Release Notes for Release 16.2

These release notes accompany Viptela Software Release 16.2, for Releases 16.2.0 through 16.2.14. The Viptela software runs on all Viptela devices, including vSmart controllers, vEdge routers, vBond orchestrators, and vManage NMSs.

Viptela Software Release 16.2
December 22, 2017
Revision 17

Below are the main product features in Viptela Software Release 16.2. All features are introduced in Release 16.2.0 unless otherwise indicated.

• **AES-GCM-256 encryption algorithm for IPsec tunnels**—The encryption algorithm on IPsec tunnel connections is either AES-256-GCM or AES-256-CBC. For unicast traffic, if the remote side supports AES-256-GCM, that encryption algorithm is used. Otherwise, AES-256-CBC is used. For multicast traffic, the encryption algorithm is AES-256-CBC. You cannot modify the choice made by the software. See Configuring Security Parameters, show ipsec inbound-connections, show ipsec outbound-connections, and show security-info.

• **Cellular interface as circuit of last resort**—On vEdge routers with cellular modules, you can configure a tunnel interface to be a last-resort circuit. See Configuring Interfaces and last-resort-circuit.

• **Cellular interface visibility on vManage server**—Starting in Release 16.2.2, you can display information about cellular interfaces. From vManage Monitor ► Network ► Interface, click the cellular interface name from the interface table in the lower part of the right pane. See Network.

• **Control authentication for admin user using authentication order**—You can configure the order in which the Viptela software tries different authentication methods when verifying access to an "admin" user. See Configuring User Access and Authentication and admin-auth-order.

• **Circuit capacity planning**—You can monitor the bandwidth usage on a transport circuit, to determine how the bandwidth usage is trending. If the bandwidth usage starts approaching a maximum value, you can configure the software to send a notification. Notifications are sent as Netconf notifications, which are sent to the vManage NMS, SNMP traps, and syslog messages. See Configuring Interfaces, bandwidth-downstream, and bandwidth-upstream.

• **Enhancements to minimize traffic usage on tunnel interfaces and BFD sessions**—To minimize traffic sent on tunnel interfaces, the maximum values for keepalive timers have been increased. For DTLS and TLS control connections, the maximum hello timer interval has been increased from 1 minute to 10 minutes, and the maximum hello tolerance has been increased from 1 minute to 10 minutes. For BFD connections in the data plane, the maximum hello timer interval has been increased from 1 minute to 5 minutes. In addition, OMP control traffic is not sent or received over cellular interfaces when other interfaces are available. See Configuring Network Interfaces, Configuring Control Plane and Data Plane High Availability Parameters, bfd color, hello-interval, and hello-tolerance.
• Filter and block SNMP based on value of OID—When configuring the OIDs to include or exclude in an SNMP view, you can include a asterisk (*) wildcard to allow any value in that position. See Configuring SNMP and view.

• Jitter in SLA definition—When defining the SLA for an application-aware routing policy, you can specify the maximum packet jitter in addition to the maximum packet latency and loss. See Configuring Application-Aware Routing and sla-class.

• OMP end-of-RIB timer—You can configure the OMP end-of-RIB (EOR) time so that after an OMP session goes down and then comes back up, an end-of-RIB (EOR) marker is sent. See Configuring OMP and timers.

• RESTful bulk APIs—You can issue a single RESTful API command to collect information for multiple vEdge routers in the overlay network. See vManage REST APIs.

• SCSI disk driver support—You can choose SCSI or Virtio SCSI as the disk driver type when you create virtual machine (VM) instances for vManage NMS, vBond orchestrators, vSmart controllers, and vEdge Cloud routers. See Create vManage VM Instance on KVM, Create vBond VM Instance on KVM, Create vSmart VM Instance on KVM, and Create vEdge Cloud VM Instance on KVM.

• SNMPv3—Viptela devices support SNMPv3 in addition to SNMPv1 and SNMPv2. SNMPv3 adds cryptographic security by authenticating and encrypting data packets send on the overlay network. See System and SNMP Overview, Configuring SNMP, group, and user.

• Source SNMP traps from specific interfaces—You can configure the interface to use to send traps to the SNMP server that is receiving the trap information. See Configuring SNMP and trap target.

• Symmetric NAT—vEdge routers can operate behind NAT devices running symmetric NAT. For a WAN tunnel, only one of the NAT devices at either end of the tunnel can use symmetric NAT. The vEdge router that is behind a symmetric NAT cannot establish a BFD tunnel with a remote vEdge router that is behind a symmetric NAT, an address-restricted NAT, or a port-restricted NAT. To allow a vEdge router to function behind a symmetric NAT, you must configure the vManage NMS and vSmart controller control connections to use TLS, because DTLS control connections do not work through a symmetric NAT. See Security Overview and Software Caveats.

• Tunnels used for application-aware routing flows—For DPI applications in application-aware routing, you can determine which tunnels flows were received and transmitted on. See show app dpi flows.

• Variables in data policies for vEdge routers—In vManage NMS, when you are configuring policy templates for vEdge routers, you can include variables in the templates. See Configure Policies.

• vContainer virtual machines for vSmart Controllers—You can deploy several vSmart controller instances as individual vContainer virtual machines. Containers allow you to launch the vSmart controllers at the same time. See Deploy the vContainer Host.

All command changes are introduced in Release 16.2.0 unless otherwise indicated.
# New and Modified Configuration Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Hierarchy</th>
<th>New</th>
<th>Modified</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin-auth-order</td>
<td>system aaa</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>bandwidth-downstream</td>
<td>vpn interface</td>
<td></td>
<td>X</td>
<td>On vEdge routers and vManage NMSs.</td>
</tr>
<tr>
<td>bandwidth-upstream</td>
<td>vpn interface</td>
<td></td>
<td>X</td>
<td>On vEdge routers and vManage NMSs.</td>
</tr>
<tr>
<td>container</td>
<td>Top level</td>
<td></td>
<td>X</td>
<td>On vSmart controller containers only.</td>
</tr>
<tr>
<td>eor-timer</td>
<td>omp timers</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>hello-interval</td>
<td>bfd color</td>
<td></td>
<td>X</td>
<td>On vEdge routers. Maximum increased to 5 minutes.</td>
</tr>
<tr>
<td>hello-interval</td>
<td>vpn 0 interface tunnel-interface</td>
<td></td>
<td>X</td>
<td>Maximum interval increased to 10 minutes. In Releases 16.2.1 and later, hello tolerance must be at least 2 times the hello interval.</td>
</tr>
<tr>
<td>hello-tolerance</td>
<td>vpn 0 interface tunnel-interface</td>
<td></td>
<td>X</td>
<td>Maximum tolerance increased to 10 minutes.</td>
</tr>
<tr>
<td>ip address-list</td>
<td>vpn (0</td>
<td>512) interface eth</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>jitter</td>
<td>policy sla-class</td>
<td></td>
<td>X</td>
<td>On vSmart controllers.</td>
</tr>
<tr>
<td>last-resort-circuit</td>
<td>vpn 0 interface cellular0 tunnel-interface</td>
<td></td>
<td>X</td>
<td>On vEdge routers with cellular modules.</td>
</tr>
<tr>
<td>oid</td>
<td>snmp view</td>
<td></td>
<td>X</td>
<td>Add support for wildcards when configuring OID subtree.</td>
</tr>
<tr>
<td>port-hop</td>
<td>system</td>
<td></td>
<td>X</td>
<td>Disabled by default on vManage NMSs and vSmart controllers.</td>
</tr>
<tr>
<td>Command</td>
<td>Hierarchy</td>
<td>New</td>
<td>Modified</td>
<td>Comments</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------------</td>
<td>-----</td>
<td>----------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>radius</td>
<td>system</td>
<td></td>
<td>X</td>
<td>Add priority command.</td>
</tr>
<tr>
<td>source-interface</td>
<td>policy cflowd-template collector</td>
<td></td>
<td>X</td>
<td>On vSmart controllers, in Releases 16.2.2 and later.</td>
</tr>
<tr>
<td>source-interface</td>
<td>snmp trap target</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>tacacs</td>
<td>system</td>
<td></td>
<td>X</td>
<td>Add authentication and priority commands.</td>
</tr>
<tr>
<td>technology</td>
<td>vpn interface cellular</td>
<td></td>
<td>X</td>
<td>On vEdge routers. In Releases 16.2.10 and later.</td>
</tr>
<tr>
<td>user</td>
<td>snmp</td>
<td></td>
<td>X</td>
<td>For SNMPv3.</td>
</tr>
</tbody>
</table>

