Release Notes for Cisco Catalyst SD-WAN Control Components Release 20.7.x

First Published: 2021-11-10

Last Modified: 2022-06-25

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**, and **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**. 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 20.7.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**, and **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**. 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 20.7.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 Devices, Cisco IOS XE Catalyst SD-WAN Release 17.7.x.

For release information about Cisco vEdge Devices, refer to Release Notes for Cisco vEdge Devices, Cisco SD-WAN Release 20.7.x.

What's New for Cisco Catalyst SD-WAN Control Components Release 20.7.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 17.7.x

This section applies to Cisco IOS XE Catalyst SD-WAN devices.

Table 1: Cisco IOS XE Release 17.7.1a

Feature	Description
Cisco SD-WAN Getting Started	

Feature	Description
Support for the Cisco Catalyst 8000V Edge Software Platform on OpenStack Train	This feature introduces support for managing a Cisco Catalyst 8000V Edge software platform hosted in the OpenStack cloud computing platform "Train" release.
Day 0 WAN Interface Automatic IP Detection using ARP	This feature enables a device to automatically learn about the available IP addresses and default gateway information when a DHCP server is not available. The device assigns an IP address to its WAN interface, and then contacts the PnP server and begins the PnP onboarding process.
Certificate Revocation	This feature revokes enterprise certificates from devices based on a certificate revocation list that Cisco SD-WAN Manager obtains from a root certificate authority.
DigiCert Migration	This feature replaces the Symantec Certificate Authority (CA) server with Digicert Certificate Authority server for signing the controller device certificates on Cisco SD-WAN controllers including Cisco vSmart Controller, Cisco vBond Orchestrator, and Cisco vManage. You can protect, verify, and authenticate the identities of organizations and domains using these certificates.
Cisco SD-WAN Systems and Interfaces	
Cisco Unified Border Element Configuration	This feature lets you configure Cisco Unified Border Element functionality by using Cisco IOS XE SD-WAN device CLI templates or CLI add-on feature templates.
Cisco ThousandEyes Support for Cisco 1000 Series Integrated Services Routers	You can deploy Cisco ThousandEyes Enterprise agent natively as a container application on Cisco ISR 1100X-6G devices.
Support for HSRP and HSRP Authentication on Cisco IOS XE SD-WAN Devices	This feature allows you to configure HSRPv2 and HSRP authentication on Cisco IOS XE SD-WAN platforms via CLI template. HSRP is a long-standing Cisco proprietary First Hop Redundancy Protocol (FHRP) to support version 2 of the protocol and authentication.
Added Support for Configuring Geofencing Using a Cisco System Feature Template	This feature adds support for configuring the geographical boundary of a device using a **Cisco System** feature template. With this feature, you can also configure automatic geolocation detection, where the device determines its own location, while configuring geofencing. A new parameter **auto-detect-geofencing-location** is added to the **geolocation (system)** command.
VRRP Interface Tracking for Cisco IOS XE SD-WAN Devices	This feature enables VRRP to set the edge as active or standby based on the WAN Interface or SIG tracker events and increase the TLOC preference value on a new VRRP active to ensure traffic symmetry, for Cisco IOS XE SD-WAN devices.

Feature	Description
TCP/UDP Endpoint tracker and Dual Endpoint Static route tracker for Cisco IOS XE SD-WAN devices	This feature enables you to configure the TCP/UDP individual Endpoint static route tracker and to configure tracker group with IPv4, TCP/UDP Dual Endpoint static route trackers for service VPNs to enhance the reliability of the probes.
DHCP for IPv6	This feature allows you to configure DHCP for IPv6 (DHCPv6) on Cisco IOS XE SD-WAN devices to assign IPv6 addresses to hosts on an IPv6-enabled network. Assigning of IPv6 addresses is accomplished using SLAAC, DHCPv6 with SLAAC, DHCPv6 with SLAAC, DHCPv6 Prefix Delegation, or DHCPv6 Relay. A Cisco IOS XE SD-WAN device can be configured for DHCPv6 as a DHCP server, DHCP client, or as a DHCP relay agent.
Hierarchical SD-WAN	Hierarchical SD-WAN provides the ability to divide the architecture of the Cisco SD-WAN overlay network into multiple regional networks that operate distinctly from one another, and a central core-region network for managing inter-regional traffic. The hierarchical architecture enables you to use different traffic transport service providers for each region, and for the central core-region network, to optimize cost and traffic performance. It also simplifies traffic configuration for some scenarios, and provides a robust, adaptive topology that can help prevent routing failures in specific network scenarios.
Co-Management: Granular Role-Based Access Control for Feature Templates	This feature introduces greater granularity in assigning role-based access control (RBAC) permissions for template use. This enables you to give a tenant self-management of network configuration tasks. Network administrators and managed service providers can use this feature to assign permissions to their end customers.
Cisco SD-WAN Routing	
RIPv2 support on Cisco IOS XE SD-WAN Devices	This feature enables you to configure RIPv2 on Cisco IOS XE SD-WAN devices. Routers redistribute RIPv2 routes to OMP for advertisement in the SD-WAN overlay and to OSPFv3 for service-side routing.
Cisco SD-WAN Policies	
Configure Default AAR and QoS Policies	This feature is an enhancement to the centralized and localized policies feature. This feature allows you to configure default application-aware routing (AAR) and quality of service (QoS) policies on Cisco IOS XE devices.
Flexible Netflow for VPN0 Interface	This feature supports Netflow on VPN0 interfaces. Flexible Netflow acts as a security tool, enables exporting data to Cisco vManage and detects attacks on devices and monitors traffic.
Cisco SD-WAN Security	

