# Release Notes for Cisco IOS XE Catalyst SD-WAN Devices, Cisco IOS XE Catalyst SD-WAN Release Bengaluru 17.4.x

**First Published:** 2020-09-30

**Last Modified:** 2025-04-02

# Release Notes for Cisco IOS XE Catalyst SD-WAN Devices, Cisco IOS XE Catalyst SD-WAN Release Bengaluru 17.4.x

**Note** To achieve simplification and consistency, the Cisco SD-WAN solution has been rebranded as Cisco Catalyst SD-WAN. In addition, from Cisco IOS XE SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Release 20.12.1, the following component changes are applicable: **Cisco vManage** to **Cisco Catalyst SD-WAN Manager**, **Cisco vAnalytics** to **Cisco Catalyst SD-WAN Analytics**, **Cisco vBond** to **Cisco Catalyst SD-WAN Validator**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

These release notes accompany the Cisco IOS XE Catalyst SD-WAN Release Bengaluru 17.4.x, which provides Cisco SD-WAN capabilities. They include release-specific information for Cisco Catalyst SD-WAN Controllers, Cisco Catalyst SD-WAN Validators, Cisco SD-WAN Manager, as applicable to Cisco IOS XE Catalyst SD-WAN devices.

For release information about Cisco vEdge Devices, refer to Release Notes for Cisco vEdge Devices, Cisco SD-WAN Release 20.4.x.

## What's New for Cisco IOS XE Catalyst SD-WAN Release Bengaluru 17.4.x

This section applies to Cisco IOS XE Catalyst SD-WAN devices.

Cisco is constantly enhancing the SD-WAN solution with every release and we try and keep the content in line with the latest enhancements. The following table lists new and modified features we documented in the Configuration, Command Reference, and Hardware Installation guides. For information on additional features and fixes that were committed to the SD-WAN solution, see the *Resolved and Open Bugs* section in the Release Notes.

*Table 1: Cisco IOS XE Catalyst SD-WAN Release 17.4.1a*

| Feature | Description |
|---|---|
| **Cisco SD-WAN Getting Started** | |
| Support for Deploying Cisco Catalyst 8000V Instances for Supported Cloud Services Provider Platforms | Starting from this release, Cisco Catalyst 8000V instances can be deployed on Cloud Services Provider portals such as Google Cloud Platform, Microsoft Azure and Amazon Web Services. |
| Support for Managing Root CA Certificates in Cisco SD-WAN Manager | This feature enables you to add and manage root certificate authority (CA) certificates. |
| Support for Subject Alternative Name (SAN) | This feature enables you to configure subject altenative name (SAN) DNS Names or uniform resource identifiers (URIs). It enables multiple host names and URIs to use the same SSL certificate. |
| Upgrade the Software of Cisco ISR1100 Series Integrated Services Routers to Cisco IOS XE | This release introduces Cisco IOS XE SD-WAN support for Cisco ISR1100 Series Integrated Services Routers (Cisco ISR1100-4G, Cisco ISR1100-6G, and Cisco ISR1100-4GLTE). These devices can use either Cisco vEdge software or Cisco IOS XE SD-WAN. You can upgrade these routers from Cisco vEdge software to Cisco IOS XE SD-WAN, or vice-versa. |
| One Touch Provisioning: Onboard Cisco IOS XE SD-WAN Devices Using Generic Bootstrap Configuration | You can generate a generic bootstrap configuration on Cisco vManage and use this configuration to onboard multiple Cisco IOS XE SD-WAN devices. When you boot a device with the generic bootstrap configuration, the device is listed on Cisco vManage as an unclaimed WAN edge device. To complete the onboarding, claim the device on Cisco vManage and attach a device template that configures the system IP address and site ID. |
| **Systems and Interfaces** | |
| Type 6 Passwords on Cisco IOS XE SD-WAN Routers | This feature allows you to use type 6 passwords that use secure reversible encryption. This encryption provides enhanced security by using more secure algorithms to encrypt your passwords. These passwords are supported for the templates detailed in . |
| Configure a Cellular Gateway | This feature provides templates for configuring a supported cellular gateway as an IP pass-through device.<br>This release supports the Cisco Cellular Gateway CG418-E. |
| Cisco SD-WAN Multitenancy | With Cisco SD-WAN multitenancy, a service provider can manage multiple customers, called tenants, from Cisco vManage. In a multitenant Cisco SD-WAN deployment, tenants share Cisco vManage instances, Cisco vBond Orchestrators and Cisco vSmart Controllers. Tenant data is logically isolated on these shared resources. |

