Illumio Core®

Version 24.2

What's New in This Release

September 2024

14000-200-24.2

Legal Notices

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.

Product Version

PCE Version: 24.2

For the complete list of Illumio Core components compatible with Core PCE, see the Illumio Support portal (login required).

For information on Illumio software support for Standard and LTS releases, see Versions and Releases on the Illumio Support portal.

Resources

Legal information, see https://www.illumio.com/legal-information

Trademarks statements, see https://www.illumio.com/trademarks

Patent statements, see https://www.illumio.com/patents

License statements, see https://www.illumio.com/eula

Open source software utilized by the Illumio Core and their licenses, see Open Source Licensing Disclosures

Contact Information

To contact Illumio, go to https://www.illumio.com/contact-us

To contact the Illumio legal team, email us at legal@illumio.com

To contact the Illumio documentation team, email us at doc-feedback@illumio.com

illumio

Contents

What's New and Changed in This Release

This chapter contains the following topics:

Before upgrading to Illumio Core 24.2, familiarize yourself with the following new and modified features in this release.

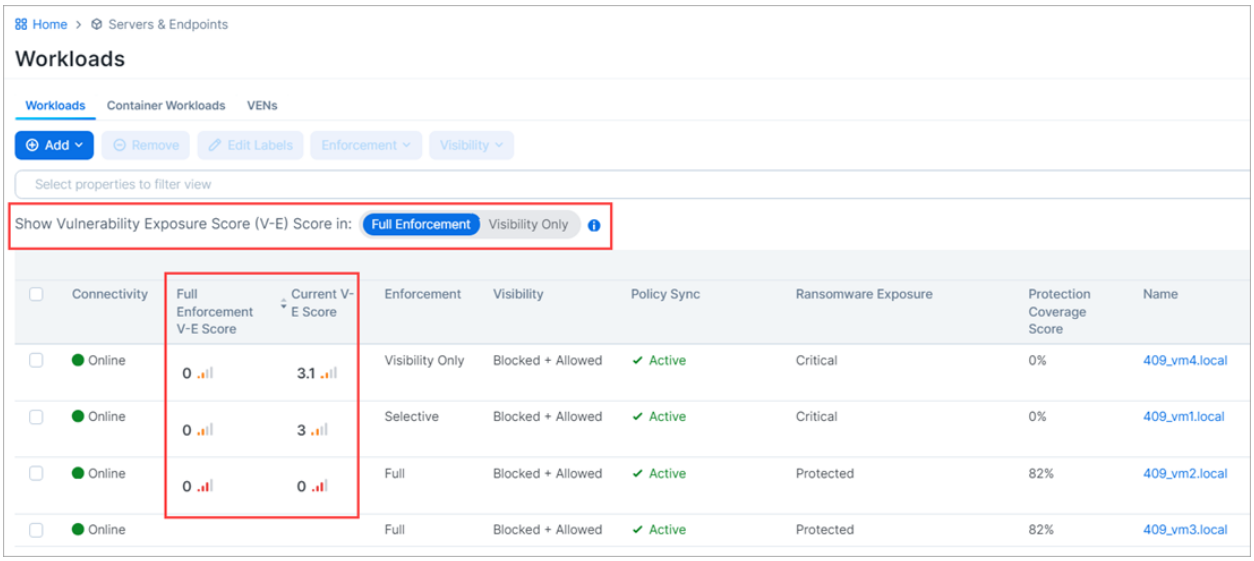
The information in this section describes the new and modified features to the PCE, REST API, and PCE web console.

What's New and Changed in Release 24.2.10

Compare V-E scores by Enforcement Type

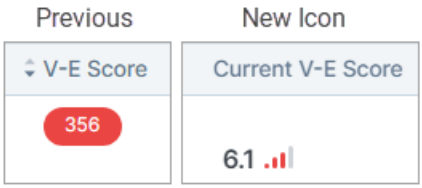
This release introduces the **Show Vulnerability Exposure (V-E) Score** tool which makes it easy to see how the security of your workloads and app groups would change if you were to change their current enforcement mode. New columns in the Workload and App Group list and details pages provide a side-by-side comparison of the effect different enforcement modes would have on Vulnerability and Enforcement (V-E) scores. A toggle allows you to simulate the switch between Full Enforcement and Visibility Only enforcement modes.

> NOTE:
> This option allows you to simulate the switch between Full Enforcement and Visibility Only modes. It doesn't change the actual enforcement mode of your workloads or app groups.



