Release Notes for Cisco vEdge Devices, Cisco SD-WAN Release 20.9.x

First Published: 2022-08-01

Last Modified: 2025-04-30

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 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 vEdge Device, Cisco SD-WAN Release 20.9.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 Release 20.9.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 vEdge devices.

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 Release 17.9.x.

For release information about Cisco Catalyst SD-WAN Control Components, refer to Release Notes for Cisco Catalyst SD-WAN Control Components, Cisco Catalyst SD-WAN Control Components Release 20.9.x

What's New for Cisco SD-WAN Release 20.9.x

This section applies to Cisco vEdge devices.

Cisco is constantly enhancing the SD-WAN solution with every release and we try and keep the content in line with the latest enhancements. The following table lists new and modified features we documented in the Configuration, Command Reference, and Hardware Installation guides. For information on additional features and fixes that were committed to the SD-WAN solution, see the *Resolved and Open Bugs* section in the Release Notes.

Table 1: Cisco SD-WAN Release 20.9.2

Feature	Description
Systems and Interfaces	
Synchronized device lists in Cisco SD-WAN Manager	This feature synchronizes the device lists on the **Configuration** > **Devices** and **Monitor** > **Devices** pages. The **Monitor** > **Devices** page now displays the devices that are newly added or synced to Cisco SD-WAN Manager using the options available on the **Configuration** > **Devices** page.

Table 2: Cisco SD-WAN Release 20.9.1

Feature	Description
Cisco Catalyst SD-WAN Getting Started	
Support for License Management Using a Proxy Server	If you configure Cisco SD-WAN Manager to use a proxy server for internet access, Cisco SD-WAN Manager uses the proxy server to connect to Cisco SSM or an on-premises SSM.
Support for Managing Licenses Using Cisco Smart Software Manager On-Prem	Cisco SD-WAN Manager supports management of device licenses, using a Cisco SSM On-Prem license server. This is useful for organizations that use Cisco SSM On-Prem to accommodate a strict security policy that does not permit devices to communicate with Cisco SSM over a direct internet connection.
Renew Device CSR	This feature allows you to reset the RSA private and public keys, and generate a CSR that uses a new key pair. In earlier releases, the generation of CSR used the existing key pair.
Systems and Interfaces	
Hardened Passwords	This feature lets you configure Cisco SD-WAN Manager to enforce predefined medium-security or high-security password criteria.
Network Hierarchy and Resource Management	This feature enables you to create a network hierarchy in Cisco SD-WAN Manager to represent the geographical locations of your network. The network hierarchy and the associated resource IDs, including region IDs and site IDs, help you apply configuration settings to a device. In addition, the introduction of the resource manager in Cisco SD-WAN Manager automatically manages these resource IDs, thereby simplifying the overall user experience of Cisco SD-WAN. You can create a region only if you enable the **Multi-Region Fabric** option in Cisco SD-WAN Manager.
Co-Management: Improved Granular Configuration Task Permissions	To provide a user with the ability to self-manage specific configuration tasks, you can assign the user permissions to configure specific features while excluding others. This feature introduces numerous new permission options, enabling fine granularity in determining which configuration task permissions to provide to a user.
RBAC for Security Operations and Network Operations Default User Groups	This feature provides the following default user groups: • network_operations user group for non-security policies • security_operations user group for security policies RBAC for policies allows you to create users and user groups with the required read and write permissions for security and non-security policies. Users can perform configuration and monitoring actions only for the authorized policy type.
Flexible Tenant Placement on Multitenant Cisco SD-WAN Controller	With this feature, while onboarding a tenant to a multitenant deployment, you can choose the pair of multitenant Cisco SD-WAN Controller that serve the tenant. After onboarding a tenant, you can migrate the tenant to a different pair of multitenant Cisco SD-WAN Controller to allow for more tenant WAN edge devices than was forecast during onboarding.

Feature	Description
Routing	
Route Leaking between Inter-Service VPN	This feature allows you to leak routes between service VPNs on the same edge device.
Policies	
Custom Applications	This feature enables you to define custom applications using Cisco Software-Defined Application Visibility and Control (SD-AVC) support. This feature is available only on Cisco vEdge devices.
Application-Aware Routing for Hub and Spoke	This feature allows you to configure AAR for traffic coming from tunnel to tunnel on Cisco Catalyst SD-WAN devices. Prior to Cisco SD-WAN Release 20.9.1, AAR policy is applied only for packets coming from service going to tunnel. With this feature, you can apply AAR policy for packets coming from tunnel to tunnel as per SLA requirements.
Lawful Intercept	This feature enhances the support for Lawful Intercept in Cisco Catalyst SD-WAN. Cisco Catalyst SD-WAN's Lawful Intercept feature enables Cisco SD-WAN Manager and Cisco SD-WAN Controller to provide the key information to LEA so they can decrypt the Cisco Catalyst SD-WAN IPsec traffic captured by the MSP.
Security	
Global SIG Credentials Template	With this feature, create a single global SIG Credentials template for each SIG provider (Cisco Umbrella or Zscaler). When you attach a SIG template to a device template, Cisco SD-WAN Manager automatically attaches the applicable global SIG Credentials template to the device template.
Disable Weak SSH Encryption Algorithms	This feature allows you to disable weaker SSH algorithms that may not comply with certain data security standards.
Cisco Catalyst SD-WAN Monitor and Maintain	
Access TAC Cases from Cisco SD-WAN Manager	This feature allows you to access Support Case Manager (SCM) wizard using Cisco SD-WAN Manager. You can create, view, or edit the support cases directly from Cisco vManage without having to go to a different Case Manager portal.
Analyze the Health of the Cisco SD-WAN Manager Cluster and Cluster Services Using the CLI	With this feature, you can analyze the health of the Cisco SD-WAN Manager cluster and the status of the cluster services using the **request nms cluster diagnostics** CLI command.