| Feature | Description |
|---|---|
| Qualified Commands for Cisco IOS XE Release 17.4.1a | Starting Cisco IOS XE Catalyst SD-WAN Release 17.4.1a, you can use additional commands in CLI Add-on feature templates. |
| Jumbo Frames Support | Jumbo Frames are supported for 1 GE interfaces on Cisco IOS XE SD-WAN devices. Starting Cisco IOS XE Catalyst SD-WAN Release 17.4.1a, the MTU can range from 576 through 9216 bytes on these 1 GE interfaces. |
| **Routing** | |
| Ability to Match and Set Communities during BGP to OMP Redistribution | This feature enhances the implementation of match and set clauses for redistribution from BGP to OMP and vice versa on Cisco IOS XE SD-WAN devices. You can redistribute the routes from a BGP into an OMP routing process, using the `redistribute` command in router configuration mode. The `route-maps` are defined locally on each device to manipulate communities. The following commands are updated:<br>`route-map`<br>`advertise bgp route-map bgp-to-omp`<br>`redistribute omp route-map omp-to-bgp` |
| **Policies** | |
| Policy Matching with ICMP Message | This feature provides support for a new match condition that you can use to specify a list of ICMP messages for centralized data policies, localized data policies, and Application-Aware Routing policies.<br>For information on matching ICMP messages in a centralized data policy, see Match Parameters - VPN List.<br>For information on matching ICMP messages in a localized data policy, see Match Parameters.<br>For information on matching ICMP messages in an Application-Aware Routing policy, see Structural Components of Policy Configuration for Application-Aware Routing. |
| Traffic Redirection to SIG Using Data Policy | With this feature, while creating a data policy, you can define an application list along with other match criteria and redirect the application traffic to a Secure Internet Gateway (SIG). |
| Enhanced Policy Based Routing for Cisco SD-WAN | This release extends Enhanced Policy Based Routing (ePBR) to Cisco SD-WAN. ePBR is a protocol-independent traffic-steering mechanism that routes traffic based on flexible policies for traffic flows. You can create ePBR policies using CLI add-on templates in Cisco vManage. |
| Per-class Application-Aware Routing | This feature enahances the capabilities of directing traffic to next-hop addresses based on the SLA definitions. These SLA definitions along with the policy to match and classify traffic types can be used to direct traffic over specific Cisco SD-WAN tunnels. The SLA definition comprises of values of loss, latency and jitter, which are measured using the BFD channel that exists between two TLOCs. |

