Release Notes

Arista VeloCloud SD-WAN

Version 6.4

Arista.com

Headquarters	Support	Sales
5453 Great America Parkway Santa Clara, CA 95054 USA +1-408-547-5500	+1-408-547-5502 +1-866-476-0000	+1-408-547-5501 +1-866-497-0000
www.arista.com/en/	support@arista.com	sales@arista.com

Contents

Arista VeloCloud SD-WAN 6.4.0 Release Notes

This document contains the following sections

Introduction

Arista VeloCloud SD-WAN 6.4.0 | 2nd May 2025

- Arista VeloCloud SD-WAN™ Gateway Version **R6400-20250429-GA**
- Arista VeloCloud SD-WAN™ Edge Version **R6400-20250429-GA**
- Arista VeloCloud SD-WAN™ Orchestrator Version **R6400-20250430-GA**

Check for additions and updates to these release notes.

What Is in The Release Notes

The release notes cover the following topics:

Recommended Use

This release is recommended for all customers who require the features and functionality first made available in Release 6.4.0.

Important:

Release 6.4.0 contains all fixes found in the 6.4.0 Release Notes as follows:

- All Orchestrator fixes up to build **R6310-20250320-GA**.
- All Edge fixes up to build **R6200-20250305-GA**.
- All Gateway fixes up to build **R6200-20250108-GA**.

6.4.0 is a Long-Term Support (LTS) Release Candidate

Arista VeloCloud SD-WAN/SASE introduced a Long-Term Support (LTS) policy to enhance the operational efficiency of our partners and customers during the implementation of new software. In continuation of this policy, the SD-WAN Release 6.4.0 is offered as an LTS Release Candidate. For additional information about our Long-Term Support program see: Arista VeloCloud SD-WAN/SASE Long-Term Support Release (326448).

Compatibility

Release 6.4.0 Orchestrators support all previous Arista VeloCloud SD-WAN Edge versions lesser than or equal to Release 6.2.0.

The following SD-WAN interoperability combinations were explicitly tested:

Orchestrator	Gateway	Edge	
		Hub	Branch/Spoke
6.4.0	5.2.4	5.2,4	5.2.4

6.4.0	6.4.0	5.2.4	5.2.4
6.4.0	6.4.0	6.4.0	5.2.4
6.4.0	6.4.0	5.2.4	6.4.0
6.4.0	5.2.5	5.2.5	5.2.5
6.4.0	6.4.0	5.2.5	5.2.5
6.4.0	6.4.0	6.4.0	5.2.5
6.4.0	6.4.0	5.2.5	6.4.0
6.4.0	5.4.0	5.4.0	5.4.0
6.4.0	6.4.0	5.4.0	5.4.0
6.4.0	6.4.0	6.4.0	5.4.0
6.4.0	6.4.0	5.4.0	6.4.0
6.4.0	6.0.0	6.0.0	6.0.0
6.4.0	6.4.0	6.0.0	6.0.0
6.4.0	6.4.0	6.4.0	6.0.0
6.4.0	6.4.0	6.0.0	6.4.0
6.4.0	6.1.0	6.1.0	6.1.0
6.4.0	6.4.0	6.1.0	6.1.0
6.4.0	6.4.0	6.4.0	6.1.0
6.4.0	6.4.0	6.1.0	6.4.0
6.2.0	6.2.0	6.2.0	6.2.0
6.4.0	6.2.0	6.2.0	6.2.0
6.4.0	6.4.0	6.2.0	6.2.0
6.4.0	6.4.0	6.4.0	6.2.0
6.4.0	6.4.0	6.2.0	6.4.0

Important:

Arista VeloCloud SD-WAN Release 4.0.x has reached End of Support; Releases 4.2.x, 4.3.x, and 4.5.x have reached End of Support for Gateways and Orchestrators.

- Release 4.0.x reached End of General Support (EOGS) on September 30, 2022, and End of Technical Guidance (EOTG) December 31, 2022.
- Release 4.2.x Orchestrators and Gateways reached End of General Support (EOGS) on December 30, 2022, and End of Technical Guidance on (EOTG) March 30, 2023.
- Release 4.2.x Edges reached End of General Support (EOGS) on June 30, 2023, and will reach End of Technical Guidance (EOTG) September 30, 2025.
- Release 4.3.x Orchestrators and Gateways reached End of General Support (EOGS) on June 30, 2023, and End of Technical Guidance (EOTG) September 30, 2023.
- Release 4.3.x Edges reached End of General Support (EOGS) on June 30, 2023, and will reach End of Technical Guidance (EOTG) September 30, 2025.
- Release 4.5.x Orchestrators and Gateways reached End of General Support (EOGS) on September 30, 2023, and End of Technical Guidance on (EOTG) December 31, 2023.
- Release 4.5.x Edges will reach End of General Support (EOGS) on September 30, 2025, and End of Technical Guidance (EOTG) December 31, 2025.
- For more information please consult the Knowledge Base article: Announcement: End of Support Life for Arista VeloCloud SD-WAN Release 4.x (88319).

Note:

Arista VeloCloud SD-WAN Release 5.x is approaching the End of Support for 5.0.x, 5.1.x, 5.2.0, 5.2.2, and 5.4.x Orchestrator and Gateway versions.

- Release 5.0.x Orchestrator, Controller, and Gateway will reach End of General Support (EOGS) on February 28, 2025, and End of Technical Guidance (EOTG) February 28, 2026.
- Release 5.0.x Edges will reach End of General Support (EOGS) on February 28, 2026, and End of Technical Guidance (EOTG) February 28, 2027.
- Release 5.1.x Orchestrator, Controller, and Gateway will reach End of General Support (EOGS) on February 28, 2025, and End of Technical Guidance (EOTG) February 28, 2026.
- Release 5.1.x Edges will reach End of General Support (EOGS) on February 28, 2026, and End of Technical Guidance (EOTG) February 28, 2027.
- Release 5.2.0 and 5.2.2 Orchestrator, Controller, and Gateway will reach End of General Support (EOGS) on February 28, 2025, and End of Technical Guidance (EOTG) February 28, 2026.
- Release 5.2.0 and 5.2.2 Edges will reach End of General Support (EOGS) on February 28, 2026, and End of Technical Guidance (EOTG) February 28, 2027.
- Release 5.4.x Orchestrator, Controller, and Gateway will reach End of General Support (EOGS) on February 28, 2025, and End of Technical Guidance (EOTG) February 28, 2026.
- Release 5.4.x Edges will reach End of General Support (EOGS) on February 28, 2026, and End of Technical Guidance (EOTG) February 28, 2027.
- For more information please consult the Knowledge Base article: Announcement: End of Support Life for Arista VeloCloud SD-WAN Release 5.x (381499).

Release **5.2.3** and **5.2.4** are Long Term-Support Releases and are not included in this notice as the Orchestrator, Gateway, and Edge for these versions do not reach EOL until March, 2027.

Upgrade Paths for Orchestrator, Gateway, and Edge

The following lists the upgrade paths for Orchestrator, Gateway, or Edge from an older release to Release 6.4.0.

Orchestrator

Only Orchestrators using Release 5.2.x or later can be directly upgraded to Release 6.4.0.

Gateway

Upgrading a Gateway using Release 5.0.0 or later to Release 6.2.0 is fully supported for all Gateway types.

Important:

When deploying a new Gateway using 6.2.0 the VMware ESXi instance must be **either version 6.7, Update 3; version 7.0, Update 3; or version 8.0, Update 1**. Using an earlier ESXi instance will result in the Gateway's Dataplane Service failing when trying to run Release 6.1.0 or later.

Important:

Prior to upgrading a Gateway to 6.2.0, the ESXi instance must be upgraded to **either version 6.7, Update 3; version 7.0, Update 3; or version 8.0, Update 1**. Using an earlier ESXi instance will result in the Gateway's Dataplane Service failing when trying to run Release 6.1.0 or later.

Edge

An Edge can be upgraded directly to Release 6.4.0 from Release 4.5.x or later.

New Features and Enhancements

Link Insights

The Link Insights feature provides insights on Edges across Enterprise. This feature displays information on Edge incidents providing insights on link performance, reasons for failure, affected applications, traffic distribution and so on. This helps in optimizing network performance, troubleshooting, managing costs, and improving user experience. Starting from the 6.4.0 release, Arista VeloCloud introduces an **Insights tab** in the Orchestrator. This tab is located in the top menu of the Orchestrator screen, next to the Monitor tab, and is activated by default. Both Enterprise and Partner users can access this tab.

