# Cisco Cloud Services Platform Release Notes, Release 2.7.1

**First Published:** 2019-04-19

**Last Modified:** 2020-06-18

## Cisco Cloud Services Platform Release Notes

This document describes the features and limitations for the Cisco Cloud Services Platforms 5000, Release 2.7.1.

**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

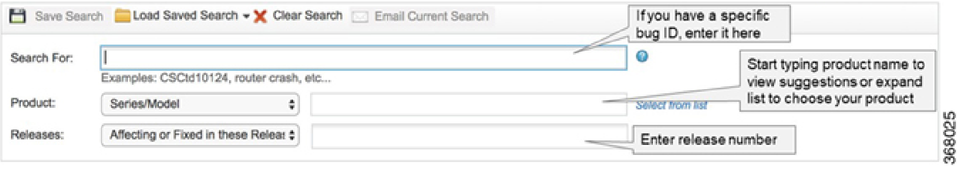
For more specific support details about VNF versions and test compatibility matrix with CSP-OS releases, see the VNF vendor release documentation on the vendor support site.

## 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.

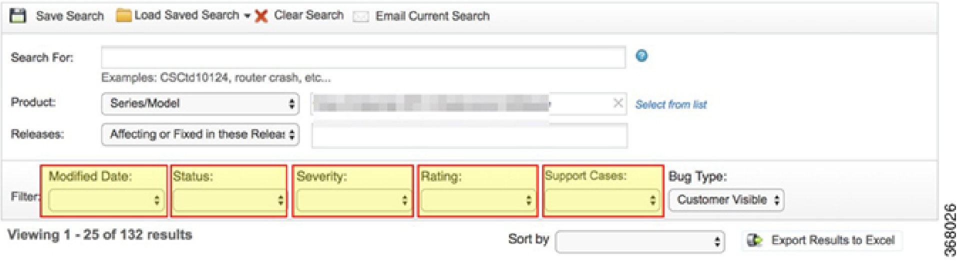


If you have a specific bug ID, enter it here

Start typing product name to view suggestions or expand list to choose your product

Enter release number

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



**Note** From the **Product** drop-down list, choose **Cisco Cloud Services Platform 5000**.

## Resolved Bugs

This is a minor release. It includes,

- all 2.7.0 content
- fixes for the following bugs:

| Bug ID | Description |
|---|---|
| CSCvu23443 | Admin-group users unable to login through SSH |

| Bug ID | Description |
|---|---|
| CSCvu41327 | Allow admin-group access privilege to all commands except for create-user |
| CSCvu28358 | Admin user lost permission while upgrading CSP from 2.3.2 to 2.7.0 |
| CSCvu28363 | Cluster creation fails, when a user is logged in as a TACACS or RADIUS admin-group user, and tries to create a cluster |
| CSCvu40789 | During clean install, CSP Day0 Questionnaire errored out with insufficient disk space |

For more information, see CSP Release 2.7.0 documentation and release notes.

## 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.

- If any active sessions with CIMC KVM console exist, ensure that you do not select **Activate Virtual devices** prior to performing CLI or REST API based upgrade of a CSP Release.
- If you have set **rsyslog_udp_only** to **True**, ensure that you set **rsyslog_tcp_port** to **0** prior to upgrading to 2.7.1 Release.
- 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

## 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