| Feature | Description |
|---|---|
| FNF Support for IPv6 and Cache Size Modification | This feature enables export of packet to external collector over IPv6 transport on Cisco IOS XE SD-WAN devices and provides the visibility of IPv6 network traffic. If you want to monitor IPv4 and IPv6 traffic together, this feature enables you to modify the cache size on the data plane. Cisco Flexible NetFlow (FNF) is a technology that provides customized visibility into network traffic. In Cisco SD-WAN, FNF enables exporting data to Cisco vManage which makes it easy for the customers to monitor and improve their network. |
| **Security** | |
| Support for Rule Sets | This feature allows you to create sets of rules called rule sets. Rule sets are a method to create multiple rules that have the same intent. You can also re-use rule sets between security policies. |
| Configure Port-Scanning Detection Using a CLI Template | This feature lets you configure port-scanning detection and apply a severity level (low, medium, or high) for identifying and classifying potential attacks using a CLI template. |
| IPSEC/GRE Tunnel Routing and Load-Balancing Using ECMP | This feature allows you to use the SIG template to steer application traffic to Cisco Umbrella or a Third party SIG Provider. The application traffic is steered to a SIG based on a defined data policy and other match criteria.<br>This feature also allows you to configure weights for multiple GRE/IPSEC tunnels for distribution of traffic over multiple tunnels. Equal-cost multi-path (ECMP) routing and load balancing is supported on multiple GRE/IPSEC tunnels. |
| **TCP Optimization** | |
| Support for Multiple, External AppQoE Service Nodes | This feature allows you to configure multiple AppQoE service nodes that are external to the intercepting edge routers or AppQoE service controllers. It extends AppQoE support to edge routers in which AppQoE can't run as an integrated service node. This feature also allows AppQoE to scale, where integrated AppQoE has limitations on the throughput and number of connections. The ability to configure multiple AppQoE service nodes help meet the scale and throughput requirements of large enterprise sites, such as data centers. |
| **Cloud OnRamp** | |
| Azure Government Cloud Support for Cisco IOS XE SD-WAN Devices | This feature allows you to configure the Cisco Catalyst 8000V devices on Microsoft Azure Government Cloud. With these cloud devices now supported on Microsoft Azure Government Cloud, Government Cloud customers can use the same advanced routing and security benefits, which are already available on Azure public cloud. |
| AWS Government Cloud Support for Cisco IOS XE SD-WAN Devices | Starting from this release, Cisco Catalyst 8000V devices are supported on AWS Government Cloud. |

| Feature | Description |
|---|---|
| Application Feedback Metrics for Office 365 Best Path Selection on Cisco IOS XE SD-WAN Devices | This feature adds new metrics as inputs to the best-path selection algorithm for Office 365 traffic. The new inputs include best-path metrics from Microsoft Cloud Services. The feature also provides a new page for viewing detailed logs of the input data used by the best path algorithm. |
| Automated Integration of Azure Virtual WAN and Cisco SD-WAN | This feature enhances Cloud OnRamp integration with Microsoft Azure by allowing Cisco Catalyst 8000V Edge Software (Cisco Catalyst 8000V) to be deployed inside the Azure Virtual WAN Hub instead of deploying it in transit VNets. It also automates the Cisco SD-WAN fabric connection to Azure Virtual WAN Hub through Cisco Catalyst 8000V. The connectivity between inter-region Azure Virtual WAN Hubs is also supported.<br><br>In addition, you can convert the Azure virtual WAN hubs created using Cisco vManage into secured hubs by deploying Azure firewall inside them. However, secured virtual hubs can only be configured using the Microsoft Azure portal. |
| Integration of Cisco SD-WAN and Azure Virtual WAN Hub Using Azure Portal | As part of the integration of Cisco SD-WAN with Azure Virtual WAN, you can also use the Azure portal to upload bootstrap configuration files for Cisco Catalyst 8000V instances. These instances can then be used to create a virtual WAN hub using the Azure portal. |
| Support for Cisco Cloud Services Platform, CSP-5456 (Cloud onRamp for Colocation) | Starting from this release, Cisco CSP-5456 is supported on the Cloud onRamp for Colocation solution. The CSP-5456 offers a higher capacity of 56 cores, which maximizes the placement of VNFs in service chains. |
| Support for Cisco Catalyst 8000V Devices (Cloud onRamp for Colocation) | Starting from this release, Cisco Catalyst 8000V devices are now supported as a validated VNF in the Cloud onRamp for Colocation solution. |
| Onboarding CSP Device with Day-0 Configuration Using USB Drive (Cloud onRamp for Colocation) | This feature enables you to onboard CSP devices by loading the Day-0 configuration file to a USB drive. Use this onboarding option when you can't access the Internet to reach the Plug-and-Play Connect server. |
| **Monitor and Maintain** | |
| Ethernet Connectivity Fault Management Support on Cisco IOS XE SD-WAN Devices | Starting from this release Cisco SD-WAN supports the Ethernet Connectivity Fault Management functionality on Cisco IOS XE SD-WAN devices. This feature helps to monitor the Carrier Ethernet Network links. |