New icon indicates vulnerability severity level

This release introduces a familiar gradient icon to indicate the vulnerability severity level of workloads and app groups. The new icon improves UI accessibility by conveying a range of severity without relying on a color scheme.



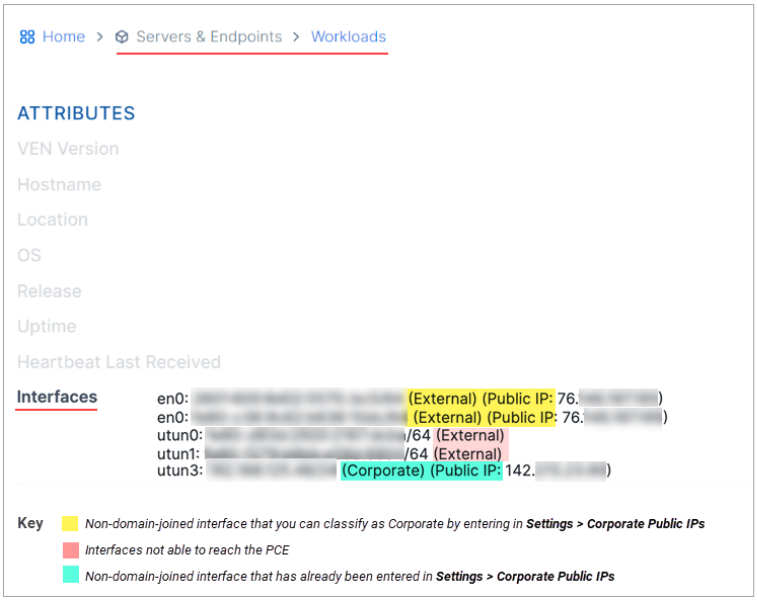
Support for Endpoint VENs on macOS Sonoma 14.4

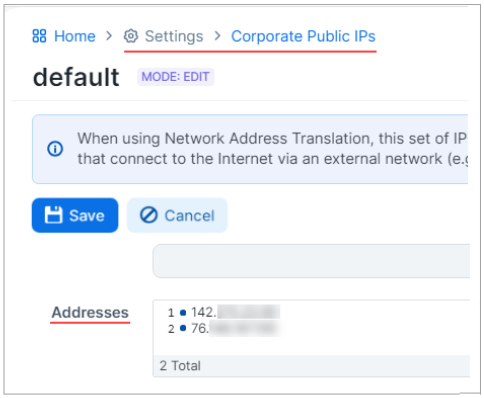
With this release, Endpoint VENs now support macOS Sonoma 14.4. For information about the Endpoint for macOS, see the Endpoint Installation and Usage Guide.

Easier Identification of Public IP Addresses for Endpoint VENs

> NOTE:
> This is an enhancement to the network profile detection feature. Network profile detection allows the PCE to determine whether a workload interface is connected to your Corporate network or to an external network (for example, a cafe or airport Wifi). The PCE uses this information to program network-specific rules on each of the endpoint's interfaces.

Beginning with this release, in the workload details pages in the PCE, the word **Public** is now prepended to the IP address (as seen by the PCE) of non-domain-joined Windows workloads and macOS endpoint interfaces reachable by the PCE. When you enter these Public IP addresses in the PCE (**Settings > Corporate Public IP**), the PCE classifies them as Corporate and programs their corresponding endpoint interfaces with the appropriate Illumio security policies. See Add Public IP addresses to the Corporate Public IPs list.





Keep in mind:

- As non-domain joined Windows endpoints or macOS endpoint VENs make network location detection calls to the PCE from each workload interface, the public IP address they report is the source of the IP address as seen by the PCE.
- In SaaS, the IP is also an organization's public egress IP to the Internet.

- If a given interface is not reachable by the PCE, its IP address is classified as "External" on the workload's details page and "Public" does not appear.
- If you enter the IP address of a non-domain-joined Windows workload or macOS endpoint in Settings > Corporate Public IPs, the PCE classifies its associated interface as "Corporate." Otherwise, the PCE classifies the interface as "External."

Enhanced VEN Platform Resiliency

To mitigate the effects of data loss and file corruption that can result from a sudden loss of power or the host crashing, VEN release 24.2.10 provides enhanced resiliency as follows:

- When VEN data is written to volatile memory, it's now simultaneously written to disc, ensuring a higher likelihood of successful recovery.
- In the event of file corruption, certain VEN configuration files are now backed up and then restored automatically.

