Release Notes for Cisco IOS XE Catalyst SD-WAN Devices, Cisco IOS XE Catalyst SD-WAN Release 17.8.x

First Published: 2022-04-22

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

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 17.8.x

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.

These release notes accompany the Cisco IOS XE Catalyst SD-WAN Release 17.8.x, which provides Cisco SD-WAN capabilities. They include release-specific information for Cisco Catalyst SD-WAN Controllers, Cisco Catalyst SD-WAN Validators, Cisco SD-WAN Manager, as applicable to Cisco IOS XE Catalyst SD-WAN devices.

Related Releases

For release information about Cisco vEdge Devices, refer to Release Notes for Cisco vEdge Devices, Cisco SD-WAN Release 20.8.x.

For release information about Cisco SD-WAN Control Components, refer to Release Notes for Cisco SD-WAN Control Components, Cisco Catalyst SD-WAN Control Components Release 20.8.x

What's New for Cisco IOS XE Catalyst SD-WAN Release 17.8.x

This section applies to Cisco IOS XE Catalyst 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 17.8.1a

Feature	Description
Cisco SD-WAN Getting Started Guide	
Support for Postpaid MSLA License Billing Models	For postpaid Managed Services License Agreement Program (MSLA) licenses, Cisco SD-WAN supports a distinction of two billing models for licenses—committed (MSLA-C) and uncommitted (MSLA-U) licenses. Beginning with Cisco vManage Release 20.8.1, the procedure for assigning a postpaid license enables you to choose one of these two MSLA license types.

Feature	Description
Cisco SD-WAN Systems and Interfaces	
Configuration Groups and Feature Profiles	This feature provides a simple, reusable, and structured approach for configuration in Cisco SD-WAN. You can create a configuration group, that is, a logical grouping of devices that share a common purpose within your WAN. You can also create profiles based on features that are required, recommended, or uniquely used, and then combine the profiles to complete a device configuration. The configuration group workflows in Cisco vManage provide a guided method to create configuration groups and feature profiles.
User-Defined Device Tagging	This feature helps you add tags to devices. You can use the tags for grouping, describing, finding, or managing devices.
Cisco Unified Communications FXS and FXO Caller ID Support	This feature lets you configure Foreign Exchange Station (FXS) and Foreign Exchange Office (FXO) caller ID features by using Cisco vManage CLI add-on feature templates.
Ability to Configure APNs under Running Configurations for Single and Dual SIMs	This feature allows you to create a data profile for a cellular device by configuring one or two SIMs in the device.
Added Support for LTE Advanced NIM Modules	Added support for Long-Term Evolution (LTE) Advanced Network Interface Modules (NIMs) for Cisco ISR 4000 routers.
Cisco ThousandEyes Support for Cisco Catalyst 8500 Series Edge Platforms and Cisco ASR 1000 Series Aggregation Services Routers	You can deploy Cisco ThousandEyes Enterprise agent natively as a container application on Cisco Catalyst 8500 Series Edge Platforms and Cisco ASR 1000 Series Aggregation Services Routers. You can install and activate the Cisco ThousandEyes Enterprise agent through Cisco vManage.
Cisco SD-WAN Routing	
RIPng (IPv6) Support on Cisco IOS XE SD-WAN Devices	This feature adds support for IPv6 addresses and prefixes on Cisco IOS XE SD-WAN devices. It also supports redistribution of connect, static, OMP, and OSPF routes into RIPng and vice versa.
Cisco SD-WAN Policies	
Traffic Redirection to SIG Using Data Policy: Fallback to Routing	With this feature, you can configure internet-bound traffic to be routed through the SD-WAN overlay, as a fallback mechanism, when all the SIG tunnels are down.