| Feature | Description |
|---|---|
| Binary Trace for Cisco SD-WAN Daemons | Binary trace enhances the troubleshooting of Cisco SD-WAN daemons. Binary trace logs messages from the daemons in a binary format. Messages are logged faster in the binary format, improving the logging performance, and use lesser storage space than in the ASCII format. The binary trace CLI allows you to set the debug levels for additional process modules compared to the **debug** command.<br>From Cisco IOS XE Release 17.4.1a, binary trace is supported for the following Cisco SD-WAN daemons:<br>• fpmd<br>• ftm<br>• ompd<br>• vdaemon<br>• cfgmgr |
| **Cisco SD-WAN Command Reference Guide** | |
| Crypto Utilization in Show Platform Resources Command | This feature adds information about crypto utilization to the **show platform resources** command on the supported routers. |
| **High Availability Configuration Guide** | |
| Disaster Recovery for a 6 Node Cisco vManage Cluster | This feature provides validated support for disaster recovery for a 6 node Cisco vManage cluster. |

# New and Enhanced Hardware Features

## New Features

- Support for UCS-E module—This feature adds a UCS-E template in Cisco vManage for configuring Cisco Unified Computing System (UCS) E-Series servers. For related information, see Getting Started Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine and Configuring Devices using vManage.

**Note** Currently, backplane interfaces are not supported for UCS-E module. Only external connectivity is supported.

- Support for Cisco IR1101 Integrated Services Router Rugged—Cisco SD-WAN capability can now be enabled onCisco IR1101 Integrated Services Router Rugged. The following notes apply to this support:
  - Controller devices (Cisco vBond orchestrators, Cisco vManage NMSs, and Cisco vSmart controllers) must run Cisco SD-WAN Release 19.2 or later.
  - The default topology is full mesh, but the hub and spoke topology is often used for IoT applications.

- Cisco SD-WAN support on the Cisco IR1101 Integrated Services Router Rugged requires Cisco IOS-XE Release 16.12.
- The Cisco IR1101 Integrated Services Router Rugged has four fixed switch-ports. Make sure to select the correct template.
- The CLI template is not currently supported.
- Starting from Cisco IOS-XE Release 16.12.1, Cisco IR1101 Integrated Services Router Rugged has dual LTE support with LTE extension module.
- We recommend using up to 50 BFD sessions for scaling.

## Important Notes, Known Behavior, and Workaround

- From Cisco SD-WAN Release 20.4.1.1, Microsoft Azure environment is supported for deploying Cisco SD-WAN controllers (Cisco vBond orchestrator, Cisco vSmart controller, and Cisco vManage). The support is limited to Cisco SD-WAN cloud-based deployments only.
- Cisco IOS XE Catalyst SD-WAN devices with the SFP-10G-SR module do not support online insertion and removal (OIR) of this module.
- Cisco vManage Release 20.3.1 implements a hardened security posture to comply with FedRamp guidelines. As a result, your vAnalytics login credentials that are stored locally get erased on upgrading the software, and you cannot access the vAnalytics service directly through Cisco SD-WAN Manager. In this case, log in to vAnalytics using this URL: https://analytics.viptela.com. If you can't find your vAnalytics login credentials, open a case with Cisco TAC support.

## Cisco SD-WAN Manager Upgrade Paths

For information about Cisco SD-WAN Manager upgrade procedure, see Upgrade Cisco vManage Cluster.

