CloudVision

2025.1.0 Release Notes

03 April 2025 (version: 1.3)

Table of Contents

1. Release Highlights

Network Hierarchy for Campus Networks

Network Hierarchy transforms the way you monitor and manage your campus network by providing an aggregated view of metrics and telemetry across distinct network layers. With just a few clicks, you can drill down through the aggregated state of the network to individual interfaces, providing you with both high-level and granular perspectives of the network, device, and interface states. The new front panel view enhances this experience by delivering a snapshot of key interface metrics, enabling quick provisioning of interface configurations and efficient execution of diagnostics.

Decommissioning Devices with Studios

Device decommissioning for EOS and third-party devices now takes place through a workspace managed by the Studios infrastructure. You can decommission devices in Device Registration, the Inventory and Topology Studio, and on the Device Overview page. This new process ensures that devices are fully removed from CloudVision, dissociated from Studios, and all related configurations created in Studios are appropriately handled. Additionally, configurations for adjacent devices, such as upstream connections, are updated automatically, and a change control is generated. This enhance›ment simplifies device management and automates the process of removing devices from the management plane, improving efficiency and reducing manual effort.

Auto-Upgrade Streaming Agent during ZTP

By enabling the Auto-Upgrade Software during ZTP toggle, you'll now be able to automatically upgrade both the EOS image and Streaming Agent of a device to a user-specified version during Zero-Touch Provisioning (ZTP). This ensures that all ZTP-enabled devices in your network have custom-defined minimum EOS image and Streaming Agent versions.

Endpoint Overview, Search, and Filtering and Entity Details

The Endpoint Overview page has a new look and updated functionality that makes exploring network entities simpler than before. View all wired endpoints that have been detected on your network and use the sunburst diagram and filters to visualize the distribution of endpoints by their classification. Individual entity pages for both physical and virtual entities allow you to gain deeper insights into the state of the different entities on your network. You can also explore the states of all the wired endpoints on your network on the Wired Authentication page.

LDAP AAA Configuration

CloudVision now supports configuring LDAP servers for user authentication and authorization. With LDAP integration, user login credentials are verified against the LDAP server's database, enabling efficient authentication and authorization workflows. Depending on the server's response, users are granted access, ensuring secure and streamlined user management.

MSS Enhancements

Updates to CloudVision's Multi-Domain Segmentation Service (MSS) allow you to add multiple monitoring rules to a single policy, view the collected sessions that CloudVision used to generate rule recommendations, and redirect traffic to a third-party firewall. View traffic sessions used to generate a policy rule recommendation to determine if traffic is trusted traffic that should be allowed. Define redirect objects using a redirect gateway IP and configure redirect rules that govern which traffic is sent to the firewall. Provide more granularity to monitoring by adding a monitor object to any rule to target specific traffic flows for visibility.

Events

CloudVision is introducing a number of events to better assist you in monitoring your network and troubleshooting issues. We've added a RADIUS server connectivity event to notify you when RADIUS server probes for a device are all down, partially down, or not configured. You'll also discover two new events designed to help you diagnose the health of MLAG on devices where it is configured. The Device Experiencing Streaming Issues event will help you determine the cause of multiple streaming events associated with a single device. We've provided new supports for monitoring abnormalities in RX power, TX power, voltage, temperature, and TX bias for optical transceivers. These five events alert for all XCVR transceiver types and models supported by CloudVision.

Event Count Threshold Dashboard Panel

Events Count Threshold is a new view mode that you can select when configuring the Events summary panel in Dashboards. Use it to monitor for the presence and the scale of potential network issues by defining a threshold for the number of events matching selected filters. Panel buttons that display the number of matching events turn red when the threshold has been exceeded. Events can be viewed by clicking the button. Configure multiple event count threshold panels into a dashboard to see counts for multiple events at a glance.

PIM Neighbor Table

Protocol Independent Multicast (PIM) is an IP multicast routing protocol used for routing multicast data packets to multicast groups. If PIM is enabled, you can view information about a device's PIM neighbors to help identify routing issues. The PIM Neighbor Table includes details like the neighbor address, uptime, type of PIM and transport, the interface that the neighbor was detected on, and more.

Per-Device RBAC (Beta)

This release brings enhanced flexibility for network management with the introduction of role-based access control for devices. Gain more granular control over provisioning by assigning users permissions for specific devices. These permissions cover key product actions, including workspace submission, change control configuration and execution, and device decommission, empowering you to streamline access control for your operations.

CloudVision-Managed Recorder Node (Beta)

The CloudVision-driven Recorder Node makes packet capture and querying simple and accessible. Traditional packet capture devices sit outside of the production network and involve a separate interface and distinct workflows. The Recorder Node is managed by CloudVision so that network management, packet capture, querying, and analysis can be done all in one place. Use Recorder Node packet capture and querying to provide point-in-time network visibility for troubleshooting. Create a packet capture session to mirror selected traffic from EOS device interfaces to the Recorder Node. Query the Recorder Node to analyze captured packets or generate packet capture (PCAP) files for use in a third-party network protocol analyzer.

For details refer to the Help Center.

2. Supported Scale

2.1 Cluster Scale

CloudVision 2025.1.0 supports provisioning and monitoring on the scales described below when deployed with the default recommended VM resources identified here. The number of active interfaces includes the number of physical (Ethernet) and virtual (port channel, VLAN, etc) interfaces that are actively processing traffic. A high performance NAS refers to network attached storage that performs similarly from a read/write bandwidth perspective to locally attached SSDs. HDDs are not supported. CPUs can be either physical or hyperthreaded cores. Note that CloudVision supports single-node deployments only for lab environments of 25 or fewer devices. Required resources include 28 CPUs, 52GB RAM, and 1TB SSDs.

Cluster Deployment	Per-Node Resources	Number of Devices	Number of Active Interfaces	Flow Tracking	WIFI Supported
Multinode	28 CPUs, 52G RAM, 2TB SSDs or high performance NAS (DCA-250-CV w/ extended disks, DCA-300-CV)	1000	100000	5K flow updates/sec	Yes
Multinode	70 CPUs, 116G RAM, 6TB SSDs or high performance NAS (DCA-350-CV)	2000	200000	5K flow updates/sec	Yes

2.2 Scale Breakdowns

The maximum number of devices supported on a given cluster depends on the average number of active interfaces per device, which can vary based on the deployment type.