Feature	Description
Configure Interface Based Zones and Default Zone	This feature enables you to configure an interface-based firewall policy to control traffic between two interfaces or an interface-VPN-based firewall policy to control traffic between an interface and a VPN group. This feature also provides support for default zone where a firewall policy can be configured on a zone pair that consist of a zone and a default zone.
Resource Limitations and Device-global Configuration Options	This feature enables you to define resource limitation options such as idle timeout and session limits, and device-global options in the policy summary page to fine-tune a firewall policy behaviour after a firewall policy is implemented in Cisco SD-WAN.
Unified Logging for Security Connection Events	This feature supports Unified Logging which is used to capture information about connection events across different security features at different stages during policy enablement and execution. With Unified Logging, you can have visibility to the log data for Zone-based Firewall and for Unified Threat Defense features such as IPS, URL-F and AMP to understand what traffic, threats, sites or malware were blocked, and the rules that blocked the traffic or sessions with the associated port, protocol or applications. Additionally, this feature also provides support for On-Demand Troubleshooting. On-Demand troubleshooting allows a user to view the connection events of different flows of traffic from a device within a configured period of time.
GRE Over IPsec Tunnels Between Cisco IOS XE Devices	This feature allows you to set up GRE over IPsec tunnels with IKEv2 RSA-SIG authentication on Cisco IOS XE SD-WAN devices in the controller mode to connect to Cisco IOS XE devices in the autonomous mode. This set up enables Cisco IOS XE SD-WAN devices to use OSPFv3 as the routing protocol and multicast traffic across the WAN network. You can configure GRE over IPsec tunnels using the CLI device templates in Cisco vManage.
High Availability	
Disaster Recovery User Password Change	This feature lets you change the disaster recovery user password for disaster recovery components from the Cisco vManage **Disaster Recovery** window.
Cisco SD-WAN Cloud OnRamp	
Cloud onRamp for SaaS Support for Webex	Added Webex to the list of cloud applications for which Cloud onRamp for SaaS can determine the best network path to the cloud server. Cisco vManage periodically downloads a list of Webex servers organized by geographic region. Cloud onRamp for SaaS uses this server list to help calculate the best network path for Webex traffic in different regions.

Feature	Description
Support for Using Microsoft Telemetry Metrics for Microsoft 365 SharePoint and Teams Traffic.	This feature adds support for using Microsoft telemetry metrics for Microsoft 365 SharePoint and Teams (Skype). Cloud onRamp for SaaS uses the metrics data when determining the best path for Office 365 traffic.
Azure Scaling, Audit, and Security of Network Virtual Appliances	This feature allows you to edit the SKU Scale value, carry out the audit to identify discrepancies, and have better security for your Network Virtual Appliances (NVAs).
Support for Cisco VM Image Upload in qcow2 Format	This feature allows you to upload a virtual machine image to Cisco vManage in qcow2 format. Earlier, you could upload only a prepackaged image file in tar.gz format.
Packet Capture for Cloud onRamp Colocation Clusters	This feature lets you capture packets at either the physical interface level (PNIC) or the virtual interface level (VNIC) on a CSP device of a colocation cluster. You can capture packets on one or more PNICs or VNICs on the same device or different devices with different browsers at the same time. This feature lets you gather information about the packet format and therefore helps in application analysis, security, and troubleshooting.
Cisco SD-WAN Monitor and Maintain	
Additional Diagnostics Information Added to Admin-Tech File	This feature enhances the output of the admin-tech file with additional diagnostics information collected from the application server, the configuration database, the statistics database, and other internal services.
Upload an Admin-Tech File to a TAC Case	This feature enables you to upload an admin-tech file directly from Cisco vManage when opening a TAC case. When you create a TAC case, you can upload the generated admin-tech files to TAC service requests (SRs) from Cisco vManage. This streamlines the steps required for working with TAC to troubleshoot a problem.
Bidirectional Packet Capture for Cisco IOS XE SD-WAN Devices	This feature enhances the embedded packet capture functionality to support bidirectional packet capture through Cisco vManage.
Software Upgrade Using a Remote Server	This feature enables you to upgrade device or controller software using software images stored on a remote server. The feature enables you to register a remote server with Cisco vManage, and add locations of software images on the remote server to the Cisco vManage software repository. When you upgrade device or controller software, the device or controller can download the new software image from the remote server. This feature also improves the listing of images available in the repository. When two or more images have the same version but different filenames, each image is listed as a separate entry.