| Starting Cisco SD-WAN Manager Version | Destination Version | | | |
|---|---|---|---|---|
| | 19.2.x | 20.1.x | 20.3.x | 20.4.x |
| 18.x/19.2.x | Direct Upgrade | Direct Upgrade | Check disk space*<br>• If the disk space is more than 2GB: Direct Upgrade<br>• If the disk space is less than 2GB: Step upgrade through 20.1<br>• If you are upgrading to 20.3.5, the available disk space should be at least 2.5 GB.<br><br>For cluster upgrade procedure**: **request nms configuration-db upgrade**<br><br>**Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later. | Step upgrade through 20.3 |

| Starting Cisco SD-WAN Manager Version | Destination Version | | | |
|---|---|---|---|---|
| | 19.2.x | 20.1.x | 20.3.x | 20.4.x |
| 20.1.x | Not Supported | Direct Upgrade | Direct Upgrade<br>For cluster upgrade procedure**: **request nms configuration-db upgrade**<br>**Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later. | Direct Upgrade<br>For cluster upgrade procedure**: **request nms configuration-db upgrade**<br>**Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later. |
| 20.3.x | Not Supported | Not Supported | Direct Upgrade | Direct Upgrade |
| 20.4.x | Not Supported | Not Supported | Not Supported | Direct Upgrade |

*To check the free disk space using CLI,

1. Use the vshell command to switch to vshell
2. In vshell, use the df -kh | grep boot command

**Cluster upgrade must be performed using CLI

- Use the following command to upgrade the configuration database . This must be done on one node only in the cluster:

```
request nms configuration-db upgrade
```

**Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.

- Enter login credentials, if prompted. Login credentials are prompted if all vManage server establish control connection with each other. After a successful upgrade, all configuration-db services are UP across the cluster and the application-server is started.

# Resolved and Open 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.

## Bugs for Cisco IOS XE Release 17.4.2

This section details all fixed and open bugs for this release. These bugs are available in the Cisco Bug Search Tool

### Resolved Bugs for Cisco IOS XE Release 17.4.2

| Bug ID | Description |
|---|---|
| CSCvw88098 | Cisco IOS XE SD-WAN device crashes while running web traffic testing with security features enabled |
| CSCvw93490 | CSR1000v crashing frequently with Critical software exception error. |
| CSCvx22995 | On-demand tunnel is not setup with AAR SLA class and CXP feature enabled |
| CSCvx58099 | C8500-12X4QC does not send logs to Cisco vManage when harddisk is not installed |
| CSCvx94798 | SDWAN BFD is not re-establishing after network flap |
| CSCvv92064 | App-aware policy need to be honored when queuing is not set by localized policy |
| CSCvw11607 | Crash in DSP causing an mcpcc-lc-ms core file |
| CSCvw68171 | Duplicate Bytes & Packet when Q in Q is configured |
| CSCvw91956 | Router reload due sdwan nbar init process |
| CSCvx82128 | Cisco IOS XE SD-WAN device object-group is not in sync between IOS and Confd. |
| CSCvs08693 | VPN label is changing upon vEdge reboot |
| CSCvx61152 | vSmarts crashing due to OOM after upgrade to 20.4.1.1 |
| CSCvy10840 | Cisco vManage available entropy exhaustion on some setup |

### Open Bugs for Cisco SD-WAN Release 17.4.2

| Bug ID | Description |
|---|---|
| CSCvy44563 | cpp-mcplo-ucode crash due to stuck thread with extranet route leaking between vpns |
| CSCvw84883 | DDNS feature triggers crash on 16.X/17.X releases due to memory corruption |

## Bugs for Cisco SD-WAN Controller Release 20.4.1.2

This section details all fixed and open bugs for this release. These are available in the Cisco Bug Search Tool through the Resolved Bug Search.

### Resolved Bugs for Cisco SD-WAN Controller Release 20.4.1.2

| Bug ID | Description |
|---|---|
| CSCvw50857 | Frequent crashes/kernel panics on vEdge 100 models |
| CSCvx49472 | Policy Template push failure from Cisco vManage 20.4.1.1 to 17.2 |
| CSCvx52311 | Order of DNS entries fails with <bad-element>dns-server-list</bad-element> |
| CSCvx57151 | Update button stops working after adding DHCP option |
| CSCvx60393 | Directory ownership changed after reload/upgrade |
| CSCvx66814 | Container logs seen growing unbounded without log rotation |
| CSCvx80910 | Devices goes "Out-of-sync" and can't re-push template with security policy and fail with "bad-cli" |

