



Cisco SD-WAN (Viptela) Release Notes for Release 18.1



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: www.cisco.com/go/trademarks. 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)

Release Notes for Release 18.1

These release notes accompany Viptela Software Release 18.1, for Release 18.1.1. The Viptela software runs on all Viptela devices, including vSmart controllers, vEdge routers, vBond orchestrators, and vManage NMSS. Release 18.1.1 is available for limited use only.

Viptela Software Release 18.1

March 30, 2018

Revision 1

Product Features

Below are the main product features in Viptela Software Release 18.1:

- **Bootloader** —On all MIPS-based vEdge routers, the bootloader (u-boot) security has been enhanced.
- **Cisco ISR 4331 router** —The Viptela software runs on the Cisco ISR 4331 router.
- **HTTPS service on vEdge router tunnel interfaces** —By default, HTTPS service is allowed on vEdge router tunnel interfaces. See [allow-service](#) and *Software Caveats, below*.
- **IPv6 enhancements** —vEdge routers support IPv6 Router Advertisement (RA) and Router Solicitation (RS) messages, and IPv6 stateless autoconfiguration (SLAAC). Using RA messages, DHCPv6 learns the default route. RA messages also allow the router to advertise DNS information to IPv6 hosts. RA and RS messages and SLAAC allow zero-touch provisioning (ZTP) over IPv6.
- **Root access** —On vBond orchestrators, vEdge routers, and vSmart controllers, root access has been disabled.

Command Changes

New and Modified Configuration Commands

Command	Hierarchy	New	Modified	Comments
allow-service	vpn 0 tunnel interface		X	Allow HTTPS for vEdge routers.

New and Modified Operational Commands

None

REST API Changes

- Under Configuration - Device Template, the `template/device/config/validate` call has been renamed to `template/device/config/verify`.

Upgrade to Release 18.1

For details on upgrading the Viptela software, see [Software Installation and Upgrade](#) .

If your vManage NMS is running as a cluster, please contact Customer Support for assistance when upgrading to Release 18.1.0 or later.

To upgrade to Release 18.1:

1. In vManage NMS, select the Maintenance ► Software Upgrade screen.

2. Upgrade the controller devices to Release 18.1 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.

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 18.1, you can never downgrade it to Release 17.2 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, 17.2 and 18.1 are examples of major releases. Releases 17.2.0 and 18.1.0 denote the initial releases, and Releases 17.2.7 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 18.1:

- 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 18.1. 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 18.1, 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 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.

Installation

- One of the steps in [installing signed certificates on vEdge Cloud routers](#) is to generate a bootstrap configuration file. On a vManage NMS running Release 18.1.1 or later, if you generate the bootstrap configuration file for a vEdge Cloud router that is running software earlier than Release 18.1.1, the generated configuration will fail on that router. This is because in Release 18.1.1, a new default configuration, [allow-service https](#), has been added for vEdge tunnel interfaces. Earlier software releases do not support the HTTPS service on vEdge router tunnel interfaces. As a workaround, edit the generated bootstrap configuration file to remove the HTTPS configuration before you attach the configuration to the router.

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.
- Traffic flow on IPsec tunnels might be interrupted when you configure only tunnel interface parameters, such as MTU and dead-peer detection. [VIP-31426]
- 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.
- DHCPv6 returns only an IPv6 address. No default information is accepted. IPv6 router solicitation and router advertisement messages are not processed.

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.

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

- When a task stops and a vEdge router reboots, the router might no longer reboot. This situation occurs after the router reboots three times within 20 minutes, five times within 60 minutes, or seven times within the last 24 hours. During this time, the control plane on the router remains up, so traffic continues to be sent to the node. To override this behavior, recover the router via the console port.
- 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.

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 18.1. The number following each issue is the bug number in the Viptela bug-tracking database.

AAA

- The Viptela software does not send a TACACS vendor-specific "service argument" field. [VIP-25629]

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]
- You cannot configure profile 16 in the [interface cellular0 profile](#) command.

CloudExpress Service

- The CloudExpress vQoE score history value might differ from the score shown for the corresponding application. [VIP-34346]

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]
- The **traceroute** command might not work if you specify an IPv6 address for the host. [VIP-30833]
- 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]

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 configure a weight on a TLOC that is also being used as a split tunnel, the weight is not used for weighted ECMP across the NATs. [VIP-27534]
- 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 **policy cloud-qos** on a vEdge Cloud router, a TLOC from the remote site might go down and then come back up when multiple traffic flows are present on the TLOC. [VIP-32369]
- When you configure inbound and outbound port mirroring on the same interface, traffic might be mirrored only in one direction. [VIP-33247]
- If you enable TCP optimization on a vEdge 1000 router, the router might drop ARP responses. [VIP-33507]
- When multiple NAT interfaces are present in VPN 0, port forwarding might not work. [VIP-34086]
- 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]
- The TCP optimization process might consume a large amount of CPU even though TCP optimization is not configured. [VIP-36675]
- 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]

