



# Cisco Container Platform 1.4.0 Release Notes

**First Published:** 2018-07-31

**Last Modified:** 2018-08-06

## Introduction

Cisco Container Platform is a fully curated, lightweight container management platform for production-grade environments, powered by Kubernetes, and delivered with Cisco enterprise-class support. It reduces the complexity of configuring, deploying, securing, scaling, and managing containers using automation along with Cisco's best practices for security and networking. Cisco Container Platform is built with an open architecture using open source components.

## Features

Feature	Description
Kubernetes Lifecycle Management	Enables you to deploy Kubernetes clusters, add or removed nodes, and upgrade Kubernetes clusters to latest versions.
Persistent Storage	Allows you to persist data for containerized applications between upgrades and updates through HyperFlex storage driver.
Monitoring and Logging	Provides dashboards, alerts, and indexing to monitor resource usage and behavior of platform components through Elasticsearch, Fluentd, and Kibana (EFK) stack and Prometheus.
Container Networking	Provides container to container and container to non-containerized application layers communication with security policies.
Load Balancing	Offers software ingress load balancing through NGINX and node port functionality of Kubernetes for containerized applications.
Role Based Access Control	Integrates with Active Directory and offers permission-based rules.

## Revision History

Release	Date	Description
1.0	May 22, 2018	First release
1.0.1	May 25, 2018	Updated the <b>Fixed Issues</b> and <b>Know Issues</b> sections
1.1.0	June 29, 2018	Added the <b>What's New</b> and <b>Upgrading Cisco Container Platform</b> sections Updated the <b>Fixed Issues</b> and <b>Know Issues</b> sections
1.4.0	July 31, 2018	Updated the <b>What's New</b> , <b>Fixed Issues</b> , and <b>Known Issues</b> sections
1.4.1	August 6, 2018	Added the <b>Fixed Issues, 1.4.1</b> section

## System Requirements

- The Cisco Container Platform Installer OVA
- The tenant OVA
- A vCenter cluster with High Availability (HA) and Distributed Resource Scheduler (DRS) enabled
- A DHCP server that provides IP addresses to the Cisco Container Platform VMs
- A vCenter datastore that is mounted on all the ESX hosts in the cluster
- Cisco Container Platform control plane VMs needs to have network access to vCenter appliance API
- Cisco Container Platform 1.3.0 and later requires hypervisor hosts to be running CPUs with an Ivy Bridge or newer microarchitecture.

## What's New

- Enhanced the Cisco Container Platform dashboard:
  - Included support for optional tenant cluster Helm add-ons
  - Included ability to configure tenant clusters with a root certificate
  - Included new web-based installer for control plane
  - Included support for node pools
- Introduced support for resizing node pools
- Included support for separate master and worker node configurations
- Upgraded Elasticsearch, Grafana, and Kibana components

- Replaced the OVF properties with a web-based installer for gathering install values
- Integrated Istio (Tech Preview)  
Only single cluster service mesh is supported in this release.
- Integrated VMware Harbor (Tech Preview)  
Multi user aware container registry. Notary and container scanning are not part of this release.

## Installing Cisco Container Platform

For step by step instructions on installing Cisco Container Platform, refer to the *Cisco Container Platform Installation Guide*.

## Upgrading Cisco Container Platform

- Upgrading Cisco Container Platform is supported from the 1.0.0 release for deployments using Calico or ACI for CNI.
- If an existing deployment uses Contiv for CNI, then upgrades to the 1.4.0 version is not supported.

### Fixed Issues, 1.4.1

- Configurable size for Harbor backend

### Fixed Issues, 1.4.0

- Improved general stability of long-running clusters
- Contiv etcd communication is secured
- Fixed the following issues in the Cisco Container Platform dashboard:
  - Cluster edit for ACI
  - Enter key advance for wizards
  - New bubble messages not appearing after being cleared
  - Do not count the provisioning node as successful
  - Force user to re-enter the password for vSphere step on installing Cisco Container Platform
  - ACI summary page duplicates removed
  - Edit networks name panel
  - Improve calculations for the subnet ranges
  - Unable to update groups
  - Handle case where no networks are available on clusters page
- Ingress is now using a fixed certificate based on the ingress VIP
- Improved overlap checking for ACI profile VLAN and POD subnet

