Illumio Core®

Version 22.4

What's New in This Release

November 2022

14000-200-22.4

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: 22.4

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 22.4

This chapter contains the following topics:

Illumio is pleased to announce the general availability of version 22.4 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 22.4 release.

> IMPORTANT:
> Illumio Core 22.4 is available for Illumio Core On Premises customers.

Product Versions

PCE Version: 22.4.0 (Standard)

VEN Version: 22.4.0 (Standard)

NEN Version: 2.5.1

FlowLink Version: 1.1.2

C-VEN Version: 21.5.17

Standard versus LTS Releases

22.4.0-PCE and 22.4.0-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 22.4 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 version22.4.

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 22.4, 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.

Illumio Core 22.4 Release Overview

Illumio Core 22.4.1 Maintenance Release

As a maintenance release, Illumio Core 22.4.1 does not add new features or content. Illumio Core 22.4.1 has been released to solve minor problems and/or security issues, to refine the software, and to improve its reliability and performance.

What's New in Illumio Core 22.4.0

Illumio Core 22.4.0 was an unreleased version of the Illumio Core software. Illumio Core Cloud customers will not see this version in their environments; however, the resolved issues plus new features and enhancements in this release are available in Illumio Core 22.4.1.

New Feature in 22.4.0

ML/AI-Based Scanner Detection

Many customer environments have scanners running that create significant traffic data which results in a lot of noise when trying to create policy. Starting in 22.4.0, Core Services can identify these scanners, and users can make the discovered scanner traffic a workload, including assigning labels to it. This new feature helps customers operationalize Illumio Core more effectively and efficiently.

For more information, see Scanner Detection in the *Security Policy Guide*.

Enhancements in 22.4.0

Usability Enhancements in the VEN Details Page

- **Enforcement Node Type** value displays the type of VEN (Endpoint, C-VEN, or VEN). Also available through the Illumio Core REST API.
- The public IP addresses for Endpoints are hidden, because they are not relevant for Endpoints.

Illumio Core REST API Enhancements

- Using the Illumio Core REST API to configure the timeout value for VEN uninstallation; see “Timeouts for Workloads and VEN Uninstall” in the What’s New in This Release Guide for Core 22.4.0.
- Support for src port collector filter in the Illumio Core REST API, which users can call to filter traffic based on the source port.
- Better telemetry around request authentication failed events caused by unpair-timed-out VENs. In previous releases, the Agents API did not provide the VEN HREF, making VEN issues harder to debug. In this release, you can query the Agents API to get the VEN HREF.
- Numerous minor changes in the Illumio Core REST API.

See Illumio Core REST API in 22.4.0 for more information about this REST API enhancements.

Illumio Core REST API in 22.4.0

The Illumio Core REST API v2 has changed in 22.4.0 in the following ways.

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

New Public Stable APIs

VEN Type

ven_type.schema.json

```
{
       "$schema": "http://json-schema.org/draft-04/schema#",
               "type": "string",
               "description": "VEN type",
               "enum": ["server", "endpoint", "containerized"]
}
```

Before this new schema was added, users needed to query the workloads GET API to get `public_ip_addr` and then VENS GET API to get `ven_type`. Now with the common schema `ven_type.schema.json`, which contains the property `ven_type`, users only have to query the workload API to get `ven_type`.

The property `ven_type` was added inside the VEN object in these APIs:

- `vens_get`
- `workloads_get`
- `container_workloads_get`
- `support_report_requests_get`

New Public Experimental APIs

Traffic Flows

traffic_flows_enforcement_boundary.schema.json

This schema provides a list of enforcement boundary details for the traffic flow endpoint in a DRAFT version.

```
{
       "$schema": "http://json-schema.org/draft-04/schema#",
               "description": "List of enforcement_boundaries details of the traffic-flow
endpoint. This is always the draft version",
               "additionalProperties": false,
                       "expose_to": [
                       "end_user_private_perm"
                       ],
                       "type": "array",
                       "items": {
                       "type": "object",
                       "required": [
                       "href"
                       ],
               "additionalProperties": false,
                       "properties": {
                       "href": {
                       "description": "The resource (URI) representation of an enforcement boundar
This is always the draft version.",
                       "type": "string"
                       }
               }
       }
}
```

