Release Notes

VeloCloud SD-WAN

Version 5.2.3

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

Chapter 1

Arista VeloCloud SD-WAN 5.2.3 Release Notes

This document contains the following sections

Introduction

Arista SASE 5.2.3 | 16th June 2025

- Arista SD-WAN™ Gateway Version **R5234-20240826-GA**
- Arista SD-WAN™ Edge Version **R5234-20250527-GA-162396**
- Arista SASE™ Orchestrator Version **R5239-20250319-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 5.2.0, as well as those customers impacted by the issues listed below which have been resolved since Release 5.2.2.

Important: Release 5.2.3 contains all Edge, Gateway, and Orchestrator fixes that are listed in the 5.2.2 Release Notes, including all UI Builds.

5.2.3 is a Long-Term Support (LTS) Release

Arista SD-WAN/SASE is introducing a Long-Term Support (LTS) policy to enhance the operational efficiency of our partners and customers during the implementation of new software. As part of this new policy, SASE/SD-WAN Release 5.2.3 is offered as the first LTS Release.

For additional information about our Long-Term Support program see: *Arista SD-WAN/SASE Long-Term Support Release (96246)*.

Compatibility

Release 5.2.3 Orchestrators, Gateways, and Hub Edges support all previous Arista SD-WAN Edge versions greater than or equal to Release 4.2.0.

The following SD-WAN interoperability combinations were explicitly tested:

Orchestrator	Gateway	Edge	
		Hub	Branch/Spoke
5.2.3	4.5.2	4.2.2	4.2.2
5.2.3	5.2.3	4.2.2	4.2.2
5.2.3	5.2.3	5.2.3	4.2.2
5.2.3	5.2.0	4.2.2	5.2.3
5.2.3	4.3.2	4.3.2	4.3.2
5.2.3	5.2.3	4.3.2	4.3.2
5.2.3	5.2.3	5.2.3	4.3.2
5.2.3	5.2.3	4.3.2	5.2.3
5.2.3	4.5.2	4.5.2	4.5.2
5.2.3	5.2.3	4.5.2	4.5.2
5.2.3	5.2.3	5.2.3	4.5.2
5.2.3	5.2.3	4.5.2	5.2.3
5.2.3	5.0.1	5.0.1	5.0.1
5.2.3	5.2.3	5.0.1	5.0.1
5.2.3	5.2.3	5.2.3	5.0.1
5.2.3	5.2.3	5.0.1	5.2.3
5.2.3	5.1.0	5.1.0	5.1.0
5.2.3	5.2.3	5.1.0	5.1.0
5.2.3	5.2.3	5.2.3	5.1.0
5.2.3	5.2.3	5.1.0	5.2.3
5.2.3	5.1.0	5.1.0	5.2.3
5.2.3	5.2.3	5.2.3	5.2.3
5.3.0	5.2.3	4.5.2	4.5.2
5.3.0	5.2.3	5.2.3	4.5.2
5.3.0	5.2.3	4.5.2	5.2.3
5.4.0	5.2.3	4.5.2	4.5.2
5.4.0	5.2.3	5.2.3	4.5.2
5.4.0	5.2.3	4.5.2	5.2.3

Important: Arista VeloCloud 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 SD-WAN Release 4.x (88319)*.

Note: Arista VeloCloud SD-WAN Release 5.x is approaching the of 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 EOGS until March, 2027.

Upgrade Paths for Orchestrator, Gateway, and Edge

The following lists the paths for customers wishing to upgrade their Orchestrator, Gateway, or Edge from an older release to Release 5.2.3.

Orchestrator

Orchestrators using Release 4.5.0 or later can be upgraded to Release 5.2.3.

Gateway

Upgrading a Gateway using Release 4.5.0 or later to Release 5.2.3 is fully supported for all Gateway types.

Important: When deploying a new Gateway using 5.2.3 the VMware ESXi instance must be **at least version 6.7, Update 3 up to version 7.0**. Using an earlier ESXi instance will result in the Gateway's Dataplane Service failing when trying to run Release 5.2.3 or later.

Important: Prior to upgrading a Gateway to 5.2.3, the ESXi instance must be upgraded to **at least version 6.7, Update 3 up to version 7.0**. Using an earlier ESXi instance will result in the Gateway's Dataplane Service failing when trying to run Release 5.2.3 or later.

Edge

An Edge can be upgraded directly to Release 5.2.3 from any Release 4.x or later.

Important Notes

Security Advisory 2024-0008

- *VMSA-2024-0008* documents the response to **CVE-2024-22247**, which details a missing authentication and protection mechanism vulnerability which impacts all supported SD-WAN Edges.
- More information on mitigating this vulnerability is found in the KB article: *Response to CVE-2024-22247 (VMSA-2024-0008) (97391)*.

LAN-Side NAT Behavioral Change

When a LAN-side NAT is configured for many-to-one translations using Port Address Translation (PAT), traffic initiated from the opposite direction can allow unexpected access to fixed addresses based on the outside mask and original IP address. This new behavior applies to Destination NAT (DNAT), Source NAT (SNAT), and Source and Destination NAT (S+D NAT) rules.

For example, a SNAT rule with an inside network of 192.168.1.0/24 and an outside address of 10.1.1.100/32 permits outside-to-inside translation to 192.168.1.100.

To address this new behavior, SD-WAN now blocks traffic when a connection is initiated in the reverse PAT direction.

To restore the original behavior, a user needs to configure two rules of the same type as the original rule (SNAT, DNAT, S+D NAT) in a particular order. For example, using the earlier SNAT scenario a user needs to configure the following:

1. SNAT rule with an inside network of 192.168.1.100/32 and an outside address of 10.1.1.100/32
2. SNAT rule with an inside network of 192.168.1.0/24 and an outside address of 10.1.1.100/32

If the original rule is a DNAT or S+D NAT, then the user would need two DNAT or S+D NAT rules with the same structure and order.

In Release 4.5.0 and forward, a user can determine if flows are dropped for this type of traffic in the *dispcnt* logs of a diagnostic bundle by searching for the counter: `lan_side_nat_reverse_pat_drop`.

Hub or Cluster Interconnect Remains Early Access

Hub or Cluster Interconnect was introduced in Release 5.1.0 with the caveat:

"Enabling Hub or Cluster Interconnect introduces a fundamental change to the Arista SD-WAN routing protocol where it allows packets to traverse more than one hop in the network. While this change has been tested in representative topologies, it is not possible to test for all routing scenarios that may be encountered when making such a change of allowing distant routes to be distributed. As a result, Arista is releasing this feature as **early access** and will be closely monitoring deployments where it is enabled for unexpected routing behavior."

Note: This limitation is applied to the Orchestrator and Gateway software only, and does not apply to the Edge version. An Edge using 5.2.x software connected to an Orchestrator and Gateway using Release 5.4.0 or later software would use the Hub or Cluster Interconnect feature as a GA feature without limitations.

Limitation with BGP over IPsec on Edge and Gateway, and Azure Virtual WAN Automation

The BGP over IPsec on Edge and Gateway feature is not compatible with Azure Virtual WAN Automation from Edge or Gateway. Only static routes are supported when automating connectivity from an Edge or Gateway to an Azure vWAN.

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 an 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 (87208)*.

Available Languages

The Arista SASE Orchestrator using version 5.2.3 is localized into the following languages: Czech, English, European Portuguese, French, German, Greek, Italian, Spanish, Japanese, Korean, Simplified Chinese, and Traditional Chinese.

Document Revision History

June 16th, 2025. Thirty-Second Edition.

- Added Fixed Issue **#162396** in the Edge **R5234-20250527-GA-162396 Resolved Issues** section.

April 15th, 2025. Thirty-First Edition.

- Added Fixed Issue **#139476** to the Edge/Gateway Resolved Issues section for Edge/Gateway build **R5230-20240313-GA**.

March 26th, 2025. Thirtieth Edition.

- Added a new Orchestrator rollup build **R5239-20250319-GA** to the **Orchestrator Resolved Issues** section. This is the eighth Orchestrator rollup build and is the new default Orchestrator GA build for Release 5.2.3.
- Orchestrator build **R5239-20250319-GA** includes the fix for issue **#157604** and **#160641** each of which is documented in this section.

February 13th, 2025. Twenty-Ninth Edition.

- Added a new Orchestrator rollup build **R5238-20250206-GA** to the **Orchestrator Resolved Issues** section. This is the eighth Orchestrator rollup build and is the new default Orchestrator GA build for Release 5.2.3.
- Orchestrator build **R5238-20250206-GA** includes the fix for issue **#136219** and **#153298** each of which is documented in this section.

January 2nd, 2025. Twenty-Eight Edition.

- Added a new Orchestrator rollup build **R5237-20241220-GA** to the **Orchestrator Resolved Issues** section. This is the seventh Orchestrator rollup build and is the new default Orchestrator GA build for Release 5.2.3.
- Orchestrator build **R5237-20241220-GA** includes the fix for issue **#108833**, **#130943**, **#151844**, and **#152892** each of which is documented in this section.

December 11th, 2024. Twenty-Seventh Edition.

- Added Resolved Issues # **108833, #130943**, **#151844** and **#152892** to the Orchestrator Resolved Issues section.

November 21st, 2024. Twenty-Sixth Edition.

- Added Open Issue **#151806** to the Edge/Gateway Known Issues section.

November 15th, 2024. Twenty-Fifth Edition.

- Added a new note to the Compatibility section regarding 5.x software and upcoming end of support dates for some versions.
- Added Open Issue **#151654** to the Edge/Gateway Known Issues section.

October 31st, 2024. Twenty-Fourth Edition.

- Added Fixed Issue **#140382** to the Edge/Gateway Resolved Issues section for Edge/Gateway build **R5230-20240313-GA**. This ticket should have been included in the March 17th, 2024 edition of these notes.
- Added Open Issue **#134125** and Open Issue **#149862** to the Edge/Gateway Known Issues section. These issues are fixed in Release 5.2.4.

September 6th, 2024. Twenty-Third Edition.

- Added a new Orchestrator rollup build **R5236-20240829-GA** to the **Orchestrator Resolved Issues** section. This is the sixth Orchestrator rollup build and is the new default Orchestrator GA build for Release 5.2.3.
- Orchestrator build **R5236-20240829-GA** includes the fix for issue **#139581**, **#143506**, **#146441**, **#148179**, **#148274**, and **#149028**, each of which is documented in this section.
- Orchestrator build 5.2.3.6 adds support for provisioning and configuring Edge models **710-5G**, **720**, and **740** on the UI.

September 3rd, 2024. Twenty-Second Edition.

- Added Open Issue **#148274** to the Orchestrator Known Issues section.

August 29th, 2024. Twenty-First Edition.

- Added a new Edge/Gateway rollup build **R5234-20240826-GA** to the **Edge/Gateway Resolved** section. This is the fourth Edge/Gateway rollup build and is the new default Edge/Gateway GA build for Release 5.2.3.
- Edge/Gateway build **R5234-20240826-GA** includes the fixes for issues **#136673**, **#143666**, **#145475**, **#147015**, **#147931**, and **#149116**, and, each of which is documented in this section.

July 25th, 2024. Twentieth Edition.

- Added a new Edge/Gateway rollup build **R5233-20240719-GA** to the Edge/Gateway Resolved section. This is the third Edge/Gateway rollup build and is the new default Edge/Gateway GA build for Release 5.2.3.
- Edge/Gateway build **R5233-20240719-GA** includes the fixes for issues **#101935**, **#110791**, **#130704**, **#134108**, **#135937**, **#142531**, **#143374**, **#143549**, **#143602**, **#144387**, and **#144653**, each of which is documented in this section.
- The Edge build remediates CVE-2024-6387, a critical vulnerability in OpenSSH. For more information on this OpenSSH vulnerability, consult the article Broadcom Software Defined Edge Division response to CVE-2024-6387.

Note: CVE-2024-6387 could potentially impact a 5.2.3 Edge, but does not impact a 5.2.3 Gateway. This is why there is a remediation for the Edge only.

July 19th, 2024. Nineteenth Edition.

- Added a new Orchestrator rollup build **R5235-20240715-GA** to the **Orchestrator Resolved Issues** section. This is the fifth Orchestrator rollup build and is the new default Orchestrator GA build for Release 5.2.3.
- Orchestrator build **R5235-20240715-GA** includes the fix for issue **#146946**, which is documented in this section.

July 2nd, 2024. Eighteenth Edition.

- Added a new Orchestrator rollup build **R5234-20240629-GA** to the **Orchestrator Resolved Issues** section. This is the fourth Orchestrator rollup build and is the new default Orchestrator GA build for Release 5.2.3.
- Orchestrator build **R5234-20240629-GA** includes the fixes for issues **#127870**, **#144891**, **#145134**, **#145810**, and **#147155**, each of which is documented in this section.

June 28th, 2024. Seventeenth Edition.

- Revised Open Issue **#138464** in the Edge/Gateway Known Issues section to read that the Active Edge, not the Standby Edge, is impacted by this issue and the result may be an unscheduled HA failover to recover the Active Edge's memory.
- Added Fixed Issue **#139428** to the Edge/Gateway Resolved Issues section for Edge/Gateway build **R5232-20240516-GA**. This ticket should have been included in the March 20, 2024 edition.

June 20th, 2024. Sixteenth Edition.

- Added Open Issue **#145393** to the Edge/Gateway Known Issues section.

June 6th, 2024. Fifteenth Edition.

- Moved **Issue #134108** from the Edge/Gateway fixed section for Edge build **R5232-20240516-GA** back to the **Edge/Gateway Known Issues** section as the fix for this issue is incomplete on Edge Version 5.2.3.2.

June 3rd, 2024. Fourteenth Edition.

- Added a new row to the interoperability combinations table located in the **Compatibility** section. This added row confirms that a 5.2.3 Orchestrator + 5.2.3 Gateway + 5.2.3 Edge (Hub and Spoke) are tested and confirmed to work with one another.

