Release Notes for Cisco vEdge Devices, Cisco SD-WAN Release 20.5.x

First Published: 2021-03-22

Last Modified: 2021-05-18

Release Notes for Cisco vEdge Device, Cisco SD-WAN Release 20.5.x

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.

These release notes accompany the Cisco SD-WAN Release 20.5.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.

For release information about Cisco IOS XE Catalyst SD-WAN devices, refer to Release Notes for Cisco IOS XE SD-WAN Devices, Cisco IOS XE Release Bengaluru 17.5.x.

For release information about Cisco SD-WAN Controllers, refer to Release Notes for Cisco SD-WAN Controllers, Cisco SD-WAN Release 20.5.x

What's New for Cisco SD-WAN Release 20.5.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 20.5.1

Feature	Description
Systems and Interfaces	

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. Beginning Cisco vManage Release 20.5.1, you can channel the HTTP/HTTPS communication through an HTTP/HTTPS proxy server.
Authorization and Accounting	This feature provides for the configuration of authorization, which authorizes commands that a user enters on a device before the commands can be executed, and accounting, which generates a record of commands that a user executes on a device.
Role-Based Access Control By Resource Group	This feature introduces role-based access control (RBAC) based on sites or resource groups. It is a method of authorizing system access for users based on a combination of user groups and resource groups. For large Cisco SD-WAN deployments across multiple geographical locations, this feature helps you to split the network administration among different regional administrators.
Migrate Single-Tenant Cisco SD-WAN Overlay to Multitenant Cisco SD-WAN Deployment	You can migrate a single-tenant Cisco SD-WAN overlay to a multitenant deployment using a sequence of Cisco vManage API calls.
Routing	
Increased OMP Path Limit for Cisco vSmart Controllers	With this feature, the number of paths that can be exchanged between Cisco vSmart Controllers is increased to 128 limit.
Policies	
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.
Best of the Worst Tunnel Selection	This feature introduces a new policy action **fallback-to-best-path** to pick the best path or color out of the available colors. When the data traffic does not meet any of the SLA class requirements, this feature allows you to select the best tunnel path criteria sequence using the **Fallback Best Tunnel** option under each SLA class to avoid packet loss.
Configure Dampening on Data Plane Tunnels	This feature introduces a configurable delay (dampening) mechanism on data plane tunnels to minimize the effects of tunnel flapping on the WAN links. The dampening process removes a tunnel from the SLA class until it stops flapping and becomes stable.
Security	

Feature	Description
Enable Layer 7 Health Check (Automatic Tunnels)	This features integrates the Layer 7 Health Check feature with automatic tunnels to SIGs. When you create an automatic tunnel using the Cisco Secure Internet Gateway (SIG) template to Zscaler or Cisco Umbrella, a tracker is also created to monitor and load balance or failover tunnels. You can customize the parameters based on which the tracker load balances or fails over tunnels.
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.
High Availability	
Disaster Recovery for a Single Node Cisco vManage Cluster	This feature provides support for disaster recovery for a Cisco vManage deployment with a single primary node.
Cloud OnRamp	
RMA Support for Cisco CSP Devices (Cloud onRamp for Colocation)	This feature allows you to replace a faulty CSP device by creating backup copies of the device, and then restoring the replacement device to a state it was in before the replacement. The VMs running in HA mode operate uninterrupted with continuous flow of traffic during device replacement.
Clone Service Groups in Cisco vManage (Cloud onRamp for Colocation)	This feature allows you to create copies of service groups for different RBAC users, without having to enter the same configuration information multiple times. By cloning a service group, you can easily create service chains by leveraging the stored service chain templates.
Colocation Multitenancy Using Role-Based Access Control (Cloud onRamp for Colocation)	This feature enables a service provider to manage multiple colocation clusters and share these clusters across tenants by using multiple colocation groups. In a multitenant setup, service providers don't need to deploy a unique colocation cluster for each tenant. Instead, the hardware resources of a colocation cluster are shared across multiple tenants. With multitenancy, service providers ensure that tenants view only their data by restricting access based on roles of individual tenant users.
Monitor and Maintain	
View Loss Percentage, Latency, Jitter, and Octet Information for Tunnels	This feature provides a single chart option in Cisco vManage for viewing tunnel information, such as packet loss, latency, jitter, and octets.
Enhanced Security Monitoring on Cisco SD-WAN Devices	This feature enhances the monitoring of Unified Threat Defense (UTD) features on Cisco SD-WAN devices. The feature allows you to view the CPU, memory, and traffic usage on your device. You can also view the health of individual UTD features.