Feature	Description
Additional Real Time Monitoring Support for AppQoE and Other Configuration Options	This feature adds support for real-time monitoring for AppQoE and other device configuration details. Real-time monitoring in Cisco SD-WAN Manager is similar to using **show** commands in the CLI of a device.
Compare Template Configuration Changes Using Audit Logs	This feature introduces a **Config Diff** option for audit logs of device templates and feature templates. The **Config Diff** option shows configuration changes made to the template, comparing the current configuration and previous configuration. The **Config Diff** option is available for audit logs to view the configuration changes when a template is not attached to a device.
Customizable Monitor Overview Dashboard in Cisco vManage	This feature adds customizability to the **Monitor Overview** dashboard. It gives you the flexibility to specify which dashlets to view and sort them based on your personal preferences.
Schedule the Software Upgrade Workflow	This feature introduces an option to schedule software upgrades for edge devices using Cisco SD-WAN Manager.
Software Upgrade Workflow Support for Additional Platforms	Added support for Cisco Enterprise NFV Infrastructure Software (NFVIS) and Cisco Catalyst Cellular Gateways.
High Availability	
Configure Disaster Recovery Alerts	This feature provides support for configuring Cisco SD-WAN Manager alerts to generate an alarm and a syslog message for any disaster recovery workflow failure or event that occurs.

Software and Hardware Behavior Changes in Cisco SD-WAN Release 20.9.1

Behavior Change	Description
A link is added from the Cisco SD-WAN Manager menu to the Cisco Catalyst SD-WAN Portal. From the Cisco Catalyst SD-WAN menu, click **SD-WAN Portal** to access the Cisco Catalyst SD-WAN Portal for provisioning, monitoring, and maintaining Cisco Catalyst SD-WAN controllers using public cloud providers.	A note is added in the Cisco Catalyst SD-WAN Solution s

Behavior Change	Description
Support is added for configuration of a device access policy having only a default action and with no policy sequences. You can now create a device access policy with only a default action and with no policy sequences for creation of a device configuration or a Cisco SD-WAN Manager configuration for both protocols, Secure Shell (SSH) and Simple Network Management Protocol (SNMP).	A note is added in the Configure Device Access Policy Using
A list of valid characters is added. These characters must be used in the user ID, password, and the URL name or path when downloading an image from a remote server manually.	A note is added in the Upgrade the Software Image on a Dev
Support is added to throttle the elephant flow (EF) traffic on vEdge2k devices.	Added a new topic Elephant Flow Throttling in Policy Guide The following new commands are added: • elephant-flow • custom-eflow • match elephant-flow • show policy ef-stats
We recommend that the Cisco SD-WAN Manager cluster interface should not be the same as the transport interface. Beginning with Cisco vManage Release 20.9.1, this is enforced. If you attempt to configure this, Cisco SD-WAN Manager displays an error message.	A note is added in the Guidelines for a Cisco SD-WAN Mana
A new option **Umbrella DNS Certificate** is available in Cisco SD-WAN Manager to upload and push to appropriate devices Umbrella root certificates for Umbrella DNS security.	The new **Umbrella DNS Certificate** option is described in th Certificates section.
A new option **Remote Server** (preferred) is available in Cisco SD-WAN Manager to add multiple remote locations and use the remote locations as the source of the virtual image.	A note is added in the Upload the Cisco Security Virtual Image section.
Configure the DNS cache timeout **timer tracker-dns-cache-timeout** command on Cisco vManage in the system configuration mode. Cisco vEdge devices cache DNS resolved SIG endpoint IP addresses for the duration of this timeout. When the cache times out, Cisco vEdge devices refresh the cache through new DNS resolution queries. The default timeout is two hours.	The new configuration option in the Support for Layer 7 Hea

Behavior Change	Description
The Cisco Catalyst SD-WAN Control Components software version must be the same or be higher that the WAN edge device software version. If the WAN edge device software version is higher than the Control Componets software version, policy download to the device fails.	A note is added in Cisco Catalyst SD-WAN Control Com and Recommended Computing Resources.

Important Notes, Known Behaviors, and Workarounds

- Starting from Cisco SD-WAN Release 20.5.1, Cloud onRamp for IaaS isn't supported for Cisco vEdge Cloud Router running on Cisco SD-WAN Release 20.5.1. However, Cloud onRamp for IaaS is supported with AWS as the cloud provider for Cisco vEdge Cloud Routers using Cisco SD-WAN Release 20.4.1 and earlier. Cloud onRamp for IaaS is also supported with Microsoft Azure as the cloud provider for Cisco vEdge Routers using Cisco SD-WAN Release 20.3.1 and earlier.
- For information about upgrade paths, see Cisco SD-WAN Manager Upgrade Paths.
- Starting from Cisco SD-WAN Release 20.9.1, feature templates support the following network interface modules for Layer 3 features:
  - Cisco 2-port 100-Mbps/1-Gbps WAN Network Interface Module with 256-bit WAN MACsec (C-NIM-2T)
  - Cisco 1-port 2.5-Gbps/1-Gbps WAN Network Interface Module with Cisco UPoE (C-NIM-1M)
- Starting from Cisco SD-WAN Release 20.9.1, the Switch Port feature template supports an interface speed of 2500 Mbps when configuring a 2-Gigabit Ethernet interface for the following modules:
  - Cisco SM-X-16G4M2X and Cisco SM-X-40G8M2X EtherSwitch Service Modules on Cisco ISR 4000 Series Routers
  - Cisco C-SM-16P4M2X and Cisco C-SM-40P8M2X EtherSwitch Service Modules on Cisco Catalyst 8300 Series Edge Platforms
- **Cloud OnRamp for IaaS**: Beginning with Cisco vManage Release 20.9.1, we recommend setting up your cloud infrastructure using Cisco Catalyst Cloud OnRamp for Multicloud. Cloud OnRamp for IaaS will be phased out in a future release.
- Cisco Catalyst SD-WAN Control Components Release 20.9.x is the last supported release version for the Cisco vEdge devices. We have announced the end-of-sale and end-of-life dates for select Cisco vEdge devices. The last day to order the affected product(s) is May 2, 2023. For more information see, End-of-Sale and End-of-Life Announcement for the Cisco Select vEdge Products.

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 Release 20.9.7

Resolved Bugs for Cisco SD-WAN Release 20.9.7

Identifier	Headline
CSCwm65800	The dbgd should be non-critical/restartable process.
CSCwj68822	The PPPoE interface goes down after upgrading from version 20.6.x to 20.9.x
CSCwm45325	An FTMD crash is observed on vEdge2000 during the upgrade to version 20.9.4.
CSCwm65356	The GRE tunnel tracker remains down, reporting an "RTT Timeout" error.
CSCwn19787	A Kernel Panic crash is observed on the ISR1100 device due to the /usr/sbin/vdhcpsd process.
CSCwn35649	An FTMD crash is observed on the ISR1100 device running version 20.9.4.
CSCwf14869	Cisco vEdge device: User traffic impacted due to IPSEC rx_replay_integrity_drops.

