



HPE Aruba Networking EdgeConnect SD-WAN Orchestrator Release Notes

Version 9.4.6_40044

Revision A: October 21, 2025

This document provides important information about HPE Aruba Networking EdgeConnect SD-WAN Orchestrator 9.4.6, including top items, limitations, new features, issues fixed, and upgrade considerations. For historical features and fixes, information about installation procedures, CLI-only features, port requirements, and configuration best practices, see [Additional information](#).

Revision history

Date	Document Version	Revisions Made
October 21, 2025	Rev A	Initial document revision.

Top items for this release

Critical items

- SD-WAN Orchestrator 9.4.x and 9.5.x releases present the critical risk of failed cryptographic functions caused by a race condition. These releases use a new, updated cryptographic library that complies with the FIPS standard. A defect in this updated library introduces a potential race condition when generating cryptographic key material. This race condition can lead to the generation of corrupted key material, causing the two endpoints to become cryptographically unsynchronized. As a result, any functions reliant on encryption and decryption will fail. There is no sustainable workaround for this issue; it is critical to upgrade SD-WAN Orchestrator to a supported version. For more information, see [Upgrade considerations](#).
- If your Orchestrator is running version 9.4.x or later on Rocky Linux, FIPS may be enabled by default. If FIPS is enabled, connectivity between Orchestrator and EdgeConnect appliances running ECOS version 9.3.x.x or earlier will fail. This is because the Orchestrator in FIPS mode only permits stronger, FIPS-compliant cryptographic algorithms, while EdgeConnect appliances running affected versions attempt to use non-FIPS compliance ciphers. To resolve the issue, disable FIPS mode on the Orchestrator.

Even if all the appliances in the network are currently running ECOS version 9.4.x.x or later, it is recommended that FIPS be disabled on the Orchestrator. This is to allow a newly deployed appliance or replacement (RMA) appliance that ships with ECOS 9.3.x.x or earlier to establish a connection with the Orchestrator during Zero Touch Provisioning (ZTP).

Note

Only an admin user can enable/disable FIPS mode.

You can check the status of FIPS mode through the CLI with the following prompt:

```
fips-mode-setup --check
```

You can enable or disable FIPS mode through the SD-WAN Orchestrator CLI with the following prompts:

```
fips-mode-setup --disable
```

```
fips-mode-setup --enable
```

Top items for this release (continued)

Note

OVA's for Orchestrator versions 9.4.3.40577 and 9.5.3.40081 have been re-issued with FIPS mode disabled by default. OVA's for future releases in all release streams will have FIPS disabled by default.

- In SD-WAN Orchestrator 9.3.0, most of the APIs changed to accommodate API-based RBAC. If you have integrated your IT systems using SD-WAN Orchestrator REST APIs, **be cautious about upgrading** to SD-WAN Orchestrator 9.4.6 until you change your integrations to work with SD-WAN Orchestrator 9.4.6. If you cannot make this change easily, please contact your account team and provide a list of APIs you use. The team will investigate whether compatibility can be provided with these older APIs in future SD-WAN Orchestrator releases. For a reference to pre-upgrade API endpoints, see [Pre 9.3 Orchestrator API Endpoints](#).
- Most of the currently installed, self-hosted SD-WAN Orchestrators run CentOS 7 as the underlying Linux operating system. CentOS 7 is going end-of-life (EOL) on June 30, 2024. After that date, it will not be possible to get Linux OS security patches or updates for SD-WAN Orchestrators running on CentOS 7. The SD-WAN Orchestrator application will continue to be maintained as per product lifecycle policy, but security patches for the underlying OS will no longer be available.

It is highly recommended that all users running CentOS move to Rocky Linux-based virtual machines (VMs) to benefit from OS features, fixes, and security patches. New installation packages of this release have Rocky Linux as the underlying OS. Simply upgrading the SD-WAN Orchestrator application does not change the underlying VM. The procedure requires creating a complete backup of your current SD-WAN Orchestrator, building a new Rocky Linux VM, and loading the backup on the new machine.

Note

Self-hosted/on-prem SD-WAN Orchestrators (IaaS AWS) are not affected. EdgeConnect Orchestrator-as-a-Service (OaaS, also known as Cloud Orchestrator) products are also not affected.

Documentation of detailed procedures for this operation is provided on the [HPE Aruba Networking EdgeConnect SD-WAN documentation site](#), and a video walkthrough is available on [HPE Aruba Networking's "Airheads Broadcasting" YouTube channel](#).

- Prior to upgrading to SD-WAN Orchestrator 9.4.6, all EdgeConnect SD-WAN appliances must be on release 8.3.2.0 or greater, or 9.x.x.x release streams. EdgeConnect SD-WAN appliances running a release prior to 8.3.2.x will lose all communications to the SD-WAN Orchestrator.
- Issuing large queries creates "temp tables" that use extra disk space, and these tables do not clear after the query is done. Using this extra space can result in a high volume of stats from the Stats Collector. If you notice a high volume of stats, reduced disk space, or degraded performance, as a workaround you can limit the number of applications an appliance reports, and also restart the SD-WAN Orchestrator periodically, which will claim back the used disk space.
- In SD-WAN Orchestrator 9.4.1 and later, RADIUS authentication using MSCHAP, MSCHAPv2, and EAP-MSCHAPv2 will fail. These SD-WAN Orchestrator versions use the FIPS-compliant Bouncy Castle library. For security reasons, the Bouncy Castle library does not support MD4 hash functionality, as the MD4 hash is a cryptographically weak, broken hashing algorithm that has been deprecated by IETF. Because MSCHAP, MSCHAPv2, and EAP-MSCHAPv2 depend on MD4, these authentication methods will not work in SD-WAN Orchestrator 9.4.1 and later.

