Cisco SD-WAN (Viptela) Release Notes for Release 18.2

Release Notes for Release 18.2

These release notes accompany Viptela Software Release 18.2, for Release 18.2.0. The Viptela software runs on all Viptela devices, including vSmart controllers, vEdge routers, vBond orchestrators, and vManage NMSs.

Viptela Software Release 18.2
February 17, 2019
Revision 2

Product Features

Below are the main product features in Viptela Software Release 18.2:

- **Cloud onRamp for Microsoft Azure** —You can create a Gateway virtual network (VNet) for hosting vEdge Cloud router instances in different Azure locations in the public internet. *See Configuring Cloud onRamp Service and Cloud OnRamp with Azure .*
- **Enterprise root certificates** —In vManage NMS, you can use enterprise root certificates to authorize the Viptela controller devices—including vSmart controllers, vBond orchestrators, and vManage NMSs—and vEdge Cloud routers in the overlay network. You can customize the certificate signing request (CSR) properties in the enterprise root certificate for vManage and vSmart controller devices. *See Configure Certificate Authorization Settings for Controller Devices and Settings .*
- **Export compliance** —vEdge routers that are hosted in countries affected by United States government embargoes cannot connect to overlay network controllers (vBond orchestrators, vManage NMSs, and vSmart controllers) that are hosted in the Cisco cloud. Any vEdge router from an embargoed country that attempts to connect to one of these controllers will be disabled. *See Deploy the vEdge Routers .*
- **IPsec in VPN 0** —You can configure IPsec on tunnels in the transport interface (VPN 0). *See Configuring IKE-Enabled IPsec Tunnels and interface ipsec .*
- **Localized data policy configuration wizard** —A vManage configuration wizard allows you to create localized data policies. *See Configuring Localized Data Policy for IPv4 , Configuring Localized Data Policy for IPv6 , and Policies .*
- **Optional rows in feature configuration templates** —In some sections of some feature configuration templates, you can mark the section as an optional row to set the parameters is the section as being variables. When you then attach the device configuration template to a device, you enter the values for these parameters. *See Use Variable Values in Configuration Templates .*
- **Reverse proxy** —You can use a reverse proxy as an intermediary to pass control traffic between VIptela controllers and vEdge routers. *See Enable Reverse Proxy .*
- **vManage configuration database** —The underlying software used for the vManage configuration database has changed.
- **vManage server logo** —You can change the vManage web application server logo and load a new custom logo. *See How To Load a Custom vManage Application Server Logo.*
- **vManage troubleshooting tools** —vManage NMS provides troubleshooting tools for running speed tests and capturing packets. *See Network .*
- **Zone-based firewalls** —Zone-based firewalls are a type of localized data policy that allows stateful inspection of TCP, UDP, and ICMP data traffic flows. A zone is a grouping of one or more VPNs. *See Zone-Based Firewalls and Security .*

Command Changes

New and Modified Configuration Commands

Command	Hierarchy	New	Modified	Comments

cipher-suite	vpn interface ipsec ike		X	
icmp-redirect-disable	vpn interface	X		
ip ipsec-route	vpn	X		
zone	policy	X		For zone-based firewalls.
zone-based-policy	policy	X		For zone-based firewalls.
zone-pair	policy	X		For zone-based firewalls.
zone-to-nozone-internet	policy	X		For zone-based firewalls.

New and Modified Operational Commands

Command	New	Modified	Comments
clear policy zbfw filter-statistics	X		For zone-based firewalls.
clear policy zbfw global-statistics	X		For zone-based firewalls.
clear policy zbfw sessions	X		For zone-based firewalls.
clear reverse-proxy context	X		On vEdge routers.
show certificate reverse-proxy	X		On vEdge routers.
show control connections		X	Add Proxy column, for vEdge routers.
show hardware poe	X		
show orchestrator reverse-proxy-mapping	X		On vBond orchestrators.
show policy zbfw filter-statistics	X		For zone-based firewalls.
show policy zbfw global-statistics	X		For zone-based firewalls.
show policy zbfw sessions	X		For zone-based firewalls.

New and Modified vManage Screens

Field	Screen	New	Modified	Comments
Add Reverse Proxy	Configuration ▶ Devices ▶ Controllers	X		
Controller Certificate Authorization	Administration ▶ Settings		X	Add Enterprise Root Certificate option.
Localized data policy	Configuration ▶ Policies	X		Add configuration wizard for localized data policy.
Maintenance window	Administration ▶ Settings		X	You can cancel a maintenance window.
Reverse Proxy	Administration ▶ Settings	X		

Security policy	Configuration ► Security	X		Configuration wizard for zone-based firewalls.

REST API Changes

The JSON output for the following REST API calls has changed:

- https:// *vmanage-ip-address* /dataservice/device/action/changepartition
- https:// *vmanage-ip-address* /dataservice/device/action/defaultpartition
- https:// *vmanage-ip-address* /dataservice/device/action/install

Upgrade to Release 18.2

For details on upgrading the Viptela software, see Software Installation and Upgrade .

Note: You cannot install a Release 17.2 or earlier image on a vEdge router that is running Release 18.2.0 or later. This is the result of security enhancements implemented in Release 18.2.0. Note that if a Release 17.2 or earlier image is already present on the router, you can activate it.

