Release Notes

VeloCloud SD-WAN 6.2

Version 6.2

Arista.com

Arista Networks

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

Chapter 1

Arista VeloCloud SD-WAN 6.2.0 Release Notes

This document contains the following sections

- Introduction
- What Is in The Release Notes
- Edge/Gateway Resolved Issues
- Orchestrator Resolved Issues
- Known Issues

Introduction

Arista VeloCloud SD-WAN 6.2.0 | **3rd June 2025**

- Arista VeloCloud SD-WAN™ Gateway Version **R6201-20250513-GA**
- Arista VeloCloud SD-WAN™ Edge Version **R6201-20250513-GA**
- Arista VeloCloud SD-WAN™ Orchestrator Version **R6207-20250327-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 6.2.0.

Important:

Release 6.2.0 contains all fixes found in the 6.1.0 Release Notes as follows:

- All Orchestrator fixes up to build **R6101-20241210-GA**.
- All Edge and Gateway builds fixes up build to **R6101-20241210-GA**.

6.2.0 is a Short-Term Support (STS) Release

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 6.2.0 is offered as an STS Release.

For additional information about Long-Term Support and Short-Term Support releases, see: *Arista VeloCloud SD-WAN/SASE Long-Term Support Release (96246)*.

Compatibility

Release 6.2.0 Orchestrators support all previous Arista VeloCloud SD-WAN Edge versions greater than or equal to Release 4.5.0.

The following SD-WAN interoperability combinations were explicitly tested:

Orchestrator	Gateway	Edge	
		Hub	Branch/Spoke
6.2.0	6.2.0	4.5.2	4.5.2
6.2.0	6.2.0	6.2.0	4.5.2
6.2.0	6.2.0	4.5.2	6.2.0
5.0.1	5.0.1	5.0.1	5.0.1
6.2.0	5.0.1	5.0.1	5.0.1
6.2.0	6.2.0	5.0.1	5.0.1
6.2.0	6.2.0	6.2.0	5.0.1
6.2.0	6.2.0	5.0.1	6.2.0
5.1.0	5.1.0	5.1.0	5.1.0
6.2.0	5.1.0	5.1.0	5.1.0
6.2.0	6.2.0	5.1.0	5.1.0
6.2.0	6.2.0	6.2.0	5.1.0
6.2.0	6.2.0	5.1.0	6.2.0
5.2.4	5.2.4	5.2.4	5.2.4
6.2.0	5.2.4	5.2.4	5.2.4
6.2.0	6.2.0	5.2.4	5.2.4
6.2.0	6.2.0	6.2.0	5.2.4
6.2.0	6.2.0	5.2.4	6.2.0
6.0.0	6.0.0	6.0.0	6.0.0
6.2.0	6.0.0	6.0.0	6.0.0
6.2.0	6.2.0	6.0.0	6.0.0
6.2.0	6.2.0	6.2.0	6.0.0
6.2.0	6.2.0	6.0.0	6.2.0
6.1.0	6.1.0	6.1.0	6.1.0
6.2.0	6.1.0	6.1.0	6.1.0
6.2.0	6.2.0	6.1.0	6.1.0
6.2.0	6.2.0	6.2.0	6.1.0
6.2.0	6.2.0	6.1.0	6.2.0

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.
- 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 6.2.0.

Orchestrator

Only Orchestrators using Release 5.2.0 or later can be directly upgraded to Release 6.2.0.

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 Arista 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 6.2.0 from Release 4.5.x or later.

New Hardware Platform

VeloCloud Edge 5100

Release 6.2.0 adds support for the VeloCloud Edge 5100. This model is capable of up to 100 Gbps of throughput and support for 16,000 tunnels. Support for up to 20,000 tunnels is expected in a future release.

The Edge 5100 is also equipped with a broad range of interfaces, including 2x 1-Gbps RJ45, 8x 10-Gbps SFP+, 4x 25-Gbps SFP28, and 2x 40-Gbps QSFP interfaces.

For more information, see the *VeloCloud SD-WAN Edge 4100/5100 Announcement*.

For a list of supported SFP modules for the Edge 5100, see *Arista VeloCloud SD-WAN Supported SFP Module List (312379)*.

Note:

The 2x40G ports have a hardware limitation, with the maximum bidirectional throughput across both ports being 96 Gbps combined. As a result, if the 40G ports are configured as the only WAN or only LAN ports, performance exceeding 96 Gbps will not be achievable. To achieve maximum throughput while utilizing the 40G ports, at least one additional port besides the two 40G ports is required. The 10G and 25G ports have no such limitations, and are capable of their full bidirectional line rate, and if only a single 40G port is used, that port can achieve full bidirectional line rate.

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)*.

Document Revision History

June 3rd, 2025. Eleventh Edition.

- Adds a new Edge/Gateway build **R6201-20250513-GA** to the Edge/Gateway Resolved Issues section.
- The Edge/Gateway build **R6201-20250513-GA** includes the fixes for the issues **#130674, #139855, #151812, #152868, #153475, #153640, #154005, #154079, #154765, #155517, #155822, #155881, #155974, #156072, #156892, #156966, #157156, #157650,#157665, #157667, #157775, #157852, #157898, #158032, #158096, #158172, #158348, #158456, #158500, #158691, #159092, #159246, #159337, #159532, #159674, #159845, #160542, #160553, #160677, #161113, #161692, #162024, #162085, #162376, #62396, #162452, #162571, #162476, #162716, 162736** and **#163436**.