To access the feature, click **Insights,** and then from the left navigation, click **Link Insights**. The following screen is displayed:

Reduce SD-WAN Control Traffic on Wireless Link

The **Wireless Link Management** feature helps reduce SD-WAN control traffic and minimize high data usage on wireless links. The Orchestrator allows enterprise users to configure Wireless Link Management settings at both the Profile and Edge levels, effectively lowering data consumption on wireless links. To enable this feature, navigate to Device > Connectivity under the Edge or Profile, click Wireless Link Management, and use the Link Control Traffic Frequency toggle button.

LACP on Edge

This feature enables **LACP (Link Aggregation Control Protocol) on Edge** to combine multiple physical network links into a single logical link for increased bandwidth and redundancy. LACP automates the creation and

management of Link Aggregation Groups (LAGs), dynamically configuring aggregation, detecting link failures, and enabling failover.

Note:

Small and medium Edge models (5x0 or 6x0 Edge without Marvell switch, Edge 710, 710-5G, 720 and 740)support a maximum of two LAG ports, while large Edge models (Edge 3400, 3800, 3810, 4100, 5100) support up to a maximum of four LAG ports. Each LAG can have up to eight members of the same interface type and speed.

In LACP only active mode is supported. In active mode, the Edge will always send out PDUs. LAG interface is not allowed to configured as HA port. LACP port priority configuration is also not supported. It will support a max of 8 ports in the bond and all of the slave ports will be in Active state i.e. It will be eligible for Tx/Rx.

Automatic LAG configuration, as defined in the IEEE specification, is not supported in Phase 1. This specification states that in the absence of manual configuration, an appropriate set of LAGs should be automatically configured, and individual links allocated to these groups. While the capability for links to aggregate automatically exists, it is not currently supported in Phase 1

Symantec IPsec Dual WAN Link Support

Pre-requisite:

1. Create an SSE Subscription.
2. Enable ECMP on Edge and DCC.

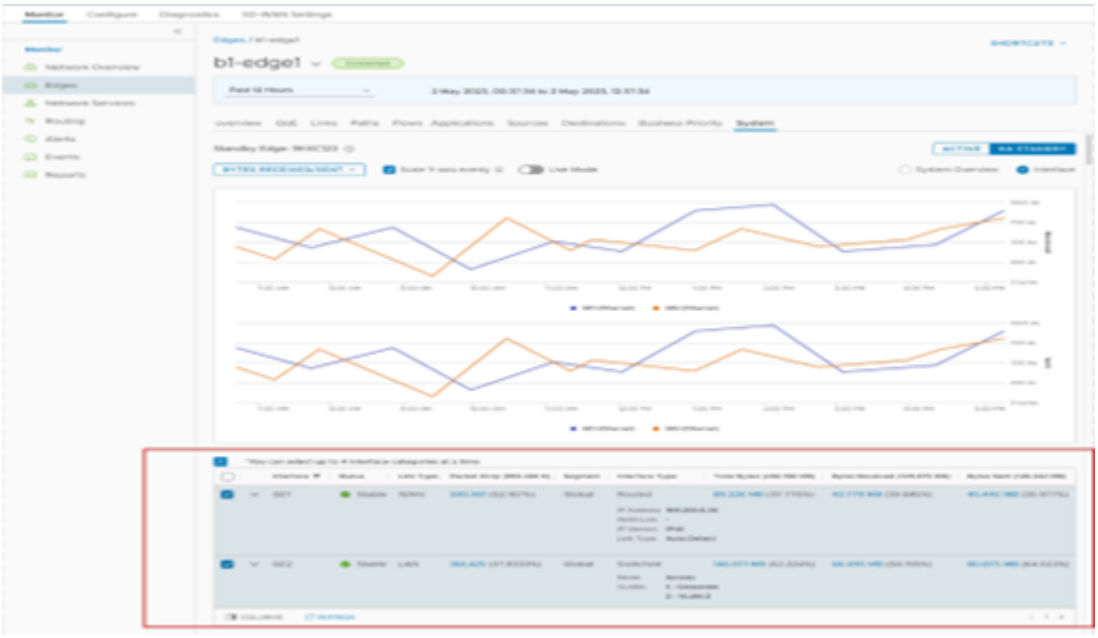
This feature provides support for the selection of dual WAN links, when creating an SSE Integration.This feature enhancement allows tunnel deployment on both the selected WAN links.

Note:

DCC is required for ECMP on Edge to work.

Network Interface Statistics Monitoring

This feature enables monitoring of data at the interface level. Customers can view both real-time and historical interface statistics on the Monitor › Edges › System › Interface screen of the Orchestrator. To access network interface stats, navigate to **Monitor** › **Edges** › **System**, then click the **Interface** radio button to view the interface statistics.



ECMP support on Edge

This feature enables **ECMP (Equal Cost Multi Path)** support on the Edge, enhancing throughput and resiliency by allowing multiple Equal Cost Multiple (ECMP) underlay routes (static/OSPF/BGP) across multiple LAN/WAN interfaces. It supports routing through BGP, OSPF, or static routing and improves traffic distribution by load balancing across multiple equal-cost NSD BGP/NSD static routes.

Note:

DCC has to be enabled.

Custom Applications

This feature enables Enterprise and Partner users to create Custom Applications and use these applications in Business Policy and Firewall rules creation.

Customizable Alerts

This feature provides an ability to configure custom events that trigger alert notifications via Webhooks, SNMP, and email. These notifications are automatically sent to target recipients when the configured event occurs. SMS alerts are not supported.

Self-Service Orchestrator Branding

This feature provides an ability for Enterprise users to brand the Orchestrator User Interface (UI) by applying their company's name, logo, and colors at a customer level.

Object Group Scalability

This feature enhances the maximum number of Object Groups that can be configured per Enterprise is increased from 1000 to 2000 (default). This limit can be adjusted using the system property "vco.object.groups.max.count.per.enterprise". Additionally, the maximum number of object group associations per Edge and its Profile is set to 1000 by default.

Firewall Rule with VLAN Behavior Enhancement

With this feature enhancement ,users can now specify the VLAN type (End-to-End or Local) to be used by the firewall engine as part of VLAN rule matches, When using a VLAN to match source or destination traffic in a firewall policy. A new field (VLAN Type) will appear when a firewall rule is matching a vlan for either the source or destination. VLAN Type will include 2 dropdown options - End-to-End, Local. End-to-End will be the default and reflects the current VLAN behavior handled by the firewall engine. Local option will allow for VLAN tags on local branches to be used by the firewall engine as part of VLAN rule matches,allowing users to disable remote VLAN significance .

Role Customization Usability Improvements

The Service Permissions tab has been improved for better role customization

Edge to Edge Unencrypted Data Channel

This feature enables SD-WAN Administrators to turn the Encryption on or off for their WAN links, from the Orchestrator. This will help customers achieving better goodout who are already leveraging Type-1 Encryptors to protect highly sensitive data and do not require additional encryption from the SD-WAN tunnel when traversing the WAN.

Enterprise Network Overview Improvements

The Network Overview dashboard is enhanced to display network traffic usage and configuration data for an Enterprise in two separate tabs and the traffic widgets are made more interactive and clickable. Clicking the link to a number in the Activated Edges or Links section, redirects to the Edges list page with the corresponding filter applied.Also, dashboard allows you to select the time range for which you want to display the traffic usage data.

The Traffic widget now displays Top Enterprise Apps by Data Volume (across Enterprise Edges) and Top Edges by Volume. Clicking on an app reveals its usage across all Edges.

User Authentication Security Policy Improvements

This feature improvement enables Partners to set their own password policies directly from the Authentication screen.

Multi-factor Authentication

This feature provides two factor authentication to be implemented for Partners. This is similar to the existing Enterprise authentication.

Qosmos Upgrade

With this enhancment, Qosmos Protobundle and the Engine is upgraded to its latest releases to support the classification of 700+ new apps along with all the AI related apps . The protobundle is upgraded to 1.730.1-24 version and engine upgraded to 5.9.0 version.

HMAC-SHA2 for VCMP tunnels

This enhancement will replace the SHA-1 by SHA-2 for IKE parent SA to improve VCMP tunnel compliance with industry security levels

Important Notes

Limitation When Deactivating Autonegotiation on Arista SD-WAN Edge Models 520, 540, 620, 640, 680, 3400, 3800, and 3810

When a user deactivates autonegotiation to hardcode speed and duplex on ports GE1 - GE4 on a Arista SD-WAN Edge model 620, 640 or 680; on ports GE3 or GE4 on an Edge 3400, 3800, or 3810; or on an Edge 520/540 when an SFP with a copper interface is used on ports SFP1 or SFP2, the user may find that even after a reboot the link does not come up.

