Illumio Core®

Version 21.2

What Is New in This Release

November 2022

14000-200-21.2

Legal Notices

Product Version

PCE Version: 21.2 (LTS release)

For the complete list of Illumio Core components compatible with Core PCE, see the Illumio Support portal (log in 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

Chapter 1

Welcome to Illumio Core 21.2

This chapter contains the following topics:

Illumio is pleased to announce the general availability of version 21.2 of the Illumio Core for the PCE and VEN Software. This new release contains many improvements and changes as described in this document.

About This Release

This documentation portal describes the new features, enhancements, platform support, and new and modified REST APIs for the Illumio Core 21.2 release.

Product Versions

PCE Version: 21.2.7 (LTS)

VEN Version: 21.2.5 (LTS)

C-VEN Version: 21.2.1+H4 (LTS)

NEN Version: 2.1.0+H7

Kubelink Version: 2.0.2

FlowLink Version: 1.1.2+H2

PCE CLI Tool Version 1.4.1

Standard versus LTS Releases

21.2.4-PCE and 21.2.5-VEN are LTS releases. For information on Illumio software support for Standard and LTS releases, see Versions and Compatibility on the Illumio Support portal.

Release Types and Numbering

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

- “a.b”: Standard or LTS release number, for example “21.2”
- “.c”: Maintenance release number, for example “.1”
- “-d”: Optional descriptor for pre-release versions, for example “preview2”
- “+e”: Hot Fix release descriptor, for example “+H1”, “+H2”, “+H3”.

VEN Version Requirements

The following minimum VEN versions are applicable to the features and changes in this release.

General Advisory or Announcement	Minimum VEN Version
Debian 11 Support	21.2.3
Changes to Teredo Tunnel Interfaces	21.2.0
Change to Limited Ruleset Manager Role	Any supported version
Higher Maximum Number of Database Results	Any supported version
Enhanced Security for TLS	Any supported version
VEN Package Format Changes	21.2.1
Containerized VEN Base Image	21.2.1
Object Limit: Max Security Principal Permissions	Any supported version
EOL: PCE Virtual Appliance	Any supported version
EOS: CentOS 6.x and RHEL 6.x	Any supported version
EOS: Illumio Core REST API v1	Any supported version
EOS: Internet Explorer 11	Any supported version
EOS: External VEN Repo	Any supported version
EOS: System Events for OVA	Any supported version
EOS: Organization Events	Any supported version
Deprecated: Runtime Environment File Parameter	Any supported version
Deprecated: Network Function Control	Any supported version

General Advisories

The information in this section provides general advisories about important aspects of this release. To ensure proper operation of the system after upgrade, you might need to take account on these advisories.

Supported Operating Systems

The 21.2.0 PCE and VEN are supported on operating systems detailed on the Illumio Support portal.

See PCE OS Support and Package Dependencies and VEN OS Support and Package Dependencies.

Supported Orchestration Platforms for Containerized VEN

In 21.2.0, the Containerized VEN now supports the OpenShift 4.*x* platform. In the previous release, the OpenbShift 4.*x* platform was in Preview.

See VEN OS Support and Package Dependencies for more information. Select the "Containerized VEN/Kubelink" option for the supported platforms.

VEN Package Format Changes

Starting with the 21.2.1 Illumio Core release, the Windows VEN installer switches from MSI to EXE package format. Customers using the PCE-based VEN deployment, such as the VEN Library, must take an extra step for the transition. Specifically, Illumio Core customers running older MSI-based Windows VENs must upgrade to 19.3.6+H1-VEN or 21.2.0+H2-VEN before upgrading their VENs to 21.2.1 or a later version. The 21.2.0+H2-VEN release contains the necessary VEN changes to handle the transition in the VEN packaging from MSI to EXE.

Containerized VEN Base Image

Illumio detected a vulnerability in the Containerize VEN (C-VEN) image for 21.2.0. The Illumio C-VEN container image used a lightweight version of RHEL 7.8. In C-VEN 21.2.1, Illumio has resolved this issue by updating the C-VEN base OS image to RHEL 7.9 to address this vulnerability. We will strongly encourage our customers to upgrade to the new image in the C-VEN 21.2.1 release.

For more information, see the Illumio Containerized VEN Release Notes 21.2.1, Resolved Issues in 21.2.1.

Open Source Package Updates

Illumio updated several open source packages for the PCE in this release. See the "Change History" in Illumio Open Source Licensing Disclosures 21.2.0 and the "Change History" in Illumio Open Source Licensing Disclosures 21.2.1 for information.

Changes to Teredo Tunnel Interfaces

Teredo tunnel interfaces are no longer reported from Windows workloads. The change is to fix an issue with the interface's IP addresses changing very frequently. The Teredo interface is used for IPv6 connectivity, and is disabled by default.

The behavior to report Teredo tunnel interfaces changed in the Core 21.2.0 release; however, Windows workloads continued to report them. This issue is resolved in Core 21.2.1; for more information see the Illumio Core Release Notes 21.2.1, Resolved Issues in 21.2.1, VEN Resolved Issues, Issue E-75043.

Change to Limited Ruleset Manager Role

Users with the Limited Ruleset Manager role can no longer create or modify extra-scope rules.

Higher Maximum Number of Database Results

IMPORTANT:
This advisory is applicable to Illumio Core On Premises customers only.

The maximum number of results that can be retrieved from the PCE database has changed. The maximum number of results that can be retrieved from the database is 200,000 for each PCE. In a Supercluster, a query run on the leader PCE can return 200,000 results for each PCE in the Supercluster, including the leader. For example, in a Supercluster with four regions, the maximum is 800,000. When logged in to a member PCE on a Supercluster, the limits are the same as for any stand-alone PCE. In every case, the maximum number of results that can be shown in the PCE web console is 100,000, as in earlier releases. If more than 100,000 results are retrieved, the full results are available as a downloaded CSV file, and the first 100,000 are available in the web console.

Enhanced Security for TLS: Changes to Configuration Settings

IMPORTANT:
This advisory is applicable to Illumio Core On Premises customers only.

This release changes PCE configuration that increases the security of TLS on the PCE. For more information about the reasons for these changes, see Enhanced Security for PCE TLS Configuration.

- This release includes a new PCE runtime parameter `insecure_tls_weak_ciphers_enabled`. You use this parameter to control how the PCE accepts weak TLS ciphers, such as cipher block chaining (CBC) ciphers. By default, this runtime parameter is enabled on the PCE. However, you can choose to disable this parameter so that your PCE uses strong ciphers. See Reference: PCE Runtime Parameters in the PCE Installation and Upgrade Guide for more information.
- The default minimum TLS version is now 1.2. This is a new default setting for the existing flag `min_tls_version`. See TLS Versions for Communications.

New Object Limit: Maximum Permissions for Security Principal

IMPORTANT:
This advisory is applicable to Illumio Core On Premises customers only.

The `max_permissions_per_auth_security_principal` is a new object limit setting. It controls how many permissions a given user can have. The default is 50. In previous releases, this was a runtime parameter.

Be Sure Prerequisites and Settings are Correct Before Installing

IMPORTANT:
This advisory is applicable to Illumio Core On Premises customers only.

The PCE Installation and Upgrade documentation contains detailed information about required prerequisites and settings. Always follow these instructions precisely to be sure your PCE continues to function properly over time.

Important documentation changes have been made in this area for 21.2.0. See the *PCE Installation and Upgrade Guide* for information.

Before Upgrading to This Release

Before upgrade, review all changes from your current version to version 21.2.0.

To ensure readiness, Illumio strongly encourages you to review the prior release notes, from your currently installed version of Illumio Core to version 21.2.0. To view the release notes for versions prior to Core 19.3.*x*, go to the Documentation page on the Support portal (login required) and select the version from the drop-down menu.

For information about the upgrade path and tools, go to the Illumio Support portal and review the PCE Upgrade paths and the VEN Upgrade paths (login required).

Manage Data and Disk Capacity Carefully

IMPORTANT:
This advisory is applicable to Illumio Core On Premises customers only.

Beginning with PCE 18.2, the amount of data collected and stored by the PCE has increased. Events, Explorer, and the internal syslog all generate more data to be stored in PCE databases and log files. If the amount of stored data is not managed carefully, disks can become overfull, or backup size can increase, making restores take longer.

To successfully manage these concerns, consider the following:

- **Identify:** Know your organization's policies, backup strategies, and monitoring strategies.
- **Detect:** Monitor ongoing disk usage.
- **Respond:** Know how to troubleshoot and fix issues related to data storage.
- **Recover:** Set up your PCE deployment to reduce disk usage.

