Release Notes for Cisco IOS XE SD-WAN Devices, Cisco IOS XE Release 17.5.x

First Published: 2021-03-22

Last Modified: 2022-11-02

Release Notes for Cisco IOS XE SD-WAN Devices, Cisco IOS XE Release 17.5.x

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

These release notes accompany the Cisco IOS XE Release 17.5.x, which provides Cisco SD-WAN capabilities. They include release-specific information for Cisco vSmart Controllers, Cisco vBond Orchestrators, Cisco vManage, as applicable to Cisco IOS XE SD-WAN devices.

For release information about Cisco vEdge Devices, refer to Release Notes for Cisco vEdge Devices, Cisco SD-WAN Release 20.5.x.

For release information about Cisco SD-WAN Controllers, refer to Release Notes for Cisco SD-WAN Controllers, Cisco SD-WAN Release 20.5.x

What's New for Cisco IOS XE Release 17.5.x

This section applies to Cisco IOS XE 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 Release 17.5.1

Feature	Description
Cisco SD-WAN Getting Started	

Feature	Description
Support for Deploying Cisco Catalyst 8000V Instances on Alibaba Cloud	Starting from this release, Cisco Catalyst 8000V instances can be deployed on Alibaba Cloud.
License Management Using Cisco vManage	Cisco SD-WAN operates together with Cisco Smart Software Manager (CSSM) to provide license management through Cisco vManage. Cisco vManage can show available DNA licenses, assign licenses to devices, and report license consumption to CSSM. Cisco vManage can show available DNA licenses, assign licenses to devices, and report license consumption to CSSM.
Cisco SD-WAN Support for the Cisco ASR 1006-X Platform with an RP3 Module	Starting from this release, Cisco SD-WAN supports the Cisco ASR 1006-X platform with a Cisco ASR 1000 Series Route Processor 3 module installed.
Systems and Interfaces	
Day 0 WAN Interface Automatic Bandwidth Detection	This feature enables a device to automatically determine the bandwidth for WAN interfaces in VPN0 during day 0 onboarding by performing a speed test using an iPerf3 server.
HTTP/HTTPS Proxy Server for Cisco vManage Communication with External Servers	Cisco vManage uses HTTP/HTTPS to access some web services and for some REST API calls. Beginning Cisco vManage Release 20.5.1, you can channel the HTTP/HTTPS communication through an HTTP/HTTPS proxy server.
Authorization and Accounting	This feature provides for the configuration of authorization, which authorizes commands that a user enters on a device before the commands can be executed, and accounting, which generates a record of commands that a user executes on a device.
Role-Based Access Control By Resource Group	This feature introduces role-based access control (RBAC) based on sites or resource groups. It is a method of authorizing system access for users based on a combination of user groups and resource groups. For large Cisco SD-WAN deployments across multiple geographical locations, this feature helps you to split the network administration among different regional administrators.
Retrieve Last Edited Configuration	This feature allows you to review the last edited configuration when a configuration push to the device fails. A copy of the last edited configuration is saved and can be retrieved to allow edits to the configuration before the next push.
Configure TCP MSS	This feature adds support for TCP MSS adjustment on Cisco IOS XE SD-WAN devices on both directions of the Cisco SD-WAN tunnel interface.