Open Bugs for Cisco SD-WAN Release 20.9.7

Identifier	Headline
CSCwo37603	Cisco SD-WAN Manager iperf test generates error "Failed to start iperf client" and reports 0/0 speeds.
CSCwo52240	Cisco vEdge device does not list tracker correctly.
CSCwo52240	Cisco vEdge device does not list tracker correctly.
CSCwk67277	(Nitro) FP Core watchdog failure is seen on vEdge 2000 running 20.9.5.1 code.

Bugs for Cisco SD-WAN Release 20.9.6

Resolved Bugs for Cisco SD-WAN Release 20.9.6

Identifier	Headline
CSCwi50508	Cisco vEdge device can't install the default gateway after reboot and establishing PPPoE session.
CSCwj26006	IPv6 fragmented packets getting dropped at Cisco vEdge device used as intermittent router.
CSCwj71739	Viptela Platforms are not following RFC standard for command accounting.
CSCwj72906	The batch deletion support of /tmp/xml stats file on Cisco vEdge devicerunning 20.6 and 20.9

Identifier	Headline
CSCwi52276	System crash rebooted with "Software initiated - zebra-1 (pid: 4221)"

Open Bugs for Cisco SD-WAN release 20.9.6

Identifier	Headline
CSCwm04186	Cisco vEdge device 5000 router crashing | Software initiated - resolvd got signal 11
CSCwk55511	ISR1100-6G running 20.9.4 has Kernel Panic reboot, core genenrated by /usr/sbin/vdhcpsd
CSCwm01407	Cisco vEdge device FP Core watchdog failed seen on the Cisco vEdge device 2000 running 20.9.5.1 code.
CSCwj68822	PPPoE interface goes down post upgade to 20.9 from 20.6
CSCwk95406	Cisco vEdge device unable to turn off syslog messages for socket connection errors for process OSPF and BGP.

Bugs for Cisco SD-WAN Release 20.9.5

Resolved Bugs for Cisco SD-WAN Release 20.9.5

Identifier	Headline
CSCwe21563	Cisco vEdge device cannot resolve Cisco Catalyst SD-WAN Validator on the loopback interface.
CSCwh22127	Software initiated reboot due to OMPD crash (segmentation fault)
CSCwf65485	Interface Diagnostic commands won't show desired output on code 20.6.3.2 for Cisco vEdge device- 2000.
CSCwf57305	ZTP service crash
CSCwh36048	Port number that is lower than 1024 are chosen as the DIA NAPT source port in Cisco vEdge device.
CSCwf44950	Cisco vEdge device : Missing info about top processes that took most CPU/Memory during stress.
CSCwf80551	Cisco vEdge device symnat flag got stuck even when not behind NAT.
CSCwc62651	Software downgrade from 20.9 to 20.6 clean activation error.
CSCwi55005	TACACs authentication was not working on ISR1100-4G after upgrade to 20.9.4 version.
CSCwf70034	DNS Cache was populating without a valid response.
CSCwh54526	Net-snmp exclude OID

Identifier	Headline
CSCwf71998	confd.smp making CPU high during SNMP polling (net-snmp looping caused by endOfMibView)
CSCwh24251	I2C bus gets hang leading h/w operation application failiure on 20.6.
CSCwe41667	Cisco vEdge device-1000/ 20.6.5 / SSHd and vConfd spiking CPU up to 100%
CSCwf54032	The "show bfd history" not showing the "up" status after BFD tunnel recovers from flapping on Hub Cisco vEdge device.
CSCwf74787	The Cisco vEdge device is crashing due to FP Core dying
CSCwf97711	On Cisco vEdge device-1000, the customer is seeing the clock getting reset after RTC reports PWRFAIL.
CSCwe80168	Cisco vEdge device-2000 ftmd daemon crash. Signal 10
CSCwf47529	BFD Tunnel convergence taking couple of more seconds longer
CSCwe42133	Cisco vEdge device: Same label is assigned to different vpns.
CSCwf68816	High CPU in Cisco vEdge device is caused by minigzip process.
CSCwf24092	The tracker on Cisco vEdge device does not come up after reboot.

Open Bugs for Cisco SD-WAN release 20.9.5

Identifier	Headline
CSCwi31443	Cisco vEdge device cannot resolve Cisco Catalyst SD-WAN Validator after reboot for software activation
CSCwi52276	System crash rebooted with "Software initiated - zebra-1 (pid: 4221)"

Bugs for Cisco SD-WAN Release 20.9.4

Resolved Bugs for Cisco SD-WAN Release 20.9.4

Identifier	Headline
CSCwd85135	FP core watchdog expired (rc = 60). Forcing fp-um core and rebooting device due to corrupted packets
CSCwf40308	Tracker on Cisco vEdge devices does not come up with Legacy VPN Template (SIG Tunnels)
CSCwe47171	FTMD crash seen when ftm next-hop count is overutilised then max limit
CSCwe90126	ISR1100:Interface went up/down state with speed 100m and no auto-neg configured post upgrade to 20.6
CSCwe86766	Current flows are not getting cleared post disabling app-visibility

Identifier	Headline
CSCwe22321	Enabling port stats command triggered an FP crash
CSCwd85846	DTLS session with the vBond does not come up due to OOO packets received at the Cisco vEdge devices
CSCwf34096	168 Cisco vEdge 5000 device inbuilt certificate expiring on 12th Nov 2023

Open Bugs for Cisco SD-WAN release 20.9.4

Identifier	Headline
CSCwe42133	Cisco vEdge devices: same label is assigned to different vpns
CSCwf14869	Cisco vEdge devices: User traffic impacted due to IPSEC rx_replay_integrity_drops

Bugs for Cisco SD-WAN Release 20.9.3.1

Resolved bugs for Cisco SD-WAN Release 20.9.3.1

Identifier	Headline
CSCwf28118	Cisco vEdge: Certificate issue on Cisco vEdge devices