This is caused by each of the listed Edge models using the Intel Ethernet Controller i350, which has a limitation that when autonegotiation is not used on both sides of the link, it is not able to dynamically detect the appropriate wires to transmit and receive on (auto-MDIX). If both sides of the connection are transmitting and receiving on the same wires, the link will not be detected. If the peer side also does not support auto-MDIX without autonegotiation, and the link does not come up with a straight cable, then a crossover Ethernet cable will be needed to bring the link up.

For more information please see the KB article Limitation When Deactivating Autonegotiation on Arista SD-WAN Edge Models 520, 540, 620, 640, 680, 3400, 3800, and 3810 (314011).

This release (6.4.0.0 does not include support for PAN. Support for PAN will be introduced in a future release.

Document Revision History

May 2nd, 2025. First Edition.

Edge/Gateway Resolved Issues

Resolved in Edge/Gateway Version R6400-20250429-GA

Edge/Gateway version R6400-20250429-GA was released on 05-02-2025 and resolves the following issues since Edge/Gateway version R6200-20250305-GA.

Fixed Issue 60896: BFD up/down events are not appearing on the Orchestrator's events monitoring page. Additionally, the Orchestrator's Routing monitoring page does not reflect the latest state of the BFD session.

MGD periodically queries the FRR BFD daemon to retrieve peer status. However, any state changes occurring within this 30-second polling interval are not reflected in the Orchestrator monitoring pages. Furthermore, when BFD is removed from the EDGE configuration, MGD's periodic poll does not explicitly notify Orchestrator about the BFD session removal. MGD only sends information about currently configured BFD sessions. If no sessions are configured, an empty blob is sent to the Orchestrator. Consequently, since Orchestrator expects explicit DOWN/ Removal events from the Edge/gateway to update its Routing monitoring page, the page remains unupdated. This results in stale BFD sessions being displayed on the Routing monitoring page.

Fixed Issue 67201: Active Edge may crash when Standby is newly detected.

When Standby is detected, the Active edge attempts to synchronize all path information with the Standby edge. If the path synchronization message exceeds 1500 bytes, the packet buffer is freed twice, resulting in a crash.

Fixed Issue 106946: On a PG VLAN handoff interface, ND6 resolution may not occur if the underlying physical interface has no IPv6 address configured.

On older releases, for PG VLAN handoff interfaces, ND6 incorrectly attempted to determine if the IP address belonged to the same subnet as the PG VLAN handoff interface by checking the IPv6 configuration of the underlying interface. If no IP was configured on the underlying interface (i.e., the IPv6 address was ::/0), ND6 considered the destination IP as belonging to the same subnet and skipped resolution altogether.

Fixed Issue 130674: IPv6 remote routes may be missing when the only physical interface configured with IPv6 is disconnected during Edge boot-up and then reconnected.

Edges do not learn IPv6 remote routes when the only physical interface configured with IPv6 is disconnected during Edge boot-up and then reconnected.

Fixed Issue 135938: When the nat_direct setting is enabled or disabled for a secondary IP, it is not applied. Instead, the nat_direct setting from the parent IP is used.

The implementation for the **nat_direct** setting on secondary IP addresses may miss the data plane. Although the configuration from Orchestrator was parsed and stored, the corresponding implementation for the expected behavior was absent.

Fixed Issue 148562: Azure Edge may not function properly when GE1 is used as the WAN link.

The kernel-to-interface mapping is incorrect when GE1 is used as the WAN link, as it currently maps to GE3. The fix involves correctly mapping the interface to the WAN link.

Fixed Issue 148486: Customers may not be able to use GE1 as a routed interface on Azure or AWS virtual Edges.

Public cloud virtual Edges use the first interface, GE1, to access the metadata server. The first interface is called the console interface, and it is used exclusively for retrieving data from the metadata server. With the fix, the interface operates as follows:

On unactivated cloud edges:

- SSH access is allowed on the interface.

On activated cloud edges:

- SSH access must be configured on the orchestrator GUI.
- The DHCPv4 address on the interface must be configured or will be overridden to support the DHCPv4 address.

Fixed Issue 148985: The kernel's default route sometimes disappears after system upgrades, DHCP lease renewals, interface status changes (up/down), or the application of static configurations.

The kernel's default route occasionally disappears for routed interfaces. These issues have been observed following release upgrades, DHCP lease renewals, interface status changes (up/down), and similar events. The exact root cause remains undetermined. In one instance, a misconfigured default gateway in a static configuration was identified as the culprit. A workaround has been implemented to check interface information in Ubus and compare it to the kernel's default route. Missing routes are then added if necessary.

Fixed Issue 150416: Users may experience long convergence time.

The users may experience an issue related to the dropping of Connect Notify Informational messages, which delays tunnel establishment.

Fixed Issue 151728: DHCPv6 relay packets, which are intended to flow from the edge towards the server, may be dropped, resulting in the failure of the relay functionality.

When a relay agent sends a DHCPv6 relay-forward message through the Edge, the Edge drops it if no relay is configured on the incoming interface.

Fixed Issue 151891: Remote Diagnostics functionality for HA_INFO command using Json APIs may get affected.

In Remote Diagnostics, HA_INFO command may fail with invalid key error when it is run using Json APIs.

Fixed Issue 152184: When a user configures the edge as a DHCP server, clients will receive Router Advertisement (RA) messages with the "advAutonomous" flag set to 1. This can lead to clients automatically generating their own autoconfiguration addresses.

Examining the **radvdump** output on the client side reveals that the edge router is sending Router Advertisements (RAs) with the **advAutonomous** flag set.

Fixed Issue 152429: After HA fails over a few remote routes may not be installed in the FIB.

After a hub HA failover, when the tunnel to a spoke comes up but is unstable for a period of time, routes from that spoke may be removed as they are considered stale. However, when the tunnel later becomes stable, the routes may not be installed back into the FIB due to mishandling of tunnel up/down events.

Fixed Issue 153261: Performance degradation in enhanced HA setup.

Setting the kernel I/O thread priority to real-time will impact the scheduling of edge threads.

Fixed Issue 153444: Port scanning reveals that ports 4321, 4322, and 5901 are exposed when VNF is enabled.

Port scanning reveals that ports 4321, 4322, and 5901 are exposed when VNF is enabled. The system is currently running monitoring services on these ports for QEMU. The fix is to run them on the localhost IP address instead of 0.0.0.0.

Fixed Issue 153469: IfXTable-related MIBTree queries are not affected currently.

IfXTable-related MIBTree queries are not affected currently.

Fixed Issue 153475: In a high-availability (HA) edge, the Link of Sight (LoS) on the standby edge may show as down when unique LAN or WAN MAC addresses are enabled.

If LoS is enabled along with unique LAN or WAN MAC addresses, the standby edge's interface LoS state is set to 0. This can negatively impact HA failover scenarios based on interface count mismatches.

Fixed Issue 153640: Overlay routes may not be present in the Zebra (BGP/OSPF) redistribution tables, preventing them from being advertised to BGP/OSPF peers.

During spoke movement between hubs/clusters, or during upgrade/reboot or service restart, a timing issue can occur. The remote-spoke UP event may be processed before hub reachability is set to true. This is followed by remote route addition triggered by the gateway and hub UP event. After this sequence, the route will be present in the FIB with reachability set to True, but it will not be synced to BGP/OSPF.

Fixed Issue 153924: Upon receiving an ingress packet on a Marvell switch port, the switch floods it to all other ports if the Edge host contains the packet's destination MAC address.

Marvell switches forward received packets using their Address Translation Unit (ATU) table. If the ATU table does not contain the destination MAC address, they flood packets to all other ports.

Fixed Issue 154005: Return traffic may be dropped unexpectedly when using a Non-SDWAN site (NSD) via Gateway backhaul with Port-Based Network Address Translation (PB NAT).

The root of the issue is the Edge is performing an unnecessary route relookup when the destination PI is already known from the NAT entry. This relookup can result in a mismatch between the intended destination and the selected path. This mismatch causes the packet to be dropped with an "nsch_*drop*_badpi" error.

Fixed Issue 154079: After the upgrade, private tunnels between the HA HUB and spokes may not be formed.

When the HA HUB is upgraded, the standby unit is upgraded first, followed by the active unit. During the standby HUB's upgrade to a newer software version, the spoke retains the tunnel context established in the older release. After the HUB upgrade, the spoke attempts to re-establish tunnels using the older tunnel context, resulting in a persistent path down state. To resolve this, disconnect the tunnel data (TD) when a peer software version mismatch is detected.

Fixed Issue 154765: Users may experience error log message cookie=0 in edged.log.

Users may encounter the error log message "cookie=0" in edged.log. In some cases, the responder side might not be able to send an IKE replay packet.

Fixed Issue 154831: EDGE SERVICE_FAILURE event may be seen on Orchestrator post reboot remote action

When a user reboots an edge via Remote Actions, a diagnostic dump and core may be generated. This crash should not be reported as SERVICE_FAILURE in Orchestrator because it is user-initiated.

