Illumio Core®

Version 21.5

What's New in This Release

March 2023

14000-200-21.5

Legal Notices

Product Version

PCE Version: 21.5 (LTS Release)

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

Chapter 1

Welcome to Illumio Core 21.5

This chapter contains the following topics:

Illumio is pleased to announce the general availability of version 21.5 of the Illumio Core for the PCE. 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 21.5 release.

Product Versions

PCE Version: 21.5.35 (LTS) | Illumio Core On-Premises customers and Illumio Core Cloud customers

VEN Version: 21.5.32 (LTS)

For the complete list of Illumio Core components compatible with Illumio Core 21.5.*x*-PCE, see the Illumio Support portal (log in required).

Standard versus LTS Releases

21.5.35-PCE and 21.5.32-VEN are LTS releases. For information on Illumio software support for Standard and LTS releases, see Versions and Releases on the Illumio Support portal.

Release Types and Numbering

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

- “a.b”: Standard or LTS release number, for example “21.5”
- “.c”: Maintenance release number, for example “.0”
- “-d”: Optional descriptor for pre-release versions, for example “preview2”

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 21.5.30 PCE is supported on operating systems detailed on the Illumio Support portal.

For information, see PCE OS Support and Package Dependencies.

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 for information.

The Upgrade to This Release

As part of the upgrade process, Illumio strongly encourages you to review the prior release notes from your previously installed version of Illumio Core to version 21.5.30.

You have the option to upgrade the VENs in your environment at any time. For information about the upgrade path and tools, go to the Illumio Support portal and review the VEN Upgrade paths (login required).

Announcements

End of Support Announcements, Deprecations , Compatibility

End of Support

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 is no longer supported in Illumio Core 19.2 and later releases. Illumio recommends Chrome, Edge, or Firefox for use with the PCE web console.

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.

Chapter 2

What's New and Changed in This Release

This chapter contains the following topics:

Before upgrading to Illumio Core 21.5.*x*, 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 21.5.35

Illumio Core 21.5.35 introduces the following enhancements.

IMPORTANT:
Illumio Core 21.5.35-PCE is available for Illumio Core On-Premises customers only.

21.5.35 Illumio Core Maintenance Release

The 21.5.35 maintenance release is available for the PCE.

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 21.5.35-PCE solved software and security issues for the PCE only 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 21.5.35-PCE" in the Illumio Core Release Notes 21.5.x.

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

Documentation Updates for Core 21.5.35-PCE

The *PCE Installation and Upgrade Guide* for Core 21.5.35 no longer includes documentation for the `kernel.shmmax` parameter. Prior to Core 21.5.35, the guide recommended that you set `kernel.shmmax` to 60000000. As of Postgres13, you no longer need to change the `kernel.shmmax` value.

Upgrade Paths from Core 21.5.35-PCE

After you upgrade your PCE to Core 21.5.35, you cannot upgrade to the Core 22.2.40-PCE release. Instead, you must upgrade the PCE to a release of Core 22.2.x delivered after the 22.2.40-PCE release. Alternatively, you can upgrade to Core 22.5.10-PCE or later.

What's New and Changed in Release 21.5.34

Illumio Core 21.5.34 introduces the following enhancements.

> **IMPORTANT:**
> Illumio Core 21.5.343-PCE is available for Illumio Core On-Premises customers only.

21.5.34 Illumio Core Maintenance Release

The 21.5.343 maintenance release is available for the PCE.

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 21.5.343-PCE solved software and security issues for the PCE only 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 21.5.34-PCE" in the Illumio Core Release Notes 21.5.x.

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 21.5.33

Illumio Core 21.5.33 introduces the following enhancements.

IMPORTANT:
Illumio Core 21.5.33-PCE is available for Illumio Core On-Premises customers only.

21.5.33 Illumio Core Maintenance Release

The 21.5.33 maintenance release is available for the PCE.

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 21.5.33-PCE solved software and security issues for the PCE only 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 21.5.33-PCE" in the Illumio Core Release Notes 21.5.x.

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 21.5.32

Illumio Core 21.5.32 introduces the following enhancements.

IMPORTANT:
Illumio Core 21.5.32-PCE is available for Illumio Core On-Premises customers only.

21.5.31 Illumio Core Maintenance Release

The 21.5.32 maintenance release is available for both the PCE and VEN.

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 21.5.32-PCE solved software and security issues for the PCE 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 21.5.32" in the Illumio Core Release Notes 21.5.x.

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 21.5.31

Illumio Core 21.5.31 introduces the following enhancements.

IMPORTANT:
Illumio Core 21.5.31-PCE is available for Illumio Core On-Premises customers only.