May 24th, 2024. Thirteenth Edition.

- Added a new Orchestrator rollup build **R5233-20240522-GA** to the Orchestrator Resolved Issues section. This is the third Orchestrator rollup build and is the new default Orchestrator GA build for Release 5.2.3.
- Orchestrator build **R5233-20240522-GA** includes the fix for issue **#145783**, which is documented in this section.

- Added Open Issues **#137083** and **#141273** to the Edge/Gateway Known Issues section..

May 21st, 2024. Twelfth Edition.

- Added a new Orchestrator rollup build **R5232-20240520-GA** to the **Orchestrator Resolved Issues** section. This is the second Orchestrator rollup build and is the new default Orchestrator GA build for Release 5.2.3.
- Orchestrator build **R5232-20240520-GA** includes the fixes for issues **#99891** and **#116666**, each of which is documented in this section.

Note: Fixed Issue **#99891** was erroneously listed in **R5231-20240510-GA** as fixed. The fix for **#99891** is included beginning with the 5.2.3.2 Orchestrator version.

- Added Open Issue **#145720** to the Orchestrator Known Issues section.

May 20th, 2024. Eleventh Edition.

- Added a new Edge/Gateway rollup build **R5232-20240516-GA** to the **Edge/Gateway Resolved** section. This is the second Edge/Gateway rollup build and is the new default Edge/Gateway GA build for Release 5.2.3.
- Edge/Gateway build **R5232-20240516-GA** includes the fixes for issues **#86786**, **#118704**, **#122267**, **#122717**, **#125275**, **#133987**, **#134108**, **#138101**, **#138131**, **#139776**, **# 141043**, **#141336**, **#141449**, **#141621**, **#141834**, **#142001**, **#142366**, **#142529**, **#142599**, and **#143485**, each of which is documented in this section.

May 13th, 2024. Tenth Edition.

- Added a new Orchestrator rollup build **R5231-20240510-GA** to the **Orchestrator Resolved Issues** section. This is the first Orchestrator rollup build and is the new default Orchestrator GA build for Release 5.2.3.
- Orchestrator build **R5231-20240510-GA** includes the fixes for issues **#99891**, **#121993**, **#138635**, **#143577**, and **#143724**, each of which is documented in this section.
- Added Open Issue **#143828** to the Edge/Gateway Known Issues section.

April 24th, 2024. Ninth Edition.

- Added a new section: **5.2.3 is a Long-Term Support (LTS) Release**. This section highlights the fact that Release 5.2.3 is the initial release to be encompassed by the organization's recently instituted *Long-Term Support* policy. While the section is new, Release 5.2.3 has carried LTS status since the first edition of these notes.

April 19th, 2024. Eight Edition.

- Added Open Issue **#143450** to the Edge/Gateway Known Issues section.

April 12th, 2024. Seventh Edition.

- Added Open Issues **#86786**, **#141336**, and **#142366** to the Edge/Gateway Known Issues section.

- Corrected the wording for Open Issue **#118704** to change the workaround from a CLI action to an action on the Orchestrator UI to restart the Edge service to remediate the issue.

April 5th, 2024. Sixth Edition.

- Made wording revisions to Edge/Gateway Known Issues **#135827** and **#141621** to clarify when these issues may be encountered by a site using High Availability.

April 2nd, 2024. Fifth Edition.

- Added an Important Note regarding **CVE-2024-22247**, which details a missing authentication and protection mechanism vulnerability that impacts an SD-WAN Edge. The response to this vulnerability is documented in *VMSA-2024-0008*. More information on mitigating this vulnerability is found in the KB article: *Response to CVE-2024-22247 (VMSA-2024-0008) (97391)*.

March 29, 2024. Fourth Edition.

- Added a new Gateway rollup build **R5231-20240321-GA** to the **Edge/Gateway Resolved** section. This is the first Gateway rollup build and is the new default Gateway GA build for Release 5.2.3.
- Gateway build **R5231-20240321-GA** adds support for Gateway deployments using Google Cloud Platform (GCP). This rollup build adds no new fixed issues.

March 27, 2024. Third Edition.

- In the **Compatibility** table for Release 5.2.3, added three new compatibility/interoperability rows that reflect additional testing to confirm compatibility between 5.4.0 and 5.2.3.
- Corrected the wording for Open Issue **#136336** to make it clear the triggering scenario involves the use of the **Common Criteria Firewall**, not the Standard or Enhanced Firewall.
- Added Open Issue **#118704** to the Edge/Gateway Known Issues section.
- Added Fixed Issue **#138303** to the Edge/Gateway Resolved Issues section. This issue should have been included in the initial edition.

March 19, 2024. Second Edition.

- Added Fixed Issue **#133199** and **#134911** to the Orchestrator Resolved Issues section for the GA build. These tickets should have been included in the initial edition.

March 17, 2024. First Edition.

New Features and Enhancements

Export Firewall Logging

Adds support for firewall logs, enabling the on-premises Orchestrator to store them using the existing data export functionality. This change integrates firewall logs into the existing data export feature.

Edge/Gateway Resolved Issues

Resolved in Edge Version R5234-20250527-GA-162396

Edge version R5234-20250527-GA-162396 was released on 06-16-2025 and is the updated GA build for Release 5.2.3. This build replaces the previous GA build R5234-20240826-GA. This Edge build addresses the below critical issue since R5234-20240826-GA.

> **Important: Customers must only use the R5234-20250527-GA-162396 build and not use R5234-20240826-GA.**

Fixed Issue 162396: 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.

Resolved in Edge/Gateway Version R5234-20240826-GA

Edge/Gateway build R5234-20240826-GA was released on 08-29-2024 and is the 4th Edge/Gateway rollup build for Release 5.2.3.

This Edge/Gateway rollup build addresses the below critical issues since the 3rd rollup build, R5233-20240719-GA.

Fixed Issue 136673: When debugging a Virtual SD-WAN Edge deployed on KVM, a user may observe that the DPDK interface reads as "-1".

In scenarios where the port default speed value has to be picked up by the Virtio-PMD, it's taking the value INT_MAX. But this value is translated by the application to -1 instead of the expected value of 10 Gpbs. This issue can be specifically observed when checking the Edge under dpdk_ports_dump or in the matching diagnostic bundle log.

Fixed Issue 143666: An Edge running 5.2.3.x software may fail to connect to the default NTP servers if there are no private NTP servers configured.

The Segment NAT entry is not being added to the routing table and this causes the Edge to not connect to the NTP servers.

On a 5.2.3.x Edge without a fix for this issue, configuring a private NTP server adds the Segment NAT entry so that the Edge can connect to even the default NTP server.

Fixed Issue 145475: SD-WAN Edge models 640 and 680 may not properly negotiate speed and duplex values for connected SFP modules, resulting in poor performance for traffic using SFP ports.

When encountering the issue, a user would observe that both LAN and WAN are negotiating to 0 and Half-Duplex instead of the correct speed and duplex values (for example, 10G and Full-Duplex). When troubleshooting the Edge, a user can confirm this issue in *dpdk_ports_dump* (either on the Edge or in the logs) where the value would show as 0 for an SFP port with an SFP module plugged in.

The issue is caused by a DPDK process not updating the correct speed and duplex value for the Edge's SFP ports once an SFP model is connected, and instead leaving it at the initial default value of 0.

Fixed Issue 147015: For a customer enterprise where Stateful Firewall is enabled with both rate limiting and a denylist, client users may experience traffic latency and disruptions if a randomized source attack occurs (also known as network flooding).

The Stateful Firewall rate-limiting table size is not limited and in the case of a random source attack, it is tracking millions of Source IP addresses for rate-limiting. This consumes large amounts of Edge memory due to the constant lookups and results in a slower cleanup of stale entries which will increase overall traffic latency. If a sufficient amount of Edge memory is consumed, the Edge service process may defensively restart to recover memory, which will disrupt all user traffic for up to 15 seconds.

Fixed Issue 147931: For a customer site deployed with a High Availability topology where BGP Graceful Restart is configured, client users may observe frequent HA TCP flaps which can disrupt their traffic.

The TCP connection between HA Edges frequently flap due to an invalid route synchronization object being parsed on the Standby Edge, potentially resulting in BGP/BFD flaps and down tunnels to a Hub site. This is due to an incorrect method of decoding the route synchronization object on the Standby Edge which results in the TCP flaps, and is observed when BGP Graceful Restart is enabled.

Fixed Issue 149116: For a customer enterprise where Stateful Firewall is enabled and one or more rules are configured to allow traffic from one VLAN to another VLAN, users my observe dropped packets for traffic matching that rule.

With this issue, the Edge drops inter VLAN traffic packets with drop reason *edged_flow_rate_limit_drop*. Troubleshooting reveals that the Edge is periodically resetting and refilling tokens for rate limiting every 250 ms. The issue is caused when the Stateful Firewall is enabled but the Flood Protection configuration is not over-ridden, and the Edge does not receive the configuration. So it is treating this rule as rate-limit all traffic at 0% instead of the default value of 25% and not refilling the tokens.

Resolved in Edge/Gateway Version R5233-20240719-GA

Edge/Gateway build R5233-20240719-GA was released on 07-24-2024 and is the 3rd Edge/Gateway rollup build for Release 5.2.3.

Important: The Edge build includes a remediation for CVE-2024-6387, a critical vulnerability in OpenSSH. For more information on this OpenSSH vulnerability, please consult the article Broadcom Software Defined Edge Division response to CVE-2024-6387.

This Edge/Gateway rollup build also addresses the below critical issues since the 2nd rollup build, R5232-20240516-GA.

Fixed Issue 101935: A Arista SD-WAN Edge may be accessible via SSH during bootup even though the configuration denies access.

When the Edge is rebooting, it can be accessed via SSH for a time window of 10-15 seconds. The SSH is blocked only after this time, as per the configuration.

Note: This issue was listed as resolved in Release 5.2.2. However, the issue is only fully resolved with this 5.2.3 Edge build.

Fixed Issue 110791: For a customer enterprise deployed using BGP with the default split-horizon rule, under rare conditions users may observe traffic loss due to routes being torn down and reforming due to a BGP process failure.

This issue can occur under high stress conditions where there are high levels of traffic, link flaps and the resulting BGP session flaps and route churn. With split-horizon enabled (which is enabled by default), if a BGP sub-group is being cleaned up while an *explicit-withdraw* entry is present, it leads to a stale BGP adjacency entry. Stale adjacency can occur during any churn in BGP routes or BGP session cleanup which can occur during high stress situations noted earlier. Accessing this stale BGP adjacency entry leads to the failure of the Edge's BGP process.

Fixed Issue 130704: Operator users may observe that a Gateway has an elevated statistics memory usage due to a leak.

While deleting a SASE (Geneve - RAS/CWS and MTGRE) *netif*, only the *netif* was freed, but the associated *netif* counter memory was not freed up.

The issue is caused by a missing *vc_netif_destroy* call while deleting the SASE *netifs* that resulted in the associated statistics memory to leak. Added this API in *vc_geneve_driver_destroy and vc_mtgre_driver_destroy*.

Fixed Issue 134108: On Edge model 520, 540 and 610 (all variants), traffic between switched ports belonging to the same VLAN may be dropped.

On these Edge platforms, if there are both tagged (Trunk) and untagged (Access) ports defined for the same VLAN, traffic between them can be dropped. In addition, on a 520 or 540, if a VLAN spans ports between the "left" (LAN1 - LAN4) and "right" (LAN5 - LAN8) banks of ports, then traffic between those ports may be dropped.

On an affected Edge model without a fix for this issue, the workaround is to ensure, for a given VLAN, that the ports that carry that VLAN are either all Access or all Trunk. In the case of the 520 and 540 models, make sure that they are all in the same bank of ports.

Fixed Issue 134332: For an Arista SD-WAN Edge that is using a Zscaler type Cloud Security Service (CSS) which uses GRE tunnels that has turned on L7 Health Check, in some instances the customer may observe CSS tunnels going down and traffic dropping that is being steered to a CSS.

This issue is encountered when the business policy corresponding to the L7 Health Check flow is modified and the probes are redirected to the internet (versus the CSS). The fix ensures the L7 Health Check probe's Business Policy is always set properly when the flow is created newly and also when the flow version is updated.

Fixed Issue 135937: For a customer enterprise configured with a Hub-Spoke topology where internet backhaul is configured, and a Hub Edge is configured a local default route, LAN side users of an Edge that is a spoke to that Hub Edge may experience traffic dropping for flows matching the backhaul rule.

A Hub Edge with a local default route drops the backhaul return packets from the Orchestrator with reason: cloud_to_edge_drop. Other Internet bound traffic is not affected. The issue is caused by the source route in the route key being set as a *cloud route* instead of the expected *any* type route. The fix for this issue ensures that the source route is not overwritten in these conditions.

Fixed Issue 142531: For a customer enterprise using a Hub/Spoke topology deployed in a multicast environment, the multicast receiver stops receiving traffic after 210 seconds.

After 210 seconds, the Edge sends a prune message on the multicast that results in traffic loss. The multicast routes remain present and after 20-60 seconds, the multicast stream resumes working. The issue occurs on the Edge during the RPT to SPT switchover, if it is unable to send periodic (S,G) joins to the PIM upstream neighbor. This results in the upstream router sending a PIM prune towards the RP after the 3 min 30 seconds timer expiration, resulting in traffic loss.

Fixed Issue 143374: For partners and customers who deploy Partner Gateways where two or more customer enterprises are connected to it, BGP or BFD handoff configurations are not applied to the Gateway.

The issue is encountered when more than one enterprise is configured without a c-tag or s-tag. Later, if the c-tag and s-tag are configured for one of the customers, the update which deletes the old entry where c-tag and s-tag = 0 and inserts the new c-tag and s-tag of the enterprise handoff configuration creates a stale vlan_vrf entry which triggers the issue.

