Illumio Core®

Version 22.3

What's New in This Release

November 2022

14000-200-22.3

Legal Notices

Product Version

PCE Version: 22.3

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 22.3

This chapter contains the following topics:

Illumio is pleased to announce the general availability of version 22.3 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 22.3 release.

IMPORTANT:
Illumio Core 22.3 is available for Illumio Core Cloud customers only, depending on the version of the Illumio Core Cloud running in their environments.Illumio Core Cloud customers can verify their version in the PCE web console.

Product Versions

PCE Version: 22.3.0 (Standard)

VEN Version: 22.3.0 (Standard)

IMPORTANT:
The VEN in Core 22.3.0 supports installing the VEN on the Illumio Endpoint only. The VEN is not available for installation on server workloads (such as bare-metal servers and virtual machines). Do not install the 22.3.0 VEN on server workloads.

NEN Version: 2.3.10 and 2.4.0

FlowLink Version: 1.1.2

C-VEN Version: 21.5.15

PCE CLI Tool Version: 1.4.2

Standard versus LTS Releases

22.3.0-PCE and22.3.0-VEN are standard 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+e”

- “a.b”: Standard or LTS release number, for example “22.2”
- “.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 22.3 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 version22.3.

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 22.3, 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 22.3.3

Illumio Core 22.3.3 introduces the following enhancements for the PCE.

Illumio Core 22.3.3 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 22.3.3-PCE solved software and security issues to refine the PCE software and improve its reliability and performance.

For the complete list of improvements and enhancements to the PCE, see "Resolved Issue in 22.3.3-PCE" in the Illumio Core Release Notes 22.3.

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 in the 22.3.0 Endpoint VEN

Illumio Core 22.3.0 introduces the following new feature.

Illumio Endpoint for macOS

Illumio Core Cloud customers can now install the VEN for the Illumio Endpoint on the latest versions of macOS; specifically, macOS versions 10.15 (Catalina), 10.16 (Big Sur), and 12.*x* (Monterey).

About a third of all endpoint platforms within an enterprise are running macOS. Not protecting this platform leaves organizations vulnerable to ransomware and malware. To prevent breaches and lateral movement in your organization, install the Illumio Endpoint on macOS and create full enforcement policies for your Mac endpoints.

For the steps to install the Illumio Endpoint on macOS, see Endpoint on macOS. For information about creating full enforcement policies, see Ruleset and Labeling Guidelines for Endpoints.

For an overview of the Illumio solution for endpoints, see Illumio Endpoint on the Illumio website.

IMPORTANT:
The VEN in Core 22.3.0 supports installing the VEN on the Illumio Endpoint only. The VEN is not available for installation on server workloads (such as bare-metal servers and virtual machines). Do not install the 22.3.0 VEN on server workloads.

What's New and Changed in Release 22.3.0

Illumio Core 22.3.0 introduces the following new features and enhancements.

Installation Change

In the name of the Illumio Core PCE installation RPM file, c6 has changed to c7. This reflects the change in CentOS support to CentOS version 7, which was made in an earlier PCE version. In the PCE Installation and Upgrade Guide, this file is referred to as `illumio_pce_rpm`.

New Features in This Release

The following new features were added in Illumio Core 22.3.0.

Support for Non-corporate (External) Interface Policy Enforcement

Endpoint VEN for Illumio Core Cloud reports on the corporate interface and non-corporate interfaces and supports writing policies to both types of interfaces for Windows On-premises AD, Azure AD only, and hybrid AD (Azure AD and On-premises AD) joined workloads.

Label Name Checking

In this release, the PCE prevents users from adding invalid label names in the PCE web console. For example, the PCE web console won't allow you to add a label name that is basically the same as an existing label but with capitalization differences; for example “Web_Servers” when the “web_servers” label already exists in the PCE.

Support for Shared SNAT Out of Public Clouds

The PCE web console now includes a new option under the **Settings** > **Security** menu for public cloud configuration. The selection for NAT detection allows you to choose between these options:

- Private Data Center or Public Cloud with 1:1 NAT

  This option is the recommended default for the AWS public cloud.

- Public Cloud with SNAT/NAT Gateway

  This option is the recommended default for the Azure public cloud.

  See the *PCE Administration Guide* for more information.

Pre-populated Services

In this release, the PCE now includes 63 pre-populated services in the PCE. These services are available to use in the PCE web console and through the Illumio REST API.