To upgrade to Release 18.2:

1. In vManage NMS, select the Maintenance ► Software Upgrade screen.
2. Upgrade the controller devices to Release 18.2 in the following order:
    a. First, upgrade the vManage NMSs in the overlay network.
    b. Then, upgrade the vBond orchestrators.
    c. Next, upgrade the vSmart controllers.
3. Select the Monitor ► Network screen.
4. Select the devices you just upgraded, click the Control Connections tab, and verify that control connections have been established.
5. Select the Maintenance ► Software Upgrade screen, and upgrade the vEdge routers.

In order for you to upgrade a vManage cluster to Release 18.2.0, the username and associated password that initially formed the NMS cluster must still exist and be unchanged. Using this account is required because the underlying vManage configuration database in Release 18.2.0 has changed. If the username and password no longer exist, or if the password has been changed, contact Customer Support for help upgrading the software.

Note: After you upgrade software on a vManage NMS to any major release, you can never downgrade it to a previous major release. For example, if you upgrade the vManage NMS to Release 18.2, you can never downgrade it to Release 18.1 or to any earlier software release.

The major release number consists of the first two numbers in the software release number. For the Viptela software, 18.2 and 18.1 are examples of major releases. Releases 18.2.0 and 18.1.0 denote the initial releases, and Releases 18.2.1 and 18.1.1 are maintenance releases.

Upgrade from Release 16.2 and Earlier Software Releases

Because of software changes in Release 16.3, you must modify the router configuration as follows before you upgrade from Release 16.2 or earlier to Release 18.2:

- Use **max-control-connections 0** instead of the **no control-connections** command in **tunnel-interface** configuration mode. The **no control-connections** command has been deprecated and has no effect on releases 17.2 and later.

- You can no longer configure RED drops on low-latency queuing (LLQ; queue 0). That is, if you include the **policy qos-scheduler scheduling llq** command in the configuration, you cannot configure **drops red-drop** in the same QoS scheduler. If your vEdge router has this configuration, remove it before upgrading to Release 17.2. If you do not remove the RED drop configuration, the configuration process (confd) will fail after you perform the software upgrade, and the Viptela devices will roll back to their previous configuration.

- For vEdge 2000 routers, you can no longer configure interfaces that are not present in the router. That is, the interface names in the configuration must match the type of PIM installed in the router. For example, if the PIM module in slot 1 is a 10-Gigabit Ethernet PIM, the configuration must refer to the proper interface name, for example, **10ge1/0** , and not **ge1/0** . If the interface name does not match the PIM type, the software upgrade will fail. Before you upgrade from Release 16.2 or earlier to Release 17.2, ensure that the interface names in the router configurations are correct.

Caveats

Hardware Caveats

The following are known behaviors of the Viptela hardware:

- On vEdge 1000 routers, support for USB controllers is disabled by default. To attach an LTE USB dongle to a vEdge 1000 router, first attach the dongle, and then enable support for USB controllers on the vEdge router, by adding the **system usb-controller** command to the configuration. When you enter this command in the configuration, the router immediately reboots. Then, when the router comes back up, continue with the router configuration. Also for vEdge 1000 routers, if you plug in an LTE USB dongle after you have enabled the USB controller, or if you hot swap an LTE USB dongle after you have enabled the USB controller, you must reboot the router in order for the USB dongle to be recognized. For information about enabling the USB controller, see USB Dongle for Cellular Connection .

- For vEdge 2000 routers, if you change the PIM type from a 1-Gigabit Ethernet to a 10-Gigabit Ethernet PIM, or vice versa, possibly as part of an RMA process, follow these steps:
  1. Delete the configuration for the old PIM (the PIM you are returning as part of the RMA process).
  2. Remove the old PIM, and return it as part of the RMA process.
  3. Insert the new PIM (the PIM you received as part of the RMA process).
  4. Reboot the vEdge 2000 router.
  5. Configure the interfaces for the new PIM.

- On a vEdge 5000 router, you cannot enable TCP optimization by configuring the **tcp-optimization-enabled** command.

Software Caveats

The following are known behaviors of the Viptela software:

Cellular Interfaces

- The vEdge 100wm router United States certification allows operation only on non-DFS channels.

- When you are configuring primary and last-resort cellular interfaces with high control hello interval and tolerance values, note the following caveats:

  – When you configure two interfaces, one as the primary interface and the other as the last-resort interface, and when you configure a high control hello interval or tolerance values on the last-resort interface (using the **hello-interval** and **hello-tolerance** commands, respectively, the OMP state indicates init-in-gr even though it shows that the control connections and BFD are both Up. This issue was resolved in Release 16.2.3. However, the following caveats exist:
  — You can configure only one interface with a high hello interval and tolerance value. This interface can be either the primary or the last-resort interface.
  — In certain cases, such as when you reboot the router or when you issue shutdown and no shutdown commands on the

interfaces, the control connections might take longer than expected to establish. In this case, it is recommended that you issue the **request port-hop** command for the desired color. You can also choose to wait for the vEdge router to initiate an implicit port-hop operation. The **request port-hop** command or the implicit port hop initiates the control connection on a new port. When the new connection is established, the stale entry is flushed from the vSmart controllers.

  - If the primary interface is Up, as indicated by the presence of a control connection and a BFD session, and if you configure a last-resort interface with higher values of hello interval and tolerance than the primary interface, if you issue a **shutdown** command, followed by a **no shutdown** command on the last-resort interface, the last-resort interface comes up and continuously tries to establish control connections. Several minutes can elapse before the operational status of the last-resort interfaces changes to Down. If this situation occurs, it is recommended that you issue a **request port-hop** command for the desired color.

