Illumio Core®

Version 21.1

What's New in This Release

November 2022

14000-200-21.1

Legal Notices

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

Product Version

PCE Version: 21.1 (Standard 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

Contents

Chapter 1

Welcome to Illumio Core 21.1

This chapter contains the following topics:

Illumio is pleased to announce the general availability of version 21.1 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 21.1 release.

Product Versions

IMPORTANT:
Some components are compatible with more than one release of the PCE. For the complete list of Illumio Core components compatible with the Core 21.1-PCE, see the Illumio Support portal (log in required).

PCE: 21.1.0+H1 (Standard release)
VEN: 21.1.0+H1 (Standard release)
C-VEN: 21.1.0
Kubelink: 2.0.0
NEN: 2.1.0
FlowLink: 1.1.2+H2

Standard versus LTS Releases

21.1.0+H1-PCE and 21.1.0+H1-VEN are Standard releases.

For information on Illumio software support for Standard and LTS releases, see Versions and Releases on the Illumio Support portal (log in required).

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 “21.1”
- “.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”.

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 21.1.0 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.

Be Sure Prerequisites and Settings are Correct Before Installing

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 21.1.0. 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 21.1.0.

To ensure readiness, Illumio strongly encourages you to review the prior release notes, from your currently installed version of Illumio Core to version 21.1.0. 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).

Preview Features

Any preview feature of the Illumio Core is for your evaluation only. The purpose of preview features is to make them more useful for your organization's needs before general availability.

Do not deploy preview features in a production environment.

To avoid inadvertently impacting your current system, install preview features only in a non-production environment.

Illumio welcomes your comments and suggestions for improving preview features and documentation. For more information and to send feedback, contact Illumio Customer Support.

Manage Data and Disk Capacity Carefully

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

In this release, 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

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

End of Support

Illumio REST API v1

The version 1 of Illumio REST APIs (API v1) is not supported effectively with the 21.1 release. 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

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

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 Illumio Core 21.1

This chapter contains the following topics:

Before upgrading to Illumio Core 21.1.0, 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, REST API, and PCE web console.

About the New Features and Changes

In Illumio Core 21.1.0, introduces the following new features and enhancements.

LDAP Authentication

In this release, the PCE supports LDAP authentication for users with OpenLDAP and Active Directory. The PCE supports user and role configuration for LDAP users and groups. You can configure up to three LDAP servers and map users and user groups from your LDAP servers to PCE roles.

For information about configuring this new feature, see LDAP Authentication in the *PCE Administration Guide*.

PCE Hardening

The PCE now takes additional steps to ensure its own security.

- Inbound connections to the PCE internal services and ports are now permitted only from other PCE host IP addresses and not from external sources. The PCE manages these IP addresses. Inbound connections on external-facing ports are not affected.
- All communication between PCE nodes is now encrypted using TLS by default. This includes all TCP connections between various PCE internal services.

Labels Restrictions for Kubernetes Namespaces

Container workloads are assigned four-dimensional labels to identify their roles, applications, environments, and locations (RAEL) just as applications running on bare-metal servers and virtual machines that are protected by the Illumio Core. These labels can then be used to apply security policies to specific parts of the containerized application environment. The PCE converts these label-based policies into rules that can be applied to the container workloads.

The previous release provided PCE support for container workloads but lacked the ability to restrict label assignment for namespaces. In Release 21.1.0, Illumio administrators have a way to control which labels can be assigned by the developers managing their Kubernetes environments.

For more information, see Configuring Labels for Namespaces, Pods, and Services in *Illumio Core for Kubernetes and OpenShift*.

Aggressive Tampering Protection for nftables

Firewall changes that are not explicitly configured by the VEN are logged as tampering attempts. This feature extends Release 19.3 nftables support with the inclusion of aggressive tampering protection.

VEN Proxy Support on Linux, AIX, and Solaris

This release extends VEN proxy support to include Linux, AIX, and Solaris devices, in addition to Windows.

