Release Notes for Cisco CSR 1000v Series, Cisco IOS XE Everest 16.4

First Published: 2016-11-30

Last Modified: 2017-04-30

Release Notes for Cisco CSR 1000v Series, Cisco IOS XE Everest 16.4

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.

Technologies Supported by a Platform

A platform's product landing page lists technology configuration guides for Cisco IOS XE technologies that the platform supports.

In each technology configuration guide, a Feature Information table indicates when a feature was introduced to the technology. For some features, the table also indicates when additional platforms have added support for the feature.

To determine whether a particular platform supports a technology, view the list of technology configuration guides posted on the platform's product landing page. For example, see Cisco Cloud Services Router 1000v Series.

System Requirements

The following sections describe the system requirements for the Cisco CSR 1000v Series Cloud Services Routers.

- Hardware Requirements, on page 2
- Software Images and Licenses, on page 2

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

Table 1: OVA Installation Filename Attributes , on page 4 lists the attributes and the release properties indicated.

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.

Features and Notes: Release Cisco IOS XE Everest 16.4.1

Features

Cisco CSR 1000v Smart Licensing Behavior Change

One change to the behavior is that the Cisco CSR 1000v router may receive an “out of compliance” message from the Smart Licensing server. For example, if the number of available licenses recorded on the Smart Licensing account has been exceeded. The system then continues to operate at a level previously allowed by the license.

Another change to the behavior occurs when smart license authorization expires after 90 days, in which case the Cisco CSR 1000v continues to run, but in Feature Restricted mode. For example, this may happen when the CSSM satellite server has had no connectivity with the Smart Licensing server for more than 90 days.

See the “Installing Cisco CSR 1000v Licenses” section of the Cisco CSR 1000v Series Cloud Services Router Software Configuration Guide for more details.

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

Show NBAR Attributes Command

To show the configured NBAR attributes, use the **show ip nbar attribute** command in privileged EXEC mode. For example:

show ip nbar attribute [application-group | business-relevance | category | encrypted | p2p-technology

| sub-category | traffic-class | tunnel]

show ip nbar attribute *attribute-name attribute-value* [*attribute-name* | *attribute-value*]

Nginx/HTTP - Web Security Features for 16.4

For detailed information, see the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/https/configuration/xe-16/https-xe-16-book.html

Bypass NAT functionality

For detailed information, see the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/xe-16/nat-xe-16-book/iadnat-addr-consv.html

QoS: DMVPN per-tunnel QoS over aggregate GEC

For detailed information, see the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_mqc/configuration/xe-16/qos-mqc-xe-16-book/aggregate-etherchannel-quality-of-service.html

Cisco SSL 6.0 FOM

Cisco SSL 6.0 is used to upgrade openssl to 1.0.2 g. The security updates will be available for the next three years. From Cisco IOS XE Everest 16.4.1, RC4 and DES ciphers have been blocked and will no longer be supported as they are considered vulnerable.

TrustSec SGACL monitor mode on routers (ASr1K, ISR4K, CSR)

For detailed information, see the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cts/configuration/xe-16/sec-usr-cts-xe-16-book/sec-cts-sgacl.html

DMVPN Multiple Tunnel Termination

For detailed information, see the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/xe-16/sec-conn-dmvpn-xe-16-book/sec-conn-dmvpn-mtt.html

Site to Site IPSEC VPN for WEBUI

- Site-to-Site VPN—A Virtual Private Network (VPN) allows you to protect traffic that travels over lines that your organization may not own or control.VPNs can encrypt traffic sent over these lines and authenticate peers before any traffic is sent. Site-to-Site VPN feature allows you to create a VPN network connecting two routers.

- Cellular Interface—The Cellular Interface feature supports the Fourth Generation (4G) Long-Term Evolution (LTE) and its primary application is Cellular WAN connectivity, which functions as a primary or backup data link for critical data applications.
- Configuring Application Visibility—Enhanced to include Application Signatures identifier based.

