Release Notes for Cisco IOS XE Catalyst SD-WAN Devices, Cisco IOS XE Catalyst SD-WAN Release 17.16.x

First Published: 2024-12-23

Read Me First

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.

Related References

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

User Documentation

- User Documentation for Cisco IOS XE Catalyst SD-WAN Release 17
- User Documentation for Cisco SD-WAN Release 20

Communications, Services, and Additional Information

- Sign up for Cisco email newsletters and other communications at: Cisco Profile Manager.
- For information on the latest technical, advanced, and remote services to increase the operational reliability of your network visit Cisco Services.
- To browse and discover secure, validated enterprise-class apps, products, solutions, and services, visit Cisco Devnet.
- To obtain general networking, training, and certification titles from Cisco Press Publishers, visit Cisco Press.

- To find warranty information for a specific product or product family, visit Cisco Warranty Finder.
- To view open and resolved bugs for a release, access the Cisco Bug Search Tool.
- To submit a service request, visit Cisco Support.

Documentation Feedback

To provide feedback about Cisco technical documentation use the feedback form available in the right pane of every online document.

Release Notes for Cisco IOS XE Catalyst SD-WAN Devices, Cisco IOS XE Catalyst SD-WAN Release 17.16.1a

These release notes accompany the Cisco IOS XE Catalyst SD-WAN Release 17.16.1a, which provides Cisco Catalyst SD-WAN capabilities. They include release-specific information for Cisco Catalyst SD-WAN Controllers, Cisco Catalyst SD-WAN Validators, Cisco Catalyst SD-WAN Manager, as applicable to Cisco IOS XE Catalyst SD-WAN devices.

Related Releases

For release information about Cisco Catalyst SD-WAN Control Components, refer to Release Notes for Cisco SD-WAN Control Components, Cisco Catalyst SD-WAN Control Components Release 20.16.x

What's New for Cisco IOS XE Catalyst SD-WAN Release 17.16.1a

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

Cisco is constantly enhancing the Cisco Catalyst 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 Cisco Catalyst SD-WAN solution, see the *Resolved and Open Bugs* section in the Release Notes.

Table 1: Cisco IOS XE Catalyst SD-WAN Release 17.16.1a

Feature	Description
Cisco Catalyst SD-WAN Getting Started	
Expired Certificate Indication and Quarantine	Cisco SD-WAN Manager indicates when devices or Cisco Catalyst SD-WAN Control Components have expired certificates. Additionally, you can quarantine all edge devices that have expired certificates. Quarantine places devices into the staging status. Quarantined devices keep their control connections to Cisco Catalyst SD-WAN Control Components, but do not handle data plane traffic.
Cisco Catalyst SD-WAN Systems and Interfaces	
Cellular Module Support for Cisco Catalyst Rugged Series Routers	Support for cellular modules on Cisco Cisco Catalyst IR1101, IR1800 and IR18340 Rugged Series Routers.

Feature	Description
Cellular Network Slicing	This feature allows multiple networks to exist on the same physical network to optimize the network for different traffic types.
Cisco ThousandEyes Support for Additional Devices in Cisco ISR 1100 Series Routers	Extended Support of Cisco ThousandEyes Enterprise agent to additional devices on Cisco ISR 1100 Series Routers.
Simplified Workflow for Onboarding Cisco ThousandEyes Agent and Configuring Tests	This feature provides a simplified workflow to easily onboard Cisco ThousandEyes agent and configure tests using Cisco SD-WAN Manager.
Configure RADIUS and TACACS Servers to Receive Authentication Requests Over Management VPN 512	This feature provides increased security by allowing you to configure tenants to send and receive AAA traffic over WAN transport VPN 0 or management VPN 512. For more information, see Configure Remote AAA.
Support for Multitenancy Providers to View Tenant's Alarms and Events	This feature allows providers to view tenant alarms and events. Multitenancy providers can enable or disable this feature for each tenant.
Support for Remote AAA and Webhook Notifications Over Management VPN 512	This feature provides increased security by allowing you to configure tenants to receive AAA traffic and webhook notifications over management VPN 512.
Support for Tenant to Access to Controller-Specific Information	This feature enables tenants to access their controller-specific restricted information, which enhances visibility and simplifies management and troubleshooting within the Cisco Catalyst SD-WAN network. This improved visibility aids in addressing issues related to OMP, routing, control connections, and more.
Upstream and Downstream Bandwidth Reference Values	Use the upstream and downstream bandwidth reference values to govern how Cisco SD-WAN Manager displays interface utilization percentages in charts. The values also act as configurable thresholds that trigger interface-bw events when a network interface's utilization exceeds a defined point.
Cisco Catalyst SD-WAN Security	
Disabled Weak SSH Encryption Algorithms	For better security, certain weak SSH encryption algorithms are disabled by default on port 22 and port 830 for devices in the Cisco Catalyst SD-WAN overlay.