  - If you have configured a primary interface and a last-resort interface that has higher hello interval and tolerance values than the primary interface, and if the last-resort interface has control connections to two vSmart controllers, if you issue a **shutdown** command, followed by a **no shutdown** command on the last-resort interface, a control connection comes up within a reasonable amount of time with only one of the vSmart controllers. The control connection with the second vSmart controller might not come up until the timer value configured in the hello tolerance has passed. If this situation occurs, it is recommended that you issue a **request port-hop** command for the desired color.

- When you activate the configuration on a router with cellular interfaces, the primary interfaces (that is, those interfaces not configured as circuits of last resort) and the circuit of last resort come up. In this process, all the interfaces begin the process of establishing control and BFD connections. When one or more of the primary interfaces establishes a TLOC connection, the circuit of last resort shuts itself down because it is not needed. During this shutdown process, the circuit of last resort triggers a BFD TLOC Down alarm and a Control TLOC Down alarm on the vEdge router. These two alarms are cleared only when all the primary interfaces lose their BFD connections to remote nodes and the circuit of last resort activates itself. This generation and clearing of alarms is expected behavior.

- For cellular interface profile, the profile number can be 0 through 15. Profile number 16 is reserved, and you cannot modify it.

Configuration and Command-Line Interface

- When upgrade to Release 17.2 from any prior Viptela software release, the CLI history on the Viptela device is lost. The CLI history is the list of commands previously entered at the CLI prompt. You typically access the history using the up and down arrows on the kayboard or by typing Ctrl-P and Ctrl-N. When you upgrade from Release 17.2 to a later software release, the CLI history will be maintained.

- When you issue the **request reset configuration** command on a vEdge Cloud router, a vManage NMS, or a vSmart controller, the software pointer to the device's certificate might be cleared even though the certificate itself is not deleted. When the device reboots and comes back up, installation of a new certificate fails, because the certificate is already present. To recover from this situation, issue the **request software reset** command.

Control and BFD Connections

- When a vBond orchestrator, vManage NMS, or vSmart controller goes down for any reason and the vEdge routers remain up, when the controller device comes back up, the connection between it and the vEdge router might shut down and restart, and in some cases the BFD sessions on the vEdge router might shut down and restart. This behavior occurs because of port hopping: When one device loses its control connection to another device, it port hops to another port in an attempt to reestablish the connection. For more information, see the Firewall Ports for Viptela Deployments article. Two examples illustrate when this might occur:

  - When a vBond orchestrator goes down for any reason, the vManage NMS might take down all connections to the vEdge routers. The sequence of events that occurs is as follows: When the vBond orchestrator crashes, the vManage NMS might lose or close all its control connections. The vManage NMS then port hops, to try to establish connections to the vSmart controllers on a different port. This port hopping on the vManage NMS shuts down and then restarts all its control connections, including those to the vEdge routers.

  - All control sessions on all vSmart controllers go down, and BFD sessions on the vEdge routers remain up. When any one of the vSmart controllers comes back up, the BFD sessions on the routers go down and then come back up because the vEdge routers have already port hopped to a different port in an attempt to reconnect to the vSmart controllers.

- When a vEdge router running Release 16.2 or later is behind a symmetric NAT device, it can establish BFD sessions with remote vEdge routers only if the remote routers are running Release 16.2 or later. These routers cannot establish BFD sessions with a remote vEdge router that is running a software release earlier than Release 16.2.0.

- When you add or remove an IPv4 address on a tunnel interface (TLOC) that already has an IPv6 address, or when you add or remove an IPv6 address on a TLOC that already has an IPv4 address, the control and data plane connections for that interface go down and then come back up.

- Release 16.3 introduces a feature that allows you to configure the preferred tunnel interface to use to exchange traffic with the vManage NMS. In the vManage NMS, you configure this on cellular, Ethernet, and PPP Interface feature templates, in the vManage Connection Preference field under Tunnel Interface. In the CLI, you configure this with the **vmanage-connection-preference** command. The preference value can be from 0 through 8, with a lower number being more preferred. The default value is 5. If you set the preference value to 0, that tunnel interface is never used to exchange traffic with the vManage NMS, and it is never able to send or receive any overlay network control traffic.
  With this configuration option, there is one situation in which you can accidentally configure a device such that it loses all its control connections to all Viptela controller devices (the vManage NMSs and the vSmart controllers). If you create feature templates and then consolidate them into a device template for the first time, the NMS software checks whether each device has at least one tunnel interface. If not, a software error is displayed. However, when a device template is already attached to a device, if you modify one of its feature templates such that the connection preference on all tunnel interfaces is 0, when you update the device with the changes, no software check is performed, because only the configuration changes are pushed to the device, not the entire device template. As a result, these devices lose all their control connections. To avoid this issue, ensure that the vManage connection preference on at least one tunnel interface is set either to the default or to a non-0 preference value.

Interfaces

- On virtual interfaces, such as IRB, loopback, and system interfaces, the duplex and speed attributes do not apply, and you cannot configure these properties on the interfaces.

- When a vEdge router has two or more NAT interfaces, and hence two or more DIA connections to the internet, by default, data traffic is forwarding on the NAT interfaces using ECMP. To direct data traffic to a specific DIA interface, configure a centralized data policy on the vSmart controller that sets two actions— **nat** and **local-tloc** color. In the **local-tloc** color action, specify the color of the TLOC that connects to the desired DIA connection.