Feature	Description
Enhanced Cisco vManage User Interface for a Consolidated Monitoring View	This feature introduces the enhanced user interface of Cisco SD-WAN Manager. The **Monitor** window provides a single-page, real-time user interface that facilitates a consolidated view of all monitoring components and services of a Cisco Catalyst SD-WAN overlay network. It provides an entry point for all Cisco SD-WAN Manager dashboards, including **Main Dashboard**, **VPN Dashboard**, **Security**, and **Multicloud**. These dashboards were earlier accessible from the **Dashboard** menu. In addition, all monitoring components have been organized into pill buttons in the user interface so that you can quickly navigate from one page to another. The **Tools** menu of Cisco SD-WAN Manager has also been enhanced in this release. The **Network Wide Path Insight** and **On Demand Troubleshooting** options that were earlier accessible from the **Monitor** menu have now been moved to the **Tools** menu so that you can easily locate these features.
Cisco SD-WAN SNMP	
Support for SNMPv3 AES-128 and AES-256 bit Encryption Protocol	This feature allows you to configure SNMPv3 users in support with SHA-1 authentication protocol and AES-128 and AES-256 encryption on Cisco IOS XE SD-WAN devices.
Cisco SD-WAN NAT	
Dual Endpoint Support for Interface Status Tracking on Cisco IOS XE SD-WAN Devices	This feature allows you to configure tracker groups with dual endpoints using the Cisco System template and associate each template group to an interface. The dual endpoints provide redundancy for tracking the status of transport interfaces to avoid false negatives.
Intra-VPN Service-Side NAT Support	Intra-VPN allows service-side LAN interfaces to communicate with other service-side LAN interfaces within the same VPN. Configure the **ip nat outside** command on the LAN interface for which you require translation of the source IP addresses to the outside local addresses. You can apply static or dynamic NAT rules for packets to be routed from other LAN interfaces to the interface configured as the outside interface. You configure intra-VPN service-side NAT using a device CLI template or a CLI add-on template.
NAT66 DIA Support	The IPv6-to-IPv6 Network Address Translation (NAT66) Direct Internet Access (DIA) feature enables an IPv6 device to translate an inside source address prefix to an outside source address prefix in IPv6 packet headers. NAT66 DIA allows you to direct local IPv6 internet traffic to exit directly to the internet from the service-side VPN (VPN 1) through the transport VPN (VPN 0). You configure NAT66 DIA using Cisco vManage, the CLI, or a device CLI template. This feature introduces new CLI commands. For more information, see the Cisco IOS XE SD-WAN Qualified Command Reference Guide.
Cisco SD-WAN Remote Access	

Feature	Description
SD-WAN Remote Access	Remote access refers to enabling secure access to an organization's network from devices at remote locations. Cisco Catalyst SD-WAN remote access (SD-WAN RA) integrates remote access functionality into Cisco Catalyst SD-WAN. SD-WAN RA enables Cisco IOS XE Catalyst SD-WAN devices to function as RA headends, managed through Cisco SD-WAN Manager. This eliminates the need for separate Cisco Catalyst SD-WAN and RA infrastructure, and enables rapid scalability of RA services. RA users can use the same software- or hardware-based RA clients as with solutions that do not integrate with Cisco Catalyst SD-WAN. For RA users, benefits include extending Cisco Catalyst SD-WAN features to remote users. RA users can access applications hosted on-premises, applications hosted in IaaS, SaaS applications, or the internet

What's New for Cisco SD-WAN Release 20.7.x

This section applies to Cisco vEdge devices.