Feature	Description
Redirect DNS in a Service-Side VPN	This feature enables Cisco IOS XE SD-WAN devices to respond to Domain Name System (DNS) queries using a specific configuration and the associated proxy servers. This feature adds support for DNS proxy for servce-side VPN hosts and DNS redirect inside the service VPNs. You can configure redirect DNS using Cisco vManage or a device CLI.
Cisco SD-WAN Security	
SIG Integration Improvements	**Source-Only Load Sharing**: When you configure two or more active tunnels to a SIG, different traffic flows from the same source IP address, with different destination public IP addresses, may be mapped to use different tunnels. With this feature, you can configure all traffic flows from a particular source IP address, irrespective of the destination IP address, to be routed to the SIG through only one of the active tunnels. **IPSec Tunnel Creation Improvements in an Active-Active Setup**: This feature ensures that when you provision an IPSec tunnel, the control and data traffic are sent through the same the physical interface toward the SIG endpoint. Pinning the control and data packets to the same physical interface removes a limitation that exists in previous releases. In previous releases, in certain situations, the control and data packets may be routed to the SIG endpoint through different physical interfaces. When the packets are routed in this way, one of the following scenarios occurs: • If the source is a physical interface, tunnel creation fails because the source IP address of the negotiation packets differs from the source IP address of the keepalive control packet. • If the source is a loopback interface, the source IP address of the data packets differs from the source IP address of the IPSec SA negotiated through the control packets. This difference causes the SIG endpoint to drop the data packets.
Layer 7 Health Check for Manual Tunnels	You can create and attach trackers to manually created GRE or IPSec tunnels to a SIG endpoint. Trackers help failover traffic when a SIG tunnel is down.
Cisco SD-WAN Cloud OnRamp	
Support for SVL Port Configuration on 100G Interfaces	With this feature, you can configure SVL ports on 100G Ethernet interfaces of Cisco Catalyst 9500-48Y4C switches, thus ensuring a high level of performance and throughput.
View Details of Microsoft Telemetry and View Application Server Information for Office 365 Traffic	This feature adds better visibility into how Cloud onRamp for SaaS determines the best path for Microsoft Office 365 traffic, if you have opted to use Microsoft telemetry. One enhancement is a chart that shows how Microsoft rates the connection quality of different interfaces, specifically for different types (called service areas) of Office 365 traffic. This is helpful for troubleshooting Office 365 performance issues. Another addition is the SD-AVC Cloud Connector page, which shows a list of Microsoft URL/IP endpoints and categories that Cisco SD-WAN receives from Microsoft Cloud.

Feature	Description
User-Defined SaaS Application Lists	This feature expands the range of SaaS applications that Cloud onRamp for SaaS can monitor, and for which it can determine the best network path. The feature enables you to define lists of one or more SaaS applications, together with the relevant application server for those SaaS applications. Cloud onRamp for SaaS handles these lists in the same way that it handles the predefined set of SaaS applications that it can monitor. When you enable a user-defined list, Cloud onRamp for SaaS probes for the best path to the application server and routes the application traffic for applications in the list to use the best path.
Periodic Audit, Enhancement to Azure Scaling and Audit, and ExpressRoute Connection	Cisco vManage provides an optional periodic audit with an interval of two hours. This automatic audit takes place in the background and generates a report of the discrepancies. If you enable the auto correct option, then Cisco vManage automatically resolves any recoverable issues found during the periodic audit. Discrepancies generated after initiating an on-demand audit are individually fixable. ExpressRoute connections are the private networks that offer higher reliability, fewer latencies, and faster connections for data transfer.
Cisco SD-WAN Interconnect to Google Cloud and Microsoft Azure	You can create software-defined interconnects to Google Cloud VPCs, or Microsoft Azure VNets or Virtual WANs to link your branch location to the cloud resources through the Equinix fabric. You can also create, update and delete device links from Interconnect Gateway in the Equinix fabric.
Cisco SD-WAN Monitor and Maintain	
Software Upgrade Workflow for Cisco SD-WAN edge devices.	This feature introduces a guided workflow through which you can upgrade the software image on your Cisco IOS XE Catalyst SD-WAN devices and Cisco vEdge devices and monitor the status of the software upgrade. With this workflow, you can choose to download, install, and activate the new software image in discrete steps or in a single step.
Bidirectional Support for Packet Tracing	This feature provides a detailed understanding of how data packets are processed by the edge devices in both the directions. The bidirectional debugging can help you to diagnose issues and troubleshoot them more efficiently.
Site Topology Visualization in Cisco SD-WAN Manager	You can now view the topology diagram of a site in Cisco SD-WAN Manager.
Cisco SD-WAN SNMP	
Cisco SD-WAN MIBs	The following Cisco SD-WAN MIBs are introduced on Cisco IOS XE SD-WAN devices: CISCO-SDWAN-PROBE-MIB.my CISCO-SDWAN-OMP-MIB.my (additional tables added) CISCO-SDWAN-SECURITY-MIB.my (additional tables added)

