Release Notes

VeloCloud SD-WAN 6.1.0

Version 6.1.0

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 6.1.0 Release Notes

This document contains the following sections

Introduction

Arista VeloCloud 6.1.0 | 16th June 2025.

- Arista VeloCloud SD-WAN™ Gateway Version **R6101-20241210-GA**
- Arista VeloCloud SD-WAN™ Edge Version **R6101-20250527-GA-162396**
- Arista VeloCloud SD-WAN™ Orchestrator Version **R6103-20250319-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
- 6.1.0 is a Long-Term Support (LTS) Release Candidate
- Compatibility
- Upgrade Paths for Orchestrator, Gateway, and Edge
- New Hardware Platform
- New Features and Enhancements
- Important Notes
- Orchestrator API Changes
- Document Revision History

Recommended Use

This release is recommended for all customers who require the features and functionality first made available in Release 6.1.0.

Important:

Release 6.1.0 contains all fixes found in the 6.0.0 Release Notes as follows:

- All Edge and Gateway fixes up to build R6001-20240709-GA.
- All Orchestrator fixes up to build R6005-20240815-GA.

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

Arista VeloCloud SD-WAN/SASE introduced a Long-Term Support (LTS) policy to enhance the operational efficiency of our partners and customers during the implementation of new software. In continuation of this policy, the SD-WAN Release 6.1.0 is offered as an LTS Release Candidate.

For additional information about our Long-Term Support program see: *Arista VeloCloud SD-WAN/SASE Long-Term Support Release (326448)*.

Compatibility

Release 6.1.0 Orchestrators, Gateways, and Hub Edges support all previous Arista VeloCloud SD-WAN Edge versions greater than or equal to Release 4.5.0.

The following SD-WAN interoperability combinations were explicitly tested:

Orchestrator	Gateway	Edge	
		Hub	Branch/Spoke
6.1.0	5.2.3	4.5.2	4.5.2
6.1.0	6.1.0	4.5.2	4.5.2
6.1.0	6.1.0	6.1.0	4.5.2
6.1.0	6.1.0	4.5.2	6.1.0
6.1.0	5.0.1	5.0.1	5.0.1
6.1.0	6.1.0	5.0.1	5.0.1
6.1.0	6.1.0	6.1.0	5.0.1
6.1.0	6.1.0	5.0.1	6.1.0
6.1.0	5.1.0	5.1.0	5.1.0
6.1.0	6.1.0	5.1.0	5.1.0
6.1.0	6.1.0	6.1.0	5.1.0
6.1.0	6.1.0	5.1.0	6.1.0
6.1.0	5.2.3	5.2.3	5.2.3
6.1.0	6.1.0	5.2.3	5.2.3
6.1.0	6.1.0	6.1.0	5.2.3
6.1.0	6.1.0	5.2.3	6.1.0
6.1.0	5.2.4	5.2.4	5.2.4
6.1.0	5.2.4	5.2.3	5.2.3
6.1.0	6.1.0	5.2.4	5.2.4
6.1.0	6.1.0	6.1.0	5.2.4
6.1.0	6.1.0	5.2.4	6.1.0
6.1.0	5.4.0	5.4.0	5.4.0
6.1.0	6.1.0	5.4.0	5.4.0
6.1.0	6.1.0	6.1.0	5.4.0
6.1.0	6.1.0	5.4.0	6.1.0
6.1.0	6.0.0	6.0.0	6.0.0
6.1.0	6.1.0	6.0.0	6.0.0
6.1.0	6.1.0	6.0.0	6.1.0
6.1.0	6.1.0	6.1.0	6.0.0
6.1.0	6.1.1	6.1.1	6.1.1

Important:

Arista VeloCloud SD-WAN Releases 5.0.x, 5.1.x, 5.2.0 and 5.2.2 have reached End of Support for Gateways and Orchestrators.

- Releases 5.0.x, 5.1.x, 5.2.0, 5.2.2 Orchestrators and Gateways have reached End of General Support (EOGS) on February 28, 2025.

For more information please consult the Knowledge Base article: Announcement: *End of Support Life for Arista SD-WAN Release 5.x (381499)*

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

Important:

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

Upgrade Paths for Orchestrator, Gateway, and Edge

The following lists the upgrade paths for the Orchestrator, Gateway, or Edge from an older release to Release 6.1.0.

Orchestrator

Orchestrators using Release 5.2.0 or later can be only directly upgraded to Release 6.1.0.

Gateway

Upgrading a Gateway using Release 5.0.0 or later to Release 6.1.0 is fully supported for all Gateway types.

Important:

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

Edge

An Edge can be upgraded directly to Release 6.1.0 from Release 4.5.x or later.

New Hardware Platform

Release 6.1.0 adds support for the VeloCloud Edge 4100.

- The Edge 4100 supports up to 30 Gbps of throughput and can manage 6,000 tunnels.
- The Edge 4100 includes 10x 1-Gbps RJ45 and 8x 10-Gbps SFP+ interfaces, ensuring compatibility with both copper and fiber networks.

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

For a list of supported SFP modules for the Edge 4100, see *Arista VeloCloud SD-WAN Supported SFP Module List (312379)*.

New Features and Enhancements

Business Policy Enhancements

Adds an ability to match the Business Policy based on a source and destination IP address on the LAN side, prior to LAN-side NAT translation. This feature is for a customer with a network topology which includes internal IP addresses that adhere to different business policies and as a result need to match the business policy based on the pre-NAT IP address.

DNS Cache Flush Support for Edges

The new **Flush DNS Cache** remote diagnostic test improves the reliability of domain-based business policies. Previously, only DNS cache entries with a time to live (TTL) of 0 were removed every 10 minutes, while deep packet inspection (DPI) based entries remained cached for 24 hours, blocking new entries from being learned. This test clears all cache entries, ensuring space for new entries and more reliable DNS lookups to support domain-based policies.

Edge Troubleshooting Improvements

These enhancements have been added to improve the troubleshooting of Edge field issues:

- Packet Capture (PCAP) filters support for Edges. You can now optionally configure filter parameters for the PCAP request through the Edge Diagnostics Bundle page.
- Remote Diagnostic improvements for IPv4 and IPv6 Route Table Dump tests. Two fields: "Preference" and "Order" are added to the log output table that helps to check route preference and order.
- Diagnostic Bundle improvements to support longer retention of log files and handling of large core files in the diagnostic bundle.
- Two new syslog events (BGP_NEIGHBOUR_UP and BGP_NEIGHBOUR_DOWN) are generated when the BGP neighbor goes up or down, respectively.

Enhanced Firewall Services Security Reporting

You can generate secure SD-WAN Enterprise reports for the analysis of your network. The secure SD-WAN Enterprise report PDF includes overall Network and Security Summary, IDS/IPS, URL Filtering, and Malicious IP related data collected from all Enhanced Firewall Service (EFS) engines (IDS/IPS, URL Filtering, Malicious IP) if EFS is activated at the customer level.

Live Flow Visibility

Phase 1 introduced Flow Visibility, the ability to visualize traffic flows and comprehend the flow patterns within the network. Phase 2 adds a **Live Mode** to the **Monitor > Flows** page, which provides the ability to monitor flows for troubleshooting. The **Monitor > Flows** page can compare up to 4 flows, provides historical views of the flows, and provides the ability to view all the attributes of the live flows.

High Availability Failover Pre-Emption

The High Availability (HA) process chooses the Active Edge device based on which Edge has the most LAN and WAN interfaces. However, this logic can cause frequent and unnecessary failovers if the interfaces frequently go down and come back up (also known as "flapping"). To address this potential issue, a new advanced setting is added to Release 6.1.0: **Pre-empt Switchover**. When enabled, this setting pre-empts an HA switchover/failover where there is LAN or WAN degradation as long as the Active Edge has at least one WAN port and one LAN interface up.

Multiple Identity Providers (IdP) for Orchestrator Single Sign On

This feature allows Partners and Service Providers the option to login as Operators on their Dedicated Orchestrator using Single Sign On (SSO). Previously, since a Dedicated Orchestrator is managed by Arista, the Edge Operations team already configured their own SSO IdP for logging in, and this forces the Partner to rely on Native Authentication (username/password) to login as an Operator user. With this feature, Arista can allocate an additional IdP for the Partner or Service Provider.

Ability to Run OSPF on a Non-Global Segment

Adds support for OSPF on non-Global segments includes enabling OSPF at both the Profile and Interface levels, with compatibility for OSPFv2 and OSPFv3. Additionally, OSPF can be enabled on subinterfaces, and OSPF-specific debug and Remote Diagnostic commands now include a filter for segments.

Note:

- BFD with OSPFv2 is not supported on non-Global Segments
- BFD with OSPFv3 not supported on Global or non-Global Segments

Security Administrator Role Customization

Adds additional privileges while resolving various issues with Security Administrator role customization.

Symantec Web Security Service (WSS) Integration (PoP-to-PoP)

This feature brings low latency, high throughput, and high availability connectivity to Symantec WSS via a multi-tenant Geneve tunnel established between the VeloCloud Gateway and Symantec WSS in GCP PoPs. Customers can configure a Business Policy to send traffic to Symantec WSS for inspection using this new feature as an alternative to the Non SD-WAN Destination via Edge capability.

Unique WAN MAC Address in High Availability Deployments

Customers deploying Virtual Edges in a High Availability topology can retain the original MAC address on the HA Edge's WAN interfaces. This feature joins the previously added Unique MAC Address for the HA Edge LAN interfaces.

Wi-Fi Radio Settings

The Wi-Fi radio setting for a Profile is improved to enable selection of dual radio frequency bands (2.4 GHz and 5 GHz).

Important Notes

High Availability Standby Monitoring Merged With System Tab

A High Availability (HA) site previously had a separate page for monitoring the Standby Edge health statistics under the **Edge > Monitor > Standby Edge** page. With Release 6.1.0, the Standby Edge tab is merged into the **Edge > Monitor > System** page. On the **System** page, a user can toggle between the Active and Standby Edge health statistics.

SD-Access Client Connector on Edge Preview

VeloCloud is launching a technical preview of SD-Access Client Connector on the SD-WAN Edge. Using our single pane of glass (VeloCloud Orchestrator), an administrator can install and manage the SD-WAN Client Connector on their VeloCloud Edge devices. The SD-Access users and machines can then access resources in the network via the SD-WAN Edges.

CAUTION:

Feature previews are intended for customers to perform lab or proof of concept testing only. This feature is not recommended for use in a production environment. The GA version of SD-Access Client Connector on Edge will be announced in a future release.

Removal of the Classic UI Option

The 6.1.0 Orchestrator removes the option to switch between the New UI and the Classic UI, with the New UI being the sole option.

SMS Behavior Changes

A VeloCloud Hosted Orchestrator utilizes an SMS service for the following functions to communicate with users: Two Factor Authentication; Password Reset; and System Alerts.

To improve the efficiency of the SMS messages, the following changes are implemented in the 6.1.0 Orchestrator:

- Long subjects crossing 100 characters will be truncated with an ellipsis (...) at the end.
- From the alert SMS body, the following contents are removed:
  - Last contact
  - Alert Triggered

- Message

- The Orchestrator URL is replaced by the Orchestrator DNS.
- A new field called *alert Id* is added to the SMS message.

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

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

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

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

Orchestrator API Changes

Developer Documentation

VeloCloud SD-WAN API documentation resides on the Developer Documentation Portal:

- **API v1 https://www.arista.com/en/support/software-download/velocloud**
- **API v2 https://www.arista.com/en/support/software-download/velocloud**

Orchestrator API Changes since 6.0.0

Category	Affected APIs	Comments

P5G Service (Private Mobile Network (PMN)) removed from Orchestrator	`/enterprise/cloneEnterpriseV2 /enterprise/insertEnterprise /enterpriseProxy/insertEnterpriseProxyEnterprise / enterpriseProxy/getEnterpriseProxyEnterprises / enterpriseProxy/getEnterpriseProxyCapabilities / network/getNetworkEnterprises`	Incompatible request parameters
		• Post change: /enterprise/cloneEnterpriseV2
		  • missing request param: serviceLicenses/P5G/enabled (in: body, type: boolean)
		• Post change: /enterprise/insertEnterprise
		  • missing request param: serviceLicenses/P5G/enabled (in: body, type: boolean)
		• Post change: /enterpriseProxy/insertEnterpriseProxyEnterprise
		  • missing request param: serviceLicenses/P5G/enabled (in: body, type: boolean)
		Incompatible response attributes
		• Post change: /enterpriseProxy/getEnterpriseProxyEnterprises
		  • missing attribute from 200 response: []/serviceLicenses/P5G/enabled (in: body, type: boolean)
		• Post change: /enterpriseProxy/getEnterpriseProxyCapabilities
		  • missing attribute from 200 response: enablePmn (in: body, type: boolean)
		• Post change: /network/getNetworkEnterprises
		  • missing attribute from 200 response: []/serviceLicenses/P5G/enabled (in: body, type: boolean)

Client Connector on Edge	`/edge/getEdgeConfigurationModules`	Incompatible Response Attributes
		• Post Change: /edge/getEdgeConfigurationModules
		  • missing attribute from 200 response: static[]/wanInterface (in: body, type: string)
		  • missing attribute from 200 response: staticV6[]/wanInterface (in: body, type: string)

Category	Affected APIs	Comments
Gateway API Optimization	`/enterpriseProxy/getEnterpriseProxyGateways / network/getEligibleReplacementGateways /network/getNetworkGateways`	For performance improvements, the API has been updated to fetch optional fields ONLY when explicitly requested for. A new field withOptionalColumns has been added for the caller to pass the list of fields that are to be fetched. By default, these fields will not be returned. withOptionalColumns is an array of strings with possible values as listed below: `['connectedEdgeList','ipsecGatewayDetail','utilizationDetail','dataCenterVpnStates','handOffDetail']` Example: withOptionalColumns: [' **connectedEdgeList'**, ' **ipsecGatewayDetail'**, ' **utilizationDetail'**]

Zero Touch Provisioning (ZTP)	`/vcoInventory/pushActivationSignUp`	ZTP sign-up page and /vcoInventory/ pushActivationSignUp API is updated to work with ERP numbers instead of SIDs (for customers) and PRM IDs (for partners). The changes are needed since Broadcom uses ERP number instead of SIDs and PRM IDs that were used by Arista.
		• Post change: /vcoInventory/ pushActivationSignUp
		  • new required request param: erpNumber
		  • missing request param: sid (in: body, type: string)
		  • missing request param: prmId (in: body, type: string)

Document Revision History

June 16th, 2025. Eighth Edition.