March 17th, 2025. Tenth Edition,

- Added fixed Issue **#153444** and updated issue **#158348** in the Edge **R6200-20250305-GA-158348 Resolved Issues** section.

March 12th, 2025. Ninth Edition

- Added a new Edge build **R6200-20250305-GA-158348** to the **Edge/Gateway Resolved Issues** section. Build R6200-20250305-GA-158348 replaces the original GA Edge build **R6200-20250108-GA**, and is the new Edge default build for Release 6.2.0.

March 12th, 2025. Eighth Edition

- Added a new Orchestrator build **R6207-20250327-GA** to the **Orchestrator Resolved** section.
- The Orchestrator build **R6207-20250327-GA** includes the fixes for the issue **#139617**, **#153859, #153911**, **#154404**, **#154709**, **#155521**, **#157604**, **#157135**, **#157196, #157340**, **#157687**, **#158030**, **#158031**, **#158166**, **#158764** and **#160641.**

February 12th, 2025. Seventh Edition

- Added a new Orchestrator build **R6206-20250210-GA** to the **Orchestrator Resolved** section.
- The Orchestrator build **R6206-20250210-GA** includes the fixes for the issue **#157796** and **#158648.**

February 6th, 2025. Sixth Edition

- Added a new Orchestrator build **R6205-20250207-GA** to the **Orchestrator Resolved** section.
- The Orchestrator build **R6205-20250207-GA** includes the fixes for the issues **#136219, #153298, #156801, #157031, #157375** and **#158108.**

January 21st, 2025. Fifth Edition

- Added a new Orchestrator build **R6204-20250116-GA** to the **Orchestrator Resolved** section.
- The Orchestrator build **R6204-20250116-GA** includes the fixes for the issues **#153373**, **#157063** and **#157545**
- Added a new Orchestrator build **R6203-20250110-GA** to the **Orchestrator Resolved** section.

- The Orchestrator build **R6203-20250110-GA** includes the fixes for the issues **#139796** and **#156729**.

January 10th, 2025. Fourth Edition.

- Adds a new Edge/Gateway build **R6200-20250108-GA** to the Edge/Gateway Resolved Issues section. This is the new default Edge/Gateway build for Release 6.2.0.
- The Edge/Gateway build **R6200-20250108-GA** includes the fixes for the issues **#139989**, **#153360**, **#154134**, **#154240**, **#154743, #155144**, **#155461**, **#155881**, and **#156079** each of which is documented in this section.
- Added Open Issues **#156072, #156213,** and **#156892** to the Edge/Gateway Known Issues section.

December 17th, 2024. Third Edition

Added a new Orchestrator build **R6202-20241216-GA** to the **Orchestrator Resolved** section.

November 25th, 2024. Second Edition.

Added a new Orchestrator build **R6201-20241121** to the **Orchestrator Resolved** section.

November 15th, 2024. First Edition.

Edge/Gateway Resolved Issues

Edge/Gateway version R6201-20250513-GA

Edge/Gateway version R6201-20250513-GA was released on 06-03-2025 and resolves the following issues since Edge/Gateway version R6200-20250108-GA.

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

An Edge will not install any IPv6 remote routes when the only physical interface configured with IPv6 is not connected to the Edge while it is rebooting and then only later connected.

Fixed Issue 139855: Default route deleted after device setting configuration.

In a unique LAN-enabled HA Edge configuration, the default route via the routed interface (with WAN overlay disabled) and the LAN interface may be removed after applying device settings configuration.

Fixed Issue 151812: On the Monitor > Edge > Flows page of Orchestrator UI, a user may observe an incorrect hostname for an Edge's local interface IP address.

In certain scenarios, the Edge's Deep Packet Inspection (DPI) engine can extract and give the server's hostname from a traffic flow that can wrongly be mapped to the Edge's IP address instead of the server's IP address. This incorrect mapping gets stored in the DNS cache as well, and then gets propagated to the Orchestrator too, causing confusion. To handle this, Edge now extracts the hostname and the IP address from the DPI.

Fixed Issue 152868: With the stateful firewall disabled, locally routed traffic can sometimes match an unintended firewall rule due to the way the firewall lookup key is constructed.

With stateful firewall disabled, firewall policy re-lookup for routed traffic can occur in the context of either the original (to) or reply (fro) packet. Due to packet path improvements in version 5.4.0 and above, the firewall lookup key's five-tuple was always populated based on the context of the current packet instead of the flow. Consequently, during the re-lookup process, the flow matched a different firewall policy and was dropped.

Fixed Issue 153475: In a high-availability (HA) edge, the Loss of Signal (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 are not present in Zebra (BGP/OSPF) redistribute tables and hence advertised to (BGP/OSPF) peers.

During spoke movement between hubs/cluster, upgrade/reboot or during a service restart, the system may end up in a timing issue. The remote-spoke UP event is processed first with hub reachability when not set to true. This is followed by remote route addition triggered by the gateway and hub UP event. After the above sequence of events, the route will be present in FIB with reachability True, but would not be synced to BGP/OSPF.

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 that 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 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 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 than6.2 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 (example: 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 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.Avoid using Azure automation for configuring BGP over IPSEC.

Fixed Issue 157898: The link may appear deactivated in Orchestrator 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 158348: HA (High Availability) does not function correctly when a two-digit port number interface (e.g., SFP12) is used as the HA interface.

The active Edge does not send the correct HA interface information to the standby Edge when a two-digit port number is used. As a result, the standby Edge starts with the wrong HA interface, preventing communication between the active and standby Edges.

Fixed Issue 158456: HA Edge drops all the traffic received on LAN interfaces.