Feature	Description
Cisco SD-WAN NAT	
Support for NAT DIA IPv4 over an IPv6 Tunnel	This feature provides support for an IPv4 client to access IPv4 servers when using an IPv6 network. IPv4 traffic is routed to the internet over an IPv6 tunnel. You can configure NAT DIA IPv4 over an IPv6 tunnel using a device CLI or a CLI add-on template.
Service-Side Conditional Static NAT Support	This feature allows you to translate the same source IP address to different IP addresses based on the destination IP addresses. You can configure service-side conditional static NAT using a device CLI.
Service-Side Static Network NAT Support	This feature supports configuration of service-side static NAT for a subnet. Instead of configuring multiple static NAT pools, you can configure a single static NAT pool for an entire subnet. You can configure service-side static network NAT using Cisco vManage or a device CLI template.
Service-Side NAT Object Tracker Support	This feature adds support for tracking LAN prefixes and LAN interfaces for service-side inside static NAT. When the object tracker that is associated with a NAT route changes state (up or down), the NAT OMP route is added or removed from the routing table. You can view notifications in Cisco vManage for monitoring the NAT routes and interfaces that are added or removed. You can configure the service-side NAT object tracker using Cisco vManage, a device CLI template, or a CLI add-on template.
Cisco Hierarchical SD-WAN Configuration Guide	
Hierarchical SD-WAN: Secondary Regions	Secondary regions provide another facet to the Hierarchical SD-WAN architecture and enable direct tunnel connections between edge routers in different primary access regions. When you assign an edge router a secondary region, the router effectively operates in two regions simultaneously, and has different paths available through its primary and secondary regions.
Hierarchical SD-WAN: Transport Gateways	An edge router or border router that has connections to two networks that lack direct connectivity can function as a transport gateway. This is helpful for enabling connectivity between routers that are configured to be within the same access region, but which do not have direct connectivity.
Hierarchical SD-WAN: Router Affinity	Often a router has multiple options to choose for the next hop when routing a flow to its destination. When multiple devices can serve as the next hop for a flow, you can specify the order of preference among the devices by configuring router affinity groups. The result is that a router attempts to use a route to the next-hop device of highest preference first, and if that device is not available, it attempts to use a route to the next-hop device of the next lower preference. Affinity groups enable this functionality without requiring complex control policies.

Software and Hardware Behavior Changes in Cisco IOS XE Catalyst SD-WAN Release 17.8.1a

Behavior Change	Description
SNMP appRoute MIB object identifiers (OIDs) are added to support **Mean Jitter**, **Latency**, and **Packet Drop** data requests from SNMP.	A note is added in the Supported SNMP MIBs section.
A new keyword **src-only** is added to the load-sharing algorithms for configuring IPv4 and IPv6 non Cisco SD-WAN traffic. New CLIs **ip load-sharing algorithm** and **ipv6 load-sharing algorithm** are added for configuring IPv4 and IPv6 Cisco SD-WAN traffic. You need to configure a CLI template for configuring the **src-only** load-sharing algorithms.	A new keyword is added in the ip cef load sharing algorit A new keyword is added in the ipv6 cef load-sharing algo A new CLI ip load-sharing algorithm is added for IPv4. A new CLI ipv6 load-sharing algorithm is added for IPv6 A new section Configure Load-Balancing Algorithm Usi
A notification is generated when there is an SNMP trap for a Bidirectional Forwarding Detection (BFD) state change.	BFD state change entries are added in the Information Abou tables.
A new command **alarms alarm bfd-state-change-syslog** is added for enabling or disabling BFD syslog messages.	A new command alarms alarm bfd-state-change syslog is A note is added in the Using the CLI section.
If a device boots using the .bin file after a plug-and-play (PnP) or auto-install process completes, the device comes up with its day-0 configuration. The device then reloads automatically and goes into install mode.	A note is added in the Software Installation and Upgrade fo
Support is added for capturing IPv6 packets for tracing and troubleshooting packets. You can now choose an IPv6 interface from the **Interface** drop-down list.	A note is added in the Capture Packets section.
Custom subnet IP address restrictions are added. The custom subnet must not conflict with the subnets used for other connections.	Updated text is added under VIF Type > Settings > Custo Private Hosted VIF to AWS Direct Connect Gateway fron Updated text is added under Connection VIF Type > Settin Connect Private Hosted Connection to AWS Direct Conn Gateway section. Updated text is added under Connection VIF Type > Settin Connect Transit Hosted Connection to AWS Direct Conn Gateway section. Updated text is added under BGP-Peering Settings > Custo Connection to Microsoft Azure ExpressRoute from Interc