Table 2: Cisco SD-WAN Release 20.7.1

Feature	Description
Cisco SD-WAN Getting Started	
Day 0 WAN Interface Automatic IP Detection using ARP	This feature enables a device to automatically learn about the available IP addresses and default gateway information when a DHCP server is not available. The device assigns an IP address to its WAN interface, and then contacts the PnP server and begins the PnP onboarding process.
Certificate Revocation	This feature revokes enterprise certificates from devices based on a certificate revocation list that Cisco SD-WAN Manager obtains from a root certificate authority.
DigiCert Migration	This feature replaces the Symantec Certificate Authority (CA) server with Digicert Certificate Authority server for signing the controller device certificates on Cisco SD-WAN controllers including Cisco vSmart Controller, Cisco vBond Orchestrator, and Cisco vManage. You can protect, verify, and authenticate the identities of organizations and domains using these certificates.
Systems and Interfaces	
TCP/UDP Endpoint tracker and Dual Endpoint Static route tracker for Cisco vEdge devices	This feature enables you to configure the TCP/UDP individual Endpoint static route tracker and to configure tracker group with IPv4, TCP/UDP Dual Endpoint static route trackers for service VPNs to enhance the reliability of the probes.
VRRP Interface Tracking for Cisco vEdge Devices	This feature enables VRRP to set the edge as active or standby based on the WAN Interface or SIG tracker events and increase the TLOC preference value on a new VRRP active to ensure traffic symmetry, for Cisco vEdge devices. Starting this release, you can configure it through Cisco vManage feature template.

Feature	Description
Co-Management: Granular Role-Based Access Control for Feature Templates	This feature introduces greater granularity in assigning role-based access control (RBAC) permissions for template use. This enables you to give a tenant self-management of network configuration tasks. Network administrators and managed service providers can use this feature to assign permissions to their end customers.
Policies	
Configure Default AAR and QoS Policies	This feature is an enhancement to the centralized and localized policies feature. This feature allows you to configure default application-aware routing (AAR) and quality of service (QoS) policies on Cisco IOS XE devices.
High Availability	
Disaster Recovery User Password Change	This feature lets you change the disaster recovery user password for disaster recovery components from the Cisco vManage **Disaster Recovery** window.
Cloud OnRamp	
Cisco CXP Gateway Support for Internet Exit through Service VPN Interfaces	This feature adds support for enabling SaaS in service VPN interfaces in Gateway sites.
Support for Cisco VM Image Upload in qcow2 Format	This feature allows you to upload a virtual machine image to Cisco vManage in qcow2 format. Earlier, you could upload only a prepackaged image file in tar.gz format.
Packet Capture for Cloud onRamp Colocation Clusters	This feature lets you capture packets at either the physical interface level (PNIC) or the virtual interface level (VNIC) on a CSP device of a colocation cluster. You can capture packets on one or more PNICs or VNICs on the same device or different devices with different browsers at the same time. This feature lets you gather information about the packet format and therefore helps in application analysis, security, and troubleshooting.
Cisco SD-WAN Monitor and Maintain	
Additional Diagnostics Information Added to Admin-Tech File	This feature enhances the output of the admin-tech file with additional diagnostics information collected from the application server, the configuration database, the statistics database, and other internal services.
Upload an Admin-Tech File to a TAC Case	This feature enables you to upload an admin-tech file directly from Cisco vManage when opening a TAC case. When you create a TAC case, you can upload the generated admin-tech files to TAC service requests (SRs) from Cisco vManage. This streamlines the steps required for working with TAC to troubleshoot a problem.

Feature	Description
Resource Monitoring on Cisco SD-WAN Controllers and Cisco vEdge Devices	With this feature, you can configure usage watermarks for resources such as CPU, memory, and disk on Cisco SD-WAN controllers and Cisco vEdge devices. In addition, on Cisco vManage servers, you can configure watermarks to monitor disk read and write speeds. Devices poll the resource usage and notify events to Cisco vManage. Cisco vManage raises alarms to alert you to changes in resource usage, or disk read or write speed so that you can take any necessary corrective action.
Software Upgrade Using a Remote Server	This feature enables you to upgrade device or controller software using software images stored on a remote server. The feature enables you to register a remote server with Cisco vManage, and add locations of software images on the remote server to the Cisco vManage software repository. When you upgrade device or controller software, the device or controller can download the new software image from the remote server. This feature also improves the listing of images available in the repository. When two or more images have the same version but different filenames, each image is listed as a separate entry.
Enhanced Cisco vManage User Interface for a Consolidated Monitoring View	This feature introduces the enhanced user interface of Cisco SD-WAN Manager. The **Monitor** window provides a single-page, real-time user interface that facilitates a consolidated view of all monitoring components and services of a Cisco Catalyst SD-WAN overlay network. It provides an entry point for all Cisco SD-WAN Manager dashboards, including **Main Dashboard**, **VPN Dashboard**, **Security**, and **Multicloud**. These dashboards were earlier accessible from the **Dashboard** menu. In addition, all monitoring components have been organized into pill buttons in the user interface so that you can quickly navigate from one page to another. The **Tools** menu of Cisco SD-WAN Manager has also been enhanced in this release. The **Network Wide Path Insight** and **On Demand Troubleshooting** options that were earlier accessible from the **Monitor** menu have now been moved to the **Tools** menu so that you can easily locate these features.
Cisco SD-WAN Command Reference	
OMP CLI Enhancements	This feature displays detailed information about OMP and TLOC routes on Cisco vSmart Controllers and Cisco vEdge devices. The following commands are enhanced to display received and advertised peering sessions for OMP. show omp routes show omp tlocs

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.

