What's New in Cisco vManage

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Table 1: Cisco vManage Release 20.9.1

Feature	Description
Cisco vManage How-Tos for Cisco vEdge Routers	
Flexible Tenant Placement on Multitenant Cisco vSmart Controllers	With this feature, while onboarding a tenant to a multitenant deployment, you can choose the pair of multitenant Cisco vSmart Controllers that serve the tenant. After onboarding a tenant, you can migrate the tenant to a different pair of multitenant Cisco vSmart Controllers, if necessary.
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 vManage automatically attaches the applicable global SIG Credentials template to the device template.
Match Traffic by Destination Region	When creating an application route policy or data policy, you can match traffic according to its destination region. The destination may be a device in the same primary region, the same secondary region, or neither of these.
Specify Path Type Preference	When configuring a centralized policy, you can create a preferred color group list, which specifies three levels of route preference, called primary, secondary and tertiary. The route preferences are based on TLOC color and, optionally, on the path type—direct tunnel, multi-hop path, or all paths. Path type is relevant to networks using Multi-Region Fabric.
Network Hierarchy and Resource Management	You can create a network hierarchy in Cisco vManage to represent the geographical locations of your network. You can create a region, an area, and a site in a network hierarchy. In addition, you can assign a site ID and a region ID to a device.

Feature	Description
Support for License Management Using a Proxy Server	If you configure Cisco vManage to use a proxy server for internet access, Cisco vManage uses the proxy server to connect to Cisco SSM or an on-prem SSM.
Support for Managing Licenses Using Cisco Smart Software Manager On-Prem	Cisco vManage can synchronize 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.
Co-Management: Improved Granular Configuration Task Permissions	To enable a user to self-manage specific configuration tasks, you can assign the user permissions to perform specific configuration tasks while excluding other tasks. This feature introduces numerous new permission options, enabling fine granularity in determining which configuration task permissions to provide to a user. .
Route Leaking between Inter-Service VPN	You can configure to leak routes between the service VPNs at the same site using the **Route Leak** option in the Cisco vManage.
Schedule the Software Upgrade Workflow	Upgrade the software of Cisco edge devices using a **scheduler** which helps in scheduling the upgrade process at your convenience.
Software Upgrade Workflow Support for Additional Platforms	Added support for Cisco Enterprise NFV Infrastructure Software (NFVIS) and Cisco Catalyst Cellular Gateways.
Compare Template Configuration Changes Using Audit Logs	This feature introduces a **Config Diff** option for audit logs of device templates and feature templates to view the configuration changes when a template is not attached to a device.
Customizable Monitor Overview Dashboard in Cisco vManage	You can customize the **Monitor Overview** dashboard. You can specify which dashlets to view and sort them based on your personal preferences.
Access TAC Cases from Cisco vManage	This feature allows you to access Support Case Manager (SCM) wizard using Cisco vManage. You can create, view, or edit the support cases directly from Cisco vManage without having to go to a different Case Manager portal.
Additional Real Time Monitoring Support for AppQoE and Other Configuration Options	This feature adds support for real-time monitoring of AppQoE and other device configuration details in Cisco vManage.

Table 2: Cisco vManage Release 20.8.1

Feature	Description
Cisco vManage How-Tos for Cisco vEdge Routers	
User-Defined SaaS Application Lists	In Cisco vManage, you can define lists of one or more SaaS applications, together with the relevant application server. 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.
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. You can configure the trackers using the SIG feature template.
Hierarchical SD-WAN: Secondary Regions	Secondary regions provide another facet to the Hierarchical SD-WAN architecture and enable direct tunnel connections between edge routers in different primary access regions. When you assign an edge router a secondary region, the router effectively operates in two regions simultaneously, and has different paths available through its primary and secondary regions.
Hierarchical SD-WAN: Transport Gateways	An edge router or border router that has connections to two networks that lack direct connectivity can function as a transport gateway. This is helpful for enabling connectivity between routers that are configured to be within the same access region, but which do not have direct connectivity.
Hierarchical SD-WAN: Router Affinity	Often a router has multiple options to choose for the next hop when routing a flow to its destination. When multiple devices can serve as the next hop for a flow, you can specify the order of preference among the devices by configuring router affinity groups. The result is that a router attempts to use a route to the next-hop device of highest preference first, and if that device is not available, it attempts to use a route to the next-hop device of the next lower preference. Affinity groups enable this functionality without requiring complex control policies.
Match Traffic by Destination: Access Region, Core Region, or Service VPN	You can apply a policy to traffic whose destination is any one of the following—access region, core region, service VPN. Use this match condition for data policy or application route policy on a border router.
Match Routes According to Path Type	When configuring a control policy for a Hierarchical SD-WAN architecture, you can match routes according to whether the route uses a hierarchical path, a direct path, or a transport gateway path.
Match Routes by Region and Role in a Control Policy	In a control policy, you can match routes according to the region of the device originating the route, or the role (edge router or border router) of the device originating the route.
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
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.
Support for Postpaid MSLA License Billing Models	For postpaid Managed Services License Agreement (MSLA) program licenses, Cisco SD-WAN supports two distinct billing models for licenses—committed (MSLA-C) and uncommitted (MSLA-U). The procedure for assigning a postpaid license enables you to choose one of these two MSLA license types.
Software Upgrade Workflow	You can now upgrade software images on edge devices using the **Workflows** menu in Cisco vManage.
Bidirectional Support for Packet Tracing	You can configure packet tracing on edge devices.