Behavior Change	Description
The **Application Usage** column and the **Application Usage** links are removed from the **Monitor** > **Devices** > **WAN - Tunnel** window. After configuring on-demand troubleshooting for a device, you can view SD-WAN Application Intelligence Engine (SAIE) usage data based on the selected filters or based on application families sorted by usage.	A note is added in the View TLOC Loss, Latency, and Jitter A note is added in the View Tunnel Connections section.
Two new fields are added. **Reference Account Name**: Cisco vManage discovers the software images and instance sizes using this reference account name. **Reference Region**: Cisco vManage discovers the software images and instance sizes in this reference region under the referenced account name.	Two new fields are added in the Configure Cloud Global Sett
Alarms are added to syslog with syslog facility and priority `local7.notice`.	Updated text is added in the Syslog Message Format section.
Change in time-out behavior for template push to CCM.	In Cisco vManage Release 20.7.x and earlier releases, the Cis and CSP device configuration tasks time out 30 minutes after case of long-running image installation operations, these conf and fail, while the cluster activation state continues to be in a From Cisco vManage Release 20.8.1, the CCM and CSP dev out 30 minutes after the last heartbeat status message that Cis the target devices. With this change, long-running image inst cause configuration tasks to fail after a predefined interval of
Change in CCM workflow.	In Cisco vManage Release 20.7.x and earlier releases, Cisco up and activation progress is reported as part of the CLOUD task shows the seven steps in the CCM bring up and activatio whether the sequence was successfully completed or not. The Configuration task shows the status of the RBAC settings co From Cisco vManage Release 20.8.1, CLOUD ONRAMP C Cisco vManage receives CCM Healthy from the target CSP d Template Configuration task shows the seven steps in the CC sequence and indicates whether the sequence was successfull with the status of the RBAC settings configuration push.

Important Notes, Known Behavior, and Workaround

- Cisco IOS XE Catalyst 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 SD-WAN Manager. 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 Catalyst SD-WAN 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 Catalyst SD-WAN Release 17.8.1a

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

Resolved Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.8.1a

Identifier	Headline
CSCwa52915	Replicator with direct multicast source reachability should be preferred among selected replicators
CSCwa42376	Cisco IOS XE Catalyst SD-WAN Device device would keep invalid IPv6 address in the tunnel to vManage and can not recover
CSCvz89460	Cisco SD-WAN: All region BRs are seen in partial connections on Vmanage
CSCwa38570	SaaS traffic not taking the best SIG tunnels when CoR SaaS with SIG tunnels configured
CSCvx74917	[17.5 Umbrella] DNS Packets are not redirected to configured Custom DNS after Umbrella Template Edit
CSCwb43605	Cisco IOS XE Catalyst SD-WAN Device OMPd crash during RIB-out attribute aspath/community processing
CSCvz23982	IOS sending UP Event for the sub interface which is in down state
CSCwa93668	FBD: flowdb entry double free during pperx pipeline collision
CSCvy78501	17.6: AAR not working properly as configured SLA classes are not shown under app-route stats
CSCvz74773	Discrepancies in CLI and GUI interface details (Truncating interface numbers)
CSCvz87855	mroute state stuck after Cisco IOS XE Catalyst SD-WAN Device failure is restored
CSCwa93930	"alarms alarm bfd-state-change syslog" command is getting rejected while reconfiguring the device.

