HPE Aruba Networking EdgeConnect Operating System (ECOS) Release Notes

Version 9.4.3.9_99734

Revision A: December 18, 2025

This document provides important information about HPE Aruba Networking EdgeConnect Operating System (ECOS) 9.4.3.9, including top items for the release, release limitations, new features, issues fixed, upgrade considerations, and known issues.

Revision history

Date	Document Version	Revisions Made
December 18, 2025	Rev A	Initial document revision.

Top items for this release

Critical items

- Before upgrading to ECOS 9.4.3.9 (except if you are upgrading from 8.3.3.0+), you need to disable the “Verify Image Signature” option under SD-WAN Orchestrator’s Advanced Security Settings. You can enable this option again after the upgrade.
- After an appliance is upgraded to ECOS 9.4.3.9 and if image signature verification is enabled, the appliance can only be upgraded to newer releases that are signed using the HPE Aruba Networking certificate.
- 1GB Fiber SFP transceivers connected on EC-10106 wan0 and wan1 ports will not link up if the link partner (for example, Switch) has Auto-negotiation disabled. Auto-negotiation is enabled by default on wan0 and wan1 ports of the EC-10106. This issue does not impact 10G Fiber SFP+ Transceivers, DAC Cables, and 1G Copper Transceivers.
- There is a risk of tunnels being down due to the incompatibility described in the ECOS IPSec UDP ESN anti-replay compatibility matrix below. If all EdgeConnects are not being upgraded simultaneously to compatible releases, then before starting the upgrade, an admin should disable either the IPSec key rotation or anti-replay settings on all labels. These settings can be re-enabled after all EdgeConnects in the environment are upgraded. For important details, see Upgrade considerations.

ECOS Version	9.4.1.0+	9.3.2.0+	9.2.8.0+	9.1.10.0+	9.2.2.x–9.2.7.x	9.1.2.x–9.1.9x
9.4.1.0+	Yes	Yes	Yes	Yes	No	No
9.3.2.0+	Yes	Yes	Yes	Yes	No	No
9.2.8.0+	Yes	Yes	Yes	Yes	No	No
9.1.10.0+	Yes	Yes	Yes	Yes	No	No

Other items

- ECOS 9.4.3.9 requires SD-WAN Orchestrator version 9.4.3 or later. Before upgrading any appliances to this version of ECOS, you must upgrade SD-WAN Orchestrator to at least 9.4.3.
- ECOS 9.4.3.9 interoperates fully with most prior versions, though it may interoperate in Reduced Functionality mode with some older prior versions.

Before you begin

Carefully review the following items and any linked sections before starting the upgrade.

- Review all items under Release limitations, Known issues, and Upgrade considerations before starting the upgrade.
- If you have customized the system limits on an EC-V (Maintenance > Software & System Management > System Limits), or if the EC-V has 4 GB memory, it is recommended that you test the upgrade in a lab environment on an identical system before upgrading the production EC-V. If the upgrade fails (e.g., the EC-V is in a continuous reboot), lower some of the system limits or increase the memory on the EC-V, then test the upgrade again.

Note

If the EC-V currently has 4 GB of system memory, increase to 8 GB

Release limitations

This section lists feature limitations and other considerations for customers who are planning to use the ECOS and SD-WAN Orchestrator 9.4.x releases. As these limitations are addressed in subsequent builds of this release, this list will be updated in future revisions of the release notes.

Feature limitations

The following features have these specified limitations:

- When multiple senders and multiple receivers use the same multicast group over SD-WAN fabric, the multicast feature may experience delays or not function properly.
- EdgeConnect appliances do not support the implementation of different max advertise intervals for different routers in the same IPv4/IPv6 VRRP group. You must configure this interval to be the same on all routers in the same VRRP group, whether they are considered master or backup.
- For all ECOS versions, flow redirection applies to WAN Optimized (Boosted) TCP traffic only. Flow Redirection only applies to the TCP protocol; UDP traffic is not flow redirected.

  In ECOS 9.4.1.0 and later, the following limitations apply when you enable Flow Redirection:

  - When segmentation is enabled, Flow Redirection works for intra-segment traffic only. It does not work for inter-segment traffic.
  - Flow Redirection does not work for IPv6 traffic.
  - When a Zone-Based Firewall is enabled, Flow Redirection only works if the interface participating in Flow Redirection is in the Default zone.

Feature limitations when segmentation is enabled

The following features are not supported when segmentation is enabled:

- IPv6
- Network Address Translation (NAT), available in the 8.3 release, is not supported when segmentation is enabled. To apply NAT rules when segmentation is enabled, use Inter-Segment NAT.
- Bridge Mode and Server Mode. Inline Router Mode is the only mode supported.
- VRRP works as expected, but you cannot configure two groups with the same IP address. Overlapping subnets are supported, but the same IP address cannot be configured on two interfaces on the same appliance.
- When segmentation is enabled, flow redirection works for intra-segment traffic only. Flow redirection does not work for IPv6 traffic. VTI interfaces are not supported in clusters.

Features supported in the default or same segment

The following features work as expected when the feature is contained to the default segment or the same segment:

- Radius snooping features work only on the default segment.
- The IPSLA HTTP monitor is supported only in the default segment.
- Multicast is supported in the default segment.
- HTTP(S), Cloud Portal, SD-WAN Orchestrator are only supported in the default segment.
- LAN-side IPSec passthrough tunnels must use the default segment.
- AWS, Azure, and Check Point work in the default segment. You will need to create inter-segment policies to access these integrations from non-default segments.
- DHCP server is only supported in the default segment, but IP address pools cannot overlap. If IP address pools do not overlap, DHCP server should work in multiple segments at the same site.

Release limitations (continued)

Additional considerations

Note the following additional considerations regarding the v9 release:

- All appliances in your SD-WAN network must be running ECOS 9.0.x.x before the advanced segmentation feature can be enabled.
- Peer priority and admin distance settings will be applied globally across all segments.
- If you are using end-to-end Zone Based Firewall, it is recommended that you review the Zone Based Firewall document linked on the SD-WAN Orchestrator/ECOS v9 documentation resources page.
- Enabling segmentation is a one-way operation. When enabled, it requires deleting the entire Overlay network and policies. SD-WAN Orchestrator will recreate every tunnel and policy for the entire network.
- In ECOS 9.2.0.0, a behavioral change was introduced that affects how the generic app group name is derived. In prior releases, if the application was not part of any app group, the app group name would be “none” and the software did not attempt to derive the app group name using the generic app (https/http). Post-9.2.0.0, if the application is not part of any app group, the app group name is blank and the software attempts to derive the app group name using the generic app.
- When creating an HPE Aruba Networking Central Account in SD-WAN Orchestrator from the Aruba Central Site Mapping tab: Because of how Aruba Central processes account information, if you click Test or Save during configuration, you must wait 30 minutes before you click Test or Save again. If you click Test or Save a second time before 30 minutes have passed, you will receive an error that the connection failed even if you successfully connected to Aruba Central. To resolve this issue, wait 30 minutes before clicking Test or Save again. For more information, see Aruba Central Site Mapping on the HPE Aruba Networking EdgeConnect SD-WAN Documentation site.
- In versions prior to ECOS 9.4.3.1, for eBGP routes with no MED attribute, the BGP route metric was being set to the local preference value configured in the inbound route map, resulting in inconsistent values for routes coming from the same peer. In ECOS 9.4.3.1, a behavioral change was introduced so that when eBGP or iBGP metric values are not specified for a route received from the BGP peer, the metric is set as follows:
  - Med value, if present and greater than zero OR
  - Admin distance plus 50

Security issues fixed

The following table contains security-related issues fixed in ECOS 9.4.x.x releases, organized by the software version that first resolved them.

Issue ID	CVE	CVSS Score	CVSS Vector	Description	First Release to Resolve
ID: 79292	N/A	8.6	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H	Addresses a security vulnerability. Customers are urged to upgrade to this version. Details of this vulnerability will be published at a later time.	9.4.3.5
ID: 79259	N/A	8.6	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H	Addresses a security vulnerability. Customers are urged to upgrade to this version. Details of this vulnerability will be published at a later time.	9.4.3.5
ID: 75364	N/A	N/A	N/A	Enabling FIPS or CC mode on the appliance was not automated and required a "y/n" response from the user.	9.4.3.0
ID: 76032	N/A	N/A	N/A	Incorrect placement of the syslog configuration file caused the system to fail files integrity check during bootup.	9.4.2.5
ID: 73257	CVE-2022-36946	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	This release was patched to address CVE-2022-36946 (Linux kernel vulnerability).	9.4.2.0
ID: 73159	CVE-2022-1012 CVE-2021-4203 CVE-2021-20322	8.2	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H	This release was patched to address CVE-2022-1012 (memory leak vulnerability), CVE-2021-4203 (use-after-free read vulnerability), and CVE-2021-20322 (ICMP vulnerability).	9.4.2.0
ID: 72696	CVE-2023-48795	5.9	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N	This release was patched to address CVE-2023-48795 (OpenSSH vulnerability).	9.4.2.0
ID: 72695	CVE-2020-14145	5.9	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N	This release was patched to address CVE-2020-14145 (OpenSSH vulnerability).	9.4.2.0
ID: 72026	CVE-2023-51385	6.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N	This release was patched to address CVE-2023-51385 (OpenSSH).	9.4.2.0
ID: 71462	N/A	N/A	N/A	Default SSH and TLS ciphers in EdgeConnect were being flagged as insecure.	9.4.2.0
ID: 71389	TBA	7.2	CVSS:3.1 /AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H	A validation error created the potential for an unauthenticated user to execute arbitrary code on the host.	9.4.2.0
ID: 71380	TBA	7.2	CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H	An issue with port forwarding created the potential for an unauthenticated user to obtain a root shell on the appliance.	9.4.2.0

Issue ID	CVE	CVSS Score	CVSS Vector	Description	First Release to Resolve
ID: 71370	CVE-2023-48795	5.9	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N	This release was patched to address CVE-2023-48795 (OpenSSH Terrapin vulnerability).	9.4.2.0
ID: 71361	TBA	TBA	TBA	A code sanitization issue created the potential for an unauthenticated user to execute arbitrary code on the appliance.	9.4.2.0
ID: 69192	TBA	3.9	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N	This release was patched to address an HTTP verb tunneling (method override) vulnerability.	9.4.2.0
ID: 68872	CVE-2023-38802	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	This release was patched to address CVE-2023-38802 (error handing vulnerability).	9.4.2.0
ID: 73160	CVE-2021-37592	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	This release was patched to address a security vulnerability related to Suricata Intrusion Detection Engine version 4.1.5.	9.4.1.0
ID: 67177	N/A	N/A	N/A	A set of existing ciphers conflicted with a set of ciphers produced for a later release.	9.4.1.0

Issues fixed

The following known issues have been fixed in ECOS 9.4.3.9. Issues fixed in past releases can be found here.

Issue ID	Description
ID: 84430	Excessive stack usage during multicast route processing caused a stack overflow in the tunneld process, resulting in the appliances rebooting unexpectedly.

Upgrade considerations

The following list summarizes considerations that must be addressed when upgrading from any previous version of appliance software to ECOS 9.4.3.9.

Summary	Description
VLAN requirement when enabling EdgeHA through a switch	When upgrading your appliance from an older version to ECOS 9.1.0.0 and later, and if your EdgeHA link runs through a switch, you must configure at least one extra VLAN between EdgeHA components on your switch device.
Change in behavior of passthrough tunnel traffic handling in ECOS 9.3.0.0+	ECOS 9.3.0.0 changed how interface passthrough tunnel traffic is handled. Prior to 9.3.0.0, the direction of a LAN-to-LAN flow (a flow that originates and terminates on LAN-side interfaces) was set to W2L (WAN to LAN). In ECOS 9.3.0.0 and later releases, such a flow is treated as L2W (LAN to WAN). Therefore, the configured routes and the associated route tags must be adjusted for matching L2W traffic, as this is the direction of the flow. For LAN-to-LAN traffic to work, the flag for the intended configured routes must be set to “FROM LAN” or “ANY”.
Routes not shared if route-map is not selected	Prior to ECOS 9.3.0.x, for route redistribution in segments other than the default segment, if you did not select a route-map from the Redistribute Routes To/SD-WAN Fabric drop-down list, the software defaulted to mirroring what was applied in the default segment. Post-9.3.0.x, if a route-map is not selected, then no routes are shared. As a workaround, you can specify subnet sharing route-maps using Route templates. To do this, create a route redistribute map, and then update the Routes template with the map name.

Change in default settings for src-ip-based DNS cache	When source IP address-based DNS caching is enabled, the EdgeConnect appliances can experience performance issues during high volumes of DNS traffic. Typical symptoms include unexpected packet loss and bouncing BGP peer session establishment. This has been observed mostly on datacenter appliances where DNS traffic to and from remote branches is concentrated.
	
	Source-based DNS caching is disabled by default in ECOS 9.2.9.0+, ECOS 9.3.3.0+, and ECOS 9.4.2.0+. For older releases, the source IP address-based DNS caching mechanism can be administratively disabled using the following CLI command. Source IP-based DNS caching is an extension of the DNS caching feature that stores the source IP of the DNS client in the cache. This has limited use in some circumstances. This recommendation disables only the source IP-based DNS cache; the DNS caching feature continues to work even when source IP-based DNS caching is disabled.
	
	Note
	
	This command is available only in software releases ECOS 9.1.4.4+ and ECOS 9.2.3.0+. Older releases must first upgrade to a fixed version to mitigate this issue.
	
	`silverpeak > enable`
	
	`silverpeak # configure terminal`
	
	`silverpeak (config) # dns cache src-ip disable`
	
	`silverpeak (config) # exit`
	
	`silverpeak # write memory`
	
	`silverpeak #`

Upgrade all appliances to avoid tunnels dropping from IPSec anti-replay incompatibility	If all EdgeConnects in the environment are not being upgraded to a compatible release simultaneously, as per the compatibility matrix, then additional upgrade planning is required. Three workarounds are available when upgrading. Use whichever of the following options works best for your environment: 1. Disable key rotation before starting upgrades and re-enable after all appliances are upgraded.