For more information, see Manage Data and Disk Capacity in the *PCE Administration Guide*.

Supported Supercluster Configuration

IMPORTANT:
This advisory is applicable to Illumio Core On Premises customers only.

Starting at Illumio Core 21.1.0, Supercluster support is limited to 3 PCEs with 25k VENs per PCE (4x2 configuration).

Announcements

End of Support Announcements, Deprecations , On-premises Upgrade Paths, Compatibility

End of Life

Virtual Appliance

This announcement is applicable to Illumio Core On Premises customers only.

The PCE Virtual Appliance will no longer be published, and you can no longer deploy a PCE using the Virtual Appliance.

End of Support

CentOS 6.x and RHEL 6.x

This announcement is applicable to Illumio Core On Premises customers only.

CentOS 6.x and Red Hat Enterprise Linux 6.x are not supported for PCE versions 21.2.0 and later. PCE versions 18.2 LTS and 19.3 LTS continue to support CentOS 6.x and RHEL 6.x until their published end-of-support dates, but upgrading to a newer version of the operating system is recommended. For PCE version 19.3, upgrade to CentOS 7 or RHEL 7. For PCE version 18.2, first upgrade to PCE 19.3, then upgrade to CentOS 7 or RHEL 7.

Illumio REST API v1

The version 1 of Illumio REST APIs (API v1) is not supported effectively with the 21.1 and later releases. Illumio recommends that you upgrade to API v2.

Internet Explorer 11

Illumio Core 19.1 was the last release to support Internet Explorer 11. Internet Explorer 11 will no longer be supported in Illumio Core 19.2 and later releases. Illumio recommends Chrome, Edge, or Firefox for use with the PCE web console.

External VEN Repo

This announcement is applicable to Illumio Core On Premises customers only.

The external VEN repo is no longer supported for VEN versions 18.2 and later releases. Customers must migrate to using the new PCE-based VEN deployment or install VEN packages directly on workloads.

System Events for OVA

Events 2.0 system events are no longer supported. (For reference, see E-48119)

Organization Events

Since the 19.1.0 release, the older form of events, known as “audit or organization events,” is no longer supported or available.

Any versions of the former SIEM Integration Guide that are earlier than version 18.2.1 are valid only for their corresponding versions, not version 18.2.1 or later releases.

Customers should upgrade to the latest version of Illumio Adaptive Security and take advantage of the newly designed auditable events. See the *Events Administration Guide* for information.

Deprecation

Runtime Environment File Parameter

This announcement is applicable to Illumio Core On Premises customers only.

The runtime environment file parameter `syslog_event_export_format` is deprecated.

Network Function Control

The Network Function Control (NFC) was discontinued in the 19.3.0 release. It is now a part of the Network Enforcement Node (NEN). You can use the NEN module to interface with the F5 Server Load Balancer. For more information, see the *NEN Installation and Usage Guide*.

Chapter 2

What's New and Changed in This Release

This chapter contains the following topics:

Before upgrading to Illumio Core 21.2.0, familiarize yourself with the following new and modified features in this release.

The information in this section describes the new and modified features by category—PCE, VEN, Supercluster, NEN, REST API, and PCE web console.

What's New and Changed in Release 21.2.7

Illumio Core 21.2.7 introduces the following new features and enhancements.

21.2.7 Illumio Core Maintenance Release

NOTE:
Illumio Core 21.2.5 is a maintenance release for the Illumio Core PCE only.

Illumio provides regular maintenance updates for reported bugs and security issues, and to add support for new operating system versions.

As a maintenance release, Illumio Core 21.2.7 solved software and security issues for the Illumio Core PCE to refine the software and improve its reliability and performance.

For the complete list of improvements and enhancements to the PCE, see "Resolved Issues in 21.2.7-PCE" in the Illumio Core Release Notes 21.2.

For more information about the Illumio software release types and software support, see Versions and Compatibility on the Illumio Support portal (login required).

What's New and Changed in Release 21.2.5

Illumio Core 21.2.5 introduces the following new features and enhancements.

21.2.5 Illumio Core Maintenance Release

NOTE:
Illumio Core 21.2.5 is a maintenance release for the Illumio Core VEN only.

Illumio provides regular maintenance updates for reported bugs and security issues, and to add support for new operating system versions.

As a maintenance release, Illumio Core 21.2.5 solved software and security issues for the Illumio Core VEN to refine the software and improve its reliability and performance.

For the complete list of improvements and enhancements to the PCE and VEN, see "Resolved Issues in 21.2.5-VEN" in the Illumio Core Release Notes 21.2.

For more information about the Illumio software release types and software support, see Versions and Compatibility on the Illumio Support portal (login required).

What's New and Changed in Release 21.2.4

Illumio Core 21.2.4 introduces the following new features and enhancements.

21.2.4 Illumio Core Maintenance Release

Illumio provides regular maintenance updates for reported bugs and security issues, and to add support for new operating system versions.

As a maintenance release, Illumio Core 21.2.4 solved software and security issues to refine the software and improve its reliability and performance.

For the complete list of improvements and enhancements to the PCE and VEN, see "Resolved Issues in 21.2.4" in the Illumio Core Release Notes 21.2.

For more information about the Illumio software release types and software support, see Versions and Compatibility on the Illumio Support portal (login required).

Windows VEN Proxy Fallback Enhancement

In Illumio Core 21.2.1 and 21.2.2, the VEN automatically detects a web proxy. However, it always attempts to connect directly to the PCE first.

In this release, Illumio enhanced the heuristic in the VEN for falling back to the configured web proxy. After an attempt fails to connect to the PCE directly due to an HTTPS intercepting proxy, the VEN falls back to use the configured web proxy.

Documentation Updates

In Replace PCE Nodes or Uninstall Cluster, Illumio added new steps to the procedure for replacing a node. In this procedure, you begin by removing one node from a PCE cluster. To prevent the node from rejoining the cluster on reboot, perform these two additional steps after running `illumio-pce-ctl cluster-leave`:

1. On the leader node, remove the failed node:

   ```
   $ sudo -u ilo-pce illumio-pce-ctl cluster-leave ip_address
   ```

2. On the removed node, run the following command:

   ```
   $ sudo -u ilo-pce illumio-pce-ctl reset
   ```

3. On the removed node, delete or rename the file `runtime_env.yml`.

These three steps are only part of the full procedure. Be sure to perform all the steps; see Replace PCE Nodes or Uninstall Cluster.

What's New and Changed in Release 21.2.3

Illumio Core 21.2.3 introduces the following new features and enhancements.

21.2.3 Illumio Core Maintenance Release

Illumio provides regular maintenance updates for reported bugs and security issues, and to add support for new operating system versions.

As a maintenance release, Illumio Core 21.2.3 solved software and security issues to refine the software and improve its reliability and performance.

For the complete list of improvements and enhancements to the PCE and VEN, see "Resolved Issues in 21.2.3" in the Illumio Core Release Notes 21.2.

For more information about the Illumio software release types and software support, see Versions and Compatibility on the Illumio Support portal (login required).

Illumio updated several open source packages for the PCE in this release. See the "Change History" in Illumio Open Source Licensing Disclosures 21.2.3 for information.

Debian 11 Support

In this release, Illumio supports installing and operating the VEN on the Debian 11 operating system.

Illumio REST API Changes

In this release, Illumio added minor non-breaking API changes in two schema.

In the schema for `workloads_post.schema.json`, the `public_ip` property now accepts a null value.

The schema for `sec_policy_get.schema.json` has the following minor changes:

- The type for the `version` property changed from a string to an integer.
- The `workloads_affected` property now accepts a null value.
- The `commit_message` property now accepts a null value.

What's New and Changed in Release 21.2.2

Illumio Core 21.2.2 introduces the following new features and enhancements.

21.2.2 Illumio Core Maintenance Release

Illumio provides regular maintenance updates for reported bugs and security issues, and to add support for new operating system versions.

As a maintenance release, Illumio Core 21.2.2 solved software and security issues to refine the software and improve its reliability and performance.

For the complete list of improvements and enhancements to the PCE and VEN, see "Resolved Issues in 21.2.2" in the Illumio Core Release Notes 21.2.

For more information about the Illumio software release types and software support, see Versions and Compatibility on the Illumio Support portal (login required).

Illumio updated several open source packages for the PCE in this release. See the "Change History" in Illumio Open Source Licensing Disclosures 21.2.2 for information.