**New and Modified Operational Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>New</th>
<th>Modified</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear app dpi summary statistics</td>
<td></td>
<td>X</td>
<td>Command removed in Releases 16.2.11 and later.</td>
</tr>
<tr>
<td>request container image install</td>
<td></td>
<td>X</td>
<td>On vSmart controller containers only.</td>
</tr>
<tr>
<td>request container image remove</td>
<td></td>
<td>X</td>
<td>On vSmart controller containers only.</td>
</tr>
<tr>
<td>request nms all</td>
<td></td>
<td>X</td>
<td>Add diagnostics option, in Releases 16.2.3 and later.</td>
</tr>
<tr>
<td>request nms application-server</td>
<td></td>
<td>X</td>
<td>Add version option.</td>
</tr>
<tr>
<td>request nms configuration-db</td>
<td></td>
<td>X</td>
<td>Add diagnostics option, in Releases 16.2.3 and later.</td>
</tr>
<tr>
<td>request nms coordination-server</td>
<td></td>
<td>X</td>
<td>Add diagnostics option, in Releases 16.2.3 and later.</td>
</tr>
<tr>
<td>request nms load-balancer</td>
<td></td>
<td>X</td>
<td>Add diagnostics option, in Releases 16.2.3 and later.</td>
</tr>
<tr>
<td>request nms messaging-server</td>
<td></td>
<td>X</td>
<td>Add diagnostics option, in Releases 16.2.3 and later.</td>
</tr>
<tr>
<td>request nms statistics-db</td>
<td></td>
<td>X</td>
<td>Add diagnostics option, in Releases 16.2.3 and later.</td>
</tr>
<tr>
<td>show app dpi flows</td>
<td></td>
<td>X</td>
<td>On vEdge routers. Add detail option.</td>
</tr>
<tr>
<td>show bfd tloc-summary-list</td>
<td></td>
<td>X</td>
<td>In Releases 16.2.3 and later.</td>
</tr>
</tbody>
</table>

Created on: Sat, 01 Jun 2019 14:32:11 GMT
Generated by: Anonymous
<table>
<thead>
<tr>
<th>Command</th>
<th>New</th>
<th>Modified</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>show container images</td>
<td>X</td>
<td></td>
<td>On vSmart controller containers only.</td>
</tr>
<tr>
<td>show container instances</td>
<td>X</td>
<td></td>
<td>On vSmart controller containers only.</td>
</tr>
<tr>
<td>show ipsec inbound-connections</td>
<td></td>
<td>X</td>
<td>On vEdge routers.</td>
</tr>
<tr>
<td>show ipsec outbound-connections</td>
<td></td>
<td>X</td>
<td>On vEdge routers.</td>
</tr>
<tr>
<td>show nms-server running</td>
<td></td>
<td>X</td>
<td>On vManage NMSs.</td>
</tr>
<tr>
<td>show policy access-list-policers</td>
<td></td>
<td>X</td>
<td>Output modified, in Releases 16.2.5 and later.</td>
</tr>
<tr>
<td>show policy data-policy-filter</td>
<td></td>
<td>X</td>
<td>Output modified, in Releases 16.2.5 and later.</td>
</tr>
<tr>
<td>show security-info</td>
<td></td>
<td>X</td>
<td>On vEdge routers.</td>
</tr>
<tr>
<td>tools ss</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>tools stun-client</td>
<td></td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

For details on upgrading the Viptela software, see [Software Installation and Upgrade](https://sdwan-docs.cisco.com/Product_Documentation/Getting_Started/Release_Notes/07Release_Notes_for_Release_16.2).

Note: It is recommended that all Viptela devices run the same software version. If this is not possible, ensure that the vManage software version is not lower than that of the other controllers and is not lower than that of the vEdge routers. That is, the vManage server software must be at least the same as the highest software version running on the controllers and the routers; it can also be higher. Also ensure that the vBond and vSmart software version is not lower than that of the vEdge routers. That is, the vBond and vSmart software must be at least the same as the highest software version running on the routers, and it can also be higher.

Note that Release 16.2.1 includes no images for vContainer hosts.

Release 16.2.2.1 is a patch release that fixes vManage issues only.

Note: Do not use vManage templates to configure vBond orchestrators. Configure them only from the CLI. If you have an existing vManage template for vBond orchestrators, detach the template from all orchestrators before upgrading the vManage NMS to Release 16.2.

Note: Before you upgrade a vEdge router or vSmart controller to a Release 16.2 software image, for RADIUS and TACACS servers, make sure that you have configured the VPN and the source interface to reach the servers (with the `system radius server vpn` and `system radius server source-interface` commands for RADIUS, and the `system tacacs server vpn` and `system tacacs server source-interface` commands for TACACS).

To upgrade to Release 16.2:
Warning: If your vBond orchestrator is hosted on Amazon Web Services (AWS), do not upgrade it to Release 16.2. Contact Viptela Customer Support for more information.

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

2. Upgrade the controller devices to Release 16.2 in the following order:
   1. First, upgrade the vManage NMSs in the overlay network.
   2. Then, upgrade the vBond orchestrators.
   3. 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.

If you are upgrading a Viptela controller—vManage NMS, vSmart controller, or vBond orchestrator—to Release 16.2.9 or later, and if you are switching from the E1000 to the VMXNET3 network adapter, you must perform the upgrade and switch in the following order:

1. Upgrade the software image to the desired version.
2. Shut down the Viptela controller.
3. Remove the existing E1000 network adapters.
4. Add the new VMXNET3 adapters to the controller, as explained in the appropriate Create VM Instance on ESXi article.

Note: You cannot add a mix of E1000 and VMXNET3 network adapters to any Viptela controller.

---

Upgrade the vManage NMS from Release 16.2.2 to Release 16.2.3

When you upgrade the vManage NMS from Release 16.2.2 to Release 16.2.3, it is recommended that you follow this procedure:

1. In vManage NMS, select Maintenance ► Software Upgrade.
2. In the Software Upgrade tab, select vManage.
3. Click Upgrade to install the new software image on all vManage servers in the cluster.
4. On each vManage server, select Tools ► SSH Terminal. From the CLI, issue the following commands:
   ```
   vManage# request nms all stop
   vManage# request software activate software-image
   ```
5. When all the vManage servers are up, on each server, from the CLI, issue the following command:
   ```
   vManage# request nms all stop
   ```
6. On each vManage server, from the CLI, confirm that the upgrade to the new software image is successful:
   vManage# request software upgrade-confirm

7. On one vManage server, from the CLI, start the statistics database:
   vManage# request nms statistics-db start

8. Repeat Step 7 for the remaining vManage servers.

9. On one vManage server, from the CLI, start the configuration database:
   vManage# request nms configuration-db start

10. Check that the configuration database has started properly:
    vManage# tail /var/log/nms/vmanage-orientdb-database.log.0
    Ensure that this file contains the following log messages:
    received new status UUID.vmanagedb=ONLINE [OHazelcastPlugin]
    updated node status to 'ONLINE' [OHazelcastPlugin]

11. Repeat Steps 9 and 10 for the remaining vManage servers.

12. On each vManage server, from the CLI, start the coordination server:
    vManage# request nms coordination-server start

13. On each vManage server, verify that the coordination server is up:
    vManage# request coordination-server status

14. After all the coordination servers are up, for each vManage server, from the CLI, start the messaging server:
    vManage# request nms messaging-server start

15. On each vManage server, verify that the messaging server is up:
    vManage# request messaging-server status

16. After all the messaging servers are up, on one vManage server, from the CLI, start the application server:
    vManage# request nms application-server start

17. Check that the application server has started properly:
    vManage# tail /var/log/nms/vmanage-orientdb-database.log.0

18. Repeat Steps 16 and 17 for the remaining vManage servers.

---

**Downgrade from Release 16.3 to Release 16.2**

You cannot downgrade from Release 16.3 to any version of Release 16.2. If you do so, the vManage NMS reports a null pointer exception for statistics settings, and as a result, the vManage NMS collects no statistics from the vEdge routers in the network. If you need to downgrade to Release 16.2, contact Customer Support for assistance.
Upgrade from Release 16.2 and Earlier Software Releases to Releases 16.3 or Later

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 16.3 or 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. 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, ensure that the interface names in the router configurations are correct.

Hardware Caveats

The following are known behaviors of the Viptela hardware:

- In Releases 16.2.2 and 16.2.3, you cannot insert a Finisar FTLF8519P3BNL transceiver into a vEdge 1000 or vEdge 2000 router. If you already have this transceiver in your router and you remove it, when you reinsert it, the software will mark is as being unsupported, and it will not function. This issue, which is being tracked by VIP-15507, was fixed in Release 16.2.4.

- On a vEdge 1000 router, 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](https://sdwan-docs.cisco.com/Product_Documentation/Getting_Started/Release_Notes/07Release_Notes_for_Release_16.2).

- By default, support for USB controllers is disabled on vEdge 1000 routers. 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.

- 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.
Software Caveats

The following are known behaviors of the Viptela software:

**Cellular Interfaces**

- 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 has been 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.

- Release 16.2.10 does not support the default cellular template. To configure cellular interfaces using vManage templates, you must configure the cellular features when you are creating a device template for a vEdge 100m router. To push any features other than the default configuration, place the cellular interface in shutdown state, push the VPN-Interface-Cellular template to the router, and then place the interface in no shutdown state and push the template to the router a second time.

**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](https://sdwan-docs.cisco.com/Product_Documentation/Getting_Started/Release_Notes/07Release_Notes_for_Release_16.2) 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 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. These routers cannot establish BFD sessions with a remote vEdge router that is running a software release earlier than Release 16.2.0.

**Policy**

- If you have configured a `preferred-color` or `backup-sla-preferred-color` action in application-aware routing policy but have not configure the associated `sla-class`, you might not be able to upgrade to Release 16.2.11. Before you upgrade to one of these software releases, add the appropriate `policy sla-class` configuration.

**Security**

- In Releases 17.1 and earlier, you cannot disable the SSH HMAC-MD5 algorithm and other weaker algorithms.