For a Gateway without a fix for this issue, the Partner administrator should always configure the c-tag and s-tag from the beginning and thus avoid an update event.

Fixed Issue 143549: Edges with interfaces configured for PPPoE do not renegotiate those links after they have been brought down and then connectivity is restored.

Edge version 5.2.2 have a defect where *lcp_echo_fail* and *lcp_echo_interval* are not set in the newer version of the PPPoE process, this results in the Edge failing to rebuild tunnels to the Gateway after the link goes down and is then later restored and capable of passing traffic.

On an Edge without a fix for the issue, a user would need to physically remove the RJ45 cable and then reconnect it to trigger tunnel rebuilds on a PPPoE link.

Fixed Issue 143602: For Edges in the 6x0 (610, 620, 640, 680) and the 7x0 (710-W) model lines, the published Flows Per Second values for these Edges are not reached when using 5.2.3.2 and earlier releases.

The **Flows Per Seconds** values for Edge models using Release 5.2.x can be found in the 5.2 version of the **SD-WAN Administration Guide > SD-WAN Edge Performance and Scale Data > Test Results**. The issue is the result of these Edge models not having connections per second (CPS) thresholds properly set which results in substandard flows per second performance.

Fixed Issue 144387: An Edge running 5.2.3.x software does not honor the type of service (ToS) value when pinging a loopback interface.

The issue is caused by the Edge always setting the IP ToS value to 0 in echo replies destined to the Edge's own IP address (as is the case with a loopback interface) irrespective of the ToS value of the incoming echo request.

Fixed Issue 144653: For a customer enterprise deployed with a Hub Cluster topology, when rebalancing cluster members with dual BGP membership to the same peer while split-horizon is enabled may result in stale BGP routes.

Whenever Spoke Edges are rebalanced to a different Hub cluster with dual neighborship to the same peer with split horizon enabled (which is done by default), the previous Hub cluster does not withdraw the BGP routes. This results in stale routes on the peer.

This is not specific to clustering and can happen with any Edge having dual BGP neighborship with the same peer and while withdrawing the advertised route. Clustering is simply noted because a rebalance is common and usually results in the withdrawal of routes.

On an Edge without a fix for this issue, restarting the cluster member, or triggering a flap of the BGP neighborship on the node which is unable to withdraw the route will clear the issue for that instance.

Fixed Issue 145564: For a customer site deployed with a standard High Availability topology, a user may observe that an attempt to manually trigger an HA failover through the Orchestrator does not succeed.

The Standby Edge does not accept promotion to Active either through **Diagnostics > Remote Actions > Force HA Failover**, or by restarting the Edge Service on the Active Edge which should force the Standby Edge to take over the Active role.

Resolved in Edge/Gateway Version R5232-20240516-GA

Edge/Gateway build R5232-20240516-GA was released on 05-20-2024 and is the 2nd Edge/Gateway rollup build for Release 5.2.3.

This Edge/Gateway rollup build addresses the below critical issues since GA build, R5230-20240313-GA.

Fixed Issue 86786: When there is an outbound BGP filter with a 0.0.0.0/0 EXACT MATCH rule associated to a default originate (implicitly attached to default originate when associated with an outbound filter for a neighbor), the default route may not be advertised to the neighbor.

The issue is the result of a design limitation in the Edge's routing process, and a Customer would need to avoid this outbound BGP filter configuration without a fix for the issue.

Fixed Issue 118704: A user may observe abnormally high latency values for paths measured between SD-WAN Edges and SD-WAN Gateways even though actual Edge-to-Gateway packet latency is much lower.

A race condition has been identified with clock synchronization resulting in latency values measured incorrectly. This issue is cosmetic and there is no performance impact to customer traffic but it does negatively impact a customer's ability to properly monitor Edge links and paths.

And an Edge without a fix for this issue, clock synchronization can be reset by restarting the Edge Service. This can be done using the Orchestrator UI by navigating to the **Diagnostics > Remote Actions** page, and then checking the affected Edge and selecting the **Restart Service** option.

Fixed Issue 122267: For a customer enterprise site configured with a High Availability topology where the Loss of Signal (LOS) is configured, the newly demoted Standby Edge does not detect the restoration of a link to up after an HA failover.

As part of the Loss of Signal feature, if a LAN link goes down, a failover is triggered, and the Standby is promoted to Active. The issue is that if the previously downed LAN link is now restored to an up state on

the new Standby Edge (previously the Active Edge), the Standby Edge does not detect this state. Should this LAN link go down again, this would not trigger another failover as would be expected with LOS. Only triggering a manual HA failover fully corrects the LAN link's status for both HA Edges.

The issue is caused by an aspect of HA design where all LAN ports are blocked on a Standby Edge which prevents any detection of a restored LAN link and thus the LAN link count is never updated until a new failover promotes the Standby to Active.

Fixed Issue 122717: For a customer enterprise site deployed with an Enhanced High Availability topology where Edge model 540's are used, if a hard reset is performed on the Standby Edge, the WAN link on the Standby Edge may go down.

The issue is the result of a spurious netlink down message on the Active Edge.

Fixed Issue 125275: A Gateway may experience a Dataplane Service failure and restart to recover if the traffic on the Gateway has any amount of jitter.

The issue is the result of a circular deadlock between the jitter buffer processing and the flow deletion process. The fix moves the lock sequence to avoid the circular lock dependency.

Fixed Issue 133987: For a customer enterprise site deployed with an Enhanced High Availability topology where the Edge models are LTE models (510-LTE or 610-LTE), if the Active Edge has a live CELL1 interface (using a SIM card) and the Standby Edge does not, the customer may receive the error message "error reading data for test" when running the Remote Diagnostic "Interface Status" on the Orchestrator UI.

The customer will face this issue when they simulate an HA failover by either disconnecting (physical connection down) or disabling an interface on the Active Edge and then try to run **Remote Diagnostics > Interface Status** from the newly promoted Active Edge.

Fixed Issue 138101: For a customer enterprise that is deployed with a Hub/Spoke topology, the customer may observe that multiple Spoke Edges cannot form tunnels with the Hub Edge for long periods of time.

Specifically, the customer can observe some Spoke-to-Hub tunnels remaining in an INIT state for about ~10-15 minutes if the Hub Edge is a lower end model (like an Edge 620 or 640). In this scenario, when the Hub Edge restarts or there is any action which requires bringing down all tunnels (for example, certificate renewal), it is possible that tunnel establishment will take ~10-15 minutes because these lower-end Edge models are close to their tunnel capacity.

Fixed Issue 138131: When a Non SD-WAN Destination (NSD) BGP neighbor is configured as passive, the SD-WAN Gateway does not form the BGP session.

This issue is due to a defect in the Gateway that prevents NSD BGP sessions from initiating TCP connections.

Fixed Issue 139428: For a customer enterprise where the Edges are deployed with a 4.5.x build and has Standard Firewall rules configured, but disables the Stateful Firewall, when the Edges are upgraded to a 5.x build traffic to some VLANs may be dropped.

On Edge builds of 5.x and later, direction-based rules (for example, one that allows traffic to a specific VLAN) are supported only when Stateful Firewall is enabled. So when the Edge is upgraded, traffic that matches

direction-based rules that previously worked on a 4.5.x Edge would be dropped after the upgrade to a 5.x build.

On an enterprise without a fix for this issue, the user would need to enable the Stateful Firewall to ensure that rules with a directional parameter work properly.

Fixed Issue 139776: An Edge may experience a Dataplane Service failure, generate a core, and restart to recover.

```
The core file logs would indicate the Edge service exited with signal SIGSEGV, Segmentation fault.
The fix addresses how ref counting in a object is handled, which can trigger this issue.
```

Fixed Issue 141043: Traffic for a Business Policy Rule configured to rate limit both inbound and outbound traffic at 0% may cause a packet queue build and impact other customer traffic.

When a business policy with a 0% rate limit is used to blackhole traffic matching that rule, the traffic is blackholed as expected, but a packet queue buildup also occurs. This can result in netscheduler queue drops even after the rule is deleted or modified.

On an Edge without a fix for this issue, the customer needs to avoid using Business Policy Rules to drop traffic and use Firewall Rules instead.

Fixed Issue 141336: For a customer enterprise site deployed with a High Availability topology, if the customer configures the HA interface to a non-default interface (in other words, some interface other than GE1), when they enable HA, they may observe the Orchestrator UI reporting that the peer state is unknown.

When HA is initially enabled with the default GE1 interface, a virtual MAC address is programmed for all interfaces except the GE1 HA Interface. However, if HA is disabled and then re-enabled with a non-default, non-GE1 HA Interface, the new HA interface continues to be programmed with a virtual MAC address. As a result, the Active Edge drops the peer heartbeat since the source MAC address is matching to the received interface MAC and sets the Standby Edge peer state as "Unknown".

In this scenario, prior to re-enabling HA with a non-default HA Interface (GE1), a Technical Support Engineer needs to delete the `/velocloud/ha/virtualmacs` file from the Active Edge. Contact Support if this step is needed.

Fixed Issue 141449: For a customer enterprise site deployed with a High Availability topology, the HA Edges may experience an Active-Active (Split Brain) state and the Standby Edge needs to reboot to resolve the condition.

The Active-Active state can occur due to a priority inversion in the Edge's service if the HA interface is down and the heartbeat packets need to be sent on a WAN link.

Fixed Issue 141621: On a customer enterprise site deployed with a High Availability topology, in rare instances the Standby Edge may restart multiple times in response to an Active/Active (split-brain) state.

When a LAN or WAN interface goes down on the Active Edge, an HA failover is triggered and the Standby Edge immediately takes the Active role based on a higher LAN/WAN interface count.

Under an extremely rare timing condition, this action could be taken before the Active Edge can restart to demote itself to a Standby role. As a result the newly active Standby Edge reports an Active/Active Panic which triggers multiple Edge service restarts to clear the issue. A site deployed with an Enhanced HA topology would experience customer traffic disruption for those flows using the WAN links connected to the Standby Edge.

There is no workaround beyond ensuring the Active Edge has a high number of interfaces than the Standby Edge so that the issue could be avoided if an interface on the Active Edge went down.

Fixed Issue 141834: The Edge model 710-W local user interface may not function properly.

There are two states where the 710-W local UI can not function properly:

- When the Edge is an unactivated state.
- When the Edge 710-W is activated with 2.4 GHz Wi-Fi radio disabled on the Orchestrator.

Without a fix, a user would need to turn on the 2.4 GHz Wi-Fi on the Orchestrator in the profile and not override the radio settings on the Edge.

Fixed Issue 142001: For a customer site deployed with a High Availability topology where the customer enterprise uses OSPFv3, the users may observe that traffic is dropping after an HA failover.

The OSPF sweep timer on the Standby Edge does not handle OSPFv3 instances and results in the sweep timer for OSPFv3 to stop running for that HA Edge. After an HA failover, with the OSPFv3 sweep timer not running on the newly promoted Active Edge, no new routes learned through OSPFv3 are synchronized to the Overlay Flow Control (OFC).

Fixed Issue 142366: For a customer enterprise site connected to Partner Gateways where one or more static routes are configured, client users working behind an SD-WAN Edge may observe intermittent traffic loss if a static route via the Primary Partner Gateway is unreachable.

When the same static route is reachable via two or more Partner Gateways, if the route via the Partner Gateway in the Primary role is unreachable, traffic from an Edge can experience intermittent traffic loss. This issue is the result of the Edge API failing to properly check for reachability on a route lookup which causes the Edge to continue to use the Primary Partner Gateway even though reachability is false.

The issue can be temporarily remediated by the Partner shutting down the Primary Partner Gateway until the static route becomes reachable again. Shutting down the Primary Partner Gateway prevents the Edge from including it in route reachability lookups and ensures traffic matching that static route uses a secondary Partner Gateway. However this can be disruptive for all customers using this Partner Gateway as their Primary Gateway and should be done in a maintenance window by the Partner if possible.

Fixed Issue 142529: When a customer switches a Cloud Security Service (CSS) GRE tunnel configuration from manual to automatic for an Edge, the Edge may experience three successive Dataplane Service failures and stop passing traffic entirely until restarted.

The Edge will still be reachable on the management side through the Orchestrator UI and the service can be restarted through **Remote Actions**.When a CSS tunnel with GRE tunneling protocol is switched from manual to automatic, this causes a change in the tunneling protocol from GRE to IPsec. However the IPsec-related parameters are not configured, resulting in the IKE identification of NULL, and this triggers an exception in the Edge service and the resulting triple failure.

On an Edge without a fix for this issue, if the customer wishes to switch from manual to automatic, the workaround is to delete the CSS configuration completely and create a new one in a maintenance window.

Fixed Issue 142599: For a customer enterprise site where LAN-side NAT is configured on the Edge, the Edge may stop passing new traffic and trigger a reboot to recover.

When LAN side NAT is configured, flows may gradually build up (due to stale flows) due to a flow container object leak in one of the LAN side NAT lookup failure cases. The flow container memory is not released back after its life cycle, and this leads to stale flow build up in the system which would prevent any new flows from being created and leads to the device triggering a reboot to recover the issue.

Fixed Issue 143485: Customers using SNMP monitoring may observe that they intermittently lose SNMP monitoring for hours at a time.

The any of the below commands are run, traceback can be encountered:

- `/opt/vc/bin/snmpdebug.py --ha verp`
- `/opt/vc/bin/snmpdebug.py --path`
- `/opt/vc/bin/snmpdebug.py -v --arp`

The traceback triggers an error that can be seen in the affected Edge's snmpagent logs and temporarily stops SNMP monitoring.

Gateway Version R5231-20240321-GA

Gateway version R5231-20240321-GA was released on 03-28-2024.

This Gateway build adds support for deployments using Google Cloud Platform (GCP).

Note: This Gateway build adds no new fixed issues over Gateway build R5230-20240313-GA.