Summary	Description
	Note Upon disabling key rotation, the SD-WAN Orchestrator generates and distributes the new key to all appliances one final time. Before you begin upgrades, make sure that the new key is distributed and activated. a. Before disabling the key rotation, navigate to **Support > Reporting > IPSec UDP Status** in Sd-WAN Orchestrator, and then verify that all appliances in the Active Key column have a status of *Yes*. b. Navigate to **Configuration > Overlays & Security > Security > IPSec Key Rotation**, and then clear the **Enable Key Rotation** check box. This triggers a new key generation, distribution, and activation. c. Repeat step a to verify that all appliances have the current and active key material. d. Proceed with appliance upgrades per your upgrade schedule. e. Navigate to **Configuration > Overlays & Security > Security > IPSec Key Rotation**, and then select the **Enable Key Rotation** check box. 2. Disable IPSec anti-replay on all network WAN labels, and then re-enable after all appliances in the network are upgraded. **Note** Disabling and enabling anti-replay causes the existing tunnel state to bounce once. Plan a maintenance window to make these changes. a. In SD-WAN Orchestrator, navigate to **Orchestrator > Orchestrator Server > Tools > Tunnel Settings**. b. Click **IPSec**. c. In the IPSec anti-replay window dropdown menu, select **Disable**. d. Click **Save**. 3. Upgrade all appliances in the network at the same time. To mitigate the risk of a tunnel being down due to the incompatibility described in the compatibility matrix, all appliances should be upgraded together to ECOS 9.1.10.0+, ECOS 9.2.8.0+, ECOS 9.3.2.0+, or ECOS 9.4.1.0+, as appropriate.
57K Dynamic Route Limit Within 60K Total Limit	IPv4 routes can hold up to 60k of total routes, including 57k of BGP/OSPF learned routes (dynamic routes). This threshold exists to keep a BGP/OSPF peer from tying up all available routing entries. The remaining 3k are local or learned routes. Alarms are thrown when IPv4 crosses the 57K boundary for dynamic routing.
C5 Instance Types Now Recommended	In previous releases, using M4 instance types was recommended for WAN bandwidth up to 500 Mbps. It is now recommended to use C5. If you are still using M4 instance types, it is strongly recommended to use c5.xlarge instead.
CIFS Functionality Removed	Starting with ECOS 9.3.0.0, support for the CIFS protocol as an optimization policy has been removed from all EdgeConnect and virtual EdgeConnect (EC-V) appliances. After upgrading to this release, CIFS connections will no longer be CIFS optimized, but CIFS traffic can still be L4 TCP-optimized with Boost.
Change in Enforce Return Tunnel Behavior	Starting with ECOS 9.0.4.0, return traffic is placed in the same tunnel from which forward traffic is received only when no better route is found. When a better route (either with lower metric or higher peer priority) is available, return traffic may be placed in a different tunnel.
Minor Alarm Upon Upgrading from Older ECOS Images	An alarm may trigger on SD-WAN Orchestrator version 9.1 or newer under the following conditions:

Summary	Description
	• A pair of appliances deployed in EdgeHA configuration are upgraded from ECOS version 9.0 or older to ECOS version 9.1 or newer, OR • A pair of appliances deployed in EdgeHA configuration running ECOS version 9.1 or newer are added and the number of EdgeHA subnets is less than 32. To clear this alarm, perform the following steps for each EdgeHA pair (or for each EdgeHA pair identified in the alarm, if the alarm contains this information): • If the number of EdgeHA subnets is less than 32, modify the EdgeHA configuration so that the number of subnets is 32 or more. • If the number of EdgeHA subnets is already 32 or more, open the Deployment page for each appliance, open HA link, click **OK**, do not make any changes, and then click **Save**.
New Configuration Requirement for IKE-based IPSec Tunnels	Under the presence of NAT devices, IKE_ID must be configured correctly for the tunnel to come up; there is no more wildcard lookup for pre-shared keys (PSK). Previously, for IKEv1 and IKEv2, PSK lookup was based on (ANY, remote IKE_ID). This caused unreliable PSK lookup when there were two different local IKE_IDs with different PSKs going to the same remote IKE_ID. Now, for IKEv1 and IKEv2, PSK lookup is based on (local IKE_ID, remote IKE_ID), which returns PSK reliably. **Note** When IKE_IDs are not configured (left blank), EdgeConnect assumes tunnel endpoint IP addresses as IKE_IDs (local IP as local IKE_ID, remote IP as remote IKE_ID). When upgrading to ECOS **Error! Unknown document property name.**: • In SD-WAN Orchestrator 9.1.3 or later, all Orchestrated third-party IPSec tunnels and SDWAN fabric IKE IPSec tunnels (with or without NAT devices in between) should come up as expected, as SD-WAN Orchestrator sets IKE_IDs explicitly. • All manually created third-party IPSec tunnels and SDWAN fabric IKE tunnels:

NAT status	IKE status	Tunnel status
With NAT devices in between	With IKE_IDs configured	Tunnel UP
With NAT devices in between	Without IKE_IDs configured	Tunnel DOWN
Without NAT devices in between	With IKE_IDs configured	Tunnel UP
Without NAT devices in between	Without IKE_IDs configured	Tunnel UP

Known issues

The following list contains known issues in ECOS 9.4.3.9.

Issue ID	Description
ID: 81082	When an untagged interface with dhcpd configurations is removed from a deployment, the dhcpd configurations of its tagged interfaces are also deleted.
ID: 80278	When the EC-10106 or EC-10108 appliance is connected to a switch on a 10G interface that goes down and comes back up on the switch side, the interface must admined down and up on the appliance side to regain the link.
ID: 77674	If you upgrade from 9.1.4.4 or 9.1.5.0+ to 9.2.0+, repeated error messages such as the following appear: **Line 205547: Oct 9 19:40:36 2023 XXXXXXXXXX tunneld[47666]: CPU 0 TID XXXXXXXXXX: [tunneld.ERR]: cnet_bond_update_master_state: Kernel reports mode 'balance-xor' for interface 'blan0' which doesn't match configured mode 'balance-rr'**. This presents no functional issues. To address the issue, make any change to the bonded interface config through the UI, which triggers binding updates to all existing interfaces.
ID: 72317	On an AWS instance with Elastic Network Adapter (ENA) enabled, ECOS does not support IPv6. On C5 and C6, ENA cannot be disabled, which means they cannot be used if IPv6 traffic is present. The only instance that allows ENA to be disabled is C4.
ID 71143	When roles-based security policies are set on the peer appliance and the destination zone is set to “Unknown,” TCP traffic does not work correctly. The branch does not recognize the destination zone. The deny policy is then evaluated on the destination appliance only for TCP traffic. As a result, the first packet is denied as per policy, but a new flow is created to permit subsequent packets.
ID: 70571	1GB fiber SFP transceivers connected on EC-10106 wan0 or wan1 ports will not link up if the link partner (for example, the switch) has auto-negotiation disabled. Auto-negotiation is enabled by default on the wan0 and wan1 ports of the EC-10106 appliance.
ID: 68602	A latency issue causes tunnels to drop unexpectedly. Debugging code was added to identify the root cause of this issue.
ID: 67561	NAT rules created from the CLI are not properly rendered in the web UI without a reboot. As a workaround, reboot the appliance to apply new NAT rules.
ID: 65980	When the hub appliance is set to “Do Not Re-Advertise Routes,” the spoke does not learn the hub’s locally connected IPv6 route.
ID: 61398	An interface with VRRP configured on it loses its IP address when it is moved from one routing segment to another. To avoid this, VRRP configuration needs to be removed before the segment change and re-added afterwards.
ID: 60120	IPv6 IPsec UDP tunnels are flapping at random intervals on AWS EC-V instances.
ID: 59585	The EC-XL-P, or any platform that uses Intel i40 NICs, does not turn off the optical signal when the interface is in the admin down state. Due to this, a device connected on the other side will see the link as up and continue to use it. It is recommended that customers using these ports perform an "admin down" on both sides of the link.
ID: 54195	When upgrading from 8.1.7.x, users must ensure that peer priority values are not zero. Peer priority values must be set to appropriate positive integer values before performing the upgrade.
ID: 23470	PPPoE is only supported in ILRM. PPPoE interfaces cannot be used for flow redirection.

Issue ID	Description
ID: 16799	Jumbo frames are not supported on Virtual Appliances installed on the XenServer hypervisor. Only one VLAN is supported on Virtual Appliances installed on the XenServer hypervisor. The XenServer hypervisor can be configured with one and only one VLAN; the hypervisor will strip the VLAN tag and send untagged packets to the Virtual Appliance.
ID: 16106	The EdgeConnect-US, EdgeConnect-XS, NX-700 and NX-1700 appliances do not support jumbo frames.
ID: 14168	Hot-swapping an SSD (or an SSD failure) may result in TCP connection resets or IP packet drops.
ID: 13155	If the https server and client negotiate an SSL compression method that is other than “NONE” (which can happen if a compression method is configured on the https server), the connection will not receive SSL-specific optimization (deduplication). If this occurs the error message reported in Current Flows will be “'unsupported SSL compression method'”. To work around this, configure the compression method on the https server as “NONE”.
ID: 12818	Using VMware Snapshots severely degrades the performance of Virtual Machines. Do not take snapshots of Silver Peak Virtual Appliances.
ID: 10929	On the VX, VRX, and EC-V Virtual Appliances, configuration of Ethernet MTU, speed and/or duplex settings requires host configuration in addition to Virtual Appliance configuration in the Appliance Manager.
ID: 9316	Application classification of http on non-standard ports relies on heuristics that are determined after flow creation. Therefore, the application classification is valid for reporting and monitoring but cannot be used for route, QoS, or optimization match lookups because these lookups occur simultaneously with flow creation. Such flows will be annotated “Heuristically Classified” in Monitoring > Current Flows.
ID: 6508	mgmt1 cannot be in the same subnet as mgmt0. Always use separate subnets for mgmt0 and mgmt1.
ID: 6370	Bonding interfaces may fail to negotiate correctly with a Cisco switch after an appliance reboot. To avoid this, enable auto-recovery on the Cisco switch to which the appliance is connected.
ID: 6333	If WCCP custom redirection is used with a 7-bit mask, add a route map entry that directs all WCCP control traffic (protocol UDP, port 2048) from Appliance IP addresses to pass-through unshaped.
ID: 6332	Auto-optimization is not effective in a network where there is a NAT implementation or a firewall that does TCP sequence offsetting. In such networks, connections will fail to optimize.
ID: 6330	While configuring tunnels, software checks are not present to disallow the VRRP virtual IP address from being the tunnel endpoint. Configuring the virtual IP address to be the tunnel endpoint can disrupt traffic when a VRRP master switch happens and is not recommended.

Additional information

This section contains additional information about ECOS software, as well as past features and fixes that are included in this release.

System requirements

Hardware compatibilities and dependencies

ECOS supports Unity EdgeConnect US, Unity EdgeConnect XS, Unity EdgeConnect S, Unity EdgeConnect M, Unity EdgeConnect L, Unity EdgeConnect XL, NX-700, NX-1700, NX-2500, NX-2600, NX-2610, NX- 2700, NX-3500, NX-3600, NX-3700, NX-5500, NX-5504, NX-5600, NX-5700, NX-6700, NX-7500, NX-7504, NX-7600, NX-7700, NX-8504, NX-8600, NX-8700, NX-9610, NX-9700, NX-10700, and NX-11700 Silver Peak Appliance hardware, and Unity EdgeConnect V, VX-500, VX-1000, VX-2000, VX-3000, VX-5000, VX- 6000, VX-7000, VX-8000 and VX-9000 Silver Peak Virtual Appliance software, and VRX-2, VRX-4, VRX-6, and VRX-8 Velocity Replication Acceleration software.

Software compatibilities and dependencies

- In the latest ECOS release, both HTTP and HTTPS connections to the Appliance Manager GUI are supported; HTTPS is the recommended method of connection. The default method supports both.
- The EdgeConnect appliance's Command Line Interface (CLI) can be accessed through a remote connection to the device's management interface using Secure Shell (ssh), or via the serial console port. For security reasons, telnet connections are not supported.
- The EdgeConnect software upgrade process supports transferring the software image from a server to the appliance via HTTP, HTTPS, FTP, and SCP (Secure Copy), via the SD-WAN Orchestrator (GMS), or transferring the image directly from a host running the Appliance Manager GUI.
- It is highly recommended that interconnected appliances run the same image version. It is also highly recommended that all appliances run the latest software version, 9.4.3.9. To ensure compatibility of your hardware platform(s) with ECOS 9.4.3.9, consult the ECOS and Orchestrator Release Compatibility matrix.
- For product and feature descriptions, detailed instructions on how to configure and monitor the EdgeConnect appliances, and detailed instructions on how to install or upgrade appliance software, refer to the EdgeConnect Appliance Manager (in SD-WAN Orchestrator, right-click an appliance from the left-side appliance tree, and then click **Appliance Manager**).
- HPE Aruba Networking does not recommend or support WCCP deployments with WCCP running on the Catalyst 6500 or 7600 running Hybrid CATOS.

New features and enhancements from past releases

The following table describes new features and enhancements that have been made in ECOS since the version 9 release.