**SNMP**
• 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.

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, you cannot 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.

The following are outstanding issues in Viptela Software Release 16.2. 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 Interface
• You might not be able to configure vEdge 100m routers using vManage templates, because switching cellular profiles requires that you first shut down the cellular interface. [VIP-24095]

• In Release 16.2.7, you cannot configure profile 16 in the interface cellular0 profile command.

Configuration and Command-Line Interface

• The show interface detail | include string command attempts to paginate the output, displaying the More prompt, even when there is nothing to paginate. [VIP-2057]

• The ping command might not work if you specify an IRB source interface as it appears in the interface table, for example irb2. The ping command works if you specify the interface name with a dot, for example, irb.2. [VIP-17075]

• An IRB interface might remain up even if all interfaces in that bridge are in the link-down state. [VIP-23307]

• 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]

• On cellular interfaces, you might not be able to modify the maximum segment size (MSS) of TCP SYN packets. [VIP-28033]

Forwarding

• The flow collector on a vEdge router might fail to collect cflowd packet statistics. [VIP-11088]

• The frequency for BFD-based PMTU discovery can use more than half of the bandwidth on low-speed links. [VIP-19887]

• On a vEdge router running Release 16.2.2, if you disable PMTU discovery, the show system statistics command output might show a large number of errors. [VIP-22145]

• For certain packet sizes, the vEdge router might send packets with incorrect ICMP checksums in ping requests. For example, packet sizes of 170 and 1300 bytes work fine, but packets of 171 and 1301 bytes end up with incorrect checksums in the response. [VIP-22174]

• After an interface goes down and then comes back up, dynamic ARP might not restart. [VIP-26215]
• A centralized policy that is pushed from the vSmart controller to the vEdge routers might not be applied on the routers. [VIP-27046]

• A forwarding management process (ftmd) segmentation fault might occur in in ftm_dpi_flow_timer_expiry_cb. [VIP-27291]

• 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]

**Kernel**

• When you upgrade a vEdge router from Release 15.4.6 to Release 16.2.5, the upgrade might fail because a previous upgrade process on the vEdge router might not have terminated properly. [VIP-20748]

• When a vEdge router reboots and the control down flag is set, the vdaemon process might an Up event indicating that a configuration commit operation has occurred even though there was no configuration change. As a result, the vManage NMS pushes a device configuration to the vEdge router. [VIP-22395]

**OMP**

• 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]

• A vEdge router might continue to attempt to establish an OMP peering session with a vSmart controller that has been invalidated. [VIP-22385]

**OMP**

• When you add an Internet transport tunnel to a vEdge router that previous had only an MPLS transport tunnel and push the modified template, OMP might crash and cause the router to reboot. [VIP-27354]

• A vEdge router might try connect to a vSmart controller that has been invalidated and deleted from the vManage NMS. [VIP-30002]

**Policy**

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

• If you have configured a policer for the LLQ, the output of the `show interface queue` command shows all queue statistics except those for the LLQ. As a workaround, use the `show policer` command to display the LLQ statistics. [VIP-4529]

• You cannot choose which TLOC is used to build the single connection to the vManage NMS. [VIP-8424]

**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]

**Policy**

- On vEdge routers, the `show policy access-list-counters` command might not display any values in the Bytes column. [VIP-28890]

**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) 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]

**Security**

- The `show tunnel statistics ipsec` command displays no information about the count of inbound decrypted packets. [VIP-20637]

- If a vSmart controller becomes unreachable, the vEdge router might still show that controller as being reachable. [VIP-22262]

**SNMP**

- When you configure loopback interfaces on a vSmart controller or a vManage NMS, performing an snmpwalk operation over VIPTELA-OPER-VPN.mib might fail. [VIP-16980]

- In a vManage SNMP feature template, if you create a Trap Group but do not specify the list of modules, no error message is displayed but the deployment of the template fails. [VIP-20404]

**System**

- Moving a device from staging to valid might reset the control connections. [VIP-15009]

- A kernel panic might cause a vEdge router to silently reboot. [VIP-16233]

- The Gigabit Ethernet and 10-Gigabit Ethernet interfaces on a vEdge router might place the following message in the `/var/log/vdebug` file: "Failed to set new phy settings (errno:122)". [VIP-19357]
• On a vEdge 100b router, upgrading from Release 15.4.1 to Release 16.2.2 might fail silently, because the uboot file is incorrect. As a workaround, copy the correct uboot file to the router before performing the upgrade. [VIP-23083]

• When a task stops and a vEdge router reboots, the router might no longer reboot. This problem occurs after the router reboots three times within 20 minutes, five times within 60 minutes, or seven times within the last 24 hours. However, the control plane on the router remains up, so traffic continues to be sent to the node. [VIP-23106]

• A vEdge 100m router might reboot continuously after you execute the request software reset command. [VIP-24149]

• 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]

• If you use the loopback interface as the source interface for a cflowd collector, the Connection State on a vEdge router running Release 16.2.9 might show as "false, while it shows true on a router running Release 16.2.10. [VIP-24770]

vBond Orchestrator

• vBond orchestrators might report a large number of control-connection-auth-fail events. [VIP-22976]

vEdge Hardware

• On a vEdge 2000 router, when you remove an SFP, trace messages might be displayed. These messages do not affect the router, and you can ignore them. [VIP-3585]

• On a vEdge 1000 router, when you issue the show ip route ospf command, it might take more than a minutes for the router to display the results. [VIP-23696]

• When a vEdge 2000 router reboots, the reboot reason field might show only a value of 0. [VIP-23941]

• After you activate Release 16.2.10 on a vEdge router, the configuration database might become corrupted, and the router might continuously reboot. [VIP-25731]

• The output of the show interface sfp detail command might show that the copper minimum length, instead of the maximum length, is 100m. [VIP-28673]

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

vManage NMS

• In vManage ► Monitor ► Network ► Overview ► Environment, the Y axis on the CPU utilization graph shows the load average instead of the CPU utilization. [VIP-8114]
• Memory usage is shown as raw data, not in percentages. [VIP-8118]

• When you attach a template to the device, but the device rejects the template because of incorrect variable values and reverts to the previous configuration, the vManage NMS does not indicate the nature of the configuration problem. [VIP-8522]

• The vManage-server.log file in the nms directory contains a large amount of logging information, and some of the logs might not be useful for debugging issues. [VIP-11014]

• vManage NMS might fail to make a Netconf connection to devices when attempting to collect statistics. [VIP-11087]

• When the default value for a command option changes in a newer software version, the changes might not be reflected in configuration templates that you created on older software versions. However, the new default value is what is used in the newer software version. [VIP-12965]

• When displayed a DPI flow's packets, the vManage NMS might sort them incorrectly. [VIP-13832]

• In a vManage cluster that has two vManage servers, if you remove one of them, the remaining vManage server is no longer able to provide any management services. [VIP-14314]

• When you configure a vEdge router to be in more than one device group, the vManage screens that allow you to select by Device Groups might list all the groups as a single group instead of as separate groups. [VIP-14480]

• After you upgrade the vManage NMS to Release 16.1.2, the Dashboard might not display any statistics data. [VIP-17462]

• When you use vManage templates to change the configuration, the configuration differences might not display when you click the Config diff tab. [VIP-17686]

• In the software version drop-down in vManage Maintenance ► Software Upgrade screen, the software versions are sorted by time, not by version number. [VIP-17942]

• The vManage NMS does not raise an alarm periodically prior to when a certificate is about to expire. [VIP-17957]

• The vManage NMS does not raise an alarm when a certificate expires. [VIP-17958]

• The information displayed by the vManage Monitor ► Network ► Real Time ► Cflowd Flows commands might not be consistent with the information displayed by the show app cflowd flows CLI command. [VIP-18133]

• After you upgrade to Release 16.2.1, the banner feature template might no longer recognize quotation marks that are included in the banner. [VIP-18509]
• A netadmin user might not have all administrative-level capabilities for operations such as API calls and setting the default software version. [VIP-18512]

• You might not be able to open log files on the vManage NMS because socket connections to the configuration database are closed. [VIP-18936]

• The vManage NMS might not recognize the serial number of a vEdge router that is already present in the network so might be unable to connect to the router. [VIP-18990]

• If a user tries add a vSmart controller that is not actually present in the network, the vManage NMS might add it to the network even after the vManage NMS displays an error message indicating that the device is not present. [VIP-19155]

• In a three vManage cluster, if one vManage server is down for a prolonged time period (vManage1), and if the connection between the other two vManage servers goes down, it is possible that connection between the latter two vManage servers will not recover until the first vManage server (vManage1) is brought back up. [VIP-19373]

• On a vManage NMS running Release 16.2.2.1, you might not be able to push a template to a vSmart controller that contains a tloc-list configuration. [VIP-19483]

• From the CLI on the vManage NMS, when you issue the request nms configuration-db restore command, the output might indicate a failure in stopping NMS service when in fact it succeeded (the message "Could not stop NMS" followed by "Failed to restore the database"). If this occurs case, simply, re-issue the request nms configuration-db restore command. [VIP-19656]

• When you push a device template in which the chassis ID/UUID field contains a whitespace, an error message might incorrectly indicate that the device's personality cannot be determined. [VIP-19810]