Supported Scale	Datacenter (Average 80 Active Interfaces/Device)	Campus PoE (Average 50 Active Interfaces/Devices)	CloudEOS (Average 8 Active Interfaces/Device
1000 Devices and 40K Active Interfaces	500	800	1000
1000 Devices and 70K Active Interfaces	875	1000	1000
1000 Devices and 100K Active Interfaces	1000	1000	1000
2000 Devices and 200K Active Interfaces	2000	2000	2000

2.3 Provisioning action scale limits

Action	Maximum Actions
Concurrent Running Tasks	500
Simultaneous Device Moves from the Undefined Container to Another Container	500
Simultaneous Device Moves from One Container to Another	500

3. Important Functionality Changes

CloudVision Upgrades

CloudVision 2024.3 included a transition from CentOS to AlmaLinux EL9. As a result, upgrades from 2024.3 onward require a full reinstall of the base operating system. This offers a number of benefits, but requires a reboot, a longer network management maintenance window for the upgrade process, and means that any customizations not described by the cvpi shell, such as cronjobs or firewall rules, will be lost and need to be reapplied. Some user-created Python scripts may not be compatible with the new OS, halting the upgrade process and leaving the base OS unchanged. Hardening configurations will need to be re-applied with each upgrade. A backup or copy of any custom configs should be kept somewhere off of the CloudVision Appliance.

Single-Node VM Resource Requirements

The resource requirements to run a single-node CloudVision VM instance have increased. The minimum resources are 28 CPUs and 52 GB of RAM. See System Requirements for more details. Note: A single node CloudVision cluster is not recommended for use in production environments. It may be used for testing or in lab environments.

eAPI-over-TerminAttr

eAPI over HTTPS is deprecated in this release. We plan to stop supporting this feature in future CloudVision releases and recommend switching to eAPI over TerminAttr by turning on "Advanced login options" toggle on the Settings page.

Updates to Built-In Studios When Upgrading CloudVision

During the CloudVision upgrade process, built-in studios may introduce updates to their functionality. These updates are applied within a system-generated workspace listed on the Workspaces page. In the case where the changes result in device configuration, the user must take steps to accept these changes. For more information, please refer to the Studios Upgrade Guide

Hypervisor support for x86-64-v2 CPU flags

The hypervisor must expose the x86-64-v2 CPU flags to the CloudVision virtual machine.

Update to AAA Server field

The 'UserID' field in the AAA server model has been renamed to 'CreatedBy'. This field represents the user that created the AAA server config

4. Upgrading to CloudVision 2025.1.0

Upgrade to the CloudVision Portal 2025.1 train is supported from existing systems running 2024.2 or above. Clusters running earlier release trains should first be upgraded to the highest supported release (currently 2024.2.2 or 2024.3.1) before upgrading to the 2025.1 train. The upgrade path follows the latest release in each major version of CloudVision, for more details please refer to the upgrade path tool on the Arista Support page.

The following steps can be taken at any point on an existing cluster as part of preparing for an upgrade to 2025.1.0.

Upgrade Checklist

1. Ensure that all devices are successfully streaming to the CloudVision cluster
2. Ensure that all devices are in image and config compliance
3. Verify that devices have TerminAttr 1.19.5+ installed (1.31.7 recommended)
4. Upgrade all EOS devices under management to an EOS 4.23+ release train
5. If not already upgraded to the 2025.1 release train then upgrade existing CloudVision clusters to at least the latest 2024.2 release (currently 2024.2.2 or 2024.3.1)
6. CloudVision Appliances should be running CVA version 6.0.5 or later
7. Ensure that all tasks are in a terminal state (Success, Failed, or Canceled)
8. Ensure that all change controls are in a terminal state
9. Take regular backups of CloudVision, including a final backup prior to upgrade
10. It is recommended that a console be connected to the primary CloudVision cluster node
11. Allow a 3-hour network management maintenance window for the upgrade process

5. Deprecated and Backwards Incompatible API Changes

CloudVision APIs are marked as deprecated at least one release train prior to removal, with instructions provided on the alternative API to use. The following APIs have been deprecated or removed. Transition all use of deprecated APIs to the alternative provided. See <a href='https://aristanetworks.github.io/cloudvision-apis/'>here</a> for more on CloudVision APIs.

Service: /cvpservice/event

Request: /event

- Deprecated in 2020.2
- Planned deletion in 2025.2

Service: /cvpservice/inventory

Request: POST /inventory/deleteDevices.do

- Deprecated in 2020.1
- Deleted in 2020.3
- Replaced in 2020.1.0 by DELETE on /inventory/devices

Service: /cvpservice/login

Request: GET /login/home.do

- Deprecated in 2020.2
- Planned deletion in 2025.2
- Can be replaced by a call to any other API, which will return a 401 if the session is not valid

Service: /cvpservice/provisioning (also available at /cvpservice/ztp)

Request: GET /provisioning/getconfigfortask.do GET /provisioning/v2/getconfigfortask

- Deprecated in 2020.2
- Planned deletion in 2025.2
- Replaced in 2018.2.3 by /provisioning/v3/getconfigfortask

Request: /provisioning/runConfigSync.do

- Deprecated in 2020.2

- Deleted in 2020.3
- Replaced in 2018.2.3 by /provisioning/checkCompliance.do

Request: POST /provisioning/validateAndCompareConfiglets.do

- Deprecated in 2020.2
- Deleted in 2020.3
- Replaced in 2018.2.3 by /provisioning/v2/validateAndCompareConfiglets.do

Request: POST /provisioning/checkCompliance.do

- Deprecated in 2020.3
- Planned deletion in 2025.2

Service: /cvpservice/task/

Request: GET /task/getLogsById.do

- Deprecated in 2020.1
- Deleted in 2020.3
- Replaced by /cvpservice/audit/getLogs.do

Service: /provisioning/devices/

Request: POST /provisioning/devices/

- Deprecated in 2023.1
- Planned deletion in 2025.2

Service: api/v3/services HTTP APIs of AAA settings

Request: api/v3/services/arista.aaa_setting.v1.AAASettingConfigService

- Deprecated in 2024.2
- Planned deletion in 2025.2
- Replaced in 2023.2 by /api/resources/aaa_setting/v1/* APIs

Service: api/v3/services HTTP APIs of SSO Providers

Request: /api/v3/services/arista.identityprovider.v1.OAuthConfigService /api/v3/services/arista.identityprovider.v1.SAMLConfigService