Bugs for Cisco SD-WAN Release 20.9.3

Resolved bugs for Cisco SD-WAN Release 20.9.3

Identifier	Headline
CSCwd20729	VRRP VIP and sub-interface not responding to hosts on LAN sourced from a different VLAN.
CSCwc67625	OU field is deprecated from CA/B Forum Certificate Authorities
CSCwd85121	After the vpn list change, the DP, AAR and CLFOWD polices stopped working on the routers.
CSCwc48809	Cisco vEdge 5000K: BFD sessions taking very long time to come up after clearing omp sessions
CSCwd43784	APP Engine ID wrongly set to 0 - invalid (0)

Open bugs for Cisco SD-WAN Release 20.9.3

Identifier	Headline
CSCwc82784	Cisco ESXI vEdge interface mac and ESXI virtual hw mac and more than 4 interface order is wrong

Identifier	Headline
CSCwd54202	Auto-RP is not working after upgrading to 20.6.4
CSCwe32036	ISR1100-4G After the upgrade all service traffic going via VEDGE-2 is not working.
CSCwc55279	Cisco vEdge - ISR1100 4G-LTE - Cellular interface last-resort-circuit

Bugs for Cisco SD-WAN Release 20.9.2

Resolved bugs for Cisco SD-WAN Release 20.9.2

Identifier	Headline
CSCwc62342	Cisco vEdge device pimd crash on 20.3.5
CSCwd33072	Cisco vEdge5K "fp_dump -ec" CLI Corrupts Forwarding Cores
CSCwc31458	Shaping-rate is programmed to another interface in the same VPN.
CSCwc69937	Sticky flow is not working for app-route preferred color on Cisco vEdge device
CSCwc56554	No DP instance in v1k/v2k after software upgrade
CSCwc69219	Cisco vEdge device/ACL is accepting traffic when default action is set to drop.
CSCwc78553	On performing OIR for 1G Fiber SFP, interface is not coming up
CSCwc31839	Cisco vEdge5k interface not coming up post shut/un-shut
CSCwc78699	ZIA not re-trying request to scaler if the WAN interface gets an ip address with a little delay.
CSCwc07584	Supress Sysmgr sig 9 from hitting wtmp history post killing critical process
CSCwc57970	"Error in packet.: (genError) A general failure occured" seen when running snmpwalk on Cisco vEdge-cloud

Open bugs for Cisco SD-WAN Release 20.9.2

Identifier	Headline
CSCwd65542	Silent reboot seen on Cisco vEdge MIPs platform
CSCwc82784	ESXI Cisco vEdge interface mac and ESXI virtual hw mac and more than 4 interface order is wrong
CSCwd58002	High CPU on Cisco vEdge due to sw process
CSCwc55279	Cisco vEdge - ISR1100 4G-LTE - Cellular interface last-resort-circuit
CSCwc67625	OU field is deprecated from CA/B Forum Certificate Authorities
CSCwd30019	Cisco vEdge not identifying Citrix traffic correctly

Identifier	Headline
CSCwd54202	Auto-RP is not working after upgrading to Cisco SD-WAN Release 20.6.4
CSCwd85121	After the vpn list change, the DP, AAR and CLFOWD polices stopped working on the routers.

Bugs for Cisco SD-WAN Release 20.9.1

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 Release 20.9.1

Identifier	Headline
CSCwb39731	Cisco vEdge 5K: Fragmented packets don't get transmitted out of the device
CSCvz20061	Cisco vEdge: OSPF route isn't removed from routing table.
CSCvz37684	Not possible to ping VRRP Virtual IP
CSCvz56337	Cisco vEdge-2000 version 20.3.2 crashed due to (reason: Daemon 'bgpd' down in vpn 7)

Open Bugs for Cisco SD-WAN Release 20.9.1

Identifier	Headline
CSCwc15570	Cisco SD-WAN 20.9 - Control connection flap on Cisco vEdge5000 - Error > "RECCABLOBFAILNOERR"
CSCwd85121	After the vpn list change, the DP, AAR and CLFOWD polices stopped working on the routers.
CSCwd85121	After the vpn list change, the DP, AAR and CLFOWD polices stopped working on the routers.

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 Catalyst SD-WAN Device Compatibility.

Cisco SD-WAN Manager GUI Changes

This section presents a comparative summary of the significant changes between Cisco vManage 20.8.x and Cisco vManage Release 20.9.1.

Workflows Menu

In Cisco vManage Release 20.9.1, the following changes have been made to the **Workflows** menu:

- The **Launch Workflows** submenu is renamed as **Workflow Library**.
- The **Popular Workflows** section is introduced for easy and quick access to the workflows.