Fixed Issue 154854: BGP neighbour debugs may not be enabled for Gateways.

BGP neighbour debugs were not enabled for Gateways.

Fixed Issue 155042: If an edge is certificate-enabled, it has been found that after the gateway's certificate renewal, the bandwidth (BW) cap to the peer edge becomes 0. This results in a drop in customer traffic experience.

During the certificate renewal process, Edge traverses a different path in the state machine and does not send the bandwidth cap to the Gateway.

Fixed Issue 155517: Multiple cyclic restarts and HA instability occur when the switch connected to the WAN port experiences flapping.

When a user restarts the DHCP client after each failover, it implicitly flaps the interface, leading to HA instability.

Fixed Issue 155822: Network traffic may be interrupted for approximately one minute when rebooting the standby edge with a Marvell switch.

When using Marvell switches on 610 and 5x0 edges in an HA setup, an L2 loop may form briefly during the reboot of the standby edge, leading to a network outage.

Fixed Issue 155881: Customers may experience random edge freezing when a DNS server is hosted behind the edge and a large volume of DNS requests are directed to the server.

If a customer has hosted a DNS server behind an Edge, and DNS queries are sent to the server via the WAN interface, those packets will still be subjected to the DPI engine, even though they are classified.

Fixed Issue 155974: The Edge process sometimes gets stuck in the init stage after a power off and power on cycle.

During a power off event, the log buffer's contents or offsets may occasionally become corrupted. This can lead to log allocation failures after power on, causing the Edge process to get stuck in the init stage when attempting to log.

Fixed Issue 156072: In low bandwidth scenarios, the QoS weights defined in the Orchestrator may not be consistently honored by the Edge or Gateway.

When a load-balancing Business Policy is defined across multiple low-capacity WAN links (e.g., 10 Mbps each) and a single TCP flow utilizes this policy while competing with other TCP flows using different Business Policies with varying Classes of Service, the single TCP flow may receive less than its weighted fair share of the capacity as defined by the CoS weights configured in the Orchestrator. Conversely, higher priority Classes might receive more than their weighted fair share.

Fixed Issue 156187: Tunnel Cap limit reached warning is not generated on edges with max total tunnels on Edge which includes 128 NVS tunnels.

Current implementation of Tunnel Cap limit does not include the 128 NVS tunnels, which results in not generating the limit reach warning.

Fixed Issue 156473: The customer may see a warning message that the integrity check failed.

The customer may see a warning message that the integrity check failed, when the customer attempts to upgrade a Gateway using an image that was generated using a different signing key internally.

Fixed Issue 156892: A stuck application thread is detected and terminated by the watchdog process. While the thread is restarted, it subsequently exits and fails to resume operation.

The configuration may not be in sync on the standby Edge, or after a failover, the Edge status may show offline despite the data plane being operational. This behavior can occur if a request to obtain an Orchestrator diagnostic bundle for the HA pair or other similar standby tasks takes an extended amount of time.

Fixed Issue 156966: When a customer downgrades HA edges from a release greater than 6.2 to a lower release that does not support secure device secrets, the HA status will show as failed in Orchestrator.

By default, EFS secrets were encrypted even when the edge device secrets feature was disabled. During an upgrade, this leads to an exception in the HA worker thread. As a result, the HA status could not be updated, causing it to display as "HA failed" on the Orchestrator.

Fixed Issue 157156: Customers may be unable to open the Edge diagnostics page.

On a large Orchestrator, if the message count reaches the Redis 'client-output-limit', it may cause issues related to websockets. As a result, customers may be unable to open the Edge diagnostics page.

Fixed Issue 157650: Loss of Network Packet Size Breakdown in Monitoring Dashboards.

A change in how network statistics are stored in this release has resulted in the temporary loss of granular packet size data export. Specifically, the ability to view the distribution of packet sizes across different ranges (e.g., 0-63 bytes, 64-127 bytes, 128-255 bytes, etc.) within monitoring dashboards (Wavefront, Grafana) is temporarily unavailable. This impacts the ability to analyze and understand network traffic patterns at a detailed level.

Fixed Issue 157665: When IDPS is enabled, the /var/log/suricata.log file grows in size over time without rotation. On low-end platforms, this leads to increased system memory usage and can quickly exhaust available memory.

With IDPS enabled, the engine generates logs during initialization, rule parsing, etc., which are directly written to '/var/log/suricata.log'. As the edge receives daily IDPS bundle updates and logs are generated during rule reloads, this can consume significant space in tmpfs over time, particularly on low-end platforms.

To address this issue, the direct file logging is disabled and instead registered a logger callback. This allows edge service to utilize its own logging infrastructure, which rotates the file based on the configured size.

Fixed Issue 157667: Spokes routes on cluster members are missing post tunnel flaps on the cluster members.

Customers may experience an ISP outage on their hub for a few minutes. This outage caused all tunnels to the spokes and the gateway to flap, generating a large number of CONNECT/DISCONNECT events. This, in turn, resulted in a delay in processing stale route timers and deleting routes from the FIB.

Fixed Issue 157775: Paths to and from a Google Cloud Platform hosted gateway may experience unexpected loss.

Paths to and from a Google Cloud Platform hosted gateway may experience unexpected loss.

Fixed Issue 157837: OSPFD may restart in an Edge.

When OSPFD is first enabled on a few interfaces and then completely disabled on an edge, the clean up of memory may lead to memory corruption and crash of OSPFD.

Fixed Issue 157852: The Gateway may crash while handling configuration from the Orchestrator during an Azure automation process that configures BGP over IPsec on an NSD via the Gateway.

The Orchestrator sends invalid or null neighbor-ip and neighbor-as strings when using Azure automation. This causes a crash during gateway configuration parsing.

Fixed Issue 157898: The link may appear deactivated in Orchestratror for a high-availability (HA) edge.

Following a specific sequence of HA state transitions, the system continues to push old events to the Orchestrator repeatedly. If LINK_DEAD is among these events, the link state will remain stuck in deactivated mode on the Orchestrator.

Fixed Issue 158032: In rare scenarios, an Edge may become stuck in the init stage after a restart.

Before the first wraparound of the logging ring buffer, allocated blocks that were not written to since the edge restarted are not reset. This could lead to issues with subsequent log buffer allocations after the restart, potentially causing the edge to become stuck in the init phase when attempting to log.

Fixed Issue 158096: When CSS is configured with L7 health check, tunnels would not come up if the common criteria firewall is enabled.

When CSS is configured alongside L7 health checks and RPF is enabled via the Common Criteria Firewall, Non SD-WAN Destination tunnels (both IPsec and GRE) will fail to come up. Users may see **edged_route_lookup_fail_v4_drop** messages in the Edge service logs.

Fixed Issue 158172: ZTP may not work on some Edge models.

Some edge models may experience issues with ZTP functionality. This is because the UUID of the device was not sent on those specific models. With the implemented fix, the UUID will now be included for all Edge models.

Fixed Issue 158500: Edges stop forwarding LAN-side tagged traffic between LAN and WAN after upgrading to 5.2 or newer if the network configuration was originally configured via 4.x Orchestrator.

When a user configures edge network settings using 4.x Orchestrator, the LAN network configuration in Orchestrator does not specify VLANs for tagged interfaces. After upgrading both Edge and Orchestrator to 5.2 or newer, the Edge software fails to generate the correct LAN network configuration. This can prevent edges from processing LAN-side tagged packets.

Fixed Issue 158691: Certain Non SD-WAN Destination or datacenter configurations are not applicable to gateways when Cisco ASA NSD type is configured on the enterprise/customer without being linked to any Edges.

When a Non SD-WAN Destination of type Cisco ASA is configured for an enterprise, the Orchestrator fetches the LAN subnets of the edges present on that enterprise and pushes them as Custom subnets to the gateways. These subnets are used for IPSEC negotiation with the remote NSD endpoint. However, when the NSD is not associated with any Edges, the Orchestrator cannot populate the mandatory 'Custom subnets' required by Cisco ASA type NSDs. This results in the failure of NSD configuration parsing at gateways.

While it is expected that Cisco ASA type NSD parsing fails (until edges are associated with it), this should not impact the application of other NSD configurations on the gateway. Currently, the gateway's config parser aborts when encountering an error in a single instance of the NSD, preventing the application of other NSDs. This behavior should be addressed, as it can negatively impact the overall network functionality and security

Fixed Issue 159092: In rare instances, the active Edge in an HA pair may report its peer as unknown, which can impact enhanced HA traffic.

Due to an error in calculating the last seen time of the standby Edge, the active Edge mistakenly assumes no communication from the standby and declares the peer as unknown. This results in the reset of enhanced HA connections.