This impacts all users using RADIUS authentication with MSCHAP, MSCHAPv2, and EAP-MSCHAPv2. It is suggested to use more secure authentication methods, such as OAUTH or SAML. If using RADIUS authentication, use PAP or CHAP options.

Other items

- HPE Aruba Networking is continuing to develop full functionality of existing features with Advanced Segmentation, and some features are not supported or require additional consideration before installing this release. See [Release limitations](#) for more information about these features and other important information. Documentation specific to the Advanced Segmentation feature can be found [here](#).



Top items for this release (continued)

- Tunnel Groups are not supported in this release and will be deprecated in a future SD-WAN Orchestrator version. If you are using Tunnel Groups, you should migrate to Business Intent Overlays (BIOs).
- SD-WAN Orchestrator must be allowed to access the internet during the upgrade to install libraries required to run Scheduled Reports. If access through the firewall is not enabled, the upgrade will succeed without installing the libraries, but Scheduled Reports will fail. If necessary, customers can install the libraries later, when access through the firewall is permitted.

If policy prohibits access at all times, customers can upgrade their current SD-WAN Orchestrator to the new version, install a new SD-WAN Orchestrator VM at the same new version, back up the existing (upgraded) SD-WAN Orchestrator, and then restore the backup on the new SD-WAN Orchestrator VM – new SD-WAN Orchestrator images will have the required libraries.



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:

- IPsec Suite B is not fully supported in SD-WAN Orchestrator 9.4.6.
- If you use preconfiguration on any appliance that is part of an EdgeHA pair, any changes to the deploymentInfo section of YAML require that both appliances have their configurations applied. If not, orchestration results in a mismatch and traffic disruption.
- In order to use the Availability feature to see availability stats (Monitoring > Performance > Availability), Orchestrator 9.4.6 requires ECOS version 9.3.4.x or later, or 9.4.2.x or later.
- The following limitations apply to the Unified Fabric feature in 9.5.x releases:
 - The feature works with EdgeConnect hardware models only.
 - No route filtering is available on EdgeConnect. All routes are sent to ORO (Overlay Route Orchestrator).
 - For deployment in an existing EdgeConnect fabric, WAN uplink labels on EdgeConnect must be set as “_inet” or “_mpls”.
 - OTO tunnels map to the VRF_Zone pair associated with the WAN interface used for tunnel establishment.
 - Roles are not transported between fabrics.
 - EdgeConnect integration with Microbranch supports only L3 Routed/NAT mode. Centralized L2 (CL2) mode is not supported.
 - The feature is only supported in Classic Central (and is not supported in Central Next).

Feature limitations when segmentation is enabled

The following features are not supported when segmentation is enabled:

- IPv6
- Network Address Translation (NAT) 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, SD-WAN Orchestrator removes and reapplies all Overlays on all appliances. Afterward, the SD-WAN Orchestrator tears down and recreates every tunnel again. Any manual tunnels and route policies present on the EdgeConnect SD-WAN are removed and must be recreated by the user manually.

Each EdgeConnect SD-WAN will experience 2-15 minutes of downtime as Overlays are removed and re-added. The SD-WAN Orchestrator will operate on up to 50 appliances at a time in no specific order until all appliances have been configured to support segmentation. The process takes longer if appliances are disconnected from the SD-WAN Orchestrator in the middle of the enablement process.

When implementing segmentation, it is recommended that you review the [Advanced Segmentation Configuration Guide \(PDF\)](#).



Release limitations (continued)

Features supported in the default or same segment

The following features have been verified if 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 only in the default segment.
- Management Services
 - HTTP(S), Cloud Portal, SD-WAN Orchestrator are only supported in the default segment.
 - RADIUS/TACACS+ are only supported in the default segment.
- LAN-side passthrough tunnels (IPSec and GRE) 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.

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.
- Customers who deploy a new SD-WAN Orchestrator (9.0.7+ or 9.1.1+) and plan to use it to manage appliances on ECOS 8.x releases, should disable routing segmentation first.
- 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](#).
- When enabling Regional Loopbacks, each loopback is assigned a sequentially incrementing loopback number. For instance, if you have two regions—"EAST" with 10.1.1.0/24 and "WEST" with 10.2.2.0/24—the SD-WAN Orchestrator creates lo20001 for EAST and lo20002 for WEST. Features such as BGP refer to an explicit loopback name and need to be adjusted after regional loopbacks are assigned to the appliance.
- Starting with Orchestrator 9.3.5, DHCP lease time values are given in seconds, not in hours. If you had set an integer value using hours in the preconfig YAML file, that value should be updated to the appropriate value in seconds to avoid causing issues. (See ID: 26511 in [Issues fixed from past releases](#).)
- Be aware of the following licensing considerations:
 - Hardware assets are not required to co-reside in the same secondary account where the software license resides (Bandwidth, Boost, Advanced Security, or Dynamic Threat Defense).
 - Software licenses applied to an appliance should be from same account (Primary/Secondary). An appliance cannot accept software licenses from multiple accounts.
 - For ease of management and optimal usability, it is recommended to co-terminate licenses or keep the number of secondary accounts to a minimum.