To access them in the PCE web console, go to **Policy Objects** > **Services** from the PCE web console main menu. For information about using them in the Illumio REST API, see the *REST API Developer Guide*.

This feature provides common service and port numbers as standard services so that application developers can speed up the process of creating security policy for their applications.

See the *Security Policy Guide* for more information.

PCE Platform Enhancements

The following enhancements were added to existing features in Illumio Core 22.3.0.

Decreased SAML Certification Lifetime

Once configured using these steps in the PCE Administration Guide, the lifetime of the SAML certificate is two years. Previously, the lifetime of the certificate was ten years.

Illumio Core REST API in 22.3.0

The Illumio Core REST API v2 has changed in 22.3.0 in the following ways.

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

New Public Experimental APIs

Network Enforcement Node Reassignment

network_enforcement_node_put

This API is used to change the target PCE FQDN of an agent. It updates (PUT) the `target_pce_fqdn` property so that the NEN can be managed by a different PCE in a Supercluster.

Here is the new schema part that defines warning and error:

```
{
	"$schema": "http://json-schema.org/draft-04/schema#",
		"description": "Update a NEN's target PCE.",
		"type": "object",
		"additionalProperties": false,
		"properties": {
			"target_pce_fqdn": {
				"description": "cluster FQDN for target PCE",
				"type": "string"
			}
		}
}
```

where

`target_pce_fqdn`: The PCE that is configured to manage this NEN or the FQDN of the Supercluster (when you configured the `supercluster.fqdn` property in your `runtime_env.yml` file).

Change Target PCE

When you have the NEN HREF, you can update the target PCE with the PCE FQDN the NEN will use. In your JSON request body, pass the following data:

```
{
       "target_pce_fqdn": "new-pce-fqdn.example.com"
}
```

The URI for this operation is:

```
PUT [api_version][nen_href]/update
```

This curl example shows how you can pass the target_pce_fqdn property containing the FQDN of the new PCE:

```
curl -u api_
xxxxxxx64fcee809:'xxxxxxx5048a6a85ce846a706e134ef1d4bf2ac1f253b84c1bf8df6b
83c70d95' -H "Accept: application/json" -H "Content-Type:application/json"
-X PUT -d '{"target_pce_fqdn":"new-pce-fqdn.example.com"}'
https://my.pce.supercluster:443/api/v1/orgs/3/network_enforcement_
nodes/f67d35d5-ea71-42da-b40d-8dcc3b1420c2/update
```

Rule Set

rule_search_post_response_rule_set.schema.json

This schema is now referenced from the API sec_policy_rule_search_post_response.

There is no structural change to the response and the schemas were just reorganized.

Parameter Exposure Changed to Public

representation=workload_labels

The parameter representation=workload_labels was private and is now Public Experimental.

This allows you to see the key and value of a workload's label and not just the href.

You don't need to call the labels API and build logic to resolve the href.

Changed Public Stable APIs

Workloads

workloads_get

The Public Stable API `workloads-get` was changed in the following ways:

- Instead referencing the `labels.schema`, the list of required labels (`href`, `key`, `value`) associated with a workload was added:

Release 22.2.20

```
"labels": {
 "$ref":
"labels.sche
ma.json"
},
```

Release 22.3.0

```
"labels": {
"description": "List of labels associated with this
workload",
"type": "array",
    "items": {
    "type": "object",
    "required": [
        "href",
        "key",
        "value"
    ],
       "properties": {
       "href": {
           "description": "The URI of the VEN that manages
this workload. This replaces the 'agent' field of this
object.",
           "type": "string"
```

```
        },
         "key": {
            "description": "Key in key-value pair",
             "type": "string"
        },
         "value": {
             "description": "Value in key-value pair",
             "type": "string"
                        }
                        }
                   }
},
```

- In addition to providing the VENs `href`, it is now required to give also its `hostname`, `name`, and `status`. The VEN properties are now clearly displayed, without a need to use expanded representations.

Release 22.2.20

```
"ven": {
     "type": "object",
     "required": [
         "href"
      ],
```

Release 22.3.0

```
"ven": {
    "type": "object",
    "required": [
        "href",
        "hostname",
        "name",
        "status"
]
```

- For selectively enforced services, the reference to the schema `href_object.s-chema.json` was removed.