• Some vManage charts might display only a maximum of six data series. [VIP-19849]

• In the vManage DPI flow output, the column "Entry Time" reports when the flow is logged, not when the flow started. [VIP-20497]

• On a vManage NMS running Release 16.2.3, you might not be able to activate policy changes. [VIP-20629]

• When you attempt to push a software upgrade from the vManage NMS to a few vEdge routers, the vManage Dashboard might display the message "This server is not the leader for that partition exception", and the vManage server might not receive any event notifications. [VIP-21062]

• In the vManage Monitor ► Device Real-Time Data drop-down, the interface queue command is missing. [VIP-21796]

• The vManage NMS might stop receiving event messages from the vEdge routers in the network. [VIP-21973]
• The Transport Interface pane on the vManage Dashboard might show information for non-transport interfaces. [VIP-21989]

• vEdge routers that have been marked as invalid might be listed in vManage device inventory API calls. [VIP-22410]

• The vManage server log file might contain "Failed to Publish" messages, and real-time commands that are executed on a device connected to another vManage NMS in the cluster might time out. [VIP-23647]

• 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]

• For an overlay network with a single vManage NMS, if the vManage NMS is stopped and move to another devices, the vManage services might not restart properly. [VIP-25692]

• When the vManage NMS is running Release 16.2.9.1, pushing device configuration templates to a large number of devices might take a long time. For example, with three vManage NMSs and about 800 devices, it might take 60 minutes to push the templates to all the devices. [VIP-26185]

• If you edit an existing centralized policy on the vManage NMS and then re-apply the policy to vEdge routers, the policy might not work. As a workaround, copy the entire policy, delete the existing policy, and then paste the copied policy before re-applying it. [VIP-26771]

• The vManage server might not process events received from vEdge routers. [VIP-28312]

• The vManage NMS might show that a vEdge router is in sync-pending state even after the router is reachable on the network. [VIP-28663]

• With Japanese versions of the Chrome and IE browsers, the vManage NMS might not display some tables and other screen fields. [VIP-28870]

**VRRP**

• 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]

**WLAN**

• 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]
Issues Fixed in Release 16.2.14

The following issue has been fixed in Viptela Software Release 16.2.14. The number following each issue is the bug number in the Viptela bug-tracking database.

Forwarding

- On a vEdge router, the flows on a tunnel might change even though no SLA policy is configured or the tunnel has not gone down. [VIP-23148: This issue has been resolved.]

Issues Fixed in Release 16.2.13

The following issue has been fixed in Viptela Software Release 16.2.13. The number following each issue is the bug number in the Viptela bug-tracking database.

Security

- During a POODLE attack against a TLS connection, all the device's CPU might be used or the vdaemon process might crash. [VIP-29376: This issue has been resolved.]

vManage NMS

- In the vManage AAA configuration feature template, when you select the RADIUS or TACACS tab, no parameter values might be displayed. [VIP-29540: This issue has been resolved.]

Issues Fixed in Release 16.2.12

The following issue has been fixed in Viptela Software Release 16.2.12. The number following each issue is the bug number in the Viptela bug-tracking database.

Forwarding

- On a vEdge 1000 or vEdge 2000 router, when NAT is enabled and fragmented packets are sent over the transport interface, the forwarding process (FP) might crash. [VIP-28084: This issue has been resolved.]

Issues Fixed in Release 16.2.11

The following issues have been fixed in Viptela Software Release 16.2.11. The number following each issue is the bug number in the Viptela bug-tracking database.

Cellular Interfaces
• If you have configured a profile for a cellular interface, when the interface is active, you cannot delete the profile. [VIP-20327: This issue has been resolved.]

Forwarding

• The show bfd sessions, show ipsec outbound-connections, and show tunnel statistics command might display inconsistent public port numbers. Also, the System IP, Local Color, and Remote Color fields in the output of the show tunnel statistics command might not contain any information. [VIP-24934: This issue has been resolved.]

• If you misconfigure a vSmart controller, the Forwarding Table Management process (ftmd) on the vEdge routers might crash when the routers receive OMP updates from the controller. [VIP-22116: This issue has been resolved.]

• When you are sending cflowd data to an external collector and the collector becomes unreachable, non-reachability messages are generated and written to the logs for every packet sent out for every flow. This process generates a huge number of log messages and might overwrite all other legitimate log messages. [VIP-22604: This issue has been resolved.]

OMP

• If a vEdge routers moves from one vSmart controller to another, and if a topology change occurs (such as a new or updated control policy or a route withdrawal), this change might not take effect on the vEdge router because it is in graceful restart mode with the previous vSmart controller. [VIP-23362: This issue has been resolved.]

Policy

• Application-aware routing policy might not take effect, causing data traffic to be directed to the incorrect tunnel interface. [VIP-26356: This issue has been resolved.]

Routing Protocols

• vEdge routers running Release 16.2.0 might not be able to receive multicast traffic. [VIP-25729: This issue has been resolved.]

Security

• On a vEdge 100m router, when you issue the show certificate root-ca-cert command, no output is displayed even when the show control local-properties command output shows certificate-status, root-ca-chain-status as installed, and certificate-validity as valid. [VIP-24316: This issue has been resolved.]

• On a vEdge router that has two Internet-facing interfaces, one of the interfaces might not be able to establish control connections or tunnels, and on this interface, many IPsec rekeying events might be occurring. [VIP-23870: This issue has been resolved.]

• The distribution of vEdge routers among multiple vSmart controllers might be inefficient, resulting in an unequal load for some of the vSmart controllers. [VIP-23915: This issue has been resolved.]

System
• The `show bfd sessions` command might indicate that BFD sessions are down when they are actually up. [VIP-12058: This issue has been resolved.]

• The kernel might crash, with the message "Watchdog: Timer started; sleeping for 600 secs..." [VIP-16463: This issue has been resolved.]

• Copying cflowd statistics from vEdge routers to the vManage NMS might take a long time, especially when there are large amounts of statistics. [VIP-23519: This issue has been resolved.]

• On a vEdge 2000 router, if you enable DPI and if the flow creation and deletion rate is very high, the forwarding table manager (FTM) might use large amounts of memory while performing flow visibility, and eventually, an out-of-memory condition might occur. [VIP-25005: This issue has been resolved.]

**vEdge Hardware**

• When you are using a fiber SFP, you are able to to configure `no autonegotiate` on the interface even though autonegotiation for 1000BaseT fiber is always enforced at the register level. [VIP-24490: This issue has been resolved.]

**vManage NMS**

• After you upgrade the Viptela controllers from Release 15.4.4 to Release 15.4.6, the vManage NMS might not be able to get updated information from the vSmart controller. [VIP-15546: This issue has been resolved.]

• The vManage NMS does not support VPN 512 for the vEdge 100b router. [VIP-23279: This issue has been resolved.]

• A user associated with a group does not have permission to read and write cannot change their own password in the vManage Administration > Manage Users screen. [VIP-24740: This issue has been resolved.]

• On a standalone vManage NMS, the messaging bus might stop operating and then restart, but when it restarts the vManage application server does not restart. [VIP-251499: This issue has been resolved.]

• Pushing a device configuration template from one of the vManage servers in a cluster might fail, with the "Failing with Server Not Leader" partition exception error. [VIP-25771: This issue has been resolved.]

• You might not be able to export the bootstrap configuration from the vManage server. [VIP-26209: This issue has been resolved.]

• In vManage NMS, the custom filter might not work when the time zone is set to UTC. [VIP-27154: This issue has been resolved.]

**Wireless WANs**
• For a vEdge100m router, ZTP fails if the technology configured for the cellular interface is set to auto. To correct this problem, set the technology to be lte. Do this either on the vManage VPN-Interface-Cellular configuration template or with the "vpn 0 interface cellular technology" CLI command. [VIP-23988: This issue has been resolved.]

---

**Issues Fixed in Release 16.2.10**

The YANG and enterprise MIB files have been modified for Release 16.2.10.

The following issues have been fixed in Viptela Software Release 16.2.10. The number following each issue is the bug number in the Viptela bug-tracking database.

**Forwarding**

• vEdge routers running Release 16.2.2 might not learn RP mappings from PIM replicators. [VIP-19829: This issue has been resolved.]

• tcpdump vulnerabilities because of multiple CVE identifiers might occur. For more information, see [Vulnerabilities in tcpdump: Multiple CVE Identifiers](https://www.tcpdump.org/security/cve-2022-27272). [VIP-23528: This issue has been resolved.]

**Routing Protocols**

• If you enable BGP on a vEdge router, the router might reboot. [VIP-24064: This issue has been resolved.]

**vBond Orchestrator**

• On a vBond orchestrator, an interface in the transport VPN (VPN 0) might not be able to renew its DHCP address. [VIP-23780: This issue has been resolved.]

**vEdge Hardware**

• On a vEdge 2000 router running Release 16.2.9, you might not be able to bring up a 1-GB SX fiber interface. [VIP-23176: This issue has been resolved.]

**vManage NMS**

• The vManage dashboard might show the incorrect certificate expiration even after certificate has been renewed. [VIP-23779: This issue has been resolved.]

• When you push a policy from the vManage NMS to the vSmart controller, an "unknown command" exception for NCS might occur on the vManage NMS. [VIP-23804: This issue has been resolved.]