- Added Fixed Issue **#162396** in the Edge **R6101-20250527-GA-162396 Resolved Issues** section.

May 12th, 2025. Eighth Edition.

- Added fixed Issues **#153444, #154079** and **#159845** in the Edge **R6101-20250305-GA-154079 Resolved Issues** section.

March 26th, 2025. Eighth Edition.

- Added a new Orchestrator rollup build **R6103-20250319-GA** to the **Orchestrator Resolved Issues** section. This is the third Orchestrator rollup build and is the new default Orchestrator GA build for Release 6.1.0.

- Orchestrator build **R6103-20250319-GA** includes the fix for issue **#135926**, **#139617,#157604** and **#160641**each of which is documented in this section.
- Added Fixed Issue **#155521** to the Orchestrator Resolved Issues section for the **R6102-20250304-GA** build.

March 12th, 2025. Seventh Edition.

- Added Fixed Issue **#154404** to the Orchestrator Resolved Issues section for the **R6102-20250304-GA** build.

March 6th, 2025. Sixth Edition.

- Added a new Orchestrator rollup build **R6102-20250304-GA** to the **Orchestrator Resolved Issues** section. This is the second Orchestrator rollup build and is the new default Orchestrator GA build for Release 6.1.0.
- Orchestrator build **R6102-20250304-GA** includes the fix for issue **#136219**, **#153298**, **#153373**, **#153911**, **#154709**, **#154711, #156729, #156801, #157063, #157156, #157196, #157340**, **#157375, #157545, #157796, #157911, #158030, #158462,** and **#158648** each of which is documented in this section.

February 5th, 2025. Fifth Edition.

- Added supportability matrix of Orchestrator: R6.1.0.0 and VCG:R5.2.4.x Branch/Spoke: R5.2.3.x.

December 28th, 2024. Fourth Edition.

- Added a new Orchestrator rollup build **R6101-20241218-GA** to the **Orchestrator Resolved Issues** section. This is the first Orchestrator rollup build and is the new default Orchestrator GA build for Release 6.1.0.
- Orchestrator build **R6101-20241218-GA** includes the fix for issue **#94634**, **#149038**, **#150366**, **#150727**, **#153402**, **#153850, #153957** and **#154850** each of which is documented in this section.

December 19th, 2024. Third Edition.

- Adds a new Edge/Gateway rollup build **R6101-20241210-GA** to the Edge/Gateway Resolved Issues section. This is the first Edge/Gateway rollup build and is the new default Edge/Gateway build for Release 6.1.0.
- The Edge/Gateway build **R6101-20241210-GA** includes the fixes for issues **#152668**, **#153643**, **#153839,** and **#153988** which are documented in this section.

November 12th, 2024. Second Edition.

- Revised the section **6.1.0 is a Long-Term Support (LTS) Release Candidate** to change it from LTS Release to LTS Release Candidate.
- Added a link to the Supported SFPs KB article for the **New Hardware Platform** section for the Edge 4100.
- Revised the **Upgrade Paths for Orchestrator, Gateway, and Edge** section to change the Orchestrator direct upgrade path from 5.4.0 to 5.2.x. In other words, a customer/partner can upgrade their on-premises Orchestrator directly from 5.2.x to 6.1.0.

November 7th, 2024. First Edition.

Edge/Gateway Resolved Issues

Resolved in Edge Version R6101-20250527-GA-162396

Edge version R6101-20250527-GA-162396 was released on 06-16-2025 and is the updated GA build for Release 6.1.0. This build replaces the previous GA build R6101-20250305-GA-154079. This Edge build addresses the below critical issue since R6101-20250305-GA-154079.

> **Important:**
>
> **Customers must only use the R6101-20250527-GA-162396 build and not use R6101-20250305-GA-154079.**

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 Version R6101-20250305-GA-154079

Edge version R6101-20250305-GA-154079 was released on 05-02-2025 and is the updated GA build for Release 6.1.0.

This build replaces the previous GA build R6101-20241210-GA. This Edge build addresses the below critical issue since R6101-20241210-GA.

> **Important:**
>
> **Customers must only use the R6101-20250305-GA-154079 build and not use R6101-20241210-GA.**

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

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

Fixed Issue 154079: Post upgrade the private tunnels between High Availability HUB and spokes may not be formed.

When the High Availability HUB gets upgraded, the standby gets upgraded first followed by the active. The spoke retains the tunnel context created in older release, when the HUB's standby is being upgraded with newer software version. Post HUB upgrade, the spoke tries to re-establish the tunnels with the older tunnel context and so the path is always down. As a fix, disconnect the TD when such a peer software version mismatch is seen.

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

Due to recent change in the suricata rules metadata by NSX, impact score calculation went wrong for some of the INFO level alerts. This does have impact only on the monitoring and not on the traffic.

Resolved in Edge/Gateway Version R6101-20241210-GA

Edge/Gateway version R6101-20241210-GA was released on 12-19-2024 and resolves the following issues since Edge/Gateway version R6100-20241030-GA.

Fixed Issue 152668: Lastline ATP not initialized on enabling EFS - IDS/IPS on HA Edge.

Lastline ATP fails to initialize on HA Edges when the IDPS EFS feature is enabled. The failure occurs due to a mismatch in the configuration time interval.

Fixed Issue 153643: Edge process exits sometimes while handling fragmented IP packets.

The Edge process may exit while handling fragmented IP packets. This is a timing issue and does not always occur.

Fixed Issue 153718:On enabling URL Filtering/Malicious IP EFS features, Edge does not download URL/IP DB from NTICS endpoint. As EFS is enabled, but DB is not downloaded, it starts to drop traffic.

As part of the GCP migration, NTICS was migrated from AWS to GCP. This resulted in DB download failure due to an extra backspace character in the Authorisation header of HTTPS POST requests. Once that was fixed, the HTTP response from NTICS was missing the content-length. The same is fixed by removing the backspace character and computing content-length in advance.

Fixed Issue 153839: A gateway crash occurs when a VCMP backup link message is received over a VCMP tunnel.

A gateway crash occurs when a Virtual Clustered Multiprocessing (VCMP) backup link message is received over a VCMP tunnel. The crash occurs as a result of a timing issue.

Fixed Issue 153988: SRIOV (x710, xL710, 82599) based nics not bound properly to DPDK drivers after vc_procmon or GWD restart on a Gateway.

SR-IOV (x710, xL710, 82599) based NICs may not be properly bound to DPDK drivers after **vc_procmon** or **GWD** restarts on a gateway. The DPDK driver bind/unbind logic for PCIe devices was updated to use **driver_override** instead of the device ID and vendor ID combination.

Resolved in Edge/Gateway Version R6100-20241030-GA

Edge/Gateway version R6100-20241030-GA was released on 11-07-2024 and resolves the following issues since Edge/Gateway version R6001-20240709-GA.

Note:

This means that a fix for an Edge or Gateway issue listed in the 6.0.0 Release Notes up to the listed build is included in all Release 6.1.0 builds.

Fixed Issue 69247: BGP neighbor events are missed in the Orchestrator's Monitor pages if the BGP flaps happen in quick succession over less than 30 seconds.

When BGP sessions flap in a short interval, these are not captured in the Orchestrator's monitoring page. This is a result of the Edge's BGP process polls BGP states every 30 seconds and if there is a state change from a previously recorded state only then is the user notified to the Orchestrator.

Fixed Issue 96353: If a 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 only with an IPv4 link, with an IPv6 link added only later. 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 does not add the IPv6 address to the file and so if the IPv4 link is removed, the Edge loses connectivity to the Orchestrator.

Fixed Issue 103367: When a user tries to activate an LTE Edge with cellular only, the activation may fail.

In particular, a customer can encounter this issue when a user tries to set the APN (or username, SIMPIN, network for LTE modems) from the Orchestrator at the time of activation, the Edge activation fails.

For an LTE Edge without a fix for this issue, the workaround is to program the APN on the SIM either by using the Edge CLI (/etc/modems/modem_apn.sh <CELL1/CELL2> set <theAPN>). Or by any other eternal method like connecting the SIM to a laptop and programming it. After programming this, do not override the settings on the Orchestrator and generate the activation link.

Fixed Issue 110283: Multiple user-defined WAN links still use the interface Rx rate for link selection.

Bandwidth based link selection considers the WAN links with least Rx rate as the best. The process uses the Rx rate of the underlying interface. As a result, the process cannot differentiate between the actual Rx rate for a specific link if there are multiple user-defined links for an interface. The fix uses the Rx rate of the WAN link instead of the interface.

Fixed Issue 111425: On an Edge model 680, the customer may observe up to a 43% throughput drop when IDS/IPS on the Enhanced Firewall Service is enabled.

In throughput tests for the Edge 680, when the Edge is subjected to an intrusion, the Enhanced Firewall takes a global flow table lock to lookup flows and then perform an inspection. The Enhanced Firewall also internally streams a depth setting which today assembles packets up to 1MB worth of data and does the signature matching. Post that any more packets are not used for signature matching. Due to the global lock, we see the throughput drop.

Fixed Issue 113600: A user may observe that the Event, "New client device seen" is not seen for DHCP clients connected via a DPDK routed interface.

The DPDK interface driver directly transmits DHCP ACK packets that are sent via the kernel onto the wire and does not give an opportunity to the DHCP analysis module in the Edge process to inspect the packets and generate the "New client device seen" message.

Fixed Issue 118704: A customer may observe that the Edge is not measuring accurate values for latency.

The values would be abnormally high when measured between the Edge and the Gateway and are the result of running the clock synchronization process in repetitive intervals, resulting in the clock sync process not moving which results in the abnormal latency observed.

Fixed Issue 120007: For a customer site deployed with a High Availability topology, the customer may observe an event for an Edge restart of the Standby HA Edge because it experienced a Dataplane Service failure and restarted to recover.

The issue can occur if NetFlow is enabled on the Standby Edge as this can result in a memory build up that ultimately triggers the Edge service failure. The core file would include a mutex_mon log in the chat_stats.

Fixed Issue 123236: A user may observe that a Gateway's device ID has a MAC address with all zeroes.

A newly deployed Gateway with no interface named eth0 will encounter this issue. The Gateway defaults to using the MAC address of eth0 as its device ID. If eth0 is missing or renamed, the Gateway's device ID defaults to 00:00:00:00:00.

Fixed Issue 123379: For a customer site deployed with a High Availability topology, the customer may observe an event for an Edge restart of the Standby HA Edge because it experienced a Dataplane Service failure and restarted to recover.

When an user tries to configure an IPv6 address on subinterfaces across 128 segments using a script, the configurations get accumulated in a queue causing a Edge service to fail. Issue is applicable only on HA scenarios on the Standby Edge.

On an HA Edge without a fix for this issue, it is advised to interleave the IPv6 address configurations on the subinterfaces on 128 segments so that the system has time to process and apply the configurations.

Fixed 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 allowed list of interfaces to process for the *snmp-request*.

Fixed Issue 130326: When a customer deploys a Cloud Security Service with redundant tunnels (in other words, active and standby) and L7 Health Check is toggled on, he secondary tunnel L7 state shows as up even if the tunnel is down on the Orchestrator's Edge tunnel monitoring page.

The Orchestrator displays L7 health information for standby CSS tunnels, even though the Edge is not building a standby CSS tunnel unless it is needed, it is thus impossible to do an L7 health check through non-existent tunnels. However, despite this the Edge sends this false information to the Orchestrator which is then displayed in the UI's Monitor section.

The issue is the result of the Edge erroneously initializing the L7 state with a default "Up" value instead of the correct "Unknown" value.

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 andvc_mtgre_driver_destroy*.

Fixed Issue 132004: For a customer enterprise site deployed with a High Availability topology, the Standby Edge may send management traffic (VCMP) not destined for its IP Address/MAC Address back to the Virtual Private LAN Service (VPLS), resulting in unicast flooding.

Since there is no destination MAC check for unicast packets received on a Standby Edge, the Edge processes these VCMP packets as valid packets destined for it, updates the TTL and sends it back, and this causes the unicast flooding.

Fixed Issue 133678: If a 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 does not add the IPv6 address to the file and so if the IPv4 link is removed, the Edge loses connectivity to the Orchestrator.

For an Edge without a fix for this issue, the 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.

