



What's New for Cisco SD-WAN

This chapter describes what's new in Cisco SD-WAN for each release.

- [What's New for Cisco IOS XE SD-WAN Releases 16.12.1b, 16.12.1d, and 16.12.2r, on page 1](#)
- [What's New for Cisco SD-WAN Release 19.2.x, on page 3](#)
- [What's New for Cisco SD-WAN Release 19.1.x, on page 5](#)

What's New for Cisco IOS XE SD-WAN Releases 16.12.1b, 16.12.1d, and 16.12.2r

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: What's New for Cisco IOS XE SD-WAN Devices

Feature	Description
Getting Started	
API Cross-Site Request Forgery Prevention	This feature adds protection against Cross-Site Request Forgery (CSRF) that occurs when using Cisco SD-WAN REST APIs. This protection is provided by including a CSRF token with API requests. You can whitelist requests so that they do not require protection if needed. See Cross-Site Request Forgery Prevention .
Systems and Interfaces	
IPv6 Support for NAT64 Devices	This feature supports NAT64 to facilitate communication between IPv4 and IPv6 on Cisco IOS XE SD-WAN devices. See IPv6 Support for NAT64 Devices .

Feature	Description
Secure Shell Authentication Using RSA Keys	This feature helps configure RSA keys by securing communication between a client and a Cisco SD-WAN server. See SSH Authentication using vManage on Cisco XE SD-WAN Devices. See Configure SSH Authentication .
DHCP option support	This feature allows DHCP server options, 43 and 191 to configure vendor-specific information in client-server exchanges. See Configure DHCP .
Communication with an UCS-E Server	This feature allows you to connect a UCS-E interface with a UCS-E server through the interface feature template. See Create a UCS-E Template .
Bridging, Routing, Segmentation, and QoS	
QoS on Subinterface	This feature enables Quality of Service (QoS) policies to be applied to individual subinterfaces. See QoS on Subinterface .
Policies	
Packet Duplication for Noisy Channels	This feature helps mitigate packet loss over noisy channels, thereby maintaining high application QoE for voice and video. See Configure and Monitor Packet Duplication. See Configure and Monitor Packet Duplication .
Control Traffic Flow Using Class of Service Values	This feature lets you control the flow of traffic into and out of a Cisco device's interface based on the conditions defined in the quality of service (QoS) map. A priority field and a layer 2 class of service (CoS) were added for configuring the re-write rule. See Configure Localized Data Policy for IPv4 Using Cisco vManage .
Integration with Cisco ACI	The Cisco SD-WAN and Cisco ACI integration functionality now supports predefined SLA cloud beds. It also supports dynamically generated mappings from a data prefix-list and includes a VPN list to an SLA class that is provided by Cisco ACI. See Integration with Cisco ACI .
Encryption of Lawful Intercept Messages	This feature encrypts lawful intercept messages between a Cisco IOS XE SD-WAN device and a media device using static tunnel information. See Encryption of Lawful Intercept Messages .
Security	
High-Speed Logging for Zone-Based Firewalls	This feature allows a firewall to log records with minimum impact to packet processing. See Firewall High-Speed Logging .
Self zone policy for Zone-Based Firewalls	This feature can help define policies to impose rules on incoming and outgoing traffic. See <i>Apply Policy to a Zone Pair</i> in Use the Policy Configuration Wizard .

Feature	Description
Secure Communication Using Pairwise IPsec Keys	This feature allows private pairwise IPsec session keys to be created and installed for secure communication between IPsec devices and its peers. See IPsec Pairwise Keys Overview .
Network Optimization and High Availability	
TCP Optimization	This feature optimizes TCP data traffic by decreasing any round-trip latency and improving throughput. See TCP Optimization: Cisco XE SD-WAN Routers .
Share VNF Devices Across Service Chains	This feature lets you share Virtual Network Function (VNF) devices across service chains to improve resource utilisation and reduce resource fragmentation. See Share VNF Devices Across Service Chains .
Monitor Service Chain Health	This feature lets you configure periodic checks on the service chain data path and reports the overall status. To enable service chain health monitoring, NFVIS version 3.12.1 or later should be installed on all CSP devices in a cluster. See Monitor Service Chain Health .
Manage PNF Devices in Service Chains	This feature lets you add Physical Network Function (PNF) devices to a network, in addition to the Virtual Network function (VNF) devices. These PNF devices can be added to service chains and shared across service chains, service groups, and a cluster. Inclusion of PNF devices in the service chain can overcome the performance and scaling issues caused by using only VNF devices in a service chain. See Manage PNF Devices in Service Chains .
Devices	
Cisco 1101 Series Integrated Services Routers	Cisco SD-WAN capability can now be enabled on Cisco 1101 Series Integrated Services Routers.
Commands	
Loopback interface support for WAN (IPsec)	This feature allows you to configure a loopback transport interface on a Cisco IOS XE SD-WAN device for troubleshooting and diagnostic purposes. See the bind command.

