

Release Notes for Cisco CSR 1000v Series, Cisco IOS XE Gibraltar 16.12.x

First Published: 2019-07-26

Last Modified: 2021-02-02

Cisco CSR 1000v Series Cloud Services Routers Overview



- Note** Explore the [Content Hub](#), the all new portal that offers an enhanced product documentation experience.
- Use faceted search to locate content that is most relevant to you.
 - Create customized PDFs for ready reference.
 - Benefit from context-based recommendations.

Get started with the Content Hub at content.cisco.com to craft a personalized documentation experience.

Do provide feedback about your experience with the Content Hub.

Virtual Router

The Cisco Cloud Services Router 1000V (CSR 1000V) is a cloud-based virtual router that is intended for deployment in cloud and virtual data centers. This router is optimized to serve as a single-tenant or a multitenant WAN gateway.

When you deploy a CSR 1000V instance on a VM, the Cisco IOS XE software functions as if it were deployed on a traditional Cisco hardware platform. You can configure different features depending on the Cisco IOS XE software image.

Secure Connectivity

CSR 1000V provides secure connectivity from an enterprise network such as a branch office or a data center, to a public or a private cloud.

System Requirements

Hardware Requirements

For hardware requirements and installation instructions, see the [Cisco CSR 1000v Series Cloud Services Router Software Configuration Guide](#) .

Software Images and Licenses

The following sections describe the licensing and software images for CSR 1000V.

Cisco Smart Licensing

The Cisco CSR 1000V router supports Cisco Smart Licensing. To use Cisco Smart Licensing, you must first configure the Call Home feature and obtain the Cisco Smart Call Home Services. For more information, see [Installing CSR 1000V Licenses](#) and [Smart Licensing Guide for Access and Edge Routers](#).

For a more detailed overview on Cisco Licensing, go to <https://cisco.com/go/licensingguide>.

Cisco CSR 1000v Evaluation Licenses

Evaluation license availability depends on the software version:

- Evaluation licenses valid for 60 days are available at the Cisco Software Licensing (CSL) portal: <http://www.cisco.com/go/license>

The following evaluation licenses are available:

- IPBASE technology package license with 10 Gbps maximum throughput
- SEC technology package license with 5 Gbps maximum throughput
- APPX technology package license with 5 Gbps maximum throughput
- AX technology package license with 2.5 Gbps maximum throughput

If you need an evaluation license for the Security technology package, or for an AX technology package with higher throughput, contact your Cisco service representative.

For instructions on obtaining and installing evaluation licenses, see the “Installing CSL Evaluation Licenses for Cisco IOS XE 3.13S and Later” section of the [Cisco CSR 1000v Software Configuration Guide](#).

Cisco CSR 1000v Software Licenses

Cisco CSR 1000v software licenses are divided into feature set licenses. The supported feature licenses depend on the release.

Current License Types

The following are the license types that are supported (Cisco IOS XE Everest 16.4.1 or later):

- IPBase: Basic Networking Routing (Routing, HSRP, NAT, ACL, VRF, GRE, QoS)
- Security: IPBase package + Security features (IP Security VPN, Firewall, MPLS, Multicast)
- AX: IPBase package + Security features + Advanced Networking features (AppNav, AVC, OTV and LISP)
- APPX Package: IPBase package + Advanced Networking features - Security features (IP security features not supported)

Legacy License Types

The three legacy technology packages - Standard, Advanced, and Premium - were replaced in the Cisco IOS XE Release 3.13 with the **IPBase**, **Security**, and **AX** technology packages.

Features Supported by License Packages

For more information about the Cisco IOS XE technologies supported in the feature set packages, see the overview chapter of the [Cisco CSR 1000v Series Cloud Services Router Software Configuration Guide](#).