Fixed 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 client requested IP address field. This was misinterpreted as an IP address change and the Orchestrator events were triggered unnecessarily with an incorrect IP address. The issue is cosmetic but can cause user confusion when seeing an IP address they do not recognize.

Fixed Issue 134332: For a 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 and also when the flow version is updated.

Fixed Issue 134799: For customers subscribed to the Enhanced Firewall Service, if the user toggles the Enhanced Firewall Service status, they may observe that it takes longer to apply the firewall configurations.

When the IDS/IPS status changes, the Edge service is restarted. If the webroot SDK RTU download is also occurring, the Edge waits until it finishes its current task before the exit is called.

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 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 Gbps. This issue can be specifically observed when checking the Edge under *dpdk_ports_dump* or in the matching diagnostic bundle log.

Fixed Issue 136949: After an Edge restarts, it may be missing Branch to Branch routes from its RIB and FIB, resulting in some customer traffic disruption.

This issue is caused by a delay in processing the 'tunnel up' event towards the Gateways immediately after an Edge service restart. The result is routes being received from the Gateways and the stale PI timer starts right after, which removes the routes from the Edge's Routing Information Base (RIB) and Forwarding Information Base (FIB) post 5 on expiry of a stale PI timer of 5 minutes.

If experiencing this issue on an Edge without a fix for this issue, the routes need to be re-initiated.

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

When a 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.

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

Fixed Issue 138464: On a customer enterprise site using a High Availability topology, a user may observe high memory utilization of the Standby Edge or even see an Event where the Standby Edge restarted due to high memory usage.

With this issue, Standby Edge memory utilization increases rapidly when the HA Edges 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 Standby Edge's service defensively restarts to recover memory. In an Enhanced High Availability topology this can cause customer traffic disruption for the part that the Standby Edge is handling through its WAN link(s).

On an HA Edge without a fix for this issue, a user should consult the **Monitor > Events** page for that HA Edge, monitor the memory utilization threshold limit warning Event or monitor memory utilization on the **Monitor > HA Standby** page and reduce the number of concurrent connections per second to maintain the memory utilization to less than 60%.

Fixed Issue 138949: If an Edge is configured with a DHCP server for LAN clients with options 66 and 67 enabled, after the Edge software is upgraded from 5.1 or older to 5.2 or later, DHCPOFFER messages are no longer sent with the fields sname/file (server name/filename) populated.

If a DHCP client requires the information from the sname/file fields in the DHCPOFFER message to boot, the DHCP client may not be able to boot after the edge is upgraded from release 5.1 or older to release 5.2 or later.

Fixed Issue 139049: When an Edge is configured as a DHCP server for LAN clients, after a software upgrade from release 5.1.x or older to release 5.2 or later, DHCPOFFER messages are no longer sent with the fields sname/file (server name/filename) populated.

DHCP options 66 and 67 are not sent after an upgrade to software version 5.2.x or later. If a DHCP client requires the information from the sname/file fields in the DHCPOFFER message to boot, the DHCP client may not be able to boot after the Edge is upgraded from release 5.1 or older to release 5.2 or later.

Fixed Issue 139622: For customers using Edge Network Intelligence, there may be a discrepancy between the statistics shown on the SASE Orchestrator and the Edge Network Intelligence portal.

Sometimes traffic is misclassified from the Analytics perspective and this results in the Analytics metadata being dropped on the Edge Network Intelligence back-end.

Fixed 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.

On a site where the Edges do not have a fix for this issue, perform a network service restart to repopulate the default routes

Fixed Issue 139860: Packets may not be forwarded properly between switched ports belonging to the same VLAN on an Edge 520/540 or Edge 610.

On platforms with a Marvell switch (Edge 520/540 and Edge 610), VLANs containing certain combinations of tagged and/or untagged ports do not forward traffic properly between ports, because the switch is not programmed properly.

Fixed Issue 139936: Client users may observe that there is instability in traffic between Edges and the Gateway.

Unstable and Unusable hold off seconds and loss percentages can be abnormally high. The issue is the result of a rmsg corruption between 4.5.x Edge and a 5.x Gateway, abnormally high junk values can be set for the management traffic hold off seconds and loss percentage. As a preventive fix, the path thresholds are sanitized before assignment.

Fixed Issue 140919: A change made to the Address Group or Port Group used by a current Firewall or Business Policy rule may not affect traffic established prior to the rule modification.

Traffic which is expected to match a particular Firewall or Business Policy rule after a change to either the Address Group and/or Port Group fails to match the rule. This results in inconsistent behavior as new traffic will match the modified rules but existing traffic with the same parameters do not match the rule.

Fixed 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.

On an Edge without a fix for this issue, ensure that any configured PPPoE link is capable of coming up, in other words ensure the peer PPPoE server is enabled.

Fixed 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 a L2 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**.

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.

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, the Standby Edge immediately takes the active role based on a higher LAN/WAN interface count. Due to a timing issue, 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 higher 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 141770: For an Edge where non-preferred and user-defined WAN links have their bandwidth statically set, those values can get overwritten.

Generally links with non-preferred (referring IP address family preference for tunnels in the interface configuration) IP address family gets the bandwidth calculated from the link with the preferred IP address family. If a user has configured a static bandwidth explicitly for links with the non-preferred IP family, the Edge may change this value.

Fixed Issue 141877: For a Partner Gateway operating at high scale may experience a Dataplane Service failure with a mutex monitor type.

High scale is understood as a Gateway used by 100 customers where each customer has 10 Edges, 600 BGP sessions and each customer has 16 segments and BGP is configured on the first 6 VRFs, for a total of 1600 VRFs. In this scenario, a mutex monitor type service fails because the configuration thread holds a lock for a long time and other threads are contending for it. This triggers the mutex monitor exception and Gateway service failure.

Fixed Issue 141929: A Gateway may experience a Dataplane Service failure and restart to recover when there is WAN link flapping and high loss.

The Gateway service fails while attempting to access an old packet. The Gateway interface structure associated with any packet is released from a garbage collector routine. If any packet stays far longer than the usual life, the Gateway service can fail while accessing the interface structure associated with the packet. This issue is fixed with the changes to complete processing packets reliably on time.

Fixed Issue 141943: An Edge 3800 running at maximum scale may experience memory consumption issues to the point of frequently triggering defensive Edge service restarts to recover the memory.

Maximum scale is understood as an Edge 3800 with 3.8M Edge to Edge flows and 4K peers, 6K tunnels, and 100K routes. Under those conditions the Edge 3800's memory utilization reaches 75% and triggers a restart which is repeated until the flows are reduced to below maximum scale.

Fixed Issue 141963: All traffic from the LAN to the WAN will be duplicated when it reaches the Edge. Specifically, the Edge will receive a copy of the packet on both the br-network1 and vce1 interfaces and will forward both to the WAN.

This will happen when IPv4 is configured on the LAN; only IPv6 is configured on the WAN (in other words, IPv6 is disabled on all interfaces on the Edge via the Orchestrator); and the Edge is sending IPv4 over IPv6 traffic.

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 142789: A user may observe an abnormally large value for the Tx/Rx rate for a WAN link.

The issue is the result of a flawed Rx/Tx rate calculation process which did not check for bad and/or negative values during the calculation.

Fixed Issue 143079: An Edge may experience a kernel panic due to an OS memory exhaustion and reboot to recover.

The processes that handle the Edge's system status may accumulate memory usage to a level that leads to the Edge's OS experiencing an Out of Memory event which triggers the kernel panic.

Fixed Issue 143329: Routes are removed from Forwarding Information Base (FIB) but present in the Routing Information Base (RIB) resulting in issues with customer traffic using those missing routes.

During the issue state the dead peer timer (120 secs) is invoked for the remote Spoke Edges via the Hub Edges, resulting in the routes being removed from the FIB. When the remote reachability for a destination Spoke Edge via the Hub Edge is received, the SD-WAN service checks for the reachability and if it is down, the route is added to the dead peer list.

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 143432: Operator and Partner Administrators may observe memory leaks on Gateways.

```
The leaks stem from situations where the IKE DS allocation fails and the Gateway service does
 not free the conf pointer. Also if source and destination JSON subnet parsing fails, then the
 allocated memory will not match the actual number of subnets, a memory leak occurs as well.
```

Fixed Issue 143447: Default route advertisement is not affected by a "propagate over uplink" configuration.

When "conditional default originate" (found when configuring BGP advanced settings) is enabled with a default remote route present, the default route is not withdrawn when "propagate over uplink" is disabled if it was advertised already, nor is it advertised if it was not already advertised.

A user encountering this issue on an Edge without a fix for this issue should disable "propagate over uplink".

Fixed Issue 143479: For a customer using the Enhanced Firewall service, when IDS/IPS is enabled on an Orchestrator where a non-zero spread factor is set, traffic gets dropped.

When IDS/IPS is enabled/disabled,the Edge goes for service restart. In the customer case, IDS/IPS was enabled and the restart of the Edge service happened when the IDS/IPS signature bundle download was half-way. The download failed and was not retried after the Edge service came up again. Due to a scale factor configured on the Orchestrator, the latest atpMetadata configuration comes again only after some time and in the meantime all of the traffic to the Edge is dropped.

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 143575: On the Edge 610 and 610-LTE, in some configurations, large, fragmented packets result in the full-sized fragments being dropped on the Gigabit Ethernet ports.

If any of the interfaces is set to a non-default MTU (i.e. not 1500), then the MTU of the interface from the hardware switch that backs the 6 GE ports to the CPU gets an incorrect MTU applied, resulting in full 1500-byte packets or fragments being dropped.

The workaround for this issue is to set at least one of the GE ports to an MTU of 1504.

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 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 143758: In rare instances, an Edge or Gateway may experience a Dataplane Service failure and restart as a result.

When an IKE thread between an Edge and a Gateway deletes the IKE DS but for some reason IPSec netif pioneer has not been created there is the potential for a Gateway or Hub Edge service failure.

If an IKE thread cannot find TD or the found TD is in DEAD state then IPSec netif interface won't be created. When this particular IKE DS is deleted it will try to free the netif pointer, which is not allocated. This can trigger an exception in either an Edge or Gateway service and cause the failure.

Fixed Issue 143901: An operator or partner administrator may observe that after a Gateway is upgraded, some interfaces may fail to come up.

Post-Gateway software upgrade, the system may need to reboot. It would ask for user input. If input is not provided as "Y" or "N", the system will not be restarted. The fix provided will automatically reboot the system if no user input is provided.

Fixed Issue 143972: After running the --nat_db_flush command on the Edge, any dynamically allocated ports for NAT'd flows will be orphaned and not cleared.

When running the *--nat_db_flush* command, dynamically allocated ports for vc_nat_src or vc_nat_src_dst (as used by Direct NAT, etc) are not released, resulting in stale NAT port entries.

Fixed Issue 144042: For a customer enterprise using Cluster-to-Cluster interconnect, a cluster member may prefer a Cluster-to-Cluster overlay route instead of a shorter underlay route for its own Spoke Edge when the Spoke Edge is connected to two clusters.

In the case of cluster Overlay Routes learned from the directly connected Spoke Edges and advertised to the underlay to the other Cluster members via BGP, these routes should be preferred over the other overlay routes learned on the peer. However, with this issue, this is not occurring.

Fixed Issue 144143: On a site deployed with a Standard High Availability topology, if the HA link is down, the Orchestrator will report the Standby Edge state as "Unknown".

This is not an expected result as the Standby Edge status can be verified through a heartbeat packet confirmation through a WAN link.

Fixed Issue 144180: For a customer subscribed to the Enhanced Firewall service, a may observe on the Monitor > Security page shows IDS/IPS statistics even though these features are not enabled.

The Orchestrator UI shows IDS/IPS statistics even if IDS/IPS is not enabled at the rule level but is enabled at the security feature level.

Fixed Issue 144253: For a customer site configured with a High Availability topology, a user may observe that the source MAC address is set to zero on an ARP probe packet sent from the Standby Edge.

This issue can impact the HA Loss of Signal (LoS) feature. On an HA enabled Edge, the original hardware address is set to zero and due to this the HA WAN heartbeat packet and ARP packet is sent with a source MAC address as zero.

Fixed Issue 144258: In an Edge, a Self route is shown as reachable when the corresponding interface is down.

Currently a self-route is considered reachable irrespective of the status of the corresponding interface in an Edge. So a self route is shown reachable even if the corresponding interface is down.

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 144497: When there is a Non SD-WAN BGP peer configured and a /32 static subnet for the peer IP address, the BGP session may not come up after a restart.

The static subnet may have been required in older SD-WAN software releases to reach the BGP peer. But in later releases, when a BGP peer is configured, a /32 'p' route is installed automatically. This issue can happen if a static IP address is configured after configuring a BGP peer as well.

For customers using a Gateway without a fix for this issue, modify the BGP peer IP address to some random value and then back to the correct value. When this is done, the static route goes away and the BGP 'p' route is installed in the Forwarding Information Base.

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 145305: WebEx traffic is being incorrectly classified as ShoreTel, which can impact customers with business policies for either application.

The application map definition of ShoreTel includes UDP 5004. However, this port is no longer used by ShoreTel but is used by WebEx, which is causing some WebEx traffic to be incorrectly classified as ShoreTel. The fix is to classify UDP 5004 as WebEx in the 6.1.0 and later application map.

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 145560: Stale BGP routes may be present in the core router connected to cluster members after a cluster rebalance with split horizon is enabled.