21.5.31 Illumio Core Maintenance Release

The 21.5.31 maintenance release is available for both the PCE and VEN.

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 21.5.31-PCE solved software and security issues for the PCE only 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 21.5.31" in the Illumio Core Release Notes 21.5.x.

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 21.5.30

Illumio Core 21.5.30 introduces the following enhancements.

IMPORTANT:
Illumio Core 21.5.30-PCE is available for Illumio Core On-Premises customers only.

21.5.30 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 21.5.30-PCE solved software and security issues for the PCE only 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 21.5.30" in the Illumio Core Release Notes 21.5.x.

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

VEN Supported on SUSE Linux Enterprise Server 11 SP2

The VEN can be installed on systems running SLES 11 SP2 when the following packages are installed:

From the SLES 11 SP2 Latest Updates:

- libipset2-6.12-0.7.7.1
- ipset-6.12-0.7.7.1
- libmnl0-1.0.3-0.5.4
- kernel-default-3.0.101-0.7.17.1
- kernel-default-base-3.0.101-0.7.17.1

From the SLES 11 SP4 DVD:

- libxtables9-1.4.16.3-1.37
- libiptc0-1.4.16.3-1.37
- iptables-1.4.16.3-1.37
- libnfnetlink0-1.0.0+git1-9.5.56

What's New and Changed in Release 21.5.21

Illumio Core 21.5.21 introduces the following enhancements.

IMPORTANT:
Illumio Core 21.5.21-PCE is available for Illumio Core On-Premises customers only.

21.5.21 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 21.5.21-PCE solved software and security issues for the PCE only 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 21.5.21-PCE" in the Illumio Core Release Notes 21.5.x.

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 21.5.20

Illumio Core 21.5.20 introduces the following enhancements.

IMPORTANT:
Illumio Core 21.5.20-PCE is available for Illumio Core On-Premises customers and Illumio Core Cloud customers.

21.5.20 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 21.5.20 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 21.5.20" in the Illumio Core Release Notes 21.5.x.

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

Change for Traffic Collector APIs

For all Traffic collector APIs, the `unicast` transmission type was added to the properties.

- `GET /settings_traffic_collector`
- `POST /settings_traffic_collector`
- `PUT /settings_traffic_collector`

The transmission types are now `broadcast/multicast/unicast`.

What's New and Changed in Release 21.5.12

Illumio Core 21.5.12 introduces the following enhancements.

21.5.12 Illumio Core Maintenance Release

> IMPORTANT:
> Illumio Core 21.5.12-PCE is available for Illumio Core On Premises customers 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 21.5.12 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, see "Resolved Issues in 21.5.12-PCE" in the Illumio Core Release Notes 21.5.x.

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 21.5.11

Illumio Core 21.5.11 introduces the following enhancements.

21.5.11 Illumio Core Maintenance Release

Illumio Core 21.5.11 is a maintenance release for the Illumio VEN.

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 21.5.11 solved software and security issues for the VEN to refine the VEN software and improve its reliability and performance.

For the complete list of improvements and enhancements to the PCE and VEN, see "Resolved Issues in 21.5.11-VEN" in the Illumio Core Release Notes 21.5.x.

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 21.5.10

Illumio Core 21.5.10 introduces the following new features and enhancements.

> IMPORTANT:
> Illumio Core 21.5.10 are available only for Illumio Core On Premises customers who install Illumio Core in their own data centers.

21.5.10 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 21.5.10 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 21.5.10" in the Illumio Core Release Notes 21.5.x.

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

VEN Enhancements

The following enhancements were added in Illumio Core 21.5.10

Support on IBM Z With RHEL 7 and RHEL 8

In this release, the system supports installing and operating the VEN on IBM Z systems running Red Hat Enterprise Linux 7 (RHEL 7) and RHEL 8.

Label-based Security Setting for IP Forwarding

Illumio has enabled IP forwarding to hosts running Linux. A container networking solution routes the traffic to the VMs. To configure IP forwarding, use the new IP Forwarding tab in the PCE web console. In this tab, you can use labels and label groups to enable IP forwarding for the workloads that match the label combination.

To enable this feature, contact Illumio Support. For details about how to set up IP forwarding for workloads, see Connectivity Settings in the PCE Administration Guide.

VEN Compatibility Report Updates for IPv6 Support

Illumio supports IPv6 for workloads. This includes providing a warning in the Compatibility Report. The Compatibility Report is used to detect the possible issues before moving VEN out of idle state. See VEN Compatibility Check in the *VEN Installation and Upgrade Guide*. In this release, Illumio updated the options in the Compatibility Report to increase it's usability.