Security issues fixed

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

Issue ID	CVE	CVSS Score	CVSS Vector	Description	First Release to Resolve
ID: 40292	CVE-2009-2475 CVE-2009-2476 CVE-2009-2689 CVE-2009-2690 CVE-2009-3728 CVE-2009-3879 CVE-2009-3880 CVE-2009-3881 CVE-2009-3882 CVE-2009-3883 CVE-2009-3884	N/A	N/A	This release was patched to address the following CVEs: CVE-2009-2475, CVE-2009-2476, CVE-2009-2689, CVE-2009-2690, CVE-2009-3728, CVE-2009-3879, CVE-2009-3880, CVE-2009-3881, CVE-2009-3882, CVE-2009-3883, CVE-2009-3884	9.4.6
ID: 27113	N/A	7.2	CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H	A prototype pollution vulnerability created the possibility for remote code execution or a denial-of-service attack.	9.4.2
ID: 27098	N/A	N/A	N/A	Java plugins were erroneously reporting security vulnerabilities from previous versions that no longer existed in the current version.	9.4.2
ID: 26683	CVE-2021-38153	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-2021-38153.	9.4.2
ID: 25005	CVE-2023-37421	8.1	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:N	A validation issue in the SAML Remote Authentication Server created the potential for a cross-site scripting vulnerability.	9.4.1
ID: 24869	CVE-2023-2650	N/A	N/A	This release was patched to address CVE-2023-2650 (OpenSSL vulnerability).	9.4.1
ID: 24804	N/A	N/A	N/A	Users were unable to populate the custom CA certificate store with certificates from the AVC dataset.	9.4.1
ID: 23957	CVE-2023-37424	8.1	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	A command issue created the potential for an unauthenticated user to execute a command injection vulnerability.	9.4.1
ID: 23596	CVE-2023-37427	7.2	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H	An issue within the sys dump process created the potential for a remote code execution vulnerability.	9.4.1



Issues fixed

The following known issues have been fixed in SD-WAN Orchestrator 9.4.6. Issues fixed in past releases can be found [here](#).

Issue ID	Description
ID: 40292	This release was patched to address the following CVEs: CVE-2009-2475, CVE-2009-2476, CVE-2009-2689, CVE-2009-2690, CVE-2009-3728, CVE-2009-3879, CVE-2009-3880, CVE-2009-3881, CVE-2009-3882, CVE-2009-3883, CVE-2009-3884
ID: 40265	An issue with a liner scan of all records during daily aggregation tasks caused performance issues on the Orchestrator and resulted in daily aggregation not completing as expected.
ID: 40238	The RMA wizard did not update the Orchestrator software version to the new appliance, which forced the Orchestrator to choose the wrong upload folder for backup upload.
ID: 40096	An issue in the RMA wizard caused a timeout error during appliance replacement due to slow reboot and initialization times.
ID: 39953	When a VM was configured as SC-only and the root partition approached capacity, the Orchestrator service stopped but was not disabled, triggering a "Failed to start Orchestrator service" error.
ID: 39924	When running the RMA wizard, a regular expression was used in SQL queries, which degraded MySQL performance and caused timeouts for other queries.
ID: 39812	Recurring Zscaler session invalidation and HTTP connection pool shutdown caused the Orchestrator to throw a recurring configuration error.
ID: 39599	When a certificate issuer used non-ASCII characters in a request to check connectivity to the portal or the Orchestrator, the system threw an exception and blocked the request.
ID: 39324	A typo in the list of country codes provided by Zscaler caused Zscaler deployment to become stuck in a pending state.
ID: 38914	Because an error flag was not reset after a file upload error, subsequent attempts caused the system to throw error messages even upon successful upload.
ID: 38795	Internal subnets were not being deleted when routing segments were deleted, creating interruptions in flows and dropped policies.
ID: 38728	When DHCP server settings were changed on one interface, relay server settings were also changed erroneously.



API changes

The following API changes are included in SD-WAN Orchestrator 9.4.6.

Important

In SD-WAN Orchestrator 9.3.0, most APIs have changed to accommodate API-based RBAC. If your IT systems are integrated with SD-WAN Orchestrator REST APIs, do not upgrade to SD-WAN Orchestrator 9.3.0 until you modify your integrations to work with SD-WAN Orchestrator 9.3.0. If you cannot make this change easily, contact your account team. The account team will determine if compatibility can be provided in future SD-WAN Orchestrator releases.

For information on the API, including post-9.3.0 changes, best practices, and more, visit <https://developer.arubanetworks.com/aruba-edgeconnect/docs/whats-new>.

Changes from SD-WAN Orchestrator 9.0.2

Application and group definitions

Added `/applicationDefinition/updatedAt`, which returns modified time and hash of applications and application groups.

Added `application_to_group` to `/applicationDefinition/export/{type}` to download application to group mapping details.

Changes from SD-WAN Orchestrator 9.0.4

To fix issue 19405, changed `/subnets/{cache}` to return only the configuration for the default segment instead of all segments.