When all the members of the clusters have dual BGP neighbors towards the core router with split horizon enabled, a cluster rebalance rebalance can leave stale routes present in the core router.

In a customer enterprise without a fix for this issue, revoke and readvertise the routes from the Spoke Edges connected to the Hub Cluster.

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.

Fixed Issue 146252: An Edge that is rebooted may experience an issue where the Edge service never starts.

When this issue is encountered, a key process that runs as the Edge shuts down for reboot remains running (or stuck) after reboot. As a result this process prevents the Edge service from starting up.

Fixed Issue VLENG-146814: When a user navigates to Monitor > Edge > Flows tab, they may observe that the Orchestrator displays incorrect Source and Host Names for local IP addresses.

The Source and Destination IP Addresses for peer generated flows will always be in reverse order. This is also the case for Source and Destination ports. When the chat stats are generated the ports are reversed for peer flows, but the Source and Destination IP addresses are not. Because of this the Orchestrator shows incorrect Source and Host Names.

Fixed Issue 146819: A multicast configuration may not take effect when the underlying interface is moved from one segment to another.

The Edge service does not properly handle the movement of interfaces across segments. In particular the Edge does not properly handle the removal of the multicast configuration from the old interface and the addition of a new interface.

On an Edge without a fix for this issue, the user can push a fresh configuration change over the interface which moved to another segment to forcefully trigger the multicast configuration parsing.

Fixed Issue 146904: On a Partner Gateway with a single hop Partner Gateway-BGP session, for any traffic destined to the PG VRF IP address, the return traffic may get dropped.

For a PG-BGP scenario (single hop), the Gateway checks to determine if a PG-BGP nexthop IP address is configured or not. If it is not present, the Gateway tries to assign the *arp dst_ip* to the *ip-packet* destination IP address. As a result, egress traffic can get dropped due to ARP failure.

For a Gateway without a fix for this issue, the Partner should use a multi-hop PG-BGP session instead of a single hop session.

Fixed Issue 147800: For a Business Policy configured with an Object Group, if a user modifies the Object Group's Address or Port Group, these changes may not be immediately applied to existing flows.

Traffic expected to match this Business Policy rule after changing the Object Group do not match the rule because the change is not triggering the Edge to re-lookup of all such rules.

Fixed Issue 147841: For a customer enterprise site deployed with a High Availability topology where the HA Edge is used as a Spoke, users may observe that the HA Spoke Edge does not form a tunnel to a Hub Edge on some of its WAN links after recovery from an Active/Active "Split-Brain" state.

This occurs if the Active/Active state was triggered by a thread starvation that fools the Standby into promoting itself to an Active state. Due to a responder being updated with the wrong Edge serial number because of thread starvation, the responder rejects the new tunnels after the Active/Active panic is resolved.

d **Fixed Issue 148017: For an Edge using a PPPoE interface, the PPPoE may go down after an upgrade from 4.5.x to 5.2.3 or higher.**

After upgrading from 4.5.x to 5.2.3, the PPPD version was changed from 2.4.7 to 2.4.9. The PPPD daemon is running with an argument in 2.4.7. In PPPD 2.4.9, It is going to parse values from a file and execute the PPPD daemon. The "#" character is treated as a comment while parsing values from this file. It will be treated as '#' if added to the Edge adds this '#' value in the configuration file. The fix allows a customer to use a password with '#' in it.

Fixed Issue 148063: A Non SD-WAN Destination (NSD) via Gateway BGP peer IP address route may be advertised into the overlay.

In scenarios when BGP is turned off completely with NSD BGP configured and then later re-enabled, the NSD BGP peer IP address route can be advertised to the overlay, due to a defect in the best route advertisement logic.

Fixed Issue 148303: For a customer enterprise deploying one or more Non SD-WAN Destinations where BGP over NSD is configured on the Edge, the NSD over BGP IP address route is being advertised into the overlay.

In scenarios when BGP is turned off completely with NSD BGP configured and re-enabled again, the NSD BGP peer IP address route gets advertised to overlay, this is due to a defect in the best route advertisement logic.

Fixed Issue 148624: A customer may observe that Edge CPU utilization may differ between the Orchestrator UI and SNMP. In addition the SNMP result may show an Edge CPU utilization of greater than 100%.

The SNMP result is load averaged and displayed results can total more than 100.

As for the Orchestrator UI and SNMP discrepancy, this is the result of using different parameters for the *cpu_percent* value and this results in different values..

Fixed Issue 148852: For a High Availability Edge pair, a network configuration may not be applied to the HA Edge.

In instances where the Orchestrator check fails and a NULL netmask is sent to the Edge, the Edge does not gracefully handle the NULL netmask. As a result it does not update the configuration for any interface.

For an HA Edge without a fix for this issue, the workaround is to add an IP address to the interface for which the netmask is NULL. Or you can set the interface to DHCP.

Fixed Issue 148882: For a customer who deploys one or more Non SD-WAN Destinations (NSD) via Gateway, after correcting an NSD PSK from an incorrect to a correct value, the NSD IPsec tunnel may remain down and generate a "tunnel id mismatch message".

These are steps that lead to the issue.

- Create an NSD via the Gateway with a Cisco ASA type, and ensure the NSD tunnel is up.
- Set up 260 traffic selectors on both the Cisco ASA and Orchestrator sides, verifying that all tunnels are up.
- Change the Phase 1 and Phase 2 lifetime values to 540 seconds and 180 seconds, respectively.
- Send background traffic from the LAN client across all traffic selectors.

- Add four incorrect traffic selectors to the Gateway in the Orchestrator.
- Change the PSK value on the NSD side, causing the tunnel to go down.
- Revert the PSK value to the correct one on the NSD side.
- Although the NSD tunnel should come up, the tunnel remains down.

An Operator or Partner with access to the Gateway can restart the Gateway service to temporarily clear the issue.

Fixed Issue 148935: For a customer using Edge Network Intelligence (ENI) where Analytics is enabled, Analytics flows may be sent to a Spoke Edge instead of the Gateway when the default route is advertised.

When a default route is sent from a Hub Edge, the ENI traffic from the Spoke Edge is shifted from the Gateway to the Hub Edge. This happens as the ENI flows are not always considered as management flows.

Fixed Issue 149251: For a customer with Enhanced Firewall Service activated, a user may observe that URL filtering is not working as expected on Chrome browsers.

In this issue, a customer is expecting to block web pages using URL filtering but users can still load web pages when using a Chrome (or a chromium-based) browser. When URL Filtering is enabled for a flow because of a firewall rule traffic may not be dropped and forwarded leading to the webpage being loaded. URL Filtering works as expected for Firefox browsers.

Fixed Issue 149307: Setting an Edge interfaces auto-negotiation to off does not get applied after changing the L2 parameter of Auto-negotiation from on to off.

When the L2 setting of a DPDK PMD-bound Edge interface is set to Auto-negotiation off with a specific speed and duplex mode, the network settings get pushed and the Edge service process gets restarted but the L2 settings on the interface still shows auto-negotiation on and advertising all available link modes.

Fixed Issue 149339: Traffic matching 1:1 NAT rules with the same inside and outside IP address are dropped by the Edge.

Due to a defect in the Edge forwarding logic, traffic matching 1:1 NAT rules with the same inside and outside IP are treated as self-destined or self-sourced and then dropped.

Fixed Issue 149674: For a customer enterprise site deployed with a Standard High Availability topology, when the HA link is toggled multiple times, the site may experience an Active/Active "Split Brain" state.

In a standard HA setup, when the HA link is toggled and then brought down again, the HA Edge fails over immediately though the Active Edge is receiving WAN heartbeats. So later when the HA link is brought up, both Edges are now Active, or in a "Split Brain" state.

Fixed Issue 149685: When the last member of a VLAN is removed, the VLAN route is not revoked from the overlay, which can lead to a traffic black-hole for packets still using that VLAN.

When the last member is removed, the VLAN should be considered down and the route must be revoked from the overlay. Otherwise the Edge would receive packets for this route and it would lead to a traffic black-hole.

Fixed Issue 149726: A Virtual Edge deployed in Azure and running 5.4.x or higher where the interfaces are configured with DHCP and Accelerated Networking is enabled may not have an IP address on its interface after a reboot.

After reboot, an Azure Edge running Edge software release 5.4.x or later may not have an assigned IP address on an interface that is configured with DHCP and enabled with Accelerated Networking support. It is caused by a race condition that may occur at the start of the Edge service that results in *dhclient* not running on that interface.

Fixed Issue 149885: For a customer enterprise deployed with Hub Clusters, when a Cluster Rebalance is performed the route auto correction is not occurring, leading to customer traffic issues.

With Gateways running on version 5.4 or higher, routes from Spoke Edges are advertised to all Hub Edges, regardless of the spoke-hub association. This causes the Spoke Edge's route to be shared with all Cluster members and included in the *remote_routes*. During Cluster member reassignment, the Gateway does not resend the Spoke Edge’s route to the new Cluster member. Since auto-correction is only triggered when BGP underlay routes or overlay routes are received, this process does not activate auto-correction.

Fixed Issue 149970: Memory usage may increase gradually in an Edge with scaled configuration, control plane messages, and traffic.

Currently when there are a scaled number of route exchanges and large amounts of traffic, the socket connection between the Edge service and a multicast routing process may be closed and re-established. The memory allocated for a previous socket connection in the Edge service is not properly freed and it leads to a leak.

Fixed Issue 150247: For a Gateway deployed on a Google Cloud Platform (GCP) instance, some internet-bound flows may be dropped by the Gateway.

A race condition during the Gateway service process initialization may result in secondary IP addresses configured on the Gateway cloud interface for Portable IP Addresses for Non SD-WAN Destinations to be used also for NAT load balancing (in other words, for Internet bound traffic). This causes the flows to be routed through a GCP Cloud NAT instance. Due to limited resources on the cloud NAT instance, some flows may be dropped.

Fixed Issue 150463: When the Protocol Independent Multicast (PIM) Rendezvous Point (RP) address is changed in a Hub Edge profile multiple times, there may be a gradual increase in memory usage on the Hub Edge.

When the RP address is changed, the entry that is created for resolving the old RP address in the Hub Edge service is sometimes not cleaned up and results in a memory leak.

Fixed Issue 150655: Setting auto negotiation to off and then turning it back to on is not working on an Edge's routed interface. The auto-negotiation does not get enabled back on the Edge interface.

The script to change auto-negotiation settings on the interface uses a hardcoded path to the GE1 interface to get the DPDK driver.

Fixed Issue 150755: When the Network & Flood protection feature is enabled for a Non Wi-Fi Edge model (for example, the Edge 680-N), connection throttling gets applied even before the configured threshold is hit.

Connection Per Seconds (CPS) thresholds are not set for Edge models without Wi-Fi or for the LTE variants (for example, the Edge 710-5G). As a result, the flood control feature does not work as expected.

Fixed Issue 150795: For an Edge with dual SIM support where two SIMs are being used, a user may observe they cannot select the Standby SIM after an automatic SIM switchover.

The *sim_switchover.sh auto* script will trigger in the *auto_sim_switchover* process. But the *sim_switchover.sh* failed due to *SWITCH_ENABLED=0*. The *SWITCH_ENABLED* value should be 1 if the automatic SIM switchover is enabled from the Orchestrator.

Fixed Issue 150807: Mandatory link steering may not work if the WAN overlay changes from auto-detect to user-defined.

When a WAN overlay is changed from auto-detect to user-defined, the link logical ID changes. The business policies continue referring to the old link logical ID and the Edge drops the packets associated with the business policy.

On an Edge without a fix for this issue, a user should delete the old business policy and recreate it so that it uses the new link logical ID.

Fixed Issue 151287: A Gateway may experience a Dataplane Service failure, generate a core, and restart to restore functionality.

When the Dynamic Bandwidth Adjustment feature is enabled on a wireless link on an Edge, the feature code on the Edge and the Gateway work in tandem to determine the real time bandwidth of the wireless link. It is possible that multiple threads on the Gateway get into a race condition in which they try to access the feature data and some other shared data at the same time, and they are blocked from executing because they each hold a lock to the data the others are waiting for. This results in the Gateway Dataplane Service being terminated due to SIGXCPU.

On a Gateway without a fix for this issue, the only way to avoid the issue is to disable Dynamic Bandwidth Adjustment feature on all the wireless links that are connected to the Gateway.

Fixed Issue 151706: For customers using the Enhanced Firewall Service (EFS), URL Filtering does not work correctly when using a Chrome browser and Stateful Firewall is not enabled.

Due to a larger client Hello, it spans two packets. The exception path processes the DPI result with the URL in the context of a reply ACK from the firewall server. Since the Edge performs a firewall lookup only for outbound packets in case of a stateless firewall, it does not perform the URL database lookup and does not get filtered.

Fixed Issue 151764: Route auto-correction may not occur for Dynamic Edge-to-Edge via Gateway routes after a route flap.

In the case of Edge-to-Edge (Branch-to-Branch) via the Gateway, the expected behavior is to have the same route in both Routing Information Base (RIB) and the Forwarding Information Base (FIB). Due to a software defect, when the tunnel towards the Gateway flaps, a new route is installed into the FIB. Because this new

route is installed on the FIB, on learning the underlay route auto-correction is done only for the route in the RIB and skipped for the FIB. This issue is only encountered where Edge-to-Edge via Gateway is enabled.

Fixed Issue 151892: A user may observe inaccurate Edge WAN link path status on the Orchestrator UI.