Feature	Description
Optimization of Alarms	This feature optimises 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**.
vEdge Packet Tracer	This feature is used to debug any packet loss on Cisco vEdge devices in the forwarding plane.
SNMP	
Support for SNMPv3 AES-256 bit Authentication Protocol	Support introduced for AES-256 bit Authentication Protocol called SHA-256.

Important Notes, Known Behavior, and Workaround

- 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.
- In Cisco SD-WAN Release 20.5.1, the cloud-init bootstrap configuration that you generate for the Cisco vEdge Cloud Router cannot be used for deploying the Cisco Cloud vEdge Router running on Cisco SD-WAN Release 20.5.1. However, you can use the bootstrap configuration for deploying the Cisco vEdge Cloud Router running on Cisco SD-WAN Release 20.4.1 and earlier versions.
- Starting from Cisco SD-WAN Release 20.4.1.1, Microsoft Azure environment support is limited to deployment of Cisco SD-WAN controllers (Cisco vBond orchestrator, Cisco vSmart controller, and Cisco vManage) and the Cisco vEdge Cloud Router is not supported in Microsoft Azure.
- Cisco vManage Release 20.3.1 implements a hardened security posture to comply with FedRamp guidelines. As a result, your vAnalytics login credentials that are stored locally get erased on upgrading the software, and you cannot access the vAnalytics service directly through Cisco SD-WAN Manager. In this case, log in to vAnalytics using this URL: https://analytics.viptela.com. If you can't find your vAnalytics login credentials, open a case with Cisco TAC support.
- For Cisco SD-WAN Release 20.4.1, you must run the messaging server on all the active instances of the Cisco SD-WAN Manager cluster when deploying the Cisco SD-WAN Manager cluster. See the High Availability Configuration Guide for vEdge Routers for more information.
- For information about upgarde paths, see Cisco vManage Upgrade Paths.

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 20.5.1

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 20.5.1

Bug ID	Description
CSCvv61267	PMTUD is not able to calculate MTU correctly when MTU changes in path on vEdge.
CSCvv76467	vEdge-5000:Auto IP feature not working on vedge5k
CSCvw31987	vEdge 1000 rebooted with Software initiated - Daemon 'ftmd' failed
CSCvw54152	vEdge 5k-LLQ policer rate on interface 10ge0/0 change after reboot on version 20.1.932
CSCvx00210	vEdge 5k crashed with reason "Software initiated - FP core watchdog fail"
CSCvx50343	Routes redistributed to the OSPF/BGP that shouldn't be filtered by the routing-policy are filtered
CSCvx63715	vEdge "show interface" command shows wrong information

Open Bugs for Cisco SD-WAN Release 20.5.1

Bug ID	Description
CSCvv25745	ISR1100/ISR1100X - Cisco vManage not showing the correct hostname for ISR1100/ISR1100X device
CSCvw28477	version property of vEdge not populated on the Cisco vManage
CSCvw63400	Incorrect MIB values in viptelaDevices for ISR11004G, ISR11006G, ISR11004GLTE
CSCvx26925	Tracker modification under interface does not take proper effect
CSCvx43829	vEdge_Cloud interfaces operation status goes down after upgrade to 20.4.1
CSCvx57679	vedge crash after route leak config
CSCvy08234	SNMPv3 AES256 trap with msgAuthoritativeEngineBoots and msgAuthoritativeEngineTime set to zero
CSCvw63400	Incorrect MIB values in viptelaDevices for ISR11004G, ISR11006G, ISR11004GLTE
CSCvw91847	In vEdge5K the default route in RIB table is not getting programmed in FIB table properly
CSCvx16541	vEdge-1000 FTMD crash with 19.2.31 (FP core watchdog fail)

Bug ID	Description
CSCvx62654	FTMD crash being observed on a vEdge 5000 with FEC ADAPTIVE configuration enabled.
CSCvx81266	vEdge OMP stuck in init state with vSmarts
CSCvx83356	Global Route leaking feature do not import routes if the route policy name is lengthy
CSCvx85654	shaping-rate value on main interface doesn't apply on traffic through sub interface on Vedge 5k

Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Server Recommendations

For compatibility information and server recommendations, see Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Server Recommendations.

Supported Devices

For device compatibility information, see Cisco SD-WAN Device Compatibility.

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)

© 2021 Cisco Systems, Inc. All rights reserved.