Identifier	Headline
CSCwa81471	AOM pending objects with loopbacks binded to tloc-extended interfaces
CSCwb02851	ISR1100 crashes due to memory corruption when pppoe dialer interface flaps
CSCvw70446	ASR1K crashes when config changed to add/delete match filters
CSCwa34783	BFD session get stuck to down after site to site speedtest with Loopback as WAN + NAT
CSCwa92331	Affinity logic not working if entire CG1 vSmart shutdown
CSCwa92411	Slowness issues casued by intermittent traffic drop on ISRv ingress from GRE tunnel
CSCwa78762	Umbrella SIG tunnel creation failed after config reset for PnP
CSCvz81428	SIT : vedaemon assert noticed in the ISR 4221 over weekend longevity
CSCvz80101	Policy XML pruning without ConfD dependency
CSCwa14226	Policy commit retry needed when ConfD commit fails.
CSCvy80654	Cisco IOS XE Catalyst SD-WAN Device router maintains persistent connections to vBond
CSCvz99320	Cisco IOS XE Catalyst SD-WAN Device: config loss on software upgrade attempt
CSCvz37340	The [service timestamps log datetime msec localtime] command cannot be pushed via CLI Addon template
CSCwa45487	DNS packets gets injected improperly with sdwan system ip and dropped from Service VPN
CSCwa25256	Installing new enterprise wan edge cert does not remove old cert causing device to use old cert
CSCwa92082	RG B2B(Box to Box), Interchassis HA, STBY is stuck in STANDBY COLD-BULK on ISR 4461
CSCwb58468	17.8 Sig Autotunnels:tunnel 409 response received

Open Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.8.1a

Identifier	Headline
CSCwb52616	Cisco IOS XE Catalyst SD-WAN Device doesn't inject ping packets due to no route although data policy has nat vpn-0
CSCwb05743	Crash seen with umbrella config during soak run
CSCwb39098	Router crashed after new IPv6 address assigned when router use specific configuration
CSCwa97951	Basic feature template fails on ASR1001-HX with TenGig interface due to negotiation auto

Identifier	Headline
CSCwb13820	C8Kv crashed at high scale with IPSEC and heavy features configured
CSCwb42807	After Enforce Software Version (ZTP) completed successfully, it automatically rolled-back
CSCwb03455	Inter-vrf route leaking not working and packet drop seen due to Ipv4Unclassified
CSCwb37587	ping failure in case of ipv4 overlay ipv6 underlay setup for some ip addresses from vm5 to vm6
CSCwb57058	Cisco IOS XE Catalyst SD-WAN Device can't establish data plane over L3 TLOC extension
CSCwb43423	Cisco IOS XE Catalyst SD-WAN Device: IOS XE image installation fails
CSCwa49721	Cisco SD-WAN HUB with firewall configured incorrectly dropping return packets when routing between VRFs
CSCwb18223	SNMP v2 community name encryption problem
CSCwa94665	Traffic getting dropped on Fugazi when AppQoE and Umbrella DNS is configured.
CSCwb16723	Traceroute not working on Cisco IOS XE Catalyst SD-WAN Device with NAT
CSCwa47197	IPsec destination IP does not get set
CSCwa98545	Checks of route leaks creates memory corruption.
CSCvy23366	C8300-2N2S + UCSE: Kernel crash on C8300-2N2S with UCSE module.
CSCwb34131	Cisco SDWAN 17.8 - Cisco IOS XE Catalyst SD-WAN Device 1002-HX > FTMd crash upon upgrade to 03/21 build
CSCwb33625	Cisco vManage: Speed Test Not working for ISR1100-4g and C8300 devices
CSCwb32635	17.6.2 Cisco IOS XE Catalyst SD-WAN Device - vdaemon file is incomplete when running admin-tech
CSCwb51595	Missing IOS config (voice translation rule) on upgrade from 17.3 to 17.6
CSCwb57437	17.3.5 - tracker stale probe present in router
CSCwb18315	Umbrella DNS security policy doesn't work with Cloud onRamp
CSCwb44275	Simulated flows with PPPoE with NAT DIA result in crash consistently over Utah platform
CSCwb31678	Custom applications are disabled for policy when NBAR is activated for the first time
CSCwb32934	uCPE8200 does not use QAT when malloc failure

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 SD-WAN Device Compatibility.