Throughput

The Cisco CSR 1000v router provides both perpetual licenses and term subscription licenses that support the feature set packages for the following maximum throughput levels:

- 10 Mbps
- 50 Mbps
- 100 Mbps
- 250 Mbps
- 500 Mbps
- 1 Gbps
- 2.5 Gbps
- 5 Gbps
- 10 Gbps

The throughput levels are supported for different feature set packages in each version. For more information about how the maximum throughput levels are regulated on the router, see the [Cisco CSR 1000v Cloud Services Router Software Configuration Guide](#).

Memory Upgrade

A memory upgrade license is available to add memory to the Cisco CSR 1000v router (Cisco IOS XE 3.11S or later). This license is available only for selected technology packages.

Additional Information about Licenses and Activation

For more information about each software license, including part numbers, see the [Cisco CSR 1000v Router Datasheet](#). For more information about the standard Cisco IOS XE software activation procedure, see the [Software Activation Configuration Guide, Cisco IOS XE Release 3S](#).

Software Image Nomenclature for OVA, ISO, and QCOW2 Installation Files

The Cisco CSR 1000v installation file nomenclature indicates properties supported by the router in a given release.

For example, these are filename examples for the Cisco IOS XE Everest 16.4.1 release:

- csr1000v-universalk9.16.04.01.ova
- csr1000v-universalk9.16.04.01.iso

- csr1000v-universalk9.16.04.01.qcow2

The filename attributes are listed below, along with the release properties.

Table 1: OVA Installation Filename Attributes

Filename Attribute	Properties
Example:universalk9	Installed image package.
03.09.00a.S.153-2.S0a	Indicates that the software image is for the Cisco IOS XE 3.9.0aS release image (mapped to the Cisco IOS 15.3(2) release).
std or ext	Standard release or extended maintenance support release.

New and Enhanced Software Features for Cisco IOS XE Gibraltar 16.12.x

New and Enhanced Features for Cisco IOS XE Gibraltar 16.12.1a

The following are the new software features that are supported on the Cisco CSR 1000v for Cisco IOS XE Gibraltar 16.12.1a release:

- [Support for L2 Extension for Public Cloud](#): From this release, you can enable enterprise and cloud providers to deploy a secure hybrid cloud extension with CSR 1000V instances using LISP. Use the command-line interface to extend a Layer 2 domain to the public cloud using one subnet from the enterprise data center. You can achieve benefits such as IP mobility and workload migration by configuring L2 extension for public cloud.
- [Using custom data for Day 0 configuration](#): When you deploy a Cisco CSR 1000v VM instance on Google Cloud Platform, you can choose to either use the console to access the startup script, or use the CLI to access the custom data to achieve a variety of automation goals. The custom data in GCP allows you to run Cisco IOS XE configuration commands, install Python packages in guestshell on Day0, run scripts in guestshell on Day0, and provide licensing information to boot the CSR 1000v instance with a desired technology package.
- [Support for IPv6 for CSR 1000v instance running on AWS](#): From the 16.12.1 release, IPv6 addressing is supported for CSR 1000v instances running on Amazon Web Services. Implementing basic IPv6 connectivity in the Cisco software consists of assigning IPv6 addresses to individual device interfaces. You can also enable IPv6 traffic forwarding globally, and Cisco Express Forwarding switching for IPv6. You can enhance basic connectivity functionality by configuring support for AAAA record types in the Domain Name System (DNS) name-to-address and address-to-name lookup processes, and by managing IPv6 neighbor discovery.
- [IPv6 support for Encrypted Traffic Analytics](#): Encrypted Traffic Analytics (ETA) uses passive monitoring, extraction of relevant data elements, and supervised machine learning with cloud-based global visibility. ETA is now extended to IPv6 addresses to identify malware communications in encrypted traffic.
- [VNF Secure Boot](#): The secure boot feature prevents malicious software applications and unauthorized operating systems from loading into the system during the system start up process. This feature ensures that the software applications that boot up on the device are certified by Cisco. A secure compute system ensures that the intended software on the system runs without malware or tampered software.