Fixed Issue 159337: TCP connections between end to end peers might stop working if one side is upgraded or loses context, even if the connections use fixed port numbers.

If a customer upgrades an Edge on only one side of an end-to-end (E2E) TCP connection, such as the client side, and the TCP server behind another edge has also lost context of the connection, new TCP connections attempted from behind the upgraded customer can become stuck in an established state without actually transmitting any meaningful traffic.

Fixed Issue 159532: When manual DNS source interface configuration is applied from the Orchestrator, it is not reflected on the Edge device. This results in DNS packets originating from the Edge carrying an incorrect source address. If appropriate routes are not configured for this source, DNS reply packets may fail to reach the Edge.

Users needs to select a specific DNS source interface in the Orchestrator instead of auto.

Fixed Issue 159674: High Availability is not formed in some scenarios when the standby is replaced.

During an HA failover, if the new standby is replaced before activation, HA will not form and the new standby will remain inactive.

Fixed Issue 159845: Severity of some of the INFORMATIONAL alerts are wrongly reported to Orchestrators.

A recent change in Suricata rules metadata by NSX has resulted in incorrect impact score calculations for some INFO-level alerts. This issue affects monitoring but does not impact traffic flow.

Fixed Issue 159733: NAT sessions are leaked when L7 Health Check is enabled on ZScaler IPsec and GRE CSS tunnels.

NAT sessions are leaked when L7 health checks are enabled on Zscaler IPsec and GRE CSS tunnels.

Fixed Issue 158012: When IDPS and URL filtering(or/and) Malicious are enabled together sometimes the Edge can crash as part of restart while going down.

When IDPS is enabled, Edge restarts. If both URL filtering and Malicious IP blocking are configured as security features, Edge crashes during shutdown. This issue only occurs when both features are enabled together, and it is not consistent.

Fixed Issue 158568: WebSocket JSON format response for "SYSTEM INFORMATION" cpu_30s_avg_pct is empty. Usually customers can request for this info via postman.

When a user requests system information, it triggers a health check. This health check retrieves the **cpu_30s_avg_pct** value. However, starting with release 5.1, we no longer send **cpu_30s_avg_pct**. Instead, we send **cpu_60s_avg_pct**. Since **cpu_30s_avg_pct** is no longer available, Postman will display its value as 0.

Fixed Issue 159329: Return packets are dropped and NAT table entries are leaked for Internet-bound flows originating from the Partner Gateway (PG) handoff interface VLANs.

Internet-bound flows that originate from the PG handoff interface are not properly handled in the Gateway leading to dropped packets and leaked resources.

Fixed Issue 159538: Routes not installed in the FIB with interconnect enabled, when the local endpoint of the tunnel flaps whereas the remote end remains stable.

With Interconnect enabled on Hubs and when the local endpoints of the tunnel flaps but the remote end remains stable, this would lead to marking the SoR entries via the nexthop as False resulting in deletion of routes from the FIB.

Fixed Issue 159793: A port is not detached from the LAG if the peer unsets the Aggregation bit in the LACP PDU.

When the peer tries to detach a port from the LAG by unsetting the aggregation bit in the LACP PDU, the edge ignores this and continues to use the port in the LAG. This is intentional per the Linux kernel implementation of LACP.

Fixed Issue 160080: Overlay and datacenter routes are being refreshed frequently, causing their age to reset to 1.

Spokes initiating Dynamic Edge to Edge (DE2E) tunnels to multiple edges with the same public IP will frequently trigger hub configuration messages towards the gateways. This occurs because DE2E tunnel establishment fails after N attempts. This failure stems from an undefined behavior when DE2E is attempted towards multiple edges sharing the same public IP. Consequently, the gateways refresh the routes they previously advertised in response to the hub configuration messages.

Fixed Issue 160542: After upgrading to software version 6.1.*, you may experience an issue where you are unable to ping your Edge's WAN link IP address from the internet.

After upgrading to software version 6.1.*, you may experience an issue where you are unable to ping your Edge's WAN link IP address from the internet. This is due to a change in how ICMP traffic destined for the Edge itself is handled. These packets are now being processed by the business policy engine, which can incorrectly route the ICMP reply through an unintended exit interface. This issue prevents external ping requests from reaching the Edge's WAN IP, potentially impacting troubleshooting and monitoring capabilities.

Fixed Issue 160805: Network connectivity failure for the gateway prevents tunnel formation and communication with the Orchestrator.

Network connectivity failure for the gateway prevents tunnel formation and communication with the Orchestrator. This issue can occur after upgrading the gateway to version 6.4. Upon reboot, the TAP device MAC address is incorrectly set during startup. This prevents the gateway from forming tunnels or communicating via the TAP interface.

Fixed Issue 161536: When an Edge is moved from HUB profile to SPOKE profile, the remote routes advertised by that edge may still remain in the current edges of the HUB profile, even after those are withdrawn by that Edge. Here HUB profile has more gateways configured and SPOKE profile is configured with only few out of those gateways.

When an edge is in a HUB profile, other members of the HUB profile receive routes from that edge via all the gateways. If the edge is moved from a HUB profile to a SPOKE profile, the current members of the HUB profile retain the remote routes received from the edge, even from gateways not part of the SPOKE profile.

If the edge subsequently withdraws the route, the gateways connected to the SPOKE profile will withdraw the route accordingly. However, gateways solely connected to the HUB profile will not withdraw the route as they are no longer connected to the edge. This occurs because the current members of the HUB profile still have remote routes from other gateways, preventing the removal of the specific route in question.

Fixed Issue 161113: When Enhanced Firewall Service is enabled on an edge device and a legacy application-based firewall rule with URL filtering is added above the Enhanced Firewall Service catch-all rule, subsequent traffic is dropped.

When URL filtering is enabled, at least 10 packets are subjected to DPI to extract the URL/domain for URL lookup. When the initial flow to MS Teams arrived, it was classified by DPI, and the DPI cache was updated. When the subsequent SYN packet arrived, it was first classified based on the DPI cache. This matched the legacy application-based firewall policy but was still subject to DPI for URL extraction. DPI re-classified the traffic as APP_TCP, leading to a firewall re-lookup. Because the traffic matched the EFS catch-all rule and the previous policy was a legacy firewall rule with no available URL for lookup, the traffic was dropped.

Fixed Issue 162452: When IPsec rekeying occurs, traffic through the tunnel is interrupted for a few seconds.

During IPsec rekeying, users detach the existing outbound child SA and attach the new outbound child SA to the cached SA. This brief process causes a temporary absence of the outbound SA, resulting in an attempt to delete and recreate the tunnel when sending packets.

Fixed Issue 162571: Firewall logs cannot be seen on Orchestrator.

While traffic is sent matching firewall rules with logging enabled, the logs are not appearing on the Orchestrator. This could be due to the user enabling local firewall logging.

Orchestrator Resolved Issues

Resolved in Orchestrator Version R6400-20250430-GA

Orchestrator version R6400-20250430-GA was released on 05-02-2025 and resolves the following issues since Orchestrator version R6310-20250320-GA.

Fixed Issue 53199: Orchestrator Network Service UI NVS via Gateway dialog for Palo Alto type shows incorrect lifetime values in IKE IPSec Configuration template.

Orchestrator Network Service UI NVS via Gateway dialog for Palo Alto type shows incorrect lifetime values in IKE IPSec Configuration template, however, there is no functional impact.

Fixed Issue 110097: In partner administration, the user delete button is disabled when filter is applied.

The User delete button is clickable even when a filter is applied, in partner administration.

Fixed Issue 116892: Users may not be able to see translated text for STANDBY tunnel state.

STANDBY tunnel state in **Monitor** > **Network Serivces** > **NSD via Edge** is hardcoded and when the page is translated, this text is not translated to the required language.

Fixed Issue 121316: Orchestrator does not allow to use IP address ending with '0' as network address during NSD configuration.

Validation check for the network address check has been removed (Destination IP address must not be Network or Broadcast IP address) and allowing users to configure the valid IP Address.

Fixed Issue 126147: Unable to save interface configuration with provinterval as null at Edge level.

Unable to save interface configuration with **provinterval** as null at the Edge level. This issue occurred because the UI was sending a null value for **provinterval** if it was somehow saved as null via profile configuration.

Fixed Issue 129524: Enterprise Support users may not see the configurations enabled by Partner Superuser.

Enterprise support users may not see the configurations enabled by Partner Superuser, this issue makes it impossible for customers to know if a feature is in use or not.

Fixed Issue 130975: OFC entry is not getting deleted for disabled subnet.

When the NSD tunnel is disabled, we can still view the corresponding OFC entry in the OFC routes list section. Ideally, this entry should not be shown here.