During certificate renewal, the established path in the Edge will tear down and a new path is established. Here the sequence is: a new path comes up and the old path is moved to a quiet state, does a fast reinit and waits for 7 seconds for the path to be deleted. When the old path is deleted, the Edge wrongly updates the connection state as DEAD for the new path and so the path state is shown as DEAD on the Orchestrator UI under the **Monitor** pages.

While the status is incorrect, this has no impact on customer traffic.

Fixed Issue 152144: Edges having interfaces configured with DHCP which have IP addresses in the same subnet may stop establishing tunnels from several interfaces after a DHCP lease renewal.

For example, if an Edge has 3 interfaces: GE3, GE4, and GE6 with IP addresses in the same network, a DHCP lease renewal on an interface or an IP address update on GE3 interface can result in the GE4 and GE6 interfaces to stop establishing VCMP (management) or IPsec tunnels.

Fixed Issue 152283: The interface GE5 and GE6 on Edge model 6x0 types with a 9.13 or newer BIOS may not detect carriers if the user disables auto-negotiation.

This behavior is inconsistent, but if encountered on a 6x0 Edge without a fix for this issue, the user should re-enable auto-negotiation on the Orchestrator and save changes, and then disable auto-negotiation.

Orchestrator Resolved Issues

Resolved in Orchestrator Version R6103-20250319-GA

Orchestrator version R6103-20250319-GA was released on 03-21-2025 and resolves the following issues since Orchestrator version R6102-20250304-GA.

Fixed Issue 135926: When disabling implicit privileges, the other actions are displayed as enabled, even when those privileges do not exist. This can lead to customers mis-configuring role privileges due to the display issue.

Fixes a display issue where enabling the "Deny Update" privilege incorrectly checks the "Read," "Create," and "Delete" privileges. This visual error has been resolved, ensuring accurate representation of role customizations without impacting functionality.

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

When a neighbor was deleted from the Edge Device Settings page, the **Monitor > Routing > Edge BGP Neighbor State** page did not remove the neighbor or mark it as REMOVED. This issue is now resolved. When neighbors are deleted from the Edge configuration and the Edge removes the BGP neighbor from its configuration, they will now appear in the REMOVED state on the monitor page.

Fixed Issue 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 R6102-20250304-GA

Orchestrator version R6102-20250304-GA was released on 03-05-2025 and resolves the following issues since Orchestrator version R6101-20241218-GA.

Fixed Issue 136219: Re-enabling a non-READ privilege after denying a READ privilege can no longer be saved in an inconsistent state.

A denied READ privilege will always override the CREATE, UPDATE, and DELETE privileges for a given permission. Trying to save an enabled non-READ privilege and disabled READ privilege will revert to all-denied.

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

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

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

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

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

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

Fixed Issue 154709: Incorrect documentation for the getEdgeSDWANPeerPathMetrics method.

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

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

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

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

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

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

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

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

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

Fixed Issue 156801: Enterprise superuser cannot access licensing page.

When enterprise superuser tries to access Orchestrator licensing service, they can see the page but not the data. They see error message saying "Error during list loading: undefined".

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

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

Fixed Issue 157156: Customers may experience difficulty opening the Edge diagnostic page.

On large Orchestrators, exceeding the Redis 'client-output-limit' message count can lead to **websocket** issues, potentially preventing customers from accessing the Edge diagnostic page.

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

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

Fixed Issue 157340: When generating Flow Tabs CSV files, the Orchestrator can experience heavy resource consumption. On vco162-usca1, this resource saturation led to an outage due to insufficient memory limits and overall resource exhaustion.

The CSV file generation process for Flow Tabs placed a large load on the system, causing excessive memory usage. While ClickHouse was already configured with CPU limits, there were no explicit memory constraints in place. This absence of a hard memory cap allowed the query to consume excessive resources, ultimately leading to an outage on vco162-usca1. In response, the fix described in VLOPS-26535 introduced stricter memory constraints for ClickHouse queries, preventing future instances of uncontrolled resource usage. After implementing these constraints, the Orchestrator service returned to normal operation.

Fixed Issue 157375: Intermittent Empty API Responses: The getEnterpriseEvents API on Orchestrator version 6.1.0.0 would sometimes return an empty response (no event data) despite a successful HTTP 200 OK status code. Missing Events: Even when events existed within the specified time range, they were not included in the API response.

The intermittent empty response issue stemmed from the new events migration feature database queries, specifically impacting the **getEnterpriseEvents** API when querying across wider time ranges. This issue may be observed on Orchestrator version 6.1.0.0.

Fixed Issue 157545: Previously, sequential IDs were omitted from event query results to maintain consistency across MySQL and ClickHouse data sources.

This release introduces a new system property, events.mysql.return.id, to control the inclusion of the MySQL sequential ID in event query results. When events.mysql.return.id is enabled (set to true):Event queries within the past month will include both sequential IDs and logical IDs.Event queries exceeding one month will include logical IDs for all events, but sequential IDs will only be present for events within the last one month. Data older than one month is sourced from ClickHouse, which does not have sequential IDs.

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

A user may encounter an issue when selecting a date in Orchestrator while adding or modifying a user license agreement.

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

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

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

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

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

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

Fixed Issue 158462: Global Settings UI does not respond and shows "loading" indefinitely.

After upgrading, the Global Settings UI may not load correctly, potentially affecting other UI services such as SSE, CWS, and more.

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

In rare cases, Orchestrator that have a high IO process running in the background (i.e. backups), there was an issue that caused the upgrades to fail.

Resolved in Orchestrator Version R6101-20241218-GA

Orchestrator version R6101-20241218-GA was released on 12-27-2024 and resolves the following issues since Orchestrator version R6100-20241105-GA.

Fixed Issue 94634: SSRF bypass in alert/sendEnterpriseAlertTestWebhook

Users may be able to bypass SSRF protections built into alert/sendEnterpriseAlertTestWebhook by using an untrusted intermediary. When system property to allow redirection is enabled, there should be a 302/301 redirect to an internal location.

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

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

Fixed Issue 150366:Issue with reports showing drastically different measurements after a VCO upgrade

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

Fixed Issue 150727: Redirection to SD-WAN is expected instead redirection to Global Settings

Wrong application redirection may occur when the user clicks on a customer.

Fixed Issue 153402: Inventory Edges get duplicated when automatically moved from pending to assigned inventory

When a user opens the pending inventory tab, if there are no potential HA Edge pairs, all inventory edges are duplicated when automatically moved from pending to assigned inventory.

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

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

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

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

Fixed Issue 154850: Cannot download application map from Orchestrator

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

Resolved in Orchestrator Version R6100-20241105-GA

Orchestrator version R6100-20241105-GA was released on 11-07-2024 and resolves the following issues since Orchestrator version R6006-20241025-GA.

Note:

This means that a fix for an Edge or Gateway issue listed in the 6.0.0 Release Notes up to the listed build is included in all Release 6.1.0 builds.

Fixed Issue 63453: An Edge WAN link whose speed is manually set to a high value may show a different value when looking at the Edge > Monitor > Overview and Links pages of the Orchestrator UI.

For example, if a link is manually set with a bandwidth at 10 Gbps, the UI shows a value of 1.41 Gbps on a **Monitor** page for that Edge. In addition, if the link is set to autodetect and monitoring is set to Live Mode, the correct value is displayed. The issue is the result of the Orchestrator code not being designed to handle a manually entered bandwidth value above 4.2 Gbps.

Fixed Issue 76694: On the Gateways section of the Orchestrator UI, a user cannot edit a Super Alternative Gateway on the Orchestrator.

A user can only edit or assign Alternative Gateways, and not the Super Alternative Gateway.

Fixed Issue 110979: Edge APIs in APIv2 cannot return link-specific data in the response even if the user specifies query parameter "include=links.*" in the API request.

If a user makes an API call to GET edge API in APIv2 with query parameter"include=links.*". No link-specific data such as link IP address, linkInternalId, etc. are returned in the API response.

Fixed Issue 114956: On the Configure > Device > Interfaces page of the Orchestrator UI, a user cannot configure subinterfaces on different segments with the same IP address configuration.

This issue is the result of an Orchestrator validation error that blocks a valid configuration action.

Fixed Issue 115488: On the Configure > Network Services section of the Orchestrator UI, any Network Services' display name changes from lower case to upper case after the Orchestrator is upgraded to 5.2.x or higher.

This behavior has no impact on functionality but the customer is expecting the name case that they used and not an alteration to upper case.

Fixed Issue 115570: For a customer enterprise site configured for a High Availability topology, if the HA Edge's HA Interface is changed from the default location and then later downgrades the Edge software to a version that does not support this feature, the interface remains fixed to the port previously configured and cannot be changed.

In the scenario the HA Edge was running an Edge version which supported configurable HA Interfaces (5.2.x or later) and then was downgraded to Edge version 5.1.x or earlier. The default HA interface is GE1 for all models except the Edge 5x0 models. Not only is the HA interface now fixed to the changed interface, the user cannot edit that interface.

Fixed Issue 117656: If a user tries to search for an Edge on the Orchestrator UI and accidentally adds a space either before or after the Edge name, the Orchestrator does not return a result.

When a user accidentally adds a space after or before the Edge name search, the Orchestrator does not trim the search string and it is sent with this space which produces incorrect result in the table. The expected behavior is for the Orchestrator to automatically trim that space either before or after the Edge name to ensure a positive search result.

Fixed Issue 117826: On the Configure > Edges page of the Orchestrator UI, users cannot select multiple Edges by pressing Shift and then right clicking their mouse on the last element after they selected the first one.

Being able to perform the mass selection of objects through the Shift + Right Click action is efficient and expected by users who do this in many other user environments.

Fixed Issue 118409: For a customer enterprise deploying a cluster, if a user navigates to Monitor > Network Services and clicks on the Edge Clusters tab, they may observe the cluster name is blank against the Edge.

In an Edge Cluster created with more than one Edges, the cluster name is seen as blank against the Edges except the first one. All the Edges associated with the profile should be listed.

Fixed Issue 118684: For customers using the monitoring/getEnterpriseEdgeStatus API where ClickHouse is enabled to store statistics data, the customer may observe data discrepancies for Edge statistics.

When this issue is encountered, the API only returns the *edgeLogicalId* instead of returning both the *edgeLogicalId* and the *edgeId*. This behavior results in data discrepancies and user confusion as they rely on the retrieval of edge IDs for various use cases within their environments. The resolution to the issue ensures that the getEnterpriseEdgeStatus API returns the edgeLogicalId and the edgeId, bringing alignment with our

documentation and providing a more predictable user experience.When this issue is encountered, the API only returns the

Fixed Issue 118780: On the Configure Partners > (select partner) > Administration > Partner Configuration > Available Software page of the Orchestrator UI, when the available Software/Firmware section contains a substantial number of items, users encounter challenges efficiently selecting their desired option, and the list does not allow users to filter items, making the selection process more difficult.

Introducing a table-based model with filtering capabilities for the Software/Firmware section in Partner configuration screen offers a compelling solution to the problem. This enhancement not only addresses the inconvenience caused by a vast number of items but also empowers users to easily locate and select their desired options. By incorporating features like search, pagination, this solution significantly improves the overall user experience.

Fixed Issue 118787: On the Administration > Operator Profiles > Application Map > Software Version drop-down, when the Software Version drop-down contains a substantial number of items, users encounter challenges efficiently selecting their desired option, and the drop-down list does not allow users to filter items, making the selection process more difficult.

Introducing a table-based model with filtering capabilities for the Software Version drop-down in Operator Profile screen offers a compelling solution to the problem. This enhancement not only addresses the inconvenience caused by a vast number of items but also empowers users to easily locate and select their desired options. By incorporating features like search, pagination, this solution significantly improves the overall user experience.

Fixed Issue 118790: On the Administration > Operator Profiles > Application Map > JSON drop-down section of the Orchestrator UI, when the JSON File selection drop-down contains a substantial number of items, users encounter challenges efficiently selecting their desired option and does not include the option to filter items, making the selection process more difficult.

Introducing a table-based model with filtering capabilities for the JSON File selection drop-down offers a compelling solution to the problem. This enhancement not only addresses the inconvenience caused by a vast number of items but also empowers users to easily locate and select their desired options. By incorporating features like search, pagination, this solution significantly improves the overall user experience.

Fixed Issue 121004: On the Configure > Edge > Device > VPN Services page of the Orchestrator UI, when the Cloud Security Services section is expanded, the GRE tunnel details information disappears if the segment is changed.

While the CSS section is expanded and collapsed, the GRE tunnels disappear when the segment is changed in the Edge configuration tab.

Fixed Issue 121843: On the SD-WAN > Configure > Edges of the Orchestrator UI, when downloading the Edges CSV list, the date format is different in the New UI than the Classic UI.

The date format should be "01/20/22, 19:16:27" but instead displays as 'April, 7, 2022 7:58:58 PM'.

On Orchestrators without a fix for this issue, the user can edit the CSV file in Excel (or a similar application) and the date format can be converted using Excel formulas.

Fixed Issue 122044: A user cannot configure OSPF area ID = 0 on a loopback interface on the Orchestrator UI.

The only way a user can successfully configure this field is if a user configures the area ID as 0.0.0.0 for the loopback interface. Other methods throw an error and the UI does not save the changes.

Fixed Issue 122350: The Configure screen, the generic search and filter box may not deliver correct results.

This is true for any screen under the Configure category and the search box does not consistently search across all fields to ensure correct results. For example, if a user searched for some term they had placed into the Description field, the generic search does not look in the Description field, and those Edges are not returned.

