Release Notes for Cisco Catalyst SD-WAN Control Components Release 20.8.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

- 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 Catalyst SD-WAN Control Components Release 20.8.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 SD-WAN Control Components, Release 20.8.x, which provides Cisco Catalyst 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 SD-WAN Manager.

Related Releases

For release information about Cisco IOS XE Catalyst SD-WAN devices, refer to Release Notes for Cisco IOS XE Catalyst SD-WAN device, Cisco IOS XE Catalyst SD-WAN Release 17.8.x.

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

What's New for Cisco Catalyst SD-WAN Control Components Release 20.8.x

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.

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.

Table 1: Cisco IOS XE Release 17.8.1a

Feature	Description
Cisco SD-WAN Getting Started Guide	

Feature	Description
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.
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	

Feature	Description
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.
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.

Feature	Description
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.
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.

Feature	Description
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)
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.

Feature	Description
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.

What's New for Cisco SD-WAN Release 20.8.x

This section applies to Cisco vEdge devices.

Table 2: Cisco SD-WAN Release 20.8.1

Feature	Description
Routing	
Verify OMP routes prefix	The verify keyword is added to "show omp route <prefix>" CLI to validate the availability of route on Cisco vEdge devices.
Policies	
Policy Checker on Cisco vSmart Controller	The test policy CLI enables you to troubleshoot large policies with numerous sequence numbers. This command identifies and displays the sequence number that matches a particular input variable and a policy name on Cisco vSmart Controllers.
Security	
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.
Single Sign-On Using Azure AD	Single Sign-On (SSO) with security assertion mark-up language (SAML) gives faster, easier, and trusted access to cloud applications without storing passwords or requiring you to log in to each application individually.
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.
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.
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: 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.

Important Notes, Known Behavior, and Workaround

- From Cisco SD-WAN Release 20.4.1.1, Microsoft Azure environment is supported for deploying Cisco SD-WAN controllers (Cisco vBond orchestrator, Cisco vSmart controller, and Cisco vManage). The support is limited to Cisco SD-WAN cloud-based deployments only.
- If SD-AVC is enabled using Cloud Connector or custom applications while upgrading from Cisco vManage Release 20.3.1 to Cisco vManage Release 20.6.1 and later releases, during the upgrade, a defect CSCwd35357 is impacting the data plane. We strongly recommend you to contact the Cisco TAC to perform a workaround while upgrading.

- Starting from Cisco SD-WAN Release 20.8.1, the unknown mandatory attributes from TACACS are not allowed. The authorization fails, when a client receives the configurations with the arguments that are not supported. For information about configuring ISE for Cisco SDWAN devices, see RADIUS and TACACS-Based User Authentication and Authorization.

Cisco SD-WAN Manager Upgrade Paths

For information about Cisco SD-WAN Manager upgrade procedure, see Upgrade Cisco vManage Cluster.

Starting Cisco SD-WAN Manager Version	Destination Version							
	19.2.x	20.1.x	20.3.x	20.4.x	20.5.x	20.6.x	20.7.x	20.8.x
18.x/19.2.x	Direct Upgrade	Direct Upgrade		Step upgrade through 20.3.x	Step upgrade through 20.3.x	Step upgrade through 20.3.x	Step upgrade through 20.3.x	Step upgrade through 20.3.x

Starting Cisco SD-WAN Manager Version	Destination Version							
	19.2.x	20.1.x	20.3.x	20.4.x	20.5.x	20.6.x	20.7.x	20.8.x
			Check disk space* • If the disk space is more than 2GB: Direct Upgrade • If the disk space is less than 2GB: Step upgrade through 20.1 • If you are upgrading to 20.3.5, the available disk space should be at least 2.5 GB. For cluster upgrade procedure**: **request nms**					

Starting Cisco SD-WAN Manager Version	Destination Version							
	19.2.x	20.1.x	20.3.x	20.4.x	20.5.x	20.6.x	20.7.x	20.8.x
			configuration-db upgrade **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.					
20.1.x	Not Supported	Direct Upgrade	Direct Upgrade For cluster upgrade procedure**: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.	Direct Upgrade For cluster upgrade procedure**: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.	Step upgrade through 20.3.x	Step upgrade through 20.3.x	Step upgrade through 20.3.x	Step upgrade through 20.3.x

Starting Cisco SD-WAN Manager Version	Destination Version							
	19.2.x	20.1.x	20.3.x	20.4.x	20.5.x	20.6.x	20.7.x	20.8.x
20.3.x	Not Supported	Not Supported	Direct Upgrade	Direct Upgrade	Direct Upgrade For cluster upgrade procedure**: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.	Direct Upgrade For cluster upgrade procedure**: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.	Direct Upgrade For cluster upgrade procedure**: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.	Direct Upgrade For cluster upgrade procedure**: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.