• On vEdge routers, the number of octets of data received on an interface might be significantly different from the recorded interface transmission speed. [VIP-24027: This issue has been resolved.]
Issues Fixed in Release 16.2.9.1

The following issues have been fixed in Viptela Software Release 16.2.9.1. This release is for vManage NMS only, so all the fixed issues address vManage NMS problems. The number following each issue is the bug number in the Viptela bug-tracking database.

vManage NMS

• In the vManage NMS Maintenance ► Software Upgrade screen, when you delete a software image, the vManage NMS might indicate that the operation is successful, but the software image might still be shown in the Delete Available Software dialog list. To remove the software version from the list, you must perform a Rediscover Network operation. [VIP-17057: This issue has been resolved.]

• The vManage NMS might create alarms that are duplicates of previously created alarms. [VIP-22936: This issue has been resolved.]

• After you upgrade the vManage NMSs and vSmart controllers to Release 16.2.7, the vSmart controllers might not have the correct policy. As a workaround, deactivate and then reactivate the policy. [VIP-22980: This issue has been resolved.]

Issues Fixed in Release 16.2.9

The following issues have been fixed in Viptela Software Release 16.2.9. The number following each issue is the bug number in the Viptela bug-tracking database.

DHCP

• Devices at a site behind a vEdge router might not be able receive IP addresses from a DHCP server, because their DHCP requests contain more options than the router supports. [VIP-20652: This issue has been resolved.]

Forwarding

• The vManage NMS might not collect and display all error messages from vEdge routers. [VIP-19868: This issue has been resolved.]

• On a vEdge router, if TLOC connections continuous go down and then come back up, causing control connections to be cleared and reset, the OMP process (ompd) might create a core file. [VIP-22954: This issue has been resolved.]

Security

• When you invalidate a vSmart controller, connections between the controller and the vEdge routers might go down and then come back up again. This flapping might interfere with OMP graceful restart. [VIP-22263: This issue has been resolved.]

vEdge Routers

Created on: Sat, 01 Jun 2019 14:32:11 GMT
Generated by: Anonymous
• On vEdge 2000 routers, an unexpected reboot might occur, and the console has no information to indicate the cause of the reboot. [VIP-17514: This issue has been resolved.]

vManage NMS

• The vManage server log files might contain a large number of duplicate BFD record messages. [VIP-22098: This issue has been resolved.]

• The vManage NMS might not be able push a template that contains a large number of variables to large number of devices.[VIP-22099: This issue has been resolved.]

Issues Fixed in Release 16.2.8

Release 16.2.8 was not released.

Issues Fixed in Release 16.2.7

The YANG and enterprise MIB files have been modified for Release 16.2.7.

The following issues have been fixed in Viptela Software Release 16.2.7. The number following each issue is the bug number in the Viptela bug-tracking database.

Cellular Interfaces

• For cellular interfaces, the default Japan APN is now OCN. [VIP-21728: This issue has been resolved.]

Kernel

• When a user is connected via an SSH session to a vEdge router, they might be able enter a magic SysRq key or issue a Break sequence from the keyboard. Entering one of these sequences allows a user to reboot the router or perform other low-level operations on the router. [VIP-20386: This issue has been resolved.]

Security

• Linux kernel vulnerability CVE-2016-8655 allows a user to gain root access by leveraging the CAP_NET_RAW capability. The fix to this vulnerability, provided by kernel.org, has been incorporated into the Viptela software. See this Viptela security advisory. [VIP-21957: This issue has been resolved.]

SNMP

• You cannot include the angle bracket characters (< and >) in SNMP community strings. [VIP-20399: This issue has been resolved.]

System

• The show interface command lists GRE interfaces as being half-duplex. [VIP-19863: This issue has been resolved.]
• Log files might not be rotated properly. [VIP-21605: This issue has been resolved.]

**vEdge Hardware**

• You might not be able to upgrade vEdge 1000 routers that are running Release 15.4.4 because of a firmware issue. [VIP-16902: This issue has been resolved.]

• A vEdge 2000 router might display the following error message on the console: "runsv: syslogd: fatal: cannot start /run: Exec format error". [VIP-17788: This issue has been resolved.]

• On the vEdge 100m router, if you upgrade from Release 16.1.1 to Release 16.2.2 using the `request software install` command, the upgrade might fail and display the error "mount: mounting /dev/mmcblk0p1 on /mnt failed: Device or resource busy". [VIP-20387: This issue has been resolved.]

• Too many statistics files under the /tmp/xml directory might cause a vEdge router to run out of memory. [VIP-21300: This issue has been resolved.]

• You might not be able to log in to a vEdge 100m router unless a console cable is connected to the router. [VIP-21774: This issue has been resolved.]

• On a vEdge 2000 router, if you install a 10-GB SFP into an 1-GB PIM, the router reboots continuously. [VIP-21888: This issue has been resolved.]

• NAT ECMP multiple next hop might cause a vEdge router to reboot. [VIP-22264: This issue has been resolved.]

**vManage NMS**

• The `show policy data-policy-filter` CLI command shows the correct information for a policy in a VPN, but the vManage Policy Data Policy Filters real-time command on the Monitor ► Network screen might show incorrect information about the policy. [VIP-19862: This issue has been resolved.]

• The vManage configuration templates might not be able to process CSV files. [VIP-22097: This issue has been resolved.]

---

**Issues Fixed in Release 16.2.6**

The following issues have been fixed in Viptela Software Release 16.2.6. The number following each issue is the bug number in the Viptela bug-tracking database.

**Forwarding**

• The forwarding table manager process (FTMD) might run out of memory, because there are numerous DPI flows. [VIP-20422: This issue has been resolved.]
• When you apply a centralized data policy applied on a vEdge router on which no GRE interface or service is configured, a route lookup might not be performed for the particular VPN and traffic might be blackholed. As a workaround, configure a GRE interface and a dummy service on the router. [VIP-21172: This issue has been resolved.]

Routing Protocols
• When the administrative and operational status of a TLOC interface are both Down, OMP might send advertisement for that interface. [VIP-21343: This issue has been resolved.]

SNMP
• Log files do not hide TACACS secret keys or SNMP community strings. [VIP-19750: This issue has been resolved.]

• The ifLastChange MIB object returns how long before the present time an interface event occurred instead of the time between when the system came up and when the interface entered its current operational state. [VIP-19915: This issue has been resolved.]

vEdge Hardware
• On a vEdge 1000 router with an LTE USB dongle, you might see a cellular1 interface in the output of the "show interface" command. [VIP-21161: This issue has been resolved.]

vManage NMS
• The vManage NMS might not display all alarm data. [VIP-18760: This issue has been resolved.]

• On a vEdge router with two tunnel interfaces, if you shut down and then bring up one interface and then the second, the Down even alarms might not be cleared properly. [VIP-20675: This issue has been resolved.]

• The vManage NMS might not display a Control TLOC Down alarm. [VIP-20986: This issue has been resolved.]

• In the vEdge Dashboard Health panel, when you click on Normal, no vEdge routers are listed, even when routers are known to be healthy. [VIP-21267: This issue has been resolved.]

Issues Fixed in Release 16.2.5
The YANG and enterprise MIB files have been modified for Release 16.2.5.
The following issues have been fixed in Viptela Software Release 16.2.5. The number following each issue is the bug number in the Viptela bug-tracking database.

Configuration
• On vEdge 1000 routers running Release 16.2.3, if you issue a **load override** command to load a configuration from another vEdge 1000 router, committing the configuration might fail. [VIP-20209: This issue has been resolved.]

Forwarding
• When a vEdge DHCP client sends a Discovery message and then responds with an Offer to another vEdge router, that vEdge router might ignore the offer and keeps sending Discovery messages. This occurs when the link layer destination address is set to client's MAC address. [VIP-20049: This issue has been resolved.]

• If you do not configure a source interface for a cflowd collector, flow collection might not occur even though there are interfaces in the VPN than can connect to the collector. One case where this has been observed is if you first configure a collection in a VPN and then configure the first interface in that VPN. [VIP-20180: This issue has been resolved.]

OMP
• In the `show ip routes` command, if you enter an IP prefix and a prefix length, the output displays all ECMP routes. If you enter just an IP prefix, the output displays only one route. [VIP-19872: This issue has been resolved.]

Security
• Linux security vulnerabilities CVE-2016-4997 and CVE-2016-4998 allow a user to gain root access by overrunning buffer sizes provided to netfilter. The fixes to these vulnerabilities, provided by kernel.org, have been incorporated into the Viptela software. See this Viptela security advisory. [VIP-16894: This issue has been resolved.]

• Linux kernel vulnerability CVE-2016-5195, also known as Dirty COW, could allow an attacker to take control of an affected system. The fix to this vulnerability, provided by kernel.org, has been incorporated into the Viptela software. See this Viptela security advisory. [VIP-20157: This issue has been resolved.]

System
• When you are using virtual machine (VM) on AWS, console instances might repeatedly spawn in the background. These instances use up memory resources, and the VM might eventually run out of memory, crash, or otherwise become unavailable. [VIP-20500: This issue has been resolved.]