Feature	Description	Baseline Release
PKI Phase II	With this release, end entity certificate support has expanded to include globally orchestrated appliance end entity profiles, which allow for automated enrollment of EdgeConnect certificates using an EST server. These profiles can be used to create certificate-based, orchestrated tunnels that are used by Business Intent Overlays.	9.4.3.0
Stateful SNAT Exceptions	To increase flexibility in how NAT traffic is handled, users can now easily configure a list of prefixes that will not be translated by the WAN-side interface firewall and will be exempted from the Stateful-SNAT process. Users can import a global list of public IP ranges into the EdgeConnect Orchestrator, and these ranges will be applied automatically to all EdgeConnects. In addition, further API enhancements have been made to support the stateful SNAT functionality added in ECOS 9.4.2.0.	9.4.3.0
SNMP Support	There is now SNMP support for standard Linux Server MIBs, such as CPU, memory, disk, and other metrics.	9.4.3.0
Availability Stats (KPI)	The Availability KPI feature helps distinguish and segregate underlay traffic by service provider, helps determine whether your service providers are meeting their contracted Service Level Agreements (SLAs), and provides insight into your SD-WAN traffic.	9.4.2.0
Support for New Appliance Model	This release adds support for the following part number: **Appliance model** — **Part number** EC-10106 — 3510325	9.4.2.0
OCSP Check During Validation	EdgeConnect now performs OCSP checking for each certificate in the chain during TLS handshakes, excluding the trust anchor.	9.4.1.0
QoS DRC	QoS DRC now controls traffic by limiting the flow rate of each traffic class sent from the appliance and reduces the total traffic in the network. This helps ease system congestions caused by the large amount of data sent from remote sites and prioritizes incoming traffic at the sender.	9.4.1.0
VXLAN and BGP EVPN Routing Support	You can now specify VXLAN settings for routing segments configured on EdgeConnect appliances. When a VNI is configured for a segment or in a template, EdgeConnect appliances automatically create an NVE as a VTEP, bind the NVE to the VXLAN segment, and specify the source interface for the VXLAN tunnel. With BGP EVPN Peer enabled, the selected loopback interface is automatically configured in the local interface field of the BGP EVPN.	9.4.1.0
Secure NTP	EdgeConnect now includes a secure NTP connection via pre-shared keys.	9.4.1.0
Enhanced Role Mapping	You can now define and map roles that are used throughout the EdgeConnect SD-WAN Fabric. For example, you can map a role to Group Policy Identifiers (GPIDs) from EdgeConnect appliances to facilitate identity awareness between Orchestrator and EdgeConnect appliances.	9.4.1.0
IPv4 Route Table Size	IPv4 subnet route table size has been increased to 60k total routes.	9.4.1.0
Doman Name Prioritization	Users can now configure a preferred domain when multiple domains are mapped to the same IP address. This results in predictable ACL matches for IP addresses even when the real domain name differs from the preferred domain name.	9.4.1.0

Feature	Description	Baseline Release
IDS/IPS on EC-10104	IDS/IPS functionality is now supported on the EC-10104 appliance (8 GB/4-core model).	9.3.0.0
VRRPv3	VRRP version 3 has been added to support IPv6, including the ability to set the advertisement timer in centi-seconds. There is now also the ability to include a free-form description of the VRRP instance.	9.3.0.0
LLDP	LLDP commands now exist in the CLI and API for enabling/disabling LLDP, showing neighbors and statistics, and configuration control, among other functions.	9.3.0.0
Improved BGP Functionality	Numerous improvements were made to BGP capabilities in Orchestrator, including the ability to use IPv6 addresses in BGP peer dialogs and to append multiple communities in the route-map rule for a BGP peer.	9.3.0.0
Availability and Availability Time Settings	You can now view Aruba SD-WAN infrastructure availability data measured as a percentage where uptime (total time minus downtime) is divided by total time. Orchestrator collects availability data based on the availability time setting for each appliance.	9.3.0.0
Internet Breakout Trends	You can now see trends for certain data about internet breakout links, such as latency, loss, and jitter.	9.3.0.0
Identity-Based Traffic Management	EdgeConnect now supports Aruba identity-based traffic management (IBTM). IBTM enables dynamically assigning SD-WAN traffic management policies based on identity match criteria such as Role Based Access Control (RBAC) username, user role, user group, user MAC address, device type, and identity context awareness from other sources.	9.3.0.0
LTE Over USB	EdgeConnect now supports Aruba USB LTE Modems (500731-001).	9.2.3.0
Branch NAT No-Translate Rules	The restriction of overlapping a translated source/destination subnet with a source/destination subnet has been removed.	9.2.3.0
Support for New Appliance Model	This release adds support for the following part number: **Appliance model** — **Part number** EC-10104 — 201857-001	9.2.3.0
Enable Logging for WAN-side Stateful Interface Drops	Users can configure Log Settings to include WAN-side stateful drops.	9.2.1.0
Proxy ARP Support	EdgeConnect now responds to any ARP received with the appliance's own local MAC address. In combination with Private/Community VLANs on the downstream switch, all traffic flows through the EdgeConnect, forming a Layer-2 hub and spoke topology within an Ethernet segment. Proxy ARP can be turned on and off per interface/label.	9.2.0.0
MAC Address Assignment for GCP Appliances	CloudInit now fetches MAC and subnet information from the metadata server and automatically assigns MAC addresses for GCP appliances.	9.2.0.0
Link Aggregation Control Protocol (LACP)	LACP provides a negotiation mechanism to control link aggregation. Link aggregation combines data from multiple interfaces into a channel group that provides a single high-speed link. Configuring link aggregation also adds failover redundancy to the interfaces in the group.	9.2.0.0

Feature	Description	Baseline Release
Multicast Group Filtering	Users can now allowlist multicast groups, so that EdgeOS processes only the groups matching the defined list.	9.2.0.0
Secure Logging	Orchestrator now allows you to configure the port number and protocol of remote log receivers and upload client certificates for remote log receivers.	9.2.0.0
OSPF and BGP Route Map Enhancements	Several enhancements to OSPF and BGP route maps now enable community filtering for OSPF routes, AS override in BGP neighbor configuration, and LE/GE prefix matching.	9.2.0.0
Large Scale Nexthop Adjacencies	The number of adjacencies (nexthops) supported over each interface has been increased from 16 to 127.	9.2.0.0
Increase in Scaling for OSPF and BGP Neighbor	This feature increases the scale of the number of OSPF neighbors supported on a single appliance, thereby increasing the maximum limit to at least 64 neighbors over two or more interfaces.	9.2.0.0
BiDirectional Forwarding Detection (BFD)	BFD is a networking protocol that detects faults between devices. In addition to supporting single- and multi-hop configurations and asynchronous mode, BFD can be configured for up to 20 segments with a maximum of 100 simultaneous sessions across all segments. The EdgeConnect appliance supports BFD for both BGP and OSPF.	9.2.0.0
AVC Attributes	There are now additional static attributes under the Address Map parameter that can be used as match criteria. These attributes are secondary parameters to the address map, and are evaluated for a policy match only when the configured address map parameter matches with the flow. This release includes support for MS Instance, MS Category, and Proxy attributes.	9.2.0.0
Firewall Protection Profiles	Users can now add firewall protection profiles in the Configuration menu. Protection profiles allow users to define firewall thresholds around specific threats and security objectives of an environment where the firewall will be used, map the profile to a segment or zone of the firewall, and quickly add/edit the profile as a template.	9.2.0.0
5K Tunnels for EC-XS	There is now support for up to 5,000 tunnels on EC-XS platforms with 16GB RAM and four cores.	9.2.0.0
IPSec Suite B	There is now a more robust set of secure algorithms for IPSec tunnel establishment and data exchange. **NOTE:** This feature is not fully supported in ECOS 9.2.0.0. Full support will be provided in a future version.	9.2.0.0
Intrusion Prevention System (IPS)	In addition to the existing Intrusion Detection System (IDS), which designates traffic for inspection using matching rules, IPS protects traffic by matching a signature and then performing a configured action (alert, block, or allow).	9.2.0.0
Radius Snooping	EdgeConnect now provides identity and context-aware micro segmentation based on user and device information collected during radius authentication. Users can write policies based on user-based match criteria for traffic steering, selecting firewall zones, and other policies.	9.2.0.0
Support for New Appliance Models	This release adds support for the following part numbers: **Appliance model** — **Part number** EC-XL-H-10G — 201915	9.2.0.0

<table>
<tr><th>Feature</th><th>Description</th><th>Baseline Release</th></tr>
<tr><td>Support for New Appliance Models</td><td>This release adds support for the following part numbers:
<table><tr><th>Appliance model</th><th>Part number</th></tr><tr><td>EC-L-H</td><td>201754</td></tr><tr><td>EC-XL-H</td><td>201756</td></tr><tr><td>EC-XS</td><td>201694</td></tr></table></td><td>9.1.1.0</td></tr>
<tr><td>Support for New Appliance Models</td><td>This release adds support for the following part numbers:
<table><tr><th>Appliance model</th><th>Part number</th></tr><tr><td>EC-M-H AC</td><td>201762</td></tr></table></td><td>9.1.0.0</td></tr>
<tr><td>Performance Enhancements</td><td>This release introduces a software-centric approach to enhancing performance for the EdgeConnect appliances, whether hardware-based, virtual, or cloud-hosted. These enhancements include improvements to total flows/sec capacity, as well as overall improvements to total throughput (packets-per-second), without requiring any upgrades to existing hardware. Performance optimizations in this release are based on new techniques to maximize parallel processing and are focused primarily on the higher-end appliances, where the most processing power is available.</td><td>9.1.0.0</td></tr>
<tr><td>Intrusion Detection System (IDS)</td><td>This release includes an Intrusion Detection System (IDS) that can monitor traffic for potential threats and malicious activity and generate threat events based on preconfigured rules. Packets are copied and inspected against signatures downloaded to Orchestrator from Cloud Portal. Traffic is designated for inspection using matching rules enabled in the zone-based firewall.</td><td>9.1.0.0</td></tr>
<tr><td>Support for ACL Group Objects</td><td>This release includes two new features related to ACLs: Address Groups and Service Groups. An address group is a logical collection of IP hosts or subnets, and a service group is a logical collection of protocols and ports. Both can be referenced in source or destination matching criteria in the zone-based firewall and security policies.</td><td>9.1.0.0</td></tr>
<tr><td>Zone Based Firewall Overrides for Control Traffic</td><td>Two new built-in policies, 65508 and 65509, will exempt Cloud Portal HTTPS and HTTP traffic to ensure that essential management services are not blocked by firewall misconfigurations.</td><td>9.1.0.0</td></tr>
<tr><td>Support for Non-routing Hub (Stub Hub)</td><td>This release adds support for designating a non-routing hub or stub hub by configuring it to not re-advertise spoke-learned routes to other hubs in the region.</td><td>9.1.0.0</td></tr>
<tr><td>Shaper Max Bandwidth for EdgeHA</td><td>This release includes an enhancement that will change the shaper max bandwidth setting when the primary circuit goes down.</td><td>9.1.0.0</td></tr>
<tr><td>Feature Licensing</td><td>In addition to traditional bandwidth and Boost licensing, this release adds support for specific feature licensing on a per appliance basis. Feature licensing allows administrators to enable specific features only on the appliances that require it.</td><td>9.1.0.0</td></tr>
<tr><td>Improved Failover between Primary and Backup Labels</td><td>This release adds support for enabling faster (more aggressive) failover between primary and backup labels. This change can be enabled or disabled via CLI using:
system aggressive-path-fail [enable | disable]
This setting is disabled by default.</td><td>9.0.5.0</td></tr>
</table>

Feature	Description	Baseline Release
Support for Link Aggregation	This release adds support for link aggregation, which allows users to combine two, three, or four interfaces into a channel group that provides a single high-speed link. Configuring link aggregation also adds failover redundancy to the interfaces in the group. You can configure link aggregation under Configuration > System & Networking > Link Aggregation.	9.0.3.0
Show BGP Routes via CLI	Routes received from and advertised to a BGP neighbor can be displayed via the CLI.	9.0.3.0
Import Management Routes to Routing Table	In this release, any non-default route added to the management table (e.g., 1.1.1.0/24-->10.1.1.1, lan0) with a datapath outgoing interface will be automatically added to routing table. This feature can be enabled and disabled and is enabled by default during an upgrade. Turning this feature on or off will add or delete any pre-configured management routes to the routing table.	9.0.3.0
NSSA Support in OSPF	This release allows the configuration of an OSPF area, and its type can be set to standard or NSSA (Not-So-Stubby Area).	9.0.3.0
DSCP Marking per Interface	This feature allows the user to configure DSCP marking on tunnel packets, normally determined by QoS policy, to be overridden on a per WAN interface basis.	9.0.3.0
Source Interface Configuration for DNS	When configuring DNS, users can now configure the source interface associated with each DNS server IP address. Source interface determines the routing segment in which the DNS server can be used and the IP address to use.	9.0.3.0
TCP Application Delay Stats for IPFIX	In this release, application delay is calculated for TCP connections and included in the NetFlow/IPFIX exports.	9.0.3.0
Advanced Segmentation Supported in OSPF	This release supports OSPF routing in multiple segments.	9.0.3.0
DHCP Support in Advanced Segmentation	This release adds support for advanced segmentation in DHCP relay. A single DHCP relay instance running on the appliance works with a remote, segmentation-aware DHCP server to serve all interfaces that may belong to different routing segments.	9.0.3.0
Custom CA Certificate Trust Store	Orchestrator's trust store can be customized by adding and deleting CA certificates under Configuration > System & Networking > Custom CA Certificate Trust Store.	9.0.3.0
Enable or Disable Portal WebSocket Connection	In the Appliance UI, under Administration > Silver Peak Cloud Portal & Orchestrator, administrators now have an option to enable or disable WebSockets as a redundant connection option.	9.0.2.0
Configure Encryption and Hash Algorithms	Using the ssh server encryption-algos and ssh server mac-algos CLI commands, administrators can select one or more provided algorithms for encryption and hashing. Selected algorithms can be reset with the no modifier.	9.0.2.0
Subnet Sharing Metric Enhancements	Subnet sharing metric values can be configured on a per-peer basis, allowing hubs in an MRSS (multi-region subnet sharing) region to redistribute a given route with different metrics.	9.0.2.0
ECMP Support for BGP	This release adds support for ECMP (Equal Cost Multi Path) routing to up to 20 BGP peers.	9.0.2.0
Dynamic Subnet Sharing Hold-down Timer	Subnet sharing automatically throttles updates to a given peer to limit update traffic.	9.0.2.0

Feature	Description	Baseline Release
Route Map Enhancements	This update enables the use of an OSPF tag as a matching criterion in route redistribution to subnet sharing.	9.0.2.0
Added Appliance CPU Stats	In this release, appliance CPU usage stats have been added to appliance historical stats.	9.0.2.0
Multicast Enhancements	This release adds stability to multicast when advanced segmentation is enabled.	9.0.2.0
New HTTP Ping Metrics	Loss and latency metrics for HTTP ping monitor are now supported.	9.0.2.0
Enhancements for Cleared and Acknowledged Alarms	The following details are now captured for alarms: Cleared By, Acked By, Acked Time, Comments	9.0.2.0
Secure WebSocket Connection to Orchestrator	To establish a secure connection to Orchestrator, appliances will now generate an auth token and encrypt it using the account key.	9.0.0.0
Advanced Segmentation (VRF)	This release includes support for Advanced Segmentation (VRF), enabling multiple routing tables on a single appliance. Segments do not share data routes – data packets are only forwarded between interfaces within the same segment. Because routing segments are independent, overlapping IP address spaces can be used by multiple segments. **NOTE:** It is recommended that you review the release notes for the Orchestrator version 9 release, as well as the Orchestrator/ECOS v9 documentation resources, available here.	9.0.0.0
Secure Shell Access	This release includes support for varying levels of security for shell access: open shell access, secure shell access, or disabled shell access. In the case of upgrades, the default mode of operation will continue to be open shell access. For new installations, the default mode of operation will be secure shell access. In this mode, shell access requires a challenge-response from Silver Peak technical support.	9.0.0.0
Certificate Verification with Orchestrator and Cloud Portal	Users can now enforce certificate verification with Orchestrator and Cloud Portal under Orchestrator's Advanced Security Settings. If this feature is enabled, the FQDN for Cloud Portal or Orchestrator must be used instead of global IPs.	9.0.0.0
Enhanced Multicast Support	This release provides additional support for multicast over the SD-WAN fabric.	9.0.0.0
Improved Software Upgrade Stability	This release increases the stability of appliance software upgrades by adding image signature and binary checksum verifications.	9.0.0.0
Security Enhancements	This release patches several low and medium severity security vulnerabilities identified in ECOS software.	9.0.0.0
Enhancements to Disabled Subnet Sharing via IP SLA	Disabling subnet sharing via IP SLA rules has been enhanced to ignore updates from appliance peers, allowing for greater control of traffic flow. Additionally, those routes will not be shared to BGP/OSPF peers.	9.0.0.0
Custom Tags in YAML Preconfig	YAML preconfig now supports the use of up to eight custom tags to be set on appliances.	9.0.0.0
IPSec Anti-Replay Improvements	IPSec anti-replay window protection has been enhanced to support a window size of up to 64K.	9.0.0.0

Feature	Description	Baseline Release
Multiple Domain Matches in DNS Cache	This release adds support for multiple domain matches in the DNS cache.	9.0.0.0
Port Flexibility for Bonding	This feature enables customers to bond only LAN side interfaces. Previously, when enabling bonding, both LAN and WAN side interfaces were bonded (blan0 and bwan0).	9.0.0.0

Issues fixed from past releases

The following table contains issues fixed in past releases that are also included in ECOS 9.4.3.9, organized by the software version that first resolved them.