The following command and command options are supported:

- On Linux and SunOS, this command option is available regardless of whether IPv6 is enabled:
  - ipv6_forwarding_enabled
    - At least 1 iptables forwarding rule is detected in the IPv6 forwarding chain. VEN removes existing iptables rules in the non-Idle policy state.
- On Windows, we do not support all IPv6 transition tunnels that is a part of the IPv6 transition technology (RFC 4213). The following options are available:
  - teredo_tunneling_enabled
    - Teredo tunneling allows for IPv6 connectivity.
    - Teredo is an IPv6 transition tunnel.
    - We do not report on Teredo adapters.
  - IPv6 enabled
    - Continues to be supported.
    - Detects potential transition technology usage on Windows.

VEN Support on Rocky Linux

Beginning in the 21.5.10 release, the VEN is supported on the Rocky Linux OS.

PCE Platform Enhancements

In addition to the information provided in the release notes, this release optimizes PCE policy in the following ways.

Policy Provisioning Operations Optimized

In environments that use many label groups with Virtual Servers or Virtual Services, this release provides faster computation and delivery of policy changes to affected workloads, as well as faster policy provisioning overall.

Improved Performance for Container Workloads

In this release, Illumio provides improved performance by programming container host CIDRs instead of container host IP addresses. For traffic initiated by a container workload and destined for outside the container cluster, the PCE replaces the container host's IP address in the external workload's inbound policy with the subnet(s) for all container hosts in the container cluster. The subnets are constructed using the IP addresses and subnet masks of IPv4 host network interfaces, with a default gateway, as reported by the VEN on container hosts. This enhancement avoids a policy recalculation on workloads outside the cluster when the following events occur:

- Scaling up of a Kubernetes service
- Deleting and recreating of a Kubernetes pod on a different node in the cluster
- Replacing of a Kubernetes node for upgrade or patch reasons.

By eliminating policy updates for workloads outside the cluster, this enhancement helps reduce the amount of time required to establish communication between the pod in the cluster and a workload outside the cluster.

IMPORTANT:
This feature must be enabled via the PCE `runtime_env.yml` using the following configuration:

```
agent_service:
use_container_host_cidrs_in_container_policy: true
```

Improved Convergence Times

In this release, Illumio provides improved convergence times by preventing unnecessary IP address list updates. Previously, inbound policies on Virtual Servers were updated with all workload IP addresses, including the IP addresses of container workloads that are routable only within the Container Cluster. This occurred even though Virtual Servers outside a Container Cluster never see inbound traffic directly from a Container Workload IP. Now, with this enhancement, Container Workload IP addresses local to a Container Cluster are no longer delivered to Virtual Servers. This prevents unnecessary updates to the list of Container Workload IP addresses maintained on the SLB device that were caused by updates to Container Workloads.

This optimization, combined with the Improved Performance for Container Workloads enhancement, significantly decreases or eliminates the time required before a Virtual

Server outside the Container Cluster allows inbound traffic from a Container Workload.

IMPORTANT:
This feature must be enabled via the PCE `runtime_env.yml` using the following configuration:

```
agent_service:
exclude_container_ips_in_virtual_server_policy: true
```

Improved Performance for Kubelink Service Updates

In this release, Illumio provides improved performance by batch processing Kubelink service updates. Previously, when Kubelink cluster service updates occurred, the PCE immediately provisioned the changes to virtual services. Now, with this enhancement, the PCE aggregates the Kubelink-reported changes across all clusters and provisions the changes as batch updates. In environments with many container clusters and/or high rates of change to cluster services, this enhancement helps reduce PCE load and decreases policy distribution times.

If enabling this enhancement in a Supercluster, do so only in an environment where the container clusters are paired to the leader PCE.

IMPORTANT:
This feature must be enabled via the PCE `runtime_env.yml`. The value you specify in the `runtime_env.yml` setting determines the provisioning interval. Illumio has only certified a value of 180 seconds for this setting. Use the following configuration:

```
agent_service:
container_cluster_service_provision_interval_seconds: 180
```

Rotate Database Passwords and Other Secrets

At any time, an Illumio Administrator can rotate the PCE database passwords and other auto-generated secrets used within the PCE. The new secrets take effect when the PCE is restarted. To rotate secrets, run the following command on any node:

```
sudo -u ilo-pce illumio-pce-ctl rotate-secrets
```

In a Supercluster, run this command once for each region.

What's New and Changed in Release 21.5.4

Illumio Core 21.5.4 introduces the following enhancements.

IMPORTANT:
Illumio Core 21.5.4-PCE was available for Illumio Cloud customers only. This release was not available for Illumio Core On Premises customers to download to install in their data centers.