• With the `tcpdump` command, a user logged into a Viptela device who enters the `–z` option with no preceding space (that is, `tcpdump -z`) or who encloses the `–z` option in quotation marks (that is, `tcpdump "-z"`) can possibly gain root access to the device. [VIP-20511: This issue has been resolved.]

vEdge Router
• You cannot mount a USB drive in a vEdge router that is offline. [VIP-19415: This issue has been resolved.]

vManage NMS
• Pushing a CLI template from the vManage NMS might get stuck, with error messages indicating a problem with the messaging bus used by the vManage cluster. [VIP-19789: This issue has been resolved.]

• When you boot a vManage NMS, VPN 512 might not start. [VIP-20503: This issue has been resolved.]
Issues Fixed in Release 16.2.4

Release 16.2.4 was not released.

Issues Fixed in Release 16.2.3

The YANG and enterprise MIB files have been modified for Release 16.2.3.

The following issues have been fixed in Viptela Software Release 16.2.3. The number following each issue is the bug number in the Viptela bug-tracking database.

Configuration and Command-Line Interface

- Including the `system archive` command in the configuration might not periodically archive a copy of the running configuration. [VIP-19643: This issue has been resolved.]

Forwarding

- For QoS, you can configure both low-latency queuing (LLQ) and random early detection (RED) drops. With the fix, you can no longer do this. If you attempt to configure both, an error message is displayed when you try to validate or commit the configuration. [VIP-361: This issue has been resolved.]

- Packets sent through a service GRE tunnel are not fragmented. [VIP-13932: This issue has been resolved.]

- When you manually configure hardware vEdge routers, the interface speed and duplex attribute on the router's interfaces might not match the configured values. [VIP-14614: This issue has been resolved.]

- BFD sessions between links might take an extra second to converge than the time configured with the BFD multiplier. [VIP-16588: This issue has been resolved.]

- DPI flows might not be exported because the out-of-memory timer does not activate. As a workaround, issue the `clear app dpi all` command. [VIP-19235: This issue has been resolved.]

- In VPN 512, you might not be able to activate a cflowd collector. [VIP-19263: This issue has been resolved.]

- Cflowd might not record the ingress interface for a GRE tunnel. [VIP-19300: This issue has been resolved.]

- The 32-bit ifMib counters wrap around after 31 bit; that is, after $2^{31} - 1$ instead of after $2^{32} - 1$. [VIP-19771: This issue has been resolved.]

Kernel

- After you push a QoS policy template from the vManage NMS to a vEdge 1000 router, the router might crash and reboot. [VIP-17849: This issue has been resolved.]

Policy
• When you include an internal delimiter such as underscore in a policer name, the forwarding policy manager process (fpmd) might create a core file. [VIP-19093: This issue has been resolved.]

• A vEdge 100 router might not have enough memory allocated to handle a large number of policy sequences. [VIP-19439: This issue has been resolved.]

Security

• When a vEdge router has a stable control connection on one color A, and when the control connection is down on color B but the BFD sessions are up and stable on color B, the router continues to make a control connection on color B. When the control connection on color B port hops, all BFD sessions flap on color B even though they are up. [VIP-17862: This issue has been resolved.]

• TACACS authentication from the vManage GUI fails if the vManage (rhost) server uses the IP address 127.0.0.1 instead the source IP address of user. [VIP-18869: This issue has been resolved.]

System

• The vManage NMS might report that a vEdge 2000 router running Release 16.1.1 is using 100% of available memory. [VIP-15432: This issue has been resolved.]

• After you upgrade from Release 15.3.8 to Release 16.2, the default software version changes to 16.2. However, you can still set the default software version to be 15.3.8, using either vManage NMS or the CLI. [VIP-18616: This issue has been resolved.]

• On vEdge routers, BFD sessions go down and then come back up when rekeying occurs. This is the expected behavior. [VIP-18954: This issue has been resolved.]

• The show control local-properties command output from the CLI or from the Monitor ► Network ► Real-Time screen might show invalid device UUIDs. The vManage configuration database creates entries for these invalid entries, and you might not be able remove or delete them from the configuration. [VIP-19574: This issue has been resolved.]

• When you instantiate a new AWS instance of the overlay network and configure the controllers and add them to the vManage NMS, the vBond orchestrator might not start unless you first reboot the orchestrator. [VIP-19575: This issue has been resolved.]

vManage NMS

• If the vManage NMS in a cluster that is running the configuration database reboots, the Dashboard on one or more of the vManage web servers might not load correctly. To recover from this situation, open an SSH session to each vManage server in the cluster and then do the following:

  1. On each vManage server, issue the request nms application-server stop command.
  2. On each vManage server, issue the request nms configuration-db stop command.
  3. On each vManage server, issue the request nms configuration-db start command.
4. Wait for 5 minutes for the configuration database to come online.

5. On each vManage server, issue the `request nms application-server start` command. [VIP-13597: This issue has been resolved.]

- The vManage NMS might stop displaying alarms for devices in the network. [VIP-14633: This issue has been resolved.]

- When you export a vManage CLI template from the Templates ► Devices ► Options screen, by clicking Export CSV, incorrect values are exported if a field contains a comma, even when you enclose the text of that field in quotation marks. As a workaround, export the CLI template from the Templates ► Devices ► Options ► Change Device Values screen, by clicking Export screen. [VIP-16550: This issue has been resolved.]

- It might take so long time for the vManage NMS to retrieve data from a vEdge router that the netconf session between the two devices times out. [VIP-17118: This issue has been resolved.]

- The vManage NMS might not be able to recognize the vEdge personality for a vEdge router. [VIP-17401: This issue has been resolved.]

- If you change the system IP address of a vManage NMS, the old address might remain in the vManage database. As a workaround, reboot the vManage NMS to update the address. [VIP-17674: This issue has been resolved.]

- From the vManage Configuration ► Devices screen, if you attempt to validate vEdge routers that have the same system IP address, the vManage NMS does not display a warning. [VIP-17924: This issue has been resolved.]

- When a control connection to a vEdge router goes down and then comes back up, the vManage NMS might push the entire configuration to the router even though the configuration has not changed. [VIP-17934: This issue has been resolved.]

- You might not be able to push a CLI template from the vManage server to a vSmart controller. [VIP-18022: This issue has been resolved.]

- The vManage NMS might display the name of a 10 Gigabit Ethernet interface as xge, not as 10ge. [VIP-18130: This issue has been resolved.]

- The vManage NMS might not be updated when one of its tunnel interfaces is shut down. [VIP-18226: This issue has been resolved.]

- After you upgrade a vEdge router to Release 16.1.2, the forwarding management process (ftmd) might crash, with the message "auto-loading has been declined by your auto-load safe-path". [VIP-18357: This issue has been resolved.]

- On the vManage NTP feature template, the template opens with the Authentication tab selected, and you cannot click the Server tab until you enter an Authentication Key. [VIP-18697: This issue has been resolved.]
• In a network with only one vManage NMS, the real-time show commands might not display any output. [VIP-18738: This issue has been resolved.]

• You might not be able to push a vEdge configuration from the vManage server if the vEdge router is already running with a different IP address from the one in the configuration to be pushed. [VIP-18739: This issue has been resolved.]

• The vManage out-of-band interface used for communicating with other vManage servers in the cluster might stop working. [VIP-18917: This issue has been resolved.]

• In the vManage VPN feature template, when you configure a secondary DNS address and set it as Global, when you edit the feature template, this address is shown as Default. [VIP-18923: This issue has been resolved.]

• When you edit an interface template that already has a primary and secondary DNS defined globally, the interface template loads the secondary DNS as a default type with an IP address, and when you apply the template, this IP address overwrites the secondary DNS. As a workaround, change the default type to global before applying the template. [VIP-18984: This issue has been resolved.]

• After you upgrade a vManage cluster to Release 16.2.0, 16.2.1, or 16.2.2, the vManage servers might not be able to synchronize the configurations of the vEdge routers if the SNMP view OID is configured to be 1.3. As a workaround, before you start the upgrade configure the SNMP view OID to be 1.3.6 (using the `snmp view oid` command). [VIP-18995: This issue has been resolved.]

• The vManage control connection screen does not properly report interfaces that are in the down administrative state. [VIP-19223: This issue has been resolved.]

• When more than 10 users are concurrently logged in to a vManage server, additional users might not be able to log in to that server. [VIP-19290: This issue has been resolved.]

• In a three-vManage cluster, if one vManage server is down for a prolonged time period (vManage1), and if the connection between the other two vManage servers goes down, it is possible that connection between the latter two vManage servers will not recover until the first vManage server (vManage1) is brought back up. [VIP-19376: This issue has been resolved.]

• On a vEdge 1000 router running Release 16.1.2, after you activate a new policy from the vSmart controller and then issue a `show policy service-path` command, the might crash and then reboot. [VIP-19389: This issue has been resolved.]

• From a vManage NMS running Release 16.2.2.1, you might not be able to push a template to a vSmart controller than contains a `tloc-list` configuration. [VIP-19452: This issue has been resolved.]

• After you upgrade to Release 16.2.2.1, the vManage audit log for the device configuration files might increase to many gigabytes, resulting in high disk usage. [VIP-19453: This issue has been resolved.]
• When you upgrade from Release 16.1.2.3 to Release 16.2.2.1, the vManage NMS might lose all its stored network configurations and might then have to re-create them after the upgrade completes. [VIP-19454: This issue has been resolved.]