Cisco vManage GUI Changes

This section presents a comparative summary of the significant changes between Cisco vManage 20.7.x and earlier releases, and Cisco vManage Release 20.8.1.

Change in Control Labels

In Cisco vManage Release 20.8.1, the labels of the following UI elements have changed:

- **DPI** to **SAIE**: The deep packet inspection (DPI) flow is now called the SD-WAN Application Intelligence Engine (SAIE) flow. As a result, all UI elements related to DPI have been renamed as SAIE.

Figure 1: Example of Labels with DPI in Cisco vManage 20.7.x and Earlier Releases

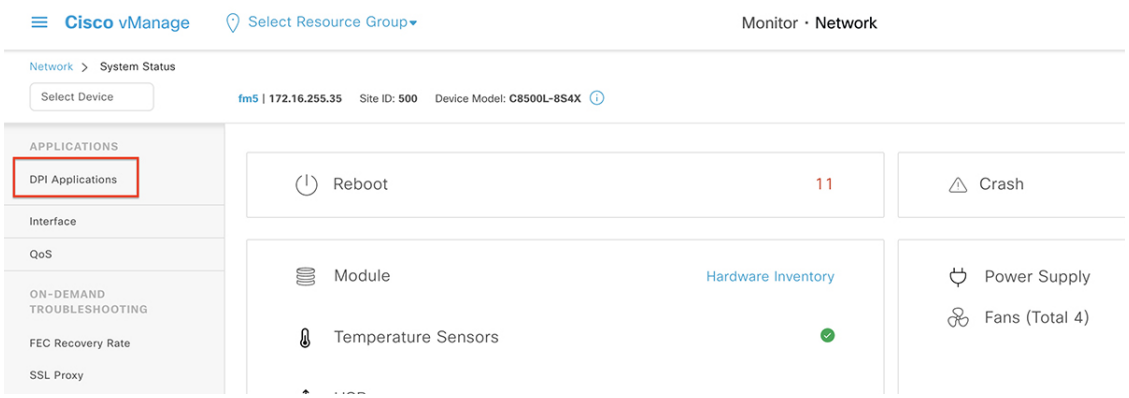
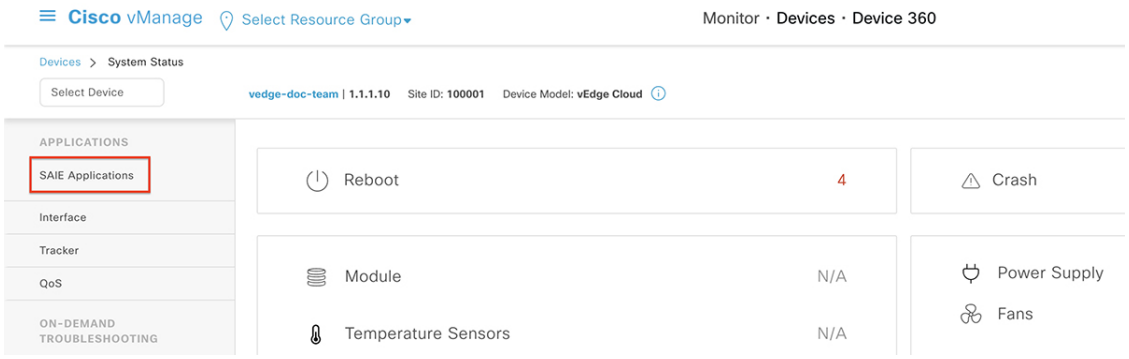


Figure 2: Example of Labels with SAIE in Cisco vManage Release 20.8.1



- **Device** to **Device Templates** (**Configuration** > **Templates**)