Release 22.2.20

```
"selectively_enforced_services": {
     "type": "array",
     "items": {
     "type": "object",
     "oneOf": [
       {
```

Release 22.3.0

```
"selectively_enforced_
services": {
       "type": "array",
       "items": {
                "type": "object",
                "required": [
```

```
            "$ref": "../common/href_
object.schema.json"
       },
       {
       "type": "object",
       "required": [
                       "proto"
       ],
```

```
                              "proto"
                    ],
```

Labels

labels_post

For the Key property, enum (enumeration) was removed for the values `role`, `loc`, `env`, and `app`.
The key value is now no longer locked to be one of those four pre-defined values.

Release 22.2.20

```
"properties": {
    "key": {
       "description": "Key in key-val
pair",
       "type": "string",
       "enum": [
               "role",
               "loc",
               "env",
               "app"
               ]
},
```

Release 22.3.0

```
"properties": {
       "key": {
       "description": "Key in key-value
pair",
                "type": "string"
       },
```

Non-corporate Public IP Addresses for Endpoints in the PCE

Endpoint VEN for Illumio Core Cloud reports on the corporate interface and non-corporate interfaces and supports writing policies to both types of interfaces on Win-

dows On-premises AD, Azure AD only, and hybrid AD (Azure AD and On-premises AD) networks.

Recognizing both corporate and non-corporate interfaces allows you to write rules for non-corporate interfaces that were not supported in earlier releases. This VEN feature is only supported on endpoints and not servers.

Writing rules between non-corporate interfaces and corporate interfaces is not supported.

POST/api/v2/orgs/:org_id/sec_policy/rule_coverage

The `sec_policy/rule_coverage` API supports non-domain interfaces. It has a new property network and now accepts the `network_href` to correctly determine if the rule applies to a flow.

Release 22.3.0

```
{
       "items": {
       "properties": {
               "network": {
                   "description": "The network that the source and destination are on",
                   "type": "object",
       "properties": {
               "href": {
                  "description": "The href of the network that the source and destination are
on",
                   "type": "string"
               }
       }
},
```

To factor in the network that the flow is in, use the rule network types (`brn`, `non-brn`, `all`) and the type of the network to determine if the rule applies.

POST /api/v2/orgs/sec_policy/rule_coverage

Request

Example for the rule coverage that specifies:

- `source`
- `destination`
- `network` (where the source and destination are in, such as a `non-brn` network in this example)
- `service`

```
    "source": {
        "labels": [
         {
             "href": "/orgs/14/labels/42"
         },
         {
             "href": "/orgs/14/labels/43"
         }
    ]
         },
     "destination": {
         "ip_list": {
             "href": "/orgs/14/sec_policy/active/ip_lists/14"
         }
     },
     "network": {
             "href": "/orgs/14/networks/c7bc9ec1-8007-419c-a175-d848f169c983"
     },
     "services": [
         {
             port: 81,
             protocol: 6
         }
```

Response

The rules returned in the API response are rules with network type `non-brn` that apply to the given input.

```
{
       "rules":
          {
```

```
            "0": { "href": "/orgs/14/sec_policy/draft/rule_sets/21/sec_rules/220" },
            "1": { "href": "/orgs/14/sec_policy/draft/rule_sets/21/sec_rules/223" },
            "2": { "href": "/orgs/14/sec_policy/draft/rule_sets/21/sec_rules/237" }
        },
        "edges": [[["0", "1", "2"]]]
}
```

Changed Public Experimental APIs

Network Enforcement Node

The two new properties have been added:

- `target_pce_fqdn`, which the Network Enforcement Node will use for future connections, and
- `active_pce_fqdn`, which received the Network Enforcement Node's last heartbeat.

network_enforcement_node_get

```
{
        "properties": {
        "target_pce_fqdn: {
                "description": "The FQDN of the PCE the Network Enforcement Node
will use for future connections",
                "type": [
                    "string",
                    "null"
                ]
        },
        "active_pce_fqdn": {
                "description": "The FQDN of the PCE that received the Network
Enforcement Node's last heartbeat",
                "type": [
                    "string",
                    "null"
                ]
}
```

network_enforcement_node_put

This API is new and explained previously in network_enforcement_node_put.

Agents

agents_get

The agents API in the VEN resource is deprecated and the VEN href is used to work with the resource.

```
{
       "properties": {
           "ven": {
           "description": "The href under the VENs resource that points to this agent.
The agents API is deprecated, and the VEN href should be used to identify and
manipulate this resource.",
               "$ref": "../common/href_object.schema.json"
           }
       }
}
```

Security Policy

sec_policy_rule_search_post_response

For this API, the following was changed:

- For `rule_set`, all previous properties have been removed (`href`, `name`, `enabled`, `external_data_set`, `external_data_reference`, and `scopes`) and a reference to the new schema was added instead:rule_search_post_response_rule_set.schema.json.