QoS: Tunnel Pre-classify uses Internal Address for fair-queue Distribution

See the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_mqc/configuration/xe-16/qos-mqc-xe-16-book/qos-evc.html

Increase FlexVPN Scale to 10K Tunnels

To increase FlexVPN scale to 10K tunnels, you can use the following commands.

Increase the Cisco IOS XE memory using the command:

platform memory add 3286

Increase the control-plane CPU using the command:

platform resource control-plane-heavy

Enable FlexVPN tcam bypass using the command:

platform ipsec flexvpn-bypass-tcam

Note that this requires a Cisco CSR 1000v with a high-speed Intel CPU (Processor Type Intel(R) Xeon® CPU E5-2670 v3 2.30GHz), 4 vCPUs, and a 12 GB memory. Additionally, you must disable hyper-threading.

Notes

Note The following feature is available in a previous release, Cisco IOS XE Denali 16.3.1a

Amazon Web Services High Availability (AWS HA)

The method for monitoring AWS HA errors such as BFD peer down events has changed from using an EEM applet (in release Cisco IOS XE 3.16 or earlier) to using new Cisco IOS XE commands (for Cisco IOS XE Denali 16.3.1a or later) that include the **redundancy** command and sub-command **cloud provider** [**aws** | **azure**] *node-id*.

Use these commands to specify routing changes to the Route-table-id, Network-interface-id and CIDR in the event of an AWS HA error (for Cisco IOS XE Denali 16.3.1a or later).

The following verification commands are also available:**show redundancy cloud provider** [**aws** | **azure**] *node-id* and**debug redundancy cloud** [**all** | **trace** | **detail** | **error**].

For further information, see the “Configuring High Availability” section in Cisco CSR 1000V Series Cloud Services Router Deployment Guide for Amazon Web Services .

Web User Interface

The Web User Interface supports an embedded GUI-based device-management tool that provides the ability to provision the router, simplifies device deployment and manageability, and enhances user experience. The following features are supported on Web User Interface for Cisco IOS XE Everest 16.4:

- Site-to-Site VPN—A Virtual Private Network (VPN) allows you to protect traffic that travels over lines that your organization may not own or control.VPNs can encrypt traffic sent over these lines and authenticate peers before any traffic is sent. Site-to-Site VPN feature allows you to create a VPN network connecting two routers
- Cellular Interface—The Cellular Interface feature supports the Fourth Generation (4G) Long-Term Evolution (LTE) and its primary application is Cellular WAN connectivity, which functions as a primary or backup data link for critical data applications
- Configuring Application Visibility—Enhanced to include Application Signatures identifier based on NBAR engine version 28. NBAR engine version changes if you update the protocol package
- Software Upgrade
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Network Address Translation (NAT)
- Virtual Routing and Forwarding (VRF)
- Application Visibility and Control (AVC)
- Custom Application
- Serial Interface

Limitations and Restrictions in Cisco IOS XE Everest 16.4.1

REST API Management Container Images Compatible with Everest 16.4.1

- When using the Cisco IOS XE REST API with the router, note the following limitation: If the router is operating with Cisco IOS XE Everest 16.4.1, use the latest REST API management container image. Attempting to use a REST API container image released prior to Cisco IOS XE Denali 16.3 may cause the router to crash repeatedly.

Caveats

Overview

Caveats, or “bugs,” describe unexpected behavior. Severity 1 caveats are the most serious. Severity 2 caveats are less serious. Severity 3 caveats are moderate caveats. This section includes severity 1, severity 2, and selected severity 3 caveats.

Terminology

The Dictionary of Internetworking Terms and Acronyms contains definitions of acronyms that are not defined in this document:

http://docwiki.cisco.com/wiki/Category:Internetworking_Terms_and_Acronyms_(ITA)

Bug Search Tool

If you have an account on Cisco.com, you can also use the Bug Search Tool (BST) to find select caveats of any severity. To reach the Bug Search Tool, log into Cisco.com and go to https://tools.cisco.com/bugsearch/search .

If a defect that you have requested cannot be displayed, it may be because the defect number does not exist or the defect does not have a description available.