Issue	First Release to Resolve
ID: 83437. When there were ECMP routes, the debug log was being printed multiple times, causing excessive route advertisement updates on the appliance.	9.4.3.8
ID: 83340. When a host was deleted from RTM, the memory allocated for the host was not freed, leading to a memory leak that caused the appliance to reboot unexpectedly.	9.4.3.8
ID: 83321. An issue with rekey functionality caused SA deletions, which led to third-party IPsec tunnels rebooting unexpectedly.	9.4.3.8
ID: 82751. When using the BGP CLI to modify the router-id parameter, the legacy OSPF router-id binding was being updated instead of the VRF-specific binding, preventing the OSPF router ID from updating successfully.	9.4.3.8
ID: 81580. A parsing error related to how dates were entered in generalized versus UTC time resulted in erroneous notification of SSL certificate expiration.	9.4.3.8
ID: 81357. BGP and OSPF session status alarms were not being generated when the session transitioned between UP and DOWN states within 15 seconds.	9.4.3.8
ID: 81111. A condition check was missing when code was merged, which led to a miscalculation of the DNS cache entries count and caused flows to be misclassified.	9.4.3.8
ID: 80878. The process manager terminated BFD erroneously because it incorrectly assessed that packet processing had stopped.	9.4.3.8
ID: 80725. When buffering, the shaper reclaimed/released buffers that created empty flows in shaper queues. Ensuing shaper checks processed those flows, resulting in empty tunnels that caused tunneld to reboot unexpectedly.	9.4.3.8
ID: 72966. Using ssh-rsa keys instead of ssh-ed25519 key pairs during setup could prevent successful login to EC-Vs.	9.4.3.8
ID: 83285. An issue with the workflow between the REST API and the mrtrd process prevented the Multicast tab of the Orchestrator UI from loading properly.	9.4.3.7
ID: 80417. After upgrade, PIM packets were being duplicated through tunnel traffic, causing tunneld to reboot unexpectedly.	9.4.3.7
ID: 79663. A memory leak issue in a hardware driver caused the EC-XS appliance to consume unnecessary memory, which consumed system resources and led to the appliance rebooting unexpectedly.	9.4.3.7
ID: 79302. An error in the loop logic of the garbage collection functionality resulted in the collector freeing up the last entry in the table twice, throwing an error, and consuming system resources until the service rebooted unexpectedly.	9.4.3.7
ID: 80576. When a LAN interface had a DHCP server or relay configured and more than one non-DHCP interface was deleted via the Deployment tab in the UI or the REST API, a memory leak occurred that caused the appliance to reboot unexpectedly.	9.4.3.6
ID: 80575. An issue with binding values being populated without masking resulted in the OSPF authentication key and MD5 password being unencrypted in the running configuration.	9.4.3.6

Issue	First Release to Resolve
ID: 79292. Addresses a security vulnerability. Customers are urged to upgrade to this version. Details of this vulnerability will be published at a later time.	9.4.3.5
ID: 79259. Addresses a security vulnerability. Customers are urged to upgrade to this version. Details of this vulnerability will be published at a later time.	9.4.3.5
ID: 79230. When a VRRP node transitioned from backup to master, the VIP VMAC neighbor entry persisted, preventing ping of management IP addresses on the appliance.	9.4.3.5
ID: 79061. By default, if BFD was enabled on an appliance with a static route configuration with a valid gateway IP address, then the session persisted even after disassociating with BGP.	9.4.3.5
ID: 78986. The USB LTE modem was sending its status information with the response for the IMSI number read query, corrupting the message and making parsing difficult.	9.4.3.5
ID: 78649. When an interface was deleted via the CLI using the no system router <router-name> command, the dhcpd bindings for that interface remained, causing the DHCP relay process to falter.	9.4.3.5
ID: 77518. A logic issue related to how ACL definition files were programmed prevented traffic from reaching the expected default BIOs.	9.4.3.5
ID: 77299. The nexthop queue was out of sync with the hash and source tables, preventing the multicast route from being properly programmed on the appliance.	9.4.3.5
ID: 76671. The hub appliance was intermittently dropping PIM messages from the branch appliance, temporarily pruning the branch from the multicast route and interrupting the multicast stream.	9.4.3.5
ID: 76301. The OSPF neighbor state was flapping from full to down when the hello timer was set to 1 second and dead timer was set to 4 seconds.	9.4.3.5
ID: 78982. REDIRECT flows were incorrectly dropping syn-ack packets, creating flow redirection errors.	9.4.3.4
ID: 78864. If packets were dropped before the NAT flow lookup flag was set, subsequent packets triggered a new NAT lookup, causing the NAT ID in the flow to be overwritten and potentially leading to a NAT flow leak.	9.4.3.4
ID: 77231. A computational error caused threshold crossing alerts (TCAs) on the number of flows to be triggered erroneously.	9.4.3.4
ID: 73530. Manipulation of an original string of address groups instead of a duplicate string caused a SIGABRT error, prompting tunneld to reboot unexpectedly.	9.4.3.4
ID: 78860. Because of a missing directory in the configuration files, the USB LTE modem does not acquire an IP address from the provider (although the modem is detected).	9.4.3.3
ID: 77676. The VRF module mishandled asymmetrical routes due to non-hairpin flow restrictions, resulting in a flow hash collision and dropped packets.	9.4.3.3
ID: 77502. The garbage collector in the DNS cache was running but was not removing entries, giving the false impression that the cache was full.	9.4.3.3
ID: 77490. Invalid peer node IDs caused a buffer leak in the RCMP message, preventing routes from redistributing to subnet sharing.	9.4.3.3

Issue	First Release to Resolve
ID: 77456. The appliance matched inbound port forwarding rules and performed NAT for the destination IP, rather than sending traffic directly to the destination, causing an interruption in the flow.	9.4.3.3
ID: 77204. Leaked SNAT entries were taking an assigned local IPSec UDP tunnel's port and were not properly mitigated, putting the local IPSec UDP tunnel in a down state.	9.4.3.3
ID: 77022. An error in the way EC-V memory size is calculated upon upgrade results in insufficient memory available, leading to continuous reboot of the appliance.	9.4.3.3
ID: 76941. A missing index check in the RADIUS-to-MAC address mapping function caused tunneld to reboot unexpectedly.	9.4.3.3
ID: 76837. An issue with rekey functionality led to multiple IKE underlay tunnels flapping unexpectedly.	9.4.3.3
ID: 77225. A packet handling issue erroneously assigned UDP packets to a "default" case, causing tunneld to reboot unexpectedly.	9.4.3.2
ID: 76981. An issue with how packets were handled in quiescent mode check caused the appliance to continue sharing default routes to LAN eBGP even after the WAN interface was disabled.	9.4.3.2
ID: 76774. Frequent calls of certain networkInterfaces API commands led to a memory leak, which triggered an increase in swap usage alerts on the appliance.	9.4.3.2
ID: 76770. The inbound shaper's performance was utilizing too much CPU, resulting in packets being dropped.	9.4.3.2
ID: 76708. An error in the configuration of retransmission count settings caused tunnels to fluctuate between up and down states periodically.	9.4.3.2
ID: 76502. A validation restriction in the Branch-NAT configuration settings that previously accepted "wan0" as a LAN interface name now only accepts "lan*" strings, preventing successful validation of the database upon upgrade.	9.4.3.2
ID: 76260. The USB LTE modem could not successfully restart because of an issue with how logic checks were run when Verizon was the registered service provider.	9.4.3.2
ID: 76029. MHR was bypassing register packet checks and incorrectly processing PIM register packets. This fix also resolved ID: 75751, where Multicast over SD-WAN fabric was not functioning properly when multiple senders and multiple receivers were present in the same multicast group.	9.4.3.2
ID: 76345. For eBGP routes with no MED attribute, the BGP route metric was being set to the local preference value configured in the inbound route map, resulting in inconsistent values for routes coming from the same peer.	9.4.3.1
ID: 76335. An issue with how the multiprotocol capability for BGP sessions processes EVPN parameters led to BGP peers throwing errors unexpectedly.	9.4.3.1
ID: 76297. External hairpin flows were not deleted properly, causing traffic disruption due to the maximum number of flows being exceeded.	9.4.3.1
ID: 76126. A change in how ICMP IDs were saved prevented translation in packets, causing the original ICMP ID traffic to return without finding the new flow.	9.4.3.1
ID: 76053. Packets were being freed before their flows were properly checked, resulting in those flows staying active and raising false alarms that the total number of flows on the appliance was approaching capacity.	9.4.3.1

Issue	First Release to Resolve
ID: 76039. DNS DPI check for security policy failed when a DNS proxy was configured.	9.4.3.1
ID: 76024. Multi-hop routes were not checking to see if better nexthops were available, causing an asymmetric routing scenario that had to be resolved by rebooting the appliance.	9.4.3.1
ID: 75986. Private ASNs were removed from the AS path in routes advertised to eBGP peers, preventing AS path propagation from working properly.	9.4.3.1
ID: 75933. VRRP configurations were missing after VLAN tags were modified on the EdgeHA deployment page.	9.4.3.1
ID: 75503. Due to a configuration change regarding broadcast entries in the ARP table, the LAN interface was sending out traffic with the broadcast MAC address.	9.4.3.1
ID: 74814. During firewall switchover with BFD enabled, BGP switched into an idle state, causing an unexpected delay in re-establishing BGP with the secondary firewall.	9.4.3.1
ID: 72265. Errors in flow counting led to a dissonance between the number of asymmetric flows reported in the Appliance Trend Flows tab and the Flows tab.	9.4.3.1
ID: 70496. Domain name compression resulted in IP phones being disconnected unexpectedly.	9.4.3.1
ID: 67953. On the EC-M-P appliance, the mrtrd process went into a pending state upon enabling multicast, rendering multicast nonfunctional.	9.4.3.1
ID: 76117. When the VLAN debug file failed to open, a coding loop error caused tunneld to reboot unexpectedly.	9.4.3.0
ID: 76063. Mishandling of packets that arrived for a redirected flow on the cluster appliance caused the appliance to reboot unexpectedly.	9.4.3.0
ID: 76057. OVF disk space was increased from 30GB to 60GB to provide EdgeConnect virtual appliances (EC-V) with enough space.	9.4.3.0
ID: 75446. A corrupted SSL record caused a decryption error during SSL acceleration.	9.4.3.0
ID: 75394. A logic error in the Firewall Protection Profiles feature prevented RSSP DPI from properly identifying valid FTP flows, resulting in some flows being blocked by security policy.	9.4.3.0
ID: 75364. Enabling FIPS or CC mode on the appliance was not automated and required a “y/n” response from the user.	9.4.3.0
ID: 75358. An issue with how parallel datapath CPUs handle message queues going to network memory created a datapath conflict that caused the appliance to reboot unexpectedly.	9.4.3.0
ID: 75321. On platforms where the core is shared between datapath and IDS/IPS, a tasklet that receives events from the IDS/IPS was creating extra UDS sockets, causing a decrease in datapath performance.	9.4.3.0
ID: 75285. A validation issue with string store data in the DNS revmap API caused tunneld to reboot unexpectedly.	9.4.3.0
ID: 75145. When a wl2 tunnel packet that matches a redirect flow is received, the appliance does not drop the packet and delete the flow as expected. As a result, Flow Redirection does not function properly in ECOS 9.4.x.x and 9.5.x.x releases.	9.4.3.0