Interfaces

- When a vEdge VRRP primary 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 primary again becomes a backup, other devices continue to point to the MAC address for the backup router, and traffic is discarded until ARP cache on the other devices expires and is updated with the correct MAC address of primary vEdge, a process that typically takes a few minutes. [VIP-33722]

Policy

- QoS shaping rates might be inaccurate for rates less than 2 Mbps. [VIP-3860]

- A centralized policy that is pushed from the vSmart controller to the vEdge routers might not be applied on the routers. If this occurs, modify the policy and push it again. [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]
- The vSmart controller might not push a policy to the vEdge routers. [VIP-33016]
- When you issue the **request admin-tech** command, the Forwarding Policy Manager process (fpm) might crash. [VIP-34031]
- After you change a policy on the vSmart controller, the OMP process (ompd) process might fail and the vSmart controller might crash. [VIP-34098]
- When the vSmart controller pushes a policy to a vEdge router and the push fails, no alarm or trap records the failure. [VIP-34131]

Routing Protocols

- When the OSPF external distance is set to 254, an IP prefix learned first from OMP and then from OSPF as an type E2 route, the route might be redistributed into OMP. [VIP-20542]
- 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]
- On a vEdge 1000 router, the OSPF process (ospfd) might fail and cause the router to crash. [VIP-30239]
- When you use the iPerf speed tool at 200 Mbps on a vEdge router, the control plane and OSPF neighbors might go down. [VIP-36152]
- The output of the **show bgp summary** and **show bgp neighbors** commands might be incorrect. [VIP-36806]

Security

- When you configure IPsec parameters for data plane security or during an IPsec rekeying operation, you might see a spike in CPU usage on the vEdge router, especially a hardware router. [VIP-31635]

SNMP

- When traffic exceeds 85% of the bandwidth configured on a transport interface, SNMP traps might not get triggered. [VIP-33435]
- The snmpwalk operation might not return SNMP data for the interface ifname. [VIP-35873]

System

- vBond orchestrators might report a large number of control-connection-auth-fail events. [VIP-22976]
- 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]
- When a vEdge router is unable to reach one of the controllers in a controller, it might not try to reach other controllers in the same group. [VIP-31881]

- 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]
- A vEdge router might choose to establish its control connection to the vManage NMS using an interface on which a tunnel interface is not configured even though an interface with a tunnel interface is operational. [VIP-32011]
- 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]
- When the vManage NMS experiences a kernel panic and reboots, the `/var/crash/crash.dump` file might be deleted. [VIP-34248]
- You cannot disable ICMP redirect messages. [VIP-36594]

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 vEdge100m router, the output of the **show interface** command might show the same interface in two different VPNs. [VIP-29069]

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]
- If you use the CLI to modify the organization name, this change might not be reflected on the vManage screens. [VIP-24343]
- 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]
- A vManage NMS might not be able to synchronize its configuration with a vSmart controller. [VIP-26270]
- 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 indicate the cause of the error. [VIP-32253]
- You might not be able to push a configuration template to a vEdge router. [VIP-32277]
- When you are using a vManage cluster, pushing policies to vSmart controllers might time out. [VIP-32630]
- Pushing a configuration template to a vEdge router might time out if the configuration has only one interface and that interface is configured as a last-resort interface. [VIP-33157]
- In a vManage cluster, if you reboot one vManage server from another vManage server (from the Maintenance ► Reboot Devices screen), the vManage configuration database might become out of sync with the actual device configurations. It is recommended that you not reboot a vManage server in this way. [VIP-33625]
- 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]

- After a vManage NMS silently reboots, it might be out of sync with the vManage cluster. [VIP-35891]
- In Viptela Software Release 17.1.4, when you use OpenStack Heat to create a vManage NMS, the /dev/vdb disk is recognized and mounts. However, in Release 17.2.3, the disk volume might not be automatically recognized and mounted. [VIP-35907]
- 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]
- A standalone vManage NMS deployed on ESXi might become inaccessible because the server_config.json file gets corrupted. [VIP-36282]
- When a vBond orchestrator is unreachable or has wrong credentials configured, pushing a vEdge list to it fails with the message "File /home/najmadmin/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]
- When you upgrade the vManage server from Release 17.1.4 to Release 17.2, you might see certificate null pointer exceptions. [VIP-34901]
- The process of installing a new certificate on the vManage NMS might take a long time, eventually failing with the message "Failed to finish the task". However, the output of the **show control valid-vsmarts** command indicates that the certificate installation has succeeded. But because the vManage server is not aware that the task has completed, you are unable to attach configuration templates to the vManage server. [VIP-36579]
- In the vManage Configuration ► Policies ► Centralized Data Policies screen, a user who does not have policy write permission might see the copy, edit, and delete actions in the More Actions icon to the right of a policy listed in the policy table. [VIP-36770]
- The default VPN 512 management feature template is named "Transport VPN", which is confusing because VPN 0 is the transport VPN. [VIP-36771]
- 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]

Fixed Issues

Issues Fixed in Release 18.1.1

Configuration and Command-Line Interface

- When you push a large policy from the vManage NMS to a vSmart controller, it might take a long time for the policy to take effect. [VIP-22115: This issue has been resolved.]