- Deprecated in 2024.2
- Planned deletion in 2025.2

- Replaced in 2023.2 by /api/resources/identityprovider/v1/* APIs

Service: api/v3/services HTTP APIs of Service accounts

Request: /api/v3/services/arista.serviceaccount.v1.AccountConfigService /api/v3/services/arista.serviceaccount.v1.AccountService /api/v3/services/arista.serviceaccount.v1.TokenConfigService /api/v3/services/arista.serviceaccount.v1.TokenService

- Deprecated in 2024.2
- Planned deletion in 2025.2
- Replaced in 2023.2 by /api/resources/serviceaccount/v1/* APIs

Service: api/v3/services HTTP APIs of admin.Enrollment

Request: api/v3/services/admin.Enrollment

- Deprecated in 2024.2
- Planned deletion in 2025.2
- Replaced in 2023.2 by /api/resources/admin.Enrollment/* APIs

Service: ccapi

Request: /api/v3/services/ccapi.ChangeControl

- Deprecated in 2023.1
- Deleted in 2023.3
- Replaced in 2021.1 by the Change Control resource API

Service: tag.v1

Request: /api/resources/tag/v1

- Deprecated in 2023.1
- Deleted in 2024.3
- Replaced in 2022.1 by tag.v2

6. Compatibility

6.1 Supported Browsers

Browser	Version
Google Chrome	115+
Mozilla FireFox	115+
Microsoft Edge	115+

6.2 Supported CloudVision Appliances

CloudVision Appliance Version	Supported CVA Version
1.1.x	Not Supported, Upgrade Required
1.2.x	Not Supported, Upgrade Required
2.0.x	Not Supported, Upgrade Required
2.1.x	Not Supported, Upgrade Required
3.0.x	Not Supported, Upgrade Required
4.0.x	Not Supported, Upgrade Required
5.0.x	Not Supported, Upgrade Required
6.0.0 - 6.0.4	Not Supported, Upgrade Required
6.0.5+	Supported CVA Version
7.0.0+	Supported CVA Version

6.3 Supported HyperVisors

Hypervisor	Supported Hypervisor Version
VMware ESXi (recommended) Hypervisor	6.7.0 and above
KVM	qemu-kvm 1.5.3+ and libvirt 4.5.0+

6.4 CentOS Version for RPM Installer

CloudVision Portal Version	Supported OS Version for RPM Installer
Supported versions for RPM Installer 2020.2 - 2021.1	CentOS Minimal 7.7.1908
Supported versions for RPM Installer 2021.2 - 2024.2	CentOS Minimal 7.9.2009
Supported versions for RPM Installer 2024.3+	AlmaLinux release 9.4

6.5 Supported EOS Versions

CloudVision Portal Version	Compatible EOS Versions
2025.1.0	4.23 - 4.33.0F

Though EOS versions 4.22 - 4.25 are supported by CloudVision, they are EOL. The recommendation is to upgrade.

6.6 Supported TerminAttr Versions

6.6.1 Supported Versions

CloudVision Portal Version	Bundled TerminAttr Version	Minimum TerminAttr Version	Recommended TerminAttr Version
2025.1.0	1.28.2	1.19.5	1.31.7

6.6.2 TerminAttr Version Bundled by EOS Version

EOS Version	Bundled TerminAttr Version	TerminAttr Extension Required
EOS 4.21 - 4.23	< 1.8.0	Yes, 1.19.5+ recommended
EOS 4.24.0F	1.8.0	Yes, 1.19.5+ recommended
EOS 4.24.1	1.9.0	Yes, 1.19.5+ recommended
EOS 4.24.2	1.10.0	Yes, 1.19.5+ recommended
EOS 4.25.0	1.11.0	Yes, 1.19.5+ recommended
EOS 4.25.1F	1.12.1	Yes, 1.19.5+ recommended
EOS 4.25.2F	1.13.1	Yes, 1.19.5+ recommended
EOS 4.25.5M	1.13.7	Yes, 1.19.5+ recommended
EOS 4.26.0	1.14.0	Yes, 1.19.5+ recommended
EOS 4.26.1	1.15.2	Yes, 1.19.5+ recommended
EOS 4.26.2	1.16.2	Yes, 1.19.5+ recommended
EOS 4.26.7M	1.19.5	No
EOS 4.27.0	1.17.0	Yes, 1.19.5+ recommended
EOS 4.27.1	1.18.1	Yes, 1.19.5+ recommended
EOS 4.27.2	1.19.0	Yes, 1.19.5+ recommended
EOS 4.27.4.1M	1.19.4	Yes, 1.19.5+ recommended
EOS 4.28.0F	1.20.0	No, but 1.22.1+ recommended
EOS 4.28.1F	1.21.0	No, but 1.22.1+ recommended
EOS 4.28.2F	1.22.1	No
EOS 4.29.0F	1.23.0	No, but 1.24.2 recommended
EOS 4.29.1F	1.24.2	No
EOS 4.29.2	1.25.0	No
EOS 4.29.3	1.25.1	No
EOS 4.30.0F	1.26.0	No, but 1.28.2+ recommended
EOS 4.30.1F	1.27.0	No, but 1.28.2+ recommended
EOS 4.30.2F	1.28.0	No, but 1.28.2+ recommended
EOS 4.30.3M	1.28.0	No, but 1.28.2+ recommended
EOS 4.31.0F	1.29.0	No
EOS 4.31.1F	1.30.0	No
EOS 4.31.2F	1.31.0	No
EOS 4.31.3M	1.31.3	No

EOS Version	Bundled TerminAttr Version	TerminAttr Extension Required
EOS 4.31.4M	1.31.4	No
EOS 4.32.0F	1.32.0	No
EOS 4.32.1F	1.33.0	No
EOS 4.32.2F	1.34.0	No
EOS 4.32.3M	1.34.1	No
EOS 4.33.0F	1.35.0	No

6.7 Supported CloudVision Extensions

The following minimum versions are required for common applications that can be installed as CloudVision extensions. If you have previously installed one of these applications, you must upgrade it to the minimum version prior to upgrading your cluster to 2025.1.

Application	Minimum Supported Versions
CloudBuilder	v2.4.7+
IPAM	v.1.3.3+
ServiceNow	v1.6.1+
CVPRAC Python Library	v1.3.1+

6.8 Supported CloudVision-Wifi

Bundled CV-Wifi Version
wm-v18.0.0-179 CV-CUE - 2024.12.06.2

7. Resolved Caveats

Cluster Deployment and Management

Severity 1 / Severity 2

- CloudVision in rare instances may become inoperable due to a cleanup routine causing heavy load on HBase.