Figure 1: Workflows Menu in Cisco SD-WAN Manager 20.8.x

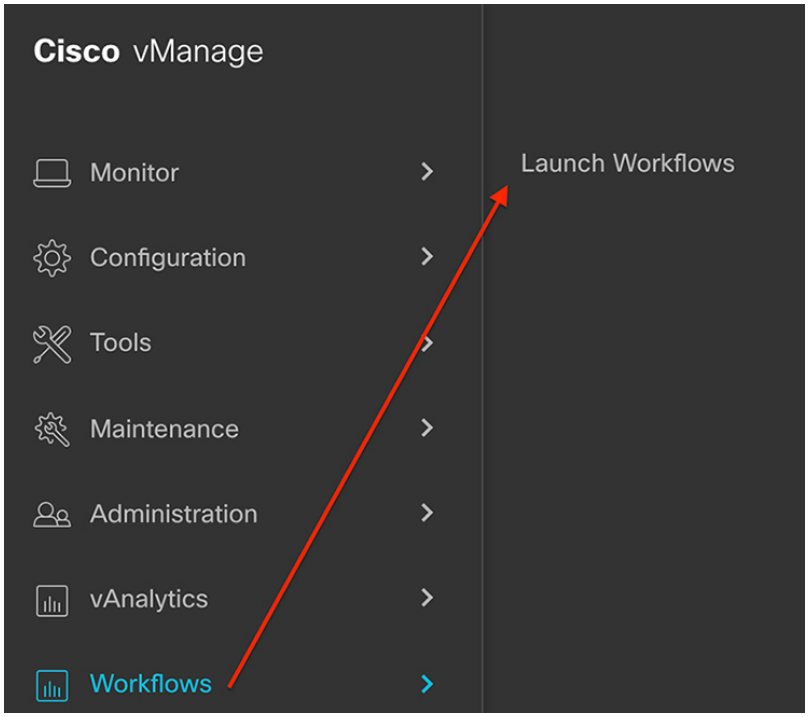
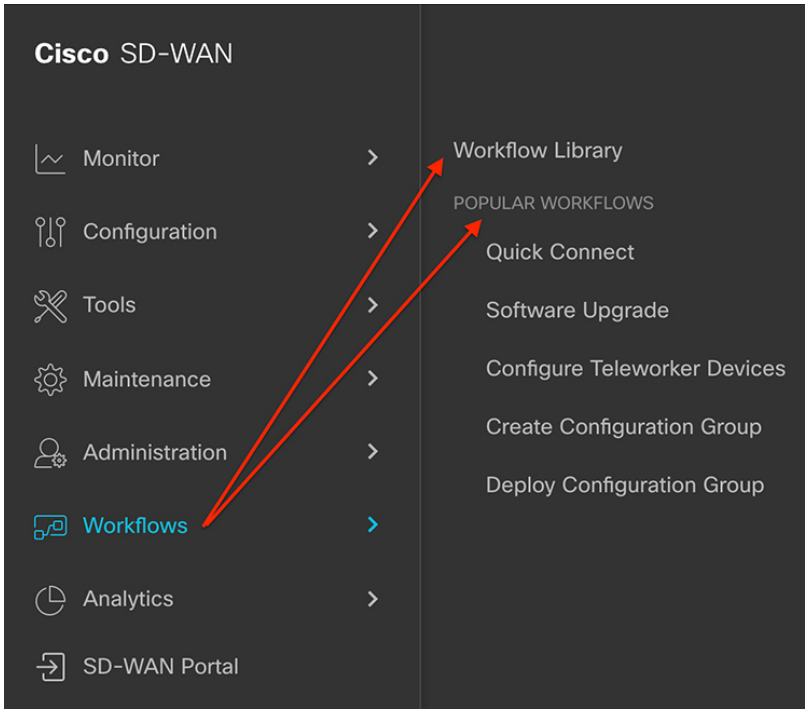


Figure 2: Workflows Menu in Cisco SD-WAN Manager 20.9.1



- The **Rapid Site Configuration Group** and **Custom Configuration Group** workflows are removed, and the **Create Configuration Group** workflow is introduced.

Figure 3: Rapid Site Configuration Group Workflow in Cisco SD-WAN Manager 20.8.x

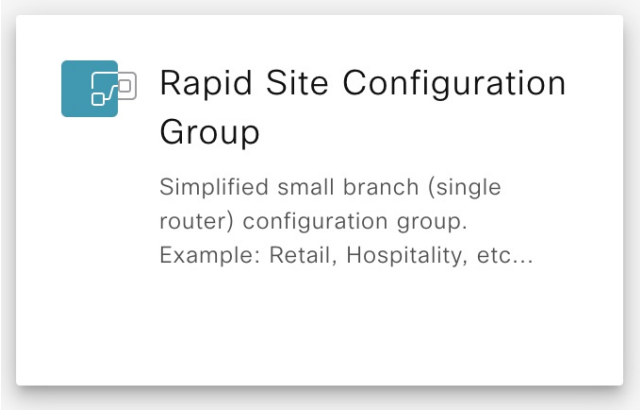


Figure 4: Custom Configuration Group Workflow in Cisco SD-WAN Manager 20.8.x

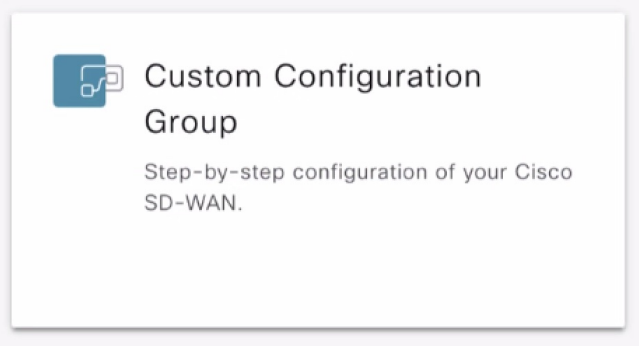
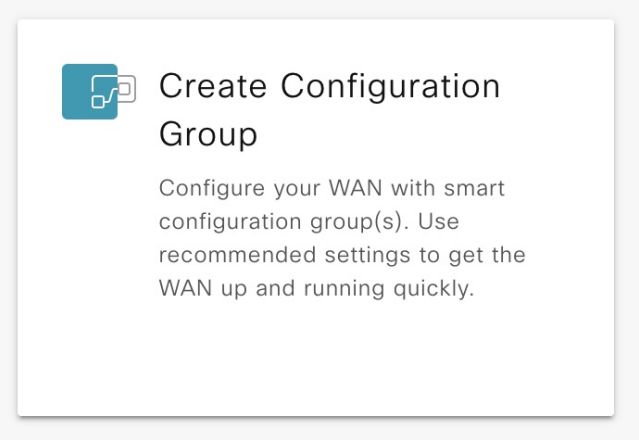


Figure 5: Create Configuration Group Workflow in Cisco SD-WAN Manager 20.9.1



- The **Provision WAN Sites and Devices** workflow is renamed as **Deploy Configuration Group**.