Fixed Issue 133200: Users on older versions (5.2 or earlier) saw interfaces that were not applicable to their Edge model. These interfaces were not editable.

Users on older versions (5.2 or earlier) saw interfaces that were not applicable to their Edge model. These interfaces were not editable.

Fixed Issue 133384: Enterprise users are encountering an error when clicking "View Gateways" from the shortcut menu and from the "View Gateways" link on the edge page.

Enterprise users do not have access to the API responsible for the View Gateways link. Only Operator and MSP users have access, as they handle sensitive information within the API response.

Fixed Issue 135482: In the UI, when requesting a PCAP bundle for Gateway cosmetic issues, cosmetic issues appear in filter.

In the UI, when requesting a PCAP bundle for Gateway cosmetic issues, cosmetic issues may appear in the filter.

Fixed Issue 139617: In Monitor > Routing > Edge BGP Neighbor State, Neighbors not configured in edge device settings page show up in ESTABLISHED state.

Previously, when a neighbor was deleted from the Edge device settings page, the **Monitor** > **Routing** > **Edge** BGP Neighbor State page did not remove the neighbor or mark it as REMOVED. This issue has been resolved. Now, when neighbors are deleted from the Edge configuration and the Edge removes the BGP neighbor from its configuration, they will also show up in REMOVED state on the monitor page.

Fixed Issue 146261: Select field has 2 underlines in UI.

In **reports** > **creation modal** > **time rang**e (step 2) > radio button: **schedule a repor**t > the dropdown input has 2 border bottom lines.

Fixed Issue 146275: Segments table cells are not aligned properly.

In **SD-WAN** > **Configure** > **Segments** page segments table cells are not aligned properly.

Fixed Issue 146665: NSD tunnels are added automatically back after deleting static routes.

When a user deletes site subnets, the associated static routes are cleared. However, when the user tries to add a new NSD with different site subnets, the previously cleared site subnets are incorrectly added again.

Fixed Issue 147978: Filters in the grid are not being saved when the page is refreshed or when the user navigates to other pages.

When a user configures a filter on any page, for example, **Monitor** > **Edges**, the link status might become disconnected. If the user navigates to a different page, such as **Monitor** > **Network Overview,** and then returns to **Monitor** > **Edges,** the previously applied filter needs to be reapplied.

Fixed Issue 148407: Operator Support user may be able to Edit/Delete DNS Services in Orchestrator despite not being authorized.

After logging into Orchestrator as an operator support user, navigate to **Customer** > **Configure** > **Network Services** and expand the DNS Services Accordion. The issue is that DNS services are currently editable by operator support users, despite these users not being authorized to make any additions, deletions, changes, updates, or modifications in this section.

Fixed Issue 148584: PSK value disappears when it fails to be decoded before saving in the server.

This issue occurs because the server is unable to decrypt the Pre-Shared Key (PSK) values. If the session context during decryption differs from the context used when encrypting the PSK values (while saving device settings from the UI), the server fails to decrypt them correctly and replaces the PSK value with null.

Fixed Issue 148600: Previously certificates for Edge and Gateway had a lifetime of 90 days and were renewed every 30 days.

Previously certificates for Edge and Gateway had a lifetime of 90 days and were renewed every 30 days. With this change, the default lifetime remains at 90 days but renewal is changed to be every 60 days. The impact to customers is that any disruption due to certificate renewal, for example momentary tunnel flaps, will be reduced . There are no other impacts other than fewer renewals over time.

Fixed Issue 148701: User was not able to update enterprise profile and was getting errors like VLAN ID cannot be removed.

If a VLAN is mapped to an interface at the Edge level, the Orchestrator UI should not allow its deletion.

Fixed Issue 149347: A cosmetic bug where role names appear differently when users log in from different locations.

When the same user logs in from two different locations, the User Management window displays different role names.

Fixed Issue 149356: The UI clears the Edge filter name after selecting a new time range.

When a user navigates to **Monitor** > **Events**, enters an edge name into the search text box, then goes to **Monitor** > **Edges**, selects an edge, and clicks **Shortcuts** > **View Events**, the events filtering does not update correctly.

Fixed Issue 149909: In some usage contexts, updating the SNMP v3 password (Edge > Telemetry > SNMP) allowed special characters to be saved.

When editing an already saved password, users were able to update it using characters that should not have been accepted. Other unreported contexts also allowed saving passwords with invalid characters.

Fixed Issue 150117: Customers have duplicate alert configurations for the same alert definition (e.g. multiple configurations for EDGE_DOWN alert). This is causing the UI not able to properly save any alert configuration changes.

The API-level validation around duplicate alert configurations doesn't work in certain scenarios, leaving the possibility to insert multiple configurations for the same alert definition.

Fixed Issue 151128: Non SD-WAN destination not showing primary and secondary SD-WAN gateway UI.

The UI for non-SD-WAN destinations was not appearing, specifically the UI for primary and secondary SD-WAN gateways.

Fixed Issue 152631: Users may not be able to select a Gateway in the Gateway route table.

Users may not be able to select a Gateway in the Gateway route table due to overflow.

Fixed Issue 152910: Users may see an empty info icon near the Autonegotiate setting on an SFP interface.

The info icon near "Autonegotiate" in the SFP interface did not provide any information on why the setting is disabled or enabled.

Fixed Issue 153298: When VLAN with id 1 does not exist at the profile level, then the customers get an error "VLAN with id 1 does not exist" when they try to save changes in existing profiles.

If the Orchestrator is running a version earlier than 5.2.0 and customers have deleted VLAN ID 1 (usually the corporate VLAN) from their profiles, they may encounter an error saying "VLAN with ID 1 does not exist" after upgrading to version 5.2.0 or later. This error occurs when attempting to make changes to their profiles. However, customers can now make profile changes even if VLAN ID 1 is not present in their profiles.

Fixed Issue 153373: The User Agreements dialog box without any action gets closed.

The User Agreements dialog box closes automatically without any user interaction on the **Monitor** page.

Fixed Issue 153859: During firewall configuration updates, firewall rule information is not pushed to the Firewall Rule Table.

Cloning profile is inserting duplicate references, which in turn is preventing firewall rule information from being pushed to the Firewall Rule Table.

Fixed Issue 153911: The QoE scores displayed in the Orchestrator UI and returned via the API are unreliable when a standby link is involved and do not reflect the actual quality of the user experience.

When calculating QoE, the scores of both active and standby links are averaged, which inaccurately reflects the health of the active link.

Fixed Issue 154008: The Orchestrator may throw an error: 'Cannot set property 'v6Detail' of undefined.

When the API request does not include **v6Detail**, Orchestrator throws an error. Ideally, it should use the default **v6Detail** if it is missing from the request.

Fixed Issue 154266: Sub-interface changes are not being reflected on the Edge.

Sub interface changes are not reflected on Edge without any bogus changes in release version 6.2.

Fixed Issue 154308: The BGP section in the Device Settings page occasionally fails to load.

On older edge devices, the BGP section in the Device Settings page may fail to load when **v6Detail** is missing from the BGP data, occurring in rare cases.

Fixed Issue 154362: When a hostname changes or is edited, the Flow Visibility tab in the Orchestrator Monitoring page does not reflect the new hostname, while the Source tab displays the updated hostname

Users relying on the Flow Visibility tab for monitoring and troubleshooting may experience confusion due to outdated hostname information. The Flow Visibility tab displays the hostname as it was recorded in the flow data, preserving the historical hostname at the time of the flow. In contrast, the Source tab shows the current, potentially edited, hostname.

Fixed Issue 154386: The API allows the deletion of BGP filters after they have been assigned to a neighbor's inbound and outbound configuration in a profile.

The API allows the deletion of BGP filters after they have been assigned to a neighbor's inbound and outbound configuration in a profile.

Fixed Issue 154404: The user is unable to access the correct documentation using the links provided in the Orchestrator.

The documentation is no longer hosted on the resource referenced in the links in Orchestrator, so the built-in help panel has been removed.

Fixed Issue 154582: The user is unable to see the selected license.

Because licenses take too long to load, the page initializes before the loading is complete, resulting in the selected license not being displayed.

Fixed Issue 154709: Incorrect documentation for the getEdgeSDWANPeerPathMetrics method.

The API documentation previously indicated that path metrics were nested within a paths array. However, this was inaccurate; the API response directly returns the array of path metrics, without the enclosing paths wrapper.

Fixed Issue 154711: Some users may encounter an “insufficient free disk space” error while upgrading from 5.x to 6.x. As a result, the upgrade process fails.