Fixed Issue 123207: On the Configure > Network Services > Edge Services page of the Orchestrator UI, when configuring a VNF with a Fortinet type, the VNF options are not shown.

Issue is seen only when a user uses a System Property with new image details which are not listed in the drop-down menu. This is probably a data issue due to an image object not containing an ID in it.

Fixed Issue 123622: On the Configure > Edge/Profile > Firewall page of the Orchestrator UI, when configuring a new firewall rule, if a user enters only a domain name, the form cannot be saved.

The issue is due to the IP address value being passed as an empty string instead of `any`. When a user does not enter any IP address value, the IP address field in the payload should be string `any` and the backend code should validate the same.

Fixed Issue 124118: On the Configure > Edge > BGP page of the Orchestrator UI, while configuring the filter in BGP, the AS-PATH_PREPEND value can accept a space without an error being thrown.

This issue occurs because Number(value) was returning NAN if value was " ".

Fixed Issue 126412: A user may observe that the DHCP Server "Lease Time" field is disabled/ grayed out.

For a customer who has configured a DHCP Server, the "Lease Time" field can show as disabled when the Edge override is enabled for the VLAN used by that DHCP Server.

Fixed Issue 126471: On the Configure > Edge > Device > Interfaces page of the Orchestrator UI, a segment name updated for an existing or new VLAN is not getting reflected at the Edge level unless Edge override is clicked.

For example, access VLAN100 at the Edge level, override it and configure an IP address and save Access to the profile and change the segment of VLAN100 to the Global Segment from Segment1. Then go to the Edge again and access VLAN100 and remove the override and a user would observe that the changed segment is not reflected.

Fixed Issue 127667: For a customer using the Enhanced Firewall Service with the IDS/IPS feature configured, the IDS/IPS Signatures page does not include a column for "Actions".

Release 6.1.0 adds an "Action" Column to the Intrusion Signatures overview tab.

Fixed Issue 128330: For an enterprise using a Non SD-WAN Destination (NSD) via Gateway network service, the UI permits the user to delete a NSD via Gateway from a Profile which includes a Business Policy rule associated with the global segment.

As a result, the Business Policy rule becomes invalid and any traffic matching that rule is not steered as expected causing a possibly significant impact to customer traffic matching that rule.

Fixed Issue 129411: On the Service Settings > Edge Management > Software & Firmware Images page of the Orchestrator UI, when an Enterprise Superuser clicks on the "Manage Customer" link, they are incorrectly redirected to the Monitor > Overview page instead of the intended destination.

Enterprise users do not have the necessary permissions to access the "Manage Customer" functionality. As a result, the system defaults to redirecting them to an unrelated page. This issue does not occur for Operator-level users, who have the correct permissions and are routed appropriately.

To prevent confusion and incorrect navigation, the "Manage Customer" link should be hidden for enterprise users, ensuring they don't encounter this issue.

Fixed Issue 129707: On the Configure > Edge/Profile > Device page of the Orchestrator UI, a user on a Firefox browser cannot create custom DHCP options.

On a Firefox browser, when a user tries to provide an input for DHCP options as 234, the browser only accepts 23 and then locks the options.

Fixed Issue 130038: On the Configure > Segments page of the Orchestrator UI, a user may observe that the Description column text overlaps with the Type column.

Basic UI text issue that is resolved so that a user can now see the text for both columns without overlap.

Fixed Issue 132615: On the Edge Management > Edge Auto-activation screen of the Orchestrator UI, the page does not show the Subscription ID after the user has set up.

Currently, the user inputs the Subscription ID, but afterwards there is no way to know what ID they submitted and it needs to be referred to on occasion.

Fixed Issue 133092: For a customer enterprise that deploys one or more Non SD-WAN Destinations via Gateway with redundant Gateways where L7 Health check is enabled, a user may observe the wrong service status for this NSD when looking at Monitor > Network Services.

There is no functional impact for the NSD as this issue is cosmetic. The issue can occur if each Gateway (Primary and Secondary) has a different L7 Health status and there can be a potentially false status when looking at the UI. For example, if the Primary VPN tunnel is down, the user may see the UI report that the NSD is completely down, when in fact the Secondary VPN tunnel is now passing customer traffic to the peer datacenter.

There is no functional impact for the NSD as this issue is cosmetic. The issue can occur if each Gateway (Primary and Secondary) has a different L7 Health status and there can be a potentially false status when looking at the UI. For example, if the Primary VPN tunnel is down, the user may see the UI report that the NSD is completely down, when in fact the Secondary VPN tunnel is now passing customer traffic to the peer datacenter.

There is no workaround to show the correct status in the UI, but an Operator or Partner can see the correct service status of each VPN in the Gateway if they log into the Gateway via SSH and run *debug.py --ike*.

Fixed Issue 133366: For a customer using BGP for routing, when looking at the Monitor > Network Services > BGP Gateway Neighbor page of the Orchestrator UI, a user can only remove states one at a time.

In a situation where multiple false monitoring states are shown, a user has to delete each one versus being able to click on all of the false states and deleting them all. This fix adds a bulk delete option.

Fixed Issue 133562: If a user disables IPv4 or IPv6 Settings for either a loopback or a routed interface, they would still observe this option as enabled in the OSPF section of the Orchestrator.

The Orchestrator did not enforce IPv4 or IPv6 dependencies for the OSPF configuration.

Fixed Issue 134498: For a customer deploying one or more Cloud Security Services (CSS) or Non SD-WAN Destination via Edge, removing an unused segment from a profile may cause CSS or NSD via Edge tunnels to delete for all segments.

The user can restore these tunnels by disabling and then re-enabling the affected CSS or NSD via Edge.

Fixed Issue 135472: On the Service Settings > Alerts & Notifications > Webhooks page of the Orchestrator UI, a user may observe an error banner with no text for a webhook that is sent properly.

A key code was not sent properly to the Orchestator's backend API call. This leads the Orchestrator to treat the webhook as unsuccessful and displays an error banner.

Fixed Issue 135560: On the Administration > User Management > Service Permissions section of the Orchestrator UI, after removing the privilege for "download the gateway diagnostics", the user is able to delete the bundle for operator standard and support users.

Issue is the result of incorrect role mapping on the Orchestrator.

Fixed Issue 135636: On the Administration > User Management > Service Permissions section of the Orchestrator UI, after removing the "create" privilege for a partner super user (cloud security service), the user can still create a CSS.

The issue is the result of incorrect role mapping on the Orchestrator.

Fixed Issue 135929: On the Administration > User Management > Service Permissions section of the Orchestrator UI, if a Partner user role has the privilege to read Diagnostics Bundle removed, the Diagnostics tab still remains visible and accessible for those users.

This is a result of incorrect role mapping on the Orchestrator.

Fixed Issue 135996: On the Monitor > Firewall page of the Orchestrator UI, when looking at the Threat Trends graph, the times are expressed in UTC instead of the local system time.

The times are expected to be displayed in the local system time for ease of user understanding.

Fixed Issue 135998: On the Administration > User Management > Service Permissions section of the Orchestrator UI, if the privilege to "update and delete" a segment is removed, the user also loses the privilege to create a segment as well.

The Orchestrator incorrectly applies the custom role package configuration to take away the create segment privilege.

Fixed Issue 136018: On the Administration > User Management > Service Permissions section of the Orchestrator UI, if the Privilege for read or create, update, or delete a Profile is removed for a Standard Operator, they can still perform all these activities.

The Orchestrator fails to apply this custom role package.

Fixed Issue 136188: On the Administration > User Management > Privileges page of the Orchestrator UI, if the Update permissions for DNS Services is removed at the profile level for the Enterprise Superuser, the Orchestrator also removes Create and Delete privileges.

The Orchestrator should only remove the Update privilege for the DNS Services.

Fixed Issue 136247: On the Administration > User Management section of the Orchestrator UI, the LAN-SIDE NAT update option works even after disabling it for enterprise admin users.

The Orchestrator is not applying this role customization configuration.

Fixed Issue 136259: A Gateway may experience a Dataplane Service failure and restart to recover.

When encountering this issue the Gateway service fails because of an invalid type of neighborAsn sent by the Orchestrator. The Gateway is expecting this field as a string, but the Orchestrator may send it as an integer and this triggers an exception on the Gateway service.

Fixed Issue 136578: On the Administration > User Management > Service Permissions section of the Orchestrator UI, When logged in as an Operator Standard Administrator, after removing "READ" privilege for High Availability, the user can still read and update High Availability.

Orchestrator fails to apply this user role configuration.

Fixed Issue 136582: On the Administration > User Management section of the Orchestrator UI, when logged in as a Superuser or Standard Administrator, after removing the "READ" privilege for L2 settings at the Edge and Profile level, the configuration for ARP is still present.

The configuration for ARP is not present, when logged in as Superuser or Standard Administrator, after removing "READ" privilege for L2 settings at edge and profile level.

Fixed Issue 136585: For a customer who uses the Enhanced Firewall Service, in the Configure > Edge > Firewall screen, if a user tries to make a dummy change, the SSG data is getting removed in the Edge heartbeat.

The Orchestrator is not attaching refs data in the *updateConfigurationModule* API call for the firewall module. So when a user tries to update the firewall module without any change from its previous version, the backend deletes the SSG data.

Fixed Issue 136696: On the Configure > Edge/Profile > Device page of the Orchestrator UI, while configuring a DHCPv6 prefix delegation a user may observe a warning message.

The warning reads: 'Addressing incomplete warning' when trying to configure DHCPv6 PD as addressing type in a routed interface/sub-interface. The message is spurious and the user can save the configuration.

Fixed Issue 137521: On the Configure > Profiles > Business Policy page of the Orchestrator UI, a user cannot change a default Business Policy rule when they select IPv4 as the sole IP Version.

The default setting is IPv4 and IPv6 and some rules will not work with this mode and throw an error that "mixed IP mode is not supported", so it is important a user can change the IP Version to something else, like IPv4.

Fixed Issue 137624: The Orchestrator does not update Edges with a Partner Gateway's private IP address details when the Local IP Address is changed in the Partner Gateway hand-off page

The Orchestrator does not update the Edges with the Partner Gateway private IP address details when the Local IP Address is changed in the Partner Gateway hand-off page.

Fixed Issue VLENG-137832: When a user looks at the logs in a diagnostic bundle, there is a discrepancy in a link's LogicalID in different link statistics entries and results in different links statistics for the same link.

In the diagnostic bundle logs, when looking at the "optvcbindebugpy-v–link_stats.out.txt", the correct LogicalID is listed. However, sometimes the .edge.info shows the "logicalId": "00:00:00:00:00:00:0000".

The fix for this ensures that link statistics, as reported by an Edge, will now cause updates to occur in the link table when the logical IDs do not match. This mechanism ensures that the reported MAC addresses remain consistent with those learned by the Edge.

Fixed Issue 138041: On the Administration > User Management > Service Permissions section of the Orchestrator UI, if a user disables the 'Create' privilege in 'Edge Device Authentication Settings' and 'Profile Device Authentication Settings', the changes do not take effect.

The user role is still able to create a new authentication service due to an Orchestrator error in role mapping.

Fixed Issue 138135: On the Administration > User Management > Service Permissions section of the Orchestrator UI, when a new service permission is created for the SD-WAN service, specifically for the operator standard admin user. The privilege to assign profiles is explicitly denied. However, upon logging in as an operator standard admin user, it is noted that the user is still able to assign profiles.

The feature privilege DENY: ASSIGN EDGE PROFILE for the operator standard admin user is not functioning as intended. Despite this restriction, the user can still assign a profile to an edge, which is inconsistent with the behavior observed in the classic UI. The issue is the result of the Orchestrator not mapping the privileges correctly.

Fixed Issue 138370: When a user attempts to make configuration changes to a Hub Edge within a profile or when trying to assign the profile to an Edge, the Orchestrator throws an error.

The issue was first observed while a customer was attempting to modify Cloud VPN settings for a profile. The error message reads: "Invalid or missing hub reference in 'Branch to Hub' vpnHubs list Segment:

'Management'." This indicates that the system is unable to locate the appropriate Hub reference necessary for the operation.

The issue is the result of the Orchestrator not performing the Hub check as expected.

Fixed Issue 138420: Users will experience gaps in the Monitoring page graphs when the Orchestrator is deployed with two or fewer cores.

In this scenario, all available cores are dedicated to statistics processing, leaving no capacity for producers. The issue arises when EdgeOps deploys an Orchestrator with two or fewer cores, resulting in the exclusive allocation of all cores to statistics workers. This configuration prevents producers from functioning, leading to noticeable gaps in the monitoring graphs.

Fixed Issue 139035: When creating a Non SD-WAN Destination via Gateway, the Orchestrator UI defaults to offering a single VPN Gateways versus a redundant pair of VPN Gateways.

Customers should be encouraged to use redundant Gateways as a default action and then the customer can choose a single Gateway if that is their preference or if there is no option to have redundant VPN Gateways as with Policy Based and Cisco ASA NSDs.

Fixed Issue 139141: For a customer using the Enhanced Firewall Service where it is enabled at the profile level, after cloning a profile, there are duplicated references for segments.

This issue occurs after creating a profile adding multiple segments to that profile and then creating an address group in Object Groups and mapping that address group to Firewall rules for different segments and then cloning the profile. While cloning the profile, the firewall object group association was getting copied in two places.