Illumio Core 21.5.4-PCE Release

In Illumio Core 21.5.4-PCE, the PCE for Illumio Core Cloud customers now supports endpoints that are joined only to Azure Active Directory (Azure AD) when using a 21.5.10 VEN paired using endpoint mode.

For information about pairing the Illumio VEN using `endpoint` mode, see "How to Install VENs By Using a Pairing Script" in .the Endpoint Installation and Usage Guide.

IMPORTANT:
Illumio Core 21.5.4-PCE was not generally available across all Illumio Core Cloud environments.

For information about the Illumio Core 21.5.3-PCE release, see What's New and Changed in 21.5.3.

To locate your Illumio Core Cloud release version, go to the drop-down menu in the top-right bar of PCE web console and view the About Illumio page.

For additional information about this release, contact your Illumio Support representative.

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 21.5.3

Illumio Core 21.5.3 introduces the following enhancements.

IMPORTANT:
Illumio Core 21.5.3-PCE is available for Illumio Cloud customers only. This release is not available for Illumio Core On Premises customers to download to install in their data centers.

21.5.3 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 21.5.3 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, see "Resolved Issues in 21.5.3-PCE" in the Illumio Core Release Notes 21.5.x.

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

What's New and Changed in Release 21.5.2

Illumio Core 21.5.2 introduces the following enhancements.

IMPORTANT:
Illumio Core 21.5.2-PCE is available for Illumio Cloud customers only. This release is not available for Illumio Core On Premises customers to download to install in their data centers.

21.5.2 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 21.5.2 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, see "Resolved Issues in 21.5.2-PCE" in the Illumio Core Release Notes 21.5.x.

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 21.5.1

Illumio Core 21.5.1 introduces the following enhancements.

21.5.1 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 21.5.1 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, see "Resolved Issues in 21.5.1-PCE" in the Illumio Core Release Notes 21.5.x.

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

What's New and Changed in Release 21.5

Illumio Core 21.5.0 introduces the following new features and enhancements.

New Features in This Release

The following new features were added in Illumio Core 21.5.

Core Services Detector

Core services (such as DNS, Domain Controller, NTP, and LDAP) are essential to your computing environment and run on one or multiple workloads. The Core Service Detector feature helps you identify these core services and suggests an appropriate label for them. The Illumio PCE can detect 51 core services. Identifying and labeling these workloads is important because they are centrally connected, and other applications depend on them.

Application owners sometimes don't know enough about the core services or how to identify them. In addition, different teams could be managing core services, and application owners must coordinate with these teams to secure their applications. When you use the Core Services Detector to label and write policies for core services, you can save time on application policies and progress to policy enforcement faster.

To learn how to set up and manage core services by using the PCE web console, see Core Services Detector the *Security Policy Guide*

To learn more about the REST APIs for core services, see Core Services Detection in the *REST API Developer Guide*.

Core Services Identification, Review, and Labeling

Core Services Detector uses a three-step process to identify core services:

- **Detect** : Run Detection Tool in the backend to recommend potential Core Services (workloads running core services). Follow the steps described in Detect Core Services.
- **Review** : Review recommendations provided by Detection Tool and accept or reject them following the steps described in Review the Detected Core Services.
- **Label** : Label accepted recommendations as described in Label the Detected Core Services.

Detection Methods

There are three ways to detect a core service of which the first two are used only for Active Directory.

- **Port Matching**: Rule-based model based on connections to specific ports
- **Port-based ML**: Machine learning model based on connections to specific ports
- **Process-based ML**: Machine learning model based on processes running on the server

These methods are NOT configurable, and all three algorithms run all the time.

PCE Support Report Bundles

In previous releases, PCE support reports could be generated using a CLI command. In 21.5, the PCE web console has a new Support Bundles page where you can generate PCE support reports.

1. Choose **Troubleshooting** > **PCE Support Bundles** from the main dropdown menu.
2. Click **Generate**.

   The support bundle generation dialog box appears.
3. (Optional) Click **Log Collection** and specify the time range.
4. Click **Generate** again in the dialog box.

   The dialog disappears. The PCE Support Bundles tab displays the report generation status for each node. When the reports for all nodes are complete, an aggregate support bundle is made available for download.
5. Click **Download**.

Up to five previously generated PCE support bundles remain available for download in a list on the PCE Support Bundles tab.

Node Hardware Requirements Alert

In the PCE Health page of the PCE web console, a message is now displayed to tell whether the hardware provisioned for each node meets the requirements as documented for the PCE in the Capacity Planning section of the PCE Installation and Upgrade Guide.