Forwarding

- When a last-resort interface has been initiated and connections on that interface are being brought up, the value of the last-resort hold-down timer might be shown incorrectly in syslog files. [VIP-30423: This issue has been resolved.]

Interfaces

- On a vEdge router WLAN interface, when you configure the RADIUS source interface as loopback0, RADIUS requests might be sourced from random interfaces. [VIP-24240: This issue has been resolved.]

PPPoE

- When you are using PPPoE on a vEdge100m router, when you initially connect to the PPP WAN interface, the interface receives an IP address. But when you unplug the PPP interface and then plug it back in, we do not get an IP address. As a workaround, either reboot the DSL modem or reset the interface from the router's CLI. [VIP-23332: This issue has been resolved.]

Routing Protocols

- When you have configured a BGP peering session to restart after receiving a more than a set number of prefixes from its neighbor, the session might not restart when the number of prefixes is exceeded. [VIP-33780: 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.]
- After you upgrade to Release 17.2.3, the vBond orchestrator might take a long time to stabilize and to establish connections to all the vSmart controllers. [VIP-35514: This issue has been resolved.]

SNMP

- When a vEdge 100 reboots, it might start SNMP on the wrong port. [VIP-24700: This issue has been resolved.]

System

- The output of the traceroute command on a vEdge router might be incorrect. [VIP-23072: This issue has been resolved.]
- If you do not use ZTP and if the Organization Name is not set on the vManage NMS and vEdge routers, control connections between the two devices might come up. [VIP-24246: This issue has been resolved.]
- When you connect to the management interface of Viptela devices via SSH, you are placed into a limited shell. However, if you issue the **vshell** command, all operations are executed as the root user. [VIP-32713: This issue has been resolved.]
- On a vEdge 2000 router, BFD sessions may go down and then come back up every 10-60 minutes. As a workaround, disable cflowd and DPI. [VIP-33784: This issue has been resolved.]
- When you access the vManage server from the Mozilla Firefox browser, if you update the interface in area 0 in the OSPF feature template, you might not be able to save the template. As a workaround, use the Chrome browser. [VIP-35584: This issue has been resolved.]

vEdge Hardware

- When a vEdge 2000 router reboots, the reboot reason field might show only a value of 0. [VIP-23941: This issue has been resolved.]

vManage NMS

- In the vManage Dashboard Application-Aware Routing pane, the search engine might not work properly. [VIP-23186: This issue has been resolved.]
- When you try to apply a BGP template to a device, you might see the error "invalid value for: shutdown". [VIP-23258: This issue has been resolved.]
- When you attach a vEdge policy template that contains variables to a device template, during the CSV import action the policy variables might not be populated with the values from the CSV file. As a workaround, manually set the policy values and then import the CSV file. [VIP-23862: This issue has been resolved.]
- On vManage NMS, when you display interface queue statistics in real time, statistics for only one of the eight possible queues might be displayed. [VIP-23898: This issue has been resolved.]
- vManage charts might not properly format values between 0 and 1. [VIP-23910: This issue has been resolved.]
- You might not be able to edit the AAA feature configuration template. [VIP-23970: This issue has been resolved.]
- When an admin user edits an existing CLI template, its device type is sometimes Null, so the user is unable to select the device type. [VIP-24182: This issue has been resolved.]
- A vManage serve might continue to attempt to fetch certificates even though all certificates are installed. [VIP-27416: This issue has been resolved.]
- On vManage NMS, you might not be able to edit a primary configuration template. [VIP-28689: This issue has been resolved.]
- The /client/activity/summary REST call might time out. [VIP-28737: This issue has been resolved.]

- From a vManage server, you might not be able to SSH into a vEdge router that is in staging mode. [VIP-33119: This issue has been resolved.]
- In the vManage Monitor ► Network ► Real Time screen, the output of the Interface Queue Stats command might show information for queue 0 only, showing no information about queues 1 through 7. [VIP-33508: This issue has been resolved.]
- When you query deviceCategory=controllers from the vManage API, the following error might be returned: "%20 characters are spaces and need to be removed". [VIP-33758: This issue has been resolved.]

Issues Fixed in Release 18.1.0

Viptela Software Release 18.1.0 was not released.

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 18.1.1**

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 .

Revision History

Release 18.1.0 was not released.

Revision 1—Release 18.1.1, March 30, 2018