Resolved in Edge/Gateway Version R5230-20240313-GA

Edge/Gateway version R5230-20240313-GA was released on 03-16-2024 and resolves the following issues since Edge build R5222-20240223-GA, and Gateway build R5221-20240206-GA. This means that a fix for an Edge or Gateway issue listed in the 5.2.2 Release Notes up to these listed builds is included in all Release 5.2.3 builds.

Fixed Issue 72762: For a customer enterprise site deployed with an Enhanced High Availability topology, the Remote Diagnostic > Traceroute does not work when run for a WAN link connected to the Standby Edge.

The Orchestrator UI shows the Standby Edge proxy WAN link when running the **Remote Diagnostic > Interface Status**, so the interface is up and the link is recognized. In addition, a traceroute run for a Standby Edge proxy WAN link does not work when run from the Active Edge.

Fixed Issue 116059: For a customer enterprise site deployed with a High Availability topology where VNF's are used, connectivity to a Standby Edge VNF fails from the VNF manager present on the VNF management VLAN.

When a VNF manager is deployed on the VNF management VLAN, a wrong MAC address entry can be learned on the Standby VNF management bridge's forwarding database (FDB) and this entry persists even after the Standby bridge ports are set to a disabled state. As a result, the Standby Edge VNF connectivity fails from the VNF manager.

Fixed Issue 116894: 1:1 NAT does not work properly when the Outside IP address and Source IP address are in the same subnet.

With this 1:1 NAT configuration the Edge changes the source port during the NAT translation and the result is traffic dropping that matches this rule for inbound traffic.

Fixed Issue 122112: For customers subscribed to the Edge Network Intelligence service with Analytics enabled, a user may observe a discrepancy between actual user traffic and the Edge Network Intelligence graphs.

The issue arises from the Edge process not handling traffic (DHCP, RADIUS, and so forth) which contains non-printable string fields. In these instances the *protobuf* messages sent by the Edge will be dropped in Edge Network Intelligence. These *protobuf* messages are sent in batches of 50 messages, and if any one message is invalid, the entire 50 message batch is dropped on the Edge Network Intelligence backend. This results in significant disparities between the data shown on the Edge Network Intelligence UI and the SD-WAN UI (**Monitor > Transport**, for example).

Fixed Issue 123283: When a customer uses Partner Gateways and enables or disables Secure BGP Routes, the BGP session is flapped and client users would observe degraded traffic.

When Secure BGP Routes is toggled on/off the only traffic that should be affected is overlay traffic on the SD-WAN network, it should not affect the underlay network which is what is happening when the BGP session is brought down and then up.

Fixed Issue 124084: An Arista SD-WAN Edge that is deployed as part of a Hub Cluster may experience a Dataplane Service failure and restart to recover.

The service failure would include a SIGXCPU message in the logs and is the result of multiple threads becoming deadlocked.

Fixed Issue 125336: A customer enterprise deployed using port forwarding rules may observe that traffic matching these rules is dropped by the SD-WAN Edge, and once the issue is encountered the behavior persists until a user toggles the Firewall status under Configure > Edge > Firewall.

The issue is triggered by an Edge interface being down and then coming up later. The Edge marks this interface as pending, but when the interface comes up, the port designation for this interface is not changed for the inbound policy index and this results in a port mismatch which results in the Edge dropping the traffic matching this rule.

Fixed Issue 125579: A customer cannot perform an SNMP walk for the attributes ifHCInOctets and ifHCOutOctets on the Standby Edge in a High Availability Edge pair.

Release 5.2.3 adds support for the SNMP attributes ifHCInOctets and ifHCOutOctets when polling the Standby Edge.

Fixed Issue 128269: If a user changes the OSPFv2/v3 cost of an Edge interface, the OSPFv2/v3 adjacency is restarted, which can result in a brief disruption in customer traffic using those routes.

When the OSPFv2/v3 cost of an interface is changed, the Edge service removes the entire OSPFv2/v3 configuration for that interface and a new configuration is added for in the Edge's routing process. This results in a restart of the adjacency.

Fixed Issue 129311: An Operator or Partner user may observe that an Arista SD-WAN Gateway has an increasing number of stale tunnel entries and stale peer entries and in some cases that the Gateway restarts its service.

This information can be found when looking at the Gateways page for a particular Gateway under the **System Information > General** screen of the Orchestrator UI. The Gateway restarts if the number of stale tunnels and/or stale peer entries reach a critical level as a way of clearing the entries.

Fixed Issue 130495: For a customer enterprise using a Cloud Security Service (CSS) with GRE tunnels, if the customer activates a new Edge that is associated with a configuration profile shared by other Edges also using this CSS, the client users at those other locations may observe that traffic using the CSS drops.

Upon receiving a control plane update for either CSS or Non SD-WAN Destination (NSD) via Edge, GRE tunnels may fluctuate. This is because the tunnel configuration is assumed to change, causing it to be torn down and recreated. The fix ensures that if no changes are detected, the GRE tunnel remains operational.

On an Edge without a fix for this issue, the workaround is to activate the Edge to an isolated configuration profile and, once the Edge is up, only then transfer it to its proper profile.

Fixed Issue 130777: On an Arista SD-WAN Edge where a routed interface is configured to be a LAN interface with NAD Direct turned off, there is a discrepancy between using a Source/Destination Interface and an IP Address, and in some scenarios packets may be allowed when filtering using an IP Address and dropped when using the Interface and vice versa.

In the reported instance for this issue, if a firewall rule is specified for a specific Edge interface, the Stateful Firewall drops the packets, but if the rule is changed to use an IP Address, the rule is not enforced and traffic is allowed to pass.

On an Edge without a fix for this issue, avoid using IP addresses in this scenario.

Fixed Issue 131122: In some cases, UDP traffic which matches a configured Business Policy rule which includes a Policy-Based NAT (PBNAT) may not be steered as expected.

The SD-WAN Gateway may not see the QOS synchronization for certain UDP flows (for example, DNS traffic). This results in UDP packets potentially not getting the expected routing and business policy rules applied. When the particular flow consists of a single packet (like a DNS flow) the impact can be significant as the entire flow is incorrectly steered.

Fixed Issue 132188: An Arista SD-WAN Edge with a large number of tunnel flaps may experience a Dataplane Service failure and restart to recover.

Each time a tunnel flaps (is torn down and then rebuilt), a new IKE security association (SA) is issued and the Edge stores these. In this instance the stale IKE SA's are not being cleared out resulting in a leak, exhausting the counters, and ultimately triggers an exception and an Edge service failure and restart to recover and also clear out the stale IKE SA's.

Fixed Issue 132253: A DNS server connected locally to an Arista SD-WAN Edge using a routed interface does not work.

The routed interface is configured with DNS Proxy enabled but the DNS server's requests are dropped by the Edge. This scenario happens when the WAN overlay configuration was enabled on the interface initially and is later disabled.

On an Edge without a fix for this issue, the user can toggle the DHCP server configuration on the interface. In other words, if the DHCP server configuration is already enabled on the interface, just disable it, save and enable again. If the DHCP server configuration is disabled, enable it , save and disable again.

Fixed Issue 132597: For a customer enterprise deployed using OSPFv3 (that is, customers using OSPF with IPv4/IPv6 addressing), when troubleshooting an OSPF issue for one of their sites a user may observe that the OSPF logs are flooded with the message "OSPF6: Message received on disabled interface" repeated over and over.

This message is posted every 30 seconds in the OSPF log and significantly impacts a user's ability to debug an OSPF issue as this message crowds out other relevant logging messages.

Fixed Issue 132693: If a customer enterprise has a name that includes special characters, an attempt to generate a Packet Capture or Diagnostic Bundle for an Arista SD-WAN Edge may fail.

A special character can be anything that is not standard alpha numeric including something like '%' or a letter that is not included in standard English like ä, ö, and ü that has an umlaut. These characters are not handled properly by the Edge and result in the PCAP or Diagnostic Bundle failing to generate.

Fixed Issue 132716: 1:1 NAT rule may not work on a VLAN-enabled PPPoE WAN link.

When adding a self-ip to the self-ip table for IP-based WAN interfaces like PPPoE, the Edge process should always account for the VLAN. The issue is that when the Edge receives packets from this type of interface, the VLAN is not present and the lookup fails and all packets steered to the PPPoE link are dropped.

Fixed Issue 133179: Rate limiting through a Business Policy rule does not work for SNMP flows.

When a business policy rule is created to rate limit the transit SNMP flows, the Edge does not honor the rate limit setting even though the rule is applied successfully. This is because these flows are considered control flows although the SNMP traffic is not for the Edge, but for remote devices.

Fixed Issue 134085: SNMP polling does not return interface status information for Edge interfaces using PPPoE links if the link is down.

When a PPPoE link is down, the monitoring tools are reporting the status of those interfaces as unknown. Issue is caused by the Edge kernel removing the interface when the PPPoE link goes down and this results in the SNMP polling failing for that interface.

Fixed Issue 134111: An Arista SD-WAN Gateway deployed as a Partner Gateway may experience multiple Dataplane Service failures with core files generated and would stop connecting to the Edges configured to use it.

If a Gateway experiences three Dataplane Service failures in a short period of time, the Gateway defensively stops restoring service after the third failure and would no longer connect to any Edge configured to use it.

The cause of this issue is rare as one of the Edges in the network classifies itself as a Gateway and sends a spurious messages to the actual Gateway which it does not expect to handle and triggers each service failure.

Fixed Issue 134461: For a customer using an Arista Edge Model 610 who also enable Stateful Firewall for this device, if the IP Unknown Protocol is toggled on, the Edge may experience a Dataplane Service failure and only recovers when this option is toggled off.

When this issue is encountered the Edge experiences 3 successive service failures which, after the third such failure, causes the Edge to defensively not attempt to recover the service and which results in all customer traffic dropping until a user intervenes. The user would first need to toggle off the IP Unknown Protocol option and then restart the Edge service through the Orchestrator or manually reboot the device depending on the user's access to the Orchestrator.

Fixed Issue 134690: For a site using an Arista SD-WAN Edge model 510-LTE or 610-LTE, there may be a discrepancy in what the Local UI shows for the CELL interface status versus what the Orchestrator UI shows for the same link.

When this issue is encountered, the Local UI shows the CELL interface as down and also indicating that the SD-WAN service is down, while the Orchestrator UI shows the same link as up and passing traffic. This issue can cause confusion for a user attempting to activate the LTE Edge model using the CELL interface and being told by the Local UI that the link is down when in fact it is up and the Edge could be activated.

Fixed Issue 135528: For a customer enterprise site using an Arista SD-WAN Edge which includes SFP ports, when accessing the Local UI for this Edge a user may observe that an SFP port with a connected WAN link shows as down and inaccessible.

Not only does the SFP link show as offline, but a user cannot configure the SFP interface on the Local UI, showing the message "Unknown error". This issue stems from the Edge not populating the SFP interfaces in a key Edge interface file which prevents the user from configuring the interface.

Fixed Issue 136566: A Partner who deploys an Arista SD-WAN Gateway may observe that their Partner Gateway is being rate limited due to an excessive number of dropped packets even though the Gateway is not under a heavy traffic load.

The issue arises if a Gateway is not provisioned using the recommended settings. In this scenario, the Gateway generates continuous DPDK L2 drops even at zero load on the Gateway. This fools the Gateways service into thinking the Gateway is at throughput capacity and the service begins to throttle traffic to the Gateway.

To avoid false positives in this scenario, a Gateway with a fix for this issue would, instead of monitoring both RX/TX drops, only monitor for RX drops and set an overcapacity condition only if the observed drops are above a certain threshold (250 packet drops/second).

Fixed Issue 136681: An Arista SD-WAN Edge may experience a Dataplane Service failure, generate a core file and restart to recover. On a customer site deployed with a High Availability topology, both the Active and Standby Edge experience this issue and client users would experience traffic disruptions the same as in a standalone topology.

In an upgrade scenario, the Orchestrator configurations designed for the 5.2.0.2 version are transmitted to the Edge, where they are parsed and applied. As part of the configuration management process, the Edge parses Cloud Gateway configurations and modifies the default "v" routes (IPv4 and IPv6) by either adding

or removing them. During this process, there is a potential for a use-after-free vulnerability in route objects, which can lead to the corruption of the route object's memory pool. If this corrupted memory pool is accessed later, it can result in the failure of the Edge service.

Fixed Issue 136992: A user can factory reset an SD-WAN Edge, even though the last factory image update attempt failed.

An Edge factory image update can be interrupted for various reasons, (for example: losing power, or rebooting). An Edge factory reset followed by an unsuccessful factory image update will leave the Edge non-bootable.

Fixed Issue 137894: SD-WAN tunnels may not establish for a configuration where one WAN link has multiple underlying interfaces.

In situations where a link possesses multiple interfaces and the primary interface is initially down, the link might not have any destinations added to it. As a result, interface switching does not occur where the link lacks any destinations.

Fixed Issue 138052: For a customer enterprise that uses ICMP Probes, a probe may stop working after 65534 iterations.

ICMP Probe's *recv seq* number can get stuck at 65533 when the 65534th response comes out of order. This issue occurs rarely as it can only occur when the ICMP probe has multiple subscribers.

Fixed Issue 138303: An SD-WAN Edge may experience a Dataplane Service failure and restart to recover.

The issue is the result of a race condition in the Edge’s DNS cache where an entry is being accessed and its reference is stored by a thread which, due to a context switch, another thread deletes. When the former thread is scheduled and tries to access the entry, it triggers a memory violation resulting in an Edge service failure because the reference to the DNS cache entry is no longer valid.

Fixed Issue 138771: For a customer enterprise using the SD-WAN Firewall feature, the Edge may not generate a Syslog for invalid cached pass-through fragments.

A packet that increments several Firewall drop counters related to fragmented packets should generate a Syslog message, but in this instance the Edge does not.