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
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

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
			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 configuration-db upgrade**				

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
			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 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

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**
20.3.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.

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
20.4.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.
20.5.x	Not Supported	Not Supported	Not Supported	Not Supported	Direct Upgrade	Direct Upgrade	Direct Upgrade
20.6.x	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	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 one node only 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 vManage 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 20.7.2

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 20.7.2

Identifier	Headline
CSCwb09564	Inability to add Device Specific names for CUCM Feature Template
CSCwb03477	Cisco vManage GUI going blank seeing HTTP 403 error
CSCwa99132	Duplicate records from device need to be ignored by vmanage before feeding to ES
CSCwa83227	Smart Account Device Sync Service task page is not loading in tenant view
CSCwa21715	When a certificate file already installed is uploaded by mistake, vM will invalidate its cert status
CSCvz67260	Generate Bootstrap Configuration for c8300 is not working, Cisco vManage 20.6.1
CSCwa73847	Cannot configure FXO voice port in Cisco vManage
CSCvz89460	HSDWAN: All region BRs are seen in partial connections on Cisco vManage
CSCwa79465	MT Cisco vManage 20.6.2 problem with users when Tacacs/Radius is enable for Provider Level
CSCvz78622	Change user groups from operator to netadmin fails
CSCwb06267	Cisco vManage reports error when configure bgp regex ^6511$ or _4$ (in as-path list)

Identifier	Headline
CSCwa79364	MT : Error in vEdgeList upload when uploading list manually or do sync from Smart Account
CSCvz94716	Unable to set multiple ip addresses for DHCP options
CSCwa50177	Unable to change Ipsec interval from feature based template
CSCvy92487	Control connection to the vBond failing because of ERR_SER_NUM_NT_PRESENT on the vBond.
CSCwa02972	Restrict feature of NAT DIA policy do not working when used with app-list
CSCwa25320	20.7: Cisco IOS XE Catalyst SD-WAN device Interface Statistics do not change regardless of which interval is chosen
CSCwb08565	Tenant Export Backup task page is not loading in tenant view
CSCwb10590	After upgrade Cisco vManage to 20.6.2 ZTP task failed
CSCvz28451	"request nms update-internal-ip new-ip" does not work on Cisco vManage 20.3.4
CSCvz94221	Cisco vManage showing '1 invalid' certificate status on dashboard
CSCwa54712	Evaluation of sd-wan for Log4j 2.x DoS vulnerability fixed in 2.17
CSCvz89536	[MSDC] 20.6.2: API delay of 90+ seconds in displaying Real Time Tunnel statistics
CSCwb62862	vSmarts OMP peerings flap with devices when taking admin tech on all vSmarts
CSCwa61498	Pushing wan edge list fails to Cisco vManage cluster nodes when tacacs user set for controllers
CSCwa60823	Unable to add Cellular Gateway CG522-E to vManage.
CSCwa87469	Enabled usage but prepaid consumption
CSCwa85813	Cisco vManage central policy push times out
CSCwa56750	MTT, site/node level alarm are missing when manually shutdown / re-start edge device
CSCwa25177	Unable to install certificate on ISRv device due to autogenerated configuration in Cisco vManage
CSCwa24042	Connection Events page is not getting loaded as api throwing 500 Internal error
CSCvy07698	20.4 Getting Wrong Control Site Down Alarm alarms
CSCvz60918	Device template push fail after ISRv comes up and online
CSCwa34632	HTTP Proxy: Unable to update IPS signature using proxy config in vmanage
CSCwa25290	20.7: vQOE score for WebEx application is low in Cisco vManage due to high latency in device

Identifier	Headline
CSCvy56278	Cisco vManage crashed due to kernal panic [20.3.3.1.2]
CSCvz98754	Cisco vManage Access Control List is providing option to fulfill the VRF id
CSCwa96700	License Management page shows vBond along with edge devices in the device list-20.7
CSCwa23351	NWPI fail to merge domain/IP for dual Cisco IOS XE Catalyst SD-WAN device site
CSCwb37899	CoR Multicloud for GCP Site-to-Cloud CGW Deployment fails with Code 400 in S2S non supported region
CSCwa18550	cannot upgrade Cisco IOS XE Catalyst SD-WAN device with "Invalid Response" error
CSCwa92964	Src Script issue in Angular JS in 20.6 Main Dashboard: UN>15 char overflow the limt set
CSCwa73732	CLI request nms server-proxy update-ratelimit-config is broken on 20.6 due to python 3 version