Figure 6: Provision WAN Sites and Devices Workflow in Cisco SD-WAN Manager 20.8.x

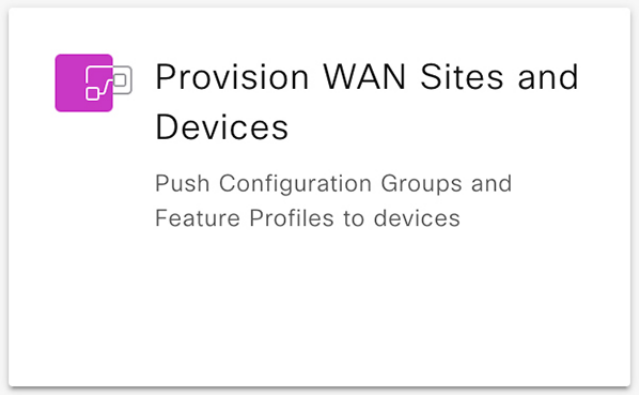
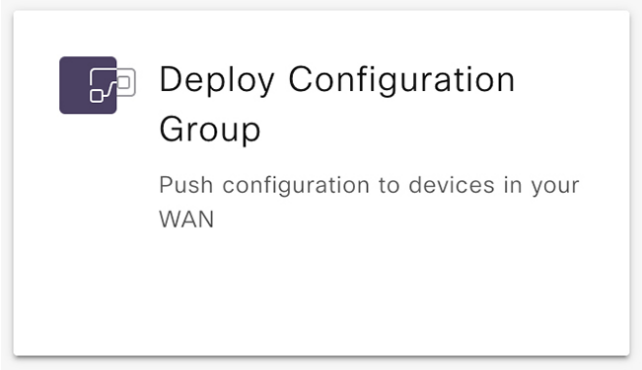


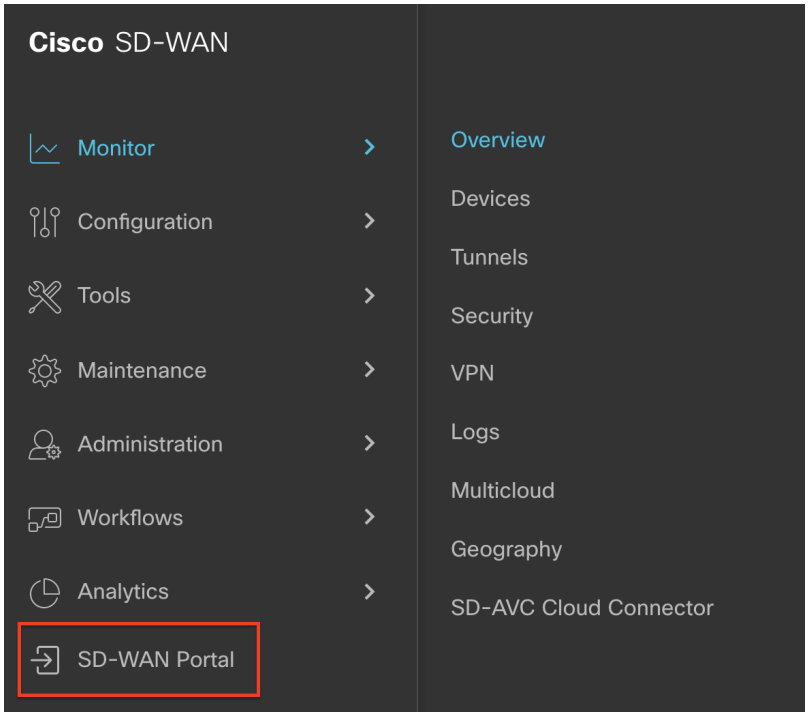
Figure 7: Deploy Configuration Group Workflow in Cisco SD-WAN Manager 20.9.1



SD-WAN Portal Menu

In Cisco vManage Release 20.9.1, **SD-WAN Portal** is added to the Cisco SD-WAN Manager menu. Choose **SD-WAN Portal** to access the Cisco SD-WAN Self-Service Portal.

Figure 8: SD-WAN Portal Menu in Cisco SD-WAN Manager 20.9.1



Monitor Overview Page

In Cisco vManage Release 20.9.1, the labels of the following UI elements have changed:

- **Devices** to **WAN Edges**
- **Device Health** to **WAN Edge Health**

- **Device Inventory** to **WAN Edge Inventory**

Figure 9: Monitor Overview Page in Cisco SD-WAN Manager 20.8.x

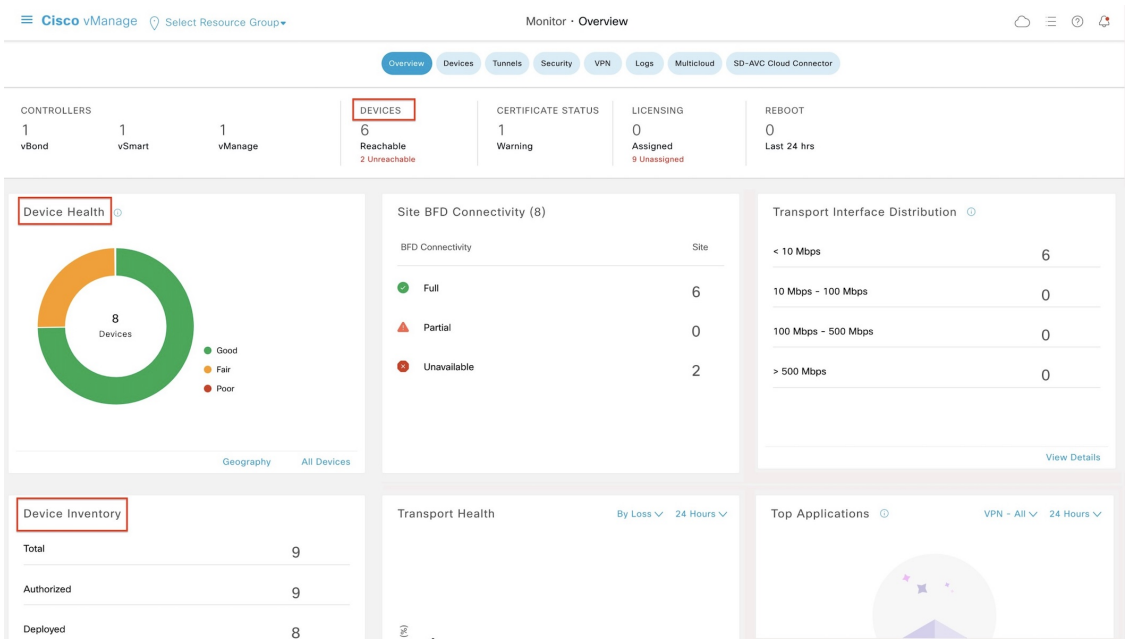
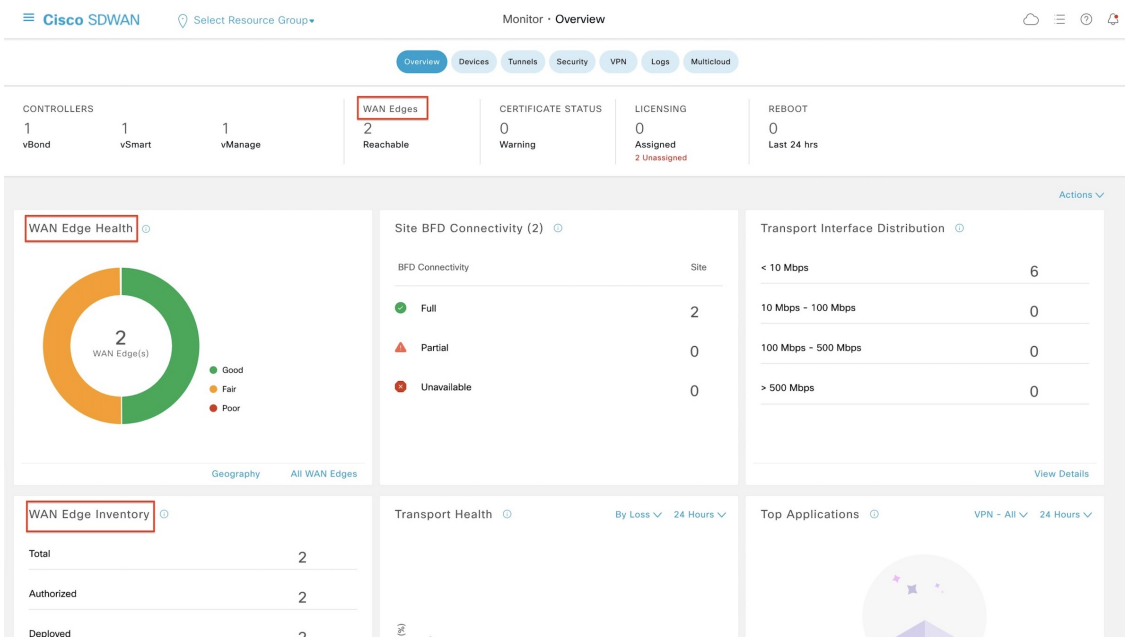


