What's New for Cisco SD-WAN

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 RFP documentation, or language that is used by a referenced third-party product.

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

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 put requests on an allowed list so that they do not require protection if needed. See Cross-Site Request Forgery Prevention.
Systems and Interfaces	

Feature	Description
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.
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.

Feature	Description
Self zone policy for Zone-Based Firewalls	This feature can help define policies to impose rules on incoming and outgoing traffic. See *Apply Policy to a Zone Pair* in Use the Policy Configuration Wizard.
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.