- **Unclassified-mac initiator with IANA:** The Unclassified Mac Initiator with IANA feature supports ISG IPv6 sessions based on the unclassified mac address of the subscriber. If subscriber uses DHCPv6 for getting IPv6 addresses, ISG supports creation of subscriber sessions based on DHCPv6 packets with the IANA option.
- **Show commands updates for SRTP Rollover Counter (ROC):** The output of the following commands is enhanced to display SRTP ROC information: show voip fpi calls, show voip fpi stats, show voip rtp connections.
- **PFS for GIKEv2:** If a Group Member (GM) is compromised, an attacker may access saved long-term keys and messages. Use Perfect Forward Secrecy (PFS) for GETVPN so that the attacker cannot use the keys and messages to obtain the keys of past or future sessions to decrypt recorded or future communication.
- **Support for SVTI multi-SA:** You can define and associate an Access Control List (ACL) with an SVTI to select traffic between specific source and destination proxies. By associating the ACL, you are modifying the default configuration that uses a single any-any traffic selector and for every non-any-any traffic selector, IPsec SAs are created so that multiple SAs can be attached to an SVTI.
- **Support for Federal Information Processing Standards:** FIPS are publicly announced standards developed by the United States federal government for use in computer systems by non-military government agencies and government contractors.

With the FIPS software, you can prevent use of non-FIPS compatible algorithms, this ensures that the device is configured to use only FIPS-approved algorithms. Some functionality in the computer systems may fail in the FIPS mode if the FIPS software attempts to use non-FIPS compliant algorithms.

- **Web User Interface to Manage Cisco 1000 Series Integrated Services Routers:** Starting Cisco IOS XE Gibraltar 16.12.1a release and later, Web UI lets you configure Cisco Unified Communications Manager Express (CUCM-E), File manager, Trustsec and Trustsec with statistics on the **Cisco 1000 Series Integrated Services Routers**. To learn more, refer to the WebUI Online Help.



Note When you upgrade from one Cisco IOS XE release to another, you may see a *%Invalid IPV6 address* error in the console log file. To rectify this error, enter the global configuration mode, re-enter the missing IPv6 alias commands, and save the configuration. The commands are persistent on subsequent reloads.

New and Enhanced Features for Cisco IOS XE Gibraltar 16.12.2

The following are the new software features that are supported on the Cisco CSR 1000v for Cisco IOS XE Gibraltar 16.12.2 release:

- **Support for Media Flow-around using Multi-VRF:** Support for Media flow-around using Multi-VRF is added following call flows in standalone and high availability scenarios:
 - Basic Audio Call
 - Call Hold and Resume
 - Re-INVITE based Call Transfer
 - 302 based Call Forward
 - Fax Pass Through Calls

- T.38 Fax Calls

Enhancements to Cisco IOS XE Gibraltar 16.12.4a

Starting from the Cisco IOS XE 16.12.1a release, Azure Advanced Networking deployments no longer require a release-specific Azure AN BIN file image. In accordance, starting from the Cisco IOS XE 16.12.4a release, the Azure AN BIN image file is no longer available for download. Instead, for Azure Advanced Networking, use the CRYPTO BIN file (for example, csr1000v-universal9.16.12.04a.SPA.bin).

Resolved and Open Bugs for Cisco IOS XE Gibraltar 16.12.x

Using the Cisco Bug Search Tool

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 the bugs specific to a product and a release.