If a node is found to have sufficient resources to meet specifications, the message "Node Specs Meet requirements" appears with a green check mark. If the node does not have sufficient resources to meet the required specifications, the alert "Node Specs Do not meet requirements" appears with a yellow triangle.

The hardware requirements vary depending on the type of PCE cluster (single-node, 2x2 multi-node, 4x2 multi-node). The hardware requirements check needs to know the cluster type so it can use the right set of hardware requirements.

WARNING:
Because the hardware requirements check needs to know the cluster type, it is now required that you set the `cluster_type` runtime parameter for every node. This parameter was previously optional.

Surface All Hidden Rules (Essential Rule Services)

The PCE web console main menu includes a new tab in the Security section for hidden rules. The menu choice open a page displaying a list of essential services used by the PCE. For more information, see the *PCE Administration Guide*.

PCE Platform Changes

New Cluster Type

A new value for the runtime parameter `cluster_type` has been added: `4node_v0_small`. Use this cluster type for a 2x2 cluster that has smaller hardware requirements the previously available 2x2 cluster type, `4node_v0`. For details about the requirements of a small 2x2 cluster, see Capacity Planning in the PCE Installation and Upgrade Guide.

Choose to Include Hostname or FQDN in Syslog

In syslog messages, the hostname is included by default. You can choose to use the FQDN instead of the hostname if this would help your organization to more easily distinguish messages from different hosts. To do so, set the following new flag in `runtime_env.yml`:

```
internal_syslog_fqdn_enabled: true
```

NTP Check

After you finish installing the PCE, you can use the following command to check that the PCE environment is set up correctly. This command now also verifies that the NTP client is installed, running, and synchronized to a time source.

```
# sudo -u ilo-pce illumio-pce-env check
```

Enhanced F5 Key Security

All F5 load balancer passwords stored in the PCE database are now encrypted at rest. These passwords are used by the NEN when it needs to program a load balancer.

Customizable NEN Encryption Key

The Network Enforcement Node uses an encryption key to encode and store certain customer secrets, such as switch passwords. This key is now customizable. In previous releases, a default encryption key was automatically generated. If your organization has more stringent cryptographic requirements, you can elect to provide your own 256-bit encryption key, or randomly generate one, for all the nodes in the cluster. This key must match on all nodes.

Application Metrics

The PCE now records additional application metrics data about the PCE. These enhanced application metrics increase our ability to troubleshoot PCE issues and resolve them faster. Illumio Support will guide you on how to obtain and send the application metrics when needed.

Two processes run on the PCE to collect application metrics:

- telegraf, an open-source metrics collection agent,runs on all core and data nodes.
- InfluxDB, an open-source time series database, runs on all data nodes.

Supercluster 8-Region Support

A Supercluster can now have a maximum of 8 PCEs.

Enhancements in Core 21.5.0

Postgres 13.x

The version of Postgres used by the PCE is now Postgres 13.x. As a result, it is very important to take a backup of your PCE before upgrading to 21.5.0. This step is included in the upgrade procedure, Upgrade the PCE in the PCE Installation and Upgrade Guide. Because of the Postgres 13.x upgrade, it is even more important not to skip this backup step when upgrading.

Improved Parallel Coordinates Format in Explorer

In Explorer, search results using the Parallel Coordinates format are improved as follows:

- A new axis called Consumer Process was added.
- For clarity, the Process axis was renamed Provider Process.

Feature Name Update

In previous releases, this feature was referred to as “Segmentation Rulesets.” In Illumio Core 21.5.0 and later releases, this feature is now referred to as “Rulesets”

VEN Robustness and Reliability

In this release, Illumio has enhanced the VEN functionality so that is more reliable and recovers from errors more effectively. These enhancements are internal to the VEN functionality.

Support for Windows Run As as a Different User with AUS

When using the Adaptive User Segmentation (AUS) feature, the VEN now recognizes when a user is running as a different user. When a user logs in, the VEN check whether the user belongs to the group represented by the group ID, and if it does, it updates policy.

VEN Support for Debian 11

In this release, you can install the VEN on workloads running Debian 11.

Documentation Changes

Updated Supercluster Migration Steps

The documented steps to migrate a Supercluster have been updated with additional useful information.

- Pre-configuring the IP addresses is required only on the PCE that is to be migrated. See Migrate to New Supercluster in the PCE Supercluster Deployment Guide.
- The need to update the `runtime_env.yml` file on data nodes has been added, where previously only core nodes were listed. See Pre-Configure New IP Addresses in the PCE Supercluster Deployment Guide.
- When updating `runtime_env.yml` with additional IP addresses, if more than one PCE is being migrated, the steps should be followed for one PCE at a time. In addition, the restart operation should be run first on the PCE that was migrated. After that PCE is up and all services are running, restart the other PCEs. See Pre-Configure New IP Addresses in the PCE Supercluster Deployment Guide.