Feature	Description
Configure Clear Don’t Fragment Option	This feature provides the option to clear the Don't Fragment bit in the IPv4 packet header for packets being sent out on a Cisco SD-WAN tunnel . When you clear the Don't Fragment configuration, packets larger than the interface MTU are fragmented before being sent.
Migrate Single-Tenant Cisco SD-WAN Overlay to Multitenant Cisco SD-WAN Deployment	You can migrate a single-tenant Cisco SD-WAN overlay to a multitenant deployment using a sequence of Cisco vManage API calls.
Support for Draft Mode in Device Template	This feature allows you to save the device template configuration changes in Cisco vManage, and then apply these configuration changes to multiple Cisco IOS XE SD-WAN devices later. The ability to save configuration changes simplifies generating larger device template configurations and applying them to devices.
Enhancement to Jumbo Frames Support	Jumbo Frames support is extended for 10 GE and 100 GE interfaces on Cisco IOS XE SD-WAN devices. Starting Cisco IOS XE Release 17.5.x, the MTU can range from 576 through 9216 bytes on these 10 GE and 100 GE interfaces.
NAT Configuration Guide	
Advertise NAT Routes Through OMP	This feature allows you to advertise NAT routes through OMP to the branch routers. You can configure this feature only through Cisco vManage device CLI template.
NAT Pool Support for Static NAT	This feature enhances the service-side NAT functionality to include the ability to configure NAT pool and centralized data policy for static NAT mapping. If configured, the static NAT can only be applied if the data policy match conditions are met.
Routing	
Increased OMP Path Limit for Cisco vSmart Controllers	With this feature, the number of paths that can be exchanged between Cisco vSmart Controllers is increased to 128.
Dynamic Rendezvous Point (RP) Selection by a PIM BSR	This feature adds support for automatic selection of an RP candidate using a PIM BSR in an IPv4 multicast overlay. There is no single point of failure because every site has a local RP. A Cisco IOS XE SD-WAN device is selected as the RP, not a service-side device.
Redistribution of Replicated BGP Routes into OSPF, EIGRP Protocols	This feature allows you to leak (or replicate) BGP routes between the global VRF and service VPNs, and redistribute the leaked BGP routes. The redistribution of the leaked routes to the EIGRP and OSPF protocols occurs after replicating the BGP routes into the corresponding VRF.
Policies	

Feature	Description
Ability to Match and Set Communities	This feature lets you match and set communities using a control policy. Control policies are defined and applied on Cisco SD-WAN devices to manipulate the communities. With this feature, you can match and assign single or multiple BGP community tags to your prefixes based on which routing policies can be manipulated.
Next Hop Action Enhancement in Data Policies	This feature enhances match action conditions to achieve parity with all the features configured on Cisco IOS XE SD-WAN devices while creating a centralized data policy. When you are setting up next-hop-loose action, this feature helps to redirect application traffic to an available route when next-hop address is not available.
Best of the Worst Tunnel Selection	This feature introduces a new policy action **fallback-to-best-path** to pick the best path or color out of the available colors. When the data traffic does not meet any of the SLA class requirements, this feature allows you to select the best tunnel path criteria sequence using the option **Fallback Best Tunnel** option under each SLA class to avoid packet loss.
Log Packets Dropped by Implicit ACL	You can now enable or disable logging of dropped packets in case of a link failure. You can also configure how often the packet flows are logged.
Security	
Geolocation-Based Firewall Rules for Allowing or Denying Network Traffic Based on Geolocation	This feature enables you to configure firewall rules for allowing or denying network traffic based on the source and destination location instead of IP addresses. This feature adds a new object group, geo, where you can specify countries and continents as objects in an Access Control List (ACL). An object group ACL simplifies policy creation in large networks, especially if the ACL changes frequently. New object-group and geo commands were added.
Support for Zscaler Automatic Provisioning	This feature automates the provisioning of tunnels from Cisco SD-WAN routers to Zscaler. Using your Zscaler partner API credentials, you can automatically provisions tunnels to Zscaler Internet Access (ZIA) Public Service Edges. You can choose **Zscaler** in the Cisco Security Internet Gateway (SIG) and SIG credentials feature templates to automate tunnel provisioning.
SGT Propagation using SXP and SGACL Enforcement	With this feature, Cisco IOS XE SD-WAN devices can exchange SGT over the overlay network using SXP. Use SXP when your hardware does not support the inline propagation of SGTs. This feature also extends support for SGACL enforcement on Cisco IOS XE SD-WAN devices by configuring SGACL policies.
Configure Unified Threat Defense Resource Profiles	This feature lets you customize the amount of resources that Unified Threat Defense features use on a router. You can use larger resource profiles to process packets simultaneously. Simultaneously processing packets reduces the latency that security features can introduce to the packet processing of the device.
High Availability	