Release 22.2.20

```
"rule_set": {
       "description": "Parent Rule Se
of the Rule",
       "type": "object",
```

Release 22.3.0

```
"rule_set": {
   "$ref": "rule_search_post_response_rule_
set.schema.json"
    }
}
```

```
"properties": {
       "href": {
              "description": "URI of the rule
set",
                     "type": "string"
                     },
       "name": {
              "description": "Name (must be
unique)",
                     "type": "string"
                     },
       "enabled": {
              "description": "Enabled flag",
                     "type": "boolean"
                     },
       "external_data_set": {
              "description": "External data
set
identifier",
                     "type": [
                            "string",
                            "null"
                     ]
                     },
       "external_data_reference": {
              "description": "External data
reference identifier",
                     "type": [
                            "string",
                            "null"
                                   ]
                            },
       "scopes": {
       "$ref": "../common/rule_set_
scopes.schema.json"
       }
}
```

max_results Query Parameter

GET /api/v2/orgs/:xorg_id/sec_policy/pending

The schema `sec_policy/pending` now has a new query parameter `max_results`, as well as the field `X-Total-Count` in the response header.

The schema itself was not changed, and the new parameter was implemented for consistency with other security policy APIs and to enhance performance.

Keep the following in mind:

- When `max_results` is not provided, object count in response is not limited.
- When `max_results` is 0, the field `X-Total-Count` still shows the full pending policies count.

Labels

core_services_labels

The enum (enumeration) was removed for the key values `role` and `app`.

The key value is now no longer locked to be one of those two predefined values.

See also labels_post.

Release 22.2.20

```
"key": {
       "description": "Label type",
       "type": "string",
       "enum": [
                       "role",
                       "app"
               ]
       },
"href": {
       "description": "Label URI",
       "type": "string",
               "format": "uri"
               }
       }
},
```

Release 22.3.0

```
"key": {
       "description": "Label type",
       "type": "string"
       },
"href": {
       "description": "Label URI",
       "type": "string",
                       "format": "uri"
               }
       }
},
```

SLB Collection API

For the following two schemas:

- `GET /api/v2/orgs/:xorg_id/slbs`
- `GET /api/v2/orgs/:xorg_id/slbs/:id`

the query parameter `max_results` was added so that schemas conform to the API conventions. It is used as a filter for the following schema parameters:

- `name`
- `description`
- `has_virtual_server`
- `status`
- `device_type`
- `number_of_devices`

Optional Features

optional_features_put

The property `configurable_label_dimensions` was added to the API `PUT /api/v2/orgs/:xorg_id/optional_features`:

Release 22.2.20

```
"properties": {
       "name": {
          "description": "Name of the
feature",
          "type": "string",
       "enum": [
          "ip_forwarding_firewall_setting
          "ui_analytics"
```

Release 22.3.0

```
"properties": {
       "name": {
          "description": "Name of the
feature",
          "type": "string",
       "enum": [
          "ip_forwarding_firewall_setting",
          "ui_analytics",
       "configurable_label_dimensions"
```

This flag is added so that the UI users can determine if an organization has enabled the user analytics.

Analytics is opt-in by default. If it has been disabled, the UI shows not to track analytics for that organization.

To set or clear the optional analytics feature, use:

```
PUT /agent/api/v2/orgs/<:xorg_id>/optional_features
```

```
{ name: "ui_analytics", enabled: false|true }
```

Conforming `multi_unpair_vens` to the new Multi Object Pattern

The function `ven_ids = VenEntity.get_unvalidated_ids(vens).uniq` currently calls an underlying `get_id` function that raises an error if the URI is invalid.

An invalid URI should not raise the error, since that halts the whole function and return.

The malformed URI should be appended to the `errors[:invalid_uri{_}{_}] key` instead.

Documentation Updates in 22.3

The following section highlights some key updates and additions to the documentation for 22.3. This list does not include every documentation change or addition.

- This *Illumio Endpoint Segmentation Guide* describes how to use Illumio Endpoint feature in Core, a single PCE formerly referred to as "Single Pane of Glass," to visualize and segment Windows endpoints.