Starting Cisco SD-WAN Manager Version	Destination Version							
	19.2.x	20.1.x	20.3.x	20.4.x	20.5.x	20.6.x	20.7.x	20.8.x
20.4.x	Not Supported	Not Supported	Not Supported	Direct Upgrade	Direct Upgrade For cluster upgrade procedure**: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.	Direct Upgrade For cluster upgrade procedure**: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.	Direct Upgrade For cluster upgrade procedure**: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.	Direct Upgrade For cluster upgrade procedure**: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.
20.5.x	Not Supported	Not Supported	Not Supported	Not Supported	Direct Upgrade	Direct Upgrade	Direct Upgrade	Direct Upgrade
20.6.x	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Direct Upgrade	Direct Upgrade	Direct Upgrade
20.7.x	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Direct Upgrade	Direct Upgrade	Direct Upgrade

*To check the free disk space using CLI,

1. Use the vshell command to switch to vshell.
2. In vshell, use the df -kh | grep boot command.

**Cluster upgrade must be performed using CLI

- Use the following command to upgrade the configuration database. This must be done on only one node in the cluster:

```
request nms configuration-db upgrade
```

Note We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.

- Enter login credentials, if prompted. Login credentials are prompted if all Cisco SD-WAN Manager server establish control connection with each other. After a successful upgrade, all configuration-db services are UP across the cluster and the application-server is started.Enter login credentials, if prompted. Login credentials are prompted if all Cisco SD-WAN Manager server establish control connection with each other. After a successful upgrade, all configuration-db services are UP across the cluster and the application-server is started.

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 SD-WAN Controllers Releases 20.8.1

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

Resolved Bugs for Cisco SD-WAN Controllers Releases 20.8.1

Identifier	Headline
CSCwb20107	Not able to change config-db credentials on 20.6.2
CSCwa39835	Clouddock cluster activation failure due to Cisco vManage sending CCM tasks to both CSPs
CSCwb27060	MT: If Cisco vEdge device is attached to device template during tagrule conflict it shows
CSCvz63280	Cisco vEdge Does Not Respond Properly to vSmart Policy Prefix-list Changes (CLI Policy)
CSCvz40247	Security policies applied to incorrect interface in cluster mode, iptables
CSCwa25355	20.7: Unreachable node still shows up in device list
CSCwa40924	Cisco vManage UI failed to update password
CSCwb21800	ST: Tag removed from devices , removed from tag management page but tag rule stays on config group

Identifier	Headline
CSCwa11465	Cloud Global Settings AWS subnet setting
CSCwa41127	Cisco vBranch: Cisco NFVIS upgrade shows "Failed to establish netconf session with device" in Cisco vManage Task Log
CSCvy59499	PNP portal is sending Cisco vManage subject serial for virtual devices such as CSR1000v and vEdge cloud
CSCvz47045	Edited security policy under main-template and this template rolled back to old one in UI
CSCvz03954	Cisco vManage clustering doesn't support CoRC (Colo/CloudDock)
CSCvz95054	System IP persists after invalidating the edge devices from the Cisco vManage which it is not connected .
CSCwb14837	Interface endpoint displayed as "null" when bfd session is between provider and tenant edge device
CSCwa71879	Config Group: WAN intf with Device Specific IP/Mask deploy failed
CSCvz66256	Filtering the data based on local tloc is returning no data in vmanage GUI for DPI stats
CSCwa13126	Device is online. Failed to attach configuration template : internal error.
CSCvz62234	Cisco Catalyst SD-WAN Manager Unauthorized Configuration Rollback Vulnerability

Open Bugs for Cisco SD-WAN Controllers Releases 20.8.1

Identifier	Headline
CSCwb52397	No option to setup cellular controller and profile during the CG creation using custom workflow
CSCwb43242	On Cluster setup, for one Node UI is not accessible, but app-server is running
CSCwb55773	Add CSP on MT cluster results in Failure
CSCwb23030	Cisco vManage GUI takes a long time to load when using Firefox
CSCwb48791	Config Group and device template both gets associated with device
CSCvy72764	services still communicate via old OOB IP after changing the vpn 0 OOB interface IP
CSCwb20070	20.8 : Disaster Recovery workflow fails during switchover
CSCwb37779	UX2.0: LAN Segment: Created two intf asso. the same VPN, device specific variables are duplicated
CSCwb43772	UX2.0: Tagging rule "Not contain" on new CG missing a device which previous deployed with another CG

Identifier	Headline
CSCwa90832	App-Server continuously restarting after the restore of config-db during Active-Backup Restore
CSCvz81664	Enabling or Disabling OMP Overlay AS Prevents Connected Routes from Being Advertised in OMP
CSCwb38655	Delete CSP(with CCM) followed by Add CSP - MT Cluster failed - Infra Exception
CSCwb48374	Unable to download admin-tech information whch is fetched from device by Cisco vManage
CSCwb48626	Quick Connect workflow still missing config group when tag is copied to a device
CSCwb65396	C1116-4P: CLI template push fails with error: 'Error: on line 48: line-mode single-wire line 0'
CSCwb60902	Umbrella stats file has incorrect format.
CSCwa56952	Unable to push radius server configuration

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.