Changes from SD-WAN Orchestrator 9.1.0

To fix issue 20153, added loopback details to the API: `GET /loopbackOrch/pool/history/{seg}`

Changes from SD-WAN Orchestrator 9.2.4

To address performance issues, `GET /appliance` no longer returns `interfaceList`, `zoneList`, `tagsList`, and `haPeer` information. This information can be found in new APIs:

- `GET /appliance/interfaceMeta`
- `GET /appliance/zoneListMeta`
- `GET /appliance/customTagMeta`
- `GET /appliance/haPeerMeta`



Upgrade considerations

The following list summarizes considerations that must be addressed when upgrading from any previous version of SD-WAN Orchestrator to 9.4.6.

Summary	Description																																																				
Outbound Orchestrator TLS support limitations	Starting from version 9.4.x, any outbound connection from Orchestrator will support only TLS 1.2 and TLS 1.3.																																																				
Zscaler locations/sublocations removed upon upgrade	Upon upgrade from Orchestrator 9.3.x, 9.4.x, or 9.5.x to version 9.3.6 or 9.5.3, Zscaler locations/sublocations gateway rules with stale appliance or network interfaces or firewall zones will be removed. It is strongly suggested to review your Zscaler sublocation rules before upgrade, as these changes could impact your network.																																																				
Allow Stats Collector to upgrade without stop or restart	<p>Upon upgrade to Orchestrator 9.3.6+, 9.4.4+, or 9.5.x, after the Orchestrator CLI upgrade commands appear to complete, the Stats Collector SQL database upgrade continues to operate in the background for a short period after the Stats Collector starts. During this time, you may observe a transient period where the Stats Collector appears "Not Connected" or unavailable to the Orchestrator UI.</p> <p>When <code>/home/gms/sc/logs/statscollector.log</code> appears after the log entries below, Stats Collector will soon appear as "Connected" and available in the Orchestrator UI.</p> <pre>- info: 0 : upgradeDatabase: Upgrading db if required . . - info: 0 : Express server listening on port 7000 and host 127.0.0.1</pre> <p>It is recommended that you do not attempt a manual or forced stop or restart of Orchestrator or Stats Collector during this period of database upgrade, as there is a risk of SQL database corruption, which would leave Stats Collector inoperable.</p>																																																				
KPI phase 2 upgrade constraints	<p>If you are upgrading from Orchestrator 9.3.6 to version 9.4.3, you will lose access to KPI phase 2 (availability stats) when the Orchestrator is paired with ECOS 9.3.4.x+ and 9.4.2.x+ appliances. This is because KPI phase 2 stats for the Orchestrator 9.4.x release stream are only available in version 9.4.4 and later. To retain access to KPI phase 2 stats, upgrade to version 9.4.4 or later. See the release matrix below for details on which ECOS and Orchestrator versions are compatible with the different phases of the KPI feature:</p> <table border="1"> <thead> <tr> <th>ECOS</th> <th>Availability stats</th> <th>Orchestrator</th> <th>Availability stats</th> </tr> </thead> <tbody> <tr> <td>9.1</td> <td>none</td> <td>9.1</td> <td>none</td> </tr> <tr> <td>9.2</td> <td>none</td> <td>9.2</td> <td>none</td> </tr> <tr> <td>9.3.1</td> <td>phase 1</td> <td>9.3.1</td> <td>phase 1</td> </tr> <tr> <td>9.3.2</td> <td>phase 1</td> <td>9.3.2</td> <td>phase 1</td> </tr> <tr> <td>9.3.3</td> <td>phase 1</td> <td>9.3.3</td> <td>phase 1</td> </tr> <tr> <td>9.3.4</td> <td>phase 2</td> <td>9.3.4</td> <td>phase 1</td> </tr> <tr> <td></td> <td></td> <td>9.3.6</td> <td>phase 2</td> </tr> <tr> <td>9.4.1</td> <td>phase 1</td> <td>9.4.1</td> <td>phase 1</td> </tr> <tr> <td>9.4.2</td> <td>phase 2</td> <td>9.4.2</td> <td>phase 1</td> </tr> <tr> <td>9.4.3</td> <td>phase 2</td> <td>9.4.3</td> <td>phase 2</td> </tr> <tr> <td>9.4.4</td> <td>phase 2</td> <td>9.4.4</td> <td>phase 2</td> </tr> <tr> <td>9.5.x</td> <td>phase 2</td> <td>9.5.x</td> <td>phase 2</td> </tr> </tbody> </table>	ECOS	Availability stats	Orchestrator	Availability stats	9.1	none	9.1	none	9.2	none	9.2	none	9.3.1	phase 1	9.3.1	phase 1	9.3.2	phase 1	9.3.2	phase 1	9.3.3	phase 1	9.3.3	phase 1	9.3.4	phase 2	9.3.4	phase 1			9.3.6	phase 2	9.4.1	phase 1	9.4.1	phase 1	9.4.2	phase 2	9.4.2	phase 1	9.4.3	phase 2	9.4.3	phase 2	9.4.4	phase 2	9.4.4	phase 2	9.5.x	phase 2	9.5.x	phase 2
ECOS	Availability stats	Orchestrator	Availability stats																																																		
9.1	none	9.1	none																																																		
9.2	none	9.2	none																																																		
9.3.1	phase 1	9.3.1	phase 1																																																		
9.3.2	phase 1	9.3.2	phase 1																																																		
9.3.3	phase 1	9.3.3	phase 1																																																		
9.3.4	phase 2	9.3.4	phase 1																																																		
		9.3.6	phase 2																																																		
9.4.1	phase 1	9.4.1	phase 1																																																		
9.4.2	phase 2	9.4.2	phase 1																																																		
9.4.3	phase 2	9.4.3	phase 2																																																		
9.4.4	phase 2	9.4.4	phase 2																																																		
9.5.x	phase 2	9.5.x	phase 2																																																		
Error when logging in with non-ASCII characters	<p>When an update is made in the Orchestrator or EdgeConnect web UI, you may see the following error message:</p> <pre>Non-ASCII characters are not supported</pre>																																																				