IPv6

- You can configure IPv6 only on physical interfaces (**ge** and **eth** interfaces), loopback interfaces (**loopback0** , **loopback1** , and so on), and on subinterfaces (such as **ge0/1.1**).

- For IPv6 WAN interfaces in VPN 0, you cannot configure more than two TLOCs on the vEdge router. If you configure more than two, control connections between the router and the Viptela controllers might not come up.

- IPv6 transport is supported over IPsec encapsulation. GRE encapsulation is not supported.

- You cannot configure NAT and TLOC extensions on IPv6 interfaces.

IRB

- On integrated routing and bridging (IRB) interfaces, you cannot configure autonegotiation .

NAT

- When you reboot a vSmart controller, the BFD sessions for all symmetric NAT devices go down and come back up. This is expected behavior.

Routing Protocols

- When a vEdge router transport interface is using an old IPv6 SLAAC address for control connections or BFD sessions, or both, the IP address used for control connections and BFD might become out of sync with the actual IPv6 address. This situation can happen when the IPv6 address that SLAAC advertises from the gateway router changes suddenly and the old IPv6 address has not first been invalidated. As a workaround, if the router has no mechanism to invalidate older prefixes when the IPv6 prefix changes, first remove the **router-advertisement** configuration on the default gateway router and then change the IPv6 address. To resolve this problem when it occurs on a vEdge router, shut down the interface and then restart it; that is, issue a **shutdown** command, followed by a **no shutdown** command.

Security

- It is recommended that you use IKE Version 2 only with Palo Alto Networks and Ubuntu strongSwan systems only. Viptela has not tested IKE Version 2 with other systems.

SNMP

- When you configure an SNMP trap target address, you must use an IPv4 address.
- The Viptela interface MIB supports both 32-bit and 64-bit counters, and by default sends 64-bit counters. If you are using an SNMP monitoring tool that does not recognize 64-bit counters, configure it to read 32-bit MIB counters.
- On a vEdge router, if you perform an snmpwalk getnext request for an OID for which there is no information, the response that is returned is the next available instance of that OID. This is the expected behavior.

System

- The Viptela software includes a version of OpenSSH that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs: CVE-2016-10009 and CVE-2016-10012.

Virtual Machines

- For a vEdge Cloud VM instance on the KVM hypervisor, for Viptela Releases 16.2.2 and later, it is recommended that you use virtio interfaces. For software versions earlier than Release 16.2.2, if you are using the Ubuntu 14.04 or 16.04 LTS operating system, you can use IDE, virtio, or virtio-scsi interfaces.

vManage NMS

- On a Viptela device that is being managed by a vManage NMS system, if you edit the device's configuration from the CLI, when you issue the **commit** command, you are prompted to confirm the commit operation. For example:
  vEdge(config-banner)# **commit**
  The following warnings were generated:
  'system is-vmanaged': This device is being managed by the vManage. Any configuration changes to this device will be overwritten by the vManage.
  Proceed? [yes,no]
  You must enter either **yes** or **no** in response to this prompt.
  During the period of time between when you type commit and when you type either **yes** or **no** , the device's configuration database is locked. When the configuration database on a device is locked, the vManage NMS is not able to push a configuration to the device, and from the vManage NMS, you are not able to switch the device to CLI mode.
- The members of a vManage cluster rely on timestamps to synchronize data and to track device uptime. For this time-dependent data to remain accurate, do not change the clock time on any one of the vManage servers of the cluster after you create the cluster.
- When you use the vManage Maintenance ► Software Upgrade screen to set the default software version for a network device, that device must be running Release 16.1 or later at the time you set the default software version. If the network device is running Release 15.4 or earlier, use the CLI **request software set-default** command to set the default software version for that device.
- When you are using a vManage cluster, when you are bringing up new vManage NMS in the cluster, use an existing vManage NMS to install the certificate on the new vManage NMS.
- In vManage feature configuration templates, for the passwords listed below, you cannot enter a cleartext password that starts with $4 or $8. You can, however, use such passwords when you are configuring from the CLI.
  - Neighbor password, in the BGP feature configuration template
  - User password, in the Cellular Profile feature configuration template
  - Authentication type password and privacy type password, in the SNMP feature configuration template
  - RADIUS secret key and TACACS+ secret key, in the System feature configuration template
  - IEEE 802.1X secret key, in the VPN Interface Ethernet feature configuration template
  - IPsec IKE authentication preshared key, in the VPN Interface IPsec feature configuration template

  - CHAP and PAP passwords, in the VPN Interface PPP Ethernet feature configuration template
  - Wireless LAN WPA key, in the WiFi SSID feature configuration template

Outstanding Issues

The following are outstanding issues in Viptela Software Release 18.2. The number following each issue is the bug number in the Viptela bug-tracking database.