Issue	First Release to Resolve
ID: 75019. A corrupted SSL handshake packet created an “invalid handshake” error that caused tunneld to reboot unexpectedly.	9.4.3.0
ID: 75009. Because of an issue with how node.js was handling the replace function, users were logged out of the appliance UI after opening the DHCP Leases tab in Orchestrator.	9.4.3.0
ID: 74819. FPOC was erroneously reusing old entries, resulting in packets being dropped as duplicates or late.	9.4.3.0
ID: 74796. The RX tunnel was not being assigned by interface, creating contradictory values between the RX action and ingress value.	9.4.3.0
ID: 74795. Virtual EdgeConnect running on KVM dropped packets on non-native VLAN interfaces due to improper handling of different MAC addresses assigned to different VLAN interfaces.	9.4.3.0
ID: 74625. A memory leak in ICMP error state processing of Firewall Protection Profiles caused tunneld to reboot unexpectedly.	9.4.3.0
ID: 74445. An issue with transit packets containing a link local destination IP address caused traffic to be sent between SD-WAN appliances in a loop.	9.4.3.0
ID: 74310. An issue with lookup logic prevented the USB-LTE modem from connecting to certain ISPs.	9.4.3.0
ID: 74167. The appliance code was unable to build a web socket using the first-resolved IP when the address was IPv6 rather than IPv4.	9.4.3.0
ID: 73768. Adding DPI for RSSP apps created an issue in the parsing logic of DNS queries, resulting in reading bytes beyond packet boundary and causing tunneld to reboot unexpectedly.	9.4.3.0
ID: 73752. An issue with converting non-ASCII characters prevented Orchestrator from rotating IPSec UDP key material, and prevented successful upgrade of the appliance.	9.4.3.0
ID: 73731. In scaled VLAN configurations, packets were being dropped between the appliance VLAN and the VLAN interface.	9.4.3.0
ID: 73697. When the EC-XS appliance was onboarded from factory settings and rebooted before activation, new seeds sent to the appliance were not properly stored on disk.	9.4.3.0
ID: 73639. On the EC-XL-P appliance, a malformed payload sent over UDP port 53 should have been rejected by the DNS deep packet parser, but instead caused tunneld to reboot unexpectedly.	9.4.3.0
ID: 73628. An issue in nat map, security map, and ACL policy evaluation caused increased latency on the LAN/WAN-side nexthops.	9.4.3.0
ID: 73626. Sanity check of the packet length parameter failed in certain scenarios, causing tunneld to reboot unexpectedly.	9.4.3.0
ID: 73556. When the mgmt0 and LAN interfaces were on the same subnet, BGP received routes from the peer were not being added to the Routing table.	9.4.3.0
ID: 73522. VRF information in packets was not set properly for traffic leaving and re-entering the LAN interface, causing packets to drop before creating hairpin flows and preventing routing from MPLS to SD-WAN.	9.4.3.0

Issue	First Release to Resolve
ID: 73466. A truncation issue in the internal timer module that occurred when the appliance's uptime exceeded approximately 994 days caused a major slowdown in packet processing.	9.4.3.0
ID: 73180. An error involving unsupported JavaScript syntax prevented interface counters from appearing in the appliance's web UI, even though they appeared in the CLI and the Orchestrator.	9.4.3.0
ID: 73097. An issue in the MGMT interface caused the mgmtd feature to sleep, triggering a restart in the ntpd service and un unexpected system reboot.	9.4.3.0
ID: 73030. An issue with DNS cache purging caused internet access to become unavailable when Proxy DNS was enabled.	9.4.3.0
ID: 73011. As the DHCP lease files grew, node.js consumed unexpectedly high CPU and memory, causing issues in the DHCP Leases table of the Orchestrator UI.	9.4.3.0
ID: 72886. The TFTP application was improperly classified in certain ECOS versions, causing a denial of the flow via security policy.	9.4.3.0
ID: 72882. Virtual EdgeConnect appliance deployed on KVM processed packets that were not destined for a local MAC address.	9.4.3.0
ID: 72800. The MGMT interface IP address was not filtered properly when performing an interface lookup, causing the IP to appear in the results erroneously.	9.4.3.0
ID: 72669. When the Stats Collector restarted after being stopped for an extended period, it checked all files from the stop date to the current date, causing performance and file issues.	9.4.3.0
ID: 70476. When multiple MACs were being authenticated to the same flow using RADIUS snooping, there was potential for mismatch of user information, leading to ACL mismatches.	9.4.3.0
ID: 76032. Incorrect placement of the syslog configuration file caused the system to fail files integrity check during bootup, resulting in the potential for a continuous reboot loop.	9.4.2.5
ID: 75917. WAN interfaces configured as stateful firewall or stateful+SNAT firewall were dropping IKE packets during IPSec IKE security association re-key events, causing IPSec IKE tunnels to drop and then re-establish.	9.4.2.4
ID: 75976. Mishandling of boundary conditions in the DNS parser and DNS cache management caused tunneld to reboot unexpectedly.	9.4.2.3
ID: 75502. The mechanism that manages the DNS cache based on domain confidence value contained a validation error that could not process the ":" and "/" characters correctly, causing tunneld to reboot unexpectedly.	9.4.2.2
ID: 72796. A configuration issue in the shaper algorithm caused traffic to queue unexpectedly slowly, resulting in high CPU usage and diminished performance.	9.4.2.1
ID: 73257. This release was patched to address CVE-2022-36946 (Linux kernel vulnerability).	9.4.2.0
ID: 73218. Peer logging was not disabled by default.	9.4.2.0
ID: 73159. This release was patched to address CVE-2022-1012 (memory leak vulnerability), CVE-2021-4203 (use-after-free read vulnerability), and CVE-2021-20322 (ICMP vulnerability).	9.4.2.0

Issue	First Release to Resolve
ID: 73156. Using ephemeral source port numbers caused packets from DHCP relay to the DHCP server to be dropped by a firewall.	9.4.2.0
ID: 73141. Routerd was leaking memory when a large number of subnet sharing/static routes were sent to RTM.	9.4.2.0
ID: 72994. An issue with the size of the port description for Type-Length-Value (TLV) prevented LLDP details from appearing on the appliance.	9.4.2.0
ID: 72969. An issue with the payload for SSDP multicast packets in VRF caused tunneld to reboot unexpectedly.	9.4.2.0
ID: 72932. A logging issue prevented BGP peer from coming up for the default segment over a VTI tunnel.	9.4.2.0
ID: 72930. Timestamp values were stored in an incorrect location, causing nexthop to use incorrect definitions and resulting in iBGP routes dropping unexpectedly.	9.4.2.0
ID: 72834. For certain platforms, the maximum interface limit was set to 127, preventing the addition of interfaces beyond that number.	9.4.2.0
ID: 72696. This release was patched to address CVE-2023-48795 (OpenSSH vulnerability).	9.4.2.0
ID: 72695. This release was patched to address CVE-2020-14145 (OpenSSH vulnerability).	9.4.2.0
ID: 72623. The transmit amplitude was set too high by default on ports and was over-driving the CPU NIC ports, creating link stability issues.	9.4.2.0
ID: 72608. Some ISPs were unable to connect to the appliance because they were unable to use hardcoded APNs.	9.4.2.0
ID: 72596. The SNMP OID in the MID.txt file was incorrect for certain hardware models.	9.4.2.0
ID: 72533. An issue with integer values in flow statistics resulted in flow count being reported as erroneously high.	9.4.2.0
ID: 72501. EdgeConnect-to-EdgeConnect BGP IPv6 sessions were not connecting because BGP socket support and wildcard sockets for IPv6 NBRs were not created.	9.4.2.0
ID: 72454. When duplicating packets, the IP header compression preamble was not accounted for when calculating worst-case packet size.	9.4.2.0
ID: 72431. EdgeConnect's BFD implementation erroneously detected faults when the BFD session did not transition into UP state and when the peer sent an "AdminDown" message.	9.4.2.0
ID: 72318. An error in the node callback chain resulted in the incorrect username appearing in audit logs for certain operations.	9.4.2.0
ID: 72255. Upon upgrade, mishandling of a template file prevented RADIUS snooping from loading properly.	9.4.2.0
ID: 72144. OSPF interface properties were being updated erroneously in tunneld's OSPF interface list during boot-up.	9.4.2.0
ID: 72026. This release was patched to address CVE-2023-51385 (OpenSSH).	9.4.2.0
ID: 72023. The ntpdate query was not properly completed on some NTP servers, resulting in false alarms in the Orchestrator UI.	9.4.2.0

Issue	First Release to Resolve
ID: 71908. A mishandling of race condition in the route table manager (RTM) caused the multicast routing daemon to restart unexpectedly.	9.4.2.0
ID: 71878. The MIB file was missing the EC-M-H appliance.	9.4.2.0
ID: 71506. There was insufficient tunbug in tunneld to gauge whether SSLPD queues were reaching their limit.	9.4.2.0
ID: 71495. An application classification issue caused inbound flows to be directed to a default security policy instead of another specified policy.	9.4.2.0
ID: 71484. Binding iperf3 to an IP in a non-default segment failed to assign an IP address.	9.4.2.0
ID: 71462. Default SSH and TLS ciphers in EdgeConnect were being flagged as insecure.	9.4.2.0
ID: 71458. When adding routes received from the subnet table to RTM in routerd, a miscalculation resulted in a segmentation fault, causing routerd to reboot unexpectedly.	9.4.2.0
ID: 71389. A validation error created the potential for an unauthenticated user to execute arbitrary code on the host.	9.4.2.0
ID: 71380. An issue with port forwarding created the potential for an unauthenticated user to obtain a root shell on the appliance.	9.4.2.0
ID: 71370. This release was patched to address CVE-2023-48795 (OpenSSH Terrapin vulnerability).	9.4.2.0
ID: 71361. A code sanitization issue created the potential for an unauthenticated user to execute arbitrary code on the appliance.	9.4.2.0
ID: 71354. A routing configuration issue prevented BGP peer routes using nexthop from being installed in RTM.	9.4.2.0
ID: 71351. A UI issue prevented the System Limits dialog box from closing as expected, blocking users from interacting with the UI.	9.4.2.0
ID: 71313. An authentication issue with the admin user created the potential for a monitor user to gain admin CLI access through a web UI shell.	9.4.2.0
ID: 71298. A buffer leak in the enqueue packet chain caused the appliance to reboot unexpectedly.	9.4.2.0
ID: 71223. If the number of long-lived flows was a sizeable fraction of the EdgeConnect packet buffer count, the EdgeConnect rebooted unexpectedly.	9.4.2.0
ID: 71083. An issue with the interface event handler caused the management layer of the appliance to become unresponsive when the USB LTE interface was put in admin down or unplugged.	9.4.2.0
ID: 70892. A data path issue caused the appliance to reboot unexpectedly.	9.4.2.0
ID: 70837. An issue with the location of PID files prevented the PPPoE interface of the appliance from getting an IP address upon reboot.	9.4.2.0
ID: 70830. Passive FTP was incorrectly identified in the Flows table.	9.4.2.0
ID: 70672. BGP was not redistributing routes to OSPF when the prefix was also advertised via the SD-WAN fabric.	9.4.2.0

Issue	First Release to Resolve
ID: 70649. An issue with the default set action code prevented route maps created from the CLI from appearing in the UI.	9.4.2.0
ID: 70647. Session-Affinity was overriding overlay policy and choosing the incorrect internet passthrough for flows with the same IP pair.	9.4.2.0
ID: 70641. Additional LAN interfaces for each EdgeHA WAN interface and HA Sync connection that did not contain user traffic flows were not being excluded by default in NetFlow exports for EdgeHA sites.	9.4.2.0
ID: 70570. Devices acting as the VRRP master were handling ARP incorrectly, causing nexthop to become unreachable.	9.4.2.0
ID: 70157. The link between the BGP route entries and nexthop entries became corrupted, causing an internal check to fail and tunneld to drop unexpectedly.	9.4.2.0
ID: 69623. When a primary interface was down, some underlay tunnels remained up through HA tunnels.. Bug.	9.4.2.0
ID: 69544. An issue with string storage capacity caused some traffic to map to the incorrect overlay.	9.4.2.0
ID: 69303. Alarms were being raised to the UI when any NTP servers were unreachable, instead of when all servers were unreachable.	9.4.2.0
ID: 69192. This release was patched to address an HTTP verb tunneling (method override) vulnerability.	9.4.2.0
ID: 68872. This release was patched to address CVE-2023-38802 (error handing vulnerability).	9.4.2.0
ID: 68798. An error in CPU affinity assignment caused a bottleneck and drops in IPSec encryption and decryption.	9.4.2.0
ID: 68611. When modifying the VLAN interface mask, the entire router (rtrx) was removed instead of the specific interface, resulting in IP tunnels rebooting unexpectedly.	9.4.2.0
ID: 66977. Moving a BGP peer with same local IP from one segment to another created an issue with BGP socket support and prevented BGP from initializing between appliances.	9.4.2.0
ID: 66644. The multicast engine was not recognizing or forwarding SSDP packets.	9.4.2.0
ID: 61853. An error in adding multihop routes to RTM prevented routes from being advertised.	9.4.2.0
ID: 73160. This release was patched to address a security vulnerability related to Suricata Intrusion Detection Engine version 4.1.5.	9.4.1.0
ID: 70918. A failure to defer logging messages caused the appliance to reboot unexpectedly.	9.4.1.0
ID: 70640. An issue with how nexthop is recognized produced some incorrect IP addresses in the nexthop table.	9.4.1.0
ID: 70580. An issue around RADIUS snooping packet handling caused the appliance to reboot unexpectedly.	9.4.1.0
ID: 70555. Cloudinit YAML configuration files were not read properly from the USB drive on bootup.	9.4.1.0
ID: 70497. In the deployment UI, the DHCP lease timer could only be configured in hours instead of seconds.	9.4.1.0

Issue	First Release to Resolve
ID: 70486. The “Subnet Error Code” column in the BGP Information table in EdgeConnect Appliance Manager was renamed to avoid confusion.	9.4.1.0
ID: 70120. The formatting of the AS path list in CLI output created a display error in log message and debug message output.	9.4.1.0
ID: 69896. The BGP local preference set via an inbound route map was not displayed in the “accepted routes” data from the CLI.	9.4.1.0
ID: 69866. A configuration issue caused domain-based policy lookup to take longer than expected, stalling the data path and generating lag for users.	9.4.1.0
ID: 69865. An error in deleting routes from the main table resulted in spurious default management routes.	9.4.1.0
ID: 69595. An error in processing multicast IP fragments caused the appliance to reboot unexpectedly.	9.4.1.0
ID: 69593. Firewall configuration changes made from the CLI did not always reflect in the Deployment UI due to how these changes were stored internally.	9.4.1.0
ID: 69531. A validation error in radius snooping caused the appliance to reboot unexpectedly.	9.4.1.0
ID: 69177. A race condition in the handling of a hairpin flow on multiple CPUs caused the appliance to reboot unexpectedly.	9.4.1.0
ID: 69163. An uninitialized handshake buffer used to process the SSLv2 handshake caused the appliance to reboot unexpectedly.	9.4.1.0
ID: 69160. Underlay tunnel flows from the EdgeHA peer were being classified as inbound and marked as DNAT, resulting in the flow ignoring policy and being routed back over the HA link.	9.4.1.0
ID: 69127. When duplicate routes were present, static routes were not being advertised to the BGP neighbor.	9.4.1.0
ID: 69088. A logic issue caused unexpected usage on LTE tunnels that were supposed to be idle.	9.4.1.0
ID: 68996. Conflicting multicast packets were not correctly dropped, causing the appliance to reboot unexpectedly.	9.4.1.0
ID: 68818. The branch and hub appliances did not properly prioritize existing routes when ECMP was enabled.	9.4.1.0
ID: 68693. Upon upgrade, an ESN synchronization issue caused tunnels to go down.	9.4.1.0
ID: 68654. When a peer priority was changed, the incorrect AS path was advertised to the LAN side of the appliance.	9.4.1.0
ID: 68641. ZTC and YAML file templates incorrectly placed the WAN interface onto a non-default segment.	9.4.1.0
ID: 68640. An issue in IPsec anti-replay handling caused keepalive packet drops, causing tunnels to go down unexpectedly.	9.4.1.0
ID: 68519. Management interface info was not being sent to routerd after routerd restart when OSPF and/or BGP was enabled.	9.4.1.0