## Bugs for Cisco IOS XE Release 17.4.1b

This section details all fixed and open bugs for this release. These bugs are available in the Cisco Bug Search Tool

### Resolved Bugs for Cisco IOS XE Release 17.4.1b

| Bug ID | Description |
|---|---|
| CSCvw17655 | vEdge DPI for MS Teams does not work well |
| CSCvw24872 | vmanage DHCP option 150 not allow multiple ip address |
| CSCvw41778 | Fragmented packets may be dropped inbound on tunnel of cEdge with service-side NAT configuration |
| CSCvw49402 | PPPoE config on Gig interface failed , vManage not handling ip mtu and mtu correctly |
| CSCvw76649 | vManage 6 Node CLuster on Azure takes 2 mins to login to vManage UI. |
| CSCvw86437 | Slowness in viewing ty policy , list & editing security policy. |
| CSCvw86827 | Mapping for AWS TGW does not start when Azure vWAN mapping exists |

| Bug ID | Description |
|---|---|
| CSCvw91717 | after upgrading to from 17.3.2 to 17.4.1, the device loses control connections |
| CSCvw97278 | 20.4 policy name restrictions may break existing templates on upgrade |
| CSCvx09069 | Increase process wait timeout for configdb upgrade |
| CSCvx16493 | cEdge stuck in INIT state with vSmart |
| CSCvx26834 | vManage misconfigures cEdge ebgp-multihop which causes BGP BFD down |
| CSCvv84956 | 20.4 template push on ISR4451 failing with VRRP config |
| CSCvw03627 | vManage template/policy push performance optimizations needed |
| CSCvw23740 | In a cluster, an App server starting dependency should check a cluster, not just local service |
| CSCvw89415 | BFD for BGP doesn't work on cEdge ASR1k |
| CSCvx07652 | statsdb container crashes on 20.4 128GB azure vmanage |
| CSCvx23764 | Template deattach got stuck after upgrade to 20.4 IR |
| CSCvw88048 | Speed test initiated from ISR1k failed |

### Open Bugs for Cisco SD-WAN Release 17.4.1b

| Bug ID | Description |
|---|---|
| CSCvw36009 | vBond/vSmart Upgrade Failed and Rollback due to Upgrade confirm not received |
| CSCvx36668 | vManage admin tech failing intermittently |
| CSCvx38058 | vBond kernel panic seen on reload |

## Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.4.1a

This section details all fixed and open bugs for this release. These bugs are available in the Cisco Bug Search Tool

### Resolved Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.4.1a

| Bug ID | Description |
|---|---|
| CSCvq63465 | Drop cEdge requirement for dot1Q subinterface MTU to be 4 Bytes less than main interface |
| CSCvs75489 | New Password is asked even when the Template used a non default admin Password |
| CSCvt28539 | explicit acl needed for cellular intf for control connection bringup |
| CSCvt45700 | [17.2.1]:policy service path and tunnel path commands stop working after reload |

| Bug ID | Description |
|---|---|
| CSCvt50136 | ASR1k - all Platform : Observing IpFragErr for EMIX traffic with basic IPSEC config |
| CSCvt81979 | ASR IOS-XE SDWAN router bfd sessions not coming up if BGP routing is not providing a local next hop. |
| CSCvu46417 | ASR1k crash when doing a FIB lookup |
| CSCvu53340 | Template push is failing as vManage is trying to disable link recovery for cellular controller. |
| CSCvu72391 | Default route missing for second TLOC during script run, and control connection get stuck |
| CSCvu80611 | cpp_cp_svr_ledp crash seen during SIT Regression |
| CSCvv09538 | [SIT] Ramanos lost control and crashed after attaching device template |
| CSCvv14263 | Day 0 Config Bringup after Power OFF/ON \| C1121X-8PLTEP |
| CSCvv21398 | sdwan multicast cEdge rpf failure even with unicast route present in rib and omp |
| CSCvv29416 | CLI template push for banner login <> configuration fails on cedge |
| CSCvv40754 | Backward compatibility issue for model between vManage version 20.3 and device version 17.2 |
| CSCvv42381 | [DyT]: TTM not updating link routes and omp routes are not getting updated |
| CSCvv64271 | IOS-XE SD_WAN router crashed after upgrade to 17.3.1a |
| CSCvv67689 | cEdge data-policy breaks SRST media stream with default-action accept or accept in sequence |
| CSCvv73691 | PMTU Discovery may negotiate an incorrect MTU on XE SDWAN routers |
| CSCvv73826 | BFD sessions flap after multiple control connection flaps to the vSmart. - Polaris side commit |
| CSCvv75771 | XE SDWAN router crash due to system memory exhaustion caused by FTM memory growth |
| CSCvv87062 | SDWAN 17.2.1/17.4.1 - cEdge router may restart after pushing multiple traffic data policies together |
| CSCvv60179 | TSN: AAA Server Down issue using type 6 password |