Fixed Issue 139369: A user may observe that their attempt to activate an Edge 710-5G fails.

The Orchestrator erroneously sends the alias name *Edge7105G* instead of the correct name *Edge710-5G* and this results in an Edge activation failure.

Fixed Issue 139409: For a customer enterprise deployed on an Orchestrator where the customer deploys one or more Cloud Security Services (CSS), if the customer makes a change to a CSS on the peer side while the Orchestrator is being upgraded, an Edge in their enterprise may experience multiple Dataplane Service failures in succession and, after the third such failure, stop passing traffic until the Edge is manually restarted by the user.

When this issue is encountered, the Orchestrator creates more than one CSS creation automation action for a single Edge WAN link, and this erroneously creates multiple CSS tunnels. The Edge receives this wrong data, which triggers an exception that causes the Edge service to fail. The nature of the issue means that even after the Edge recovers from the initial failure, the Orchestrator will continue to provide the erroneous tunnel information, causing additional failures and, on the third such failure in succession, the Edge defensively stops trying to recover which results in all customer traffic dropping.

On an Orchestrator without a fix for this issue, the user must clear the erroneous CSS tunnel information the Orchestrator is generating to remediate the issue, and this is done by disabling all CSS instances for that Edge, wait for the tunnels to be deleted, and then re-enable all CSS instances.

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 rules 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 139789: A user may not be able to see the user-defined WAN link tunnel that they created as it gets converted to an auto-discovered link.

This issue occurs when a WAN module update follows these steps: The Orchestrator deletes a user-defined link from the **Configure > Device** settings page or via API (updateConfigurationModule).

Before receiving this update, the Edge sends a pushLinkStats message containing the deleted user-defined link.

Since the link is no longer in the Orchestrator, it incorrectly converts the user-defined link to an auto-discovered link and adds it to the WAN module's network configuration. This results in an incorrect internal logical ID for user-defined links in the network, which is the basis of this ticket.

Fixed Issue 139796: When a customer deploys a Edge model 710-5G, the Orchestrator UI shows the wireless link as 3G/4G under the Monitor page.

The Orchestrator should show a CELL1/CELL2 link WAN type as 5G on the Monitor Page.

Fixed Issue 139918: Customers using Role Customization may observe that Orchestrator UI pages load slower than expected.

High counts of redundant MySQL queries cause slow page loading and performance times. Role Customizations were being queried one at a time (Select * where id = ?) instead of performing a single query and processing the results one row at a time (select * where id in (?,?,?,?)).

Fixed Issue 140024: On the Configure > Edge/Profile > Device page of the Orchestrator UI, when a user is editing and saving BGP rules, the Orchestrator may throw an error.

The error reads: "Cannot read properties of null ('reading message')". The issue can occur because the configuration object size caused a significant performance impact when the new object was JSON serialized and compared with the old object.

Fixed Issue 140183: On the Global Settings > Customer Configuration > SD-WAN Configuration > Software Image page of the Orchestrator UI, a user can select a deprecated software image.

When selecting a software image in the image selection modal on the SD-WAN configuration page, deprecated software images can be selected which leads to an API error.

Fixed Issue 140539: If a user attempts to perform a rebalance of Edges that have no routes to a Non SD-WAN Destination via Gateway will not work properly.

Any time the user attempts to rebalance selected Edges for better load distribution to Gateways, desired end outcome will not be seen if there is no NSD configuration present.

Fixed Issue 140796: If a user configures an Edge link as private and enables SD-WAN Service Reachable, they may observe an error.

The error reads "Connection missing to getDRConfig", which occurs when there is no connection to the Orchestrator's Disaster Recovery database. Connection to the DR database is not set while calling the API.

Fixed Issue 141040: If there are more than 10 rules in a BGP filter table, newly added options do not work if the configuration is carried out from the 2nd page of this table or onwards.

If a user tries to add a new rule on the 2nd page of the Orchestrator UI, they are actually visible in the first page. Rules are not created with respect to the current row.

Fixed Issue 141089: A newly created Enterprise Security Admin user cannot create and delete rules on the Configure > Edge/Profile > Firewall > Firewall Rules page of the Orchestrator UI.

The Orchestrator is not properly mapping the correct privileges for the Enterprise Security Admin role.

Fixed Issue 141376: On Monitor > Firewall Logs screen of the Orchestrator UI, if a user tries to filter logs based on the destination domain, the attempt fails.

When a user tries to filter Firewall logs with the destination domain, the Orchestrator is retrieving all the existing logs without considering this filter. This was due to an incorrect column name mapping from the Orchestrator backend to the UI.

Fixed Issue 141617: When a customer enterprise Profile is updated, on the Monitor > Events page the "Profile updated" Event Detail has the Principle field showing as "unknown".

For the "Profile updated" Event, a user should see when clicking on the Event to open the **Event Detail** box, the user should observe a value for the "principle" field. With this issue that value is always "unknown" and prevents the user from knowing what aspect of the Profile was updated.

Fixed Issue 141884: For a customer enterprise deployed with a Hub Cluster topology, a user may observe that they cannot add additional segments to a profile.

If a user updates the Hub Cluster in the network service with the old association combination, there is the possibility of missing the Hub Cluster in the references part because the Orchestrator is not doing a version check to this Hub Cluster before they are updated.

Adding the missing configuration entry in the VPN references will resolve the issue

Fixed Issue 141899: On the Partner Gateway Hand-off page of the Orchestrator UI, the user may observe that updating a Customer Tag (C-Tag) configuration does not work.

The C-Tag configuration changes are not saved if a user changes the segment and removes the C-Tag configuration.

Fixed Issue 141941: For a customer using the Enhanced Firewall Service where IDS/IPS is configured, in the Monitor > Security screen for IDS/IPS of the Orchestrator UI, the impacted Edge count is limited to 10.

The Orchestrator limits the SQL query response to 10 records by default. The SD-WAN service is not passing any limit in the API request and this results in the Orchestrator only giving the Top 10 Edges. Even though more than 10 Edges had IDS/IPS data, the UI is only showing 10 as a count.

Fixed Issue 141974: On the Authentication > User Management > Service Permissions page for the Orchestrator UI, if a user creates a new Enterprise Security admin user where that role is denied the Update privilege for Customer General Information under Enterprise Settings, that user can continue to update that section of the UI.

The Orchestrator is not applying the customized user privilege to this role package and the result is the Enterprise Security user can update the Customer General Information section.

Fixed Issue 142092: On the Configure > Network Services page of the Orchestrator UI, the filter selected for a Non SD-WAN Destination via Gateway's redundant Gateway is not locked.

Filter selected in redundant Gateway is not locked and users will be able to modify the filters. These filters should match the primary Gateway.

Fixed Issue 142210: On the Monitor > Network Services page of the Orchestrator UI, a user may observe that the VPN Tunnel status does not display correctly.

A "VPN Disabled" shows a status of "Disconnected" in the UI when the status should show as "Deactivated".

Fixed Issue 142316: Updating a VLAN or Edge routed interface setting of a profile used by a large number of Edges (>7500) takes a long time to complete and may even time out in some instances.

If the attempt times out on the Orchestrator UI, if the user reloads the **Configure > Profile > Device** page after more than 60 seconds, the changes are expected to show as applied and there is no need to do the same changes again.

Fixed Issue 142608: On the Profile/Edge > Configure > Device > Routing & NAT > Multicast page of the Orchestrator UI, when a user enables Multicast with a RP configured they may find that they cannot configure a 'Join Prune Send Interval' value of less than 60 seconds.

The **Join Prune Send Interval** setting is found under the **Advanced Settings** - **PIM Timers** and the expected behavior is for this value to be configurable in a range from 5-600 seconds.

Fixed Issue 142666: On the Configure > Edge page, the Edge Details dialogue has a small font size which makes the text difficult to read.

On the **Configure > Edge** page, the Edge's details are shown next to the Edge name at the top when the user clicks the drop down symbol and the text automatically adjusts the font size to something that fits that box, something very small and hard to read.

A user can increase the zoom percentage on their browser to better see the smaller text.

Fixed Issue 142785: For a customer enterprise site where the Edge has a WAN link configured for dual-stack mode (IPv4 and IPv6) and IP Preference is IPv4, if a Cloud Security Service (CSS) is configured for this Edge but the user does not configure FQDN, the user can change the preference mode to IPv6.

Changing the **IP Preference** mode when a CSS or a Non SD-WAN Destination (NSD) via Edge is deployed should be blocked as both types use the IPv4 WAN Overlay and changing to IPv6 will cause traffic to drop. The expected Orchestrator UI behavior is for the IP Preference option to be grayed out and not accessible while a CSS or NSD via Edge is associated with that interface.

There is no workaround beyond ensuring IPv4 is used and not changed as the IP Preference.

Fixed Issue 142787: If a user switches to a different Segment on the Orchestrator UI, they may observe that Business Policy Rules are missing on the new segment page.

When the switched Segment does not have rules setup specifically for it, the Orchestrator UI does not pre-populate the data with the default Business Policy rules.

Fixed Issue 142878: On the Authentication > User Management > Service Permissions page for the Orchestrator UI, if a user removes the privilege "Edge Device Configuration Visibility Mode" from the Standard Operator user role, the Operator with that role can still override the Edge Visibility mode.

In effect, the Standard Operator can check the **Override** box for the Visibility Mode feature for any Edge and save that change.

Fixed Issue 143074: Customers with large Orchestrator deployments may experience increased loading times and delays when accessing the Monitor > Edge > Flows tab on the Orchestrator UI.

This was due to inefficient database queries used by the affected API. Specifically, the original query attempted to retrieve configurations for all Edges within an enterprise, leading to performance degradation on large Orchestrators. The optimized query now targets Edge-specific configurations, minimizing database load and improving response times.

Fixed Issue 143234: On the Monitor > Network Services > Non SD-WAN Destination via Gateway page of the Orchestrator UI, the tunnel status graph colors are not consistent.

A user can observe a new color for the same NSD whenever the graphs are re-rendered (for example, when a user changes the time period). The color for the NSD neighbor is changed by the UI because the NSD IP address order is changed, so the color is updated for the same NSD every time.

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 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 143625: Edge model 710 interfaces show up incorrectly in a profile after an upgrade to 6.0.x.

The *updateconfigurationmodule* API has no validation to prevent the removal of GE1 or any other mandatory interfaces and the result is that GE1 is missing from the Edge model 710.

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.

Fixed Issue 144053: On the VPN Services > Cloud VPN > Edge to Non SD-WAN Sites page of the Orchestrator UI, the Orchestrator may not update a change to this page.

If an enabled status is changed and the user switches to another segment, the enabled status is not updated properly.

Fixed Issue 144066: An Operator user configured for Sign Sign-On (SSO) authentication cannot be converted to use Native authentication (username/password).

Part of that process is to reset the user's password, but SSO users do not have a password in the Orchestrator database. So, when they reset the password, the Orchestrator looks for a current password and sees none and does not send the reset.

Fixed Issue 144140: A user with a customized role that denies them the privilege of Network Services - Create can still update Cloud Security Services (CSS) details on the Orchestrator UI.

Users with this customized role can access the Cloud Security Service list details in the **Configure > Network Services** section, and change CSS details.

Fixed Issue 144175: When a user makes a configuration change at the Profile level on the Orchestrator, they may observe that it takes a long time (up to 4 hours) for the changes to be applied to the Edges using the Profile.

The issue is related to the control plane spread factor variable, which is set in Orchestrator's System Properties. When a spread factor is set, the configuration update to the Edges is usually spread over a few heartbeats. For example, if the control plane update is set to 20, it should take up to 20 heartbeats for all Edges to receive the configuration update. When this issue is encountered, the spread factor does not work correctly and changes can take hours to be applied to all Edges in the Profile.

On an Orchestrator without a fix for this issue, the workaround is to trigger an Edge specific configuration change to force that Edge's control plane to update immediately.

Fixed Issue 144393: When an Orchestrator is upgraded to version 6.0.0.1, the Operator user may observe that the migration of some customer statistics fails.

The issue specifically impacts the */store2/velocloud/file_store* folder, causing operational disruptions by misaligning user and group information to its subdirectories and preventing the Orchestrator from processing the backlog of files mostly related to PATHSTATS.

Fixed Issue 144405: On the Edge > Configure page of the Orchestrator UI, the Assign Software Image box is missing a description of the Edge software image.

For each Edge software image the UI should include the description found in the Operator Profile but for this issue there is only the name showing.

Fixed Issue 144469: After an Orchestrator is upgraded to version 6.0.0.1 or higher, users who log in with Single Sign On (SSO) may have difficulty logging in.

With this issue, users are only able to authenticate after multiple attempts because some SSO logins are timing out too quickly on the Orchestrator.

Fixed Issue 144613: On the Edge/Profile > Configure > Firewall page of the Orchestrator UI, a user may observe they cannot save a Firewall configuration after modifying it.

This issue is found on Orchestrators upgrade to Release 6.0.0.1. After the upgrade to this version, legacy firewall rules are not being correctly updated, and this results in additional firewall module updates attempts to fail.

Fixed Issue 144622: On the Monitor > Network Services page of the Orchestrator UI, for a customer with Non SD-WAN Destinations via Gateway, they may observe that the page shows as empty with no information.

Whenever there is datacenter data without a *tunnelMode* field, this issue may be encountered.

Fixed Issue 144789: When an Orchestrator is upgraded to version 6.0.0.1, users may observe that they cannot download reports.