Illumio Core REST API in 21.5

The Illumio Core REST API v2 has changed in 21.5.0 in the following ways.

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

New Public Stable APIs

Lots of APIs have changed exposure from Public Experimental to public Stable.

Public Experimental APIs changed to Public Stable APIs

- `audit_event_min_severity.schema.json`
- `destination_get.schema.json`
- `health_definitions.schema.json`
- `health_get.schema.json`
- `health_status_percent.schema.json`
- `orgs_access_restrictions_get.schema.json`
- `orgs_access_restrictions_post.schema.json`
- `orgs_access_restrictions_put.schema.json`

- org_scope.schema.json
- orgs_permission_get.schema.json
- orgs_permission.schema.json
- orgs_permissions_get.schema.json
- orgs_permissions_post.schema.json
- orgs_permissions_put.schema.json
- pairing_profiles_get.schema.json
- pairing_profiles_post.schema.json
- pairing_profiles_put.schema.json
- permission_uri.schema.json
- resource_update_info.schema.json
- settings_events_get.schema.json
- settings_events_put.schema.json
- settings_syslog_destinations_get.schema.json
- settings_syslog_destinations_post.schema.json
- settings_syslog_destinations_put.schema.json
- settings_traffic_collector_get.schema.json
- settings_traffic_collector_post.schema.json
- settings_traffic_collector_put.schema.json
- settings_trusted_proxy_ips_get.schema.json
- settings_trusted_proxy_ips_put.schema.json
- settings_workload.schema.json
- settings_workloads_get.schema.json
- settings_workloads_put.schema.json
- users_post.schema.json
- workloads_bulk_create_put.schema.json
- workloads_bulk_delete_put.schema.json
- workloads_bulk_update_put.schema.json

New Public Experimental APIs

APIs for Managing Core Services

Users have the ability to change port numbers on which a specific core service is running so that they can adjust them to their environment. They cannot change ports using the UI, only the APIs.

The user authorized to manage core services is the Organization Administrator.

Common schemas for managing core services

- `core_services_labels.schema.json`
- `core_services_type_ports_def.schema.json`
- `core_services_type_ports.schema.json`

Core Services Methods

Functionality	HTTP	URI
Fetch all detected core services for this org. Retrieve and examine core services identified by the PCE.	`GET`	`[api_version][org_href]-detected_core_services`
Get a detected core service by UUID	`GET`	`[api_version][org_href]/-detected_core_services/<uuid>`
Get detected core service summary details. Retrieve a summary of the detected core services.	`GET`	`[api_version][org_href]/-detected_core_services_summary`
Get a detected core service by UUID. Accept, reject or skip the core service recommendation. Take the appropriate action for the identified core services: accept the recommendation to apply the suggested labels to the workload.	`PUT`	`[api_version][org_href]/-detected_core_services/<uuid`
Fetches all core service types for this org. Get the list of core service types, including: • core service name • port information • suggested labels	`GET`	`[api_version][org_href]/core_service_types`

Functionality	HTTP	URI
This information has previously been referred to as the core service 'bible'.		
Fetches core service type by UUID	GET	[api_version][org_href]/core_service_types/<uuid>
Edit suggested labels of a core service type for the organization.	PUT	[api_version][org_href]/core_service_types/<uuid>

New Parameters for Core Services

Parameter	Description
max_results	Maximum number of results to be returned
action	Action that is taken on the detected core services such as accept/skip/reject.
core_service_type	Get all detected core services of a particular type, such as Splunk/NFS. The hrefwill be given in the query parameter.

Sample URLs and Payloads

GET /api/v2/orgs/1/detected_core_services/ ddfe5204-ad29-4bcd-9821-fcb62353a985

```
{
        "href" :  "/orgs/1/detected_core_services/ddfe5204-ad29-4bcd-9821-fcb62353a985" ,
        "ip_address" :  "103.10.11.44" ,
        "workload" : {
                "hostname" :  "SE555Q5" ,
                "href" :  "/orgs/2/workloads/e62d71b3-36c4-4c27-926b-411b93ba6d6f" ,
                "labels" : []
        },
        "core_service_type" : {
                "href" :  "/orgs/1/core_service_type/3555d1e4-fcb2-49c2-9a4a-215c4d5e36dc"
        },
        "confidence" :  100 ,
        "method_name" :  "process_based" ,
        "created_at" :  "2020-08-04T05:02:46.648Z" ,
        "updated_at" :  "2020-08-04T05:02:46.648Z" ,
        "last_detected_at" :  "2020-09-05T05:02:46.648Z"
}
```