Figure 10: Monitor Overview Page in Cisco SD-WAN Manager 20.9.1



Monitor VPN Page

In Cisco vManage Release 20.9.1, the labels of the following UI elements have changed:

- **Device Status** to **WAN Edge Reachability**

- **Device Health** to **WAN Edge Health**

Figure 11: Monitor VPN Page inCisco SD-WAN Manager 20.8.x

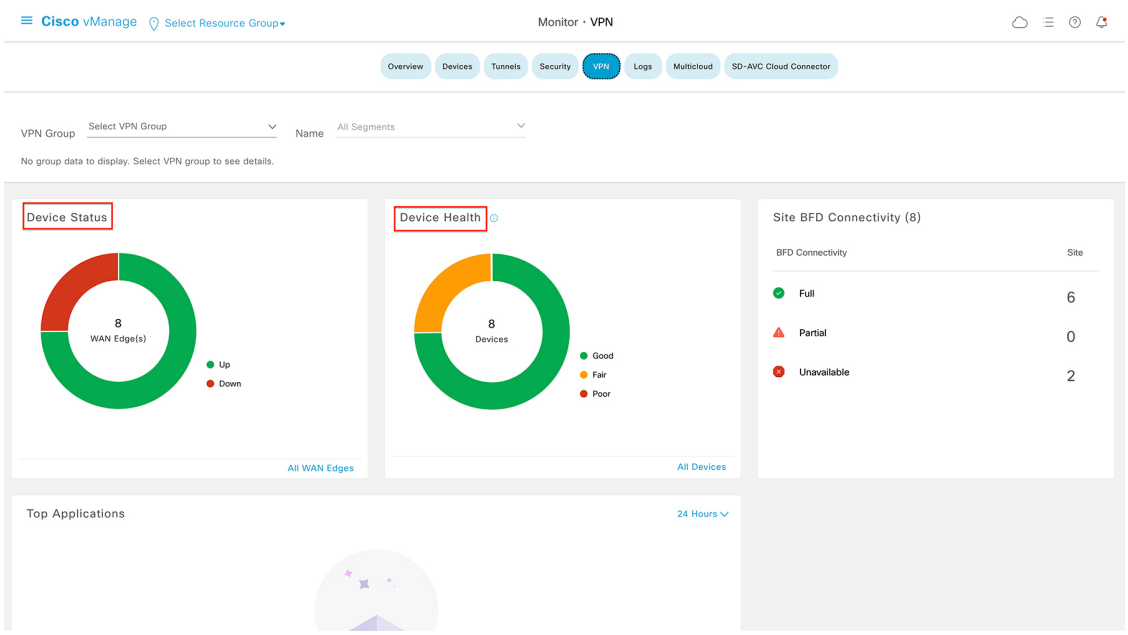
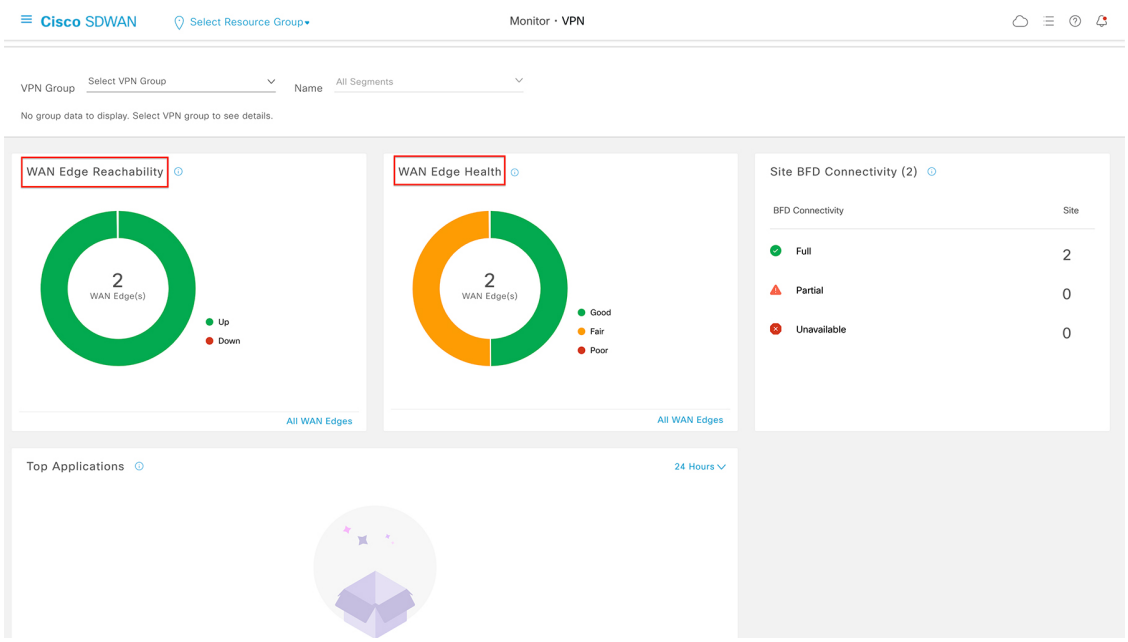