traffic_flows_rules.schema.jsoN

This schema provides alow rules for the specific policy objects.

```
{
        "$schema": "http://json-schema.org/draft-04/schema#",
                "description": "Allow rules for specific policy objects",
                "additionalProperties": false,
                        "expose_to": [
                        "end_user_private_perm"
                        ],
                        "type": "array",
                        "items": {
                        "type": "object",
                        "oneOf": [
                        {
```

```
            "required": [
            "href"
            ],
        "additionalProperties": false,
            "properties": {
            "href": {
            "description": "The resource (URI) representation of an allow rule. This is
always the draft version.",
            "type": "string"
        }
    }
    },
        {
            "required": [
            "essential_service_rule"
            ],
        "additionalProperties": false,
            "properties": {
            "essential_service_rule": {
            "description": "The name of an essential service rule.",
            "type": "string"
            }
        }
    }
}
```

Reports

ves_report_params.schema.json

This schema provides report parameters for the new ves (vulnerability-exposure score) report type.

It is referenced from the following APIs:

- report_schedules_get
- report_schedules_post
- report_schedules_put
- report_templates_get

- `reports_get`
- `reports_post`

```
{
        "$schema": "http://json-schema.org/draft-04/schema#",
                "description": "Report parameters for VES report",
                "type": "object",
                "additionalProperties": false,
                        "properties": {
        }
}
```

Deprecated Public Experimental APIs

Server Load Balancers (SLB)

slb_config.schema.json

This schema was used for `nfc` (Network Function Controller), which is now deprecated.

```
{
        "$schema": "http://json-schema.org/draft-04/schema#",
                "type": "object",
                "additionalProperties": false,
                "properties": {
                "name": {
                        "description": "The short friendly name of the server load balancer",
                        "type": "string"
                        },
                        "description": {
                        "description": "The long description of the server load balancer",
                        "type": "string"
                        },
                "nfc": {
                        "description": "Network function controller managing this SLB",
                        "type": "object",
                        "additionalProperties": false,
                        "required": [
                "href"
                        ],
                        "properties": {
                                "href": {
                                "description": "NFC URI",
                                "type": "string"
                        }
                        }
                },
                "device_type": {
                        "$ref": "slb_device_type.schema.json"
                        },
                "devices": {
                        "description": "Management configuration of the devices associated with thi
SLB Network VF.",
                        "type": "array",
                        "minItems": 1,
                        "items": {
                        "type": "object",
                        "required": [
                        "href"
                                ],
                        "additionalProperties": false,
                        "properties": {
                        "href": {
                                "description": "SLB device URI.",
                                "type": "string"
                                },
                        "config": {
                                "$ref": "slb_device_config.schema.json"
                                }
                        }
                }
        }
}
```

Changed Public Stable APIs

Port Vulnerability

detected_vulnerability_get

The new property `port_vulnerability_exposure_score` allows for calculating the part based on the port's exposure and vulnerability.

```
{
        "properties": {
                "port_vulnerability_exposure_score": {
                "description": "The vulnerability exposure score calculated for the port, based
on the port exposure and vulnerability",
                "type": [
                "integer",
                "null"
                ]
        }
}
```

Timeouts for Workloads and VEN Uninstall

resource_canonical_representations.schema.json

Two new properties have been added to the schema `resource_canonical_representations` to calculate timeouts for workloads and VEN uninstall:

- `workload_goodbye_timeout_seconds`
- `ven_uninstall_timeout_hours`

```
 },
        "workload_goodbye_timeout_seconds": {
                "description": "Goodbye timeout in seconds",
                "type": "integer"
                },
        "ven_uninstall_timeout_hours": {
                "description": "VEN uninstall timeout in hours",
                "type": "integer"
},
```

Services

sec_rule_ingress_services.schema.json

The schema `sec_rule_ingress_services` has a new required property `additionalProperties`.

```
{
        "type": "object",
                "required": [],
                "additionalProperties": false,
                "properties": {}
};
```

service_ports.schema.json

The parameter name was changed from `min_items` to `minItems`.

```
{
        "minItems": 1
}
```

service_protocol_def.schema.json

The property `proto` was changed so that the reference to the common schema `service_ports_protocol_numeric.schema.json` was removed, and it looks as follows:

```
 },
        "proto": {
                "description": "Transport protocol",
                "type": [
                "integer",
                "null"
```

```
       ]
},
```