Fixed Issue 139173: An entry level model of the SD-WAN Edge (A 510, 520, 610, 620, or 710 type) may report increasingly high memory utilization if the Enhanced Firewall Service's Intrusion Detection System/Intrusion Prevention System (IDS/IPS) is being used.

Memory utilization is observed on the **Edge > Monitor > System** screen of the Orchestrator UI. This is a memory leak and over time if the memory usage reaches a critical point, the Edge will trigger a service restart to clear the memory. The entry-level Edge models are more vulnerable due to their lower hardware memory specifications (4 GB).

Fixed Issue 139476: If a static route for a destination prefix coexists with another route and the static route's next hop interface fails, traffic to that destination might be dropped.

In certain scenarios, the flow route lookup fails to select an alternative route when the static route is unreachable. This causes the flow to attempt using the unreachable static route, leading to dropped traffic.

Fixed Issue 140382: On a customer enterprise site deployed with an Enhanced High Availability topology, the Standby Edge may restart in response to an Active/Active (Split-Brain) state, even though the Standby Edge is receiving heartbeats from the Active Edge.

On an Enhanced High Availability topology, a timing condition on the Standby Edge can result in it receiving a heartbeat right before processing a failover event, the event logged on the edged logs will read: "Reason - No Heartbeat seen for the past 0ms" and the Standby device will transition to an Active state by triggering a failover. This results in an Active/Active state.

Orchestrator Resolved Issues

Resolved in Orchestrator Version R5239-20250319-GA

Orchestrator version R5239-20250319-GA was released on 03-28-2025 and resolves the following issues since Orchestrator version R5238-20250206-GA.

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 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.

Resolved in Orchestrator Version R5238-20250206-GA

Orchestrator version R5238-20250206-GA was released on 02-13-2025 and resolves the following issues since Orchestrator version R5237-20241220-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, 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.

Resolved in Orchestrator Version R5237-20241220-GA

Orchestrator version R5237-20241220-GA was released on 01-02-2025 and resolves the following issues since Orchestrator version R5236-20240829-GA.

Fixed Issue 108833: BGP configuration on a segment is overwritten after editing BGP in other segment using new UI

Some customers may experience an outage after editing the new BGP filter using the new UI. One segment's configuration is overwritten by another segment's configuration (Global Segment), forcing to recreate the configuration from scratch to recover connectivity.

Fixed Issue 130943: ValidationError: "linkLogicalId" is not allowed is causing LINK_DEAD alerts to fail

When the edge sends internalId instead of logicalId as a part of the params, pushLinkQualityEvents API schema fails validation.

Fixed Issue 151844: DR is not established when the Orchestrator is in FIPS-enabled mode.

Customers in FIPS Orchestrator mode may experience Disaster Recovery (DR) issues due to an issue where certain passwords with special characters were not being read correctly. It also causes downstream replication issues.

Fixed Issue 152892: Failing issues when switching from fips-strict to fips-compliant mode

Some customers may experience failing issues when switching from fips-strict to fips-compliant mode.

Resolved in Orchestrator Version R5236-20240829-GA

Orchestrator build R5236-20240829-GA was released on 09-06-2024 and is the 6th Orchestrator rollup for Release 5.2.3.

This Orchestrator rollup build addresses the below critical issues since the 5th rollup build, R5235-20240715-GA.

Orchestrator build 5.2.3.6 adds support for provisioning and configuring Edge models 710-5G, 720, and 740 on the UI.

Fixed Issue 139581: The Orchestrator allows a user to create or update a Business Policy rule or a BGP route filter and use a name already used by another rule or filter.

The Orchestrator lacks a validation check for duplicate Business Policy rule and BGP route filter names. This validation check would be expected to throw an error that the name the user configured is already in use.

Fixed Issue 143506: For a Partner or Operator user on the Customer & Partners > Manager Partner Customers > Manage Customers screen of the Orchestrator UI, the customer settings "Edge Config Updates Enabled" and "Edge Config Updates Enabled on Upgrade" may display an incorrect value.

When encountering the error, a user would observe that both settings always show "Not Enabled" when they are in fact both "Enabled" as can be observed in the **Service Settings > Edge Management** for that same customer.

Fixed Issue 146441: An Operator or Partner may observe assigning an Operator Profile to a customer fails.

With this issue, when a user attempts to save the configuration change to the new profile, the Orchestrator would display the following error: *CANNOT_EXCLUDE_EDGE_OVERRIDDEN_OPERATOR_PROFILE: Operator profile(s) #####,#####,#####,##### are in use by edges and cannot be excluded*.

The issue is traced to the Orchestrator backend not handling Edge software images marked as "Deprecated" properly.

On an Orchestrator without a fix for this issue, the user can use the Classic Orchestrator to assign the affected Operator Profile.

Fixed Issue 148179: For an Edge where the Firewall is enabled, if navigates to Diagnostics > Remote Diagnostics and runs "List Active Firewall Sessions", they may observe that the TCP State value "SYN_RECEIVED" overlaps the value show for Bytes Sent in the adjoining column.

Because the TCP State value Syn Received overlaps the numerical value for Bytes Sent, the user cannot see the Bytes Sent value.

Fixed Issue 148274: A user may observe gaps in charts on the Monitor > Edge section of the Orchestrator UI.

When an Orchestrator's database receives a high volume of simultaneous queries, it does not properly queue requests beyond the maximum concurrent query limit.

As a consequence, queries are rejected, leading to client failures. Clients without proper retry mechanisms or error handling capabilities fail to correctly handle this failure, resulting in gaps in visualizations, like **Monitor > Edge** charts (QoE, Links, Flows, and so forth).

Fixed Issue 149028: A user may observe that the Advertise option for a VLAN is grayed out and not selectable at the Profile level if no IPv4 address is configured for that VLAN and Assign Overlapping Subnets is not selected.

The expected behavior is for the Orchestrator UI to permit a user to **Advertise** a VLAN at the Profile even in the absence of a configured IPv4 address and **Assign Overlapping Subnets** not being selected.

Resolved in Orchestrator Version R5235-20240715-GA

Orchestrator build R5235-20240715-GA was released on 07-19-2024 and is the 5th Orchestrator rollup for Release 5.2.3.

This Orchestrator rollup build addresses the below critical issue since the 4th rollup build, R5234-20240629-GA.

Fixed Issue 146946: When a an Operator is logged into the Orchestrator and navigates to the Global Settings section, they may not observe the Partner's name on the banner at the top.

The partner banner is not displayed within the **Global Settings** page due to the history service not correctly populating and sharing the unique data between the Orchestrator UI and the **Global Settings** UI when navigating between them.

Resolved in Orchestrator Version R5234-20240629-GA

Orchestrator build R5234-20240629-GA was released on 07-02-2024 and is the 4th Orchestrator rollup for Release 5.2.3.

This Orchestrator rollup build addresses the below critical issues since the 3rd rollup build, R5233-20240522-GA.

Fixed Issue 127870: On the SD-WAN > Configure > Edges page of the Orchestrator UI, for enterprises with a large number of Edges, the Edges list may take more than a minute to load when it is expected to take seconds to do so.

The issue is caused by the API call **getEnterpriseEdgeList** taking a long time to return.

Fixed Issue 144891: When a user navigates to Monitor > Edge > Sources tab, they cannot change the hostname for a Client

A user should have the option to change the hostname for a client by clicking the Edit icon and opening the Change Hostname box. While they can enter in the text under the Change Hostname field, when they click Save Changes, the new hostname is not applied.

Note: This issue was originally tracked with ticket **#127037** and marked as resolved in Orchestrator version 5.2.0. However the issue is only fully resolved with this ticket, and in this Orchestrator build.

Fixed Issue 145134: For a customer enterprise using Zero Touch Provisioning (ZTP) and who deploy one or more sites with a High Availability topology, users may observe deployed HA Edge serial numbers in the ZTP Available inventory list.

When an Orchestrator requests the Edge inventory from the Maestro service, it is expected to exclude Edges that are being used in HA pairs. The issue is caused by the Orchestrator not checking if the incoming serial numbers are specifically used as HA pair serial numbers and results in the Orchestrator hiding some of HA serial numbers, but not all of them.

Fixed Issue 145810: For a customer enterprise that deploys two or more Non SD-WAN Destination (NSD) via Gateway where redundant Gateways are configured, if the user has BGP for one NSD, and then looks to enable BGP for an additional NSD, they may observe that the Orchestrator automatically changes the Gateway assignment to another Gateway already in use by a different NSD.

In order to enable BGP on a second NSD, the redundant Gateways have to be ones unused by the first NSD already configured with BGP. To meet this condition, the user manually changes the second NSD's redundant Gateway assignments to ones not used by the first NSD. The issue is that, upon enabling BGP, that the Gateways are reverted back to the original Gateways already in use by the first NSD.

Fixed Issue 147155: Customers deployed on an Orchestrator using Version 5.2.3.x may observe that Edge WAN links do not show an ISP name under Monitor > Edge > Network Overview.

Recently the Orchestrator software migrated to a different method of establishing geolocation for an Edge. The issue is that this new method did not include the ISP information for the WAN link(s) an Edge is using which are needed for ISP mapping under **Network Overview > Links**. As a result, the WAN links lacked ISP information.

Resolved in Orchestrator Version R5233-20240522-GA

Orchestrator build R5233-20240522-GA was released on 05-24-2024 and is the 3rd Orchestrator rollup for Release 5.2.3.

This Orchestrator rollup build addresses one issue since the 2nd rollup build, R5232-20240520-GA.

Fixed Issue 145783: On some Orchestrators that use customized branding, users may observe that control buttons at the top of the page are difficult to locate.

Some branded Orchestrators have a header color scheme that matches the colors of the top-right controls (**Help**, **User Information**, and **Menu**) on the Global Settings page, with the result that the buttons blend with the Orchestrator coloring and become difficult to locate.

This issue does not affect Arista cloud hosted Orchestrators, which use a default color scheme whose header colors contrast with interface buttons.

Resolved in Orchestrator Version R5232-20240520-GA

Orchestrator build R5232-20240520-GA was released on 05-21-2024 and is the 2nd Orchestrator rollup for Release 5.2.3.

This Orchestrator rollup build addresses the below critical issues since the 1st rollup build, R5231-20240510-GA.

Fixed Issue 99891: When a Partner Administrator logs onto the Arista SASE Orchestrator and uses the New UI, when they are on the Manage Partner Customers page and select Customer > Global Settings > Customer Configuration, they will observe an error.

The error message reads "not allowed to method" when the Partner Administrator attempts to access the customer configuration even though they have full privileges to that page.

Note: This issue was listed as resolved in Release 5.2.0. However, the issue is only fully resolved with this 5.2.3 Orchestrator build.

Fixed Issue 116666: A Partner with a Superuser role does not have the option to activate Enhanced Firewall Service for one of their supported customer enterprises.

This option should be available for a Partner Superuser when navigating to **Global Settings > Customer Configuration** on the Arista SASE Orchestrator.

Note: This issue was fixed in Orchestrator build **R5202-20230729-GA**. However, the fix for this issue was not included in any succeeding 5.2.1, 5.2.2, or 5.2.3 Orchestrator version. As a result the fix is included in this **R5232-20240520-GA** Orchestrator build.

Resolved In Orchestrator Version R5231-20240510-GA

Orchestrator build R5231-20240510-GA was released on 05-13-2024 and is the 1st Orchestrator rollup for Release 5.2.3.

This Orchestrator rollup build addresses the below critical issues since the original GA build, R5230-20240315-GA.

Fixed Issue 121993: A user may not have the option to edit the VLAN properties for an Arista SD-WAN Edge on the Arista SASE Orchestrator UI.

The issue does not affect all VLANs in use by an Edge but when the issue is encountered the user would click on a VLAN in the UI and the result is nothing happens.

Note: This issue was initially marked as fixed in Release 5.2.2. However, the issue fix did not include a scenario where there was no IPv6 configured for the VLANs, and is only fully fixed with this 5.2.3 Orchestrator build.

Fixed Issue 138635: For a customer deployed on an On Premises Orchestrator, when deploying a Zscaler Cloud Security Service (CSS), the user may observe an error saying Zscaler is unavailable.

This even can occur when the Orchestrator uses a trusted issuer certificate list that not include the Digicert certificates used by Zscaler. In this case the Operator would see the error message: UNABLE_TO_GET_LOCAL_CERTIFICATE. The fix adds the Digicert certificates to the Orchestrator trusted list.

Fixed Issue 143577: On the Edge > Configure > Device page of the Orchestrator UI, changes to an Edge's configuration do not save if the Edge does not have a license.

The Orchestrator UI will not allow a user to create an Edge without binding it to a license, so this only impacts API users that did not associate a license to an Edge. Or an Edge without a license, the Orchestrator sometimes does not perform license validation when saving Edge device configuration changes even though that field is meant to be mandatory.

On an Orchestrator without a fix for this issue, the customer or partner needs to associate a license to the API-created Edge before attempting to modify its configuration settings.

In addition, the UI does not highlight the error except for adding an asterisk (*) to required fields. This part of the issue will be fixed in a future release.

Fixed Issue 143724: On a customer enterprise's Global Settings > Enterprise Settings page of the Orchestrator UI, an Operator with a Superuser role may observe that under the SD-WAN PCI section, if they toggle the Enforce PCI Compliance setting, the Orchestrator UI does not keep the change and toggles that setting back.

This issue is experienced by Superusers only when they navigate directly to the Enterprise Settings page.

Resolved in Orchestrator Version R5230-20240315-GA

Orchestrator version R5230-20240315-GA was released on 03-16-2024 and resolves the following issues since Orchestrator version R5220-20231214-GA. This means that a fix for an Orchestrator issue listed in the 5.2.2 Release Notes is included in all Release 5.2.3 builds.

Fixed Issue 66636: Arista SD-WAN Edge does not honor source interface configuration for RADIUS authentication traffic when the source is a loopback interface.