This issue can occur if the report storage location is not the default one, after the container is restarted the Orchestrator is looking for the reports in the default location and not the custom one.

Fixed Issue 144805: On the Configure > Edge > Device > Connectivity page of the Orchestrator UI, if a user attempts to remove a Wi-Fi LAN (WLAN) SSID to an interface and clicks Save on the dialog box, the WLAN removal is not reflected on the VLAN.

However, if the user then clicks **Save Changes** at the bottom, the WLAN then shows as removed from the VLAN.

Fixed Issue 144807: On the Configure > Edge > Device > Connectivity page of the Orchestrator UI, if a user attempts to add a Wi-Fi LAN (WLAN) SSID to an interface and clicks Save on the dialog box, the WLAN is not reflected on the VLAN.

However, if the user then clicks **Save Changes** at the bottom, the WLAN then shows up on the VLAN.

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.

Fixed Issue 145118: For a customer enterprise site with a High Availability topology, if Loss of Signal is configured on the HA Edge interfaces, a user may observe these configurations being removed on the Orchestrator UI.

The issue is inconsistent and when it occurs the configuration does not always disappear from all HA Edge interfaces.

Fixed Issue 145137: An enterprise migration may fail in the post-import stage.

During the post-import process, an Orchestrator API call is executed to the destination Orchestrator. With the latest changes in the node version, the import fails in the destination Orchestrator.

Fixed Issue 145167: A user may observe that they cannot update the Device settings configuration for a profile with the Orchestrator throwing an error.

The error may read: "validateProfileDeviceSettings: invalid enterpriseObjectId". A user can encounter this issue when an otherwise correct configuration has empty reference values present in the request. In such a case the Orchestrator backend validation does not allow the user to save the changes for device settings on a profile.

Fixed Issue 145301: Under Global Settings > Customer Configuration > Gateway Pools on the Orchestrator UI, if a user configures BGP on a Gateway and then disables BGP later, the BGP states are not removed and there is no BGP down event.

As BGPneighborSummary is empty from the Gateway after disabling BGP from Global Settings, as a result the Orchestrator has no information to update the states as removed.

Fixed Issue 145567: On the Configure > Edge > Overview page of the Orchestrator UI, if a user tries to change the profile the Orchestrator throws an error and prevents the user from saving the changes.

Issue is traced to an invalid license form, which is the result of the attribute control in the properties form becoming invalid as the license field is marked as required but the value is not getting patched properly from child to the parent component.

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, the Gateways are reverted back to the original Gateways already in use by the first NSD.

Fixed Issue 146143: On the Administration > User Management > Service Permissions section of the Orchestrator UI, if a user creates a new service permission for an Enterprise Standard Admin user where all DNS privileges are disabled, this user role can still perform all DNS activities.

The Orchestrator uses the wrong set of privileges for this service permission.

Fixed Issue 146323: On the Administration > Operator Profile page of the Orchestrator UI, if a user clicks on Operator Profile, the Operator Events page opens instead.

The fix ensures the expected result of loading the Operator Profile instead of the Operator Events page.

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 146551: On the Configure > Network Services > Non SD-WAN Destinations page of the Orchestrator UI, the UPDATE ALERTS button does not allow the user to change the alerts.

In particular, the user cannot switch the Alerts to Off and this is the result of a defect in the Orchestrator's backend validation for a VPN type prior to the Alerts enablement, which does not need a VPN type.

Fixed Issue 146576: When looking at the Monitor > Edge > Paths page of the Orchestrator UI, a Path quality score of 5 is showing the wrong color.

The Path Stats quality score of 5 should show as yellow but instead shows as red. The correct color codings are: <5 = RED, <8 = YELLOW, and GREEN for the rest.

Fixed Issue 146588: For a customer who has configured an Edge GRE tunnel, the customer may observe that the Edge GRE tunnel is down after upgrading to Release 5.2.3 or later.

The Edge was able to trim the extra space of the IP address before the upgrade, but post-upgrade the Edge does not trim the IP address and it becomes invalid due to that extra space.

The fix includes Orchestrator validations to prevent a user from adding an IP address with an extra space on the UI.

Fixed Issue 146831: On the Configure > Edges > Device > Interfaces page of the Orchestrator UI, when a user examines the segment configuration for an interface, they may observe that they cannot see the associated Edge interface for a particular segment.

Since the interface data is updated properly to the Edge, the segment associated with the interface in the profile is not displayed in the Edge segment drop-down.

Fixed Issue 147155: Customers deployed on an Orchestrator using Version 5.2.3.x or later 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.

Fixed Issue 147160: On the Administration > User Management > Service Permissions section of the Orchestrator UI, if an Operator Superuser applies role customization to an Operator Standard Admin and removes the Create, Update, and Delete "Customer Keys" privilege, the Operator Standard Admin can still navigate to Configure > Edge Overview > Properties and the "Encrypt Device Secrets" checkbox can be edited.

The Orchestrator is not correctly mapping the privileges for this custom role.

Fixed Issue 147195: On either the Configure > Edges or Monitor Edges page of the Orchestrator UI, if a user hovers their mouse pointer over the Edge Name, they cannot see the Edge Description.

The expected behavior is for a user to see Edge Description when hovering over the Edge Name.

Fixed Issue 147739: On the Configure > Edge/Profile > Device page of the Orchestrator UI, a user may observe that they cannot configure a VLAN for the segment they want.

In addition, the option list of segments includes one that is not in that profile.

Fixed Issue 147846: For Partners and Customers signed up for Zero Touch Provisioning (ZTP) on a 5.x Orchestrator, when the Orchestrator is upgraded to a 6.0.x version, the user may observe the ZTP sign-up page shows even though they are already signed up.

This is a cosmetic issue as the customer's ZTP functionality is still in effect on the Orchestrator, but users could not see inventory lists or assign Edges.

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 148873: When an Operator or Partner upgrades an Orchestrator to 5.4.0.x build, the user may observe that the upgrade fails.

The failure would show the following symptoms:

The package python3-update-manager was not upgraded, and its installation failed. WARNING - ========== VCO upgrade failed ==========

Starting with Release 4.0.0, a breaking change was introduced in the *python3-update-manager* which prevents its upgrade in subsequent Orchestrator releases. This issue becomes more prominent with Release 5.x Orchestrator versions due to additional sanity checks performed by the Orchestrator. As a result, users can encounter the warning message: **VCO upgrade failed** during the upgrade process and point to the *python3-update-manager* package. Despite this warning, the overall Orchestrator upgrade completes successfully, and there is no functional impact on the system beyond this package issue.

Fixed Issue 148874: A user may observe that when editing a VLAN where the Override is set to on, the "Done" button is grayed out and they cannot save the changes.

A user cannot save the changes made to the VLAN because the Orchestrator has a mandatory validation that is blocking the option to save.

Fixed Issue 149094: If a customer attempts to deploy a pair of Edge 720's as a High Availability pair and enable HA, they may observe that the HA Edges go offline.

This can occur if the customer performs an RMA Reactivation for the Edge 720s and then enables HA. Disabling HA before reactivation through RMA is not required and the user can directly perform the reactivation process which avoids the issue.

Fixed Issue 149139: On the Gateway Management > Gateways page of the Orchestrator UI, if a user clicks on the name of a Pool in the Gateways list, they may observe that nothing happens.

The user cannot be redirected to the Gateway Pool that is selected from the Gateways list.

Fixed Issue 149430: A user attempting to reactivate a Gateway through the Orchestrator UI may observe that the attempt fails.

The Gateway reactivation fails with the reason being a Gateway heartbeat failure. When the tunnelMode is ACTIVE_HOTSTANDBY and the primary Gateway is disabled and the Secondary Gateway alone is enabled for the redundant (and is active in the Gateway enterprise association), this will result in an exception being thrown at the Gateway heartbeat code while processing dataCenters for a Non SD-WAN Destination.

Fixed Issue 149768: On the Monitor > Edge > Flows page of the Orchestrator UI, flows with Route "Branch to Branch" may be missing Next Hop information.

With this issue, the flowPath indicates "Branch to Branch," but the corresponding Next Hop field remains empty. Issue caused by a defect in the mapping logic used to display the Next Hop name. The system failed to search the correct database tables for certain flowPath values. Specifically, for a flowPath value of 4 ("Branch to Branch via Hub"), the mapping logic only searched the Edge table for the next hop entity. However, when the next hop is a Hub Cluster, the information resides in the enterpriseObject table.

Fixed Issue 150038: When a customer attempts to configure a local DNS entry and that entry is > 32 characters, the Orchestrator throws an error stating the "Max length 32".

The RFC standard for a domain name is 253 characters while the Orchestrator was enforcing a 32 character limit. The fix lifts this limit and puts the Orchestrator in alignment with the RFC standard.

Fixed Issue 150435: An Operator may observe that the Gateway experiences three Dataplane Service failures in succession after upgrading the Gateway to a 6.0.0.x build.

The Gateway service fails due to an invalid type of neighborAsn. The Gateway is expecting the field as a string, and if the Orchestrator sends it as an integer this triggers an exception in the Gateway process which causes the service failure. A triple service failure requires a manual reboot from a user to recover and until that is performed, the Gateway does not pass traffic.

Fixed Issue 150669: The Partner Gateway Handoff option is incorrectly displayed as "None" when logged in with a partner account, while it correctly shows "Allow" when using an operator account.

The API getEnterpriseProxyGatewayPools is being invoked with an incorrect enterpriseProxyId value of 0 when logging in using a partner user account.

Fixed Issue 151380: On the Monitor > Edge > Overview page of the Orchestrator UI, a user may observe that under the Links column the UI shows the IP address versus the ISP name for that link.

The browser shows the error "No English found for key" and is the result of an incorrect implementation in HTML.

Fixed Issue 151576: On the Administration > User Management > Authentication section of the Orchestrator UI, a user may observe that they cannot configure Single Sign-On (SSO) for a Partner/ MSP account.

When encountering this issue, the user would observe that the **Update** button under the SSO table is grayed out and not accessible trying to configure SSO.

Fixed Issue 151696: On the Configure > Profiles > VPN Services > Gateway Handoff Assignment page of the Orchestrator UI, on page 2 a user may observe that the option to reorder the Gateway Handoff Assignments is not present.

With this issue drag and drop does not work properly for Gateway Handoff assignments due to an incorrect implementation of the *cdkDrag* & *cdkDropList*.

Fixed Issue 151785: Users may observe that the Orchestrator becomes slow and even unresponsive.

All users on an affected Orchestrator can encounter this issue if the customers using the Orchestrator make a large number of APIv2 calls, especially calls used for monitoring. An Operator user would observe that the Orchestrator CPU utilization was at 100%. The issue is the result of the Orchestrator experiencing an API database connection leak.

Fixed Issue 151927: For a customer enterprise where a Zscaler Cloud Security Service (CSS), when a user attempts to Edit the Zscaler CSS they may observe that the Sub Cloud value is not populated with a value when it should be.

If a Zscaler CSS is created with a Sub Cloud, the value is not displayed on the **Edit** screen. The user will see that the **Sub Cloud** field is blank like the value is not saved.

Fixed Issue 152022: On the Configure > Edge > Device > Interfaces page of the Orchestrator UI, when looking at a segment a user may not see the associated interface.

Since the interface data is updated properly to the Edge, the segment associated with the interface in the profile is not displayed in the Edge segment drop-down.

Fixed Issue 152178: On the Configure > Firewall section of the Orchestrator UI, if a user sets Syslog override to true and saves changes, then turns off the override and saves changes, the user may observe that the override will still show as true.

The Orchestrator UI enables the override flag based on the *syslog_forwarding* boolean variable. However, it is only checking the existence of the property but not its boolean value and this results in the UI ignoring the deactivation of the override.

Fixed Issue 152305: When viewing the Support panel on the Orchestrator UI, if a user clicks a link to a KB article for more information, they may observe that the link is broken.

The links were directed to a legacy kb.vmware.com URL, which is now decommissioned. The 6.1.0 Orchestrator updates the links to the correct knowledge.broadcom.com URL.

Fixed Issue 153208: For a customer enterprise configured to use two factor authentication (2FA) with SMS, administrators may observe that they do not receive the 2FA SMS message when attempting to log into the Orchestrator.

Arista VeloCloud uses Twilio to send the 2FA SMS messages and there is an issue where some countries (like Indonesia) require alphanumeric sender ID registration. Without this registration, the carrier blocks US originated SMS messages. The correction registers the Arista name in Twilio and ensures the messages are no longer blocked by a local carrier.

Known Issues

Open Issues in Release 6.1.0.

Edge/Gateway Known Issues

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 25742:

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

Issue 32960:

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

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

Issue 32981:

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

Workaround: There is no workaround for this issue.

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

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

Workaround: There is no workaround for this Issue.

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

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

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

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

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

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

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

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

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

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

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

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

Workaround: There is no workaround for this issue.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Workaround: Change the configuration to avoid the above scenario.

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

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

Workaround: None.

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

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

Workaround: There is no workaround for this issue.

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

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

Workaround: There is no workaround for this issue.

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

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

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

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

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

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

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

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

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

Orchestrator Known Issues

Issue 41691:

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

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

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

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

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

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

Workaround: There is no workaround for this issue.

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

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

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

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

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

Workaround: No workaround for this issue.

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

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

Workaround: There is no workaround for this issue.

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

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

Workaround: There is no workaround for this issue.

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

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

Workaround: An Operator user from technical support can assist the customer in configuring a workaround.