Cellular Interfaces

- If you configure IPv6 on a cellular interface, the control connections might go down and come back up continuously. [VIP-21970]
- On a vEdge 100m-NA router, when you configure profile 1 for a wireless WAN, you might see the error "Aborted: 'vpn 0 interface cellular0 profile': Invalid profile 1 : APN missing". [VIP-31721]

Configuration and Command-Line Interface

- When you issue the **show vrrp interfaces** command from the vEdge router's CLI, the CLI might not recognize the command and might show a "syntax error: unknown argument" error message. [VIP-23918]
- If a physical interface is part of a bridge, you cannot adjust the MTU on the interface. As a result, the 802.1x interface's MTU has to be lowered to 1496. If the interface needs to also run OSPF, this MTU size can cause an MTU mismatch with other interfaces that have an MTU of 1500. [VIP-26759]
- When two routes exist to the same neighbor, if you specify a single IP address in the **show ip routes** command, the command might return only one of the routes, but if you specify an IPv4 prefix and prefix length, the command returns both routes. [VIP-32736]
- With the **ping source ip-address** command, if you type it as **ping so ip-address** , the CLI does not autocomplete **so** and the command fails. You must type out the keyword **source** . [VIP-36087]
- In the same sequence in a data policy that you configure on a vManage server, you might not be able to configure both individual ports and port ranges. [VIP-36864]
- When you use the **show ip route** command to query a route that is not present in the route table, the command might return no output or no failure message. [VIP-36725]
- When you configure a hostname that includes a period (.), only the portion of the hostname before the period is displayed. As a workaround, use an underscore (_) or a hyphen (-). [VIP-38369]
- A color that you configure using a vManage configuration template might not be applied correctly on a vEdge router. [VIP-38735]

Forwarding

- For IEEE 802.1X, you cannot configure a RADIUS server for MAC authentication bypass (MAB). [VIP-18492]
- In application-aware routing policy, the salesforce_chatter, oracle_rac, and google_photos applications might not be classified properly. [VIP-21866]
- When you switch data traffic from one tunnel to another (for example, from a biz-ethernet to an lte tunnel), a small amount of traffic might be lost. [VIP-27992]
- For a source and destination NAT, return traffic might not be able to reach the VPN that originates the session. [VIP-31299]
- When you configure inbound and outbound port mirroring on the same interface, traffic might be mirrored only in one direction. [VIP-33247]
- When you have a localized data policy (ACL) that mirrors traffic on an interface in both directions, if you change the IP address of the interface and the mirror destination but do not remove the ACL, the outbound mirroring continues to work but the inbound mirroring stops working. If you then remove and reapply, the ACL, the mirroring again works in both directions. [VIP-33275]

- If you disable deep packet inspection (DPI) on a vEdge router, traffic directed towards queue 0 (LLQ) might become bursty or might be dropped. [VIP-34211]
- When you configure a cellular interface as a last-resort interface, the cellular interface might remain up at all times. [VIP-34495]
- The vEdge router might not fragment packets that are larger than the interface's MTU. [VIP-35044]
- Routes might be installed in the routing table with the incorrect color. [VIP-35088]
- Traffic might be blackholed because of stale BFD sessions. This happens in a scenario when there are two vEdge routers at a site, both configured with TLOC extension between them, and the circuit that they are connected to goes down. One router clears all its BFD sessions, but the second one does not, so all traffic is sent to the uncleared BFD sessions and is blackholed. [VIP-35113]
- On a vBond orchestrator, if you configure **allow-service netconf** , the vBond orchestrator does not open TCP port 830 and thus cannot connect to the vManage NMS. As a workaround, configure **allow-service all** . [VIP-35916]
- When you enable TCP optimization, all TCP flows might fail. [VIP-37974]
- A GRE tunnel might negotiate an MTU size of 512 bytes, so packets larger than about 500 bytes cannot be sent over the tunnel. [VIP-38791]

Interfaces

- When a vEdge VRRP master is connected to a Cisco switch, the switch might report error messages indicating that the source MAC address is invalid. [VIP-28922]
- When a VRRP backup vEdge router that has been promoted to a master again becomes a backup, other devices continue to point to the MAC address for the backup router, and traffic is blackholed until ARP cache on the other devices expires and is updated with the correct MAC address of master vEdge, a process that typically takes a few minutes. [VIP-33722]
- On a vEdge router that has two TLOCs, one on a loopback interface and the second on a physical interface, when the physical interface goes down, the loopback interface might not be able to forward traffic. [VIP-34646]
- You might not be able to configure the Cloud Onramp VPC even when vEdge routers are present. [VIP-34655]
- When you configure interface tracking on two interfaces in a vEdge router, the router might crash. [VIP-38829]

Policy

- You can no longer configure a QoS map (with the **vpn interface qos-map** command) on a VLAN interface (also called a subinterface). You also cannot configure the aggregate traffic rate on a VLAN interface (with the **vpn interface shaping-rate** command). [VIP-22820]
- A centralized policy that is pushed from the vSmart controller to the vEdge routers might not be applied on the routers. [VIP-27046]
- On vEdge routers, the **show policy access-list-counters** command might not display any values in the Bytes column. [VIP-28890]
- In vManage NMS, when you use the policy configuration wizard to create policies for a mesh topology, you might need to create an additional policy using a CLI template for the mesh policy to work. This situation is known to occur in a network that has two regions, where each region is mesh that is a subset of the entire network, where each region has its own data center, and where the branch vEdge routers in one region communicate with branch routers in the other region through the data centers. We will call these Region 1 and Region 2. Assume that Region 1 has a control policy that advertises its TLOCs to the data center in Region 2, and Region 2 has a control policy that prevents the spokes and data center in Region 2 from advertising TLOCs to the spokes in Region 1. The result is that the data center in Region 2 repeatedly attempts to form control tunnels to the data center in Region 1, but these attempts fail. As a workaround, you must a policy using a CLI template that allows the data center in Region 2 to exchange TLOCs with the data center in Region 1 and then attach that policy to the vEdge routers. [VIP-29933]
- On x86 vEdge routers (Cloud vEdge routers and vEdge 5000 routers), when you configure QoS schedulers, any traffic that queued in a queue to which no bandwidth or buffer is assigned will be dropped. [VIP-38008]
- In the vManage Centralized Policy UI Builder, the Membership has no options to accept or reject and no way to change the default action. These options are all available in CLI and need to be added to the UI builder for the same capabilities. [VIP-38730]
- An implicit or a configured ACL might not work on loopback interfaces. [VIP-38731]