Traffic Collector

- **settings_traffic_collector_get**
- **settings_traffic_collector_post**
- **settings_traffic_collector_put**

For all listed traffic collector APIs, a new property `src_port` was added. This allows users to filter traffic based on the source port.

```
{
        "properties": {
                "target": {
        "properties": {
                "src_port": {
                "type": "integer"
                }
        }
}
```

Workload Settings

If a VEN is unpaired from the PCE by a user with no acknowledgment that unpair was successful for seven days, the PCE moves the VEN automatically from the state `uninstalling` to `deactivated_unconfirmed`. When that happens, the VEN record is subject to purging from the PCE database.

The reason for the VEN not to acknowledge unpairing often results from the host being down for an extended time, such as when a backup server comes up only once a month for some task.

This API change was introduced to provide a configurable frequency. Setting a longer time (for example, one or six months) allows users to query for VENs that are unpaired from the PCE using the API. In a longer time frame, the VEN comes back and is instructed to unpair.

settings_workloads_get

In the schema below, the **bold** lines are added:

```
{
"$schema": "http://json-schema.org/draft-04/schema#",
   "type": "object",
   "description": "Workload setting properties",
   "required": [
       "workload_disconnected_timeout_seconds",
       "workload_goodbye_timeout_seconds",
       "ven_uninstall_timeout_hours",
       "workload_disconnected_notification_seconds"
       ],
   "properties": {
       "workload_disconnected_timeout_seconds": { "$ref": "settings_
workload.schema.json" },
       "workload_goodbye_timeout_seconds": { "$ref": "settings_workload.schema.json" },
       "ven_uninstall_timeout_hours": { "$ref": "settings_workload.schema.json"}, ,
       "workload_disconnected_notification_seconds": { "$ref": "settings_workload_
notifications.schema.json" }
   }
}
```

Example Reply:

```
{
       "href": "/orgs/1/settings/workloads",
       "workload_disconnected_timeout_seconds": [{
               "scope": [],
               "value": 3600
       }],
       "workload_goodbye_timeout_seconds": [{
               "scope": [],
               "value": 900
       }],
       "ven_uninstall_timeout_hours": [{
               "scope": [],
               "value": 168
       }],
       "workload_disconnected_notification_seconds": [{
               "info": -1,
               "warning": -1,
               "error": -1,
               "scope": []
       }]
}
```

settings_workloads_put

In the schema below, the **bold** line is added:

```
{
   "$schema": "http://json-schema.org/draft-04/schema#",
   "type": "object",
   "description": "Workload setting properties",
   "additionalProperties": false,
   "properties": {
       "workload_disconnected_timeout_seconds": { "$ref": "settings_
workload.schema.json"},
       "workload_goodbye_timeout_seconds": { "$ref": "settings_workload.schema.json"},
       "ven_uninstall_timeout_hours": { "$ref": "settings_workload.schema.json"},
       "workload_disconnected_notification_seconds": { "$ref": "settings_workload_
notifications.schema.json" }
   }
}
```

Virtual Service

virtual_service_service_ports.schema.json

The parameter name was changed from `min_items` to `minItems`.

```
{
       "minItems": 1
}
```

Windows service

windows_service.schema.json

For this API, the properties `service_name` and `process_name` are now available as a `null` value (in **bold**) in addition to a `string`.

```
"properties": {
       "service_name": {
       "description": "Name of Windows Service",
       "type": [
               "string",
               "null"
               ]
       },
       "process_name": {
       "description": "Name of running process",
       "type": [
               "string",
               "null"
       ]
},
```

The property `proto` was also changed so that the reference to the common schema `service_ports_protocol_numeric.schema.json` was removed, and it looks as follows:

```
 },
       "proto": {
       "description": "Transport protocol",
       "type": [
               "integer",
               "null"
       ]
},
```

windows_services.schema.json

The parameter name was changed from `min_items` to `minItems`.

```
{
        "minItems": 1
}
```