Summary	Description
	<p>This message stems from a fix made to prevent non-ASCII characters from being entered. As part of the fix, users cannot enter any non-ASCII characters into any user input field in Orchestrator (version 9.3.6+, 9.4.3+, or 9.5.2+) or EdgeConnect (9.4.3.0+, 9.5.2.0+, or 9.6.0.0+). To avoid this error message, do not enter non-ASCII characters into text fields of the web UI. If some fields already contain non-ASCII characters, those characters must be corrected to ASCII text manually.</p>
Review RBAC roles post-Orchestrator upgrade	<p>Because new menus are not automatically included in existing RBAC roles during the upgrade process, it is recommended that the Orchestrator administrator reviews the RBAC roles each time the Orchestrator is upgraded.</p>
Vulnerable algorithm ciphers retired in SD-WAN Orchestrator 9.4.3	<p>For security purposes, the underlying library used to upload SD-WAN Orchestrator backups to the SFTP/SCP server has been upgraded to the latest version. The following vulnerable algorithm ciphers have been retired as of SD-WAN Orchestrator 9.4.3:</p> <ul style="list-style-type: none"> • Server host key algorithms: ssh-rsa, ssh-dss • Encryption algorithms: aes128-cbc, aes192-cbc, aes256-cbc, 3des-cbc, blowfish-cbc <p>The following algorithm ciphers have been added in SD-WAN Orchestrator 9.4.3:</p> <ul style="list-style-type: none"> • Server_host_key_algorithms: rsa-sha2-512, rsa-sha2-256 • Encryption_algorithms: aes192-ctr, aes128-gcm@openssh.com, aes256-gcm@openssh.com • Mac algorithms: hmac-sha2-512
Local Breakout uses only passthrough tunnel status	<p>Current computation passthrough tunnel availability does not consider the IPSLA state and only uses tunnel state. When a passthrough tunnel's state is "up - ip sla disabled," it is treated as "Local Breakout Up" in availability computation, when it should be treated as "Local Breakout Down."</p>
Risk of failed cryptographic functions in Orchestrator 9.4.x and 9.5.x releases caused by race condition	<p>In Orchestrator 9.4.x and 9.5.x releases, a race condition encountered while generating cryptographic material for encryption/decryption operations can cause cryptographic key corruption. This issue leads to various failure symptoms on functions dependent on cryptographic keys. These symptoms include, but are not limited to:</p> <ol style="list-style-type: none"> 1. EdgeConnect SD-WAN tunnels going down on key rotation. 2. EdgeConnect third-party IPsec tunnels going down and Orchestrator audit logs filling with Action = "Modify pass through tunnels" and Task Status = "IN_PROGRESS." 3. Orchestrator raising "Orchestration failed. Failed to apply Overlays" alarms. 4. Orchestrator being unable to synchronize with the appliances and audit logs showing Action = "Push Orchestrator meta data to Appliances" and Task Status = "IN_PROGRESS." <p>The affected Orchestrator versions are 9.4.1.41583, 9.4.2.40572, 9.4.2.40572, 9.4.2.40586, 9.5.0.40631, 9.5.0.x, and 9.5.1.x. As a precaution, HPE engineering has removed all affected versions from the portal.</p> <p>To resolve this issue, upgrade the Orchestrator to one of the fixed versions—Orchestrator 9.4.2.40649 and later, or Orchestrator 9.5.2.x and later—as soon as possible.</p>
Large queries use extra disk space and produce a high volume of stats	<p>Issuing large queries creates "temp tables" that use extra disk space, and these tables do not clear after the query is done. Using this extra space can result in a high volume of stats from the Stats Collector. If you notice a high volume of stats, reduced disk space, or degraded performance, as a workaround you can limit the number of applications an appliance reports, and also restart the SD-WAN Orchestrator periodically, which will claim back the used disk space.</p>
Admin and gms users now separate users	<p>In SD-WAN Orchestrator 9.4.1 and later, SD-WAN Orchestrator separates the admin user from the gms user. Previously, these users had been tracked as one user. While admin users still log in via SSH, admin users now have sudo access as well. Going forward, the gms user will be a sandboxed user without admin privileges.</p>