  Work around the issue by disabling and then stopping aerisdiskmonitor by running the following commands on a shell on one of the CloudVision nodes:
  cvpi disable aerisdiskmonitor
  cvpi stop aerisdiskmonitor (1076548)

- Upgrading CloudVision on AWS will bootloop on the dracut upgrade step. (1039643)

- When upgrading, if a configlet script contains the word "import" and is not used for the importing of a python library, the upgrade will be blocked until the line is removed. The upgrade code has been enhanced to make it more discerning, only activating when the "import" keyword applies to a python package import. (1061634)

- When doing default backup restore (not using translate), tags may stop working within studios and generate no matches.

  If this happens backup restore could be performed using translate (not default):

  For using the translate variant of backup/restore, please refer to the most recent backup/restore documentation.
  At present, to restore using translate, run as cvp user, and set the required environment variable, before the restore is executed:
  export RESTORE_SYNC={}; cvpi restore cvp cvp.<timestamp>.tgz eosimages.<timestamp>.tgz (1077134)

- CloudVision cluster upgrade does not abort when the user responds "n" to the OS upgrade acknowledgment. (1098081)

- CVP installs that use the cvp-<version>-kvm.tgz or cvp-<version>.atswi images will result in the CVP VM having only a single interface.

  For KVM installs, this can be fixed by editing the cvpTemplate.xml file to include a second interface prior to install. For atswi installs, this can be fixed by patching the install via virsh edit after install instead of fixing this in the template. In either case, please reach out to your support representative for guidance. (1101834)

Severity 3

- For DNS servers configured with long timeout or for complex DNS setups, "cvpi debug all" can take a long time (sometimes over an hour). Workaround is to modify the /cvpi/conf/debug.yaml and add "-n" flag to the below commands so that they look like below:
netstat: ["sudo", "netstat", "-n", "-p", "-a", "-W", "-v", "-e", "--numeric-ports"]
netstat_statistics: ["netstat", "-n", "-s"] (795389)

Network Provisioning

Severity 1 / Severity 2

- ZTP may not succeed when a large number of devices are trying to ZTP against a CV cluster. (1018061)

- When a user starts executing a changecontrol, the changecontrol doesn't seem to progress and there are no logs seen in change control. Similar behavior can be seen with dashboards page, devices page, etc. where the page doesn't load or workflows are stuck.

  The workaround is to restart ambassador:
  - kubectl delete DaemonSet/ambassador
  - cvpi start ambassador (1084465)

- Virtual Router Deployment screen fails to load. (1095395)

- Device decommissioning might fail with the error "Failed to delete references to the device". (928028)

- Set Config action for a device in ZeroTouch mode may fail when bringing device out of ZeroTouch mode (949086)

- While running change control actions (Set Image, Set Configuration, etc) if there is an error reaching the device using 'show version', 'show redundancy status' eAPI commands, the actions will be retrying for 24 hours, instead of the user configured action timeout. Users can stop the change control for these stuck actions. (969812)

- Containers in the Static Configuration Studio were incorrectly displayed as removed in the View Modification Details screen (1028496)

- Logs in custom python actions are not visible in the Change Control log panel. Changing python script logging to use ctx.alog(<message>, customKey=ctx.action.ccId) will cause future runs of the action to have the logs appear (1029624)

- Configlets in the Static Configuration Studio created prior to 2024.2.0 cannot be seen in the Configlet Library. (1041701)

- After a changecontrol-manager app restart, if an attempt is made to stop a running CC, changecontrol-manager can end up deadlocked. This prevents all other change controls from running or stopping.

  Workaround: cvpi stop ambassador && cvpi start cvp (1041161)

Severity 3

- The "Onboard Devices" menu under the "Add Device" button does not support device registration using IPv6 addresses (952619)
- Change Control action count in the Action Summary section may show inaccurate percentage due to rounding errors. Review the actual counts for precise information. (961140)
- Improved copy/pasted functionality for the tag query editor (981362) (1)
- When viewing a single change control, the search input will show all actions and stages when no matches are found. The expected behavior is to show no actions and a message indicating that filtering is active. (982615)
- The page controls in the Access Configuration Modal were partially clipped. They are no longer clipped. (1032293)
- Dropdown options whose widths were greater than the width of the original dropdown would be clipped with an ellipsis. If 2+ options had the same prefix that spanned the visible width, it was not possible to distinguish one option from another. Now, options that are wider than the original dropdown are displayed with their full width. (880341)
- When there are many registered devices in Studios, trying to add a Device in the Static Configuration Studio may result in a hard to use scrollbar, forcing the user to scroll to the bottom of the modal to click on the Add Device Button. (1050612)
- The Studios Software Repository defaults the Reboot Required flag to False for EOS swi files that do not start with 'EOS' (1042089)
- The information displayed when hovering over an entry in the "Existing Assignments" column in the Software Repository table and the "Devices" column in the Software Assignment table of the Software Management Studio may be incorrect for devices that have once been assigned but were later decommissioned. (965353)
- Sometimes, when editing a tag query in Studios, the Clear, Save, and Help buttons do not work. (1058504)
- Inputs that have dynamic options may have their values cleared or changed unexpectedly if any of multiple source entries is changed or deleted.

Example in Enterprise Routing Studio - BGP Peers VRF values are built from Routed Interfaces and SVIs VRF values. If any of the interfaces that are part of a specific VRF are changed or removed then all BGP peers with that VRF see their entries changed or removed to match. Even if there are other interfaces with the same VRF that aren't changed. (1049462)

Limitations and Restrictions

- Management connectivity can only generate config for devices with either Management0 or Management1 as the primary management interface. (1048043)

Telemetry

Severity 1 / Severity 2

- Inconsistencies across turbine-generated data within CloudVision may result when backend turbine components exit unexpectedly during their start-up phase. Components may still process data received while exiting, producing invalid writes based on incomplete input data. (1051431)

- Dashboards could crash when input panels are configured to subscribe to other inputs. (1104830)

- In Topology, filtering Inband Telemetry paths using the checkboxes in the Flows sidebar does not function. (1023751)