Issue	First Release to Resolve
ID: 68130. The peer list did not strictly guarantee peer ID-to-peer index matches with appliances. This could cause traffic to be routed to an incorrect peer.	9.4.1.0
ID: 67232. Suricata logs were not able to be viewed via the CLI.	9.4.1.0
ID: 67177. A set of existing ciphers conflicted with a set of ciphers produced for a later release.	9.4.1.0
ID: 66533. An issue with the way DF flags were stored and propagated in IPv6 flow labels caused performance issues on the appliance.	9.4.1.0
ID: 66475. A stats collection issue caused the average out-of-order packets to erroneously appear at more than 100% capacity.	9.4.1.0
ID: 63472. When there were ECMP routes on the LAN side, IP spoof check dropped flows coming on LAN interfaces that have ECMP.	9.4.1.0
ID: 69598. Flows not resetting automatically after hardware failover.	9.3.1.0
ID: 68847. Boost stats were not reset after the configuration was changed, resulting in insufficient Boost.	9.3.1.0
ID: 68816. The appliance rebooted unexpectedly when the number of labels in internet policy exceeded 16.	9.3.1.0
ID: 68783. An issue with the maximum number of interfaces allowed on a single Nexthop caused tracked entries to point to nonexistent interface indexes.	9.3.1.0
ID: 68775. An issue with the tunbug configuration file created a potential command injection vulnerability in the command line interface.	9.3.1.0
ID: 68760. Alarms erroneously reported that the NTP server was unreachable.	9.3.1.0
ID: 68731. If an EdgeHA peer was unreachable, an issue with checking the socket status resulted in unnecessary CPU usage.	9.3.1.0
ID: 68596. An issue with ICMP stateful verification caused tunneld to reboot unexpectedly.	9.3.1.0
ID: 68543. A queuing issue caused the LAN Rx queue to become full, leading to performance issues across the appliance.	9.3.1.0
ID: 68464. An API issue caused a mismatch between the SNMP IfIndex on the appliance and SNMP browser inquiries.	9.3.1.0
ID: 68459. When BGP ECMP was enabled, both peers dropped unexpectedly, with only one recovering before reboot.	9.3.1.0
ID: 68356. While inferring internet link quality, the metrics from idle tunnels were ignored, causing gaps in Internet Breakout.	9.3.1.0
ID: 68236. A configuration check required creation of non-default zones to export zone-based firewall stats.	9.3.1.0
ID: 68215. On a segment without any configured route filtering map, the default subnet sharing map was not populated.	9.3.1.0

Issue	First Release to Resolve
ID: 68197. A validation error created the possibility for a malicious user to modify the prototype of a JavaScript object.	9.3.1.0
ID: 68195. A configuration change created an issue where the license limit value was no longer updated when the appliance license was updated.	9.3.1.0
ID: 68146. On the Internal Subnets dialog box, the “Consider Non-default routes as internal subnets” check box was not considered before taking an ACL action.	9.3.1.0
ID: 68043. Multiple sysdumps created at the same time created a drain on system memory, causing the appliance to reboot unexpectedly.	9.3.1.0
ID: 67768. A string in any custom IE exceeding 255 characters in length caused an encoding error.	9.3.1.0
ID: 67577. The EC-10104 appliance does not currently support bridge mode.	9.3.1.0
ID: 67355. Upon upgrade, the DNS proxy configuration was not accepted.	9.3.1.0
ID: 67215. If a security policy was added via Appliance Manager and previous Orchestrator rules existed, then the appliance repeatedly tried to apply the firewall zone policy.	9.3.1.0
ID: 66743. Peer priority hostnames had to be updated manually after changing appliance hostnames.	9.3.1.0
ID: 66445. After eBGP was disabled and the appliance rebooted, eBGP ECMP could not be started.	9.3.1.0
ID: 64787. Certain packets continually bounced between LAN ports of appliances in a VRRP pair.	9.3.1.0
ID: 58535. A DNS issue caused issues viewing the interface state for the appliance on a KVM hypervisor.	9.3.1.0
ID: 00542. When using a DNS proxy, the appliance does not modify the TC bit sent from the DNS server from 1 to 0.	9.3.1.0
ID: 00512. On the EC-10104 appliance, a port initialization issue caused the admin status to appear incorrectly in the web UI.	9.3.1.0
ID: 00498. The EC-10104 appliance does not currently support bridge mode.	9.3.1.0
ID: 72333. This release was patched to address CVE-2021-41617 (OpenSSH vulnerability).	9.3.0.0
ID: 67725. Traceroute through the appliance was incorrect because the ICMP "TTL Expired" message was generated with the IP address of a down interface.	9.3.0.0
ID: 67151. A validation error in upgrade image integrity verification could expose a security vulnerability.	9.3.0.0
ID: 66962. Some CLI commands accepted parameters that could have potentially led to an unauthorized user accessing sensitive operating system files.	9.3.0.0
ID: 66725. Addresses CVE-2021-41182, CVE-2021-41183, and CVE-2021-41184.	9.3.0.0
ID: 66592. A filename issue prevented the deletion of tcpdump files from the web UI.	9.3.0.0

Issue	First Release to Resolve
ID: 66351. An error in the loss calculation formula led to the Overlay/Underlay loss presenting as much higher in the web UI than it actually was.	9.3.0.0
ID: 66232. Under certain conditions, both the software and hardware watchdogs failed to reboot the appliance when the appliance entered a hung state.	9.3.0.0
ID: 63821. An issue with authentication tokens resulted in appliances with the same security policy configuration displaying different behavior.	9.3.0.0
ID: 63579. Due to missing bindings in certain scenarios, the appliance cannot synchronize with the Orchestrator upon upgrade from ECOS 8.1.x to ECOS 8.3.x or later.	9.3.0.0
ID: 63509. Some devices became unreachable after accessing management services (HTTP/S, Cloud Portal, Orchestrator).	9.3.0.0
ID: 63095. REST response was not handled correctly for empty redist maps pushed from templates.	9.3.0.0
ID: 63049. When a protection profile is enabled, traceroute via SD-WAN tunnel receives no response from the remote appliance.	9.3.0.0
ID: 62964. Fragmented multicast packets from the source may not be delivered correctly.	9.3.0.0
ID: 62880. The appliance was unable to ping from the CLI with segment routing enabled.	9.3.0.0
ID: 62864. Route status indicates Up when peer interface is Down.	9.3.0.0
ID: 62722. The denylist was not functioning as expected for SD-WAN flows.	9.3.0.0
ID: 62593. On the Interface Summary tab, inbound firewall log drops appear blank even if there have been drops.	9.3.0.0
ID: 60805. A JavaScript heap issue could lead to potential denial of service via an authenticated HTTP request.	9.3.0.0
ID: 60804. An authentication error in the REST API could lead to arbitrary file execution on the system.	9.3.0.0
ID: 68655. BGP-learned routes were not being redistributed into OSPF and SD-WAN fabric.	9.2.6.0
ID: 68598. After ECMP is enabled for LAN-side BGP, the connection to the web UI rebooted intermittently.	9.2.6.0
ID: 67845. The Cluster Peer Down alarm was being raised too often, resulting in asymmetric flow redirection.	9.2.4.0
ID: 67473. A configuration issue stored incorrect Admin distance values in a helper data structure, resulting in BGP route loop prevention not functioning as expected.	9.2.4.0
ID: 67397. A misconfiguration in the cifs_proxy_monitor's select timer resulted in the proxy service rebooting unexpectedly.	9.2.4.0
ID: 67361. When segmentation was enabled, an IPv6 configuration error led to tunnel traffic erroneously appearing in application reports for EdgeHA appliances.	9.2.4.0
ID: 67296. When trying to establish BGP peering from a newly created VRF segment, the Peer State value appeared empty in the web UI.	9.2.4.0

Issue	First Release to Resolve
ID: 67027. On the EC-10104 appliance, a routing error erroneously classified standard ports such as lan0 and wan0 as VLAN sub-interfaces, resulting in a configuration error that caused routerd to reboot unexpectedly.	9.2.4.0
ID: 66760. A command issue created a potential vulnerability where admin users could execute arbitrary code as the root user.	9.2.4.0
ID: 66644. The multicast engine was not recognizing or forwarding SSDP packets.	9.2.4.0
ID: 66641. The BGP peer was not establishing to the ISP neighbor on wan0.	9.2.4.0
ID: 66590. If no subnets were specified in VRF, then the "force-internal" flag was not set, causing a classification issue where traffic was improperly identified as internal.	9.2.4.0
ID: 66545. Subnet API documentation contained some missing fields, resulting in dropped API calls.	9.2.4.0
ID: 66433. A stale flow entry in the hash table caused IPsec tunnels to drop unexpectedly.	9.2.4.0
ID: 66398. A duplicate or overlay ID was causing a bonded tunnel to enter a misconfigured state.	9.2.4.0
ID: 66252. The jsond process stopped unexpectedly, causing the web UI to reboot.	9.2.4.0
ID: 66144. A configuration vulnerability allowed the potential upload of malicious files through the web UI.	9.2.4.0
ID: 66024. If the appliance rebooted during the period between when active and passive seed-ids were pushed, the active seed-id was lost and tunnels dropped unexpectedly.	9.2.4.0
ID: 65904. A validation issue created a potential command injection vulnerability in the command line interface.	9.2.4.0
ID: 65888. ECOS interface changes caused the NTPD service to restart, in turn causing NTP to reboot unexpectedly.	9.2.4.0
ID: 65842. A validation issue prevented IPv6 addresses from being used in passthrough tunnel configuration.	9.2.4.0
ID: 63884. An invalid tunnel flow entry caused packets to be dropped.	9.2.4.0
ID: 63835. Default SSH options on the appliance were erroneously presenting as security issues during vulnerability scans.	9.2.4.0
ID: 62644. A file authentication issue created a potential vulnerability where admin users had read access to sensitive files.	9.2.4.0
ID: 62643. A command issue created a potential vulnerability where admin users had read access to sensitive files.	9.2.4.0
ID: 62609. A command issue created a potential vulnerability where admin users could execute shell commands as the root user.	9.2.4.0
ID: 59961. A network monitoring vulnerability allowed the potential execution of arbitrary shell scripts.	9.2.4.0
ID: 00447. Addresses CVE-2022-4304, CVE-2022-4450, CVE-2023-0215, and CVE-2023-0286.	9.2.4.0
ID: 66614. An authorization issue caused the EC-XS appliance to reboot unexpectedly.	9.2.3.0

Issue	First Release to Resolve
ID: 66520. Errors in memory deletion and ruleset functionality caused incorrect IPS action to be performed.	9.2.3.0
ID: 65648. A change in the Linux kernel version used in ECOS 8.3 prevented LACP packets from being bridged properly, causing the neighboring switch to declare some interfaces as down.	9.2.3.0
ID: 57761. A packet handling issue in tunneld caused checksum verification errors.	9.2.3.0
ID: 66174. A configuration database validation issue prevented successful upgrade of the appliance.	9.2.2.0
ID: 65828. A pre-configuration issue caused an unexpected loss of connectivity between the appliance and the Orchestrator.	9.2.2.0
ID: 65736. A subnet sharing issue caused OSPF routes to drop unexpectedly if there were no routes in the default segment.	9.2.2.0
ID: 64342. An internal flow timer issue led to SYN packets being dropped unexpectedly.	9.2.2.0
ID: 63809. LAN RX and LAN TX bytes were present in some Netflow reports even when they were not configured to be.	9.2.2.0
ID: 63774. TCP traffic was moving slowly between the remote server on AWS and the on-premise appliance.	9.2.2.0
ID: 63651. An issue with how packet loss is calculated led to “Inbound WAN lost” and “Inbound WAN jitter counter” values that seemed excessive.	9.2.2.0
ID: 63598. ACL matching failed when an address group containing 1.1.1.1/32 was used.	9.2.2.0
ID: 63575. Packets were being dropped in FPOC for reaching the maximum buffer limit.	9.2.2.0
ID: 63574. The Overlay-Interface-Transport report was not generating when the Transport option was selected.	9.2.2.0
ID: 63289. Upon upgrade to newer versions, OSPF routes were experiencing unexpected interruptions due to the way the appliance was improperly deleting and then adding routes (instead of upgrading them).	9.2.2.0
ID: 63253. Changed passwords in BGP peer connections were not taking effect until the connections were restarted.	9.2.2.0
ID: 63243. After a spoke appliance was upgraded to 8.3.6.1, it routed traffic to unexpected hub peers. Rebooting it resolved the issue.	9.2.2.0
ID: 63114. TCA alerts remained active after tunnels were deleted.	9.2.2.0
ID: 63071. Accessing the precursor table from multiple datapath threads concurrently resulted in IP SLA tunnels going down unexpectedly.	9.2.2.0
ID: 63062. A configuration issue caused the appliance to not recognize SaaS Optimization settings if certain RTTs were set.	9.2.2.0
ID: 62883. After the appliance was upgraded to an ECOS 8.3.6.x version, fiber interfaces on some hardware models failed to come up.	9.2.2.0
ID: 62759. An assertion failure while processing a multicast packet caused the appliance to restart unexpectedly.	9.2.2.0