Routing Protocols

- When you are upgrading vEdge routers to Release 16.2.12, the BGP process (bgpd) might crash during the reboot process, when the router is shutting down. [VIP-29523]
- You two IPv6 interfaces on a vEdge router are active at the same time, basic packet forwarding (such as ping) might fail. Only one interface works at a time, and the router switches back and- orth between the two interfaces. [VIP-37810]
- When you configure VPN-specific OMP route advertisement parameters to two VPNs on a vEdge router, they might not be applied properly in the VPNs. [VIP-37860]
- In the BGP feature template, the BGP neighbor route policy variable name is displayed as the default name (bgp_neighbor_policer_out_pol_name) rather than the name you enter. However, the name you enter does show up when you are attaching the template to the device. [VIP-37988]

Security

- After you upgrade from Release 17.1.0 to Release 17.2.0, the vBond orchestrator might lose its certificate. As a workaround, re-install the certificate. [VIP-34926]
- When you specify a DNS destination for IPsec on a tunnel in VPN 0, the Forwarding Table Management process (ftmd), the OMP process (ompd), or the IKE procee (iked) might crash. [VIP-38888]

SNMP

- When traffic exceeds 85% of the bandwidth configured on a transport interface, SNMP traps might not get triggered. [VIP-33435]
- When you poll the VIPTELA-OPER-VPN MIB, interface descriptions are limited to 32 characters. [VIP-35787]

System

- vBond orchestrators might report a large number of control-connection-auth-fail events. [VIP-22976]
- In an overlay network with three vSmart controllers, if a controller group list configured on a 100 vEdge router contains two vSmart controllers, the maximum number of controllers that the router can connect to is set to two, and the maximum number of OMP sessions on the router is set to two, 50 routers connect to each of two vSmart controllers. If you bring these two controllers down, all 100 connections then move to the third vSmart controller. However, if you then bring up one of the other vSmart controllers, 50 connections move to that controller, but the third controller might still have 100 connections. [VIP-27955]
- The vManage server might not process events received from vEdge routers. [VIP-28673]
- When a certificate for controllers is about to expire, no syslog message is generated. [VIP-28960]
- When NAT is configured between in a service-side VPN, a ping operation between a vEdge router in that service VPN and another vEdge router reachable through the transport network might be successful even though it should be blocked because of the NAT. [VIP-31078]
- On vEdge routers, when you issue an **nping** command for IPv6, the command might fail, and a core file might be created on the router. From vManage NMS, you issue this command from the Monitor ► Network ► Troubleshooting ► Ping pane. From the CLI, you use the **tools nping** command, specifying **options "--ipv6"** . [VIP-31924]
- The vdebug log file might contain no entries. [VIP-33662]
- A vSmart controller might crash and create the core file /rootfs.rw/var/crash/core.vtracker.vSmart, indicating an issue with the vtracker process, which pings the vBond orchestrator every second. [VIP-33719]
- The TCP optimization process might consume a large amount of CPU even though TCP optimization is not configured. [VIP-36675]
- On vManage NMS, you cannot create AAA user groups that contain a greater-than sign (>) in their names. [VIP-37069]
- Log file messages might now include the correct date in the timestamp. [VIP-37086]

- The **show omp tlocs advertised** command might show that the **default** TLOC color is being advertised even when this color has not been assigned to any vEdge interface. [VIP-37090]
- When you change the negotiated interface speed on a vEdge router, the buffer allocation also changes. [VIP-37238]

vEdge Hardware

- On a vEdge 100m router, after you execute the **request software reset** command, the router might reboot continuously. [VIP-24149]
- A vEdge 2000 router physical interface might drop packets larger than 1480 bytes that are sent on loopback interfaces. [VIP-27216]
- On a vEdge 100b, when you change the IP address on an interface, that IP address might not be detached from the interface. [VIP-35047]
- In a vEdge 5000 router, if you remove and replace an SFP without powering off the router, the router is unable to detect the new SFP module details. For example, the **show hardware inventory** command will not list the SFP module. However, the ports on the SFP still connect and work as expected. [VIP-37562]
- A vEdge 5000 router might not be able to start because of issues with its internal verification hardware. [VIP-38219]