### Open Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.4.1a

| Bug ID | Description |
|---|---|
| CSCvv21200 | SDWAN17.3- "NAT" Ping fails for packets originated from router - Reason packets drop "Ipv4NoRoute" |

| Bug ID | Description |
|---|---|
| CSCvv39559 | After enable FEC and FNF with 100K flow per seconds for 40mins, C8500 crashes |
| CSCvv50783 | IPSEC tunnels to AWS TGW failing when VPN tunnel doesn't allow all traffic |
| CSCvv58652 | O365 CoR-SaaS shows random losses |
| CSCvv58786 | Connected route is not imported into OMP database unless flap interface with C8KV platform |
| CSCvv69702 | 4451 : FTMD crash @ bfdmgr_session_get_from_record_index with traffic soak |
| CSCvw01038 | [cEdge/CSR1kv] IPv6 Underlay, IPv6 fragmented but packet size is smaller than MTU |
| CSCvw01238 | Enable AES encryption on cEdge and encrypt umbrella and zscaler secret/password |
| CSCvw02548 | tunnel interface remains up even when the physical interface not have IP address |
| CSCvw16091 | vEdge/cEdge - rekey timer expires, but tunnels stay up |
| CSCvw30618 | Not all OMP routes getting installed |
| CSCvw41778 | Fragmented packets may be dropped inbound on tunnel of cEdge with service-side NAT configuration |
| CSCvw46210 | Bfd session stuck in invalid state |
| CSCvw46258 | Intra-zone ZBFW policy does not apply on hardware level |
| CSCvw46753 | After reload cEdge cellular interfaces in shutdown state are brought up |
| CSCvw52661 | crash. seen during sh plat sof sdwan fo next-hop overlay id 0xf8000090 |
| CSCvw54383 | DPI flow telemetry generated by IOS-XE, for some flows tunnel identifiers are missing |
| CSCvw58543 | Traceroute from Service VPN to remote Service VPN not showing the correct Hops |
| CSCvw61731 | ASR-1K router is not programming correct next-hop for the destination prefix. |
| CSCvw62005 | cEdge: IP MTU and MTU misconfiguration |
| CSCvw63896 | Promethium: Box crashed at cpp_bfd_sdwan_stats_modify during longevity testing |
| CSCvw70262 | cEdge directly-connected routes missing from routing table |
| CSCvw72021 | nat pool config using sub-interfaces does not work after reload |
| CSCvw74035 | Broadcast packets dropped even with "ip network-broadcast" and "ip directed-broadcast" configured |

# Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Server Recommendations

For compatibility information and server recommendations, see Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Server Recommendations.

## Supported Devices

For device compatibility information, see Cisco SD-WAN Device Compatibility.

## Related Documentation

- Release Notes for Previous Releases
- Software Installation and Upgrade for Cisco IOS XE Routers
- Software Installation and Upgrade for vEdge Routers
- Field Notices
- Recommended Releases
- Security Advisories
- Cisco Bulletins

## Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2021 Cisco Systems, Inc. All rights reserved.