Issue	First Release to Resolve
ID: 62658. IKE IPsec tunnel traffic loss was observed during the rekey process.	9.2.2.0
ID: 62654. An issue in the IPsec anti-replay setting while changing a tunnel configuration caused the appliance to reboot unexpectedly.	9.2.2.0
ID: 62884. Flow-redirected flows were not deleted fast enough, causing the number of redirection entries to grow too large and eventually resulting in flow redirection failure.	9.2.1.0
ID: 62783. Adding 0.0.0.0/0 to the list of internal subnets did not account for non-default segments.	9.2.1.0
ID: 62486. The main packet handling process became unresponsive and caused the appliance to reboot unexpectedly.	9.2.1.0
ID: 62481. When a label was used for an action interface, VRRP priority was not decreased for all VRRP instances.	9.2.1.0
ID: 62472. A control message buffer depletion prevented routes from being distributed properly in subnet sharing.	9.2.1.0
ID: 62323. Upon upgrade, a UI issue prevented real-time stats from rendering correctly in the Orchestrator Live View.	9.2.1.0
ID: 62304. After upgrading the appliance, pings were not being successfully relayed between HA interfaces.	9.2.1.0
ID: 60916. In some cases, the appliance was unexpectedly reverting to previous bandwidth license limits.	9.2.1.0
ID: 62480. An error in sequence number handling caused the packet daemon to become unresponsive, resulting in an unexpected appliance reboot.	9.2.0.0
ID: 61905. A race condition during Orchestrator update was causing conflicts in API calls, resulting in SaaS optimization running for sites that did not have it enabled.	9.2.0.0
ID: 61876. A UI issue was incorrectly validating invalid distance values in Orchestrator.	9.2.0.0
ID: 61612. A logic issue in the processing of static routes erroneously created multiple route entries but did not mark them as duplicates, causing a conflict and unexpected reboot of the appliance.	9.2.0.0
ID: 61142. Some sub-interfaces were using the same interface name, creating issues in public IP discovery.	9.2.0.0
ID: 60920. AWS URLs were not successfully being added on the Application Definition page.	9.2.0.0
ID: 60894. A validation issue was allowing invalid admin distance values for OSPF routes.	9.2.0.0
ID: 60702. Zscaler GRE tunnels were unexpectedly going offline.	9.2.0.0
ID: 60192. Yocto mii-tool output was displaying advertising and link partner fields backwards.	9.2.0.0
ID: 60125. Some appliances were unexpectedly switching to System Bypass mode and then recovering within a short time.	9.2.0.0
ID: 59496. On the flow details page, Configured Tx Action was not being updated in all conditions, and the Subnet field was not being displayed when there was no route available.	9.2.0.0

Issue	First Release to Resolve
ID: 59166. iperf3 running in UDP mode on LAN was being capped by the WAN inbound shaper.	9.2.0.0
ID: 58892. If IP fragments were received with DF bit set, they would be dropped by the far-end appliance across the SD-WAN fabric.	9.2.0.0
ID: 69293. In a rare case, interface measurements were incorrectly discarded, resulting in a suboptimal interface being chosen for internet breakout traffic.	9.1.9.0
ID: 69047. The appliance web server was restarted repeatedly after upgrading from 8.1.9.18 to 9.1.6.2, causing unstable connectivity to the Orchestrator.	9.1.8.0
ID: 68679. After the appliance was upgraded to 9.1.6.2_92636, the appliance restarted unexpectedly.	9.1.8.0
ID: 68465. HTTP-based IPSLA probes were not sent to the intended Zscaler tunnel on the appliances where segmentation was disabled and an overlay was configured to match traffic to the Zscaler VPN service.	9.1.8.0
ID: 68369. An issue with NAT allocation caused local internet breakout to improperly route NAT traffic.	9.1.8.0
ID: 68364. Flows from wireless access points were disconnected after a tunnel flap, requiring the customer to reset the flows.	9.1.8.0
ID: 68343. This release was patched to address CVE-2023-2650 (OpenSSL vulnerability).	9.1.8.0
ID: 68226. After appliances were upgraded to 9.1.4.2_92345 from 8.3.6.1_86378, idle tunnels on hub appliances began sending more data to spoke appliances.	9.1.8.0
ID: 68019. An anti-replay window de-synchronization issue in IPsec UDP tunnels caused underlay fabric tunnels to drop unexpectedly.	9.1.7.0
ID: 67995. Under certain conditions, the peer index tracking a particular peer ID was reused with a different peer ID, resulting in the new peer erroneously showing it owned a different bonded tunnel.	9.1.7.0
ID: 67484. The Inbound WAN lost count on some appliances was incorrect.	9.1.7.0
ID: 67422. An error during the packet sane check process created a packet double-free in the FPOC/REO engine, causing tunneld to reboot unexpectedly.	9.1.7.0
ID: 67997. A DNS cache issue caused some appliances to lose connectivity to Orchestrator.	9.1.6.1
ID: 67175. An invalid redirect flow caused tunneld to reboot unexpectedly.	9.1.5.0
ID: 65931. A static route with unreachable NextHop was still advertised by the appliance.	9.1.5.0
ID: 66312. A socket leak in the RADIUS module caused a connectivity error when logging in to the appliance from the web UI.	9.1.5.0
ID: 66251. When an IPSEC DPD timeout originated from transient WAN packet loss, third-party IPSEC tunnels would erroneously stay up on the appliance, requiring manual recovery of the tunnel.	9.1.5.0
ID: 66678. A validation error caused the HASync peer to go down, forcing tunneld to reboot unexpectedly.	9.1.4.4

Issue	First Release to Resolve
ID: 66294. A data corruption error led to the appliance rebooting unexpectedly when receiving a flow redirection bulk delete request.	9.1.4.4
ID: 65945. During IPsec rekey, active SAs were being deleted erroneously, causing packet drops.	9.1.4.4
ID: 62479. The EC-XL-H appliance rebooted unexpectedly while testing flow redirection.	9.1.4.4
ID: 66824. An issue with a high rate of concurrent flows caused the current number of flows to be incorrect.	9.1.4.3
ID: 66744. The EC-10104 appliance had no IP configured by default for lan0.	9.1.4.3
ID: 66634. A proxy manager deadlock condition in the appliance caused the appliance to restart.	9.1.4.3
ID: 66613. When the flow redirection feature was enabled, the counter for internal packet drops with the “LAN Rx q full” drop code continued incrementing.	9.1.4.3
ID: 66478. If there are multiple hosts on the WAN-side of the router, the appliance may have issues accessing some external URLs.	9.1.4.3
ID: 66458. A memory issue created a tunneld error and caused the appliance to reboot unexpectedly. This issue was given a temporary fix in a previous release. This update provides a permanent fix.	9.1.4.3
ID: 66451. A configuration issue incorrectly allowed read/write permissions on SNMPv3.	9.1.4.3
ID: 66444. A counting issue caused packet order correction buffer limit to max out, causing unexpected packet drops.	9.1.4.3
ID: 66416. An issue with the curl library in OpenSSL caused the system daemon to restart unexpectedly.	9.1.4.3
ID: 66378. An issue with flow deletion caused the appliance to reboot unexpectedly. The root cause is still unknown. In this release, additional debugging code was added to capture additional information when this issue happened.	9.1.4.3
ID: 66143. A race condition stemming from a flow issue in the inbound shaper caused the appliance to reboot unexpectedly.	9.1.4.3
ID: 66333. The Link Integrity test was not properly executing after upgrade.	9.1.4.2
ID: 63692. An issue with CIFS acceleration disrupted tunneld function, causing the appliance to reboot unexpectedly.	9.1.4.2
ID: 62110. During EC-V deployment, Cloud-init failed to configure Account Name if it contained a comma.	9.1.2.0
ID: 62081. After a subnet configuration change, mgmt0 interface became unstable.	9.1.2.0
ID: 61789. An internal error in TCP flow management caused the appliance to reboot unexpectedly.	9.1.2.0
ID: 61781. Scans running against EdgeConnect were causing appliances to be intermittently grayed out in Orchestrator.	9.1.2.0
ID: 61778. The appliance was incorrectly reporting model information on SNMP discovery.	9.1.2.0

Issue	First Release to Resolve
ID: 61695. A routing issue involving multiple ECMP paths was causing unexpected interruptions to multicast traffic.	9.1.2.0
ID: 61264. The appliance was patched to address CVE-2022-0778 (OpenSSL advisory).	9.1.2.0
ID: 61254. The appliance was unable to configure an IPV6 address due to an error in subnet validation.	9.1.2.0
ID: 60968. Upon upgrade, a provisioning issue prevented Azure waagent from starting as expected.	9.1.2.0
ID: 60955. The appliance was not able to renew the license from the Cloud Portal.	9.1.2.0
ID: 60935. Excessive OSPF logging was causing performance issues on the appliance.	9.1.2.0
ID: 60891. DHCP relay was sometimes not working due to mishandling of interface labels.	9.1.2.0
ID: 60875. When the user clicked the Soft Reset button, a BGP route refresh message was not sent to the BGP peer as expected.	9.1.2.0
ID: 60694. The DHCP client was incorrectly handling the timeout state.	9.1.2.0
ID: 60156. The appliance failed to route some user traffic terminating on a VRRP interface with segmentation enabled due to a default route that was not properly installed.	9.1.2.0
ID: 59552. Tunnels were incorrectly reporting latency measurements when the tunnels were in an idle state.	9.1.2.0
ID: 59162. An issue in how tunnel bandwidth usage was calculated prevented HT link bonding policy from working as expected.	9.1.2.0
ID: 59068. Appliance CLI access was not working from Orchestrator.	9.1.2.0
ID: 62544. A configuration change for the tunnel retry timer caused underlay tunnels to go down unexpectedly.	9.1.1.3
ID: 62289. An error in hair-pinned packet processing caused the appliance to reboot unexpectedly.	9.1.1.3
ID: 62201. When a port-based application definition includes TCP/UDP port 65535, it causes an internal variable overflow that results in perpetual reboot of the appliance.	9.1.1.3
ID: 61728. When an “OR” operator was used in a firewall rule’s matching criteria, the rule was not matched and, as a result, packets were incorrectly denied.	9.1.1.3
ID: 61240. Certain flow state variables caused an issue where flow reclassification was not triggered as expected.	9.1.1.3
ID: 60927. The appliance was throwing the error “appliance could not get license lease” even though it could reach the Cloud Portal.	9.1.1.3
ID: 66092. An issue with the DNS snooping cache caused high CPU utilization, causing user traffic slowdown.	9.1.1.2
ID: 61193. When an ACL rule contained more than one group name, it incorrectly matched some flows, resulting in the flows being dropped.	9.1.1.2
ID: 60892. DHCP relay was sometimes not working due to mishandling of PPP interfaces.	9.1.1.2

Issue	First Release to Resolve
ID: 60786. LAN to LAN traffic did not work without configuring a static route on the outgoing LAN interface.	9.1.1.2
ID: 60745. After upgrading ECOS, some packets related to Microsoft Office were being dropped internally.	9.1.1.2
ID: 61069. The appliance failed to forward Radius response messages due to a race condition in an internal queue.	9.1.1.1
ID: 60638. In some use cases, tunnel's quiescent state was misconfigured, prompting tunnels to send too many keepalive packets and causing excessive LTE data usage.	9.1.1.1
ID: 60668. BGP multihop peers were configured from 169.254.0.0/16, resulting in unexpected NLRI prefix import failure.	9.1.1.0
ID: 60649. During route redistribution, prefixes of larger prefix length were being incorrectly matched with routes of smaller prefix length.	9.1.1.0
ID: 60637. A race condition in an internal queue caused the appliance to stop sending PIMv2 Hello messages.	9.1.1.0
ID: 60623. Some vrf-names were not properly updated in DHCP failover settings when tagged interfaces were not part of the default vrf.	9.1.1.0
ID: 60529. A WAN routing policy was not marking LAN SNAT flows as internet traffic, resulting in the flows being dropped.	9.1.1.0
ID: 60445. When IPsec pre-shared keys were changed, EdgeConnect was causing unexpected reboots due to a race condition in the encryption code.	9.1.1.0
ID: 60409. Improperly set ack_by,clear_by parameters caused an unexpected reboot when the appliance raised an alarm.	9.1.1.0
ID: 60361. An issue with incorrectly setting an interface index resulted in ARP not getting resolved on HA control link VLAN interfaces.	9.1.1.0
ID: 60280. Some SNMP traps were still being received for alarms that were no longer active and had been cleared on the appliance.	9.1.1.0
ID: 60236. When specific appliance models were configured for traditional HA, an issue with packet validation for ICMP/traceroute traffic was causing the appliances to reboot unexpectedly.	9.1.1.0
ID: 60204. An issue with BGP continuous route updates was triggered by default route received.	9.1.1.0
ID: 60166. For certain appliance models, using the Configuration History to compare configuration records was generating an error.	9.1.1.0
ID: 60141. EdgeConnect was rebooting due to memory corruption resulting from incorrect handling of redirected flows.	9.1.1.0
ID: 60083. A recommendation for setting the HTTP IPSLA "Request Timeout" value smaller than the "Inactive Flow Aging Interval" was missing from the help text.	9.1.1.0
ID: 60078. Security policy caused SaaS return traffic for hair-pinned flows to drop unexpectedly.	9.1.1.0
ID: 60076. Trying to process an FTP payload caused an unexpected reboot in certain EdgeConnect devices.	9.1.1.0