Discontinued Dependency on PowerShell

Starting with VEN release 24.2.10, customers can perform VEN tasks in any Windows Command Line shell capable of executing `*.exe` commands. This includes Command Prompt (cmd.exe) and PowerShell, among others. As all modern Windows machines include Command Prompt by default, all PowerShell commands in Illumio VEN documentation have been changed to equivalent `*.exe` commands.

LW-VEN 1.1.0 supports flow reporting for legacy Windows servers

Beginning with release 1.1.0-LW-VEN, the LW-VEN can enable the native Windows Firewall log on your legacy Windows server, which allows the LW-VEN to generate and log traffic flow information for ingestion by the PCE. After ingesting the log information, the PCE displays it in its Map and Traffic views to help you gain insights about and create policy for your business applications.

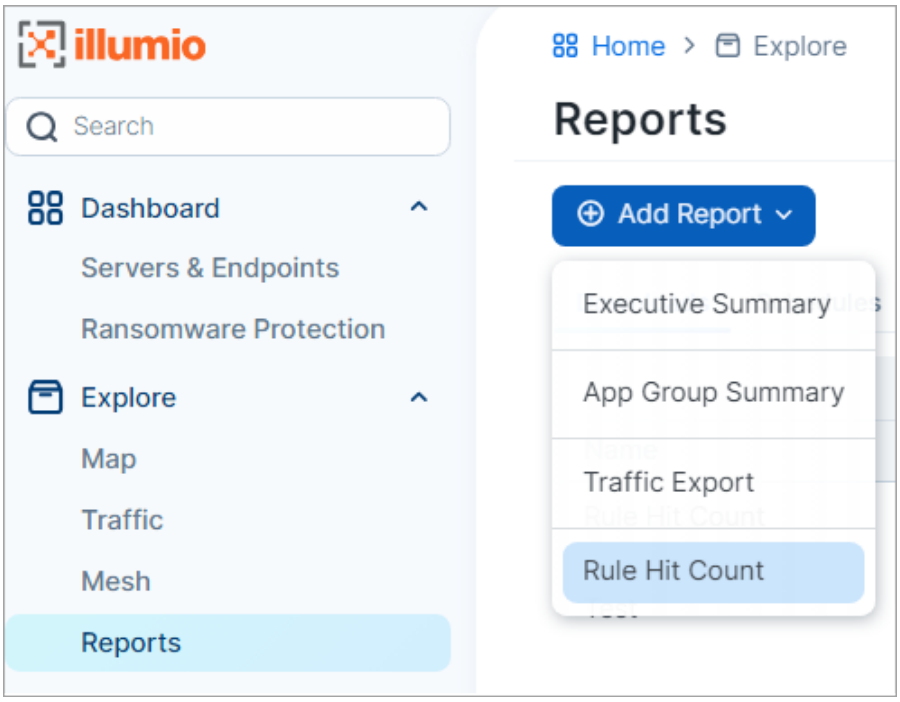
Illumio IPFilter Update

The release of IPFilter 5.3.0.5003 provides increased throughput over the loopback interface when the VEN is in Visibility, Selective Enforcement, or Full Enforcement mode. This improves performance for some applications and tools that are sensitive to latency of the loopback interface.

What's New and Changed in Release 24.2

The following new features were added in Illumio Core 24.2.

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 PCE UI or through the Illumio REST API.

The Rule Hit Count Report provides the following:

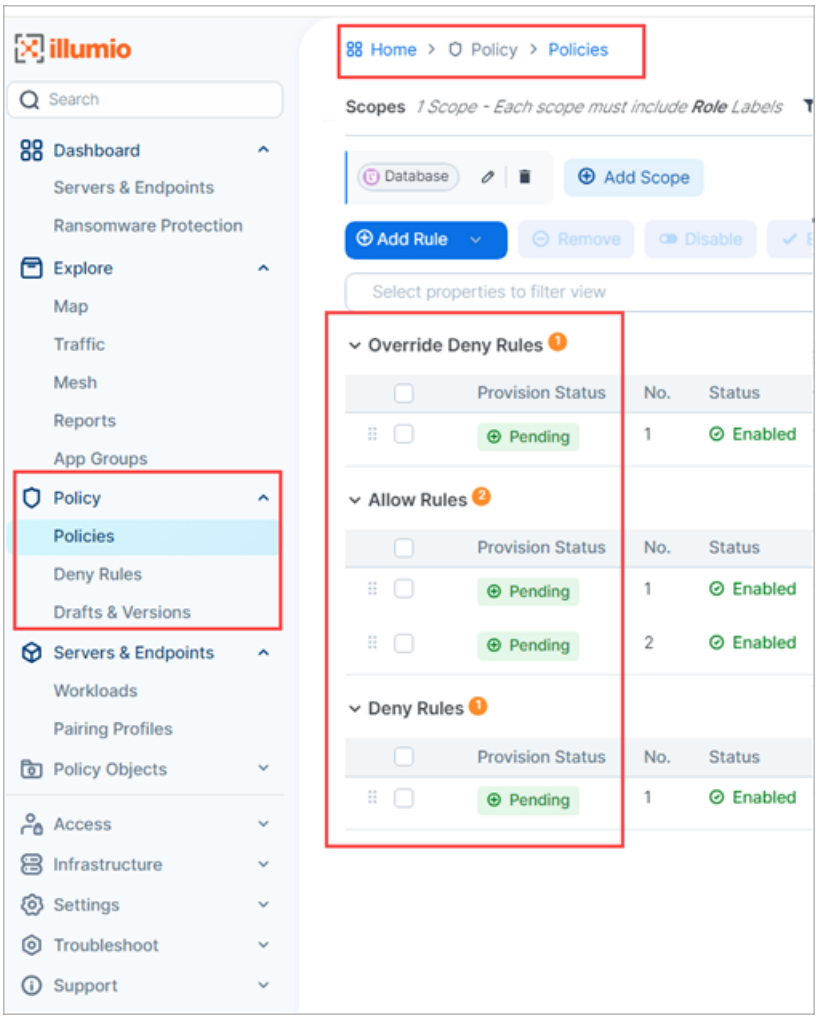
- Policy Compliance: Generate a Rule Hit Count Report to provide evidence that security controls are in place and working effectively, demonstrating compliance to auditors.
- Redundancy Removal: Identify unused or less-used rules so you can remove or modify them to reduce redundancy and clutter in your 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 About Reports.

Policy is a new section in the left navigation

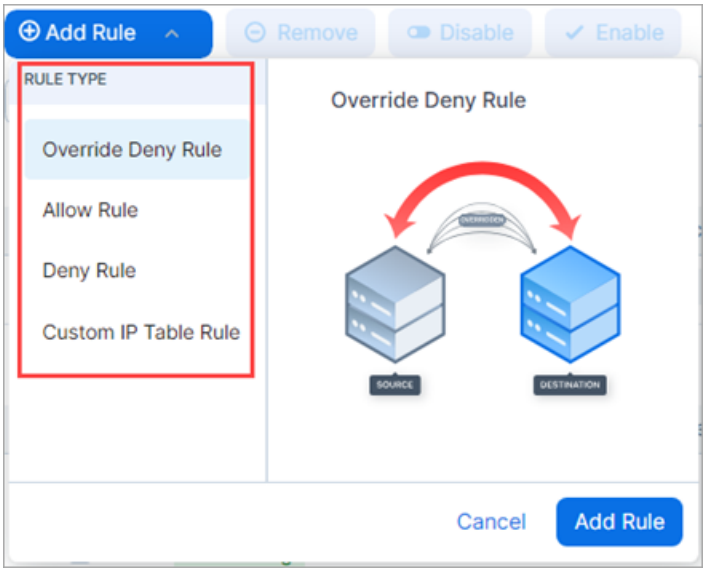
The Policy section replaces Rules & Rulesets in the left navigation.

> 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.