Open Bugs for Cisco SD-WAN Controllers Releases 20.7.2

Identifier	Headline
CSCwb65034	Search for tunnel is not working
CSCwc23260	CXP : Cisco vManage not pushing probe color when new color added to color list.
CSCwa39457	"Enforce Software Version (ZTP)" does not support version format for NFVIS-SDWAN-BRANCH
CSCvy72764	Services still communicate via old OOB IP after changing the vpn 0 OOB interface IP
CSCvz81664	Enabling or Disabling OMP Overlay AS Prevents Connected Routes from Being Advertised in OMP
CSCwb68441	VPN drop menu shows empty in NWPI when we iniiate trace for first time
CSCvz62751	Cisco vManage: Noticed RouteMap attribute modification failure , while attempting through CLI Template

Bugs for Cisco SD-WAN Controllers Release 20.7.1

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 Release 20.7.1

Bug ID	Description
CSCvz55034	Cisco vManage 20.6.1 Dashboard does not show custom application server logo

Bug ID	Description
CSCvz68624	Login to Cisco SD-WAN OS fails if plain-text password was set in cloud-init write_files
CSCvz80036	vEdge: google-accounts getting classified as google-services in DPI Application
CSCwa04434	CSR generation failure and incomplete error message
CSCvz06108	Enhancement: Cisco VPN Interface IPsec template does not DH group 2 as option
CSCvz53305	Cisco vManage: Local device access policy with SNMP is not getting pushed correctly.
CSCvz46043	Device inventory sections shows incorrect count.
CSCvz94799	MTT : OptIn status is not updated to the Cisco IOS XE SD-WAN devices in a tenant
CSCvz60100	20.6: Cisco vManage UI stuck when we create a new device temp and create and attach a global temp at creat
CSCvz40568	Server error: illegal reference ncs devices
CSCvr52579	Cisco vManage network template allows vlan range "-" (vlan 71 - 75) on OVS network setting
CSCvz05132	CoR SaaS "vQoE Score History" not getting displayed for vEdge on Cisco vManage
CSCvy39849	Cisco vManage pushes invalid service route command
CSCvz49299	Cisco vManage services do not start on upgrade from 20.3 to 20.6 due to upgrade-context.json incorrect
CSCvz34413	Replication starts from time value 0, if the replication leader entry is not present in the replication status table
CSCvw20686	UUID lookup fail for vBond which behind NAT device while adding vBond in DR setup
CSCvz87812	Provide "Migrate Device" option in Cisco vManage UI before the device has been onboarded to Cisco vManage
CSCvz33123	Shared clouddock cluster activation shows FAILED after claiming its successful
CSCvy53930	Failed to create deviceactionstatusnode table entry in DB for device: Validation
CSCvz83966	Cisco vManage 20.4.2 - Interface template doesn't pushing encapsulation frame-relay
CSCvy73839	Cisco vManage is not compliant with RFC3411 when it generates the SNMP EngineID through feature template
CSCvz50700	Error occurred while generating report
CSCvz31054	Cisco vManage Tunnel States API is not backward compatible between 20.6 and 20.4.1
CSCvy92992	Unexpectedly redirect to previous provision device variable page when save config for another branch
CSCvz89195	CFGmgr crash on Cisco vManage when user added on GUI

Bug ID	Description
CSCvz25201	Intermittent Cisco vManage control up count mismatch
CSCvy83790	CCM config rejection does NOT cause Cluster to be marked in "Failed" State
CSCvz24023	Root cert sync not working for large scale deployments
CSCvz37973	SRST Feature Template "CUCM Media Resource Group" does not accept variable for field
CSCvz06952	vSmart crash on ompd process
CSCvz59356	Unexpected redirect to previous provisioned branch variable page on saving
CSCvy01378	Device Specific field is not usable
CSCvy44723	control connection to the edege device doesnt come up with v6 and reverse proxy
CSCvz74374	ip dhcp client default-router distance not working for Eth interface in DSL IPOE feature template
CSCvy22416	Security policies applied to incorrect interface in cluster mode, iptables
CSCvz65989	Root cert sync failures not reported to the UI
CSCvz75471	New sequence in RPL with set as-path has both prepend and exclude as required fields
CSCvz28684	Huge Data replication observed during DR process of 3 node cluster running 20.3.4
CSCvz05221	Impossible to install UTD software with "Task cannot proceed. Similar task is in progress" error
CSCvy39355	CSR generation fails if given OU differs from org-name on the Cisco vManage
CSCvz30153	ES(ex. Alarm/Event/Audit) replication import fail
CSCvz32341	custom application list not replicated in Disaster Recovery for a Single Node Cisco vManage Cluster
CSCwa47745	Evaluation of Cisco vManage for Log4j RCE (Log4Shell) Vulnerability
CSCvw59643	Cisco Catalyst SD-WAN Manager Information Disclosure Vulnerability
CSCvz62234	Cisco Catalyst SD-WAN Manager Unauthorized Configuration Rollback Vulnerability