Feature	Description
MACsec Support for Cisco Catalyst IR1101 and IR1800 Rugged Series Routers	This feature adds MACsec support for Cisco Catalyst IR1101 and IR1800 Rugged Series routers.
Unified Logging Records Include Logs of Inspect, Pass or Drop Actions	This feature allows generating log data of inspect, pass, or drop actions about security connection events when Unified Logging is enabled.
Cisco Catalyst SD-WAN Cloud OnRamp	
Cloud OnRamp for Multicloud	This feature provides a single common dashboard in Cisco SD-WAN Manager that displays unified information of accounts, gateways, and connections for both cloud and interconnect providers. This feature enhances the user experience by helping you identify resources and monitor each provider's utilization.
Cisco Catalyst SD-WAN Monitor and Maintain	
Data Plane CPU and Memory Utilization	With this feature you can monitor data plane CPU and memory utilization on Cisco IOS XE Catalyst SD-WAN devices using Cisco SD-WAN Manager.
Energy Management	This feature introduces a new dashboard that displays the Cisco SD-WAN Manager power utilization, energy usage, device capability, and consumption data.
Multiple Remote Devices and Circuits to View Tunnel Health	With this feature, add multiple remote devices and circuits to view the tunnel health data in the line chart. You can add a maximum of five devices at a time and the tunnel health data is displayed for each path.
Cisco Catalyst SD-WAN NAT	
Mapping of Address and Port Using Encapsulation (MAP-E) with Transport Locator (TLOC)	This feature extends the support for IP over Ethernet (IPoE) MAP-E to include TLOC interfaces. The integration of MAP-E with TLOC allows the device to handle IPv4 traffic efficiently over an IPv6 network.
Support for Site-Local Failover for NAT DIA	Support for NAT DIA traffic failover in sites with more than one edge device. The support for same-site NAT DIA local failover works with NAT44 and NAT66 by tunneling the traffic from one edge device to another edge device that has NAT DIA access within a site.
Cisco Catalyst SD-WAN Policy Groups	

Feature	Description
Application Compliance	When you update the reference Protocol Pack, Cisco SD-WAN Manager checks whether any protocols in the Protocol Pack introduce name conflicts with currently defined custom applications. If so, Cisco SD-WAN Manager does not complete the update of the reference Protocol Pack.
Cloud-Sourced Applications	Cloud-sourced applications, derived from the Cisco SD-AVC component, complement applications from other sources, such as Protocol Packs and custom applications. You can use cloud-sourced applications in security and centralized policies, and in Cloud OnRamp for SaaS.
Configure Source Interface for Security Logging	This feature enables configuring source interfaces for High-Speed Logging (HSL) and SysLog for security logging in Cisco SD-WAN Manager.
Enhancements to Security Policy Using Policy Groups	The following enhancements are introduced with this release: • **Embedded Security** is called **NGFW** in Cisco SD-WAN Manager. • Create copies of security policy and sub-policy. • View all configured rules for specific policies in the **NGFW** policy dashboard. • For each rule, **Clone rule**, **Add rule on top**, and **Add rule below** options are added.
Server Label For High Speed Logging Source Interface and External Syslog Source Interface	This feature allows users to configure the High-Speed Logging Source Interface and SysLog Source Interface for security logging based on the security policy level for SD-WAN.
Cisco Catalyst SD-WAN Network-Wide Path Insight User	
Synthetic Traffic Packet Capture Replay	With this feature, you can simulate traffic of a trace by replaying a PCAP file.
Cisco Managed Cellular Activation	
Managed Cellular Activation Support for Cisco Catalyst Heavy Duty Routers	Specific pluggable interface modules of Cisco Catalyst IR8140 Heavy Duty Routers support the Managed Cellular Activation solution.
Cisco Catalyst SD-WAN Integrations	
Cisco Secure Equipment Access Integration	Cisco Secure Equipment Access (SEA) is a solution that provides remote access to network-connected assets. Assets can include anything reachable by IP address, such as servers, industrial internet of things (IIoT) devices, and so on. Integration with Cisco Catalyst SD-WAN enables you to use Cisco SD-WAN Manager to deploy the Cisco SEA solution within a Cisco Catalyst SD-WAN network.