Table 3: Cisco vManage Release 20.7.1

Feature	Description
Cisco vManage How-Tos for Cisco vEdge Routers	
Certificate Revocation	You can revoke enterprise certificates from devices based on a certificate revocation list that Cisco vManage obtains from a root certificate authority.
Configure Default AAR and QoS Policies	You can configure Default AAR and QoS policies.
Cisco Unified Border Element Configuration	You can configure Cisco Unified Border Element functionality by using Cisco IOS XE SD-WAN device CLI templates or CLI add-on feature templates.
Disaster Recovery User Password Change	You can change the disaster recovery user password for disaster recovery components from the Cisco vManage **Disaster Recovery** window.
Hierarchical SD-WAN	You can use Cisco vManage to enable and configure Hierarchical SD-WAN, which provides the ability to divide the architecture of the Cisco SD-WAN overlay network into multiple regional networks that operate distinctly from one another.
TCP/UDP Endpoint Tracker and Dual Endpoint Static Route Tracker for Cisco vEdge devices	You can now configure static route tracker with TCP/UDP endpoint using Cisco system template, and configure a static route using the Cisco VPN template. You can then add the configured dual trackers in a tracker group using **New Endpoint Tracker Groups** option.
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.

Feature	Description
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 .
Additional Diagnostics Information Added to Admin-Tech File	You can access 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	You can upload an admin-tech file to a TAC case from Cisco vManage.
Support for Cisco VM Image Upload in qcow2 Format	You can now upload a virtual machine image to Cisco vManage in qcow2 format. Earlier, you could upload only a prepackaged image file in tar.gz format.
Software Upgrade Using a Remote Server	This 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.
Packet Capture for Cloud onRamp Colocation Clusters	You can now capture packets at either the physical network interface card (PNIC) level or the virtual network interface card (VNIC) level on a Cloud Services Platform (CSP) device of a colocation cluster. To do this, you need to choose a PNIC or VNIC on the Cisco vManage interface and set the required traffic filters.

Table 4: Cisco vManage Release 20.6.1

Feature	Description
Cisco vManage How-Tos for Cisco vEdge Routers	
Cisco vManage Persona-based Cluster Configuration	You can add Cisco vManage servers to a cluster by identifying servers based on personas. A persona defines what services run on a server.
Dual Endpoint support for interface status tracking on Cisco vEdge devices	This feature allows you to configure tracker groups with dual endpoints using the Cisco vManage 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.
Tenant Device Forecasting	While adding a new tenant to the multitenant Cisco SD-WAN deployment, a service provider can forecast the number of WAN edge devices that the tenant may deploy in their overlay network. Cisco vManage enforces this forecast limit. If the tenant tries to add devices beyond this limit, Cisco vManage responds with an appropriate error message and the device addition fails.
Cloud onRamp for SaaS Over SIG Tunnels	This feature lets you to connect to Cloud onRamp for SaaS by means of a SIG tunnel.

Feature	Description
Route Manipulation for Leaked Routes with OMP Administrative Distance	You can configure route redistribution between the transport VPN and service VPNs using the **Global Route Leak** option under the VPN feature template.
Support for License Management Offline Mode and Compliance Alarms	You can manage Cisco SD-WAN licenses through a Cisco vManage instance that is not connected to the internet. To synchronize license and compliance information between Cisco vManage and Cisco SSM, you must periodically download synchronization files from Cisco vManage and upload the files to Cisco SSM.
RBAC for Policies	Configure RBAC for policies in Cisco vManage.
Cisco vManage Persona-based Cluster Configuration	You can add Cisco vManage servers to a cluster by identifying servers based on personas. A persona defines what services run on a server.
Generate System Status Information for a Cisco vManage Cluster Using Admin Tech	You can collect system status information for a Cisco vManage cluster. Prior to this feature, Cisco SD-WAN was only able to generate an admin-tech file for a single device.
Support for Reverse Proxy with Cisco IOS XE SD-WAN Devices and Cisco SD-WAN Multitenancy	With this feature, you can deploy a reverse proxy device in your overlay network between Cisco IOS XE SD-WAN devices and Cisco vManage and Cisco vSmart Controllers. Also, this feature enables you to deploy a reverse proxy device in both single-tenant and multitenant overlays that include Cisco vEdge or Cisco IOS XE SD-WAN edge devices.
Manage Data Collection for Cisco SD-WAN Telemetry	This feature allows you to disable data collection for Cisco SD-WAN telemetry using Cisco vManage. Data collection for telemetry is enabled by default.
Geofencing	If the location of the device goes beyond its geographical boundary, you can restrict network access to the device using Cisco vManage operational commands. For more information, see the Cisco SD-WAN Monitor and Maintain Configuration Guide.
View Generated Admin-Tech Files at Any Time	You can view a list of generated admin-tech files and determine which files to copy from your device to Cisco vManage. You can then download the selected admin-tech files to your local device, or delete the downloaded admin-tech files from Cisco vManage, the device, or both.
On-Demand Troubleshooting	You can view detailed information about the flow of traffic from a device. and use this information to assist with troubleshooting.