Feature	Description
Disaster Recovery for a Single Node Cisco vManage Cluster	This feature provides support for disaster recovery for a Cisco vManage deployment with a single primary node.
Cloud OnRamp	
Load Balancing Across Multiple Interfaces	This feature adds the ability to balance traffic for cloud applications across multiple direct internet access (DIA) interfaces.
Support for Pay As You Go License for Cisco Catalyst 8000V Edge Software Instances	Added support for using Cisco Catalyst 8000V Edge Software instances with pay as you go (PAYG) licenses when creating a new cloud gateway in Amazon Web Services (AWS), in addition to the previously supported bring your own license (BYOL) model.
RMA Support for Cisco CSP Devices (Cloud onRamp for Colocation)	This feature allows you to replace a faulty CSP device by creating backup copies of the device, and then restoring the replacement device to a state it was in before the replacement. The VMs running in HA mode operate uninterrupted with continuous flow of traffic during device replacement.
Clone Service Groups in Cisco vManage (Cloud onRamp for Colocation)	This feature allows you to create copies of service groups for different RBAC users, without having to enter the same configuration information multiple times. By cloning a service group, you can easily create service chains by leveraging the stored service chain templates.
Colocation Multitenancy Using Role-Based Access Control (Cloud onRamp for Colocation)	This feature enables a service provider to manage multiple colocation clusters and share these clusters across tenants by using multiple colocation groups. In a multitenant setup, service providers don't need to deploy a unique colocation cluster for each tenant. Instead, the hardware resources of a colocation cluster are shared across multiple tenants. With multitenancy, service providers ensure that tenants view only their data by restricting access based on roles of individual tenant users.
Software-Defined Interconnects via Megaport	You can deploy a Cisco Catalyst 8000v Edge Software (Cisco Catalyst 8000V) instance as the interconnect gateway in the Megaport fabric and connect an SD-WAN branch location to the interconnect gateway. From the interconnect gateway, you can create software-defined interconnects to an AWS cloud onramp or another interconnect gateway in the Megaport fabric.
Service Area Mapping	This feature enables you to specify the service area that your Microsoft 365 application belongs to.
Integration of Cisco SD-WAN Branches with AWS using Cisco IOS XE SD-WAN Devices and the AWS TGW Connect	This release enables the use of the AWS TGW Connect feature to connect a cloud gateway to an AWS Transit Gateway. This GRE based connection type offers improved bandwidth, scaling, and security compared to the use of IPSec VPN tunnel connections.

Feature	Description
AWS Branch Connect Solution	This feature leverages the AWS Transit Gateway support to connect branch devices to the cloud. The branch devices connect to transit gateway using an IPSec tunnel-based secure channel to access the applications hosted in the cloud. This feature supports scenarios where Cisco vManage instantiates, manages, and controls the AWS Transit Gateway.
Cisco SD-WAN Cloud Gateway in Google Cloud	The feature allows branch sites to access workloads running in the Google Cloud. It also allows branch sites to send and receive traffic across different regions and sites through Google Global Network. As part of the solution, cloud gateways are instantiated in different regions. Cloud gateways consist of a pair of Cisco Catalyst 8000V instances with their interfaces anchored in three different VPCs. This feature supports site-to-cloud and site-to-site connectivity.
AppQoE	
Support for Additional Platforms as Controllers for AppQoE Service Nodes	This release extends the service controller role to additional device models—C8500L-8S4X and ASR1006-X.
Support for Automated MTU Setting for Tunnel Adjacency	This feature enables a programmatic setting of the maximum transmission unit (MTU) size to 1500 for the network connecting the service controllers and service nodes. This automation prevents broken communication due to packet fragmentation that can bring down the throughput requirements.
Traffic Optimization with DRE	This release extends DRE to Cisco SD-WAN. DRE is a compression technology that reduces the size of data transmitted over the WAN and enables more effective utilization of the WAN.
Application Performance Monitor	This feature provides an express method for configuring an intent-based performance monitor with the help of predefined monitoring profiles. Configure this feature using the CLI Add-on feature template in Cisco vManage.
Monitor and Maintain	
View Loss Percentage, Latency, Jitter, and Octet Information for Tunnels	This feature provides a single chart option in Cisco vManage for viewing tunnel information, such as packet loss, latency, jitter, and octets.
Enhanced Security Monitoring on Cisco SD-WAN Devices	This feature enhances the monitoring of Unified Threat Defense (UTD) features on Cisco SD-WAN devices. The feature allows you to view the CPU, memory, and traffic usage on your device. You can also view the health of individual UTD features.
Optimization of Alarms	This feature optimises the alarms on Cisco vManage by automatically suppressing redundant alarms. This allows you to easily identify the component that is causing issues. You can view these alarms in **Monitor** > **Alarms**.

