Cisco Cloud Services Platform Release Notes, Release 2.8.0

First Published: 2019-04-19

Last Modified: 2021-08-20

Cisco Cloud Services Platform Release Notes

This document describes the features and limitations for the Cisco Cloud Services Platforms 5000, Release 2.8.0.

> **Note** CSP-OS End of Life was announced on June 15, 2021.

Guest VNFs

Cisco CSP can host Cisco VNFs or third-party VNFs that are supported on KVM hypervisors. For more information about the support for VNFs, see the individual product release documentation.

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)

Non-Cisco Vendor Owned VNFs

You can run VNFs owned by various vendors on Cisco CSP 5000 Series Platforms that are running on the CSP-OS. Formal support for these VNFs requires a joint effort between Cisco and the VNF vendor.

Cisco offers VNF vendors a "for-fee" NFVIS 3rd-party certification program to test and certify their VNFs on Cisco's virtual platforms. After the testing and certification is complete, the results are published on this page- Cisco Enterprise NFV Open Ecosystem and Qualified VNF Vendors

For more specific support details about VNF versions and test compatibility matrix with CSP-OS releases, see the VNF vendor release documentation on the vendor support site.

New and Enhanced Features

Cisco CSP Release 2.8.0 includes the following features and enhancements along with security and bug fixes:

New Features

- Preserve MAC addresses on VNF import: Ability to retain MAC addresses of an exported service when the service is imported. If you choose to retain the service UUID, then MAC addresses of VINCs are also retained.

- On-demand VNF migration with Day-N configuration: Ability to migrate a powered off service with Day-N configuration between cluster nodes for services deployed in Gluster. You can choose a new node or use **Auto Selection** to let the system select the best available node from the cluster.

- Enhanced cluster operation using REST APIs: Introduced enhanced cluster REST APIs for cluster operations. The cluster operations were only available using CSP GUI in the earlier releases.

- SRIOV based LACP port channel: Provides support for LACP on SRIOV port channels.

- Secure CSP boot: Enables secure boot for CSP. This feature enables firmware to validate the signature of the boot software including UEFI firmware drivers, EFI applications, and CSP software.

- Secure VNF boot: Enables secure boot for services. This feature enables CSP to validate the service signature before deploying the service. The secure boot is only supported with UEFI boot mode, and not supported with legacy BIOS boot mode.

- More Virtio disks per VNF: Ability to add up to 5 Virtio disks for each service. A maximum of 3 disks could be added in earlier releases.

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: 5.6.5

- I40e PF driver version: 2.10.19.82

Important Notes

- You can only upgrade from CSP Release 2.5.0 or later to this release.

- Ensure that you upgrade to the latest Cisco UCS firmware available on CCO. The minimum required version being 4.1(1d). However before upgrading the firmware to 4.1(1d) or a newer version, perform the following steps:

  1. In CIMC BIOS/Advanced/LOM and PCIe Slots configuration, disable **OptionROM on LOM Ports**, **PCIe Slots for MLOM**, and **PCIe slots for network adapters**.

  2. Refer to the bug, CSCvq74492 in the UCS release notes for more information. See UCS Release Notes.

- The following field notice might impact CSP 5000 models that are running CIMC versions earlier than 4.0(4e) with earlier versions of CSP software. Therefore, it is recommended to upgrade the CIMC version to 4.0(4h) on these models.
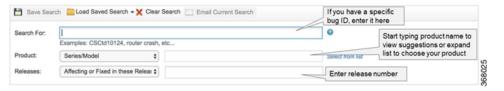
  https://www.cisco.com/c/en/us/support/docs/field-notices/704/fn70432.html
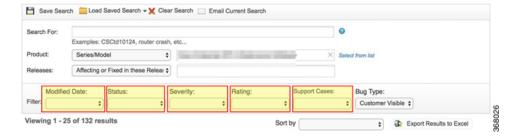
Access CSP Bugs

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.

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

✎

Note For the **Product** drop-down list, choose **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 Plarform

• Configuration Guide for Cisco Cloud Services Platform

• Command Reference Guide for Cisco Cloud Services Platform

• REST API Guide for Cisco Cloud Services Platform