- For a freshly configured Wifi Connector, the "View in CV-CUE" button is not displayed in the Infrastructure Access Points and Wireless Endpoints sections in the "Campus Health Overview" dashboard. This can be fixed by running the following commands. Knowledge of Wifi customer ID is required to execute these steps. SSH into any of the CloudVision nodes as the root user and run the following commands.
1. /cvpi/apps/aeris/bin/aeris-cli create dataset --storage hbase --storageoption table=aeris_v2 --storageoption zkquorum=localhost:2181 --type device --org Default --name "WIFI_CONTROLLER/<wifi-customer-ID>"
For a multinode setup, replace the zkquorum storage option value with "${PRIMARY_HOSTNAME}:2181,${SECONDARY_HOSTNAME}:2181,${TERTIARY_HOSTNAME}:2181"
2. /cvpi/apps/aeris/bin/aeris-cli --storageoption zkquorum=127.0.0.1:2181 --storageoption table=aeris_v2 permission --org "Default" --srcName "WIFI_CONTROLLER/<wifi-custmore-id>" --srcType "device" --targetName "AllDevices" --targetType "group" --perm "inherit" --inherit true
zkquorum needs to be replaced here as well for a multinode setup.
3. cvpi stop apiserver && cvpi start all
The UI needs to be refreshed after all the commands are run successfully, the "View in CV-CUE" button should be available. (1023792)

Severity 3

- ChangeControl services in CloudVision generate app audit logs for various actions. Some of these logs are not really audit logs but are Change Control execution logs which show up on the UI. These are also being exported as syslogs along with other audit logs. These logs will not exported from 2024.4.0 release. (924782)

- Improved copy/pasted functionality for the tag query editor (981362) (1)

- Change control groups will no longer stay active for 1 hour after all the inner events have ended, if the Change Control Succeeded event or Change Control Failed event is part of the group it will end immediately. (985064)

- Device Hardware Capacity donut graphs have been removed as they were considered to be misleading. (1007023)

- Datapoints on various time aggregated metrics might linger even after the data source has been removed/deleted, possibly resulting in stale dashboards. The potentially affected metrics are: fan speed, XCVR DOM metrics, device temperature, power supply readings and inlet temperatures. (1013571)

- When filtering events by a decommissioned device the Event List will be empty and the Summary title will show 0 Events, but the Summary graph will sometimes show non-zero results. (1029307)

- When device statuses are churning, the Event Timeblock panel may experience flickering (1038783)

- When viewing DOM metrics, some large time windows can show N/A even though aggregate data is present. (1035170)

- When CV Syslog Events are active and event generation rule changes are made which should result in the event ending, the event may fail to end and remain stuck active if the backend component responsible for ending the event was down/restarting at the time when the rule change was saved. (1042406)

- Inputs starting with 'devices:' may reset while typing if there are device status updates rapidly occurring in the system (1045264)

Limitations and Restrictions

- The Event Notification Microsoft Teams sender platform uses an old template format that is nearing deprecation on the Microsoft Teams side. (992699)

8. Known Software Caveats

Cluster Deployment and Management

Severity 1 / Severity 2

- When creating or editing a provider in Settings > Access Control > Providers, the save button is disabled initially and there is no obvious indication of what needs to be done to enable the save button. The red asterisk on each field indicates that it is required, but this is not explicitly described. (818479)

- In the Settings > Provider section, when modifying the client ID of an existing OAuth provider, the client secret must also be input and will become a required field in order to save the changes. Other than the changing of the required icon by the client secret field, there is no explicit warning or notification that it is now required and must be input. (884140)

- On rare occasions, CloudVision cluster nodes may experience high filesystem inode usage due to the ClickHouse backend database creating too many small files. Some symptoms include CloudVision portal errors and cvpi commands failing with errors such as "Error in processing command: ZK lock could not be created". Inode usage can be checked with the linux "df -i" command.

  Inode usage can be reduced by removing files under /data/clickhouse/data/*/*/detached/* folders. (1009690)

- This bug can be hit when upgrading from CVP versions lower than 2024.3.0 to 2024.3.0 or higher, where the default gateway is setup on the cluster interface.
  Starting from 2024.3.0, we setup the default gateway on the "device" interface only and if there is a mismatch the upgrade will fail with an error "Not proceeding with upgrade. Default gateway of node <node-ip> is <gw-ip> and and is different from <gw-ip> as stated in the cvp-config.yaml"

  Users can wait for the next CVP maintenance releases (2024.3.3 or 2025.1.1) for the fix and not proceed with the upgrade in this case. (1055134)

Severity 3

- Space check during upgrade to 2025.1.0 might complain about lack of sufficient space in root partition despite not strictly needing the space to complete the upgrade.
  The workaround is to clear sufficient space on the root partition before proceeding with the upgrade. (1112159)

Network Provisioning

Severity 1 / Severity 2

- CloudVision 2024.3.0 and greater operating in FIPS mode will fail to upgrade EOS releases older than 4.32.0. Temporarily disabling FIPS mode on the nginx server and upgrading the EOS devices is the only workaround.

  The workaround is:
  1. ssh into a CVP node and disable FIPS mode in nginx with: kubectl set env daemonset/nginx-app ARISTA_ENABLE_FIPS=0
  2. verify with: kubectl exec -it $(kubectl get po -l="app=nginx-app" -o name | head -n 1) -c nginx -- openssl version (should display the openssl version only and not "FIPS mode is enabled")
  3. go to the UI and run the EOS upgrades
  4. after the upgrades have completed, ssh into a CVP node and reenable FIPS mode in nginx with: kubectl set env daemonset/nginx-app ARISTA_ENABLE_FIPS=1
  5. verify with: kubectl exec -it $(kubectl get po -l="app=nginx-app" -o name | head -n 1) -c nginx -- openssl version (should display "FIPS mode is enabled" and the openssl version)

  This workaround is meant to be temporary and only enabling EOS upgrades for releases older than 4.32.0. The kubernetes config changes won't persist across cvpi commands (cvpi stop, cvpi start, cvpi config, etc.). (1034941)

- Moving actions from one stage in a change control to another stage results in the action erroneously appearing in both stages. (1072418)

Severity 3

- The software management repository has a download/export feature which does not work when there are table filters applied. The download functionality exports the whole table in the repository irrespective of filters. (949593)

- Large scale change controls that execute all actions in parallel might cause a browser out of memory crash. The browser crash has no impact on the backend execution of the change control. A page refresh will rectify the issue. (955162)

- The Change Control "Action Summary" gauges do not indicate red failed stages until the change control is complete. While the change control is in progress, failed stages or actions will be rendered as blue. (969185)