Upgrading from 5.x to 6.x requires at least 30 GiB of free disk space. However, the upgrade script miscalculates available space by counting bytes in GB instead of GiB. Consequently, if a system has slightly under 30 GiB of free space, the process incorrectly proceeds and ultimately fails in later stages.

Fixed Issue 154712: A user might observe an inconsistency in the Edge interface configuration where the OSPF status is displayed as "enabled" in the interface table, but it appears as "disabled" in the interface modal.

OSPF is enabled in the profile and associated with the Edge interface. However, when OSPF is disabled in the profile, the Edge interface grid does not reflect this change accurately and still displays OSPF as enabled.

Fixed Issue 154913: User was not able to select images in new operator profile.

The configuration JSON file in the template lacks the window properties for the software image. Consequently, when a new operator profile is created, it inherits this incomplete configuration data. During validation checks, the Angular

UI encounters an error when it attempts to locate the missing window property. The CanJS UI functioned correctly because it did not have the same validation checks implemented in the older user interface.

Fixed Issue 155037: When there are more than 2048 (say 3000) rows in the events page, selecting "Objects Per Page" as 3000 in the footer pagination component will not load 3000 rows. It will only load 2048 rows but the footer will show like 3000 rows.

In the Events page, let's say there are 3000 rows. The "Objects Per Page" dropdown in the footer offers five options: 50, 100, 500, 1000, and 3000. Previously, selecting the "3000" option would display a message indicating that 3000 rows were loaded, but due to an API limit, only 2048 rows were actually displayed.

This issue has been fixed. The dropdown options now correctly reflect the API limit, with the options being 50, 100, 500, 1000, and 2000. If you need to view more than 2000 rows, you will need to navigate to the next page.

Fixed Issue 155171: Orchestrator currently allows invalid values for cTag and sTag to be configured in handoff configurations via the API. However, the UI enforces validation, requiring that cTag and sTag values fall within the range of 0 to 4096

cTag and sTag values in handoff configurations must be within the range of 0-4096. While the Orchestrator UI correctly enforces this validation, previously it was missing from the API. Configuring out-of-range values via the API caused parsing errors on SD-WAN gateways. This issue has been resolved by adding validation to the Orchestrator API.

Fixed Issue 155521: Applications are shown as an empty list while creating a new business policy rule.

The application list appears empty when creating a new business policy rule because the current version of PrimeNG's autocomplete dropdown does not support virtual scrolling.

Fixed Issue 155804: In the Remote Diagnostics page, invalid data previously seen in 6.1 on-wards, is fixed in 6.4.

The invalid data previously observed in the Edge's Drop Down Pop-over details under the Remote Diagnostics page in versions 6.1 and onward has been resolved in version 6.4.

Fixed Issue 156174: The issue with gateway handoff assignment is that when the local IP address of a handoff gateway is updated on the PG handoff page, the edges do not receive the update unless it is overridden at the edge-specific level.

When gateway handoff is assigned at the profile level and not overridden at the edge level, all edges associated with that profile fail to receive updates when the local IP of the handoff gateway is updated on the PG handoff page.

Fixed Issue 156183: Users are able to input loopback IP addresses that end with 255.

Users are now able to input loopback IP addresses that end with 255.

Fixed Issue 156729: After upgrading to the 6.2.0.2 build, customers may experience significantly slower performance when running select queries related to the enterprise events table. These queries may turn into long-running queries (LRQs), leading to increased MySQL resource usage and overall system degradation. The affected components include the MySQL database and the event migration task, which is directly impacted by this issue. This behavior is particularly noticeable when dealing with enterprise events and operator event tables.

The issue occurs when running select queries against the enterprise events table, post-upgrade to the 6.2.0.2 build. This behavior begins to consume significantly more time and resources than expected, turning into long-running queries (LRQs). This results in MySQL performance degradation, which can also negatively affect the event data migration task, as the same table is used during this process. In turn, this problem can also lead to further degradation of overall Orchestrator performance, especially in environments where enterprise events and operator event tables are heavily utilized. Customers may observe delays or failures in event data migration tasks, as well as slow database response times.

Fixed Issue 156801: Enterprise Superuser cannot access licensing page.

When an enterprise superuser tries to access the Orchestrator licensing service, the user can see the page but not the data. They see the error message stating 'Error during list loading: undefined.'

Fixed Issue 156977: Users may face failure creating automated Zscaler tunnels.

In some cases, users may notice that despite correct configuration, automated creation of Zscaler tunnels will still fail, and error messages on the UI may not fully reflect the underlying issue.

Fixed Issue 157031: The gateway list table does not make the full API call needed when users click expand on individual rows that are WSS-enabled gateways. This leads to data being wiped from the table (would not come back until user refreshes the table)

If the customer is on the gateway management page (gateway list table) and clicks 'expand' on a gateway row that is also a WSS-enabled gateway, the WSS-related statuses will clear and will not be repopulated unless the user refreshes the table.

Fixed Issue 157063: The getEnterpriseEvents, getOperatorEvents, and getProxyEvents APIs previously allowed using is or isNot operators with a list of values, which was inconsistent with other paginated APIs.

This behavior has been corrected to align with the existing approach. The correct way to filter with a list of values is to use the "in" and "notIn" operators. The backend now automatically converts "is" with a list input to in, and "isNot" with a list input to "notIn", ensuring consistent behavior across all APIs. Using "is" or "isNot" with a list will continue to work but is deprecated.

Fixed Issue 157077: The 'assign image' dropdown options may not be visible properly, making it difficult to check the available options.

The 'assign image' dropdown options may not be visible properly, making it difficult to check the available options. added required spaces in the modal for the dropdown menu.

Fixed Issue 157135: The Remote diagnostics page does not load, and the data spinner remains active indefinitely.

Response trimming has been added to the backend starting with release 6.2.0. Now, if data is null, an empty object is returned instead of an empty array.

Fixed Issue 157196: Customer may not be able to configure CSS Zscaler manual Network Service on the Orchestrator.

On the Orchestrator UI, The customer tries to configure Network Service, CSS, Zscaler manual. If the customer enters FQDN in the primary or secondary VPN Gateway then the user will get a validation error while saving the network service.

Fixed Issue 157340: When generating Flow Tabs CSV files, the Orchestrator can experience heavy resource consumption. The resource saturation led to an outage due to insufficient memory limits and overall resource exhaustion.

The CSV file generation process for Flow Tabs placed a large load on the system, causing excessive memory usage. While ClickHouse was already configured with CPU limits, there were no explicit memory constraints in place. This absence of a hard memory cap allowed the query to consume excessive resources, ultimately leading to an outage.

Fixed Issue 157375: Customers using the 'getEnterpriseEvents' API on Orchestrator version 6.1.0.0 intermittently receive empty responses. API sometimes returned no event data, even when events existed within the specified time range.

Customers using the 'getEnterpriseEvents' API on Orchestrator version 6.1.0.0 intermittently receive empty responses. Despite receiving a successful HTTP 200 OK status code, the API sometimes returned no event data, even when events existed within the specified time range. This issue primarily affected queries across broader time ranges and stemmed from the new events migration feature. Customers relying on the API for real-time monitoring or automated alerting were impacted, as missing events could delay responses to network issues or cause problems to remain

undetected. This fix also addresses several other identified bugs, including missing operators and query inefficiencies. Post-upgrade, the 'events.mysql.return.id' system property needs to be created and set to TRUE.

Fixed Issue 157604: Customers, partners, and operator users may be unable to see post- day 2 licenses.

Post-day 2 licenses are not present in the Edge Licensing list or the database. This prevents them from being assigned to customers or partners, and customers/partners are unable to assign these licenses to Edges.

Fixed Issue 157649: In static route settings, users are encountering an "N/A" value for the interface, whereas in the CanJS UI, users are able to see the interface value in a dropdown menu.

When the next hop IP in a static route matches the VLAN subnet mask IP, and the VLAN is assigned to an interface, the interface in the static route is marked as "Invalid". The UI reflects this as "N/A". However, due to a bug, even when the VLAN is not assigned to an interface, the UI for the static route still displays "N/A".

Fixed Issue 157687: Error thrown in API because of invalid parameters.

Gateway Id parameter is not considered for filtering in **getEnterpriseProxyGatewaysListPaginated**.

Fixed Issue 157796: Users cannot select a date in the Orchestrator user agreement popup since the calendar is not visible.

Users may face the date selection issue when adding or modifying a user license agreement.

Fixed Issue 157911: The removal of the id field from the getEnterpriseEvents API response caused disruptions to customers' data processing and other operations. Additionally, customers were unaware of new fields being added or removed from the getEnterpriseEvents API response.

The **getEnterpriseEvents** API response previously included an **id** field, which was removed in a recent update. This change broke existing data processing operations for customers who relied on the **id** field. While new fields were added to the API response, the documentation was not updated to reflect these changes, leaving customers unaware of the new fields and how to use them.