CloudLink Available Through the PCE Web Console

Without installing agents, you can use Illumio CloudLink to accomplish the following functions:

- Collect object metadata and flow telemetry from your public cloud accounts.
- Automatically build a model and application dependency map of workloads and connected objects. The map shows VMs, managed DBs, ENIs, workloads, flows, and application dependencies as unmanaged workloads in a single, unified Illumination map.

In this release, you can launch CloudLink from the PCE web console main menu > **Infrastructure** > **CloudLink**. The CloudLink login page opens in a new browser tab from which you can either authenticate or sign up as a new CloudLink user.

What's New and Changed in Release 21.2.1

Illumio Core 21.2.1 introduces the following new features and enhancements.

21.2.1 Illumio Core Maintenance Release

Illumio provides regular maintenance updates for reported bugs and security issues, and to add support for new operating system versions.

As a maintenance release, Illumio Core 21.2.1 solved software and security issues to refine the software and improve its reliability and performance.

For the complete list of improvements and enhancements to the PCE and VEN, see "Resolved Issues in 21.2.1" in the Illumio Core Release Notes 21.2.

For more information about the Illumio software release types and software support, see Versions and Compatibility on the Illumio Support portal (log in required).

Supercluster 8-Region Support in 21.2.1

A Supercluster can now have a maximum of 8 PCEs.

Open Source Package Updates for 21.2.1

Illumio updated several open source packages for the PCE in this release. See the "Change History" in Illumio Open Source Licensing Disclosures 21.2.1 for information.

VEN Version Requirements

The following minimum VEN versions are applicable to the features and changes in this release.

Feature or Enhancement	Minimum VEN Version
RHEL 8 support for PCE	Any supported version
New threshold configuration settings	Any supported version
Change in syslog forwarding	Any supported version
VEN Package Format Changes	21.2.1-VEN
Containerized VEN Base Image	21.2.1-C-VEN
New VEN File Settings Option	21.2.1-VEN

Changes in This Release

RHEL 8 Support

Version 21.2.1 of the PCE supports RHEL 8 for on-premises installation of the PCE. In version 21.2.0, this support was provided as a preview only. In 21.2.1, RHEL 8 is fully supported as a general availability release for use in production environments.

The RHEL 8 version of the PCE software has a separate download RPM file. Look for "c8" in the file name. This RPM file can only be used on Red Hat version 8 and will fail to install if used on an earlier version of Red Hat.

NOTE:
If you are using 1024-bit certs, you will need to use 2048-bit (or longer) certs when moving to RHEL 8.

Change in Syslog Forwarding

When remote syslog forwarding is turned on, events are now logged using the local5, local6, and local7 syslog facilities for audit, traffic, and health events respectively. In releases before 21.2.1, all events were logged with the user syslog facility.

For more information, see Syslog Forwarding in the *PCE Administration Guide*.

New Threshold Configuration Settings

Health metrics are returned by both the health API and system_health messages. Configurable thresholds for many of these metrics have been available since version 19.3.2. New settings have been added in 21.2.1: `disk_space_percent_thresholds`, `disk_inode_percent_thresholds`, `memory_percent_thresholds`, `cpu_max_percent`, and `cpu_tolerance_seconds`.

For more information, see PCE Health Metrics Reference in the *PCE Administration Guide*.

VEN Package Format Changes

Starting with the 21.2.1 Illumio Core release, the Windows VEN installer switches from MSI to EXE package format. Customers using the PCE-based VEN deployment, such as the VEN Library, must take an extra step for the transition. Specifically, Illumio Core customers running older MSI-based Windows VENs must upgrade to 19.3.6+H1-VEN or 21.2.0+H2-VEN before upgrading their VENs to 21.2.1 or a later version. The 21.2.0+H2-VEN release contains the necessary VEN changes to handle the transition in the VEN packaging from MSI to EXE.

Containerized VEN Base Image

Illumio detected a vulnerability in the Containerize VEN (C-VEN) image for 21.2.0. The Illumio C-VEN container image used a lightweight version of RHEL 7.8. In C-VEN 21.2.1, Illumio has resolved this issue by updating the C-VEN base OS image to RHEL 7.9 to address this vulnerability. We will strongly encourage our customers to upgrade to the new image in the C-VEN 21.2.1 release.

For more information, see the Illumio Containerized VEN Release Notes 21.2.1, Resolved Issues in 21.2.1.

New VEN File Settings Option

In 21.2.1, the VEN IPFilter state table supports a new option for AIX workloads to support traffic from NFS servers:

VEN File Setting: `IPFILTER_TCPCLOSED=<value>`

ipfilter Setting: `fr_tcpclosed=<value>`

For more information about this option, see VEN Activate Command Reference in the *VEN Installation and Upgrade Guide.*

Labels Category in Explorer Allows Searching for Labels Across All Types

New default Labels category in Explorer makes it easier to create queries. When you begin to enter text in an **Include** or **Exclude** field, Explorer immediately displays a matching list of up to five Labels from across all label types (Roles, Environment, Applications, Location). Prior to this enhancement, Explorer fields displayed Environment-type labels by default, which was less intuitive. With this update, the Labels category in Explorer now behaves like the Labels category in **Segmentation Rule Search** except that Explorer also allows you to easily limit your search to labels within a specific category.

What's New and Changed in Release 21.2

Illumio Core 21.2.0, introduces the following new features and enhancements.

VEN Version Requirements

The following minimum VEN versions are applicable to the features and changes in this release.

Feature or Enhancement	Minimum VEN Version
Enforcement Boundaries	21.2.0
Asynchronous Queries (Explorer)	Any supported version
Label Groups for RBAC	Any supported version
Loopback Interface Support	Any supported version
FQDN Enhancements in Data Visualization	Any supported version
Uninterrupted Traffic between the VEN and the PCE	21.2.0
Linux Pairing Script Activation for Proxy Servers	21.2.0
PREVIEW: Network-Specific Policy	21.2.0
Global Explorer	Any supported version
Supercluster Replication Enhancements	Any supported version
LDAP Improvements	Any supported version
Enhanced Security for PCE TLS Configuration	Any supported version
Supercluster Rolling Upgrade	Any supported version
PREVIEW: Reports Preview in 21.2.0	Any supported version
PREVIEW: RHEL 8.3 Support for PCE	Any supported version

New Features in This Release

Containerized VEN in 21.2.0

In this release, the Containerize VEN supports deploying a local policy convergence controller.

The local policy convergence controller provides a deterministic way of setting the readiness state of pods in your cluster after local policy has converged. By controlling the readiness state of pods, you can prevent them from receiving and sending traffic through Kubernetes until they are ready. Using a controller ensures that the network and security infrastructure is ready for a multi-microservice application.

In this release, the Kubernetes Custom Pod Conditions feature introduced in v1.14 is available for containerized VENs.

For more information, see Local Policy Convergence Controller in the *Illumio Core for Kubernetes and OpenShift Guide*.

Enforcement Boundaries

IMPORTANT:
This feature requires the Illumio Core VEN version 21.2.0 or later.

In the Illumio Core 21.2.0 release, Illumio introduces Enforcement Boundaries, a new feature to speed your journey toward Zero Trust.

The Illumio security policy model is based on the principle of Zero Trust. Achieving Zero Trust security is possible with Illumio Core because it bases security policy on an allowlist model. From a security perspective, creating policy based on allowlists is the preferred method and has the advantage of specifying what you trust explicitly. However, you can encounter situations when you need more flexibility in segmenting your data centers. The solution is to introduce a new set of rules that determine where segmentation rules apply. These rules are referred to as Enforcement Boundaries in Illumio Core. Enforcement Boundaries can block traffic from communicating with workloads you specify, while still allowing you to progress toward a Zero Trust environment.