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

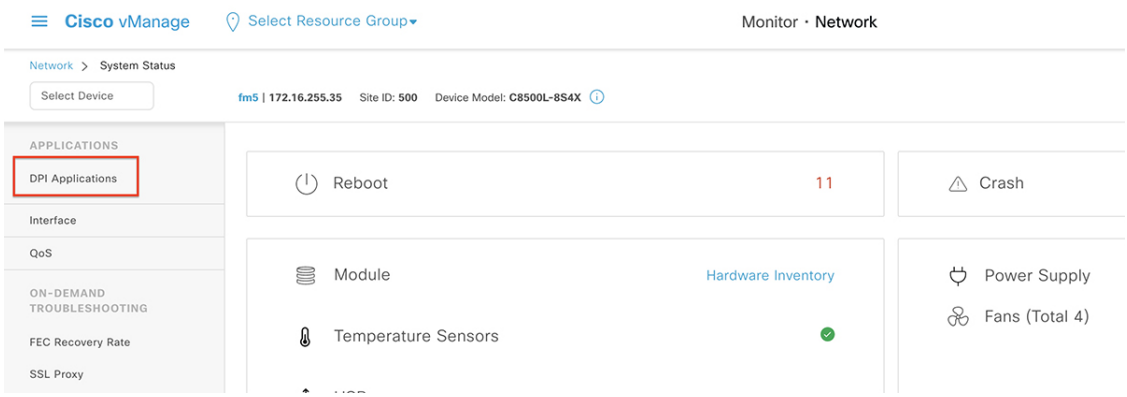
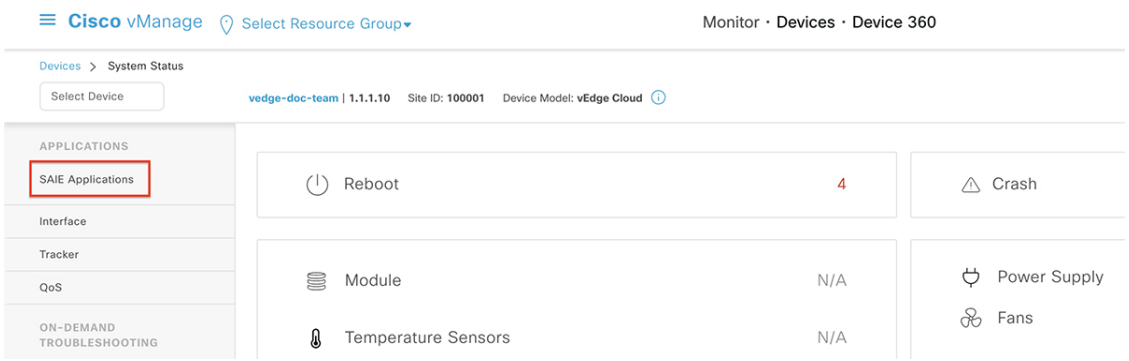