vManage NMS

- If you try to configure a vEdge router using vManage configuration templates, you might see errors related to lock-denied problems. As a workaround, reboot the router. [VIP-23826]
- When the majority of vManage cluster members are down, you can make changes to the device configuration templates on one of the cluster members that is up, and you can then push these changes when the cluster members come back up. This might lead to a situation in which the configuration templates on the vManage NMSs in the cluster are out of sync. [VIP-26016]
- The vManage server might not process events received from vEdge routers. [VIP-28312]
- When you use the vManage NMS and the CLI **show system status** command, the reboot reason is incorrect; it is shown as unknown. Looking in the /var/log/tmplog/vdebug logs shows that the system reboot happened because of a user-initiated upgrade to Release 17.1.3. [VIP-31222]
- In the vManage AAA feature template, you might not be able to enter the RADIUS secret key even though you can enter that same key in the CLI. [VIP-31856]
- When you push a policy that contains an error to the vSmart controller, the error message might not correctly indicated the cause of the error. [VIP-32253]
- You might not be able to push configuration templates to vEdge routers. [VIP-34886]
- When you change the names of the route policies in a localized policy, the modified policy might not work as expected. [VIP-35026]
- After a vManage NMS silently reboots, it might be out of sync with the vManage cluster. [VIP-35891]
- When a vBond orchestrator is unreachable or has wrong credentials configured, pushing a vEdge list to it fails with the message “File /home/ *user* /vedge_serial_numbers must be in home directory”, which does not provide any useful information to the user to understand what is wrong. [VIP-36285]
- The default VPN 512 management feature template is named "Transport VPN", which is confusing because VPN 0 is the transport VPN. [VIP-36771]
- If NMS services are down on one of the servers in a vManage cluster, you might not be able to perform an CLI operations from the vManage NMS. [VIP-37672]
- In the vManage policy builder, you can configure a site list name that is longer that is allowed on the vSmart controller. When you attempt to activate the policy, an error occurs on the vSmart controller, [VIP-37859]
- The vManage interface feature configuration templates do not have drop-downs for selecting interface speed and duplex settings. [VIP-37973]

- After a CSR request is sent to Symantec but before the certificate has been approved, the vManage request to retrieve the certificate might die, and so the vManage NMS might not be able to retrieve the certificate even after it has been approved. [VIP-38092]
- In a vManage cluster with two servers, if both servers go down, you might need to manually restart the vManage services to return the vManage servers to an operational state. To do this, issue the **request nms configuration-db restart** command from the vManage server. One way to determine whether you need to restart the services is to check the /var/log/nms/debug.log file on the vManage server for a message indicating that neo4j needs to be restarted. [VIP-38228]
- If you reboot one of vManage servers in a cluster while the vManage NMS is downloading a software image to a vEdge router, the cluster might report server errors and might stop operating properly. [VIP-38556]
- In Forwarding Class/QoS in the Localized Policy wizard, if you create a class map, assign a queue to that class map, successfully add the queue, and then delete the class from the class map list, the Forwarding Class column might be empty instead of displaying the class name. [VIP-38690]
- When a localized policy that includes a policer is attached to a vEdge router and is active on that device, you might not be able to edit the policer in the vManage policy wizard. [VIP-39294]

Fixed Issues

Issues Fixed in Release 18.2.0

The following issues have been fixed in Viptela Software Release 18.2.0. The number following each issue is the bug number in the Viptela bug-tracking database.

CloudExpress Service

- The CloudExpress vQoE score history value might differ from the score shown for the corresponding application. [VIP-34346: This issue has been resolved.]

Forwarding

- The output of the traceroute command on a vEdge router might be incorrect. [VIP-23072: This issue has been resolved.]
- When the output of the **show ipsec outbound-connections** command shows that tunnel MTU is 1441 bytes, a router fragments packets with the size (iplen) of 1438 bytes, but 1437-byte are not fragmented. There seems to be a 4-byte gap between tunnel MTU and the size at which the router actually starts fragmenting a packet. Also the TCP MSS seems to be 40 bytes smaller than expected for IPv4 packets and 60 bytes smaller for IPv6. [VIP-33527: This issue has been resolved.]
- If the vEdge routers in your overlay network are running Release 17.2, you cannot add routers to the network that are running Release 15.4. [VIP-35084: This issue has been resolved.]

Interfaces

- Traffic flow on IPsec tunnels might be interrupted when you configure only tunnel interface parameters, such as MTU and dead-peer detection. [VIP-31426: This issue has been resolved.]

Policy

- After you change a policy on the vSmart controller, the OMP process (ompd) process might fail and the vSmart controller might crash. [VIP-34098: This issue has been resolved.]

Routing Protocols

- When OMP redistributes BGP routes, it might not include in the origin metric. [VIP-36580: This issue has been resolved.]

Security

- If an IPv6 address for the IPsec tunnel source interface, the IPsec tunnel does not come up. [VIP-29912: This issue has been resolved.]
- The vEdge 100m and vEdge Cloud routers use an outdated and known vulnerable version of the OpenSSL library. [This issue has been resolved.]