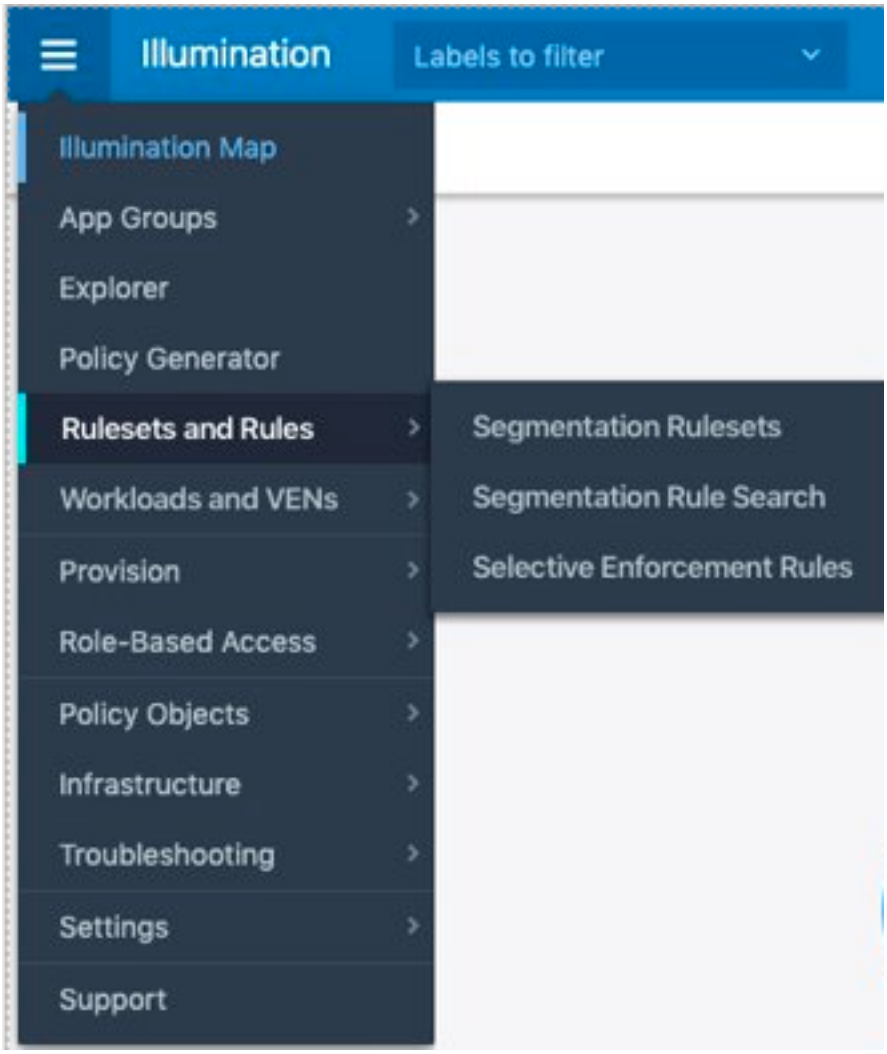
With the introduction of Enforcement Boundaries, the PCE web console and Illumio Core REST API changed to support the new feature.

For information about this new feature, see Policy Enforcement in the *Security Policy Guide* and Enforcement Boundaries in *REST API Developer Guide*.

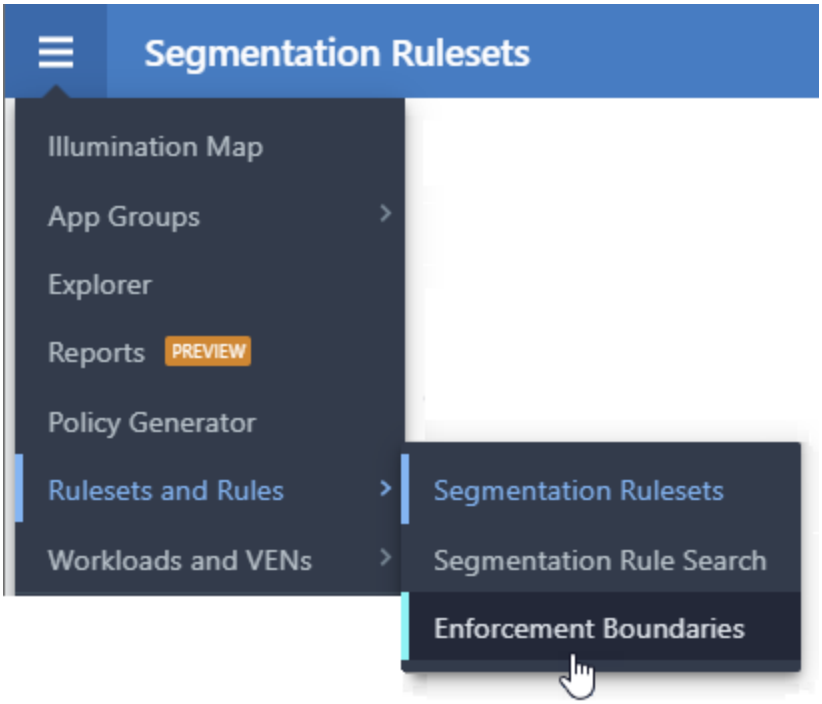
Changes to Selective Enforcement

Illumio Core 20.2.0 introduced Selective Enforcement as a new feature. In Illumio Core 21.2.0, Selective Enforcement changed from being delivered as a type of Illumio Core rule to being strictly a workload enforcement state. In 21.2.0, Enforcement Boundaries appear as a type of rule in lieu of Selective Enforcement.

PCE web console menu in 20.2.0



PCE web console menu in 21.2.0



In addition to the menu changes, other functional changes occurred. In Illumio Core 20.2.0, creating a Selective Enforcement rule allowed you to define only provider-centric enforcement by allowing traffic from a subset of applications or processes on a workload.

In Illumio Core 21.2.0, you can use Enforcement Boundaries to block traffic for both provider-centric and consumer-centric flows. An Enforcement Boundary can block traffic from communicating with workloads you specify, while still allowing you to progress toward a Zero Trust environment.

Global Explorer

IMPORTANT:
This feature is available for Illumio Core On Premises customers only.

This release provides support for asynchronous queries for every region in a Supercluster. If you initiate a query from the Supercluster leader, the results from all its members will be presented in Explorer. In the context of Supercluster, Explorer is referred to as Global Explorer.

For more information about this new feature, see Work with Explorer in the *Visualization Guide*.

Asynchronous Queries

Search queries can take time to display results depending on the size of the query. The current software allows you to initiate multiple queries when you need to, and then view the results of these queries at your convenience. This release overcomes a prior limitation with Explorer. Previously, going offline during a query resulted in lost query results. With this feature, results are preserved for 24 hours.

More importantly, after you start a query, you can work on something else in the product, while the query processing will continue until it finishes. Whether you remain online or offline, are temporarily away from your device, or come back within the day, your search results will still be available for 24 hours. The search results can either be exported to comma-separated-values (CSV) format files that capture information on traffic flows or be displayed in the Explorer PCE web console.

For more information about this new feature, see Work with Explorer in the *Visualization Guide*.

Enhancements for Explorer Results

Release 21.2.0 introduces the following capabilities:

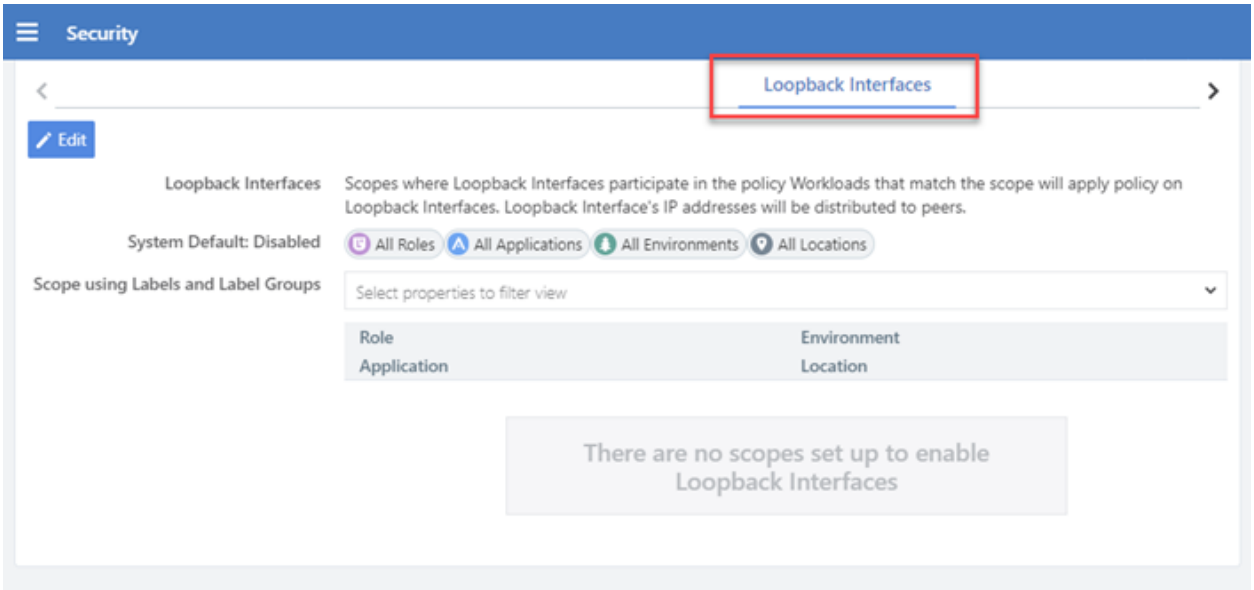
- Queries can be initiated and processed asynchronously. If you initiate a time-consuming query, you can start and run another query (or navigate away from the query page to other parts of the product) while the first query results continue to be processed. Previously, you had to wait for the first query to finish before initiating another. Now, you have the ability to run multiple queries simultaneously.
- The Load Filter drop-down will display both Recent and Saved queries. Prior to release 21.2.0, there were two separate drop-down menus for each type of query. Existing filters continue to function as they did before this release.
- A previous limitation allowed only 100,000 results from the database to be returned. This value has increased; for information, see General Advisories.

