



Illumio[®] Core for Kubernetes

Version 4.3.0

Compatible PCE Versions 22.5.0 and later

Release Notes

07/26/2023

19750-100-4.3.0

Contents

Welcome	3
What's New in This Release	3
Product Version	3
Updates for Core for Kubernetes 4.3.0	4
C-VEN.....	4
Resolved Issues	4
Known Issue.....	4
Kubelink.....	4
Resolved Issue	4
Known Issue.....	5
Security Information for Core for Kubernetes 4.3.0.....	5
Base Image Upgraded	5

Welcome

These release notes describe the resolved issues and related information for the 4.3.0 release of Illumio Core for Kubernetes, formerly known as Illumio Containerized VEN, or C-VEN. Illumio Core for Kubernetes also includes the related required component, Kubelink. Because of this heritage, many references to this product as "C-VEN" are still used throughout the documentation.

Document Last Revised: July 2023

Document ID: 19750-100-4.3.0

What's New in This Release

The following are new and changed items in this release from the previous releases of C-VEN and Kubelink:

- **New Kubelink 3.3.1**
This Kubernetes 4.3.0 release includes an upgraded Kubelink component, version 3.3.1.
- **New C-VEN 22.5.14**
This Kubernetes 4.3.0 release includes an upgraded C-VEN component, version 22.5.14. Note that C-VEN 22.5.14 requires PCE version 22.5.0 or later, and supports PCE 23.3.0 or later.

Product Version

Compatible PCE Versions: 22.5.0 and later releases

Current Illumio Core for Kubernetes Version: 4.3.0, which includes:

- C-VEN version: 22.5.14
- Kubelink version: 3.3.1
- Helm Chart version: 4.3.0

Release Types and Numbering

Illumio release numbering uses the following format: "a.b.c-d"

- "a.b": Standard or LTS release number, for example, "21.2"

- “.c”: Maintenance release number, for example, “.1”
- “-d”: Optional descriptor for pre-release versions, for example, “preview2”

Updates for Core for Kubernetes 4.3.0

C-VEN

Resolved Issues

- **C-VEN support report does not contain container workload firewalls (EYE-106932)**
VEN support reports for C-VEs were missing the active firewall information for all container workloads. This issue is resolved. Support reports now include full firewalls from each network namespace, as gathered by `iptables-save` and `ipset list` output.
- **Contrack tear-down for containers with policy updates (E-44832)**
Although policy was changed to block a container workload from talking to another, traffic was still passing between the workloads, due to a contrack connection remaining incorrectly active. This issue is resolved. Contrack connections on sessions affected by a policy change are now properly torn down.

Known Issue

- **C-VEs not automatically cleaned up after AKS upgrade (E-103895)**
After upgrading an AKS cluster, sometimes a few duplicate C-VEs might not be automatically removed as part of the normal upgrade process, and remain in the PCE as “non-active.” Note there is no compromise to the security or other functionality of the product. Workaround: Manually prune the extra unmigrated C-VEs from the PCE by clicking the **Unpair** button for each of them.

Kubelink

Resolved Issue

- **Kubelink does not pair with PCE when a separate management port is used (E-107001)**
Kubelink would crash after start when the PCE had `front_end_management_https_port` set to 9443 instead of 8443, because of a missing `label_map` URL. This issue is resolved.

Known Issue

- **Kubelink does not properly apply label mappings with PCE using two-sided management ports** (E-105391)

Label mappings are not properly applied when using the LabelMap CRD if the PCE uses two-sided management ports.

Workaround: Use the label map feature only with a PCE that uses only one management port.

Security Information for Core for Kubernetes 4.3.0

For information about security issues, security advisories, and other security guidance pertaining to this release, see Illumio's Knowledge Base in Illumio's Support portal.

Base Image Upgraded

The C-VEN base OS image is upgraded to minimal UBI for Red Hat Linux 7.9-979.1679306063, which is available at <https://catalog.redhat.com/software/containers/ubi7/ubi-minimal/5c3594f7dd19c775cddfa777>.

Customers are advised to upgrade to Core for Kubernetes 4.1.0 or higher for these security fixes.