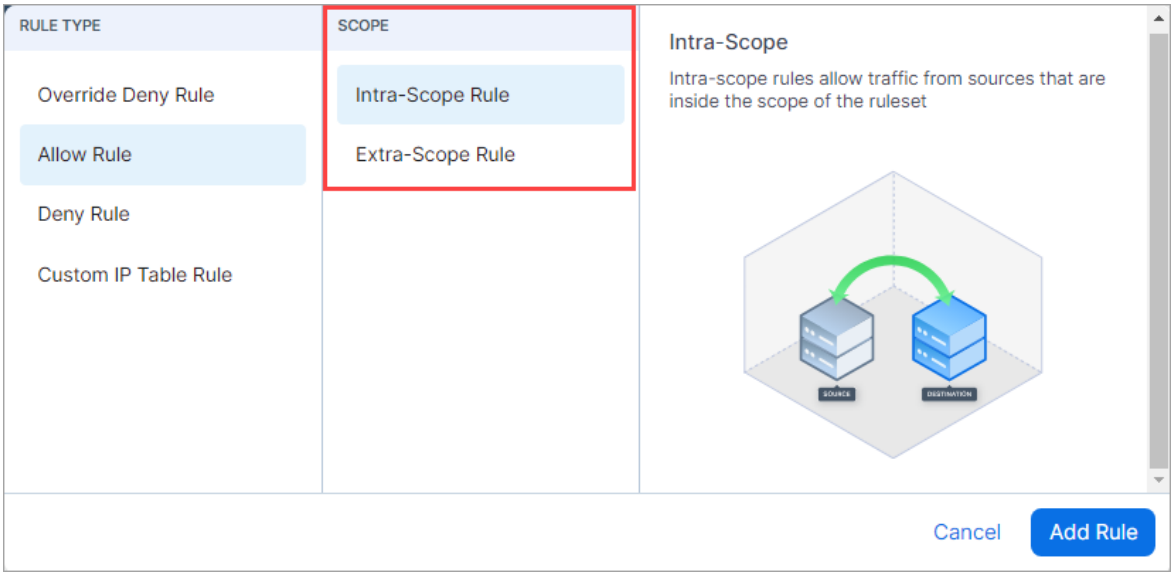


The Policies page differs from Rulesets & Rules in the following ways:

- 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:

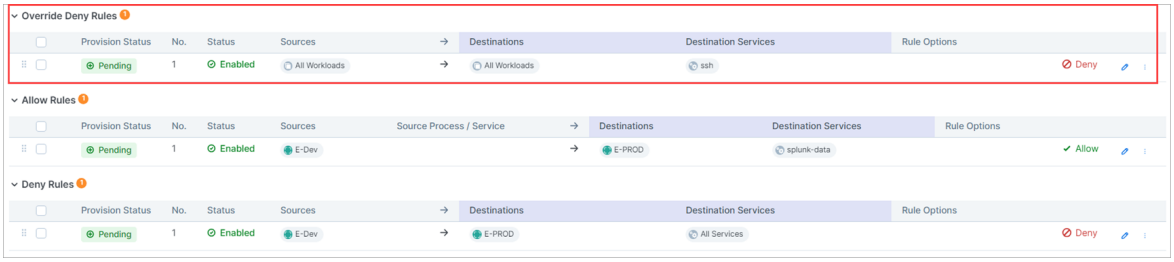
- Provide an additional type of granular control for blocking network traffic, helping to ensure that only explicitly authorized communications are permitted.
- Block traffic with a type of Deny rule that can't be overridden.
- Can be used in scoped and un-scoped rulesets.
- Impact the calculation of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

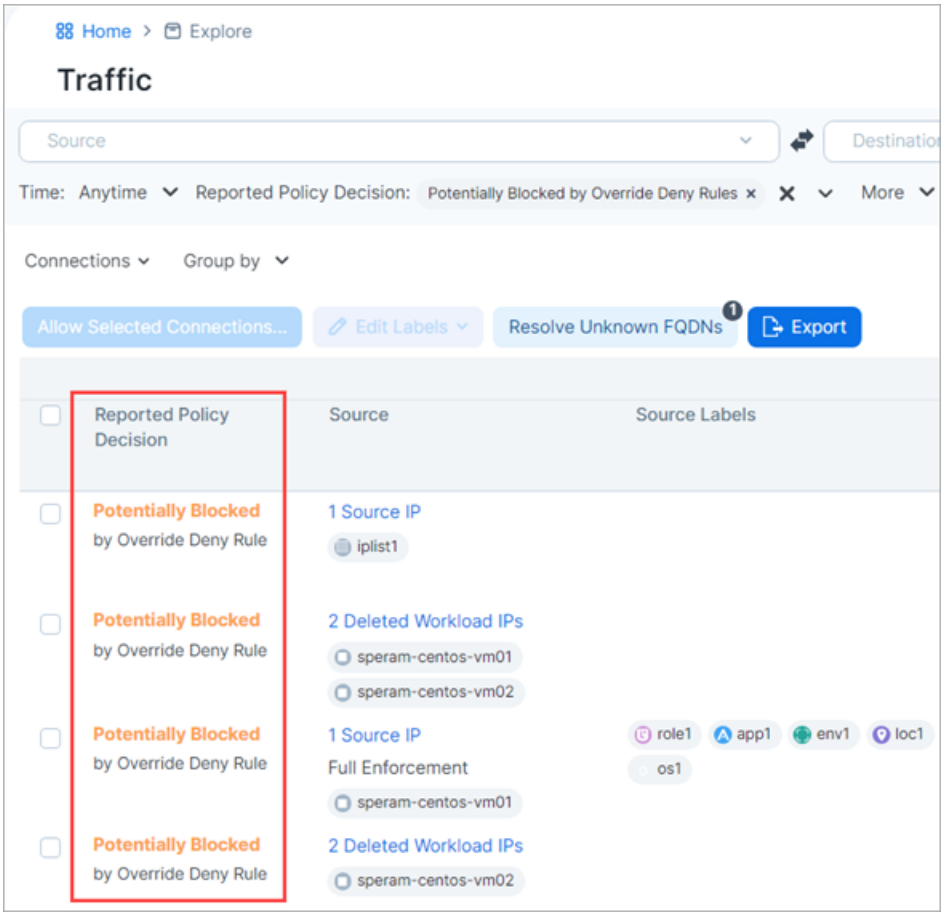
rule.