Summary	Description
	With this change, <code>/home/gms/gms/orch-setup -c</code> and <code>/home/gms/gms/orch-setup -p</code> now require a sudo password for the admin user, instead of a root user password. In addition, to perform upgrades, <code>/home/gms/gms/orch-setup -u</code> must now be run as <code>sudo /home/gms/gms/orch-setup -u</code> .
Check Point CloudGuard Connect disabled with version 9.4.1	Upon upgrade to SD-WAN Orchestrator 9.4.1, the Check Point CloudGuard Connect option is no longer available under Configuration > Cloud Services. This is because Check Point has discontinued support for the CloudGuard API. Users can instead use Service Orchestration for Check Point (Configuration > Cloud Services > Service Orchestration).
RADIUS authentication using MSCHAP, MSCHAPv2, and EAP-MSCHAPv2 will fail	In SD-WAN Orchestrator 9.4.1 and later, RADIUS authentication using MSCHAP, MSCHAPv2, and EAP-MSCHAPv2 will fail. These SD-WAN Orchestrator versions use the FIPS-compliant Bouncy Castle library. For security reasons, the Bouncy Castle library does not support MD4 hash functionality, as the MD4 hash is a cryptographically weak, broken hashing algorithm that has been deprecated by IETF. Because MSCHAP, MSCHAPv2, and EAP-MSCHAPv2 depend on MD4, these authentication methods will not work in SD-WAN Orchestrator 9.4.1 and later. This impacts all users using RADIUS authentication with MSCHAP, MSCHAPv2, and EAP-MSCHAPv2. It is suggested to use more secure authentication methods, such as OAUTH or SAML. If using RADIUS authentication, use PAP or CHAP options.
REST API limitations for Appliance Access Groups	Appliance Access Groups formed using groups instead of regions do not have the privileges to post using the REST API.
Changes to Zscaler orchestration starting with version 9.3.0	Before Orchestrator 9.3.0, the Orchestrator synced with the Zscaler portal to download artifacts such as location, sublocation, VPN credentials, and static IP, and then used this information to update settings on the Orchestrator. However, this process involved making multiple, rate-limited API calls to the Zscaler portal, creating issues and delays for orchestration. To address this, in Orchestrator 9.3.0 and later, Zscaler orchestration requires users to make corresponding changes directly to the Orchestrator, rather than downloading and syncing with the Zscaler portal for these artifacts. As a result, these settings are no longer downloaded by the Orchestrator from the Zscaler portal, and Orchestrator will not recognize any manually created artifacts or manually updated parameters after 9.3.0.
MFA required for OaaS starting with version 9.3.0	Starting from SD-WAN Orchestrator 9.3.0, multi-factor authentication (MFA) is required when using the Orchestrator-as-a-Service (OaaS) offering from Silver Peak, also known as Cloud Orchestrator. For on-premise SD-WAN Orchestrator deployments, MFA is optional.
Upgrade unavailable on FC27 OS	If running FC27 as the OS, then upgrade from version 9.2.5.40075 to 9.4.1 is currently unavailable.
Default settings in Advanced Security Settings	Upgrades to SD-WAN Orchestrator 9.4.6 retain previous Advanced Security Settings, with the exception of Perform Additional Identity Verification on Web Sockets. This setting is now always enabled and is no longer displayed as an option in the Advanced Security Settings dialog box.
28.5K Dynamic Route limit within 30K total limit	IPv4 routes can hold up to 30k of total routes, including 28.5k 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 1.5k are local or learned routes. Alarms are thrown when IPv4 crosses the 28.5K boundary for dynamic routing.
REST API	If you are using the REST API to manage your network, take extra caution with upgrading to SD-WAN Orchestrator 9.3.0, as some existing APIs are currently undergoing changes. These changes are planned to be completed in a future SD-WAN Orchestrator release. For more information, see Top items for this release .
Zscaler integration requires GRE to be enabled	When upgrading to SD-WAN Orchestrator 9.4.6, the Zscaler integration requires the Zscaler account to have GRE enabled. If GRE is not enabled, the upgrade fails. If GRE is disabled on



Summary	Description
	<p>your account, the Zscaler integration will report errors upon upgrade, and you must enable GRE on your Zscaler account.</p> <hr/> <p>Note</p> <p>You are not required to use GRE tunnels. However, you must have GRE enabled on your account even if you do not use the functionality.</p>
Internet Breakout Policy on hub appliances	<p>After SD-WAN Orchestrator is upgraded to version 9.1.0 or later, hub appliances may start to drop internet traffic if the hub internet breakout policy is explicitly configured and the only action is Drop. To keep hub appliances from dropping internet traffic, configure the hub internet breakout policy properly. Update the Business Intent Overlay Internet Policy (Preferred Policy Order) for all hub appliances prior to upgrade.</p>
IPSec anti-replay window incompatibility	<p>SD-WAN Orchestrator 9.1.4 disables IPSec anti-replay window functionality unless all appliances are running ECOS 9.1.2.0 or later. This avoids a compatibility issue that prevents IPSec tunnels from forming between appliances running older ECOS versions. Note that depending on the network size and conditions, it is possible that some tunnels may briefly go down when IPSec anti-replay is disabled.</p>
User names limited to 40 characters	<p>User Names created in Orchestrator 9.2.x cannot exceed 40 characters. In future versions of Orchestrator, user names will have a 512-character limit.</p>
Minor alarm upon upgrading from older ECOS images	<p>An alarm may trigger on SD-WAN Orchestrator version 9.1 or newer under the following conditions:</p> <ul style="list-style-type: none"> 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. <p>To clear this alarm, perform the following steps for each EdgeHA pair:</p> <ul style="list-style-type: none"> 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.
Issue 1236: Tenant single sign-on not working	<p>The OrchestratorSP tenant single sign-on feature is not working in Orchestrator (tenant) version 9.1.0. This issue will be fixed in a future release of OrchestratorSP, which is targeted for the October 9th maintenance window. Service providers will not need to upgrade tenants to get this fix.</p>
Duplicate routes in EdgeHA with regional routing	<p>In an EdgeHA configuration with regional routing, hubs are resending routes learned from the EdgeHA site back to the same site. To work around this issue, do the following on each appliance in the EdgeHA pair:</p> <ol style="list-style-type: none"> On the BGP page (Configuration > Networking > Routing > BGP), enable BGP, configure the ASN and Router ID, and then click Apply. <hr/> <p>Note</p> <p>It is not necessary to configure BGP peers if you are using OSPF on the LAN side.</p> <hr/> <ol style="list-style-type: none"> On the Routes page (Configuration > Networking > Routing > Routes), select the checkboxes for "Filter Routes From SD-WAN Fabric With Matching Local ASN" and "Include BGP Local ASN to routes sent to SD-WAN Fabric," and then click Apply.