Open Bugs for Cisco SD-WAN Controllers Release 20.7.1

Bug ID	Description
CSCwa11465	Cloud Global Settings AWS subnet setting
CSCvz89254	vManage config roll back failed after vManage template is attached to the Cisco IOS XE SD-WAN device
CSCvy72764	services still communicate via old OOB IP after changing the vpn 0 OOB interface IP

Bug ID	Description
CSCvz95054	System IP persists after invalidating the edge devices from the Cisco vManage which it is not connected .
CSCvz02667	Cisco vManage ODT : Monitoring Stats collection takes > 3 hours when selected for 1 day duration.
CSCwa25355	20.7: Unreachable node still shows up in device list
CSCvz99938	OIB DayN: "Manage Network Design" button is disabled when add service. Need wait for task completed
CSCvz60689	Cisco vManage with IPv6 interface with local user fails until we login with ipv4 once
CSCvz89536	20.6.2: API delay of 90+ seconds in displaying Real Time Tunnel statistics
CSCvz89460	HSDWAN: All region BRs are seen in partial connections on Cisco vManage
CSCwa29191	OMPD crashed on vSmart running on 20.6.1.1
CSCvz47162	Cisco vManage MTT : An empty popup is displayed
CSCwa21248	boot up time to bring up the containers takes considerable amount of time in 20.6 compared to 20.5
CSCvz62751	Cisco vManage: Noticed RouteMap attribute modification failure , while attempting through CLI Template
CSCvz66256	Filtering the data based on local tloc is returning no data in Cisco vManage GUI for DPI stats

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.

Redesign of Cisco vManage GUI

From Cisco vManage Release 20.7.1, Cisco vManage GUI is redesigned and offers a new visual display. This section presents a comparative summary of the significant changes between older Cisco vManage releases and Cisco vManage Release 20.7.1 and later.

Changes in Monitor and Tools Menus

Cisco vManage Release 20.7.1 includes the following changes:

- The **Dashboard** menu is removed, and all submenus that were earlier accessible from the **Dashboard** menu are now part of the **Monitor** menu.
- The **Monitor** page provides a real-time user interface with a consolidated view of the monitoring information for the components and services of a Cisco SD-WAN overlay network.
- Using the pill buttons on the **Monitor** page, you can navigate to monitoring information for specific components or services of a Cisco SD-WAN overlay network.

- The **Network Wide Path Insight** and **On Demand Troubleshooting** options that were earlier accessible from the **Monitor** menu are now part of the **Tools** menu so that you can easily locate these features.