PUT /api/v2/orgs/1/detected_core_services/3ddd5204-ad29-4bcd-9821-fcb62353a98f

```
Example  1 :
       { "action" : "accept" }

Example  2 :
       { "action" : "accept" ,  "workload" :{ "href" :  "/orgs/2/workloads/e62d71b3-
36c4-4c27-926b-411b93ba6d6f" }} # for   the  case   when an IP is converted to
UMWL and accepted as core service

Example  3 :
       { "action" : "reject" }

Example  4 :
       { "action" : "reject" ,  "feedback" : "Not a core service." }

Example  5 :
       { "action" : "skip" ,  "feedback" : "Check with Ops if this is a core service." }

Example  6 :
       { "labels_applied" : true }
```

GET /api/v2/orgs/ :xorg_id /core_service_types/44dd5204-ad29-4bcd-9821-fcb62353a98f

```
{
       "href" : "/orgs/2/core_service_type/44dd5204-ad29-4bcd-9821-fcb62353a98f" ,
       "core_service" : "splunk" ,
       "required_ports" :[{ "port" : 9997 ,  "to_port" : 10000 }],
       "optional_ports" :[{ "port" : 112 }, { "port" : 455 }],
       "labels" : [
       {
              "value" : "app-splunk" ,
              "key" :  "app"
              "href" : "/orgs/1/labels/2"
       },
       {
              "value" : "role-splunk" ,
```

```
                "key" :  "role" ,
                "href" : "/orgs/1/labels/12"
        } ],
                "created_at" :  "2020-08-04T05:02:46.648Z" ,
                "updated_at" :  "2020-08-05T05:02:46.648Z"
}
```

PUT /api/v2/orgs/ :xorg_id /core_service_types/44dd5204-ad29-4bcd-9821-fcb62353a98f

```
{
"labels" : [
        {
                "href" : "/orgs/1/labels/3"
        },
        {
                "href" : "/orgs/1/labels/10"
        }]
}
```

Optional Features

This API was introduced to help avoid issues with misconfigured DNS, which can cause problems with VEN connectivity. Likewise, misconfiguring DHCP can cause problems with IP addresses.

When you invoke `/optional_features` API to enable `editable_dns_client_rule` or `editable_dhcp_client_rule` , a key is required. Such a key involves a portion that is tightly controlled so that it cannot be randomly generated.

Once the key is generated, it cannot be used in more than one place, which means that an API call provided to customer #1 cannot be replayed at customer #2 who must request their own key.

An example of the generated key:

```
secret =  '...'   # value embedded in code
```

```
       data = Base64.strict_encode64({
       'pce_fqdn'   => Illumio::RuntimeEnvironment.pce_fqdn,
       'org_id'   => xorg_id,
       'optional_feature'   =>  'editable_dns_client_rule' ,
       'not_valid_after'   => Time.now.utc.iso8601
})

key = data + OpenSSL::HMAC.hexdigest( 'SHA256' , secret, data)
```

A new schema as well as two endpoints were added:

- `optional_feature.schema.json`
- `optional_features_get`
  Get the optional features collection
- `optional_features_put`
  Set the optional features for an organization

```
PUT /orgs/ 1 /optional_features
[
       { "name" :  "editable_dns_client_rule, " enabled ": true, " key": ( key as
generated above )}
]
```

orgs_roles_get

The APIs GET roles and GET role_name have been promoted from Internal to Public Experimental.

They allow the users to list user roles and role names:

- `/orgs/:xorg_id/roles, GET`

  Get the roles in the org
- `/orgs/:xorg_id/roles/:role_name, GET`

  Get information for this role name

Support Bundle Requests

Several APIs have been introduced to provide a mechanism to generate a support bundle on each node, including a time range and possibly additional options.

The APIs have the following functions:

- `/orgs/:xorg_id/support_bundle_requests, GET`
  Return the collection of PCE support bundle requests
- `/orgs/:xorg_id/support_bundle_requests, POST`
  Create a PCE support bundle request
- `/orgs/:xorg_id/support_bundle_requests/:uuid, DELETE`
  Delete a PCE support bundle request
- `/orgs/:xorg_id/support_bundle_requests/:uuid, GET`
  Return a specific PCE support bundle request

Common Schema rule_network_type

This new common schema defines the network types to which a rule should apply.