Feature	Description
SNMP	
Configure SNMP with Encrypted Strings Using CLI Templates	This feature enables you to configure SNMP using a CLI template or a CLI add-on feature template. You can also encrypt the supported variables in the CLI configuration.
Plug and Play	
Monitor and Troubleshoot Device PnP Onboarding using WebUI	You can now monitor and troubleshoot your Day-0 device onboarding using WebUI through PnP onboarding. If the automated PnP onboarding fails, you can manually onboard your device.
Admin-Tech Enhancement	With this feature, the admin tech file now includes the **`show platform hardware qfp active classification feature-manager statistics`** command, which displays CFM error statistics.

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 on Cisco IR1101 Integrated Services Router Rugged. The following notes apply to this support:
  - Controller devices (Cisco vBond orchestrators, Cisco vManage, 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 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 vManage. 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.
- Starting from Cisco IOS XE Release 17.5.1a, the **`table`** keyword is added to all show sdwan commands for which the output needs to be displayed in a tabular format. Using **`| tab`** is restricted for all Cisco SD-WAN commands starting from Cisco IOS XE SD-WAN Release 16.11.x.

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 17.5.1a

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

Open Bugs for Cisco IOS XE Release 17.5.1a

Bug ID	Description
CSCvx94798	SDWAN BFD is not re-establishing after network flap
CSCvx26065	1006-X: Box rebooted due to ucode crash, with 2M CFLOW and 8K BFD sessions
CSCvy00325	ISR1k 17.5: ConfD crashed due to high memory utilization
CSCvw85989	SunRPC ALG resets connection with ZBFW inspection enabled
CSCvx18561	BFD sessions flapping with pairwise rekey in latest 17.3,17.4,17.5,17.6
CSCvx57615	ZBFW blocking ACK packets for applications using cloudexpress SaaS set to use a Gateway with synsent
CSCvx68704	Cisco IOS XE SD-WAN device Packet-Duplication is duplicating traffic on same transport

Bug ID	Description
CSCvx72305	XE-SDWAN device would keep invalid IPv6 address in the tunnel to Cisco vManage and can not recover
CSCvx86804	c8500 / 17.3.2 / 17.4.1a / Cisco vManage is not pushing auto negotiation for 10Gig Interfaces on Cisco IOS XE SD-WAN device
CSCvx89481	Ping and Traceroute failing when initiated from Cisco vManage
CSCvx90820	AppQoE DRE Original and Optimized Data shown in Monitoring Graphs and device reflects discrepancy
CSCvx94798	SDWAN BFD is not re-establishing after network flap
CSCvy01438	Remote TLOC not getting installed

Controller Compatibility Matrix and Server Recommendations

For compatibility information and server recommendations, see Cisco SD-WAN Controller 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

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.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

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)