Label Groups for Role-based Access Control

You can now use label groups to grant RBAC privileges. The user who has the correct RBAC privileges (having label groups in the user's scope) can create and modify rulesets and rules that are within the scope defined in the label group. The result is simpler, cleaner, and more understandable policies, and better ease of defining the permissions for scoped user roles. See Add a Scoped Role.

Loopback Interface Support

The PCE web console and the REST API include support for the loopback interface in this release. In the PCE web console, go to **Settings** > **Security** >



Workloads that match the scope will apply policy on loopback interfaces and the loopback interface's IP address will be distributed to peers.

What's Changed in this Release

Supercluster Replication Enhancements

> IMPORTANT:
> This feature is available for Illumio Core On Premises customers only.

The commands to restore a Supercluster have changed. For the new step by step instructions, see Restore a PCE or Entire Supercluster.

- In the `supercluster-restore` command, the options `--supercluster-data-replication-timeout` and `--supercluster-config-replication-timeout` are removed and no longer needed.
- In the `supercluster-data-dump` command, the `--restore-type` option is no longer needed.
- A restoring PCE restores data from all live PCEs on the fly, as part of `supercluster-restore`. Previously, the data was restored from a file.

- Some parameter names have changed in the `supercluster-data-restore` command.
- A new `--retry-count` option has been added to all Supercluster commands. This controls how many times the command will attempt to run if an error occurs. The default is 5, and typically there is no reason to change this value.

The time required to run certain commands has changed:

- `supercluster-join` is faster, especially for customers with many regions.
- `supercluster-drop` is slower, because the command was made more robust. Many checks and retries were added to the command, so it fails less often.
- `supercluster-data-restore` is faster when restoring a single PCE, because data is no longer restored from a file.
- `supercluster-restore` might be slower when restoring a single PCE, because it restores data from all live PCEs on the fly, instead of from a file. The time required for this command depends on network latency and packet loss. Since both `supercluster-data-restore` and `supercluster-restore` commands are needed to perform a single PCE restore, the total time should be similar to the Supercluster replication process in earlier PCE versions.

LDAP Improvements

IMPORTANT:
This feature is available for Illumio Core On Premises customers only.

Earlier versions of the PCE had a restriction that required all LDAP users to be in the same branch of an LDAP tree structure. The new implementation does not require that all LDAP users be in the same branch of the directory.

As a result, the configuration of anonymous bind in the LDAP Server Create Screen has changed. The Bind DN field is now optional, not required as in previous versions. When configuring an LDAP server, choose **Allow** if you want to use anonymous bind; in this case, Bind DN is not needed. On the other hand, when using Active Directory, the use of Anonymous Bind is not recommended. Choose **Do not Allow** and specify values for Bind DN and Bind Password. In both cases, the User DN Pattern is no longer used. See Configure LDAP Authentication.

PCE behavior has also changed when multiple LDAP servers are configured. If the PCE successfully connects to an LDAP server but the user is not found, the PCE attempts to connect to the next server in the configured order, and searches for the user again.

In earlier versions, if the user is not found on the first server, the search stops. See How the PCE Works with Multiple LDAP Servers.

Enhanced Security for PCE TLS Configuration

IMPORTANT:
This feature is available for Illumio Core On Premises customers only.

For increased security, the PCE default minimum version is now TLS 1.2. Illumio recommends that you use TLS 1.2, the most secure version. However, some older operating systems might not support TLS 1.2. In these circumstances, you can change the default TLS version on the PCE. For information about changig the default TLS version, see TLS Versions for Communications.

The use of weak TLS ciphers, such as cipher block chaining (CBC) ciphers, is enabled on the PCE by default. Stronger ciphers are recommended. However, certain clients or operating systems might only be able negotiate TLS using CBC ciphers. If your managed environment if free from this limitation, Illumio recommends that you disable the use of weak TLS ciphers. See Reference: PCE Runtime Parameters in the *PCE Installation and Upgrade Guide* for more information about setting the `insecure_tls_weak_ciphers_enabled` PCE runtime parameter.

IMPORTANT:
The Illumio Core 21.2.0+H3-PCE release changes the default value of this PCE runtime parameter. The behavior change only affects customers who have already upgraded their Illumio Core PCE to 21.2.0-PCE, 21.2.0+H1-PCE, or 21.2.0+H2-PCE.

Supercluster Rolling Upgrade

IMPORTANT:
This feature is available for Illumio Core On Premises customers only.

Rolling upgrade is supported for PCEs in a Supercluster.

NOTE:
This feature is supported only when upgrading to a hotfix or a maintenance release for the PCE.

Rolling upgrade keeps the Supercluster operational while individual PCEs are upgraded one at a time. With a rolling upgrade, the Supercluster continues to operate.

Use the `--upgrade-type rolling` option on the `migrate` command:

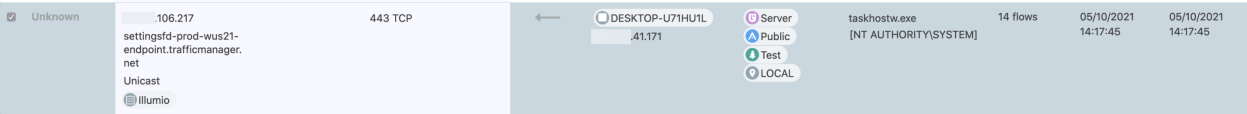
```
illumio-pce-db-management migrate --upgrade-type simple|rolling
```

For more information, see Upgrade Supercluster in the *PCE Supercluster Deployment Guide*.

FQDN Enhancements in Data Visualization

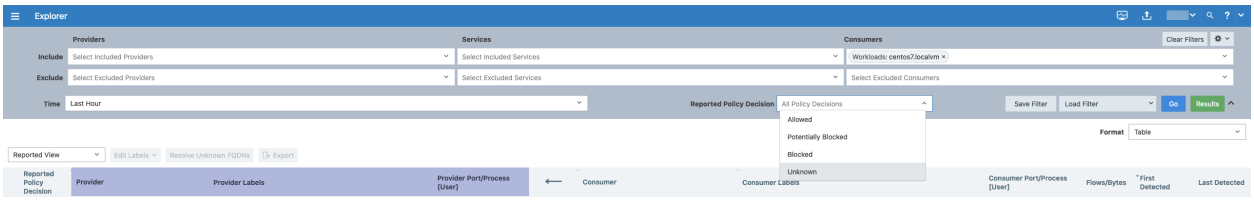
Prior to Release 21.2.0, Explorer used to display certain packets as Blocked before an FQDN policy rule was decided. After the FQDN policy rule was decided, these flows were Allowed:

In Release 21.2.0, the VEN behavior for reporting of such dropped packets before an FQDN policy decision is made, are flagged uniquely as an Unknown state. This change is visible in Explorer and Illumination. Explorer now displays these initial packets as Unknown:



The PCE interprets these flows as an unknown policy decision. When the firewall has been programmed with the FQDN rule, a subsequent reported flow displays the policy decision as Approved.

Unknown packets are stored and can be queried from the Reported Policy Decision drop-down in Explorer. This allows you to filter packets that are in an Unknown state:



Illumination displays Unknown states in Gray. Once these flows are allowed, their color changes from Gray to Green.

Uninterrupted Traffic between the VEN and the PCE

IMPORTANT:
This feature requires the Illumio Core VEN version 21.2.0 or later.