You can use to the Bug Search Tool to view new and updated caveats: https://tools.cisco.com/bugsearch/search
.

For Best Bug Search Tool Results

For best results when using the Bug Search Tool:

- In the **Product** field, enter Cloud Services Router.
- In the **Releases** field, enter one or more Cisco IOS XE releases of interest. The search results include caveats related to any of the releases entered in this field.

The tool provides autofill while you type in these fields to assist in entering valid values.

A search using release number **16.6** should find the caveats for Cisco IOS XE Everest 16.6.1.

Field Notices

We recommend that you view the field notices for the current release to determine whether your software or hardware platforms are affected. You can access the field notices from the following location:

http://www.cisco.com/c/en/US/support/tsd_products_field_notice_summary.html

Caveats: Cisco IOS XE Everest 16.4.1

Open Caveats—Cisco IOS XE Everest 16.4.1

Table 2: Open Caveats—Cisco IOS XE Everest 16.4.1

Caveat	Description
CSCvb36269	AWS: Second CSR interface comes up automatically when attached
CSCvb83122	ISR 43xx, CSR 1000v Possible intermittent interface failure of rx traffic
CSCvc19074	AWS: CSR, with a t2 instance, crashes when it has been running for more than 12 hours

Resolved Caveats-Cisco IOS XE Everest 16.4.1

Table 3: Resolved Caveats—Cisco IOS XE Everest 16.4.1

Caveat	Description
CSCuz50549	CSR 1000v may boot with its default configuration because the startup-config fails to be read properly
CSCuz64902	AWS: CSR csr_mgmt container fails to learn default route
CSCva07535	AWS: CSR Crashed after copying configuration file using kron-policy
CSCva20296	CSR 1000v linux_iosd_vxe core seen after Qcow install
CSCva45347	PCIe pass-thru w/ ixgbe driver causes MaxTu drops due to TCP reassembly

Caveat	Description
CSCuz09519	CSR Ingress over-subscription not represented by “show controllers”
CSCuz58508	CSR interfaces do not support user settable MTU
CSCuz96475	1vCPU CSR scale degradation on 5/28 vs 5/21 Cisco IOS XE Denali 16.3
CSCva65218	RestAPI/LICENSE: 500 is returned to use /api/v1/license
CSCva65638	RestAPI/LICENSE: udi in restapi response is different with CLI

Caveats: Cisco IOS XE Everest 16.4.2

Open Caveats—Cisco IOS XE Everest 16.4.2

Table 4: Open Caveats—Cisco IOS XE Everest 16.4.2

Caveat	Description
CSCve09400	AWS CSR 1000v: HA fails to send HTTPS request for China region
CSCve09469	CSR 1000v Crash Due to Packet Length Inconsistency
CSCvd47657	Router crashed in afw application
CSCvd89428	ASR1002-HX crash on configuring mpls-lsp-monis-lsp-monitor
CSCvc08361	Crash in XE3.17 in TCP-TLS B2B call scenario
CSCve07263	IPSec Tunnel stuck in Up/Down state after shut/no-shut - VPN Interop

Resolved Caveats—Cisco IOS XE Everest 16.4.2

Table 5: Resolved Caveats—Cisco IOS XE Everest 16.4.2

Caveat ID Number	Description
CSCus85486	CSR 1000v Default Licence of 0.1 Mbps blocking running IWAN on CML
CSCvc26824	AN: ACP is not getting created after save & reload in some specific scenario
CSCvb62685	AN: Channel/Nbr flap during bootstrap in ASR903 with standby RSP.
CSCuz85280	AN: Standby reload due to config-sync failure at CISCO_AN_IPSEC_PROFILE
CSCvc42729	Autonomic Networking Infrastructure Adjacency Discovery DoS Vulnerability
CSCvc42717	Autonomic Networking Infrastructure Registrar Device Reload
CSCvc89965	After reload route policy processing not re-evaluate with route-map using match RPKI
CSCvd09584	eVPN PMSI VNI decoding / encoding as MPLS label