System

- When the configuration process (confd) on a vEdge router crashes, the router might not reboot as expected. Instead, it remains at the Linux Bash shell. [VIP-28441: This issue has been resolved.]
- Pushing a device configuration template to a vEdge router might fail because of a bridge configuration validation failure. This issue occurs when a bridge with VLAN and interfaces is already configured on the router and the template being pushed modifies these parameters. As a workaround, copy the template, delete the entire bridge configuration, and push the template to the router. Then add the original bridge configuration to the template, and push that template to the router. [VIP-33204: This issue has been resolved.]
- When you copy the configuration database from the primary vManage NMS to bring up a secondary vManage NMS, the certificates for vEdge Cloud routers are not included, and the control plane and data plane for these routers do not come up. [VIP-34085: This issue has been resolved.]
- After you upgrade the vManage NMS to Release 17.2.2.1, you might not be able to log into the NMS. The error message displayed is "Server is initializing, please wait". [VIP-34697: This issue has been resolved.]
- The vManage NMS might not be able to retrieve records from the configuration database. When this occurs, the vManage NMS displays exception errors. [VIP-35702: This issue has been resolved.]
- In a vManage cluster, when you try to display the Maintenance ► Software Upgrade ► vEdge screen, the screen might not display, and the vManage-Server.Log shows an exception error. [VIP-35926: This issue has been resolved.]
- A standalone vManage NMS deployed on ESXi might become inaccessible because the server_config.json file gets corrupted. [VIP-36282: This issue has been resolved.]
- In a vManage cluster running Release 17.2.3, one of the vManage servers might not be able to connect to the configuration database. As a workaround, issue the **request nms all restart** command on the vManage server to restart all NMS services. [VIP-36805: This issue has been resolved.]

vEdge Hardware

- On a vEdge router WAN interface, the forwarding process (fp) might crash when the router is checking implicit access lists (ACLs). [VIP-37919: This issue has been resolved.]

vManage NMS

- A vManage NMS might not be able to synchronize its configuration with a vSmart controller. [VIP-26270: This issue has been resolved.]
- You might not be able to push a configuration template to a vEdge router. [VIP-32277: This issue has been resolved.]
- A vManage multitenant dashboard might show inconsistent information about vEdge routers. [VIP-33402: This issue has been resolved.]
- The vManage configuration database might not be able to process records. [VIP-34251: This issue has been resolved.]
- When you upload the list of vEdge routers to the vManage NMS, an improper file might be uploaded. [VIP-34465: This issue has been resolved.]
- In a vManage cluster, the vManage server might run slowly, and the vmanage-server.log file might contain "Reached maximum number of concurrent connections" exception messages. [VIP-34594: This issue has been resolved.]
- The vManage latency and jitter graphs might not match the reported values. [VIP-36729: This issue has been resolved.]
- The vManage device database might list a vBond orchestrator with the vEdge routers. [VIP-36876: This issue has been resolved.]
- In the vManage SNMP feature configuration template, when you try to add trap types to a trap group, the ADD button might not work. [VIP-37376: This issue has been resolved.]

- If you try to push a Service VPN configuration template, the operation might fail with the error "Failed to create input variables". [VIP-37705: This issue has been resolved.]

YANG Files for Netconf and Enterprise MIB Files

Netconf uses YANG files to install, manipulate, and delete device configurations, and Viptela supports a number of enterprise MIBs. Both are provided in a single tar file. Click the filename below to download the file.

- **YANG and Enterprise MIB files for Release 18.2.0**

Using the Product Documentation

The Viptela product documentation is organized into seven modules:

Module	Description
Getting Started	Release notes for Viptela software releases, information on bringing up the Viptela overlay network for the first time, quick starts for vEdge routers, software download and installation, and an overview of the Viptela solution.
vEdge Routers	How to install, maintain, and troubleshoot vEdge routers and their components. Provides hardware server recommendations for the controller devices—vManage NMS, vSmart controller, and vBond orchestrator servers.
Software Features	Overview and configuration information for software features, organized by software release.
vManage How-Tos	Short step-by-step articles on how to configure, monitor, maintain, and troubleshoot Viptela devices using the vManage NMS.
Command Reference	Reference pages for CLI commands used to configure, monitor, and manage the Viptela devices. Includes reference pages for Viptela software REST API, a programmatic interface for controlling, configuring, and monitoring the Viptela devices in an overlay network.
vManage Help	Help pages for the vManage screens. These pages are also accessible from the vManage GUI.

Tips

- To create a PDF of an article or a guide, click the PDF icon located at the top of the left navigation bar.
- To find information related to an article, see the Additional Information section at the end of each article.
- To help us improve the documentation, click the Feedback button located in the upper right corner of each article page and submit your comments.

Using the Search Engine

- To search for information in the documentation, use the TechLibrary Search box located at the top of each page.
- On the Help results page, you can narrow down your search by selecting the appropriate documentation module at the top of the page. If, for example, you are searching for power supply information for your vEdge router model, select the Hardware module and then select your vEdge router model.
- When a search returns multiple entries with the same title, check the URL to select the article for your hardware platform or software release.

- When the search string is a phrase, the search engine prioritizes the individual words in a phrase before returning results for the entire phrase. For example, the search phrase *full-cone NAT* places links to "NAT" at the top of the search results. If such a search request does not return relevant results, enclose the entire search string in quotation marks (here, for example, *"full-cone NAT"*).

Issues

- The maximum PDF page limit is 50 pages.
- It is recommended that you use the Chrome browser when reading the production documentation. Some of the page elements, such as the PDF icon, might not display properly in Safari.
- The screenshots for the vManage NMS screens that are included in the vManage help files and other documentation articles might not match the vManage NMS software screens. We apologize for the inconvenience.

Requesting Technical Support

To request technical support, send email to support@viptela.com .

To provide documentation feedback or comments, send email to docs@viptela.com .

Open Source Documentation

The following links provide documentation details about open source software included in Viptela software:

- **MIPS platforms**
- **vContainer platform**
- **vManage NMS**
- **x86 platforms**

Revision History

Revision 1—Release 18.2.0, June 18, 2018
Revision 2—Update, February 17, 2019