- Improved error reporting on upgrades when authenticating to existing Cisco Container Platform cluster fails

## Known Issues

The known issues in this release are as follows:

- Contiv as the CNI for tenant clusters is only supported as Tech Preview, and upgrading to a newer version of Cisco Container Platform is not supported.
- In an ACI environment, the link to a tenant cluster Kubernetes Dashboard from the Cisco Container Platform dashboard is not supported. To view the tenant cluster in the Kubernetes Dashboard, you need to obtain the Ingress IP of external IP address using `kubectl get svc`.
- The Cisco Container Platform web interface displays links to external pages such as Smart Licensing. You cannot launch these pages if you do not have access to them.
- Virtual IP address is not released when cluster creation fails.
- If ACI fabric is running 3.1(1i), you need to turn on the promiscuous mode in the corresponding tenant port group in order to make the ACI load balancer functional.
- In a Contiv deployment, you should not use `matchExpressions` for a NetworkPolicy.
- In a Contiv deployment, network policy does not work with the hostnetwork pod.
- In a Contiv deployment, various networks are used internally by Contiv, and communication to IP addresses outside the cluster is blocked if there is an overlap.
- In a Calico deployment:
  - The network policy matching on labels will not block hostnetwork access to pods or services.
  - Host IP change may impact pod networking. Restart calico pods will resolve the issue.
- `istioctl` is not installed when user enables istio. You can follow the Cisco Container Platform documentation for the installation process.
- A master VIP is required for a tenant cluster upgrade. Creating tenant clusters using the API without specifying a master VIP has a risk of corrupting the tenant cluster during tenant cluster upgrades.
- When you upgrade tenant clusters the Prometheus and EFK components are purged before installing the new versions. If you want to save history, a manual backup and migration is required before a tenant cluster upgrade.
- After an upgrade, the Cisco Container Platform web interface port may be different from the previous version.
- Taking a snapshot of the VMs managed by Cisco Container Platform is currently unsupported and results in failures during upgrades.
- ACI deployments are only supported in online mode.
- ACI deployments do not support Kubernetes security context.

## Viewing Open and Resolved Bugs

The open and resolved bugs for this release are accessible through the Cisco Bug Search Tool. This web-based tool enables you to access the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in this product and other Cisco hardware and software products. You can search for bugs using bug IDs or keywords.

### Before you begin

Ensure that you have a Cisco username and password to login to the Cisco Bug Search Tool.

If you do not have a Cisco username and password, you can register for them at <http://tools.cisco.com/RPF/register/register.do>.

### Procedure

- 
- Step 1** Log in to the [Cisco Bug Search Tool](#) with your Cisco username and password.
- Step 2** To search for a specific bug, enter the bug ID in the **Search For** field and press the **Enter** key.
- Step 3** To search for the bugs that belong to the current release, enter **Cisco Container Platform 1.4.0** in the **Search For** field, and then press the **Enter** key. (Leave the other fields empty.)
- Note**
- Once the search results are displayed, you can use the **Filter** options to easily find the bugs that are of interest to you.
  - You can search for bugs by status, severity, modified date, and so on.
- Step 4** To export the results to a spreadsheet, click the **Export Results to Excel** link.
- 

For more information on the Cisco Bug Search Tool, refer to <http://www.cisco.com/web/applicat/cbsshelp/help.html>.

## Related Documentation

The following table lists the documents available for the Cisco Container Platform 1.4.0 release.

Document	Description
Cisco Container Platform 1.4.0 Installation Guide	Provides information on installing Cisco Container Platform on your deployment environment.
Cisco Container Platform 1.4.0 User Guide	Provides information on administering and managing Kubernetes clusters, and deploying applications on them.
Cisco Container Platform 1.4.0 Third-Party License Attributions	Provides the legal attributions for third-party software and components included in the Cisco Container Platform product.
Open Source Used In Cisco Container Platform 1.4.0	Provides information on licenses and notices for open source software used in this product.

These documents are available on [cisco.com](https://www.cisco.com).

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see [What's New in Cisco Product Documentation](#).

What's New in Cisco Product Documentation lists all new and revised Cisco technical documentation. You can subscribe to it, and receive free RSS feed service directly to your desktop using a reader application.

---

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com go trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2018 Cisco Systems, Inc. All rights reserved.