Figure 3: Device Tab in Cisco vManage 20.7.x and Earlier Releases

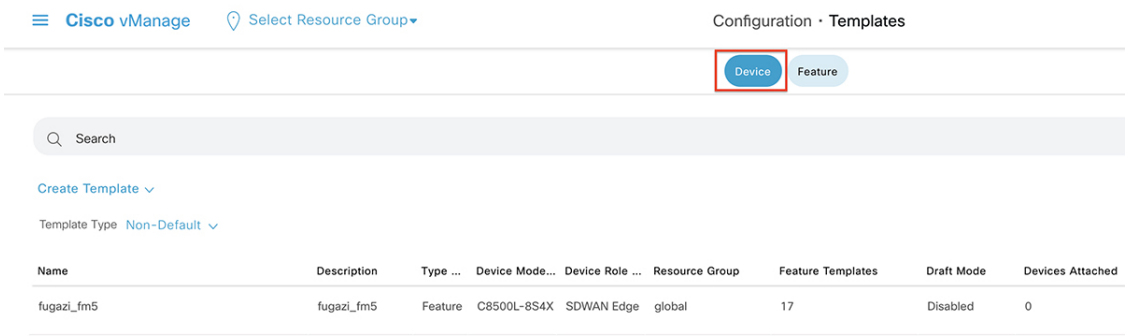
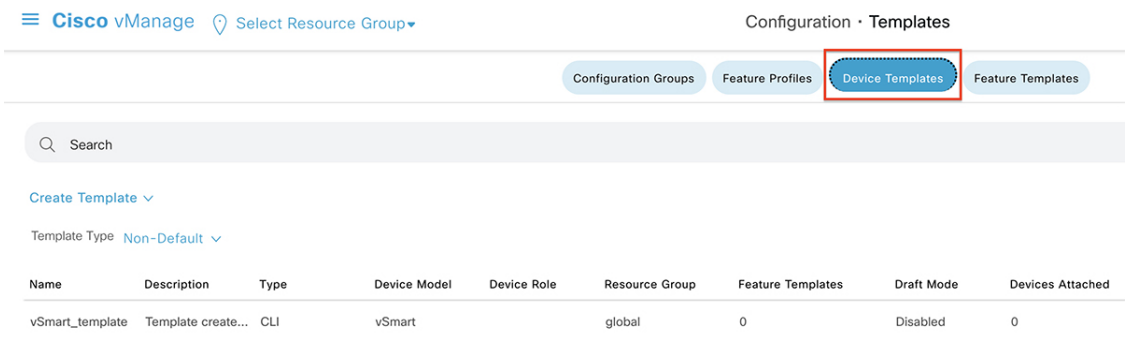


Figure 4: Device Templates Tab in Cisco vManage Release 20.8.1



- **Feature** to **Feature Templates** (**Configuration** > **Templates**)

Figure 5: Feature Tab in Cisco vManage 20.7.x and Earlier Releases

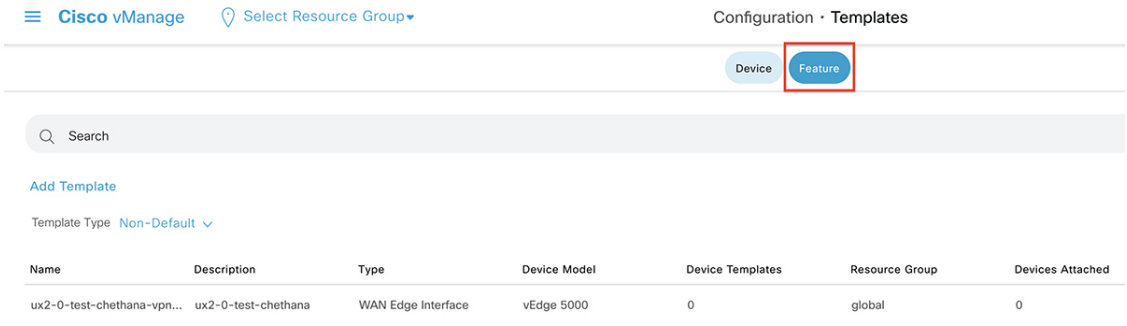
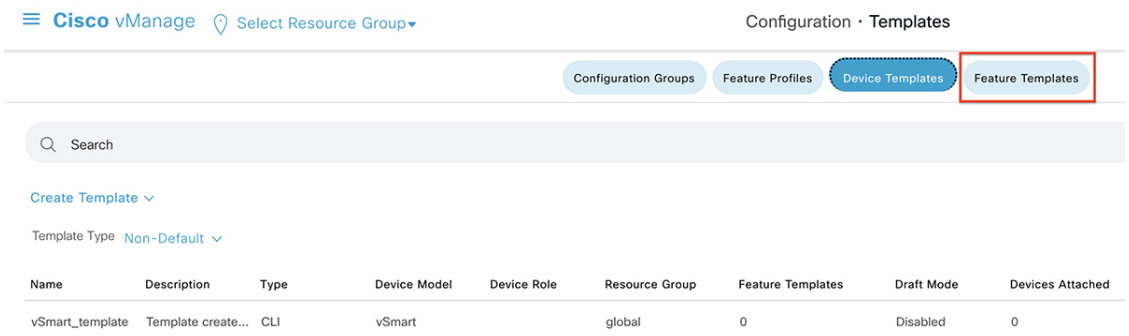