Changed Public Experimental APIs

Added new Properties

vens_get.schema.json

The new property `ven_type` was added inside the VEN object with a reference to the common schema `ven_type.schema.json` as follows:

```
{
        "properties": {
        "ven_type":
{
        ~~"type": "string",~~
        ~~"description": "VEN type",~~
        "$ref": "../common/ven_type.schema.json"
        }
}
```

workloads_get.schema

The new property `ven_type` was added inside the VEN object as follows:

```
{
        "properties": {
        "ven": {
        "properties": {
        "ven_type": {
        "$ref": "../common/ven_type.schema.json"
        }
}
```

Virtual Servers

discovered_virtual_servers_get

- For this API, two changes have been introduced:
- Description for nfc (Network Function Controller) was changed to indicate that it was deprecated and replaced.
- The property network_enforcement_node (in **bold**) was added in place of the deprecated nfc.

```
 },
       "nfc": {
          "description": "DEPRECATED AND REPLACED (USE 'network_enforcement_node'
INSTEAD) URI of
           the NFC for this discovered virtual server",
          "$ref": "../common/href_object.schema.json"
       },
       "network_enforcement_node": {
          "description": "URI of the Network Enforcement Node for this discovered
virtual server",
          "$ref": "../common/href_object.schema.json"
```

Reports

In this release, there are several changes to the report APIs.

For these schemas:

- explorer_report_params.schema.json
- report_time_range_definitions.schema.json

the report parameters for the executive summary report were replaced with the report parameters for the Explorer report.

```
{
       "description": {
       "Report parameters for explorer report"
       }
}
```

For the following APIs, the parameter ves_report_params.schema.json was added in form of a reference:

- report_schedules_get
- report_schedules_post
- report_schedules_put
- report_templates_get
- reports_get
- reports_post

```
{
        "properties": {
                "report_parameters": {
                "oneOf": [
                ---------
                {
                "$ref": "ves_report_params.schema.json"
                }
                -----------
```

report_templates_get.schema.json

In addition to ves_report_params.schema.json, this API has one more new property: show_in_ui. It was added to determine whether the report will be shown in the PCE UI.

```
{
        "properties": {
                "show_in_ui": {
                "description": "Determines whether this report is to be shown in the PCE UI",
                        "type": "boolean",
                        "default": true
```

Firewall Settings

sec_policy_firewall_settings_get

sec_policy_firewall_settings_put

The new property `allow_captive_portal_outbound` was added, which defines whether to open the endpoint firewall to all outbound traffic when a captive portal scenario is discovered by the VEN. This Boolean property can be `true` or `false`.

```
{
       "properties": {
               "allow_captive_portal_outbound": {
               "description": "Defines whether or not to open the endpoint firewall to all
outbound traffic
                when a captive portal scenario is discovered by the VEN",
               "type": "boolean"
       }
}
```

Server Load Balancers (SLB)

For the folllowing APIs

slbs_get

slbs_post

slbs_put

two changes have been introduced:

- Description for `nfc` (Network Function Controller) was changed to indicate that it was deprecated and replaced.
- The property `network_enforement_node` (in **bold**) was added in place of the deprecated `nfc`.

```
 "nfc": {
       "description": "DEPRECATED AND REPLACED (USE 'network_enforcement_node' INSTEAD)
Network Function Controller managing this SLB",
       "type": "object",
       "required": [
               "href"
               ],
       "properties": {
               "href": {
               "description": "NFC URI",
               "type": "string"
               }
       }
},
"network_enforcement_node": {
       "description": "Network enforcement node managing this SLB",
       "type": "object",
       "required": [
               "href"
               ],
       "properties": {
               "href": {
               "description": "Network enforcement node URI",
               "type": "string"
               }
       }
},
```

Traffic Flows

traffic_flows_async_queries_download_get

These two changes have been introduced:

- Reference to the schema `traffic_flows_traffic_analysis_queries_post_response.schema.json` is removed
- The description is added as "The list of traffic flows matching the query"

```
{
        ~~"$ref": "traffic_flows_traffic_analysis_queries_post_response.schema.json",~~
        "description": "The list of traffic flows matching the query",
```

traffic_flows_ip_list.schema.json

Two properties have been added: `rules` and `enforcement_boundaries`.

```
{
        "properties": {
                "rules": {
                        "description": "Explorer query parameters",
                        "$ref": "traffic_flows_rules.schema.json"
                        },
                "enforcement_boundaries": {
                        "description": "Explorer query parameters",
                        "$ref": "traffic_flows_enforcement_boundary.schema.json"
                }
        }
}
```