When LoS (Loss of Signal) is configured on the HA Edge, the LAN port is incorrectly blocked on the Active Edge. This results in all traffic received on the LAN interfaces being dropped.

Fixed Issue 158500: Edges stop forwarding LAN-side tagged traffic between LAN and WAN after upgrading to 5.2 or newer when the network configuration is managed by a 4.x Orchestrator.

When using a 4.x Orchestrator, administrators configure Edge network settings. Orchestrator uses untagged interfaces for LAN, meaning it does not specify VLANs in the configuration.

After upgrading both Edge and Orchestrator to version 5.2 or newer, the Edge software fails to generate the correct LAN network configuration due to the missing VLAN information. This incompatibility prevents the 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.

Fixed Issue 159092: When the active edge in an HA pair occasionally reports its peer as "unknown," this can disrupt 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 159246: When an Edge device is configured with a single physical interface (without VLANs or subinterfaces), it incorrectly accepts and processes VLAN-tagged packets, including IPv6 Neighbor Discovery (ND) packets, instead of dropping them.

Customers with an Edge device that has only one physical interface connected to a network sending VLAN-tagged packets (example: IPv6 ND packets) will encounter this issue. The Edge will process these packets as if they were untagged, leading to unintended behavior. For example, the Edge may respond to IPv6 Router Advertisement (RA) packets that are VLAN-tagged, causing it to autoconfigure IPv6 addresses on the physical interface. This can lead to unexpected routing behavior or other network issues. Other types of tagged traffic may also be processed instead of being dropped.

Fixed Issue 159337: TCP connections between e2e peers may be disrupted when one side is upgraded or loses context, especially if the connections use fixed port numbers.

When a customer upgrades their Edge on one side of an e2e TCP connection (e.g., the client side) and the TCP server behind another edge has also lost context of the connection, new TCP connections initiated from behind the upgraded customer can become stuck in an established state without transmitting any meaningful traffic.

Fixed Issue 159532: Manual DNS source interface configuration from the Orchestrator is not reflected on the Edge device.

Manual DNS source interface configuration from the Orchestrator is not reflected on the Edge device. Consequently, DNS packets originating from the Edge device carry an incorrect source IP address. If appropriate routes are not configured for this source IP, DNS reply packets will not reach the Edge. Users must select a specific DNS source interface in the orchestrator instead of relying on the "auto" setting.

Fixed Issue 159674: In certain scenarios, HA (High Availability) may not be formed when the standby device is replaced.

When an HA failover occurs and the new standby device is replaced, HA will not be formed, and the new standby device will not be activated.

Fixed Issue 159845: The severity levels of some INFORMATIONAL alerts are incorrectly reported to the Orchestrator.

Recent updates have resulted in incorrect impact score calculations for some INFO-level alerts. This issue only affects monitoring and has no impact on traffic.

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

This issue stems from a change in how ICMP traffic destined for the Edge itself is handled. These packets are now processed by the business policy engine, which may incorrectly route the ICMP reply through an unintended exit interface. Consequently, external ping requests are unable to reach the Edge's WAN IP address, potentially impacting troubleshooting and monitoring capabilities.

Fixed Issue 160553: When generating an ICMP error packet, the Edge device may leak a small amount of memory.

In highly stressed environments, when generating an ICMP error packet, the Edge device may leak a small amount of memory.

Fixed Issue 160677: An Edge Dataplane Service failure may occur when a large number of idle flows are being flushed.

In scenarios with a high number of connections/flows per second consisting of short-lived flows, the code could spend excessive time flushing idle flows, leading to an Edge Dataplane Service failure.

Fixed Issue 161113: With EFS (Enhanced Firewall Security) enabled on the Edge, subsequent traffic may be dropped if a legacy app-based firewall rule is added above the EFS catch-all rule with URL Filtering enabled.

When URL filtering is enabled, a minimum of 10 packets are subjected to DPI (Deep Packet Inspection) to extract the URL/domain for URL lookup. In the described customer scenario, the initial flow to MS Teams is classified by DPI, and the DPI cache is updated. When the SYN packet from a subsequent flow arrives, initial packet classification occurs due to the DPI cache. This matches the app-based legacy firewall policy but is still subjected to DPI for URL extraction. DPI re-classifies the traffic as APP_TCP, leading to a firewall re-lookup. As a result, the traffic matches the catch-all EFS firewall rule and is dropped because the previous policy was a legacy firewall policy and the URL is not available for lookup.

Fixed Issue 161692: The known IP-Port information for Zoom and Office 365 is not updated to the latest version in the appmap.

Zoom and Office 365 frequently update their firewall IP addresses. The current list in our appmap has not been updated for a significant period. The list has been refreshed using information from their respective support pages.

Fixed Issue 162024: The {{debug.py --enterprise_top}} command may fail and not display any valid output. This bug has no functional impact.

Users will encounter this bug when attempting to run the **{{debug.py --enterprise_top}}** command in scenarios where the displayed counter's value would have 12 digits or more.

Fixed Issue 162085: A gateway or Edge device may experience a core dump due to a SIGXCPU signal, indicating that its CPU usage has exceeded the defined limit. This can cause all VCMP tunnels to be taken down and re-established.

When a large number of idle flows are cleaned up simultaneously, the Edge/Gateway may consume more CPU time than permitted. This can result in the termination of the Edge/Gateway process, requiring its service to be restarted.

Fixed Issue 162376: On Edge devices with WiFi support, the factory WiFi SSID remains visible even after the device is activated with WiFi disabled.