Caveat ID Number	Description
CSCvb85945	Router crash @ IP RIB Update while deleting bgp config
CSCvb75286	RP crash @ BGP router with "import l2vpn evpn re-originate"
CSCvb53469	Ephone-DN remains in down state when restart all is given in telephony-service
CSCvc63958	SIP CME relays out "Authorization: header" received from IP Phone.
CSCvb51806	Router crash when removing EIGRP
CSCvd04210	IKEV2 Tunnels are flapping, rekey request received from PD, lifetime kilobytes configured
CSCvc55378	ASR1k crashed while unconfiguring Netflow
CSCvc32062	Evaluation of IOS XE BinOS component for Openssl September 2016
CSCva05558	IKEv2 IPv6 GRE IPSec fails to stabilize on asr1k on 16.3
CSCvd40880	Modifying crypto ACL leads to a removal of crypto map config
CSCvc59750	IKEv2 Aggregate-auth Timing Issue
CSCvc99738	IKEv2 tunnel fails to come up b/w Cisco routers post upgrading one router to 15.5(3)S5, 15.5(3)M5
CSCvd69373	IKEv2: Unable to initiate IKE session to a specific peer due to 'in-neg' SA Leak
CSCvd47757	csr1000v is not able to poll CISCO-IPSEC-FLOW-MONITOR-MIB
CSCvc51408	ISIS route oscillation due to ldp sync and interface max metric
CSCvb58857	LDP NSR : Remote Side VCs stays up even with local access interface shut after SSO
CSCvb49730	VFI is down after provisioning a new new VFI to the existing
CSCvc35325	MK51-UCI, Mcast trafic is blackholing on ISSU CV while upgrading from FC5 to FC6
CSCvc17525	complete traffic drop with DATA MDTs with latest polaris_dev
CSCvc90685	Accounting Stop not sent for PMIPv6 tunnel in LMA
CSCvc54049	Ignore home address is broken in MAG/LMA
CSCvd28966	MAG crash with traffic on and home interface config is removed
CSCvc03651	SSH / Telnet / Console freezes while bringing up PMIPv6 tunnel interface
CSCvc21452	ASR903:ISIS routes are set with Max Metric due to IGP LDP Sync
CSCva44687	ASR 1K Running IOS-XE 3.16S w/ MPLS Crashes on 'clear ip route *'
CSCvb88373	MRCP V2 logging tag support

Caveat ID Number	Description
CSCvc99925	ASR 1k NHS Fallback fails for NHRP on secondary path
CSCva70115	ISR4331 crash due to NHRP running 03.16.03.S
CSCva97469	VA stuck in protocol down state after failing to establish IPSec session
CSCvc19234	Old Constrained Node Sid not getting deleted from MPLS forwarding table on changing SID
CSCvb34173	OSPF SR SID Conflict: SID is not installed for route via virtual-link
CSCvc12420	OSPF SRTE: CSTR path is not installed in some cases properly.
CSCvc19844	SID conflict: Even after an area is removed from topology, SID database does not remove the area.
CSCvc54359	SRTE: Single hope tunnel doesn't install any repair path.
CSCvc23238	SRTE: when i/f address is removed, traceback is seen and adj-sids not destroyed.
CSCvc54211	Tunnel & repair path continuously flapping on disabling SR on next node from head-end.
CSCvb96706	Client auth and enroll to subca fails
CSCvc33707	crash after multiple renew
CSCvd58884	During PKI enrollment, Cisco router rejects CA/RA reply containing HTTP 500 "Internal Server Error"
CSCvb73018	PKI: Cannot import RSA SubCA signed by ECDSA
CSCva31708	SR:RSP2:Object download failure(EOS object)error seen randomly
CSCvb44207	CTS/SGT across GRE p2p tunnel broken when doing inline tagging
CSCvc26599	ASR crashes when attempting SRTP/TLS call
CSCvb48683	Evaluation of all for Openssl September 2016

Related Documentation

For information about the Cisco CSR 1000v Series and associated services, see: Documentation Roadmap for Cisco CSR 1000v Series, Cisco IOS XE 16.