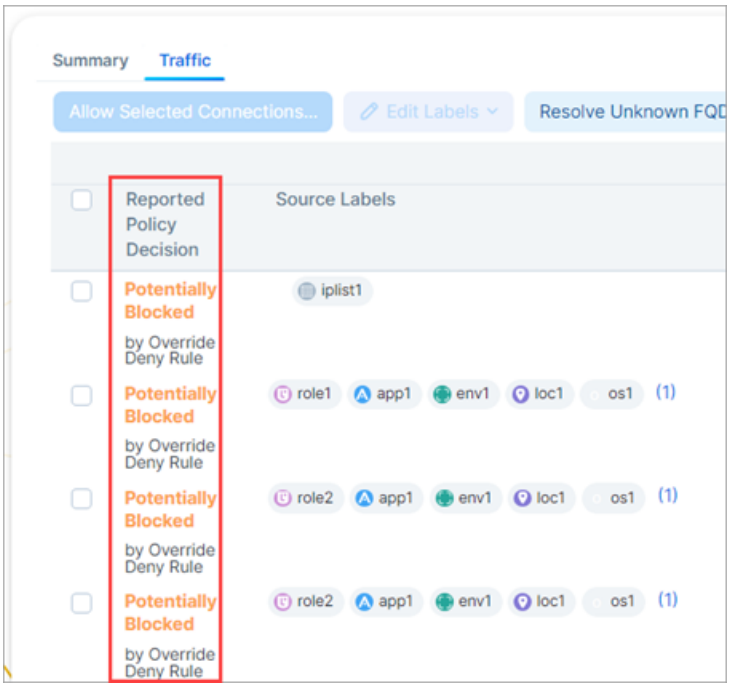
Appearance in Visualization tools

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 PCE UI.

As seen in Traffic view



As seen in the details panel in Map view



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

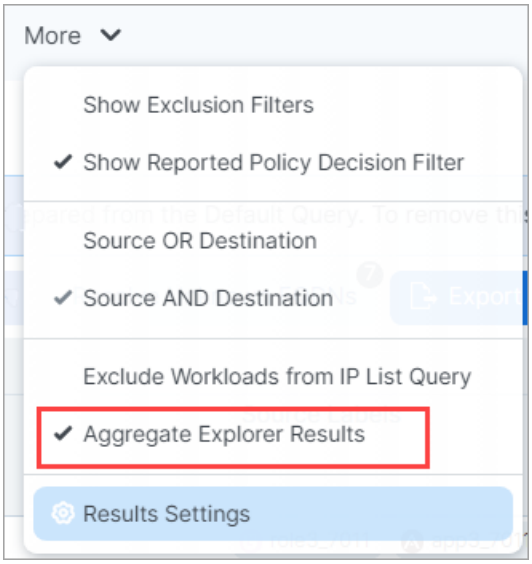
- The separate tabs that contained Intra-Scope and Extra-Scope options in previous releases are removed and a new column called Scope Type appears in the Allow rules section of the Policies page.
- Extra-Scope and Intra-Scope rules occupy different sections within Allow Rules, separated by a gray line.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

Only Allow Rules are listed on some pages

The badge ALLOW RULES ONLY appears in the following areas of the PCE UI 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 (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**.