Figure 12: Monitor VPN Page in Cisco SD-WAN Manager 20.9.1



Configuration Groups Edit Page

In Cisco vManage Release 20.9.1, the feature profiles are presented in a tabular format, thereby enabling you to scan all the profiles at once. In Cisco vManage Release 20.8.x, the feature profiles were organized in a card-based presentation.

Figure 13: Configuration Groups Edit Page in Cisco SD-WAN Manager 20.8.x

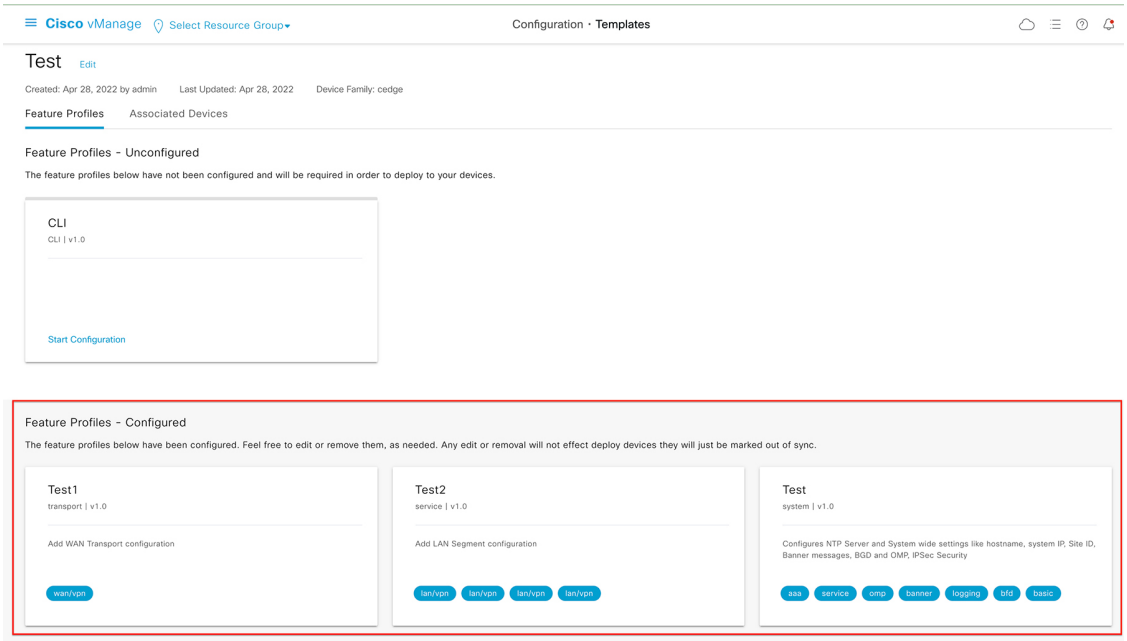
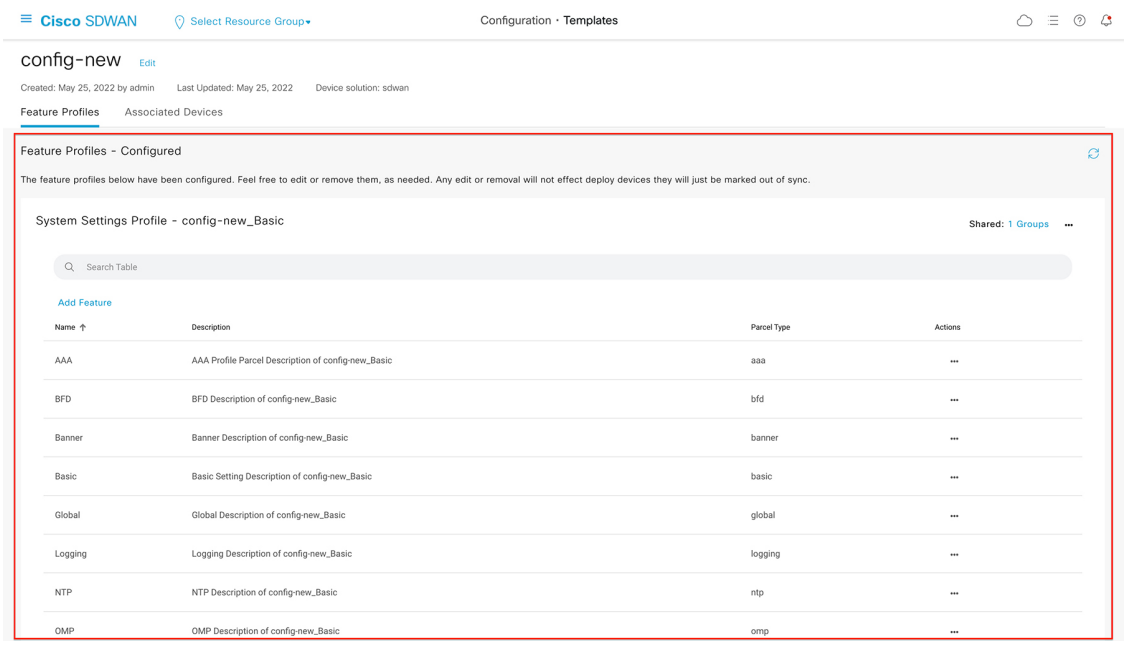


Figure 14: Configuration Groups Edit Page in Cisco SD-WAN Manager 20.9.1



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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

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)