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

Open Bugs for Cisco IOS XE Gibraltar 16.12.1a

Caveat ID Number	Description
CSCvq42124	Azure: CSR with Custom data throws % (CVAC) Command failed: PRC_INVALID, PRC_FAILURE_PERMANENT
CSCvq39428	1 NIC deployment in Azure: not able to SSH into the box

Resolved Bugs for Cisco IOS XE Gibraltar 16.12.1a

Caveat Number ID	Description
CSCvo02336	CSR1kv Factory Reset - Retaining eval timers
CSCvo78046	AWS: UDI serial changes when CSR 1000v instance type is changed from c4 to c5 or vice versa
CSCvm81058	The management IP address is not properly configured with CSR1K VNF
CSCvo28444	Support MBRv2 partition scheme and Grub2 install in all clouds
CSCvo28017	CSR1000v IC2M Self Integrity Test Bypassed
CSCvp29906	CSR1kv router crash due to file descriptor leak
CSCvp37231	CSR1000v - i40evf interface shows Up but does not pass traffic
CSCvp17502	CSR1000v No User Settable MTU

Open Bugs for Cisco IOS XE Gibraltar 16.12.2

Caveat ID Number	Description
CSCvr78580	CSR1000v Azure HAv3 route table update fails with non-IP address next hop entries

Resolved Bugs for Cisco IOS XE Gibraltar 16.12.2

Caveat ID Number	Description
CSCvp38857	unable to modify interface speed for CSRv cEdge
CSCvp99550	ISRV GE interfaces show ingress traffic even in admin shut down state
CSCvq71877	CUBE must preserve ROC values after master key is re-keyed
CSCvq75994	Issue with installing CSR 1KV MEMORY 4G license with SLR
CSCvr27714	CSR+SDWAN on AWS will install default route in startup config which conflicts with some topologies
CSCvr39955	Throughput defaulted when UDI is corrupted

Resolved Bugs for Cisco IOS XE Gibraltar 16.12.2s

Caveat ID Number	Description
CSCvs35311	MAP-E: Remove embedded customer specific data from the image

Open Bugs for Cisco IOS XE Gibraltar 16.12.3

Caveat ID Number	Description
CSCvs45225	Flash devices not mounted on 16.10 or later CSR1000v



Note In Cisco IOS XE Release 16.12.3, the semantic version number for the YANG models is not updated and is therefore not accurate. However, this limitation does not impact the functionality of the YANG models.

Open Bugs for Cisco IOS XE Gibraltar 16.12.4

Caveat ID Number	Description
CSCvs45225	Flash devices not mounted on 16.10 or later CSR1000v
CSCvu52185	CSR1000v may unexpectedly reload (or hang) due to keepalive failures

Resolved Bugs for Cisco IOS XE Gibraltar 16.12.4

Caveat ID Number	Description
CSCvs81791	Fix for kernel driver issue causing wake up for empty block, packet too large to process
CSCvt05340	CSR controller mode interface total drops counter wrong behaviour
CSCvt16915	CSR Gig3 Interface not created even after ENI is attached to VM instance in AWS
CSCvt37981	CSR cannot create Azure VHD images
CSCvt50394	Custom Data: bash/python scripts in Scripts section does not execute
CSCvu45109	CSR: Azure AN: MLX5 driver fails to load in 16.12.2 & 16.12.3

Open Bugs for Cisco IOS XE Gibraltar 16.12.5

Caveat ID Number	Description
CSCvs45225	Flash devices not mounted on 16.10 or later CSR1000v
CSCvw66424	STUN protocol operability with multi-VRF on CSR1000v CUBE

Caveat ID Number	Description
CSCvw93490	CSR1000v crashing frequently with Critical software exception error.
CSCvx11972	GuestShell Gets removed during the IOS upgrade