Figure 1: Dashboard Menu in Cisco vManage Release 20.6.1 and Earlier

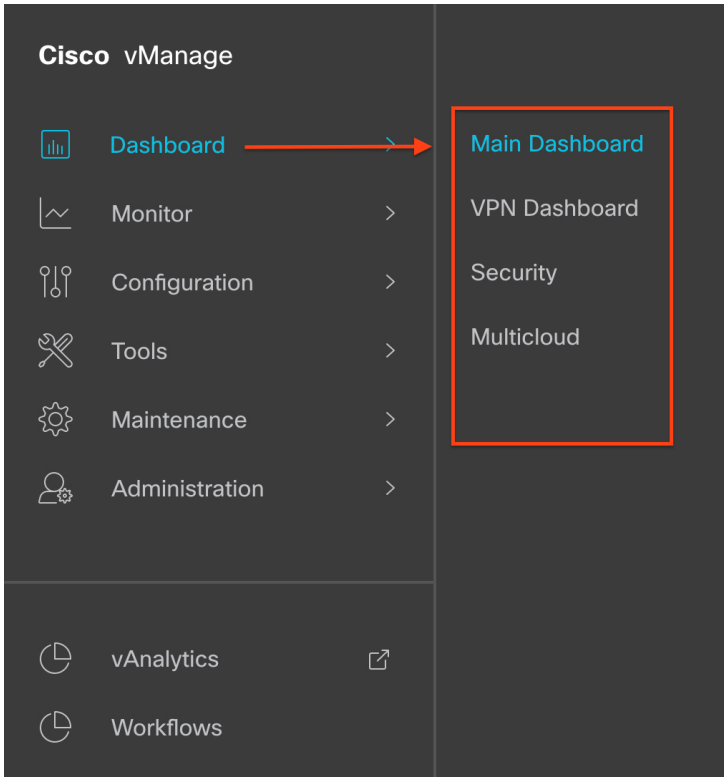


Figure 2: Monitor Menu in Cisco vManage Release 20.7.1 and Later

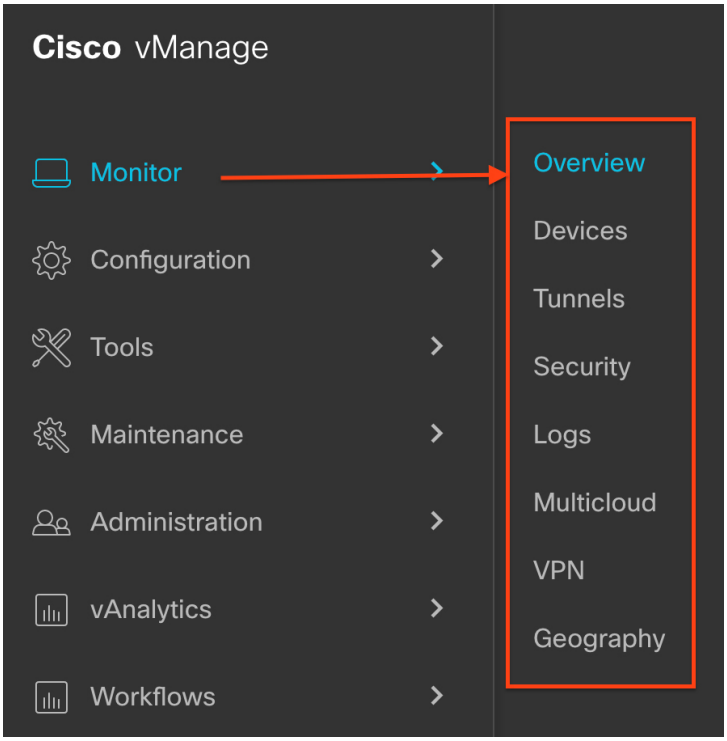


Figure 3: Tools Menu in Cisco vManage Release 20.7.1 and Later

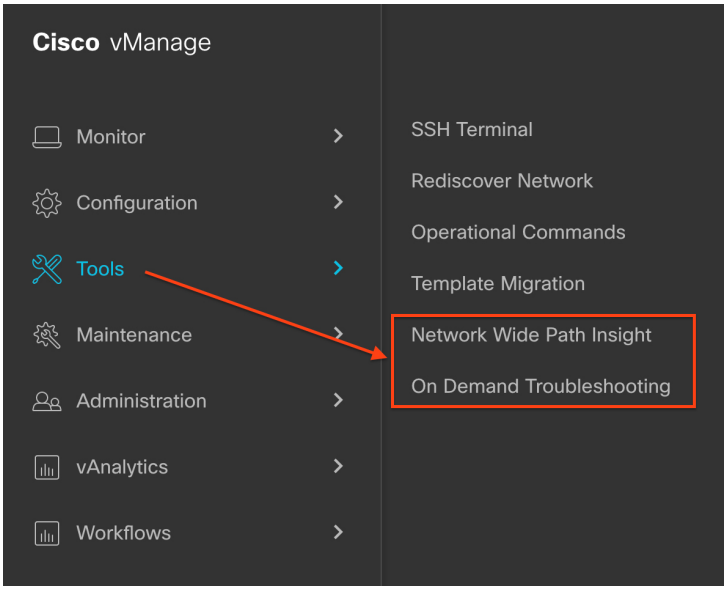
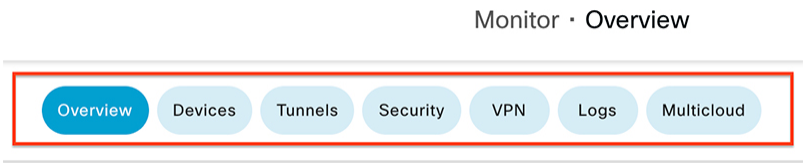


Figure 4: Pill Buttons in Monitor Window in Cisco vManage Release 20.7.1 and Later



Support for Web Content Accessibility Guidelines (WCAG) 2.0 Standard

Cisco vManage Release 20.7.1 supports Web Content Accessibility Guidelines (WCAG) 2.0 standard for the AA conformance level, with the following limitations:

- You cannot exit from SSH terminal using the keyboard.
- Cisco SD-WAN Manager cannot skip repetitive navigation links.
- Data charts on Cisco SD-WAN Manager use colors as the only visual means of conveying information, which is not compliant with WCAG 2.0.
- Some text elements as well as non-text elements in Cisco SD-WAN Manager do not meet the color contrast ratio as defined in WCAG 2.0.

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

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST 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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)