When Wi-Fi radios are disabled, Edge devices stop generating Wi-Fi configurations. Because the Wi-Fi devices are not present in the configuration, the Edge fails to stop the radio upon activation.

Fixed Issue 162396: In the Edge Local UI's "Activation" screen, the "Activation Orchestrator" field may accept certain invalid strings, which can lead to command injection attacks on the Edge device.

The Edge Local UI's field validation logic for the "Activation Orchestrator" field, intended to allow only hostnames or IP addresses, is incorrect. It permits other characters that, when used to construct command invocations in the local UI's backend, can result in command injection attacks. These attacks can compromise the security of the Edge device. An explanation of the issue (not necessarily a root cause), and additional details (example: logs, Orchestrator events specific to the issue, error messages on the Orchestrator UI).

Fixed Issue 162452: When an IPSEC rekey occurs, traffic flowing through the tunnel will be interrupted for a few seconds.

During an IPSEC rekey, the existing outbound child SA is detached, and the new outbound child SA is then set to cached SA. During this brief period, when attempting to send a packet, the outbound SA may not be found, leading to an attempt to delete and recreate the existing tunnel.

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

Even though traffic matching firewall rules is sent with logging enabled, the logs may not appear on the Orchestrator. This could be due to the user enabling local firewall logging.

Fixed Issue 162476: NTICS authentication fails, potentially preventing the download of the latest Webroot SDK.

NTICS authentication fails during an upgrade from a version that lacks the Edge Device Secrets feature to an image that supports it.

Fixed Issue 162716: During customer upgrades from version 4.5.1 to 5.2.4.3, paths may not come up in rare scenarios, and connectivity to the orchestrator may also be lost.

In Edge releases starting from version 5.0 onwards, the **dscpTag** field in the WAN blob is mandatory. While Orchestrator release 3.4.2 introduced support for the **dscpTag** field, it was not utilized by Edge code at the time. Due to an incomplete implementation in Orchestrator versions 4.5.x and below, if API calls were used to intentionally or unintentionally remove the **dscpTag**, the orchestrator config database would not contain the **dscpTag** field. Consequently, the tag was never pushed or maintained in the Edge configuration. Therefore, when upgrading an Edge device from version 4.5.x to a later version, tunnel formation issues may occur over user-defined WAN links. If the impacted link is used for Orchestrator communication, connectivity to the Orchestrator will also be lost, and the Edge device will appear offline in the Orchestrator.

Fixed Issue 162736: Edges fire a misleading MGD_DEVICE_CONFIG_ERROR ("VLAN mismatch found...") event when a switched port is disabled or used as an HA interface.

When a switched interface is disabled or used as an HA interface, its VLAN information may not match the corresponding network VLAN information. This triggers a misleading event. Because network configurations are generated and applied correctly, no actual errors result from the event.

Fixed Issue 163436: A newly unpacked or freshly hard-reset Edge 4100 or 5100 device does not attempt to check for factory image updates or invoke zero-touch activation.

The zero-touch activation mechanism was unintentionally left disabled in the factory image version R6100-20241031-MR-GA.

Resolved in Edge Version R6200-20250305-GA-158348

Edge version R6200-20250305-GA-158348 was released on 03-24-2025 and is the updated GA build for Release 6.2.0. This build replaces the original GA build R6200-20250108-GA, which was released on 01-14-2025. This Edge build addresses the below critical issue since R6200-20250108-GA.

> **Important:**
>
> **Customers must only use the R6200-20250305-GA--158348 build and not use R6200-20250108-GA.**

Fixed Issue 153444: This security issue was identified as part of our internal Secure Software Development Life Cycle activities.

Our recommendation is to consume the latest version at the earliest.

Fixed Issue 158348: High Availability does not come up properly when two digit port number interface is used as HA interface (example: SFP12)

The active Edge does not send the correct HA interface information to the standby Edge when a two digit port number is used. As a result, the standby Edge comes up with the wrong HA interface resulting in no communication between active and standby Edge.

Resolved in Edge/Gateway Version R6200-20250108-GA

Edge/Gateway version R6200-20250108-GA was released on 01-14-2025 and resolves the following issues since Edge/Gateway version R6101-20241210-GA.

Fixed Issue 139989: On 610 and 5x0 Edges, clients connected to the copper ports cannot reach the Edge or other clients.

610 and 5x0 Edges use switches for managing the copper ports. Clients connected to the ports cannot reach the Edges or other clients because of the underlying switch configuration.

Fixed Issue 153360: The Gateway might crash when NVS via the Gateway (policy-based) is configured, and any configuration changes are made afterward.

When NVS is configured via the gateway (policy-based), a change in configuration is received where the DC configuration remains unchanged, but the key version is modified, which leads to a crash. In the case of a policy-based tunnel, the **gw_link_ip** and **dc_link_ip** values are not received. Consequently, attempting to access these values while comparing configurations leads to invalid memory access, resulting in a crash.

Fixed Issue 154134: Users might experience longer tunnel convergence time.

The problem is related to the QuickSec tunnel limit, specifically on devices where tunnel limits are low. The IKE descriptor and QuickSec tunnels are not in sync when tunnels are deleted. This can cause it to hit the QuickSec tunnel limit quicker, which will not allow the creation of new tunnels.

Fixed Issue 154240: A LAN client cannot connect to the Edge for some VLAN configurations on Edge 520/540.

On an Edge 520/540, if a VLAN is configured so that it only contains ports from among LAN1..LAN4, the underlying switch cannot forward packets out via the correct port. This leads to failure in reaching clients from the Edge.