Resolved Bugs for Cisco IOS XE Gibraltar 16.12.5

Caveat ID Number	Description
CSCvs93857	Failed to apply custom data to CSR in AWS/Azure
CSCvt20227	16.12.3: Curl failures observed while doing FTP for 10MB file
CSCvt21771	Device may crash due to racing in configuration for route-map attachment and set action
CSCvt57538	IOSd crash due to Segfault in Crypto IKEv2 in ikev2_free_id
CSCvu27060	evpn ipv6 route-type 5 mistake to use vrf ipv4 route-target.
CSCvu77890	excess fcmd memory consumption :CSR1000v rebooted with reason 'CPU Usage due to Memory Pressure'
CSCvu98884	Rapid BFD events on CSR running HA solution causes CSR to get stuck in a non-operational state
CSCvv03800	Platform lost all configuration after upgrade from 16.12 to 17.3
CSCvv04959	GRUB2 Arbitrary Code Execution Vulnerability
CSCvv25529	16.12.4 ucmk9 cedge not able to join overlay with 19.2.3 and 20.3
CSCvv27219	ONEP fails to process a REST API request due to "Too many active vty processes,. ONEP_FAIL" error
CSCvw64559	Throughput license grace period starts counting down after upgrade router software

Open Bugs for Cisco IOS XE Gibraltar 16.12.6

Caveat ID Number	Description
CSCvt27778	Evaluation of csrc-bpr for Apache Tomcat Ghostcat vulnerability
CSCvw23197	BFD sessions go down on Service VPN after UTD is enabled on cEdge
CSCvx37573	CSR1000v: Delay in DMVPN tunnel line protocol going down
CSCvx62167	Route-map corruption when configured using Netconf with ncclient manager
CSCvz22268	With curl schedule download, stuck Failed to send the request. There is another request in progress

Resolved Bugs for Cisco IOS XE Gibraltar 16.12.6

Caveat ID Number	Description
CSCvv12401	ZBFW HA redundancy stuck in STANDBY-COLK-BULK. Bulksync Traceback seen in logs
CSCvw66424	STUN protocol operability with multi-VRF on CSR1000v CUBE
CSCvx11972	GuestShell Gets removed during the IOS upgrade
CSCvx50806	Corruption of memory in the SIP History Headers
CSCvx84786	NAT ALG breaks(Drops) ICMP control messages (ICMP Fragmentation Needed) for PMTUD
CSCvx87726	CSR1000v Multicast Over OTV Not Forwarding

Resolved Bugs for Cisco IOS XE Gibraltar 16.12.7

Caveat ID Number	Description
CSCvz57415	128.0.0.0/2 is installed into CEF as unusable on a PETR after EID-Prefix is removed.
CSCvy79950	Cannot force the switch to ask for option 12 to be assigned from the DHCP server
CSCvz24267	Static NAT entry is injecting a route to Null0
CSCvz69851	CSR: Missing iid_certs for AWS invite-only regions
CSCwa36699	Prefetch CRL Download Fails

Resolved Bugs for Cisco IOS XE Gibraltar 16.12.8

Caveat ID Number	Description
CSCvy91615	Open SSH vulnerability for IOS-XE platforms.
CSCwb08932	Standby device crashed due to SISF BT MAC MOV.
CSCvz77313	Device reload due to SFF8472.
CSCwa27659	Virtual VRRP IP address unreachable from the BACKUP VRRP.
CSCwa82143	INTSCHED: 'may_suspend' disabled -Process="HSRP IPv4" log generate during boot up.
CSCwb26335	RSP3:Err reading data from table dmi-general: Could not get boolean val for feature.side_effect_sync.
CSCwb96964	Device crashes on creating telemetry subscription.

Caveat ID Number	Description
CSCvw60355	DHCPv6: Memory allocation of DHCPv6 relay option results in crash.
CSCwb24680	LLDP System Description not correctly seen in ISE.
CSCvz80171	SIP call fails egress dial-peer uses "session server-group" and "sip options-keepalive".

Related Documentation

- [Release Notes for previous versions of Cisco Cloud Services Router 1000V Series](#)
- [Configuration Guides for Cisco Cloud Services Router 1000V Series](#)
- [Product Landing page for Cisco Cloud Services Router 1000V Series](#)
- [Datasheet for Cisco Cloud Services Router 1000V Series](#)
- [Field Notices](#)
- [Deferral Notices](#)
- [Cisco Bulletins](#)