- The latest successful device onboarding attempt overrides the previous failed ones. In this case, the user cannot see the failed attempts. (992647)

- Software listed in the Software Management Studio assignment page drop-down box may not be ordered by version (1005935)

- When a device is decommissioned, there are a small number of places in Campus Fabric, Mirroring, and MSS Service Studios where related inputs are not removed, and they have to be removed manually. This does not cause any issue with the functioning of the Studio. (1022244)

- The Campus Fabric Studio can sometimes generate an invalid MLAG interface ID when modular interfaces are used in a port channel for MLAG. (1024151)

- At the moment 32 Set Image actions are executed in parallel. In case a change control has large number of Set Image actions, and the Set Image action timeout is at the default 1 hour limit, this timeout might not be sufficient. Increasing the timeout to a larger value will help in executing all actions within the change control. (955184)

- Long device query strings or queries that capture many devices in the software management studio assignment page can appear truncated. These can be scrolled when the user hovers on the row to view the whole query. (1045010)

- When using the "Add Campus Devices" quick action to onboard devices that are in ZTP mode, configuration items that provide connectivity to CloudVision may be marked for removal as part of the onboarding. Examples include config for Streaming Agent (TerminAttr), DNS, NTP, IP Address, and static routes. Users should review the quick action's proposed config and ensure necessary configuration is preserved via the Static Config studio's reconcile functionality. (1001108)

- Usually seen when there are multiple Campus Pods. NodeIds are not reliably auto-generated unless the user refreshes their browser's tab before triggering the auto-generation. (1089782)

- Hidden static arguments for python action scripts cannot be saved (1096045)

- If user has created a change control with a schedule timestamp, there is a possibility that on the change control overview and detail page, this change control disappears and reappears on refreshing the browser. This behavior can be seen even after the schedule timestamp is removed. (1112188)

- If already using the evpn-services studio with the enterprise-routing studio, then the upgrade of the evpn-services studio may not proceed. In this case, the upgrade can be deferred, and the two studios can continue to be used together.
If the evpn-services studio is upgraded to a version that has this issue, then subsequently trying to use the evpn-services studio with the enterprise-routing studio may fail, with a studio build error of the form: "Only 1 data center role should be applied to the switch."
Workarounds will require TAC involvement. (1087228)

- When the Submit Workspace button is clicked twice in quick succession, the resulting Change Control may not include all modified devices. The workaround is to edit the Change Control to include any missing devices. (1117615)

Packet Capture

Severity 1 / Severity 2

- After internal certificate authority rotation at CloudVision, previously onboarded recorder node will stop communicating with the CloudVision. In order to resume the communication, the recorder nodes need to be re-onboarded with a newly generated onboarding token. (1033384)

Severity 3

- When modifying the ACL from present to absent, the session parameters cannot be correctly applied to the session. The session creation needs to be abandoned.
  Reopen the Create Packet Capture Session modal to create a new session with the correct ACL option or without the ACL option, and remove the original session as needed. (1081910)

- For the CloudVision Managed Recorder Node feature, the name of a decommissioned recorder node can show up in the create capture session page. This limitation does not have any functional impact. (987128)

- Changes to packet capture session parameters, specifically when transitioning a parameter from a present to an absent state, are not immediately reflected in the session table display. Currently, a manual page refresh is required to view the updated session information. (1017375)

- The GUI may incorrectly display the state of packet capture sessions even when they have been updated.
  Users may need to refresh the page in browser to view the updated status. (1023309)

- Following a recorder node reboot, packet capture sessions established prior to the reboot may display outdated statuses, even if the node is operating normally. To correct this, manually deactivate and then reactivate any affected packet capture sessions. (1032090)

- When configuring a packet capture session based on device/interface selection, the system will initially display "1 interface selected," reflecting the requirement for at least one device/interface to be specified. (1061317)

- Recorder node profile update invalidates the filter criteria of capture sessions.
  The intended set of filters (e.g., device, interface etc.) need to be reselected after modifying or setting of the recorder node profile. (1071122)

- DSCP values must be between 0 and 63. Entries outside this range will be automatically adjusted to the nearest limit (0 or 63). (1086205)

- When editing an existing query, changing the query type does not automatically reset the Protocol.
The protocol option needs to be manually updated to the desired selection. (1086325)

- Large PCAP files from packet queries may cause Recorder Node upload failures with the error "Failure on the recorder node: (Error occurred while archiving query response. Check floodlight log)." To avoid this, please refine your query with a shorter time range and more specific filters to reduce the data volume. (1086870)

- The GUI displays Recorder Node ingress rates at 1/8th of actual values on the device details page and when creating packet capture sessions. Multiply shown rates by 8 for accurate measurements. (1073607)

- The operational mode of a recorder node must be set via the "management self" configuration mode command. (1126427)

Telemetry

Severity 1 / Severity 2

- Events of type Syslog Event Detected could get generated for a mix of fields (text, mnemonic, facility, severity, progName) belonging to different log messages in the scenario where a syslog log was followed by a non syslog log and the combined state of the fields match the event generation criteria. (1034297)

- The "Wireless Client Health" panel in the Network Hierarchy access-pod overview page may show incorrect counts. See CV-CUE for accurate information. (1044304)

- The traffic flows stacked area graph may incorrectly display no data for a few seconds at the start or end of the graph. This is most noticeable for small time windows. (1087362)

- The stacked area graph in the traffic flows page may show an incorrect "Other" line if the selected time window is less than 1 minute. To avoid seeing incorrect data, select a time window that is larger than 1 minute. (1084441)

Severity 3

- The "LLDP Neighbour states" will not show the "Disconnected" state, if the state is disconnected at the beginning of the selected time period. (1018103)

- When filtering Inband Telemetry flows by path using the Topology Flows sidebar, the filters no longer reflect on the graph after the flow data refreshes. (1031296)

- When filtering out all Inband Telemetry flow paths in Topology, the Filter to Flow toggle switches off if it was previously on. (1031299)

- Within the Telemetry Browser page when a user is switching from one device to other in the device selection dropdown, this operation can be slow and take 10-15 seconds. (1031879)

- When an 802.1X supplicant moves to another port and back to the original port, the table may show the Auth Mode of the supplicant as (unknown). (826161)

- The space for the row label of the time blocks is relatively small and truncates at the end, making it hard to differentiate long device names with the identifier at the end of the name. Hovering over the label will show the full value (1041656)