Feature	Description
Additional Real Time Monitoring Support for Routing, License, Policy, and Other Configuration Options	This feature adds support for real time monitoring of numerous device configuration details including routing, license, policy, Cisco vBond Orchestrator, TCP optimization, SFP, tunnel connection, logging, and Cisco Umbrella information. Real time monitoring in Cisco vManage is similar to using **show** commands in the CLI of a device. There are many device configuration details for Cisco vManage. Only a subset of the device configuration details is added in Cisco SD-WAN Release 20.6.1 and Cisco vManage Release 20.6.1.

Table 5: Cisco vManage Release 20.5.1

Feature	Description
Cisco vManage How-Tos for Cisco vEdge Routers	
Next Hop Action Enhancement in Data Policies	This feature enhances match action conditions in a centralized data policy for parity with the features configured on Cisco vEdge devices. When you are setting up next-hop-loose action, this feature helps to redirect application traffic to an available route when next-hop address is not available.
Clone Service Groups in Cisco vManage	You can easily create copies of service groups, download, and upload service group configuration properties using Cisco vManage.
Authorization and Accounting	You can configure authorization, which authorizes commands that a user enter on a device before the commands can be executed, and accounting, which generates a record of commands that a user executes on a device.
Day 0 WAN Interface Automatic Bandwidth Detection	You can enable a device to automatically determine the bandwidth for WAN interfaces in VPN0 during day 0 onboarding by performing a speed test using an iPerf3 server.
RMA Support for Cisco CSP Devices	You can configure the **Backup** information to enter storage server settings and backup intervals.
Service Area Mapping	To specify the service area that your Microsoft 365 application belongs to, choose an option from the **Service Area** drop-down list.
Enable Layer 7 Health Check (Automatic Tunnels)	You can configure Automatic Tunnels using Cisco vManage.
Support for Zscaler Automatic Provisioning	This feature automates the provisioning of tunnels from Cisco SD-WAN routers to Zscaler. Using your Zscaler partner API credentials, you can automatically provisions tunnels to Zscaler Internet Access (ZIA) Public Service Edges. You can choose **Zscaler** in the Cisco Security Internet Gateway (SIG) and SIG credentials feature templates to automate tunnel provisioning. You can configure provisioning of tunnels from Cisco SD-WAN routers.

Feature	Description
HTTP/HTTPS Proxy Server for Cisco vManage Communication with External Servers	Cisco vManage uses HTTP/HTTPS to access some web services and for some REST API calls. With this feature, you can channel the HTTP/HTTPS communication through an HTTP/HTTPS proxy server.
Best of the Worst Tunnel Selection	You can configure Best Tunnel Path to pick the best path while configuring SLA class.
License Management for Smart Licensing Using Policy, Using Cisco vManage	Cisco vManage shows available DNA licenses, assigns licenses to devices, and reports license consumption to Cisco Smart Software Manager (Cisco SSM).
Role-Based Access Control By Resource Group	You can configure role-based access control (RBAC) based on sites or resource groups in Cisco vManage.
Enhanced Security Monitoring on Cisco SD-WAN Devices	You can view traffic, CPU, memory usage, health and reachability of UTD.
View Loss Percentage, Latency, Jitter, and Octet Information for Tunnels	You can view the loss percentage, latency, jitter, and octet information for tunnels in a single chart option in Cisco vManage.
Optimization of Alarms	This feature optimizes the alarms on Cisco vManage by automatically suppressing redundant alarms. This allows you to easily identify the component that is causing issues. You can view these alarms in **Monitor** > **Alarms**.