The current VEN implementation in Release 21.2.0 provides an extra layer of self-protection that prevents any erroneous policy from being applied to the VEN. The VEN employs a defensive approach that reviews policies before applying them. In case the VEN detects that the new policy may disrupt communications between the VEN and the PCE, the VEN automatically isolates that policy and logs an error in the event log. The VEN then continues to communicate with the PCE using the existing functional policy.

Prior to Release 21.2.0, if an erroneous policy was inadvertently propagated from the PCE to the VENs, it caused a permanent disruption in communications. All VENs and all workloads were impacted and would remain in an undesirable state until the correct policies were reapplied. Manual intervention was required to reload the correct policy to resume communications between the VEN and the PCE. This is no longer required.

Linux Pairing Script Activation for Proxy Servers

IMPORTANT:
This feature requires the Illumio Core VEN version 21.2.0 or later.

Typically, VENs are paired with the PCE directly. However, if a workload is behind a Web Proxy, you must follow these steps to enable your Linux/Unix VEN to successfully pair to your PCE:

1. From the PCE web console menu, choose **Pairing Profile**.
2. Copy the pairing line from the Linux/Unix OS Pairing Script window.

3. Paste this pairing line into a text file so that you can edit it.
4. Edit the pairing line to make the following two changes (displayed in **bold**):
    a. Add **–x <proxy-string>** to the curl command to indicate the proxy string.
    b. Add **--proxy-server <proxy-string>** to the switch to pass the proxy string to the pairing script.

    rm -fr /opt/illumio_ven_data/tmp && umask 026 && mkdir -p /opt/illumio_ven_data/tmp && curl **–x <proxy-string>** --tlsv1 "https://test23.io:8443/api/v18/software/ven/image?pair_script=pair.sh&profile_id=1" -o /opt/illumio_ven_data/tmp/pair.sh && chmod +x /opt/illumio_ven_data/tmp/pair.sh && /opt/illumio_ven_data/tmp/pair.sh --management-server <server fqdn> **--proxy-server <proxy-string>**
5. Paste the revised script into the Linux/Unix terminal and press **Enter**.

The workload starts the pairing process. As the pairing script runs, you will see success messages appear. Wait until you see the message "Workload has been SUCCESSFULLY paired with Illumio," which means your VEN (behind a proxy server) and the PCE are paired.

Updated SNC Capacity Requirements

The minimal and recommended sizes for CPU and memory for a single-node PCE cluster (SNC) have been updated.

For physical hardware:

- Cores: 3 (previously 2)
- RAM per node: 16GB (previously 8 GB)

For virtual machines:

- Virtual cores: 6 (previously 4)
- RAM per node: 16GB (previously 8 GB)

See Capacity Planning.

Chapter 3

What's New and Changed in the REST API

This chapter contains the following topics:

This section explains in detail all the ways that the Illumio Core REST API changed in release 21.2.0.

For information about new features in the Illumio REST API, see the *REST API Developer Guide*.

Illumio Core REST API in 21.2.2

The Illumio Core REST API v2 has changed in 21.2.2 in the following ways.

See the *REST API Developer Guide* for more information.

New REST APIs

legacy_workload_modes.schema.json

This common schema was deprecated.

The current workload enforcement modes are:

"idle", "visibility_only", "full", "selective".

```
{
        "$schema": "http://json-schema.org/draft-04/schema#",
       "description": "DEPRECATED AND REPLACED (Use enforcement_mode instead)",
```

```
        "type": "string",
        "enum": ["idle", "illuminated", "enforced"]
```

Changed APIs

pairing_profiles_get.schema.json

The new schema contains changes in capitalization of the used terminology, such as "Pairing Profile" instead of "pairing profile" and "Label" instead of "label".

In addition, for the users who created or updated the Pairing Profile, the description now includes a reference to the common schema `href_object.schema.json`.

```
},
        "created_by": {
        "type__deleted": "object",
        "required__deleted": [
                "href"
        ],
        "properties__deleted": {
                "href": {
                        "description": "User who originally created this pairing profile",
                        "type": "string"
                }
        },
        "description__added": "User who originally created this Pairing Profile",
        "$ref__added": "../common/href_object.schema.json"
},
        "updated_by": {
        "type__deleted": "object",
        "required__deleted": [
        "href"
        ],
        "properties__deleted": {
                "href": {
                        "description": "User who last updated this pairing_profile",
                        "type": "string"
                }
        },
        "description__added": "User who last updated this Pairing Profile",
```

```
        "$ref__added": "../common/href_object.schema.json"
        },
```

sec_policy_label_groups_get

The main changes for the API sec_policy_label_groups_getis that these properties are now required:

`href`, `name`, `description`, `key`, `created_at`, `updated_at`, `deleted_at`, `created_by`, `updated_by`, and `deleted_by`.

In addition, all the descriptions have been changed so that the terms such as "label", and "label group" now are written as "Label" and "Label Group".

software_ven_releases_get.schema.json

In the previous release 21.2, there were only three optional properties: `release`, `href`, and `default`.

In 21.2.2, the properties have changed as follows:

Required properties: `release`, `href`, `default`, `org_id`

Optional properties: images (object) which contains these properties: `release`, `distribution`, `architecture`, `major_version`, `min_minor_version`, and `max_minor_version`.

software_ven_releases_images_get.schema.json

In the previous release 21.2, there were these required properties: `distribution`, `architecture`, `major_version`, `min_minor_version`, `filename`, and `href`. The property `max_minor_version` is optional.

In 21.2.2, the required properties are: **`release`**(new, OS frelease), `distribution`, `architecture`, `major_version`, `min_minor_version`, `filename`, and `href`.

Only `max_minor_version` is optional.

pairing_profiles_put.schema.json

This schema is now referencing the new schema legacy_workload_modes.schema.json instead of the deprecated schema `workload_modes.schema.json`.

pairing_profiles_post.schema.json

This schema is now referencing the new schema `legacy_workload_modes.schema.json` instead of the deprecated schema `workload_modes.schema.json`.

common-workload_modes.schema.json

The current workload enforcement modes are:

"idle", "visibility_only", "full", and "selective".

Illumio Core REST API in 21.2

The Illumio Core REST API v2 has changed in 21.2.0 in the following ways.

See the *REST API Developer Guide* for more information.

New REST APIs

Asynchronous Explorer Queries

Explorer queries are required to support both the single-node and multi-node Explorer in the Supercluster environment.

The asynchronous Explorer queries include the following new APIs:

- traffic_flows_async_queries_download_get.schema.json
- traffic_flows_async_queries_get.schema.json
- traffic_flows_async_queries_post_response.schema.json
- traffic_flows_async_queries_post.schema.json
- traffic_flows_async_queries_put.schema.json

Enforcement Boundaries

Enforcement Boundaries facilitate the implementation of allow-lists by narrowing the scope for segmentation so that users can reach a high level of system maintainability using a simple policy model.

Enforcement boundaries are an extension of the selective enforcement rules. Instead of using scope and service for selective enforcement rules, they look like traditional segmentation rules use with providers, consumers, and service.

APIs for Enforcement Boundaries replace the APIs connected to Selective Enforcement as follows:

The following list indicates the previous and replacement (new) APIs for Enforcement Boundaries:

- `sec_policy_selective_enforcement_rules_get.schema.json` is replaced with `sec_policy_enforcement_boundaries_get.schema.json`

- `sec_policy_selective_enforcement_rules_post.schema.json` is replaced with `sec_policy_enforcement_boundaries_post.schema.json`
- `sec_policy_selective_enforcement_rules_put.schema.json` is replaced with `sec_policy_enforcement_boundaries_put.schema.json`

In addition to these endpoint name changes, Enforcement Boundaries appear in the following schemas:

GET /sec_policy/[:pversion]

In the request, the field `enforcement_boundaries` was added:

```
 },
        "secure_connect_gateways": {
                "type": "integer"
},
        "enforcement_boundaries": {
                "type": "integer"
}
```

In the response, the field `selective_enforcement_rules` is renamed to `enforcement_boundaries` in the `object_counts` property.

```
  },
                "object_counts": {
                "rule_sets": 164,
                "services": 326,
                "ip_lists": 95,
                "firewall_settings": 1,
                "label_groups": 28,
                "secure_connect_gateways": 18,
                "virtual_servers": 1,
                "enforcement_boundaries": 14,
                "virtual_services": 40
        }
```

POST /sec_policy

PUT /sec_policy/delete

These two APIs allow you to provision and revert a subset of policy objects in the `change_subset` field.

```
{
        "update_description": "provisioning an enforcement boundary",
        "change_subset": {
                enforcement_boundaries": [
        {
                        "href": "/orgs/2/sec_policy/draft/enforcement_boundaries/2243"
                        }
        ]
}
```

