload Manager and the Limited Ruleset Manager.

Workload Manager Role

The following use cases describe scenarios that are well-suited for the solution of the Workload Manager role.

- Use Case 1

  You want to use scripts in your development environment to programmatically spin up and bring down workloads; your scripts create pairing profiles and generate pairing keys without you granting elevated Admin privileges to the scripts.
- Use Case 2

  Your application teams are in charge of changing the security posture of workloads, such as changing the policy enforcement states. You want to allow your application teams to manage workload security without granting them broad privileges, such as All access (for the standard Application, Environment, and Location label types, or for any customer label types you have defined).
- Use Case 3

  You want to prevent your users from accidentally changing workload labels by moving the workloads in Maps, Traffic, or other Console views.

Solution

Users with the Workload Manager role can create, update, and delete workloads and pairing profiles. This role is a scoped role; when you assign a user to a scope, they can only manage workloads within the allocated scope. The Workload Manager can pair, unpair, and suspend VENs and change the policy state. It is an additive role; you can assign the Workload Manager role to a user, and combine it with any other Illumio Console role to provide additional privileges for that user.

Users assigned the Workload Manager role can view applications that are outside their scopes but can only modify those applications that are within their scopes. A Workload Manager user cannot clear traffic counters from workloads within their scope.

To assign the Workload Manager role when first adding a new user:

1. **Access > Users > Add**
2. In **Roles**, select the Workload Manager role (and any other you want to assign).

To assign the Workload Manager role to an existing user:

1. **Access > Users**
2. Click the user name.
3. Click **Add Role**.
4. Choose **Add Scoped Role**.
5. In Select Roles, choose **Workload Manager** from the list.
6. (Optional) In Select Scope, specify a scope for this user's Workload Manager role.

Limited Ruleset Manager Role

A user has the role Limited Ruleset Manager role and access to the following scope:

All Applications | Production Environment | All Locations

The user can create and manage:

- Any ruleset that matches the Production environment
- Intra- or extra-scope rules that match this scope:
  All Applications | Production Environment | All Locations
  Where the destination and source of the rule are both within the Production environment scope.

For intra-scope rules, all workloads can communicate within their group (as defined by the scope), so the rule source is not restricted. However, in extra-scope rules, the Environment label of the resource selected as the source must match the label in the scope exactly.

The user cannot create a rule with the scope “All | All | All” because that scope is broader than the user's access, which is only for the Production environment.

Because the user is a member of the Limited Ruleset Manager role, the user cannot manage custom iptables rules and the following resources cannot be selected as consumers in extra-scope rules: IP lists Label groups, User groups, or Workloads.

Combined Roles

Illumio includes fine-grained roles to manage security policy. The roles control different aspects of the security workflow. By mixing and matching them, you can effectively control the access needed by your company.

Ruleset Only Roles

You can add users to the Ruleset Manager and Ruleset Provisioner roles so that they can edit the security policies for workloads in their scope and provision them

These users can write rules for their workloads and provision them when the rules do not have dependencies on global objects, such as services or IP lists.

Owner Roles

You can add security professionals professionals to the Owner role so that they can define all security policy for an enterprise.

Provisioner Roles

Provisioners have the capability to modify global objects, such as services, IP lists, and label groups.

Legal Notice

The content in this documentation is provided for informational purposes only and is provided "as is," without warranty of any kind, expressed or implied, of Illumio. The content in this documentation is subject to change without notice.

Resources

- Legal information
- Trademarks statements
- Patent statements
- License statements

Contact Information

- Contact Illumio
- Contact Illumio Legal
- Contact Illumio Documentation