Issue	First Release to Resolve
ID: 60071. The reply to external traffic that was allowed to pass using a port forwarding rule was being sent to the incorrect WAN interface and dropped.	9.1.1.0
ID: 59945. An unexpectedly high sequence number packet was causing a problem with the FPOC engine, causing the appliance to reboot unexpectedly with no snapshot generated.	9.1.1.0
ID: 59944. On appliances with two PPPoE interfaces, the appliance stopped sending IPSLA traffic to the correct interface after one of the interfaces went down.	9.1.1.0
ID: 59927. After upgrading to 8.3.0.x, the bonding configuration on the EC-M-H appliance was changing from copper (wan0/wan1, lan0/lan1) to fiber (twan0/twan1, tlan0/tlan1).	9.1.1.0
ID: 59910. SHA256 and SHA512 were not supported on the EdgeConnect SSH client.	9.1.1.0
ID: 59883. Moving an interface from one segment to another segment caused the DHCP failover configuration to become invalid.	9.1.1.0
ID: 59806. When using branch NAT, a rule was setting the SNAT IP to the source IP, causing the appliance to reboot unexpectedly.	9.1.1.0
ID: 59794. If advanced segmentation was not enabled in CGNAT deployments, IPsec UDP tunnels and some PAT tunnels could enter a down state.	9.1.1.0
ID: 59744. Appliance generated spurious Disk SMART alarms.	9.1.1.0
ID: 59694. NTP alarms were reporting the NTP server as unreachable from the appliance even though the server was reachable.	9.1.1.0
ID: 59657. Traffic was being backhauled due to brownout limits, but appliance jitter, loss, and latency reports indicated no cause for brownout.	9.1.1.0
ID: 59629. TACACS+ authorization requests were not binding to the right source IP, causing them to go via mgmt0.	9.1.1.0
ID: 59582. A packet that should have been dropped due to a length mismatch was allowed to pass, causing the appliance to reboot unexpectedly.	9.1.1.0
ID: 59505. The GCM cipher configuration was blocking SSH to the appliance.	9.1.1.0
ID: 59412. When regional routing was enabled on a hub appliance, adding a local static route caused some prefixes received from spoke appliances to stop being advertised.	9.1.1.0
ID: 59347. Some appliances were unable to establish multiple IPsec tunnels toward Cisco Umbrella.	9.1.1.0
ID: 59147. Child SA ESP packets were sometimes dropped during phase2/IPsec rekeying in IKEv1 and IKEv2.	9.1.1.0
ID: 59131. Routes were being shared with BGP peers even though the outbound BGP route map did not permit it.	9.1.1.0
ID: 58267. When a tunnel went down and ICMP flows failed over to passthrough, they were not being reclassified even if the tunnel came back within the reclassification window.	9.1.1.0
ID: 58181. An issue with shared memory resources on an EC-V caused the appliance to reboot unexpectedly, resulting in VRRP failures.	9.1.1.0

Issue	First Release to Resolve
ID: 56994. A match string validation error caused an issue syncing ACL/policy maps.	9.1.1.0
ID: 55397. Flows were not getting reclassified to a new peer when a better route having the same metric and different peer priority was found.	9.1.1.0
ID: 60105. Following the upgrade to 9.1, some locations experienced performance issues.	9.1.0.3
ID: 60451. Following the upgrade to 9.1, some locations experienced performance problems due to packet drops on the inbound shaper	9.1.0.2
ID: 59848. An issue with select system calls was causing CPU0 to be stuck at 100% on EdgeHA appliances.	9.1.0.2
ID: 59794. If advanced segmentation was not enabled in CGNAT deployments, IPSec UDP tunnels and some PAT tunnels were ending up in a down state.	9.1.0.1
ID: 59716. The default admin credentials on a new KVM EC-V were not working in some earlier versions of ECOS.	9.1.0.1
ID: 59397. OSPF peering was not working on the lan0 interface, and various troubleshooting steps failed to fix the issue.	9.1.0.0
ID: 59257. When adding a new security policy rule from the table view, an additional "deny everything" rule was being added. The new rule could be deleted from the matrix view but not from the table view.	9.1.0.0
ID: 59254. A BGP neighbor configured with a leftover interface from a previous configuration was causing memory issues that eventually caused the appliance to reboot unexpectedly.	9.1.0.0
ID: 59235. When using preconfig to deploy new sites with lan0 set as the DHCP server, DHCP settings were being removed from some appliances.	9.1.0.0
ID: 59112. File transfer throughput, via FTP or Windows file sharing, was getting throttled when both Advanced Segmentation and DNAT were configured.	9.1.0.0
ID: 59037. Following the upgrade to ECOS 9.0.2.6, two separate EC-Vs deployed in Azure were rebooting unexpectedly on a frequent basis.	9.1.0.0
ID: 58946. UDP DNS packets were being dropped at the firewall due to a bad checksum after SNAT had been performed.	9.1.0.0
ID: 58875. If a native interface was admin down and a VLAN interface was deployed on it, the appliance would fail to send ARP requests on that interface after it was brought up.	9.1.0.0
ID: 57683. The ip mgmt-ip command was allowing any IP as input without validating that the IP address was configured on the appliance.	9.1.0.0
ID: 57670. The total length of ACL rule entries was not being validated, resulting in issues when pushing new security policies.	9.1.0.0
ID: 57459. An appliance that had mgmt0 disconnected was generating a large amount of alarm emails because DHCP was continuously trying to gen an IP address for it.	9.1.0.0
ID: 57296. Cloud Orchestrator showed a top talker IP for a specific appliance with a lot of flows that was not showing up in flow details or TCP dumps.	9.1.0.0

Issue	First Release to Resolve
ID: 57252. All EC-Vs with 8 GB or 12 GB of RAM and default system limits will continue to support 5000 and 10000 tunnels, respectively, but network memory allocation is reduced by 800 MB.	9.1.0.0
ID: 57116. During a file transfer between two sites, live view showed the backup link in red but the circuit had been up and available.	9.1.0.0
ID: 56968. Options to enable or disable validation of the Cloud Portal SSL certificate are now available in the Appliance Manager UI.	9.1.0.0
ID: 56943. DNS proxy self flows were not matching ACL rules with interface label match criteria.	9.1.0.0
ID: 56772. This release includes some code changes intended to block attackers from executing unauthorized shell commands.	9.1.0.0
ID: 56453. The monitor account had lost access to traceroute, ping, slogin, and other diagnostic commands.	9.1.0.0
ID: 56194. On an appliance with three OSPF peers, one of the peers was expectedly remaining in 2-way state, but the appliance was erroneously generating an alarm for it.	9.1.0.0
ID: 62320. The grub boot command line option for resetting to factory defaults failed to clear application definition-related files.	9.0.9.0
ID: 60307. With DNS proxy enabled on the EdgeConnect, certain systems did not register on the AD server with their domain name.	9.0.6.0
ID: 59132. After bringing up a new site, switches at multiple datacenters stopped receiving SD-WAN routes via OSPF, causing all sites to lose access to critical applications.	9.0.3.2
ID: 58947. After making changes to an overlay configuration, appliances were deleting and recreating the overlay and ending up with an incorrect configuration.	9.0.3.2
ID: 57799. After changing the IP of the internet interface with NAT turned on, the interface's public IP was not getting discovered.	9.0.3.0
ID: 57688. With advanced segmentation enabled, a route was not being removed from the routing table after the BGP peer stopped advertising the prefix.	9.0.3.0
ID: 57585. Orchestrator was failing to apply the TACACS+ configuration in the Management template on certain appliances.	9.0.3.0
ID: 57330. For appliances with uptime greater than one year, the calculation to number of days was being converted incorrectly for display in the appliance WebUI banner.	9.0.3.0
ID: 56999. A default route added to the route table via the GUI was not showing up in the CLI.	9.0.3.0
ID: 56955. A software issue encountered during the upgrade from ECOS 8.1.9.12 to 8.3.2.1 caused the appliance to become unresponsive.	9.0.3.0
ID: 56842. Following the migration from NX appliances, traffic in the Flows table was not displaying correctly.	9.0.3.0
ID: 56724. After upgrading to ECOS 8.3.0.x, a tunnel that had a space in its name would not come up.	9.0.3.0

Issue	First Release to Resolve
ID: 56619. Enabling advanced segmentation and moving lan0 from the default segment caused the appliance to reboot unexpectedly.	9.0.3.0
ID: 56156. Routes were flapping on one appliance of an EdgeHA pair due to ARP failures for some neighbors.	9.0.3.0
ID: 55853. Sending an appliance bandwidth increase at the same time as a shaper bandwidth increase that exceeded the current maximum bandwidth was resulting in a 50 Gbps max auto bandwidth on a 1 Gbps circuit. In addition, the maximum license bandwidth was not enforced in the inbound shaper.	9.0.3.0
ID: 58261. When disabling BGP, a flag that indicated a route had been advertised was not being reset, so routes were not being advertised when BGP was enabled again.	9.0.2.5
ID: 57259. Packets chained together by the Shaper had been inbound from passthrough and bonded tunnels and only passthrough was expected, causing the appliance to reboot unexpectedly.	9.0.2.5
ID: 57491. An issue when handling multicast join/prune messages caused the appliance to reboot unexpectedly.	9.0.2.2
ID: 57123. DNS snooping did not properly handle domain names that might be mapped to distinct IP addresses based on the client IP address.	9.0.2.2
ID: 57000. In some cases, during an upgrade, multiple calls were being made to management processes for database query operations. This was creating a race condition, the result being that OSPF route map rules were not getting configured correctly.	9.0.2.2
ID: 56967. When a loopback interface was selected as the source interface for management services such as NetFlow/IPFIX, traffic associated with these services was getting routed incorrectly as passthrough.	9.0.2.2
ID: 56910. ECOS 9.0.2.0 had a memory leak in the multicast routing process.	9.0.2.1
ID: 56881. The default route in the advanced segmentation route table was missing, causing connectivity issues with an appliance in a specific segment.	9.0.2.1
ID: 56877. Following a route change from a remote appliance, a tunnel mismatch on an inbound packet caused the appliance to reboot unexpectedly.	9.0.2.1
ID: 56791. In a case where two firewalls were sending packets to one another at the same time, the advanced segmentation code was dropping inbound packets.	9.0.2.1
ID: 56707. The interfaces page was displaying incorrect segment information when VLANs were in use.	9.0.2.0
ID: 56580. A default route learned from an eBGP peer was not always advertised to the SD-WAN fabric.	9.0.2.0
ID: 56164. Appliance rebooted due to a mishandling of sequence number wraparound in the packet order correction function.	9.0.2.0
ID: 56150. Previous ECOS versions failed to populate RTM and subnet route table with AWS TGW eBGP prefix updates.	9.0.2.0
ID: 56141. BGP sessions were not coming up with VTI in a non-default segment.	9.0.2.0
ID: 55993. An RTCP (RTP Control Protocol) connection was not properly classified when it was established using SIP.	9.0.2.0

Issue	First Release to Resolve
ID: 55933. Compound applications were not matching correctly when using a hyphen to indicate an IP range.	9.0.2.0
ID: 55806. When advanced segmentation was enabled, enabling Boost with IP Header Compression disabled was causing udp flows to fail with invalid checksums.	9.0.2.0
ID: 55798. A path characterization packet was mishandled when it was received after the corresponding tunnel had been deleted, causing the appliance to reboot.	9.0.2.0
ID: 55739. Hub site tunnels were stuck in "MTU discovery," which caused a network outage.	9.0.2.0
ID: 55692. There were memory leaks associated with certain tunnel configuration steps, causing system memory depletion and eventually appliance reboot.	9.0.2.0
ID: 55663. ECOS stats from the Orchestrator Rest API were returning interface stats and details but the label but the label wasn't showing up.	9.0.2.0
ID: 55586. At times, when MySQL traffic was being sent over the Default BIO, WAN latency was spiking and causing application issues.	9.0.2.0
ID: 55500. After adding back an interface that had been deleted more than 100 days earlier, packets were getting held up in a shaper queue, resulting in a LAN Rx buffer shortage.	9.0.2.0
ID: 55352. Updated the SSH library to address a number of CVEs.	9.0.2.0
ID: 55181. The WebSocket connection to Orchestrator was being closed incorrectly after receiving a delayed close event from the kernel TCP stack.	9.0.2.0
ID: 55073. After deployment with ECOS 8.3.1.x, the lan3 and wan3 interfaces on an EC-V were down and required manual intervention to make operational.	9.0.2.0
ID: 54959. RADIUS/TACACS+ were not available under Management Services.	9.0.2.0
ID: 54593. Appliance rebooted when it hit an ACL configuration error in the configuration database during initialization.	9.0.2.0
ID: 55830. If advanced segmentation was enabled, errors were being generated when trying to add more than 10 BGP peers from the routing segmentation page.	9.0.1.1
ID: 55728. Following the upgrade to ECOS 9.0.1.0, BGP sessions to AWS Transit Gateway stopped working.	9.0.1.1
ID: 55555. When deleting many BGP/OSPF routes learned from a peer subnet update, some routes were left undeleted but marked as pending deletes. This was causing affected appliances to show as DOWN for remote SD-WAN routes.	9.0.1.0
ID: 55203. ssh was listening on all interfaces even though it was enabled only on loopback.	9.0.1.0
ID: 54980. Internet flows were performing poorly and there was an increase in packet decode errors when Boost was enabled.	9.0.1.0
ID: 54956. BGP routes were flapping at multiple sites in different locations at the same time.	9.0.1.0

Issue	First Release to Resolve
ID: 54928. With advanced segmentation enabled, OSPF peers were not coming up unless BGP was enabled in the default segment.	9.0.1.0
ID: 54926. Multicast pimX interface IP addresses were being advertised to OSPF/BGP peers, requiring users to add route-filtering rules to OSPF and BGP outbound maps to prevent advertisement of internal subnets used for multicast.	9.0.1.0
ID: 54373. DNS proxy was not supported with advanced segmentation enabled.	9.0.1.0
ID: 53538. Under heavy logging demand, some log messages were overwritten resulting in corrupted messages.	9.0.0.0
ID: 51178. Added more logging around tunnel stats to help in troubleshooting tunnel down/flapping issues.	9.0.0.0
ID: 48844. HA traffic (inbound flow) was being sent to LAN0 when the secondary appliance (LAN1) was powered down.	9.0.0.0

Resources

If you have any questions, contact your HPE Aruba Networking sales representative.

For product and technical support, contact HPE Aruba Networking using any of the methods below:

Contract Support

If you are an existing HPE Aruba Networking customer, contact Support at 1.800.633.3600 (toll-free in the USA).

Support Portal

The HPE Networking Support Portal provides one-click entry to case management, digital RMA, asset management, custom notification settings, and software and document downloads. Process an RMA online or enjoy the convenience of live chat in multiple languages.

- https://networkingsupport.hpe.com/home

Global TAC

HPE Aruba Networking's technical assistance centers provide AI-driven 24x7x365 support with world-class customer satisfaction and net promoter scores. It is not just break/fix information, but includes advice on configuration, administration, interoperability, and other best practices.

- https://www.hpe.com/us/en/networking/hpe-aruba-networking-support-services.html

Airheads Community

Learn and share about wireless and wired LANs, network security, mobile devices, applications, software-defined networking (SDN), network management, and mobile engagement in the vibrant, interactive Airheads Community.

- https://community.arubanetworks.com/home

Learn more at

hpe.com

Chat now (sales)

© Copyright 2025 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty.
Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Trademark acknowledgments, if needed. All third-party marks are property of their respective owners.

Hewlett Packard Enterprise