GET /sec_policy/pending

In this API, you can view a list of all policy objects pending provisioning bucketed by type. The field `selective_enforcement_rules` is replaced by `enforcement_boundaries`.

```
 },
        -    "selective_enforcement_rules":
{
        +    "enforcement_boundaries": {
                "$ref": "../common/sec_policy_pending_objects.schema.json"
        }
```

POST /sec_policy/:pversion/dependencies

This public experimental API allows you to determine provisioning or to revert dependencies for a particular policy object. The field `selective_enforcement_rules` is replaced by `enforcement_boundaries`.

```
},
        -        "selective_enforcement_rules":
```

```
{
        +        "enforcement_boundaries":
{
                "type": "array",
                "items": {
                "$ref": "../common/href_object.schema.json"
```

GET /label

The additional field `enforcement_boundaries` was appended to the he current GET schema.

```
         "blocked_connection_reject_scope": {
                "description": "Label is referenced by blocked connection reject scope",
                "type": "boolean"
        },
                "enforcement_boundary": {
                        "description": "Label is referenced by at least one enforcement
boundary",
                        "type": "boolean"
        }
}
```

In the response, `enforcement_boundary` appears as a result:

```
},
        "usage": {
                "virtual_server": false,
                "label_group": false,
                "ruleset": true,
                ...
                "enforcement_boundary": true,
        };
```

REST API Changes

Firewall Settings

The Firewall Settings schema changed and the resulting JSON applies to:

- `sec_policy_firewall_settings_get.schema.json`
- `sec_policy_firewall_settings_put.schema.json`

A new property has been added to both endpoints:

```
...
               "loopback_interfaces_in_policy_scopes": {
                  "description": "Workloads that match the scope will apply policy on
loopback interfaces and the loopback interface's IPs will be distributed
to peers.",
                  "type": "array",
                  "items": {
                       "$ref": "../common/rule_set_scope.schema.json"
                  }
```

- `loopback_interfaces_in_policy_scopes`: Workloads that match the scope will apply policy on loopback interfaces and the loopback interface's IPs will be distributed to peers.

labels_get.schema.json

This schema is no longer referencing `label_get.schema.json` and the new object has four required properties (`key`, `value`, `created_at`, and `updated_at`) and several optional ones:

```
{"$schema": "http://json-schema.org/draft-04/schema#",
       "type": "object",
       "required": [
               "key",
               "value",
               "created_at",
               "updated_at"
       ],
```

security_principals_get.schema.json

A new object named `URI of security principal` was added with the following required properties: `href`, `sid`, `name`, `deleted`, and `used_by_ruleset`.

```
 "properties": {
       "href": {
              "description": "URI of security principal",
              "type": "string"
       },
       "sid": {
              "description": "Active Directory SID (or any other unique identifier)",
              "type": "string"
       },
       "name": {
              "description": "Name of the security principal",
              "type": "string"
       },
       "deleted": {
              "description": "Flag to indicate if security principal has been
deleted",
              "type": "boolean"
       },
       "used_by_ruleset": {
              "description": "Flag to indicate if this security principal is being
used by a ruleset",
              "type": "boolean"
       }
}
```

orgs_permission.schema.json

This schema now references `org_scope.schema.json` for the scope instead of `labels_summary.schema.json`.

The earlier schema version did not specify the object type. The schema is now updated to include support for specifying label groups and follows the convention used to define rule actors in providers and consumers in the security policy.

This schema change impacts the following endpoints:

- `GET /api/v1/orgs/1/permissions`
- `GET /api/v1/orgs/1/permissions/:permission_id`
- `POST /api/v1/orgs/1/permissions`
- `PUT /api/v1/orgs/:xorg_id/permissions/:permission_id`

orgs_permissions_put.schema.json

This schema now references `org_scope.schema.json` instead of `labels.schema.json`.

LDAP Configuration

In two LDAP endpoints, the property `bind_distinguished_name` changed from `string` to `string` and `null`. This property is now `optional` instead of `required`.

- `authentication_settings_ldap_configs_put.schema.json`
- `authentication_settings_ldap_configs_post.schema.json`

Log Events

In the property `info`, the type of `null` was added.

```
 "info": {
       "type": {
              "__old": "object",
              "__new": [
                     "null",
                     "object"
              ]
       }
}
```

This type change also affects the `notification_log_event.schema-json` schema.

events_get_schema.json

This API has the following changes:

- The required property `created_by` was an object that listed several entities responsible for the creation of the event: `user`, `agent`, `container_cluster`, or `system`.

Chapter 3

Preview Features in Illumio Core 21.2

This chapter contains the following topics:

In Illumio Core 21.2.0, Illumio has introduced these preview features for the PCE and VEN software:

- RHEL 8.3 Support for PCE
- Network-Specific Policy
- Reports Preview in 21.2.0

About the Previewed Features

Illumio provides preview features for your evaluation only so that we can make them more useful for your organization's needs before general availability. Illumio welcomes your comments and suggestions for improving preview features and documentation. For more information and to send feedback, contact Illumio Customer Support.

Preview features won't appear in the PCE web console until you enable them. Contact your Support representative for instructions on how to enable a preview feature after upgrading to Illumio Core 21.2.0.

IMPORTANT:
As a rule, Illumio advises against deploying preview features in a production environment. To avoid inadvertently impacting your current system, install preview features only in a non-production environment.

RHEL 8.3 Support for PCE

IMPORTANT:
This feature is available for Illumio Core On Premises customers only.

Version 21.2.0 of the PCE supports RHEL 8.3 as a preview feature. The RHEL 8.3 version of the PCE software has a separate download RPM file. Look for "c8" in the file name.

NOTE:
If you are using 1024-bit certs, you will need to use 2048-bit (or longer) certs when moving to RHEL 8.3.

Network-Specific Policy

IMPORTANT:
This feature requires the Illumio Core VEN version 21.2.0 or later.

As a preview feature, version 21.2.0 of the PCE adds the capability to group interfaces by CIDR range and apply policies to those groups.

Reports Preview in 21.2.0

In this release the Reports feature is provided as a preview. Illumio provides preview features for your evaluation only so that we can make them more useful for your organization's needs before general availability. Illumio welcomes your comments and suggestions for improving preview features and documentation. For more information and to send feedback, contact Illumio Customer Support.

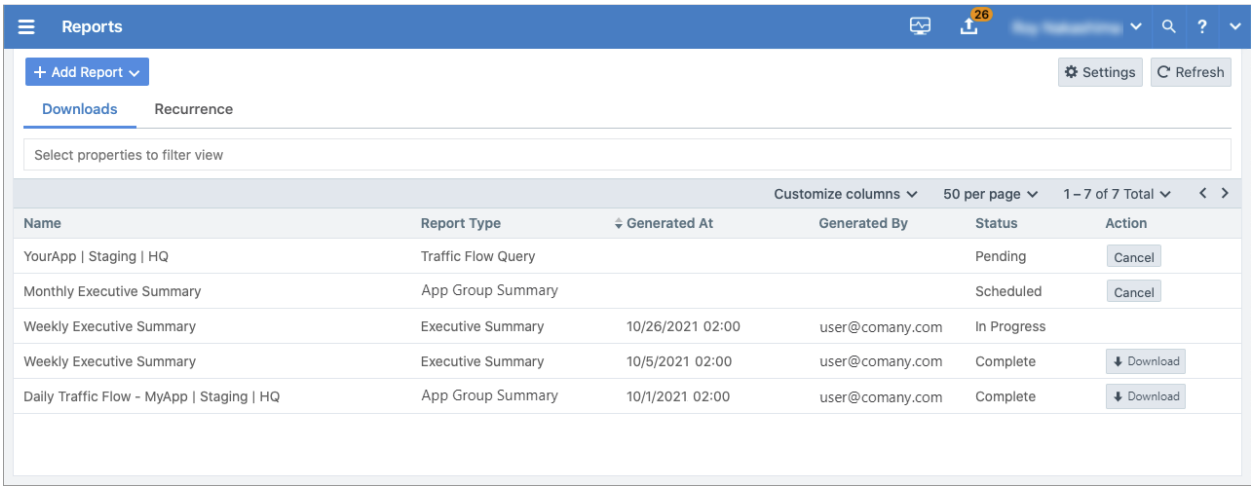
As a preview, the Reports feature won't appear in the PCE web console until you enable it. Contact your Support representative for instructions on how to enable the Reports preview feature after upgrading to Illumio Core 21.2.0.

