Release Notes for Illumio Console 24.22

October 10, 2024

Table of Contents

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, CloudSecure, 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 CloudSecure 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