- Without Event Notifications sent to external endpoints, the CloudVision Event source url available in Microsoft Teams alert does not provide a hyperlink. (1047492)

- For device event component event layouts which show a "Adjacent Device" panel which is intended to show the state of directly connected devices, this panel may incorrectly show "No adjacent devices". (1033203)

- The IP address of 802.1X supplicants may not be visible in the 802.1X device table if the IP addresses was learned though another protocol by CloudVision. (1044586)

- 802.1X supplicants that re-authenticate with cached results may show an authentication status of TIMEOUT in the 802.1X pages. (1031688)

- Several timezones are missing from the Timezone selectors in Google Chrome. This issue is specific to Chrome and does not occur in Firefox since it still supports legacy timezones such as UTC/WET. This is not a functional limitation as the timezones are still available under different names. For example, 'Europe/London' is the same as 'UTC'. (1055911)

- The 802.1X device pages may take longer to load when there's a lot of history built up over time, regardless of how many authenticated endpoints are currently present on the device. (1056137)

- When viewing an event counts dashboard, the total number of events may not match the total on the events page. The events app is only showing events that started during the selected time window. The events dashboard is showing events that started during the selected time window, plus any active events that started before the selected time window. (1041249)

- The list of flows shown in the Topology sidebar when viewing link details often shows flows through the link's endpoints, but not on the selected link. (1092315)

- The MS Teams event notification format did not provide hyperlinks to event in CloudVision. (1047556)

- Within the XCVR metrics, values of DOM metrics which were unavailable and should be shown as "N/A" were instead displayed as "Infinity". (1084499)

9. Limitations and Restrictions

Cluster Deployment and Management

Limitations and Restrictions

• In case you have custom firewall rules, please back them up before upgrade as the files under /etc/firewalld/ will be replaced with default configuration for CloudVision.

1. Backup (on all nodes)
   cp /etc/firewalld/zones/my-zone-file.xml /tmp/
2. Run upgrade
3. Restore (on all nodes)
   cp /tmp/my-zone-file.xml /etc/firewalld/zones/
   firewall-cmd --reload (811099)

Telemetry

Limitations and Restrictions

• XCVR DOM anomaly events may not be shown on the Topology page as part of the active events topology overlay, even when there are active events. (982430)

• The level of aggregation for a metric is automatically selected based on the length of the time range selected, irrespective of how far in the past the timeline is. If the timeline is set to view historical data which is far in the past, depending on the size of the time range selected the UI may show a level of aggregation where the data might not exist anymore. The workaround is to select a larger time window to force the display of a larger aggregation interval for which we retain a longer historical data range.
Examples of minimum data retention periods are: 10 second interval data retained for 5 days, 60 second interval data retained for 30 days, 15 minute interval data retained for 90 days. (350069)

10. Appendix

Relevant EOS Limitations and Software Caveats

- Within a config session, configuring VLANs that are currently in use as internal VLANs may fail. The error message will state that internal VLANs cannot be created even if a VLAN would no longer be used as an internal VLAN once the config session is applied. (132550) Introduced in 4.14.0. Fixed in 4.21.9,
  4.22.4,
  4.23.0

- Modifying an existing daemon through config session or config replace fails to restart the daemon.

  The workaround is to manually shutdown and no shutdown the daemon. (154022) Introduced in 4.14.0. Fixed in 4.18.5,
  4.19.2,
  4.20.1

- Starting a daemon that has run previously may cause the system to fail to start any new agents, daemons, and CLI sessions. (190407) Introduced in 4.18.1. Fixed in 4.18.4,
  4.19.1,
  4.20.1

- BGP peer-group configuration may not be correctly applied if configuration changes are made within a configure session or with a configure replace command. (212396) Introduced in 4.20.5.

- The ConfigAgent process will grow in memory size for every eAPI request. The only workaround is to periodically restart ConfigAgent. Doing so will terminate all CLI connections. (235573) Introduced in 4.20.1. Fixed in 4.20.2

- During Zero Touch Provisioning, the device might fail to download the config script from the file server. (242292) Introduced in 4.20.2. Fixed in 4.20.3

- When using one of the following CLI commands; "reload", "install source", or "boot system" for an EOS-2GB.swi on a system with 2Gb flash memory and an SSD and/or external clock, the command fails with an error message saying the software image is not compatible with the hardware.

  The workaround for that bug is to download the image to flash memory, edit the boot-config and use the "reload force" CLI command instead of "reload". (242578) Introduced in 4.19.6. Fixed in 4.20.4

- "mpls ldp password" will show the same encoded password every time "show running-config" is run from the CLI. (242633) Introduced in 4.15.4. Fixed in 4.20.6

- After running "rollback clean-config" in a config session, interface range commands include inactive interfaces. (243338) Introduced in 4.14.0. Fixed in 4.18.8,
  4.19.6,
  4.20.3

- The Launcher agent will restart repeatedly if a user daemon is configured with a string containing a "%" character. (247398) Introduced in 1.0.0. Fixed in 4.18.7,
  4.19.7,
  4.20.5

- When "channel-group" command is applied through eAPI on an Ethernet interface, its switchport configuration may override the switchport configuration of the port-channel that the Ethernet interface is configured in.

  Workaround is to add the required switchport configuration on all member interfaces of the port-channel. (412920) Introduced in 1.0.0. Fixed in 4.21.9,
  4.22.3,
  4.23.1

- Configuring a monitor session with many source interfaces may cause the CLI prompt to be become unresponsive. The command is expected to complete but just take longer. A separate CLI session can be used to enter other configuration commands. (520357)

Introduced in 4.21.3. Fixed in 4.25.2

- Configuring VLAN to VNI mapping within a config session may fail with a message that the VLAN conflicts with an internal VLAN, even if conflict is resolve when the config session is applied. (532496) Introduced in 1.0.0. Fixed in 4.22.9,
  4.23.7,
  4.24.4,
  4.25.2

- Using comments inside the route map mode may result in the config being rejected with an internal error.
  Remove the comments to work around this. (536882) Introduced in 4.25.1. Fixed in 4.25.3,
  4.26.1

- The Routing Control Function CLI may show as out of compliance when the RCF configuration is edited locally. (553342) Introduced in 4.24.2.

- When CloudVision verifies configlets, unsupported commands may not be rejected. (560938) Introduced in 4.20.1. Fixed in 4.22.11,
  4.23.8,
  4.24.6,
  4.25.4,
  4.26.1

- The 'logging level all' CLI expands to individual commands in the configuration, preventing dynamic updates of the logging list as part of EOS upgrades. (579047) Introduced in 1.0.0.