IMPORTANT:
This feature is available for Illumio Core On Premises customers only.

About Reporting in the PCE

In 21.2.0, the PCE includes the ability to generate, download, and manage Executive Summary reports. When the Reports feature is enabled, the PCE web console menu

includes the new “Reports” option. When you choose the Reports option, the Reports page appears. This page includes two tabs: Downloads and Recurrence. Generated reports appear on the “Downloads” tab. By default, the list is sorted in descending order by the “Generated At” time.



Because Illumio provides the reports as downloadable PDF files, you can share them with people in your organization who don’t have access to the PCE web console or PCE REST API.

The data in the reports is not customizable. However, you can configure the time range of the data that the reports are generated from and the frequency at which they are run. Both types of reports include when a specific report was generated, which Illumio user generated it, and the PCE version from which the data was obtained.

Recurring reports are run on the following schedule:

- **Daily:** Midnight each day
- **Weekly:** At midnight on the first Saturday after the report was added, then weekly at Saturday midnight
- **Monthly:** Midnight on the last day of month after the report was added, then monthly on the last day at midnight

The PCE does not cap the number of reports you can create, only the length of time you can retain them. Generated reports include data for provisioned security policy, managed and unmanaged workloads, and provisioned policy objects. They do not include changes you have made to your environment but haven't provisioned.

Executive Summary Reports

Executive Summary reports are high-level by design. They provide information to decision makers, such as an organization's CISCO or VP if IT, about the overall deployment of Illumio within the organization's computing environment. These reports are intended to provide more business-oriented information than tactical data.

Executive Summary reports give the decision makers a snapshot into how Illumio policy enforcement is progressing and can display the return on investment (ROI) for purchasing and deploying Illumio software.

Executive Summary reports answer the following questions for decision makers:

- How are we progressing in deploying security policy into our environment?
- How many of our workloads are being managed by Illumio (VENs are installed on the hosts but they aren't in the enforcement state)?
- How quickly is enforcement progressing over time (the number of workloads that have moved into the enforcement state over the report's specified time range)?
- What potentially dangerous traffic is Illumio blocking that wouldn't have been blocked without Illumio Core, resulting in a security risk?
- What sort of vulnerabilities do our workloads have? Vulnerability information is provided as a V-E score that is the sum of all app groups.

IMPORTANT:
To include app group and workload vulnerability data in the Executive Summary report, you must have purchased a license for the Vulnerability Map feature. The Vulnerability Map is a separately licensed feature of Illumio Core. The licensing is based on the number of workloads. The license is required to import Qualys report data into the Illumio PCE. For information about obtaining the Illumio Core Vulnerability Map license, contact Illumio Customer Support.

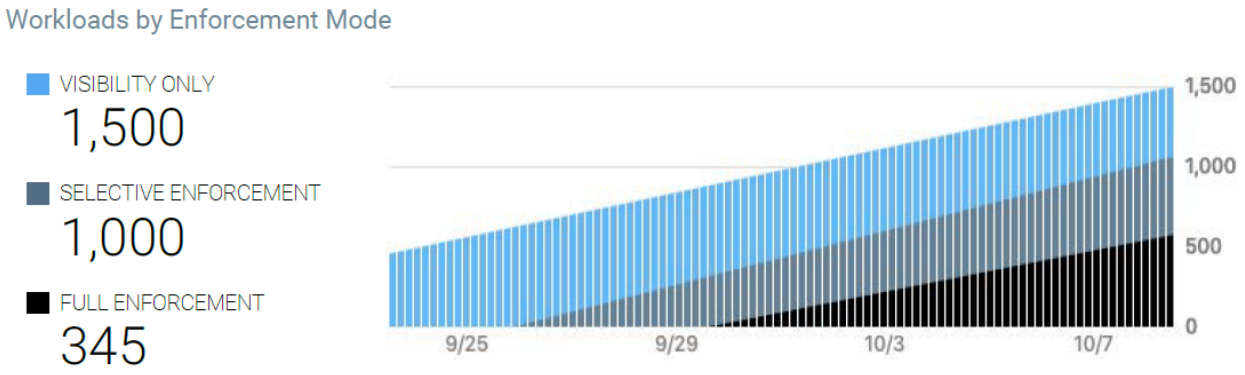
For more information about Vulnerability Maps, see Vulnerability Map in the *Visualization Guide.*

To see all the categories of data included in an Executive Summary report, see the Sample Illumio Core Executive Summary Report 21.2.0 available in this documentation portal.

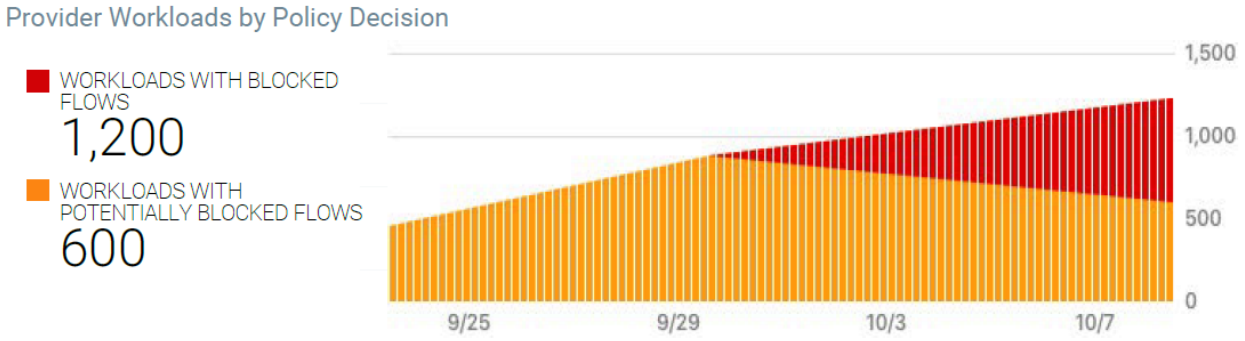
Tips for Reading Executive Summary Reports

Executive Summary reports provide high-level information for decision makers. They are meant to show trends and patterns in your roll out of Illumio Core into your data center environment.

For example, an executive who has approved deploying Illumio Core might want to know how many of their workloads are being managed (enforced) by Illumio policy. The Workloads by Enforcement Mode graph shows the trend for how quickly is enforcement progressing over time and percentage of workloads in deployment versus enforcement.



The Provider Workloads by Policy Decision graph can help confirm when the segmentation rules you have created for your data center look viable and you can start enforcing policy on your workloads. This example graph shows a tend you want to see; and visually represents how you initially had workloads deployed but not in enforcement.



Add a Report

1. From the PCE web console menu, choose **Reports**. The Reports page appears.
2. Click **Add Report** and select the report type from the drop-down menu.

A dialog box appears so that you can configure the report.

3. Configure the following report settings and click **Save**:
    - **Name:** Specify a name that describes the purpose of the report. Report names must be from 2-255 characters and can contain special characters.
    - **Recurrence:** From the drop-down list, select how frequently the PCE will run the report.
    - **Time Range:** From the drop-down list, select the time range for the report (the time range differs by report type).

The new report appears on the **Recurrence** tab.

Manage Reports

Perform the following tasks to manage how you generate reports for your organization and computing environment.

To set the retention period for all reports:

You can configure globally how long the PCE retains the PDF files generated for each report you add. You can only retain PDF files up to 7 days in the PCE. By default, reports are configured to be retained 7 days.

1. From the PCE web console menu, choose **Reports**. The Reports page appears.
2. Click **Settings** in the top right corner of the page.
3. In the Retention field, specify the number of days to retain PDF files.
4. Click **Save**.

To download a report:

1. From the PCE web console menu, choose **Reports**. The Reports page appears.
2. Click the **Downloads** tab.
3. In the row of a completed report, click the **Download** button.

To edit the settings for a report:

1. From the PCE web console menu, choose Reports. The Reports page appears.
2. Click the Recurrence tab.
3. Click the row for the report you want to modify.
4. Change the recurrence rate, time range, or report name.
5. Click **Save**.

To end the recurrence of a report:

Removing a report from the Recurrent tab stops the report from running again. Existing PDF files generated for the report remain in the PCE until the global retention period expires and they are deleted by the PCE.

1. From the PCE web console menu, choose **Reports**. The Reports page appears.
2. Click the **Recurrence** tab.
3. Click the row for the report you want to stop being regenerated.

   A dialog box appears prompting you to confirm that the report won't be generated again.
4. Click **Remove**.