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 Release 16.12.1b, 16.12.1d, and 16.12.2r

This section applies to Cisco 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 XE SD-WAN Device

Feature	Description
Getting Started	
Multitenancy support in Cisco XE SD-WAN Devices	Starting release Cisco IOS XE SD-WAN 16.12.2r, multitenancy is supported on the following platforms: • Cisco ASR 1000 Series Aggregation Services Routers, Cisco ASR 1001X • Cisco ISR 4000 Series Integrated Services Routers, Cisco ISR 4321, Cisco ISR 4461 • Cisco ISR 1000 Series Integrated Services Routers. Cisco ISR 1111-4P • Cisco CSR 1000 Series Cloud Services Routers, Cisco 1000v Multitenancy allows service providers to manage multiple customers or tenants.

Feature	Description
Tenant data backup solution in multitenant mode	Starting from Cisco IOS XE SD-WAN 16.12.2r, when databases are shared by multiple tenants in2 a multitenant mode, you can back up data for a specific tenant and restore it.
Systems and Interfaces	
IPv6 Support for NAT64 Devices	This release supports NAT64 to facilitate communication between IPv4 and IPv6 on Cisco IOS XE SD-WAN routers. For related information, see Configure NAT64 CLI Equivalent on Cisco XE SD-WAN Routers.
Secure Shell Authentication Using RSA Keys	You can now configure RSA keys to secure communication between a client and a Cisco SD-WAN server. For related information, see SSH Authentication using vManage on Cisco XE SD-WAN Devices.
DHCP option support	You can now use DHCP server options 43 and 191 to configure vendor-specific information in client-server exchanges. For related information, see Configure DHCP.
Communication with an UCS-E Server	This feature provides an interface in the interface feature template list to configure an UCS-E interface to connect to an UCS-E server. For related information, see Create a UCS-E Template.
Bridging, Routing, Segmentation, and QoS	
Subinterface QoS	A physical interface may be treated as multiple interfaces by configuring one or more logical interfaces called subinterfaces. This feature enables Quality of Service (QoS) policies to be applied to individual subinterfaces. For related information, 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. This feature is supported on Cisco XE SD-WAN devices as well as on Cisco vEdge devices. For related information, see Configure and Monitor Packet Duplication.
Integration with Cisco ACI	The 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. For related information, see Integration with Cisco ACI.
Encryption of Lawful Intercept Messages	Lawful intercept messages between a Cisco XE SD-WAN router and a Media Device can now be encrypted using static tunnel information. For related information, see Lawful Intercept.
Security	
High-Speed Logging for Zone-Based Firewalls	High-Speed Logging (HSL) allows a firewall to log records with minimum impact to packet processing. For related information, see Firewall High-Speed Logging.

Feature	Description
Self zone policy for Zone-Based Firewalls	Self-zone is an default zone in the firewall that is associated with the VPN for punt and inject interface. You can define policies to impose rules on the incoming and outgoing traffic. For related information, see Configure Firewall Policies Using vManage.
Secure Communication Using Pairwise IPsec Keys	This feature enables support to create and install private pairwise IPSec session keys to secure communication between IPSec devices and its peers. For related information, see IPSec Pairwise Keys Overview.
Network Optimization and High Availability	
TCP Optimization	TCP optimization fine tunes the processing of TCP data traffic to decrease round-trip latency and improve throughput. For related information, see TCP Optimization: Cisco XE SD-WAN Routers. This feature support was added in Cisco IOS XE SD-WAN Release 16.12.1d
Commands	
Loopback interface support for WAN (IPsec)	You can now configure a loopback transport interface on a Cisco IOS XE SD-WAN router to help in troubleshooting and diagnostics. For related information, 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	
Tenant data backup solution in multitenant mode	Starting from Cisco SD-WAN release 19.2.1, when databases are shared by multiple tenants in2 a multitenant mode, you can back up data for a specific tenant and restore it.
Systems and Interfaces	
Secure Shell Authentication Using RSA Keys	This feature enables secure shell authentication between a client and a Cisco SD-WAN server using RSA keys. For related information, see SSH Authentication using vManage on Cisco XE SD-WAN Devices.
Policies	

Feature	Description
Packet Duplication for Noisy Channels	This feature helps mitigate packet loss over noisy channels, thereby maintaining high application QoE for voice and video. This feature is supported on Cisco XE SD-WAN devices as well as on Cisco vEdge devices. For related information, 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 vEdge 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. For related information, see Configure Localized Data Policy for IPv4 vManage.
Security	
IPSec Pairwise Keys	This feature enables support to create and install private pairwise IPSec session keys to 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 vManage in an active or standby mode to counteract hardware or software failures that may occur due to unforeseen circumstances. For detailed information, 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. For related information, 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. For related information, 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. For related information, see Manage PNF Devices in Service Chains.