A solution is available for customers who require the **id** field. By setting the system property **events.mysql.return.id** to **true**, they can continue to receive the **id** field. However, this field is only returned for the first 30 days of event data. After this period, the response payload will no longer include the **id** field.

When an API call requests data for a two-month period of events, the response payload may include some records with the **id** field and some without.

Fixed Issue 157985: Radio settings are not working after upgrade.

Radio settings are not working after upgrade and it can be fixed via the patch file.

Fixed Issue 158030: Customers may notice Edges / Gateways going offline. No monitoring data being shown either. It may seem like the network is operating in a headless mode.

There is a certain corner case when it comes to processing discovery of a new client device event coming from an Edge. When that occurs, there is a database overload which causes the Orchestrator to stop responding to new incoming requests.

Fixed Issue 158031: CSS-related issues may be observed on the IDPS and Malicious IP pages.

Legend text block under the charts section is overlapped causing CSS related issues to be seen on the IDPS and Malicious IP pages.

Fixed Issue 158045: On the monitor page of NSD gateway, the redundant tunnel status may be shown as UNKNOWN, even if its actually connected when we have redundant dataCenterPublicIp different from its primary dataCenterPublicIp.

When redundancy is enabled for a VPN gateway with ACTIVE_ACTIVE tunnel mode, and its dataCenterPublicIp is different from it's primary dataCenterPublicIp, the redundant tunnels display an UNKNOWN tunnel status.

Fixed Issue 158108: Events Data Migration complete after upgrading to Orchestrator to 6.1 version. Notice the connections acquired by events migration jobs not getting released while disabling the job.

After upgrading Orchestrator to 6.1 version, historical events migration backend job (processMigrateJob) migrates events from MySQL to ClickHouse. Once historical events are successfully migrated, there is an issue in releasing the connection when it tries to disable the job. The connection leak can be a maximum of 120 connections. This will not have any impact on the Orchestrator services.

Fixed Issue 158166: In a High Availability (HA) environment, when an Edge fails over, the Orchestrator's user interface incorrectly displays the serial numbers of other Edges in the same enterprise instead of the serial number of its HA peer.

During an events migration, a new **getEnterpriseEventsList** API call was introduced. This API call mistakenly omitted the **edgeLogicalId** in its WHERE clause, resulting in data retrieval for all Edges within the enterprise, rather than just the specific edge in question. As a consequence, the Orchestrator UI selects the first Edge from this unfiltered query result, leading to the display of incorrect serial numbers in the System tab. This discrepancy can cause confusion for users who expect to see the serial number of the HA peer.

Fixed Issue 158538: Users may see the same NTICS license displayed for all enterprises.

License updates have not been implemented for individual enterprises, resulting in all enterprises sharing the same NTICS license key.

Fixed Issue 158648: After upgrade and reboot, Orchestrator is stuck on the GRUB menu.

In rare cases on Orchestrator, where a high I/O process (e.g., backups) is running in the background, an issue occurred that may cause the upgrades to fail.

Fixed Issue 158764: Customers may notice that exported metric files are not being cleaned up at the top of the hour as expected. This issue affects the backend file cleanup component responsible for removing these exported metrics.

When metric files are exported, a backend job is scheduled to delete them at the start of each hour. However, after a recent upgrade, a breaking API change was introduced that caused the cleanupExportFile module to malfunction. As a result, some exported metric files remain in the system longer than intended, which can lead to unnecessary disk usage.

Fixed Issue 158808: SubInterfaces are deleted based on subinterface ID.

SubInterfaces are deleted based on subinterface ID , should be done based on name and subinterface ID.

Fixed Issue 159250: When editing a business policy rule, the 'Service Class Selection' option is not disabled even when a valid value is chosen for the 'Application Type' in the match criteria.

When editing a business policy rule, if a user selects a valid value for the 'Application Type' in the match criteria, the 'Service Class' selection within the action class should be disabled. This functionality aligns with the tooltip description and works as expected when creating new rules.

Fixed Issue 159758: While LACP configuration on Edges with Marvell switches is not supported, the interfaces page does not block or warn against it.

While LACP configuration on Edges with Marvell switches is not supported, the interfaces page does not block or warn against it.

Fixed Issue 160180: When editing an NSD via the gateway in the Configure->Network Services section, if the user changes any fields and saves, the PSK is either removed or replaced with '********'**

If "Allow access to sensitive data" is not enabled for a customer's partner users, any changes made by a partner user to the network service from the UI will result in the PSK being saved as '**********'

If the user lacks the READ ENTERPRISE_KEYS permission, attempting to view the PSK will trigger a "decodeEnterpriseKey" error. This will set the PSK as empty, and any subsequent changes by the user will also result in an empty PSK.

Fixed Issue 160407: Wrong data may be seen in the monitoring screen when the time frame is changed.

Users may wrong data in the graph because the redundant data's are not properly rendered in the graph when both primary and redundant IP addresses are the same.

Fixed Issue 160926: The Edge remote diagnostic window's "Edge Overview" dropdown menu does not populate with the expected edge information.

The "Edge Overview" dropdown in the Edge Remote Diagnostic window is empty because the **getEdge** function is not being called with the necessary configuration and site information.

Fixed Issue 162064: Some Edge configuration changes may fail to apply silently.

A user may encounter a situation where settings do not apply after pushing the save button on the Edge configuration pages.

Known Issues

Open Issues in Release 6.4.0.

Issue 60896: BFD up/down events are not appearing on the Orchestrator's Events Monitoring page. Additionally, the Orchestrator's Routing Monitoring page does not reflect the current state of BFD sessions.

MGD periodically queries the FRR BFD daemon to fetch the peer status. Any state changes that occur within this 30-second interval are not notified on the Orchestrator monitoring pages. When BFD is removed from the EDGE configuration, MGD's periodic queries will not explicitly notify Orchestrator about the removal of the BFD session. MGD only sends the BFD sessions that are currently configured. If none are configured, no data is sent to Orchestrator. Since Orchestrator expects an explicit DOWN/Removal event from the Edge/gateway to update its Routing monitoring page, this page will remain outdated, displaying stale BFD sessions.

Workaround: Log in to the Edge's CLI and check the BFD session status.

Issue 148562: Azure Edge does not function properly when GE1 is used as the WAN link.

The kernel-to-interface mapping is incorrect for GE1, as it currently maps to GE3. The fix involves correctly mapping the interface to the WAN link.

Workaround: Use GE3 as WAN interface.

Issue 159758: LACP configuration on edges with Marvell switches is not supported, but the interfaces page does not block or warn against it.

LACP configuration on edges with Marvell switches is not supported, but the interfaces page does not block or warn against it.

Workaround: There is no workaround for this issue.

Issue 159793: A port is not detached from a LAG if the peer unsets the Aggregation bit in the LACP PDU.

When a peer attempts to detach a port from the LAG by unsetting the aggregation bit in the LACP PDU, the edge ignores this action and continues to use the port in the LAG. This behavior is intentional and aligns with the Linux kernel's implementation of LACP.

Workaround: There is no workaround for this issue.

Issue 160805: Network connectivity for the gateway fails, tunnels aren't formed and the gateway loses communication with the Orchestrator.

This issue can occur after upgrading the gateway to version 6.4. Upon reboot, the TAP device MAC address is incorrectly set during startup. This leads to the gateway being unable to form tunnels or communicate through the TAP interface.

Workaround: Restart Gateway's dataplane service.

Issue 161536: When an Edge is moved from HUB profile to SPOKE profile, the remote routes advertised by that edge may still remain in the current edges of the HUB profile, even after those are withdrawn by that Edge. Here HUB profile has more gateways configured and SPOKE profile is configured with only few out of those gateways.

When an edge is in a HUB profile, other members of the HUB profile receive routes from that edge via all the gateways. If the edge is moved from a HUB profile to a SPOKE profile, the current members of the HUB profile retain the remote routes received from the edge, even from gateways not part of the SPOKE profile.

If the edge subsequently withdraws the route, the gateways connected to the SPOKE profile will withdraw the route accordingly. However, gateways solely connected to the HUB profile will not withdraw the route as they are no longer connected to the edge. This occurs because the current members of the HUB profile still have remote routes from other gateways, preventing the removal of the specific route in question.

Workaround: There is no workaround for this issue.

Issue 162467: On an High Availability edge, LACP PDUs are sent with the same source MAC address for all member ports.

The issue is observed when LAG is enabled followed by HA configuration. On the active edge, LACP PDUs are sent on all slave ports using the first member port's original MAC address as the source MAC. While this behavior does not impact traffic or performance, it deviates from the standard.

Workaround: Restart the Active Edge.