Fixed Issue 154743: Route VLAN attribute is not getting updated on the peer when changing interface VLAN number on Edge.

When E2E is enabled via Gateway, remote routes and FIB contain identical copies of the routes. Whenever an overlay route is received, any updates should happen in the remote routes, since the same is used to update the FIB as well. Due to this software issue, remote routes are not updated when the VLAN attribute is changed.

Fixed Issue 155144: HA standby Edge does not become active immediately after LAN/WAN degradation and takes some additional time in rare scenarios.

HA failover time is increased to a maximum of 7 seconds after adaptive failover kicks in due to repeated A/A panics. After the 7-second failover time, when LAN/WAN degradation occurs, the active Edge restarts as expected. But if active Edge's HA interface is initialized before 7 seconds (current failover time) post the restart and starts sending broadcast packets to standby Edge, standby would assume that active Edge is up and would not become active.

Fixed Issue 155461: Edges may go into 'mgmt-only' mode if all interfaces are configured as switched.

Edge interfaces support two modes, namely switched and routed. The issue may show up if one configures all the interfaces in switched mode.

Fixed Issue 155881:Customers will see Edge freezing randomly when the DNS server is hosted behind Edge and a lot of DNS requests are sent to the DNS server.

If a customer has hosted a DNS server behind an Edge and if we have DNS queries to the DNS server via WAN interface the packets are subjected to the DPI engine even though the packet is classified.

Fixed Issue 156079: Occasional over capacity packet drops may be noticed even when the Edge is not under over capacity.

Under certain timing constraints, few packets (tens of packets per second) could get dropped. This in turn may cause a mild impact to the overall application performance.

Orchestrator Resolved Issues

Orchestrator version R6207-20250327-GA

Orchestrator version R6207-20250327-GA was released on 03-28-2025 and resolves the following issues since Orchestrator version R6206-20250210-GA.

Fixed Issue 139617: Neighbors not configured in the edge device settings page appear in the ESTABLISHED state within the Monitor > Routing > Edge BGP Neighbor State section.

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 is now resolved. When neighbors are deleted from the Edge configuration and the Edge removes the BGP neighbor from its configuration, they will now appear in the REMOVED state on the monitor page.

Fixed Issue 153859: After a firewall configuration update, the firewall rule information is not pushed to the firewall rule table.

Cloning a profile results in duplicate references being inserted, which prevents 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 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 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 155521: While creating a new business policy rule, the application selection list is empty, despite there being applications available on the network.

The current version of PrimeNG's autocomplete dropdown lacks virtual scrolling support, causing the application list to appear empty when creating a new business policy rule.

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 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 157687: additionalProperty "gatewayIds" exists in instance when not allowed

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

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 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 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 160641: BGP inbound/outbound filters inadvertently removed.

Tenants may experience loss of internet connectivity due to the removal of previously configured BGP inbound/outbound filters.

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.

Orchestrator version R6206-20250210-GA

Orchestrator version R6206-20250210-GA was released on 02-12-2025 and resolves the following issues since Orchestrator version R6205-20250207-GA.

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 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.

Orchestrator Version R6205-20250207-GA

Orchestrator version R6205-20250207-GA was released on 02-10-2025 and resolves the following issues since Orchestrator version R6204-20250116-GA.

Fixed Issue 136219: When denying a Read privilege, if the corresponding Create, Update, or Delete privileges are re-checked before the Deny Read is published, then the Service Permission is unable to remove the non-Read privilege.

The API for customizing privileges lists added denies and removed denies (re-enabling a privilege) as separate arguments. When a customer first denies an Update privilege, then re-enables the Update but removes the READ privilege, publishing the package leads to the role not having READ but having UPDATE, and cannot be corrected.

Fixed Issue 153298: When VLAN with ID 1 does not exist at the profile level, customers receive an error stating 'VLAN with ID 1 does not exist' when they try to save changes in existing profiles.

When the Orchestrator is running pre 5.2.0 release versions and customers have deleted VLAN with ID 1 (usually the corporate VLAN) from their profiles, they receive an error 'VLAN with ID 1 does not exist' when they try to make any changes to those profiles. This issue has been fixed, and customers should be able to make profile changes even if they do not have VLAN ID 1 in their profiles.

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 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 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 158108: Events Data Migration complete after upgrading to Orchestrator to 6.1 version. Notice the connections acquired by events migration job 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.

Orchestrator Version R6204-20250116-GA

Orchestrator version R6204-20250116-GA was released on 01-16-2025 and resolves the following issues since Orchestrator version R6203-20250110-GA.

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 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 157545: Sequential IDs were omitted from event query results to maintain consistency across MySQL and ClickHouse data sources.

A new system property *events.mysql.return.id* is introduced to control the inclusion of MySQL sequential IDs in event query results. When *events.mysql.return.id* is enabled (set to true), event queries within the past month will include both the sequential IDs and logical IDs.

Event queries exceeding one month will include logical IDs for all events, but sequential IDs will only be present for events within the last one month. Data older than one month is sourced from ClickHouse, which does not have sequential IDs.

Orchestrator Version R6203-20250110-GA

Orchestrator version R6203-20250110-GA was released on 01-10-2025 and resolves the following issues since Orchestrator version R6202-20241216-GA.

Fixed Issue 139796: The links list in the Monitor page interface column displays only the 3G/4G interface, even though 5G is supported.

We support 5G in our latest models so now the **Interface** column in the **Monitor** > **Edge** page displays 3G/4G/5G wireless interfaces.