Table 6: Cisco vManage Release 20.4.1

Feature	Description
Cisco vManage How-Tos for Cisco vEdge Routers	
Traffic Redirection to SIG Using Data Policy	You can create a data policy where you can selectively define an application list along with other existing match criteria in the data-policy to redirect the application traffic to a Secure Internet Gateway (SIG).
Cisco SD-WAN Multitenancy	For a multitenant Cisco SD-WAN deployment, you can configure Cisco vManage to operate in multitenant mode. Through the multitenant Cisco vManage, you can add new Cisco vSmart Controllers, manage tenants, and view tenants being served by a Cisco vSmart Controller and the OMP statistics for a tenant.
Per-class Application-Aware Routing	This release supports Per-class application-aware routing to Cisco SD-WAN. You can configure Application Probe Class using Cisco vManage.

Feature	Description
Cellular Gateway Configuration	You can configure a supported cellular gateway as an IP pass-through device from the Templates tab.
IPSEC/GRE Tunnel Routing and Load-Balancing Using ECMP	You can now use the SIG template to steer application traffic to Cisco Umbrella or a Third party SIG Provider. You can also configure weights for multiple GRE/IPSEC tunnels for distribution of traffic among multiple tunnels based on the configured weights.
Configure a Cisco vEdge Device as an NTP Parent and Optionally to Support NTP in Symmetric Active Mode.	Use the Cisco vManage device CLI template to configure a Cisco vEdge device as an NTP parent and configure the device to support NTP in symmetric active mode.
Support for Password Policies using Cisco AAA	You can now configure password policies to ensure that your users use strong passwords and can be customized based on your requirements. To configure password policies, push the `password-policy` commands to your device using Cisco vManage device CLI templates.
Policy Matching with ICMP Message	You can now define a new match condition that can be used to specify a list of ICMP messages for centralized data policies, localized data policies, and Application-Aware Routing policies.
Static Route Tracker for Service VPNs for Cisco vEdge Devices	To configure Static Route Tracking on Cisco vManage, configure an endpoint tracker using Cisco System template, and Configure a static route using the Cisco VPN template.
VRRP Interface Tracking for Cisco vEdge Devices	Use the Cisco vManage device CLI template to add an interface or a SIG container to a track list and configure tracking and priority decrement for that interface and container.

Table 7: Cisco vManage Release 20.3.1

Feature	Description
Cisco vManage How-Tos for Cisco vEdge Routers	
Self Zone Policy for Zone-Based Firewalls	This feature allows you to define firewall policies for incoming and outgoing traffic between a self zone of an edge router and another zone. When a self zone is configured with another zone, the traffic in this zone pair is filtered as per the applied firewall policy.
Extended DNS (EDNS) and Local Domain Bypass Support with Cisco Umbrella Integration	You can now configure Cisco Umbrella registration, define domain lists, and configure Umbrella DNS policy from the **Configuration** > **Security** screen in Cisco vManage.

Feature	Description
New Configuration Workflow for Cloud onRamp for SaaS for Cisco vEdge devices	Using Cloud onRamp for SaaS, you can select specific SaaS applications and interfaces, and let Cisco SD-WAN determine the best performing path for each SaaS applications.
Dynamic On-Demand Tunnels	You can configure on-demand tunnels between any two Cisco SD-WAN spoke devices. These tunnels are triggered to be set up only when there is traffic between the two devices.
Flexible Topologies	You can configure the Stackwise Virtual Switch Link (SVL) and uplink ports of switches, and Cisco CSP data ports using the **Port Connectivity** configuration settings of Cloud OnRamp for Colocation cluster .
Route Leaking Between Transport VPN and Service VPNs	You can configure route leaking between transport VPN and service VPNs using the **Global Route Leak** option under the VPN feature template.
Service insertion tracker support	You can configure service chaining for a device, from the **Service** tab.
Configure Sessions in Cisco vManage	This feature lets you see all the HTTP sessions that are open within Cisco vManage. It gives you details about the username, source IP address, domain of the user, and other information. A user with User Management Write access, or a netadmin user can trigger a log out of any suspicious user's session.
TACACS Authentication	You can configure the TACACS authentication for users using the **TACACS** configuration settings of Cloud OnRamp for Colocation cluster.
Network Assurance –VNFs: Stop/Start/Restart	You can now stop, start, or restart VNFs on Cisco CSP devices from the **Colocation Clusters** tab.
Cisco vManage Cluster Upgrade	This feature outlines the upgrade procedure for Cisco vManage servers in a cluster to Cisco vManage Release 20.3.1. To upgrade Cisco vManage instances in a Cluster, use the **Tools** > **SSH Terminal** screen.
Embedded Packet Capture	This feature is an onboard packet capture facility that allows network administrators to capture packets flowing to, through, and from the device. The administrator can Manage to analyze these packets locally or save and export them for offline analysis through Cisco vManage. This feature gathers information about the packet format and therefore helps in application analysis, security, and troubleshooting.