• You might not be able to push a device template when the vManage NMS is synchronizing configurations with network devices. [VIP-19455: This issue has been resolved.]

• The vManage NMS might process events slowly. [VIP-19459: This issue has been resolved.]

• When one of the vManage NMSs in a vManage cluster takes over the collection of statistics and the processing of alarms from another vManage server, alarm collection might stop. [VIP-19460: This issue has been resolved.]

• Changing from vManage mode to CLI mode for a device might be successful even if the configuration synchronization from that device failed. [VIP-19488: This issue has been resolved.]

---

**Issues Fixed in Release 16.2.2.1**

The following issues have been fixed in Viptela Software Release 16.2.2.1. The number following each issue is the bug number in the Viptela bug-tracking database.

**vManage NMS**

• The performance of a vManage server might slow gradually because of inefficient memory usage. [VIP-18729: This issue has been resolved.]

• Using the vManage API, a user with read-only permissions might be able to retrieve a list of all users and their user groups and might be able to change the password of another user. [VIP-18833 and VIP-18834: These issues have been resolved.]

• For a vEdge 1000 router, the vManage Monitor ► Network ► System Status screen might not display any information. [VIP-19020: This issue has been resolved.]

• The vManage NMS might indicate that a device is unreachable even though it has a control connection to the vManage server. [VIP-19038: This issue has been resolved.]

• The vManage NMS might be unable to collect statistics from network devices. [VIP-19041: This issue has been resolved.]

---

**Issues Fixed in Release 16.2.2**

The YANG and enterprise MIB files have been modified for Release 16.2.2.

The following issues have been fixed in Viptela Software Release 16.2.2. The number following each issue is the bug number in the Viptela bug-tracking database.
Bridging

• If you create IRBs on two vEdge routers, their interfaces might be assigned the same MAC address. As a workaround, manually change one of the MAC addresses. [VIP-17047: This issue has been resolved.]

Forwarding

• If you push a new data policy from the vManage server to a vEdge router, the policy might not take effect. [VIP-17790: This issue has been resolved.]

System

• When you configure a GRE interface, the tunnel interface might stop transmitting traffic, and you might need to shut down the tunnel interface and bring it back up. [VIP-14666: This issue has been resolved.]

• When a vEdge 1000 router running Release 16.1.2 reboots, it might lose its configuration. [VIP-18434: This issue has been resolved.]

vEdge Hardware

• When you upgrade a vEdge 1000 router to Release 16.2, the router’s control connections to the vManage NMS might start going down and coming back up. This problem stops occurring when you downgrade to the previous software version. [VIP-17538: This issue has been resolved.]

vManage NMS

• When you click Send to Controller to push serial numbers to network controllers, you might see the error message "resource denied: duplicate command". [VIP-13765: This issue has been resolved.]

• The vManage NMS might not display cflowd statistics. [VIP-14533: This issue has been resolved.]

• When you add an RMAed device back into the network, it might take a long time before the device is viewable from the vManage NMS. [VIP-15173: This issue has been resolved.]

• No show commands identify software patches that have been applied to Viptela devices. To identify software patches, issue the request nms application-server version command on the vManage NMS. [VIP-15477: This issue has been resolved.]

• Users who have a read-only account on a vManage server can view the running configuration of controller devices, but cannot view the running configurations of vEdge routers. [VIP-17692: This issue has been resolved.]

• In the vManage Configuration ► Devices screen, you might not be able to sort the devices by system IP address. [VIP-16837: This issue has been resolved.]

• In the vManage BGP feature template, when you enter a 4-byte AS number in ASDOT syntax, the AS number might be truncated. For example, the AS number 65500.100 is truncated to 65500.1. [VIP-16960: This issue has been resolved.]
• When you rename a vManage device template, the new name appears on the device template screen, but the old name might still appear on the Edit template screen. [VIP-17080: This issue has been resolved.]

• On the vManage NMS, sort-by-date functions do not sort properly. [VIP-17196: This issue has been resolved.]

• When you enable "default information origination" in the vManage OSPF feature template, the feature template does not display it as enabled, but the configuration does appear on the vEdge router. [VIP-17246: This issue has been resolved.]

• In feature configuration templates, for fields in which you can enter multiple values, how you enter the values and the delimiters between them is inconsistent. [VIP-17278: This issue has been resolved.]

• On a vManage NMS, a main task might remain in the "in_progress" status when the task status for individual devices goes to the "Success" state. [VIP-17289: This issue has been resolved.]

• The vManage server might not display the application-aware routing summary information and might show an index not found exception error. [VIP-17397: This issue has been resolved.]

• When you are pushing a template from the vManage NMS, the push process might get stuck for a long time. [VIP-17844: This issue has been resolved.]

• You might not be able to log in to the vManage GUI. [VIP-17989: This issue has been resolved.]

• When you upgrade from Release 16.1 to Release 16.2, the vManage statistics database might get stuck during the upgrade operation. [VIP-17901: This issue has been resolved.]

---

**Issues Fixed in Release 16.2.1**

The YANG and enterprise MIB files have been modified for Release 16.2.1.

The following issues have been fixed in Viptela Software Release 16.2.1. The number following each issue is the bug number in the Viptela bug-tracking database.

**SNMP**

• SNMP might crash, with a segmentation fault error. [VIP-17536: This issue has been resolved.]

**vManage NMS**

• The vManage Monitor ► Network screen might not display interface and tunnel information for a device. [VIP-16682: This issue has been resolved.]

• The data displayed on summary charts might be inconsistent. [VIP-17015: This issue has been resolved.]
• When you change the system IP address of a device, the vManage NMS might still display the old system IP address. [VIP-16799: This issue has been resolved.]

• When you configure a service using vManage feature templates and assign the service to two interface, the configuration that the vManage NMS pushes to the vEdge router encloses the two interface names in quotations and so the configuration does not work. As a workaround, change the configuration from the CLI. [VIP-17245: This issue has been resolved.]

• If you modify the VPN-Interface-Etherface feature template, you might not be able to attach the device template containing this feature template to a device that has an operational Ethernet interface. [VIP-17478: This issue has been resolved.]

---

**Issues Fixed in Release 16.2.0**

The following issues have been fixed in Viptela Software Release 16.2.0. The number following each issue is the bug number in the Viptela bug-tracking database.

**Forwarding**

• When the watchdog timer expires, crash information might not be collected when the system reboots. [VIP-14822: This issue has been resolved.]

**Security**

• When you upgrade the vManage software, the Viptela software process (vdaemon) might crash. [VIP-16570: This issue has been resolved.]

**System**

• A vEdge router might reboot constantly, giving the reason as "Software initiated-temperature fault." [VIP-12063: This issue has been resolved.]

• The vSmart controller might stop operating and generate the syslog message "vsmart kernel: INFO: rcu_preempt detected stalls on CPUs/tasks". [VIP-14706: This issue has been resolved.]

• When the watchdog timer expires, crash information might not be collected when the system reboots. [VIP-14822: This issue has been resolved.]

• If a vEdge router establishes a connection with the vManage NMS, but the vManage NMS has no configuration for the router, the Viptela process (vdaemon) on the vManage NMS might slow down noticeably because it is searching the configuration database for the router's configuration. [VIP-15204: This issue has been resolved.]

• When you using the vManage NMS to upgrade the software on a vEdge 1000 router from Release 15.3.8 to Release 15.4.6, the routers might continuously reboot and display a message indicated that files are not found in the root filesystem. [VIP-16947: This issue has been resolved.]
vManage NMS

- In the Control Status: Control Up table, the entries are listed in random order. [VIP-6001: This issue has been resolved.]

- The `show policy qos-scheduler` command does not show which hardware queue is mapped to the scheduler. [VIP-7721: This issue has been resolved.]

- A vEdge router might try to establish a connection to a vBond orchestrator on an interface that is operationally down. [VIP-8269: This issue has been resolved.]

- In the vManage Attach Devices pop-up window, the search field filters the devices in the left and right lists at the same time. [VIP-8687: This issue has been resolved.]

- The power supply dashboard pane does not clearly indicate which power unit is operational. [VIP-9149: This issue has been resolved.]

- If you had configured a non-default value in a prior software release and that then became a default value in a later release, the value might still be displayed in the `show running-config` command as if it were a non-default value. You might see this with timers for security, OMP graceful, and BFD hello interval. [VIP-9164: This issue has been resolved.]

- When a vEdge router sends critical notifications to the vManage NMS, alarms might not be triggered on the vManage NMS. [VIP-9957: This issue has been resolved.]

- After you power down a device, the keystroke file for SSL certificates might become corrupted. As a workaround, regenerate the SSL certificates. [VIP-10070: This issue has been resolved.]

- After you push templates to devices a few times, the vManage NMS might not display information about the active devices. [VIP-10083: This issue has been resolved.]

- An exception event on the vManage NMS might occur every 5 seconds, and this event might make the NMS unusable. [VIP-10305: This issue has been resolved.]

- If you configure two vEdge routers with the same system IP address and then change the system IP address of one of them, the vManage dashboard does not display correct information about the routers. [VIP-10739: This issue has been resolved.]

- When you download an image to a vEdge router, the following message might be displayed: `java.net.SocketTimeoutException`. [VIP-10836: This issue has been resolved.]