For more information, see VEN Proxy Support in *VEN Installation and Upgrade Guide.*

Chapter 3

What's New and Changed in the REST API

This chapter contains the following topics:

This section describes the ways that the Core REST API changed in Core 21.1.

For more information about these changes, see *REST API Developer Guide*.

Illumio Core REST API in 21.1

The Illumio Core REST API v2 has changed in 21.1.0 in the following ways.

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

New Features

The following new features have been added to the release 21.1.0:

LDAP Authentication

The new Public Experimental API provides user authentication with the PCE using LDAP with OpenLDAP and Active Directory.

LDAP authentication comes in addition to the two previously available methods:

- API keys, which provide persistent authentication, and
- Session credentials, which provide temporary authentication.

Before you map your LDAP settings to PCE settings, determine your user base Distinguished Name (DN). The DN is the location in the directory where authentication information is stored.

If you don't have this information, contact your LDAP administrator for assistance.

These are the current limitations for LDAP authentication:

- Any locally created user has precedence over an LDAP user of the same name.
- LDAP and SAML single sign-on authentication methods cannot be used together. In this release of the PCE, an organization can either use LDAP or SAML single sign-on for authenticating external users.

For more details and explanations, see *REST API Developer Guide* LDAP Authentication.

Label Restrictions

Kubernetes pods and services running in a namespace (Kubernetes) or project (OpenShift) must be labeled (RAEL) to be included in policy within Illumio Core. The container workload profile defines how labels will be assigned to pods and services within a namespace.

Illumio labels can be statically assigned from the PCE or defined in the Kubernetes manifest files using annotations. For each label key (RAEL), the PCE administrator can define four options:

- No label will be assigned.
- One label will be assigned from PCE.
- A restricted list of labels can be assigned from Kubernetes using annotations. Label restrictions prevent misuse of Illumio labels by the people managing the Kubernetes platform and makes sure the labels inherit the policy they should be receiving.
- Any label can be assigned from Kubernetes.

You can set role labels for the following APIs:

- `PUT /api/v2/orgs/:xorg_id/container_clusters/<:cluster_id>/container_workload_profiles`
- `POST /api/v2/orgs/:xorg_id/container_clusters/<:cluster_id>/container_workload_profiles`

For more details and explanations, see *REST API Developer Guide* Lebel Restrictions.

Virtual Server Filtering

Filtering of the discovered virtual servers and draft virtual servers endpoints makes it easier to manage large numbers of virtual servers.

The existing Public Experimental API endpoints for virtual servers have been changed to support the required filters and associated UI operations. You can now filter a discovered virtual server collection by:

- name
- SLB (API uses href as per conventions)
- VIP: IP, proto, port (any or all)
- virtual server href

New filters have been added for the following existing endpoints:

- `GET /orgs/:xorg_id/discovered_virtual_servers`
- `GET /orgs/:xorg_id/sec_policy/:pversion/virtual_servers`

For more details and explanations, see *REST API Developer Guide* Virtual Server Filtering.

API Exposure Changes

✓ NOTE:
Exposure changes apply only for v2 APIs.

Exposure changed to Public Experimental APIs):

- `authentication_settings_ldap_configs_get`
- `authentication_settings_ldap_configs_post`
- `authentication_settings_ldap_configs_put`
- `authentication_settings_ldap_configs_verify_connection_post`

Exposure changed to Public Stable APIs:

- `sec_policy_label_groups_get`
- `sec_policy_label_groups_post`
- `sec_policy_label_groups_put`
- `sec_policy_virtual_services_bulk_create_put`
- `sec_policy_virtual_services_bulk_update_put`
- `sec_policy_virtual_services_get`

- `sec_policy_virtual_services_pos`
- `sec_policy_virtual_services_put`
- `virtual_service_service_addresses`
- `virtual_service_service_ports`