When a user configures RADIUS on a Profile or Edge and specifies a loopback interface as the desired source interface for outgoing authentication traffic, the Edge fails to create a NAT rule as expected due to a parsing error stemming from an inconsistency in the expected versus actual type of the "port" parameter for

the authentication service that is dispatched from the Arista SD-WAN Orchestrator. This value should be an integer, and the Orchestrator API validation logic has been modified accordingly.

Fixed Issue 72386: On the Monitor > Edge section of an Arista SD-WAN Orchestrator, when looking at the QoE tab under monitoring, the user will observe samples indicating no-data towards the right tail of the time series.

The issue is observed if a user goes to a **Monitor > Edge** page for any Arista SD-WAN Edge and selects the QoE tab with a time range of 12 hours or more. Without the fix, the user will have to query for the desired time range in increments of 1 hour. When done this way, the user would not observe any gaps.

Fixed Issue 80593: A user's deny permission for the privileges used on the "Remote Diagnostics" page doesn't have any effect if the Arista SASE Orchestrator localization changes to a Non-English language.

Role Customization Package permissions for the privileges used in the **Remote Diagnostics** page are not applied when the Orchestrator locale changes to a language other than English. The reason for this issue is that the Orchestrator's Role permission check is done in a translated value, but is compared against an untranslated value which is failing the string match condition.

Fixed Issue 96108: When an Arista SASE Orchestrator is upgraded to a 5.x build, a customer may observe missing memory usage statistics for their Arista SD-WAN Edges when looking at the Monitor > Edge pages of the UI.

The issue is caused during the migration to a 5.x Orchestrator by older Edges sending a different name for their health statistics memory field (**memPct**) when the Orchestrator is expecting to receive the Edge's historic health statistics memory field using the current name (**memoryPct**). As a result, the Orchestrator ignores the Edge health statistics memory field value submitted with the unexpected **memPct** name, and the Orchestrator defaults the health statistics memory field value to zero. The fix for this issue resolves the other cause of missing Edge health statistics on the Orchestrator UI, with the first cause being fixed in #90749 on the original 5.0.1 GA build.

Fixed Issue 110097: For a user logged in as a Partner Administrator, on the Administration > User Management page of the Orchestrator UI, when that user applies a filter to the list of users, the Delete button is grayed out and inaccessible.

The **Delete** button is supposed to be grayed out/inaccessible only if deleting the users results in zero users with a Superuser role. For this issue, the UI is not calculating the number of existing Superusers properly and is making the **Delete** button inaccessible for all filtering scenarios.

Fixed Issue 117627: The Monitor > Network Overview page may return empty/null values for "Top Applications by Data Volume" and "Top Edges by Data Volume".

This issue is caused by a defect in the API **getEnterpriseFlowMetrics**, which can return an empty response. This results in the views 'Top Apps by Data Volume' and 'Top Edges by Data Volume' not being rendered for some customers.

Fixed Issue 120892: Integer values for a BGP Community greater than 65535 will not be properly applied by the Orchestrator to the affected Arista SD-WAN Edges.

BGP filters can be configured at the Edge or Profile **Configure > Device** page, the Non SD-WAN Destination BGP configuration page, or the Partner Handoff BGP configuration section. In all these BGP filters, it is

possible to select an action in the filter with type as *Community*. With this issue, any community value greater than 65535 in integer format is not properly applied by the Orchestrator to the Edges.

On an Orchestrator without a fix for this issue, instead of using integer values for the BGP Community string, convert the value to a colon format when the integer value is greater than 65535.

Fixed Issue 125604: On the Configure > Profile > Device > VLAN page of the UI, when a user edits a VLAN and for IPv4 DHCP Server they enter an invalid value for *Num. Addresses*, the Orchestrator returns an error with no meaningful reason why.

For example, if the user entered '6.18' for the Number of Addresses, the UI rejects this value but only posts "Required" as a reason. The UI should be more precise that the reason the value is rejected is that it is not an integer and the user should enter an integer for this field.

Fixed Issue 125677: On the Configure > Profile > Device > VLAN page of the UI, a user may experience multiple issues configuring a DHCP server.

These issue include:

- For a DHCP option, in the Data Type field, if a user selects Text as an option, the UI does not allow the user to change this value later.
- The UI will occasionally change the DHCP Server option without user input.
- The first time a user edits either the Code or Data Type, the UI may revert the edit after it is saved.

Fixed Issue 125678: On the Configure > Edge > Device > VLAN page of the UI, when a user edits a VLAN and for IPv4 DHCP Server they enter an invalid value for 'DHCP start', the Orchestrator does not return an error.

The UI does not throw an error at the VLAN editing level and allows the user to save the value, but does throw an error at the Interface level of configuration.

Fixed Issue 125684: On the Configure > Edge > Device > VLAN page of the UI, when a user edits a VLAN and sets IPv4 to inactive, they can still edit the IPv4 DHCP Server on the Orchestrator UI.

If IPv4 is deactivated for that VLAN, the IPv4 DHCP Server settings should be grayed out and not accessible.

Fixed Issue 127268: User cannot perform a password reset by entering the provided Two Factor Authentication (2FA) pin number.

The Orchestrator backend API improperly handles the new reset request format included with the New Orchestrator UI and this causes the failure to reset the password.

Fixed Issue 128368: User cannot manually change the Gateway allocation when it is associated with a Non SD-WAN Destination (NSD) via Gateway configuration.

The issue is caused by the Orchestrator only displaying active the Gateway and not the redundant Gateway. As a result, all the possible Gateways are not available to the user.

Fixed Issue 128372: A user can switch a Cloud Security Service (CSS) to a different profile even though a Business Policy configured for Internet Backhaul is associated with that CSS.

The Orchestrator UI should prevent the CSS from being moved with a clear error message regarding the CSS being anchored to an internet backhaul rule.

Fixed Issue 129239: For a large scale enterprise customer (~1000 or more Edges), on the Configure > Profile page of the Orchestrator UI, when a user edits any setting at the Profile level and attempts to Save, they may observe that the API call times out and is not successful.

The issue is the result of other Orchestrator database queries taking too long to complete and causing the attempt to save the new Profile settings to time out. When this issue is encountered, the Orchestrator UI displays a red error banner on the browser page that reads `configuration/updateConfigurationModule time out`.

Fixed Issue 129694: If a user configures the BGP keep alive and hold times as blank on the Orchestrator UI, the peer device will remain up and a restarted Edge will try to connect via BGP but fail.

The neighbor status will say that keep alive and hold time are 0. The Orchestrator should not allow blank values as these are sent as an empty string. The expected behavior for the UI is to have default values and if these are deleted with no replacement value and saved the Orchestrator should throw an error and require an actual integer value.

Fixed Issue 130139: An RMA Reactivation fails if the WAN interface the Arista SD-WAN Edge uses to connect to the Orchestrator is not configured with IPv4 DHCP.

When attempting the RMA Reactivation the Orchestrator UI will throw an error "Uncommon interface proto NONE" and the effort fails.

Fixed Issue 131997: An ICMP probe may be erroneously marked as down when it is configured for one segment but not for another.

The Orchestrator fails to send the NULL ICMP probe configuration when it is not configured in a segment. As a result, the configuration of a different segment is reused, and this causes the probes to fail.

On an Orchestrator without a fix for this issue, configure a dummy ICMP probe for the other segments.

Fixed Issue 132372: On a customer enterprise where Dynamic Cost Calculation (DCC) is activated, the customer can only use an Operator Profile for Edge platform firmware if that profile also includes an Edge software version.

The expected behavior is for an Operator Profile configured to upgrade the Edge's platform firmware to only be configured for the firmware, and not be concerned with the Edge software version as this might trigger an unexpected upgrade or downgrade of the Edge's software. Thus the Operator Profile under **Software Version** should be toggled to **Off** with a "Do not upgrade" message.

The issue is that the Orchestrator does not accept an Operator Profile configured like the above and requires **Software Version** to be toggled **On** with an Edge Version specified. For customers with several Edges on multiple different Edge software versions this is unacceptable and disruptive.

Fixed Issue 132997: On the Orchestrator UI page Configure > Edge > Device > Interfaces, if a user changes an Edge interface's IP address from DHCP to a static IP address, the Orchestrator accepts the configuration and saves the change, but Edge's IP address does not change.

For example, if the user runs **Remote Diagnostic > Interface Status**, they will see the same IP address for the interface as if the DHCP configuration had not been changed to a static IP one.

On an Orchestrator running Release 5.2.x, the UI does not generating the netmask field if the user did not include it in the configuration for the static address type of an Edge interface. This is also true of API users updating the configuration without a netmask field for static addressing type of an interface or sub interface. The Orchestrator should automatically calculate from the IP address prefix and generate the netmask field even when its not present in the earlier configuration for either method.

To avoid this issue on an Orchestrator without a fix for this issue, make sure the static IP address includes the correct netmask value using the API.

Fixed Issue 133198: A user who logs in using RADIUS authentication cannot create a custom role on the Global Settings > User Management section of the Orchestrator UI.

A RADIUS-authenticated user can go through the steps of creating a customer role but when they attempt to save the configuration, the UI throws the error "Error occurred while creating composite role" and the configuration is not saved.

Fixed Issue 133199: When an enterprise user with read-only access pulls up the Configure > Device > Edit Interface dialog, an untagged VLAN is displayed as empty.

A read-only user should be able to view (though not edit) the untagged VLAN configuration.

Fixed Issue 133240: On the Global Settings > Customer Configuration page of the Orchestrator UI, a user cannot make SD-WAN service configuration changes if the customer has no licenses selected.

The issue is that in this instance Edge licensing is disabled for the customer enterprise, which means the Orchestrator should not consider the absence of licenses a consideration when validating the configuration.

Fixed Issue 134378: An Arista SD-WAN Edge upgraded to a 5.2.x software may experience continuous Dataplane Service failures and restart each time to recover.

The issue can be encountered in a scenario where the Edge interface used to activate the Edge is configured with a VLAN that also includes a VLAN on the subinterface with the same VLAN ID for both. This can occur if the user adds the VLAN to the Edge through the Local UI while already having the Edge configured for a subinterface VLAN with the same ID through the Orchestrator for that Edge. The Orchestrator does not harmonize the Local UI configuration with the configuration it controls, and the Edge is provided with a corrupted configuration that triggers the repeated service failures.

If a customer wishes to upgrade their Edges to 5.2.x the workaround is to ensure there are no duplicate VLAN IDs for the interface and subinterface as outlined in the description.

Fixed Issue 134498: For a customer enterprise where a Cloud Security Service (CSS) or Non SD-WAN Destination via Edge is used, if a user removes a non-global segment from a profile, the CSS/NSD via Edge tunnels will be deleted from all other segments, including the global segment.

A common example of a CSS or NSD via Edge involves Zscaler and in this issue when all tunnels are deleted by the Orchestrator, the result is all traffic dropping that matches the rule(s) to be backhauled to the CSS.

On an Orchestrator without a fix for this issue, the user must first disable and then re-enable the CSS or NSD via Edge.

Fixed Issue 134911: A user may observe that the Diagnostics > Remote Diagnostics page for any SD-WAN Edge does not load for potentially more than an hour.

The portal logs would include multiple occurrences of the error message: "Enterprise WebSocket connection limit exceeded". The issue is caused when a **Remote Diagnostics** page for an Edge times out and then the user clicks **Reconnect**. Upon this action the Orchestrator initiates not one, but numerous reconnect attempts that trigger a rate limit function on the Orchestrator and prevent the page from loading.

Fixed Issue 134940: The Orchestrator may assign an Edge a primary and secondary Gateway from the same datacenter location.

Doing this undermines Gateway resiliency through geographic diversity while also potentially creating imbalances in Gateway usage for a Gateway Pool. The issue arises out of the Orchestrator's use of a geolocation service that relies on the Gateway's IP address to establish location. This service can sometimes place an IP address significantly farther away from the Gateway's actual location in the datacenter and fool the Orchestrator into classifying it as geographically diverse from other Gateways in the same datacenter. This is corrected by adjusting the Orchestrator's geolocation tolerances to allow for this service's behavior so that all Gateways in that location are properly classified and ensure geographic diversity for a customer site.

Fixed Issue 135551: If a user creates a Service Permission for a specific user denying the Read Remote Diagnostics privilege, the affected user would observe that on the Diagnostics menu both Remote Diagnostics and the Remote Actions sub-menus are removed.

After removing the Read privilege for **Remote Diagnostics**, the **Remote Actions** sub-menu is also removed. Only the **Remote Diagnostics** sub-menu should be removed.

Fixed Issue 135644: After removing the Create Privilege > Non SD-WAN Destination via Gateway for an Operator with a Standard Administrator role, the Operator user cannot update the service.

The Operator should be able to update an existing NSD via Gateway from the existing list found in the **Configure > Network Services** page, just not create new ones.

Fixed Issue 136247: A user with an Enterprise Administrator role where the privilege to update LAN-Side NAT is denied can still update these rules.

This issue is found in a user role created using the Role Customization feature and the Orchestrator UI is not applying the LAN-Side NAT parameter as part of this custom role package.

Fixed Issue 136454: On the Configure > Edges > Firewall > Edge Security page of the Orchestrator UI, the parameter USB Port Access does not include the Edge 7x0 model.

With this defect, **USB Port Access** only specifies Edge models 510/510-LTE and 6x0 in their deny list. With the introduction of the Edge 710-W, the deny list should also include this model and all upcoming Edge models in the 7x0 line as they are USB enable/disable capable.

Fixed Issue 136810: If an administrator user's Update privilege for Service Settings > Edge Management is removed, the affected user can still update the Edge Management data.

The Orchestrator UI lacked the API to enforce this privilege which is corrected in the fix for this issue.