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.

Orchestrator Version R6202-20241216-GA

Orchestrator version R6202-20241216-GA was released on 12-17-2024 and resolves the following issues since Orchestrator version R6201-20241121-GA.

Fixed Issue 94634: SSRF bypass in alert/sendEnterpriseAlertTestWebhook

Users may be able to bypass SSRF protections built into **alert/sendEnterpriseAlertTestWebhook** by using an untrusted intermediary.

Fixed Issue 149038: Using the back button after logout allows you to see the previous screen's data

If the user clicks the back button in the browser after logging out, they may be still able to view the data from the previously visited screen.

Fixed Issue 150366: Issue with reports showing drastically different measurements after an Orchestrator upgrade.

Discrepancy in the enterprise transport distribution report may occur when customers try to generate reports for Edges having a total number of links greater than 2048.

Fixed Issue 154850: Cannot download application map from Orchestrator

Orchestrator may crash when the Edge sends the application map download request to an Orchestrator.

Orchestrator Version R6201-20241121-GA

Orchestrator version R6201-20241121-GA was released on 11-25-2024 and resolves the following issues since Orchestrator version R6200-20241113-GA.

Fixed Issue 143982: Enhancement to support Symantec WSS for partner gateway.

The enhancement supports the Symantec Web Security Service (WSS) for partner Gateway operators.

Fixed Issue 150366: Issue with reports showing drastically different measurements after an Orchestrator upgrade

There are discrepancies in reports in the enterprise transport distribution report after the Orchestrator upgrade. The discrepancy may occur when customers try to generate reports for more than 2048 Edges at a single time.

Orchestrator Version R6200-20241113-GA

Orchestrator version R6200-20241113-GA was released on 11-15-2024 and resolves the following issues since Orchestrator version R6100-20241105-GA.

Orchestrator version R6200-20241113-GA also enables support for the upcoming VeloCloud Edge 5100.

> **Note:**
>
> **All fixes found in Orchestrator version R6100-20241105-GA are also included with R6200-20241113-GA.**

Fixed Issue 153850: A customer subscribed to SD-Access may observe that when they are logged in as an Enterprise Administrator on the Orchestrator that SD-Access does not load unless an SD-WAN license is also enabled for that enterprise.

SD-Access is designed for use as a standalone application that does not require a customer to also have an SD-WAN license. This issue only affects Customer Enterprise level users and Operator users can load SD-Access.

Fixed Issue 153957: For a customer using the Enhanced Firewall Service, a user may observe that they cannot generate a report as there is no option to do so.

When using the Enhanced Firewall reporting service wizard, the security reporting options are missing from the selection options due to missing reporting service privileges.

Known Issues

Open Issues in Release 6.2.0.

Edge/Gateway Known Issues

Issue 156072: In certain low BW scenarios, the QoS weights as defined in the Orchestrator may not be respected by the Edge or Gateway.

When a load balancing Business Policy is defined utilizing multiple WAN links of limited capacity (e.g., 10Mbps each), a single TCP flow hits this business policy, while competing with other TCP flows using other business policies defined using different 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, while higher priority classes may receive more than their weighted fair-share.

Workaround: If the application using the single TCP flow can be configured to use more than one concurrent flow, the issue may be mitigated.

The issue may also be resolved if other applications are using the same Class of Service and pushing traffic through the Edge and/or Gateway along with single TCP flow. Other workarounds include increasing the capacity of the WAN links and/or change the Business Policy's link steering or Network Service.

Issue 156892:Configuration is not in sync on standby Edge or post failover, Edge status shows offline although data plane is up. A request to obtain an Orchestrator diagnostic bundle for the HA pair or other similar standby tasks taking an extended amount of time could cause this behavior.

A stuck application thread is detected and exited by the watchdog process. The thread is restarted but exits and does not come back up.

Workaround: Restart mgd service on the Edge exhibiting the issue.

Issue 14655:

Plugging or unplugging an SFP adapter may cause the device to stop responding on the Edge 540, Edge 840, and Edge 1000 and require a physical reboot.

Workaround: The Edge must be physically rebooted. This may be done either on the Orchestrator using **Remote Actions > Reboot Edge**, or by power-cycling the Edge.

Issue 156213: Route-dump failing for an Edge from an Orchestrator diagnostic page.

At a highly scaled Edge having around 20k tunnels, control plane threads such as path_fsm and ike_workers compete for the 4 available cores in Edge 5100 platform. This in turn might prevent the completion execution of the route-dump task from being scheduled onto the CPU and thus causing the failure.

Workaround: Do per-prefix lookup from Orchestrator or use edge-cli to dump the max allowed routes at once.

Issue 25742:

Underlay accounted traffic is capped at a maximum of the capacity towards the Arista SD-WAN Gateway, even if that is less than the capacity of a private WAN link which is not connected to the Gateway.

Issue 32960:

Interface “Autonegotiation” and “Speed” status might be displayed incorrectly on the Local Web UI for activated Arista SD-WAN Edges.

Workaround: Refer to the Orchestrator UI under **Remote Diagnostics > Interface Status**.

Issue 32981:

Hard-coding speed and duplex on a DPDK-configured port may require a Arista SD-WAN Edge reboot for the configurations to take effect as it requires turning DPDK off.

Workaround: There is no workaround for this issue.

Issue 52955: DHCP decline is not sent from Edge and DHCP rebinding is not restarted after DAD failure in Stateful DHCP.