- Any change to inband telemetry profile in profile mode gets applied only when inband telemetry mode is exited. (606599) Introduced in 4.26.1.

- When inband telemetry is disabled, some flow information reported by CloudVision will be incorrect for a short time. (606609) Introduced in 4.26.1.

- "default switchport mode routed" and "no switchport" config commands may need to be manually reconciled in CloudVision after ZTP. (665217) Introduced in 4.26.2. Fixed in 4.26.8,
  4.27.6,
  4.28.2

- When using in-band management, Arista's best practice is to enable LACP fallback on the upstream LAG and/or MLAG links to prevent a temporary disruption when provisioning a downstream device. (676588) Introduced in 1.0.0. Fixed in 4.26.7,
  4.27.7,
  4.28.1

- When performing a config-replace over eAPI, RCF compilation errors may be treated as warnings. (688732) Introduced in 1.0.0. Fixed in 4.30.0

- If 'dot1x...' and 'mac security...' CLIs appear sequentially in the same CloudVision configlet the designed configuration will fail to validate. This automatically occurs if both CLIs are reconciled into the reconcile configlet.

  Separating the CLIs into different configlets will allow the designed configuration to validate. (798565) Introduced in 4.17.0.

- A device may hold stale dynamic MSS-G configuration after an OpenConfig restart. After OC restart, deletes to previous configs will have no effect, however, new updates to the config will be correctly set. Due to this, customer may experience unexpected data drop/forward or unexpected resource usage due to the stale config. (814432) Introduced in 4.27.1. Fixed in 4.31.1

- Changing certain MLAG configuration parameters (MLAG domain ID, local MLAG interface, MLAG peer address, MLAG peer interface) will cause the MLAG session to temporarily go down while the connection is renegotiated. This can lead to transient L2 loops in the network until the MLAG session is re-established. If EVPN is also being used, this can lead to rapid MAC flaps between devices in the network, causing those MACs to become blacklisted by EVPN. To see if a particular MAC has been added to the EVPN blacklist, use the "show bgp evpn host-flap" command.

  As a workaround, configuring EVPN host-flap recovery will allow the blacklisted MACs to age out after a configured time once the MLAG session has been re-established. Blacklisted MACs may also be cleared manually with the "clear bgp evpn host-flap" command. (891929) (1) Introduced in 4.20.5.

Relevant TerminAttr Limitations and Software Caveats

- Streaming Agent (TerminAttr) fails to stream the running config when there are 65533 or more lines that have changed since the last time the running config was streamed. Initialization is not affected, only subsequent running config changes. (375243) Introduced in TerminAttr-v0.1. Fixed in TerminAttr-v1.8.0
- Streaming Agent (TerminAttr) may restart unexpectedly when streaming a large collection under /Smash. (409785) Introduced in TerminAttr-v1.6.0. Fixed in TerminAttr-v1.7.0
- Token authentication may fail if one node in a multi-node CloudVision cluster is down when a retry on another node would succeed. (421336) Introduced in TerminAttr-v1.6.0. Fixed in TerminAttr-v1.7.2
- Streaming Agent (TerminAttr) low memory mode can cause increased load on the Sysdb process. (422612) Introduced in TerminAttr-v1.5.0. Fixed in TerminAttr-v1.7.3
- In low memory mode Streaming Agent (TerminAttr) does not stream to CloudVision. (423940) Introduced in TerminAttr-v1.7.1. Fixed in TerminAttr-v1.7.3
- Unable to identify devices from snooped DHCP packets with user-defined Circuit IDs. (426567) Introduced in TerminAttr-v1.6.0. Fixed in TerminAttr-v1.7.3
- Streaming Agent (TerminAttr) may restart unexpectedly if Flow Telemetry is enabled and encounters an sFlow packet with an empty AS Path. (443083) Introduced in TerminAttr-v1.6.0. Fixed in TerminAttr-v1.7.7
- On a dual-supervisor system, Streaming Agent (TerminAttr) may report incomplete information to CloudVision 2020.3.0 or later when verifying compliance. This may result in CloudVision reporting a system as being in compliance even when the standby supervisor is not configured with the expected boot settings. (512196) Introduced in TerminAttr-v0.1. Fixed

in TerminAttr-v1.10.4,
TerminAttr-v1.11.1,
TerminAttr-v1.12.0,
TerminAttr-v1.8.6,
TerminAttr-v1.9.8

- Streaming Agent (TerminAttr) may restart unexpectedly when "Advanced login options" is enabled in CloudVision. (533996) Introduced in TerminAttr-v0.1. Fixed in TerminAttr-v1.10.6,
TerminAttr-v1.12.2

- Streaming Agent (TerminAttr) may consume significant CPU resources on CloudVision when connecting with invalid credentials. (548733) Introduced in TerminAttr-v1.10.0. Fixed in TerminAttr-v1.10.7,
TerminAttr-v1.12.3,
TerminAttr-v1.13.2

- On EOS 4.25.2 or later the route type information is shown as unavailable for the routing table. (558429) Introduced in TerminAttr-v1.13.3. Fixed in TerminAttr-v1.14.1

- The reported compliance status maybe incorrect sometimes after a config push task with large number of config lines is executed.
Workaround is to restart Streaming Agent (TerminAttr) on the device. (600308) Introduced in 4.30.1.

- If Streaming Agent (TerminAttr) is enabled and streaming to CloudVision 2022.3.0 or above and 'management api gnmi' is configured, then the Streaming Agent's CPU and memory usage may increase.
Workaround this issue by adding "-cvconfig=false" to the Streaming Agent configuration or disabling 'management api gnmi'. (772493) Introduced in TerminAttr-v1.19.0. Fixed in TerminAttr-v1.19.5

- Pushing changes to the Streaming Agent (TerminAttr) configuration via CloudVision may cause the config update to fail. The workaround is to push the Streaming Agent configuration separate from other configuration changes. (795985) Introduced in 1.0.0.

- Streaming Agent (TerminAttr) is calculating the interface metric rates, including interface errors. When the device is having connectivity problems to CloudVision, the rate notifications may be coalesced during periods where the device is unable to connect which causes a loss of intermediate state. (807166) Introduced in 1.0.0.

- Streaming Agent (TerminAttr) does not stream the devices running configuration when running in low memory mode. (946459) Introduced in TerminAttr-v0.1.