Fixed Issue 136937: On the Configure > Edge > Device > Interfaces page of the Orchestrator UI, the SD-WAN Edge models 710-W displays the wrong interfaces.

The Edge 710-W shows CELL interfaces, which it does not possess.

Fixed Issue 137281: Customers may observe that their Edges show as offline on the Orchestrator UI though the Edges are in fact up, connected, and passing traffic.

When an Edge configuration is changed, each Edge is expected to make just 3 database calls, which the Orchestrator can effectively manage even there is a mass Edge configuration change (for example when a Profile that a large number of Edges use is changed). For this issue, the mass configuration change has most of the Edges making from 20 to 30 database calls and this overwhelms the Orchestrator and impacts the Edge heartbeat management and results in the Orchestrator missing heartbeat checks and marking the Edges as offline.

Fixed Issue 137447: On the Configure > Edge > Device > Interfaces page of the Orchestrator UI where a user has deployed an Edge 710-W, the Orchestrator is not selecting the correct configuration for the Wi-Fi radio based on what is seen on the UI.

This is specific to when the Orchestrator autodetects the Wi-Fi type (2.4 GHz or 5 GHz). The Orchestrator will select the type based on the location of the Edge, making sure to select 2.4 GHz when the country where the Edge is located requires it (for example, China and Taiwan). However with this issue, the Orchestrator shows the Edge 710-W is using the 2.4 Ghz but it is in reality using the 5 GHz type. The issue relates to the 710-W having dual-band capable radio, which is new for any SD-WAN Edge model.

This issue can be worked around by overriding the setting and manually configuring the correct Wi-Fi type.

Fixed Issue 137826: The Arista SD-WAN Edge model 710-W do not show up in the Orchestrator's available list; in addition if the 710-W is shown, the UI shows the wrong interface configuration for the 710-W physical ports.

This issue can be observed on the **Configure > Profile > Device** page, under the **Interfaces** section.

Fixed Issue 139966: For a customer enterprise configured to use multiple segments, one or more cloud security services (CSS), and which has Cloud VPN toggled on, if Cloud VPN is disabled on any segment, all CSS tunnels are deleted for all segments with traffic steered to those tunnels being dropped.

This issue is limited to a scenario where a single Edge is assigned to a profile with multiple segments. In that scenario, when Cloud VPN is toggled off any used segment, the Orchestrator deletes the Pre-Shared Keys (PSK) and FQDN's for all CSS instances, which results in the deletion of all tunnels.

Known Issues

Open Issues in Release 5.2.3.

Edge/Gateway Known Issues

Issue 151806: High Availability PANIC is noticed on Edges.

Standby Edge restarts multiple times or multiple HA_SPLIT_BRAIN_DETECTED events are sent by High Availability enabled Edge. Standby Edge misses heartbeat from peer due to stall in packet processing and this leads to Standby Edge moved to Active State. When the packet processing is resumed, Edge detects split brain (Active/Active state) and to resolve the split brain the newly High Availability state transition edge goes for restart to avoid any packet loss.

Workaround: Increase High Availability default failover time to a higher value may reduce or solve the HA split brain.

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 25595:

A restart may be required for changes to static SLA on a WAN overlay to work properly.

Workaround: Restart Edge after adding and removing Static SLA from WAN overlay.

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 an 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 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 53219: After an Arista SD-WAN Hub Cluster rebalances, a few Spoke Edges may not have their RPF interface/IIF set properly.

On the affected Spoke Edges, multicast traffic will be impacted. What happens is that after a cluster rebalance, some of the Spoke Edge fail to send a PIM join.

Workaround: This issue will persist until the affected Spoke Edge has an Edge Service restart.

Issue 53934: In an enterprise where an Arista SD-WAN Hub Cluster is configured, if the primary Hub has Multihop BGP neighborships on the LAN side, the customer may experience traffic drops on a Spoke Edge when there is a LAN side failure or when BGP is not configured on all segments.

In a Hub cluster, the primary Hub has Multihop BGP neighborship with a peer device to learn routes. If the physical interface on the Hub by which BGP neighborship is established, goes down, then BGP LAN routes may not become zero despite BGP view being empty. This may cause Hub Cluster rebalancing to not happen. The issue may also be observed when BGP is not configured for all segments and when there are one or more Multihop BGP neighborships.

Workaround: Restart the Hub which had the LAN-side failure (or BGP not activated).

Issue 57210: Even when an Arista SD-WAN Edge is working normally and is able to reach the internet, the LED in the Local UI's Overview page shows as "Red".

The Edge's Local UI determines the Edge's connectivity by whether it can resolve a well known name via Google's DNS resolver (8.8.8.8). If it cannot do so for any reason, then it thinks it is offline and shows the LED as red.

Workaround: There is no workaround for this issue, except to ensure that DNS traffic to 8.8.8.8 can reach the destination and be resolved successfully.

Issue 61543: If more than one 1:1 NAT rule is configured on different interfaces with the same Inside IP, the inbound traffic can be received on one interface and the outbound packets of the same flow can be routed via different interface.

For the NAT flows from Outside to Inside, the 1:1 NAT rules will be matched against the Outside IP and the interface where the packets are received. For the outbound packets of the same flow, the Arista SD-WAN Edge will try to match the NAT rules again comparing the Inside IP and the outbound traffic can be routed via the interface configured in the first matching rule with "Outbound Traffic" configured.

Workaround: There is no workaround for this issue outside of ensuring no more than one 1:1 NAT rule is configured with a particular Inside IP address.

Issue 65560: Traffic from a customer to PE (Provider Edge) device fails.

BGP neighborship between a Partner Gateway and Provider Edge does not get established when tag-type is selected as "none" on the handoff configuration. This is because ctag, stag values get picked from /etc/config/ gatewayd instead of the handoff configuration on the Orchestrator when tag-type is "none".

Workaround: Update the ctag, stag values to 0 each under vrf_vlan->tag_info in /etc/config/ gatewayd. Do a vc_procmon restart.

Issue 67879: A Cloud Security Service (CSS) tunnel is deleted after a user changes a WAN Overlay setting from auto-detect to user-defined on a WAN interface setting.

After saving the changes, the CSS tunnels do not come back up until the customer takes down and then puts back up the tunnel. Changing the WAN configuration will bring down the CSS tunnel and parse the CSS setup again. However, in some corner cases, the *nvs_config>num_gre_links* is 0 and the CSS tunnel fails to come up.

Workaround: Deactivate the CSS setup, and then reactivate it and this will bring the CSS tunnel up.

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 68851: If an Arista SD-WAN Edge and Arista SD-WAN Gateway each have the same TCP syslog server configured, the TCP connection is not established from the Edge to the syslog server.

If the Edge and Gateway each have the same TCP server and if the syslog packets from the Edge are routed via the Gateway, the syslog server sends a TCP reset to the Edge.

Workaround: Send the syslog packets direct from the Edge instead of routing via a Gateway or configure a different syslog server for the Edge and Gateway.

Issue 81852: For an Arista SD-WAN Edge that is using a Zscaler type Cloud Security Service (CSS) which uses GRE tunnels that has turned on L7 Health Check, when that Edge is upgraded to Release 5.0.0, in some instances the customer may observe L7 Health Check errors.

This is typically seen during software upgrade or during startup time. When L7 Health check for a CSS using GRE tunnels is turned on, error messages related to socket getaddress error may be seen. The observed error is intermittently seen, and not consistent. Because of this, L7 Health Check probe messages are not sent out.

Workaround: Without the fix, to remediate the issue, a user needs to turn off and then turn back on the L7 Health Check configuration, and this feature would then work as expected.

Issue 82184: On an 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 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 92421: When a public and private overlay are configured on the same Edge interface with different custom VLAN tags, there is a chance that the underlay routed traffic may get dropped.

When a public and private overlay are configured on the same interface with different custom VLAN tags, the Edge may learn the ARP entries with the wrong VLAN tags, resulting in the traffic being dropped.

Workaround: Avoid using this configuration. This issue is fixed on Release 5.4.0 and later.

Issue 98136: For customer enterprises using a Hub/Spoke topology where Dynamic Branch To Branch VPN is configured, client users behind a SD-WAN Spoke Edge may observe that some traffic has unexpected latency resulting from the traffic using a sub-optimal path.

Spoke Edge traffic that experiences this issue uses a route that was initially a non-uplink route for a Hub Edge not included in the Profile the Spoke Edge was using. A Dynamic Branch-to-Branch VPN tunnel can be formed from the Spoke Edge to the Hub Edge because of traffic being sent towards some other unrelated prefix and in this instance the non-uplink route is installed in the Spoke Edge.

As a result of this non-uplink route, all traffic towards this prefix starts going through the

Hub Edge and the non-uplink route becomes uplink (community change to uplink community) but the non-uplink route installed previously is not revoked and the traffic takes the Hub Edge path as long as the Dynamic Branch-to-Branch VPN tunnel remains up.

Workaround: Wait for the Dynamic Branch-to-Branch VPN tunnel to tear down, after which the uplink route will not be installed in the Spoke Edge when a new Dynamic Branch-to-Branch VPN tunnel is formed towards the Hub Edge.

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 111085: When an Arista SD-WAN Edge's WAN link is configured with an IP address in the same network as the Edge's loopback IP, the Edge uses the MAC address of the WAN interface while responding to an ARP request for the Edge's loopback IP address.

This can cause ARP spoof and results in the Management IP being deprecated and network disruptions as a result.

Workaround: There is no workaround for this issue.

Issue 113877: For customers who configure BGP/GRE LAN, those using a TGW GRE will experience BGP flaps and traffic interruption on the TGW secondary tunnel in all segments when the BGP configuration for TGW GRE is modified on the Global segment.

When customer changes a BGP configuration of TGW GRE on the global segment then the secondary tunnel in the global and other segments flap, leading to a BGP connection reset and reconvergence and traffic interruption. The BGP connection will form again, and traffic will restore.

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, an Arista SD-WAN HA Edge may experience multiple restarts.

When **Enhanced Firewall Services** 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 118710: The IP address and mask are not allocated to the VLAN interfaces that are created on the WLAN interfaces.

The Edge kernel fails to assign the VLAN interfaces onto the WLAN interfaces, which prevents the Edge from applying the configuration to these VLAN interfaces. Additionally, the assignment of network interface (netif) corresponding to vc-ifaces is also omitted, rendering these interfaces unusable since there are no IP addresses assigned to them.

Workaround: Assign a physical interface (in other words, an Edge port like GE1, GE2 or the like) to the VLANs.

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 130885: An OSPFv3 route tag may not be updated for an IPv6 external route.

In some corner cases, OSPFv3 does not consider the tag updated by the neighbor for an external route if the update is received within very short interval.

Workaround: Withdraw and re-advertise the external route from the OSPFv3 neighbor.

Issue 131674: ICMP traffic from a Spoke Edge using internet backhaul via a Hub Edge fails if the ICMP flow has to be steered from one link to a different one.

ICMP traffic passing on one of two or more links is expected to be steered to a different link if the existing link goes down or is unusable per QoE.

Workaround: There is no workaround for this issue.

Issue 133678: If an Arista SD-WAN Edge is configured for IPv4/IPv6 dual stack, the Edge may lose connectivity to the Orchestrator if the IPv4 link is down.

This issue can occur if the Edge was activated with only an IPv4 link, and an IPv6 link is added only later to the device. At the time the Edge is activated, only the IPv4 Orchestrator address is written to the Edge that manages Orchestrator connectivity. Adding an IPv6 link later does not add the IPv6 address to the file and so if the IPv4 link is removed, the Edge loses connectivity to the Orchestrator.

Workaround: An Edge activated with only an IPv4 link would need to keep at least one IPv4 WAN link connected even though the Edge is dual stack.

Issue 134125: On the Monitor > Events page of the Orchestrator, a customer may observe that the event "New Client Device Seen" contains an incorrect IP address.

When a new client acquires a DHCP IP address, or an existing IP mapping changes, an event is sent to the Orchestrator with the IP address, hostname, and the device OS details. However, a defect in the code where the DHCP structure is not initialized properly results in incorrect values being present in the *clientrequested* IP address field. This was misinterpreted as an IP address change and the Orchestrator events were triggered unnecessarily with an incorrect IP address.

Workaround: This is a cosmetic issue and can be safely ignored, and there is no workaround beyond upgrading the Edges to any build of Version 5.2.4.

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.

Under extreme load/scale environments where the flow, tunnel, and routes scale to the limits of a hardware Edge model in conjunction with aggressive route timers (OSPF = 3/12, BGP = 1/3), the HA Standby Edge can sometimes miss an HA heartbeat and be moved 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.

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 not 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 136336: For a customer who configures a Cloud Security Service (CSS) with a Zscaler type, return traffic from Zscaler may get dropped if the Edge has the Common Criteria Firewall enabled.

The Edge would have a Business Policy rule to backhaul internet traffic via that Zscalar tunnel and in this case the return traffic is dropped due to a Reverse Path Forwarding (RPF) failure that occurs during the route lookup for the return traffic.

Workaround: Do not use the Common Criteria Firewall feature while also using Zscaler as a CSS.

Issue 137083: An Edge may initiate a service restart when a user generates a diagnostic bundle for it.

When diagnostic bundle trigger is received from the Orchestrator, the Edge's Dataplane Service experiences a failure and restarts to recover.

The issue is caused by the diagnostic bundle script running *debug.py --dns_name_cache,* which still has some freed entries and triggers the Edge service failure.

Workaround: Without a fix for the issue, a user should seek to generate a diagnostic bundle in a maintenance window, if possible.

Issue 137932: For a customer using Partner Gateways, when the Handoff IP Address is changed on the Orchestrator UI, this change is not applied to the Gateway even though the UI shows that it has been applied, which leads to customer traffic failure.

This can be confirmed on the Gateway using the *debug.py --ifaces* command. The issue is caused by a defect in the Gateway process for handling only a handoff IP address update, though a first time handoff configuration does work.