Figure 6: Feature Templates Tab in Cisco vManage Release 20.8.1



Support for Web Content Accessibility Guidelines (WCAG) 2.1 Standard

Cisco vManage Release 20.8.1 supports Web Content Accessibility Guidelines (WCAG) 2.1 standard for the AA conformance level, with the following limitations:

Table 2:

WCAG Success Criterion	Support	Limitation
2.1.2: No Keyborad Trap	Not Supported	You cannot exit from SSH terminal using the keyboard.
2.4.5: Multiple Ways	Not Supported	You can locate pages on Cisco SD-WAN Manager using only one method.
1.1.1: Non-text Content	Partially Supported	Cisco SD-WAN Manager partially supports alternative text.
1.3.1, 3.3.1, 3.3.2, and 4.1.3: Screen Reader	Partially Supported	Cisco SD-WAN Manager partially supports screen reader for annoucements, error messages and data tables.
1.3.5: Identify Input Purpose	Partially Supported	Some input fields which collect personal information are not entirely supported by identify input purpose.
1.4.1: Use of color	Partially Supported	Cisco SD-WAN Manager uses colors to convey certain information and is partially compliant with WCAG 2.1 criterion for the use of colors.

WCAG Success Criterion	Support	Limitation
1.4.3: Contrast	Partially Supported	Cisco SD-WAN Manager contains GUI elements that are not visible in the OS high contrast setting. Some text does not fully comply with the WCAG 2.1 color contrast ratio standards.
1.4.4: Resize text	Partially Supported	Cisco SD-WAN Manager partially supports browser resize text functionality.
1.4.10: Content reflow	Partially Supported	Cisco SD-WAN Manager partially supports content reflow.
1.4.11: Non-text contrast	Partially Supported	Cisco SD-WAN Manager partially supports non-text contrast ratio of 3:1.
1.4.13: Content on hover or focus	Partially Supported	Cisco SD-WAN Manager partially supports content on hover or focus.
2.1.1: Keyboard	Partially Supported	Cisco SD-WAN Manager elements provide partial support to access the elements using the keyboard.
2.4.2: Page titled	Partially Supported	Cisco SD-WAN Manager does not have meaningful page titles.
2.4.3: Focus order	Partially Supported	Some elements in Cisco vManage do not have a logical focus order.
2.4.4: Link purpose (in-context)	Partially Supported	Cisco SD-WAN Manager partially supports link purpose (in context).
2.4.6: Headings and labels	Partially Supported	Cisco SD-WAN Manager partially supports label in name.
2.4.7: Focus visible	Partially Supported	Cisco SD-WAN Manager partially supports visible focus indicator.
2.5.3: Label in name	Partially Supported	Cisco SD-WAN Manager contains some accessible names that do not match with their visible label.
4.1.1: Parsing	Partially Supported	Some GUI elements do not have a unique ID on a page.
4.1.2: Name, role, value	Partially Supported	Cisco SD-WAN Manager contains some elements that do not have corrected names and roles.

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

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.