This schema exposure is both Public Stable and Public Experimental.

```
{
       $schema": "http://json-schema.org/draft-04/schema#",
       "description": "Network types that this rule should apply to.",
       "type": "string",
       "enum": ["brn", "non_brn", "all"],
       "default": "brn"
}
```

This common schema is referenced from multiple APIs, such as:

- `sec_policy_rule_sets_put`
- `sec_policy_rule_sets_sec_rules_get`
- `sec_policy_rule_sets_sec_rules_post`
- `sec_policy_rule_sets_sec_rules_put`

Traffic Flows

The new APIs are:

- `traffic_flows_all_actors_param.schema.jso`
- `traffic_flows_label_group_param.schema.json`

Changed APIs

agents_get

This API was DEPRECATED and replaced (use `/orgs/:xorg_id/vens/:ven_uuid` instead).

Security Policy Changes

sec_policy_delete_put

C

```
 "properties": {
       "change_subset": {
               "$ref": "sec_policy_change_subset.schema.json"
}
```

sec_policy_dependencies_post

All properties have been deleted and substituted with two properties:

```
"required": [
       "operation",
       "change_subset"
],
       "properties": {
       "operation": {
               "description": "Commit or revert",
               "type": "string",
               "enum": [
                       "commit",
                       "revert"
               ]
       },
       "change_subset": {
               "$ref": "sec_policy_change_subset.schema.json"
       }
}
```

sec_policy_get

- Property "version" changed type from string to integer
- Property workload_affected changed type from integer to (integer, null)

- Property commit_message changed type from string to (string, null)

sec_policy_label_groups_get.schema

Additional required properties are:

- `blocked_connection_reject_scopes`
  "description": "Label Group is referenced by Blocked Connection Reject Scopes",
  "type": "boolean"
- `loopback_interfaces_in_policy_scopes`
  "description": "Label Group is referenced by Loopback Interfaces in Policy Scopes",
  "type": "boolean"
- `ip_forwarding_enabled_scopes`
  "description": "Label Group is referenced by IP Forwarding Enabled Scopes",
  "type": "boolean"

Property deleted:

- `blocked_connection_reject_scope`
  "description": "Label Group is referenced by Blocked Connection Reject Scope",
  "type": "boolean"

sec_policy_pending_get.schema

This schema is changed as follows:

The required object "affected_workloads" was deleted

The property firewall_settings (Firewall settings updated by the current policy draft) is now changed and only contains a reference:

```
},
       "firewall_settings": {
              "$ref": "../common/sec_policy_pending_objects.schema.json"
```

sec_policy_post.schema

In 21.4.0, this schema contained a hash of pending hrefs organized by model:

```
{
"$schema": "http://json-schema.org/draft-04/schema#",
"type": "object",
"additionalProperties": false,
"properties": {
       "update_description": {
              "description": "Optional description for the requested change or update.",
              "type": "string"
       },
       "change_subset": {
              "description": "Hash of pending hrefs, organized by model",

                     ............

              ...........
```

All these properties (`label_groups`, `services`, `rule_sets`, `ip_lists`, `virtual_services` and so on are now replaced with a reference to a schema `sec_policy_change_subset.schema.json`.

Traffic Flows Changes

traffic_flows_destination_exclude_array.schema

This schema contains a list of excluded sources or targets. One more item was added:

```
"$ref": "traffic_flows_label_group_param.schema.json"
```

traffic_flows_destination_include_array_list.schema

This schema contains a list of included sources or targets. Two more items have been added:

```
"$ref": "traffic_flows_label_group_param.schema.json"
```

```
"$ref": "traffic_flows_all_actors_param.schema.json"
```

traffic_flows_exclude_array,schema

This schema contains a list of excluded sources or targets. One more item was added:

```
"$ref": "traffic_flows_label_group_param.schema.json"
```

traffic_flows_include_array_list,schema

This schema contains a list of included sources or targets. Two more items have been added:

```
"$ref": "traffic_flows_label_group_param.schema.json"
```

```
"$ref": "traffic_flows_all_actors_param.schema.json"
```

traffic_flows_virtual_service,schema

This schema supplies virtual service details of the traffic-flow endpoint.

One more additional optional property was added:

```
},
        "workload_enforcement_mode": {
                "$ref": "../common/workload_enforcement_mode.schema.json"
}
```

traffic_flows_traffic_analysis_queries_post_response.schema

This schema provides a list of traffic flows matching the query.

The object "network" was added at the end with additional properties name and href.

```
 },
       "network": {
                "type": "object",
                "description": "PCE network on which this flow was observed.",
                "additionalProperties": false,
```

```
                "properties": {
                        "name": {
                        "description": "The network name.",
                        "type": "string"
                },
        "href": {
                "type": "string",
                "description": "network href"
                }
}
```