Feature	Description
Third-Party Custom Application Integration	Cisco SD-WAN Manager supports integration with third-party-developed Cisco IOx applications. These custom applications add functionality to devices that run Cisco IOSXE Catalyst SD-WAN software.

Software and Hardware Behavior Changes in Cisco IOS XE Catalyst SD-WAN Release 17.16.x

Software and Hardware Behavior Changes in Cisco IOS XE Catalyst SD-WAN Release 17.16.1a

Behavior Change	Description
The following show commands are no longer supported: • show sdwan from-vsmart policy • show sdwan from-vsmart tag-instances	See the show sdwan from-vsmart policy section.
The range for *instance id* in **l2vpn sdwan instance** command is 1 to 511 and 513 to 65527.	See the L2VPN Commands section for more details about this command.
The **Use Custom Commands** field does not support certain OMP and TTM show commands.	See the Generate Admin-Tech Files section for more details.
Configuring services using the **allow-service** *all* command on Cisco Catalyst SD-WAN Controllers is only applicable for the following services: **bgp**, **dhcp**, **dns**, **https**, **icmp**, **netconf**, **ntp**, **ospf**, **sshd**, and **stun**. Note that configuring **allow-service** *all* overrides any commands that allow or disallow individual services.	See the following sections for more details about this command: • allow-service command • Configure Adaptive QoS Using the CLI • Configure Implicit ACL on Loopback Interfaces Using CLI
The default OMP hold time is increased to 5400 seconds.	See the Configure OMP Timers section for more details.

Important Notes, Known Behaviors, and Workarounds

Border router requirement for transport gateways

From Cisco IOS XE Catalyst SD-WAN Release 17.16.1a and Cisco Catalyst SD-WAN Control Components Release 20.16.1, in a network using Multi-Region Fabric, Cisco Catalyst SD-WAN only supports configuring border routers as transport gateways. It does not support configuring edge routers as transport gateways.

Resolved and Open Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.16.x

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

Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.16.1a

Resolved Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.16.1a

Identifier	Headline
CSCwk42493	Cellular interface in last-resort mode should be admin up, line protocol down.
CSCwh01678	20.12 ISR1100 platform FTM crash with SIG enabled.
CSCwm48459	Software crash with critical process vip_confd_startup_sh fault on rp_0_0 (rc=6)
CSCwm50619	Data policy commit failure occurs when export-spread is enabled in Cflowd configuration.
CSCwj01917	After Upgrade to 17.9.4a, Cellular Interface IP Address Negotiated mismatching.
CSCwm72748	Crash in OMPd process crashes due to Sig-abort when hitting pthread limit.
CSCwk05354	SD-Routing: Interface flap with auto-neg CLI.

Open Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.16.1a

Identifier	Headline
CSCwn32668	L2 traffic go to blackhole due to mac-route originated from blocked node after power-cycle.
CSCwn26353	BFD sessions via TLOC-Ext do not come up when IPv6 is dynamically changed.
CSCwn12594	17.16 SIG zscaler ipsec - VPN credentials for primary tunnel not created.
CSCwn45512	Router is reaching the show ip nat translations total limit even with low active NAT table entries.
CSCwn40906	Router crash observed when optimizing encrypted traffic with DRE.
CSCwm43089	Low throughput with CAT8000V vc CSR1000.
CSCwn48140	Failing to ping to service-side IPv4 interface from remote Cisco IOS XE Catalyst SD-WAN device with IPv6 tunnel and LTE Cellular.
CSCwn45328	Unable to create unified policy with IPv6 rule when any other rule has AIP with TLS action decrypt.

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 Catalyst 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
- Cisco Recommended Catalyst SD-WAN Software Versions for Controllers and WAN Edge Routers

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)

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)

© 2024 Cisco Systems, Inc. All rights reserved.