Figure 2: Example of Labels with SAIE in Cisco vManage Release 20.8.1



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

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

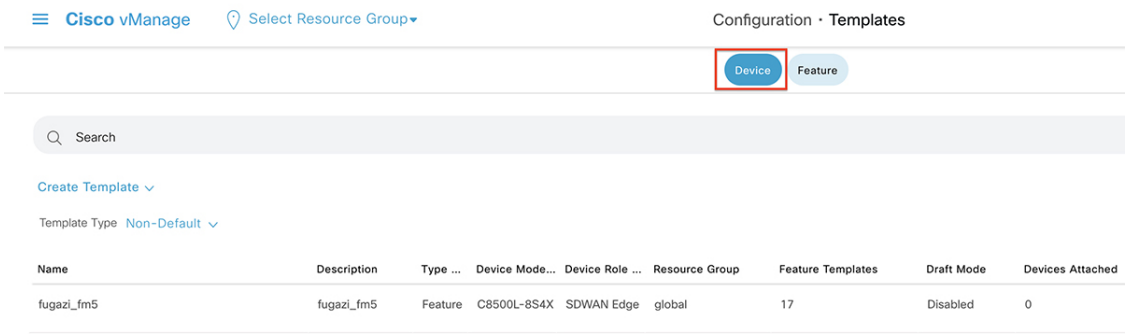
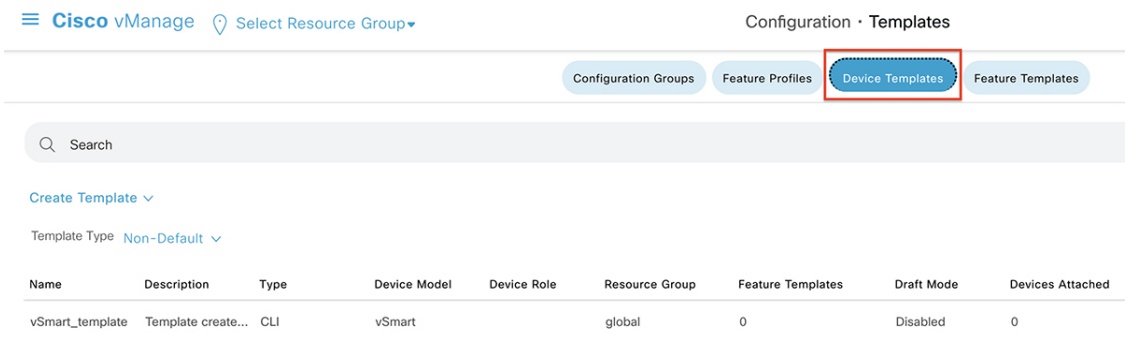


Figure 4: Device Templates Tab in Cisco vManage Release 20.8.1



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

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

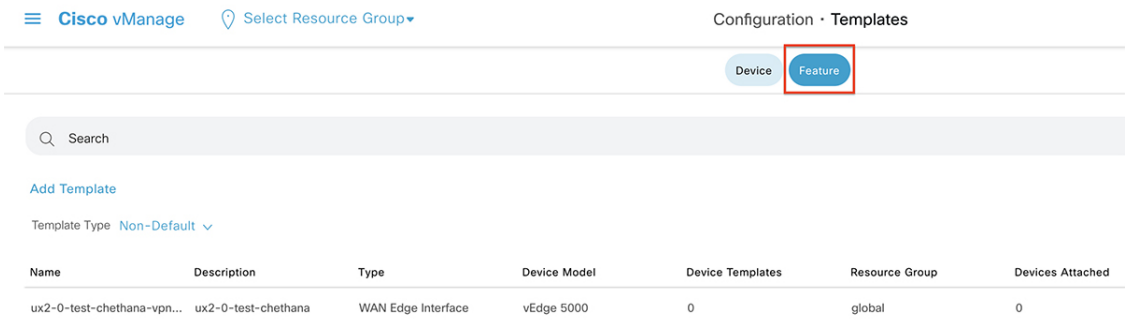
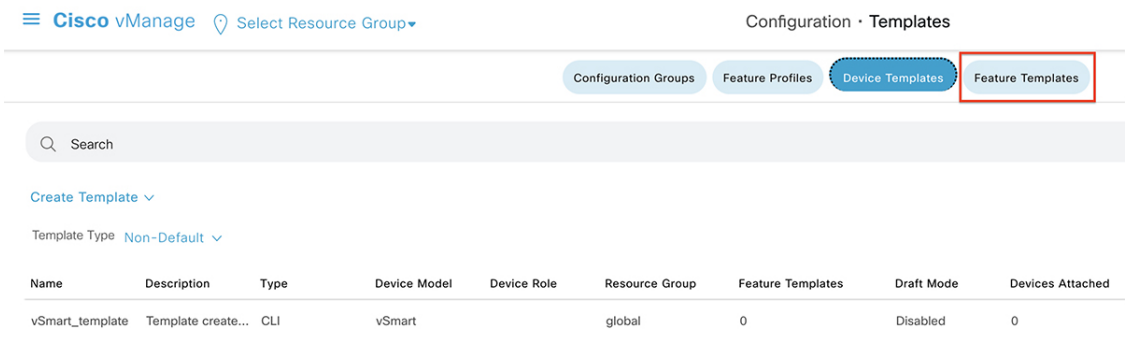


Figure 6: Feature Templates Tab in Cisco vManage Release 20.8.1



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 3:

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.

WCAG Success Criterion	Support	Limitation
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.
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.

WCAG Success Criterion	Support	Limitation
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 vEdge Routers
- Field Notices
- Recommended Releases
- Security Advisories
- Cisco Bulletins

Full Cisco Trademarks with Software License

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.