What's New for Cisco SD-WAN Release 19.2.x

This section applies to Cisco vEdge 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 2: What's New for Cisco vEdge Device

Feature	Description
Getting Started	
API Cross-Site Request Forgery Prevention	This feature adds protection against Cross-Site Request Forgery (CSRF) that occurs when using Cisco SD-WAN REST APIs. This protection is provided by including a CSRF token with API requests. You can whitelist requests so that they do not require protection if needed. See Cross-Site Request Forgery Prevention .
Systems and Interfaces	
Secure Shell Authentication Using RSA Keys	This feature helps configure RSA keys by securing communication between a client and a Cisco SD-WAN server. See SSH Authentication using vManage on Cisco XE SD-WAN Devices. See Configure SSH Authentication .
Policies	
Packet Duplication for Noisy Channels	This feature helps mitigate packet loss over noisy channels, thereby maintaining high application QoE for voice and video. See Configure and Monitor Packet Duplication .
Control Traffic Flow Using Class of Service Values	This feature lets you control the flow of traffic into and out of a Cisco device's interface based on the conditions defined in the quality of service (QoS) map. A priority field and a layer 2 class of service (CoS) were added for configuring the re-write rule. See Configure Localized Data Policy for IPv4 Using Cisco vManage .
Security	
Secure Communication Using Pairwise IPsec Keys	This feature allows private pairwise IPsec session keys to be created and installed for secure communication between IPsec devices and its peers. For related information, see IPsec Pairwise Keys Overview .
Network Optimization and High Availability	
Disaster Recovery for vManage	This feature helps you configure Cisco vManage in an active or standby mode to counteract hardware or software failures that may occur due to unforeseen circumstances. See Configure Disaster Recovery .
Share VNF Devices Across Service Chains	This feature lets you share Virtual Network Function (VNF) devices across service chains to improve resource utilisation and reduce resource fragmentation. See Share VNF Devices Across Service Chains .
Monitor Service Chain Health	This feature lets you configure periodic checks on the service chain data path and reports the overall status. To enable service chain health monitoring, NFVIS version 3.12.1 or later should be installed on all CSP devices in a cluster. See Monitor Service Chain Health .

Feature	Description
Manage PNF Devices in Service Chains	This feature lets you add Physical Network Function (PNF) devices to a network, in addition to the Virtual Network function (VNF) devices. These PNF devices can be added to service chains and shared across service chains, service groups, and a cluster. Inclusion of PNF devices in the service chain can overcome the performance and scaling issues caused by using only VNF devices in a service chain. See Manage PNF Devices in Service Chains .

What's New for Cisco SD-WAN Release 19.1.x

This section applies to Cisco IOS XE 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 3: What's New for Cisco IOS XE Device

Feature	Description
Systems and Interfaces	
IPv6 for Transport	For related information, see IPv6 Functionality .
CLI Templates Support on vEdge Routers	For related information, see CLI Templates for Cisco XE SD-WAN Routers .
Enterprise Certificates	For related information, see Configure Controller Certificate and Upload WAN Edge Router Authorized Serial Number File .
EIGRP Support	For related information, see EIGRP and EIGRP Configuration .
VPN Interface IPsec (for XE Routers)	For related information, see VPN Interface IPsec (for XE Routers) .
IP Directed Broadcast	For related information, see IP Directed Broadcast .
RBAC by VPN	For related information, see RBAC by VPN .
Enable DHCP Server using vManage	For related information, see Enable DHCP Server using vManage .
Configure an Interface as a NAT Device	For related information, see Configure an Interface as a NAT Device .
Policies	
Lawful Intercept for SD-WAN	For related information, see Lawful Intercept for SD-WAN .

Feature	Description
Forward Error Correction	For related information, see Forward Error Correction .
vEdge Router as a NAT Device	For related information, see vEdge Router as a NAT Device .
Integrate Cisco XE SD-WAN Router with Cisco ACI	For related information, see Integrate Cisco XE SD-WAN Router with Cisco ACI .
Security	
Advanced Malware Protection	For related information, see Advanced Malware Protection .
Cisco PKI support for SD-WAN controllers	For related information, see Control Plane Authentication .
Network Optimization and High Availability	
Cloud OnRamp Support	For detailed information, see Cloud OnRamp Support .