If a DHCPv6 server allocates an address which is detected as duplicate by the kernel during a DAD check, then the DHCPv6 client does not send a decline. This will lead to traffic dropping as the interface address will be marked as DAD check failed and will not be used. This will not lead to any traffic looping in the network but traffic blackholing will be seen.

Workaround: There is no workaround for this issue.

Issue 68057: DHCPv6 release packet is not sent from the Arista SD-WAN Edge on the changing of a WAN interface address mode from DHCP stateful to static IPv6 address and the lease remains active till reaching its valid time.

The DHCPv6 client possesses a lease which it does not release when the configuration change is done. The lease remains valid till its lifetime expires in the DHCPv6 server and is deleted.

Workaround: There is no way of remediating this issue as the lease would remain active till valid lifetime.

Issue 82184: On a Arista SD-WAN Edge which is running Edge Release 5.0.0, when a traceroute or traceroute6 is run to the Edge's br-network IPv4/IPv6 address, the traceroute will not properly terminate when a UDP probe used.

Traceroute or traceroute6 to the Edge's br-network IPv4/IPv6 address will not work properly when Default Mode (in other words, UDP probe) is used.

Workaround: Use -I option in traceroute and traceroute6 to use ICMP probe and then traceroute to br-network IPv4/IPv6 address will work as expected.

Issue 85402: For a customer enterprise using BGP with Partner Gateways configured, a user may observe that some BGP neighborships are down and this causes customer traffic issues.

If a customer has maximum-prefix configured on a router which has BGP peering with the Edge and Gateway, the BGP session may be dropped by the router.

For example, if the router has BGP configured to only receive max 'n' number of prefixes, but the Edge and Gateway have more than 'n' number of prefixes to be advertised in the absence of any filters. Now if the BGP filter configuration is changed on the Orchestrator, even if the total number of prefixes allowed in the outbound direction is less than 'n', the issue will be encountered where more than 'n' prefixes are sent to the peer before any filters are applied. This causes the router to tear down the session.

Workaround: If BGP goes down due to this issue (Maximum Number of Prefixes Reached), flap BGP on the peer using CLI (For FRR/Cisco, "neighbor x shut" followed by "no neighbor x shut"), and the BGP will produce only the desired number of prefixes advertised to the peer.

Issue 110561: Dynamic tunnels may not come up between the same set of Arista SD-WAN Edges with bidirectional traffic when traffic stops and then restarts.

Issue is observed in a test environment where there are 6000 dynamic tunnels with high bidirectional traffic being sent between the Edges. Even in lower scale testing at 1000 dynamic tunnels, not all the tunnels come up.

Workaround: There is no workaround for this issue.

Issue 117876: In a customer site using a High Availability topology, if a user activates or deactivates the Enhanced Firewall Services, a Arista SD-WAN HA Edge may experience multiple restarts.

When the **Enhanced Firewall Service** is activated or deactivated, only the Active Edge's Device Settings configuration is synchronized immediately with the Standby Edge, with the remainder of the configuration synchronization is only in response to a Standby Edge heartbeat. When the Active Edge is restarted to apply the latest configuration prior to receiving a heartbeat from the Standby Edge it will result in a configuration mismatch between the two HA Edges, and they will undergo multiple restarts to complete the configuration synchronization.

Workaround: The only workaround is to turn on or off Enhanced Firewall Services during a maintenance window for HA Edges.

Issue 125274: When a customer runs an SNMP walk, the loopback interface of the Arista SD-WAN Edge is not discovered.

The Edge loopback interface is a unique interface category that the Edge does not classify as either WAN or LAN. As a result, the loopback interface is not in the 'allow list' of interfaces to process for the *snmp-request*.

Workaround: There is no workaround for this issue. The loopback interface status would have to be individually monitored through the Orchestrator UI.

Issue 132492: For a customer who has one or more Non SD-WAN Destinations via Edge configured and uses BGP, when no traffic is passing through the IPsec tunnels, the customer may observe that the tunnels are torn down and BGP routes flap.

This issue is only seen when there is no traffic on the path from the NSD via Edge to the peer. The issue stems from a premature IKE Phase 1 rekey on the Edge and the peer sends multiple Dead Peer Detection (DPD) packets with an old cookie that the Edge does not acknowledge. This results in the peer side deleting both Phase 1 and Phase 2 IKE and tearing down the tunnels which also causes BGP flaps.

Workaround: A user should configure the NSD with IKEv2. Alternatively, a user could set up a LAN side client to send a continuous ping to the NSD via Edge peer to prevent the scenario from arising.

Issue 135827: For a customer site deployed with a High Availability topology, the customer may observe multiple HA failovers due to the site experiencing an active-active (split brain) condition.

A user would observe a HA_SPLIT_BRAIN_DETECTED on the Events page. The HA Standby Edge may miss the HA heartbeat from the Active Edge and promotes itself to an Active state. When the HA heartbeat is resumed it will report the HA_SPLIT_BRAIN_DETECTED event to the Orchestrator and the Standby Edge will restart to tie-break the HA split brain. This issue is observed where the enterprise uses Edge Network Intelligence with Analytics turned on and runs aggressive route timers.

Workaround: To mitigate the risk of an active-active panic, configure the HA failover time to a higher value.

Issue 135938: For an Edge configured with a routed LAN interface and a secondary IP address configured on the routed interface, traffic sent to the secondary IP address connected interface is NAT'd with the parent interface's IP address.

Whether the user checks the NAT Direct Traffic option or not has no impact, as the traffic is sent out based on the NAT direct configuration of the parent interface.

Workaround: There is no workaround beyond ensuring that the secondary IP address is configured with the expectation that the NAT Direct Traffic option is only applied at the parent level.