Known issues

The following list contains known issues in SD-WAN Orchestrator 9.4.6.

Issue ID	Description
ID: 38519	Having a large number of staged appliances offline but not in maintenance mode can cause Orchestrator performance issues when saving new appliance deployments or making other changes to appliance configurations from Orchestrator.
ID: 30443	It is possible to experience slowness when upgrading SD-WAN Orchestrator to version 9.4.x and later. This has to do with the CentOS 7 operating system, which reached End of Life on July 1, 2024. SD-WAN Orchestrator users attempting to upgrade to version 9.4.x and later should not be installing or upgrading to new versions of CentOS. While some packages can be accessed via the CentOS vault repository, these should not be used for staying on CentOS 7 for longer than is required to migrate to a new server. Packages provided by the vault repository will no longer receive updates, which means that software installed from the vault repository will have unpatched security vulnerabilities and other defects. It is recommended that SD-WAN Orchestrator users migrate to Rocky Linux when possible.
ID: 27372	Current computation passthrough tunnel availability does not consider the IPSLA state and only uses tunnel state. When a passthrough tunnel's state is "up - ip sla disabled," it is treated as "Local Breakout Up" in availability computation, when it should be treated as "Local Breakout Down."
ID: 23170	After upgrading to version 9.2.2.40302, cross-connected INET tunnels may be deleted or rebuilt, which could lead to intermittent tunnel connectivity.



New Stats Collector required for some features

SD-WAN Orchestrator collects statistical data from appliances to monitor performance, network traffic, and appliance status. Before Orchestrator 9.1.0, the process of collecting, storing, and retrieving this data impacted performance due to the amount of data stored on and requested from the database.

To improve Orchestrator performance, Orchestrator 9.1.0 included a new method called the *Distributed Stats Collector*, which eliminated the use of Orchestrator resources for monitoring appliances. This new architecture helps scale networks with greater performance.

The Stats Collector feature collects statistics from appliances and provides the information to Orchestrator. When enabled, the new Distributed Stats Collector runs in parallel with the Legacy Stats Collector to collect the necessary historical statistical data. After collecting that data, legacy stats collection can be discontinued.

Note

You will not experience performance improvement until you discontinue legacy stats collection.

It is recommended that you confirm the new Distributed Stats Collector is collecting historical data before you disable the Legacy Stats Collector by doing the following:

1. In Orchestrator, navigate to **Support > Technical Assistance > Partition Management**.
2. Verify the inserted rows and sizes of the Stats Collector's table partitions.

If you are running ECOS 9.1.0.0 or later and Orchestrator 9.1.0 or later, HPE Aruba Networking recommends that you set up the new Stats Collector so that you can take advantage of new stats introduced in future releases. Some new features introduced after ECOS 9.1.0.0 that require the new Stats Collector include:

- KPI Availability (ECOS 9.3.0.0)
- IP SLA Summary (ECOS 9.3.0.0)
- Internet Breakout (ECOS 9.3.0.0)
- Application Summary (ECOS 9.3.0.0)
- Application Trends (ECOS 9.3.0.0)
- User Trends/Bandwidth (ECOS 9.3.0.0)
- AppExpress (ECOS 9.4.1.0)

Important

Reporting and monitoring functions in AppExpress will not work properly unless Stats Collector is enabled.

To enable New Stats Collection on a self-hosted Orchestrator (on-prem), navigate to **Orchestrator > Software & Setup > Setup > Stats Collector Configuration**. To enable New Stats Collection on an Orchestrator as a Service (Cloud Orchestrator managed by HPE Aruba Networking), contact Technical Support, as this can only be done through HPE DevOps.



Additional information

This section provides additional information including historical features and fixes included in the release, installation and upgrade details, CLI-only features, ports used by SD-WAN Orchestrator, and configuration best practices.

Installation and upgrade

SD-WAN Orchestrator supports only HPE Aruba Networking appliances running ECOS release 7.3.0 or higher. Refer to the [Orchestrator Installation and Upgrade Guide](#) for installation and upgrade procedures. SD-WAN Orchestrator's IP address, DNS, hostname, and NTP must be configured via CLI. Refer to the [Orchestrator Installation and Upgrade Guide](#) for more information about configuring these items.

Upgrade path

Currently, all SD-WAN Orchestrator releases from 9.0.0 and later support a direct upgrade to version 9.4.6.