- After you upgrade to Release 15.4.1, information about some network devices might not be displayed on the vManage dashboard. [VIP-11061: This issue has been resolved.]
• After you generate the CSR and send it to Symantec, the vManage NMS might not be able to retrieve the signed certificate. [VIP-10810: This issue has been resolved.]

• When you upgrade from Release 15.3.8 to Release 15.3.4, device information on vManage NMS might be inconsistent or stale. [VIP-11879: This issue has been resolved.]

• When you change the system IP address of a vEdge or vManage device, the vManage dashboard might show duplicate devices, one with the old IP address and one with the new address. [VIP-11924: This issue has been resolved.]

• When you configure vEdge routers to be in device groups, when you select the group on the Monitor ► Network screen, no routers might be listed. [VIP-11938: This issue has been resolved.]

• The time duration for displayed alarms and active alarms is not clear. [VIP-11997: This issue has been resolved.]

• When you push a device template, the status does not show which template is being pushed. [VIP-12710: This issue has been resolved.]

• The vManage Dashboard might display inaccurate information about BFD sessions running on vEdge routers. [VIP-13072: This issue has been resolved.]

• The vManage Interface Statistics screen might not list any interfaces. [VIP-13169: This issue has been resolved.]

• When you are transferring files to and from the vManage NMS during a software upgrade, the units are shown in bytes instead of megabytes. [VIP-13590: This issue has been resolved.]

• When you attach a configuration template to a device on the vManage Configuration ► Template screen, the preview page might not display the differences between the existing and the new configurations. [VIP-13600: This issue has been resolved.]

• In a network with multiple vSmart controllers and multiple vBond orchestrators, when one vSmart controller or one vBond controller is unreachable, the vManage NMS might generate a page timeout message instead of reporting which controller is down. [VIP-13764: This issue has been resolved.]

• The Controllers tab on the vManage Configuration ► Devices screen might indicate that a vEdge router acting as a vBond orchestrator is in CLI mode even though it is in vManaged mode. [VIP-13880: This issue has been resolved.]

• The vManage NMS might report that a site is down even if some vEdge routers at the site still have operational BFD sessions. [VIP-13958: This issue has been resolved.]

• In a vManage cluster, removing and then re-adding the cluster members one at a time is not supported. That is, if the cluster members are A, B, and C, after you remove and re-add A, then remove and re-add B, and finally remove and re-add C, the cluster does not resume functioning. [VIP-14089: This issue has been resolved.]
• When you attach a device template to a vEdge router, after the control connections between the router and the vManage NMS come up, the template might not get pushed to the router. The vManage NMS reports that the router device is offline. [VIP-14145: This issue has been resolved.]

• When you are deleting a default image from a device, the status messages displayed on the vManage NMS might not be helpful. [VIP-14151: This issue has been resolved.]

• When you create a login banner for a device using a vManage configuration template, entering a "\n" might not produce a line break in the banner text. [VIP-14273: This issue has been resolved.]

• In an overlay network with a cluster of vManage NMSs, if you add a valid vSmart serial number file on a vManage server via the CLI, or if you make changes to this file from the CLI, the changes are transient and are lost when you reboot the vManage NMS. This issue occurs on fresh deployments of Release 16.1. It does not occur if you are upgrading from Release 15.4 to Release 16.1. [VIP-14298: This issue has been resolved.]

• The vManage NMS might delete the cflowd records received from vEdge routers before it processes them. [VIP-14326: This issue has been resolved.]

• After a web browser has been on the vManage Monitor ► Network screen for about 20 minutes, when you search for devices, the list of devices displayed is incorrect. As a workaround, refresh the page or open a new browser window and navigate to the Monitor ► Network screen. [VIP-14722: This issue has been resolved.]

• The vManage GUI might become inaccessible. As a workaround, restart the vManage NMS server. [VIP-14953: This issue has been resolved.]

• On the Monitor ► Geography screen, when you click a device and then click Links, no links might be displayed. [VIP-15012: This issue has been resolved.]

• After you remove a vBond orchestrator and invalidate it from the vManage NMS, when you add a new vBond orchestrator, the vManage might show two entries for the orchestrator, one for the valid and one for the invalid orchestrator. [VIP-15153: This issue has been resolved.]

• On vManage NMS, when you are performing a software upgrade on 25 or more devices at a time, after the upgrade completes and control connections are operational, the vManage GUI might not show that the upgrade has succeeded. [VIP-15195: This issue has been resolved.]

• When you are configuring policy on the vManage NMS, scrolling through the policy might be slow or unresponsive. [VIP-15211: This issue has been resolved.]

• The vManage task list might show that a task is successful (with a green check), but the event level shows it as having failed. [VIP-15212: This issue has been resolved.]

• vManage alarms might not be displayed on the vManage alarm screens. [VIP-15221: This issue has been resolved.]
• When you detach and reattach a vManage NMS from one VM to another, the vManage database might end up with incorrect information for the vManage UUIDs. [VIP-15266: This issue has been resolved.]

• When you move the third disk partition on a vManage VM, the organization name might be lost. [VIP-15267: This issue has been resolved.]

• When you are creating a device template for a vEdge router on the vManage Configuration ► Templates ► Device screen, if you first choose feature templates for AAA, BFD, OMP, and Security, and then you choose a System feature template, the selections you made for BFD and OMP templates might be lost. As a workaround, choose a System feature template first, then choose the AAA, BFD, OMP, and Security feature templates. [VIP-15272: This issue has been resolved.]

• The vManage statistics database might generate search event processing exceptions. [VIP-15278: This issue has been resolved.]

• With a standalone vManage NMS, when you upgrade the vBond orchestrator from Release 16.1.0 to Release 16.1.1, the vManage NMS receives the upgrade confirmation and the "up" event. However, the Netconf connection from the vManage NMS to the vBond orchestrator might time out. If this occurs, the vManage server shows that the vBond orchestrator is unreachable. If you wait about 6 minutes, the vManage NMS checks for control connections, discovers the vBond orchestrator, and shows that the vBond orchestrator is reachable. [VIP-15307: This issue has been resolved.]

• In vManage NMS, on the Configuration ► Templates ► Feature screen, the default templates might not be displayed. [VIP-15350: This issue has been resolved.]

• If you update an existing OSPF configuration template and push the template to the vEdge router, the new configuration takes effect but the vManage server might show that the old OSPF template is still attached to the router. [VIP-15634: This issue has been resolved.]

• After you upgrade the vManage NMS from Release 15.4.6 to Release 16.1.1 using the management interface in VPN 512, the vManage GUI might not work. As a workaround, first upgrade from Release 15.4.6 to Release 16.1.0, and then to Release 16.1.1. [VIP-16010: This issue has been resolved.]

• The vManage CLI template variables page might display variables in a different order from how they appear in the actual CLI template. [VIP-16167: This issue has been resolved.]

• It might take a long time to delete a non-active software version from a vManage server in a cluster. [VIP-16573: This issue has been resolved.]

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 16.2.0
• YANG and Enterprise MIB files for Release 16.2.1
• YANG and Enterprise MIB files for Releases 16.2.2 and 16.2.2.1
• YANG and Enterprise MIB files for Release 16.2.3
• YANG and Enterprise MIB files for Releases 16.2.5 and 16.2.6
• YANG and Enterprise MIB files for Releases 16.2.7 through 16.2.9.1
• YANG and Enterprise MIB files for Releases 16.2.10 through 16.2.14

The Viptela product documentation is organized into seven modules:

<table>
<thead>
<tr>
<th>Module</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Getting Started</td>
<td>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.</td>
</tr>
<tr>
<td>vEdge Routers</td>
<td>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.</td>
</tr>
<tr>
<td>Software Features</td>
<td>Overview and configuration information for software features, organized by software release.</td>
</tr>
<tr>
<td>vManage How-Tos</td>
<td>Short step-by-step articles on how to configure, monitor, maintain, and troubleshoot Viptela devices using the vManage NMS.</td>
</tr>
<tr>
<td>Command Reference</td>
<td>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.</td>
</tr>
<tr>
<td>vManage Help</td>
<td>Help pages for the vManage screens. These pages are also accessible from the vManage GUI.</td>
</tr>
</tbody>
</table>

**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.

Issues

• The maximum PDF page limit is 50 pages.

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

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

Revision 1—Release 16.2.0, July 15, 2016
Revision 2—Release 16.2.1, August 3, 2016
Revision 3—Release 16.2.2, August 31, 2016
Revision 4—Release 16.2.2.1, September 16, 2016
Revision 5—Release 16.2.3, October 7, 2016
Revision 6—Release 16.2.4 was not released
Revision 7—Release 16.2.5, November 7, 2016
Revision 8—Release 16.2.6, December 2, 2016, for vManage NMS only
Revision 9—Release 16.2.6, December 6, 2016, for all platforms
Revision 10—Release 16.2.7, December 20, 2016
Release 16.2.8 was not released.
Revision 11—Release 16.2.9, January 17, 2017
Revision 12—Release 16.2.9.1, for vManage NMS only, January 23, 2017
Revision 13—Release 16.2.10, March 14, 2017
Revision 14—Release 16.2.11, May 16, 2017
Revision 15—Release 16.2.12, July 26, 2017
Revision 16—Release 16.2.13, August 29, 2017
Revision 17—Release 16.2.14, December 22, 2017