Issue 138023: For a customer using a Partner Gateway (PG), a PG-BGP session does not come up when the BGP local IP address and PG Handoff local IP address are both from the same subnet.

SD-WAN treats this scenario as two interfaces on a router from the same subnet, which is not supported and can lead to ARP related issues.

Workaround: Change the configuration to avoid the above scenario.

Issue 140194: For a customer enterprise site deployed with an Enhanced High Availability topology where a PPPoE link is used on the Standby Edge interface, an SNMPWalk does not work properly for this site.

SNMPWalk output is incomplete for interface related MIBs when there is a PPPoE interface on the Standby Edge in Enhanced HA.

Workaround: None.

Issue 140785: An SD-WAN Edge configured with IPv4 and IPv6 loopback interfaces and their advertise flags enabled may experience a Dataplane Service Failure and restart to recover.

Packet fragmentation from packets 1350 bytes and greater is triggering an exception with the Edge service if configured as above and causing a service failure.

Workaround: There is no workaround for this issue.

Issue 141008: On the Diagnostics > Remote Diagnostics page of the Orchestrator UI, Traceroute using an IP/Hostname destination does not for IPv6 addresses.

The result from an IPv6 **Traceroute** shows the destination alone, and intermediate hops do not display. IPv4 addresses work as expected.

Workaround: There is no workaround for this issue.

Issue 143450: On a customer enterprise site configured with an Enhanced High Availability topology where Dynamic Branch to Branch VPN is also enabled, client users may observe extended traffic loss after an HA failover.

The issue can be encountered if the Enhanced HA site also has a Business Policy rule configured which includes mandatory link steering. Combined with Dynamic Branch to Branch, this combination can result in a prolonged period of traffic disruption after an HA failover.

Workaround: The customer can either remove the Business Policy rule with mandatory link steering entirely or modify that rule to remove the mandatory link steering option.

Issue 145393: A customer enterprise site deployed with an Edge model 620, 640, or 680 where firewall logging is configured may observe that the Edge no longer stores new firewall or standard debugging logs.

When this issue is encountered, a 6x0 Edge's eMMC storage experiences an excessive level of wear due to the high volume of writes and rewrites that can be triggered by enabling logging for firewall rules which are matched by a large number of new connections per second in a high traffic customer environment. This issue results in the Edge defensively moving the file partition which hosts logging to a read-only state, and no additional logs are stored.

Workaround: If a customer has an Edge 620, 640, or 640 Edge model and is also using firewall logging, they should avoid enabling logging for firewall rules which can potentially match a large number of new connections in a high traffic environment. The excessive logging frequency that would result can cause undue wear on the Edge's storage and trigger this issue.

Issue 153475: In a HA Edge, LoS on Standby Edge will show down when unique LAN or WAN MAC is enabled

If LoS is enabled along with a unique LAN or WAN MAC address, on the standby Edge the interface LoS state is set to 0. This will impact the HA failover scenarios based on interface count mismatch.

Workaround: Manually update the /velocloud/ha/origMACs file to add the MAC address of the missing interface and restart the Edge service.

Orchestrator Known Issues

Issue 41691:

A user cannot change the 'Number of addresses' field although the DHCP pool is not exhausted on the **Configure > Edge > Device** page.

Issue 51722: On the Arista SASE Orchestrator, the time range selector is no greater than two weeks for any statistic in the Monitor > Edge tabs.

The time range selector does not show options greater than "Past 2 Weeks" in **Monitor > Edge** tabs even if the retention period for a set of statistics is much longer than 2 weeks. For example, flow and link statistics are retained for 365 days by default (which is configurable), while path statistics are retained only for 2 weeks by default (also configurable). This issue is making all monitor tabs conform to the lowest retained type of statistic versus allowing a user to select a time period that is consistent with the retention period for that statistic.

Workaround: A user may use the "Custom" option in the time range selector to see data for more than 2 weeks.

Issue 60522: On the Arista SD-WAN Orchestrator UI, the user observes a large number of error messages when they try to remove a segment.

The issue can be observed when adding a segment to a profile and then associating the segment with multiple Arista SD-WAN Edges. When the user attempts to remove the added segment from the profile, they will see a large number of error messages.

Workaround: There is no workaround for this issue.

Issue 125663: A user can configure the same IPv4/IPv6 IP address for multiple Edge interfaces.

The Arista SASE Orchestrator is allowing a user to configure the same IP on multiple WAN, LAN, or Sub Interfaces.

Workaround: There is no workaround for this issue beyond ensuring you are not configuring the same IP Address for multiple interfaces.

Issue 130115: For a Arista SASE Orchestrator configured with a Disaster Recover (DR) topology, the Active and Standby Orchestrator's DR pages show different details under the History section.

The user sees additional rows for a failing DR state on the Active Orchestrator compared to the Standby Rows under the History section and these rows are not sorted by time on the Active Orchestrator.

Workaround: No workaround for this issue.

Issue 142456: On the Monitor > Firewall Logs page of the Orchestrator UI, a user may not be able to sort data on this page.

A user should be able to click on the column header to sort between the various data included in a firewall log, but cannot.

Workaround: There is no workaround for this issue.

Issue 142672: On the Edges > Monitor > Sources page of the Orchestrator UI, a user cannot change the Host Name for an entry.

The user can click the **Change Hostname** option, but on the dialog box, if they enter a different host name and try to Save Changes, the Orchestrator throws an error, and the changes are not saved.

Workaround: There is no workaround for this issue.