Workaround: Disable handoff for the enterprise + the segment and save the configurations. Then re-enable handoff and configure the new handoff IP. This should only be done in a maintenance window.

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 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 138452: For a customer who uses a Cloud Security Service (CSS) or a Non SD-WAN Destination via Edge, if a user changes an Edge interface's WAN overlay from auto detect to user defined, the customer would observe duplicate tunnel entries and traffic drops.

When an interface overlay is modified, the expected behavior is for the Edge to delete all the CSS/NDS paths linked with the interface. With this issue the Edge is deleting only one CSS/NSD path linked to the interface, which results in duplicate tunnels.

Workaround: Only change the Edge interface WAN overlay in a maintenance window. After the change is made, disable all CSS or NSD's via Edge and then re-enable them as this will delete all the tunnels.

Issue 138464: On a customer enterprise site using a High Availability topology, a user may observe high memory utilization on the Active Edge which can result in an HA failover due to high memory usage.

With this issue, the Active Edge's memory utilization increases rapidly when the HA Edge is handle a higher number of concurrent connections per second. Once the memory utilization reaches 60% and is sustained there for more than 90 seconds, then the Active Edge's service defensively restarts to recover memory, resulting in an HA failover. In an Enhanced High Availability topology this can cause customer traffic disruption for traffic using a WAN link on the Active Edge that is affected by this issue.

Workaround: On the **Monitor > Events** page for that HA Edge, monitor the memory utilization threshold limit warning Event or monitor memory utilization on the **Monitor > Edges > System** page and reduce the number of concurrent connections per second to maintain the memory utilization to less then 60%.

Issue 139855: For a customer enterprise where a High Availability topology is used and the Edges are virtual (not hardware Edges), if a user changes any Edge device setting, the Edge may delete the default route.

This issue is limited to sites where the virtual HA Edges use a unique MAC Address on the LAN interface and have routing configured on the LAN interface. In that scenario the default route via a route interface (WAN overlay) and LAN interface may be removed after any changes on the **Configure > Edge > Device** page, resulting in customer traffic disruption.

Workaround: Perform a network service restart to repopulate the default routes.

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 loop back 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 141041: For a customer enterprise site deployed with a High Availability topology with VNFs installed, where the HA Edge pair or either Edge models 520/540 or 610, reachability to the Standby Edge's VNF from a LAN-connected client may fail.

The Ethernet switch board on these Edge models drops ARP reply packets sent to a LAN client from a Standby Edge's VNF resulting in a loss of reachability.

This issue was first observed for the 5.4.x Edge build and documented in 102583 of the 5.4.0 Release Notes. This ticket tracks the issue for 5.2.3.

Workaround: There is no workaround for this issue.

Issue 141113: An SNMP walk may get timed out and fail to complete when the Edge has an interface configured for a PPPoE link which is stuck in a down state.

This issue only occurs if the PPPoE link on the interface is never up, if the interface is up and goes down for some reason the SNMP walk will successfully complete.

Workaround: Ensure that any configured PPPoE link is capable of coming up, in other words ensure the peer PPPoE server is enabled.

Issue 141273: For a customer enterprise site deployed with a High Availability topology, when HA is later deactivated, the virtual MAC addresses persist on the now standalone Edge ports.

The virtual MAC addresses (VMAC) are programmed on the Active and Standby Edge when HA is activated to facilitate faster convergence during HA failover. However, when HA is deactivated on the Edge, the VMAC is still programmed on it. Also, if the Standby Edge is removed and also used as a separate standalone Edge, the result is duplicate MAC addresses and this leads to switch loop if both Edges (old Active and old Standby) are on the same broadcast Network.

A user can confirm this issue is present because the virtual MAC address prefix always begins with **F0:8E:db**.

Workaround: On an Edge without a fix for this issue the user can either force a factory reset on each standalone Edge to clear the port configuration, or the Support team can remove the */velocloud/ha/virtualmacs* file from the Edge and reboot it.

Issue 141327: If a user performs a VNF insert using a Palo Alto Networks (PAN) VNF for an Edge model 520v, the VNF Insertion remains down after the required Edge Service restart.

The issue occurs when using the VM-50 lite Authcode.

Workaround: Redeploy the VNF.

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: A 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 143828: A customer may observe that an Edge has an unexpectedly high level of memory usage that may get sufficiently high to reach a critical level and trigger a defensive Edge service restart to recover the memory.

One of the factors that contributes to this memory leak is extensive use of CLI commands on the Edge by either a Partner or Operator as part of troubleshooting or monitoring the Edge. These commands are accumulated and never cleared from the relevant Edge process. The use of **Remote Diagnostics** on the Orchestrator UI does not contribute to this issue.

As with any Edge memory usage issue, entry level Edge models with lower RAM specifications (in other words, the Edge models 510, 610, 710, or 520) would be more likely to experience the issue, but it can happen on any Edge model with sufficiently high memory usage.

Workaround: Extensive use of CLI commands on the Edge by either an Operator or Partner should be avoided, and if troubleshooting work is done, the customer should check the Edge's memory usage on the **Edge > Monitor > System** page.

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 149862: For a Virtual Edge that does not have a LAN adapter, when this Edge is upgraded to Release 5.2.3.3, it does not form tunnels and sends out the message: "VeloCloud Edge service started in mgmt-only mode" .

This issue is the result of network configurations not being fully generated on Virtual Edges (including AWS, Azure, and GCP) that do not have LAN adapters.

Issue 151654: A link may not come up on a VeloCloud Edge where both the Edge's Ethernet port and the peer port have auto-negotiation set to off.

For the Edge port, auto-negotiation is set to off and the user has manually configured the speed and duplex of the port through the UI. The issue is the result of differing implementations of auto-negotiation between the Edge and the peer device.

Workaround: On an Edge without a fix for this issue, the user should turn on autonegotiation on the Edge's Ethernet port.

Orchestrator Known Issues

Issue 41691:

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

Issue 43276:

User cannot change the Segment type when a Arista SD-WAN Edge or Profile has a Partner Gateway configured.

Workaround: Temporarily remove the Partner Gateway configuration from the Profile or Edge so that the Segment can be changed between private and regular. Alternatively, the user can remove the Segment from the profile and make the change from there.

Issue 47713:

If a Business Policy Rule is configured while Cloud VPN is toggled off, the NAT configuration must be reconfigured upon turning on Cloud VPN.

Issue 47820:

If a VLAN is configured with DHCP toggled off at the Profile level, while also having an Edge Override for this VLAN on that Edge with DHCP activated, and there is an entry for the DNS server field set to none (no IP configured), the user will be unable to make any changed on the **Configure > Edge > Device** page and will get an error message of ‘invalid IP address []’ that does not explain or point to the actual problem.

Issue 48085: The Arista SD-WAN Orchestrator allows a user to delete a VLAN which is associated with an interface.

When encountering this issue, the user would see an error message similar to "VLAN ID [xx] cannot be removed, in use by edge [b1-edge1 (GEx-disabled]".

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 the 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 82095: User can configure invalid device settings for Edge VLANs that will result in significant connectivity issues for the Edge.

The Orchestrator is not attempting to validate device configurations. In particular, a VLAN configuration for a switched port with an empty table. Some configurations can be so full of errors that the Edge's management process will fail.

Workaround: Review all VLAN Device settings and ensure they are valid as the Orchestrator is not checking.

Issue 82680: For customer using MT-GRE Tunnel Automation, when a user turns off the Cloud-to-Cloud Interconnect (CCI) flag on a Arista SD-WAN Gateway which is configured to use CCI, the Zscaler MT-GRE entries may not get deleted from the Zscaler portal consistently.

After a CCI site has been deleted from the Gateway, the entries for this site should also be removed. This issue has only been seen during test automation and has not been reproduced manually, but remains a risk.

Workaround: Manually delete the resource from Zscaler before retrying.

Issue 82681: For customer using MT-GRE Tunnel Automation, when a user turns off the Cloud-to-Cloud Interconnect (CCI) flag on a Arista SD-WAN Gateway which is configured to use CCI, and the user deactivates the CCI flag from a Arista SD-WAN Edge with CCI configured which is using a Zscaler Cloud Security Service, the Zscaler MT-GRE entries may not get deleted from the Edge or from the Zscaler portal.

After a CCI site has been deleted from the Gateway, the entries for this site should also be removed. This issue has only been seen during test automation and has not been reproduced manually, but remains a risk.

Workaround: Manually delete the resource from Zscaler before retrying.

Issue 103769: An Operator may observe that a Arista SASE Orchestrator in a large scale deployment is experiencing performance issues which include 100% disk utilization and the Orchestrator no longer accumulating logs.

This issue arises a change in logging behavior for the 5.1.0 Orchestrator that may result in the folders that store logs becoming full and also causing the Orchestrator CPU to reach 100% utilization. This issue arises a change in logging behavior for the 5.1.0 Orchestrator that may result in the folders that store logs becoming full and also causing the Orchestrator CPU to reach 100% utilization.

Workaround: A Superuser Operator needs to log into the Orchestrator and clean up the pending logs.

Issue 117699: An Operator attempting to upgrade a 4.2.x Arista SD-WAN Orchestrator to become a Release 5.2.0 SASE Orchestrator may observe that the upgrade fails.

The upgrade does not succeed, effectively stuck at the "Waiting for the CWS service up...". This issue is limited to 4.2.x Orchestrators.

Workaround: The workaround for this issue is to upgrade the 4.2.x Orchestrator to 4.5.1 first, and then to Release 5.2.0.0.

Issue 125082: If a user configures a Arista SD-WAN Edge with an overridden DNS Server IP address on a VLAN, and then changes an interface setting for the Profile that Edge is using, the DNS Server IP address is no longer present for the Edge VLAN.

The New UI does not send the override flag inside of the DHCP section and this causes any Profile changes to trigger an override of the DHCP section.

Workaround: There is no workaround for this issue.

Issue 125504: If a static route is configured with next hop as a VLAN with IPv4/IPv6 address at the Profile level and then overridden at the Edge level and add an IPv4/IPv6 address to the VLAN, the static route is not marked as N/A and the Arista SASE Orchestrator asks for the interface in a drop-down menu.

The expected behavior is where a static route configured with a next hop as a VLAN with IPv4/IPv6 address, the Orchestrator does not ask for the interface and the route is marked as N/A.

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 126421: For Partners using a Partner Gateway, when configuring the Hand Off Details, the "Use for Private Tunnels" option is always checked no matter what a user does.

This is not a cosmetic issue as the Orchestrator will apply the **Use for Private Tunnels** configuration to the Partner Gateway handoff and can impact customer traffic using the Partner Gateway.

Workaround: There is no workaround for this issue on an Orchestrator with only a New User Interface.

Issue 126425: When looking at Configure > Device > Routing & NAT page at the Profile level, the OSPF On/Off toggle button is missing.

The OSPF On/Off toggle button was not migrated to the New UI at the Profile level and only shows at the Edge level.

Workaround: There is no workaround for this issue on an Orchestrator with only a New User Interface.

Issue 126465: The Arista SASE Orchestrator UI is not applying changes a user makes to create an Edge Cluster.

If a user goes to the **Configure > Edge > High Availability** section of the UI and turns on HA with a Cluster type and creates a Hub Cluster with name xxxx, and saves changes, the user would observe that post-save the Cluster option is not selected under HA section and the created Hub Cluster with name xxxx is not present.

Workaround: There is no workaround for this issue on an Orchestrator with only a New User Interface.

Issue 126695: If a user is configuring webhooks for Alerts, when they click on the "Configure Payload Template" button the menu is not displayed.

This issue occurs when configuring webhooks on the **SD-WAN > Settings > Alerts > Webhooks** page of the UI. When looking at the browser console, a user would also observe the message: **ERROR TypeError: Cannot read properties of undefined (reading 'invalid')**.

Workaround: There is no workaround for this issue on an Orchestrator with only a New User Interface.

Issue 127152: Users cannot save modified Interfaces with OSPF configurations on the Arista SASE Orchestrator UI.

At the Profile level, when configuring either OSPFv2/OSPFv3, the Edit Interface dialog becomes invalid after changing any OSPF data.

Workaround: On an Orchestrator without a fix for this issue, a user would need to activate MD5 Authentication and change the Key ID to any number from 1 to 255, and then deactivate MD5 Authentication.

Issue 128070: When a user is configuring OSPFv3 for a VLAN at the Edge level and attempts to add IPv6 Settings to the VLAN, the Arista SASE Orchestrator UI does not save the changes.

The option to Save is grayed out and not available when attempting to add **IPv6 Settings** to a VLAN with OSPF3 at the Edge level.

Workaround: There is no workaround for this issue on an Orchestrator with only a New User Interface.

Issue 139854: On the Configure > Edge > Device > Interfaces page of the Orchestrator UI, when a user configures a route interface for IPv6, the UI does not treat the Gateway field as mandatory.

The user can leave the **Gateway** field blank and save the configuration, even though this IPv6 interface configuration will not work without a Gateway.

Workaround: Ensure the Gateway field is configured.

Issue 141194: For a customer deploying a Cloud Security Service (CSS), on the Monitor > Events page of the UI, the user may observe a "Related State Change Events" even message continuously despite there being no actual tunnel state change.

The user can observe that the CSS tunnel is up on the **Monitor > Network Services** page despite the spurious messages indicating otherwise.

Workaround: Ignored the messages and check the status on Monitor > Network Services.

Issue 145720: For an Orchestrator deployed with a Disaster Recovery (DR) topology, an Operator may observe that the Active Orchestrator upgrade fails, while the Standby succeeds.

The failure is traced to package *libssl1.0.0* failing to upgrade on the Active Orchestrator. which results in the Orchestrator upgrade failing. This issue is not observed on the Standby Orchestrator, as it successfully completes its upgrade.

Workaround: Failover the Standby Orchestrator to Active, and re-initialize a new DR Standby.