



Cisco Cloud Services Platform Release Notes, Release 2.6.0

First Published: 2019-04-19

Last Modified: 2019-12-17

Cisco Cloud Services Platform Release Notes

This document describes the features and limitations for the Cisco Cloud Services Platforms 2100 and 5000, Release 2.6.0.

Supported Cisco Networking Services

Cisco CSP can host any Cisco or third-party VNF that is supported on KVM hypervisor. Some of the Cisco VNFs available include the following:

- Cisco Cloud Services Router (CSR) 1000V virtual router
- Cisco IOS® XRv 9000 Router
- Cisco Adaptive Security Virtual Appliance (ASAv)
- Cisco Firepower™ NGFW Virtual
- Cisco Prime® Virtual Network Analysis Module (vNAM)
- Cisco Virtual Wide Area Application Services (vWAAS)
- Cisco Web Security Virtual Appliance (WSAv)
- Cisco Identity Services Engine (ISE)
- Cisco Firepower Management Center (FMC)
- Cisco Virtual Security Gateway (VSG) for Cisco Nexus® 1000V Series Switch deployments
- Cisco Virtual Supervisor Module (VSM) for Cisco Nexus 1000V Series Switch deployments
- Cisco Data Center Network Manager (DCNM)

New and Enhanced Features

Cisco CSP Release 2.6.0 includes the following features and enhancements along with security and bug fixes:

New Features

- NETCONF notifications: NETCONF notifications are generated for various PNIC and services events.

- Statistical snapshot of pNIC and vNIC: Ability to capture statistics for pNICs and vNICs during a period of time controlled by start or stop commands.
- vNIC statistics: Statistical information is now available for native OVS, OVS-DPDK, and SRIOV interfaces.
- Patch upgrade: Ability to upgrade selected CSP software components through patch packages without reboot, instead of ISO upgrade for the entire CSP software.
- vNIC admin status support: The admin status of vNICs assigned to services can be configured in shut or no shut state. This functionality is available for vNICs on Intel X710, XL710, XXV710 and i350 NICs.
- vNIC bandwidth control: The bandwidth for traffic originating from a vNIC can be limited to a designated Mbps value. This functionality is available for vNICs on Intel X710, XL710, XXV710, X520, and i350 NICs.
- Disk encryption using TPM: Ability to encrypt selected directories of CSP by using keys stored on board TPM security chip.
- Virtual to physical CPU mapping per service: Ability to view virtual to physical CPU mapping per service.
- GUI enhancements: The GUI has been enhanced to show CSP hardware information and system information such as, core and services CPU utilization graphs.

Network Interface Card Driver Compatibility

This release includes the following NICs Physical function (PF) drivers. See VNF documentations for more information about compatibility between the Virtual function (VF) driver included in VNF and the NICs PF drivers.

- Ixgbe PF driver version: 5.6.1
- I40e PF driver version: 2.9.21

Important Notes

- Ensure that you upgrade to the latest Cisco UCS firmware available on CCO. The minimum required version being 4.0(4h).
- You can only upgrade from CSP Release 2.4.0 or later to this release.
- The following field notice might impact CSP 5000 models that are running CIMC versions earlier than 4.0(4e). Therefore, it is recommended to upgrade the CIMC version to 4.0(4h) on these models.

<https://www.cisco.com/c/en/us/support/docs/field-notices/704/fn70432.html>

Access CSP Bugs

About the Cisco Bug Search Tool

Use the [Cisco Bug Search Tool](#) to access open and resolved bugs for a release.

The tool allows you to search for a specific bug ID, or for all bugs specific to a product and a release.

Save Search Load Saved Search Clear Search Email Current Search

Search For: +
Examples: CSCId10124, router crash, etc...

Product: Series/Model Select from list

Releases: Affecting or Fixed in these Release: Enter release number

368025

You can filter the search results by last modified date, bug status (open, resolved), severity, rating, and support cases.

Save Search Load Saved Search Clear Search Email Current Search

Search For: +
Examples: CSCId10124, router crash, etc...

Product: Series/Model Select from list

Releases: Affecting or Fixed in these Release:

Filter: Modified Date: Status: Severity: Rating: Support Cases: Bug Type: Customer Visible

Viewing 1 - 25 of 132 results Sort by Export Results to Excel

368026



Note For the **Product** drop-down list, choose either **Cisco Cloud Services Platform 2100** or **Cisco Cloud Services Platform 5000**.

Known Behavior

- Management interfaces cannot be configured as passthrough interfaces.
- Only local users can log in to Cisco CSP using CIMC console. Remote TACACS+ users cannot log in to Cisco CSP by using CIMC console.
- Only the vNIC e1000 model is supported with Cisco VSM and Cisco VSG services.
- Only ISO image files are supported with Cisco VSM and Cisco VSG services.

Related Documentation for Cisco Cloud Services Platform

- [Data Sheet for Cisco Cloud Services Platform 5000 Series](#)
- [Release Notes for Cisco Cloud Services Platform](#)
- [Quick Start Guide for Cisco Cloud Services Platform](#)
- [Hardware Installation Guide for Cisco Cloud Services Platform](#)
- [Regulatory Compliance and Safety Information for Cisco Cloud Services Platform](#)
- [Configuration Guide for Cisco Cloud Services Platform](#)
- [Command Reference Guide for Cisco Cloud Services Platform](#)
- [REST API Guide for Cisco Cloud Services Platform](#)