Notes

- Every 100GB of data will take approximately 4-6 hours to migrate. For example, 800GB of data will require approximately 32-48 hours of migration time.
- Statistics migration is a background activity that will not disrupt normal operations. SD-WAN Orchestrator will collect new statistics throughout the migration period.

Upgrade procedure

1. Acquire the SD-WAN Orchestrator installation image from the HPE Aruba Networking support site (the image name is Orchestrator 9.4.6.40044.gip).
2. Refer to the [Orchestrator Installation and Upgrade Guide](#) for details about the SD-WAN Orchestrator upgrade procedure.

Initial installation procedure

For detailed installation instructions, refer to the [Orchestrator Installation and Upgrade Guide](#).

Recover from a failed SD-WAN Orchestrator upgrade

Option A: Restore the previous version of SD-WAN Orchestrator

Important

You can only restore SD-WAN Orchestrator with a backup taken from the same release. Do not attempt to restore SD-WAN Orchestrator with a backup from any other release.

Restoring the previous version must be performed manually from the SD-WAN Orchestrator CLI, as follows:

1. Copy the SD-WAN Orchestrator backup file from your backup server to the /home/gms directory on your SD-WAN Orchestrator server, and name it **gms.zip**.
2. SSH into SD-WAN Orchestrator as the admin user and do the following:

```
$ su
```

```
Password: <root user password>
```

```
# service gms stop
```

```
# cd /home/gms
```

```
# readlink gms
```

```
gms.99.99.99.34368
```

```
# ls -d gms.*
```

```
gms.7.3.10.29906/   gms.8.3.0.34387/   gms.99.99.99.34368/
```



```
# unlink gms
# ln -s <previous version> gms
# chown -R gms.gms gms
# setcap cap_net_bind_service=+ep /home/gms/gms/java/bin/java
# exit
$ /home/gms/gms/setup/restore.sh 2>&1 | tee /tmp/restorelog
$ su
Password: <root user password>
# service gms start
```

If your SD-WAN Orchestrator still does not start, contact the HPE Aruba Networking Support team for assistance.

Option B: Proceed with the upgraded SD-WAN Orchestrator version

If you want to continue upgrading following a failed upgrade, contact the HPE Aruba Networking Support team for assistance.

Features only available through SD-WAN Orchestrator CLI

Certain SD-WAN Orchestrator operations can only be performed through SD-WAN Orchestrator CLI. There are no new CLI capabilities introduced in this release.

Feature	Comments
Changing IP Address, hostname, DNS Server, Time zone, NTP Servers of SD-WAN Orchestrator	For more information about these items, refer to the Orchestrator Installation and Upgrade Guide .
Upgrade SD-WAN Orchestrator	<p>If you are already using SD-WAN Orchestrator 9.0.0 or later and want to upgrade to a newer version, refer to the Orchestrator Installation and Upgrade Guide.</p> <p>Warning</p> <p>A failed upgrade can result in SD-WAN Orchestrator being in a corrupt state. Ensure that you back up SD-WAN Orchestrator before you start the upgrade process.</p> <p>Note</p> <p>The upgrade process can take several hours to complete. Run the below command as admin via SSH to check if the SD-WAN Orchestrator upgrade is in progress:</p> <pre>ps ax grep "install_orchestrator"</pre> <p>If you see any output, the SD-WAN Orchestrator upgrade is still in progress.</p>



Feature	Comments
Restore SD-WAN Orchestrator from Backup	<p>This must be performed manually from SD-WAN Orchestrator SSH CLI, as follows:</p> <ol style="list-style-type: none"> 1. Copy the SD-WAN Orchestrator backup file from your backup server to the /home/gms directory of the new SD-WAN Orchestrator server and rename it gms.zip. 2. SSH into SD-WAN Orchestrator as admin and do the following: <ol style="list-style-type: none"> a. If you are running release 9.4.x or later, enter: <pre>whoami</pre> <p>If it is not gms, enter the following, and then provide the password:</p> <pre>sudo su - gms</pre> b. Switch to the root user and stop the Orchestrator service: <pre>\$ su</pre> <pre>\$ service gms stop</pre> c. Log out of root and run the restore script: <pre># exit</pre> <pre>\$ /home/gms/gms/setup/restore.sh 2>&1 tee /tmp/restorelog</pre> d. Switch to the root user and start the Orchestrator service: <pre>\$ su</pre> <pre># service gms start</pre>

Security Updates	<p>For SD-WAN Orchestrators that are running on Fedora core Linux 23 and above, refer to the Orchestrator Installation and Upgrade Guide for information about updating security patches.</p> <p>Important</p> <p>Back up SD-WAN Orchestrator before applying any patches. If a kernel or library update corrupts the OS, restore SD-WAN Orchestrator from the backup. Some updates may require a machine reboot. Run the following command as root to see if the update requires a reboot:</p> <pre># dnf needs-restarting</pre>
------------------	---

Reset IP Whitelist	<p>SSH into SD-WAN Orchestrator as admin and run the resetWhitelist script to remove IP addresses configured in Whitelist:</p> <pre>\$ home/gms/gms/resetWhitelist.sh</pre>
--------------------	---

Ports used by SD-WAN Orchestrator

The table below lists the ports used by SD-WAN Orchestrator. Ensure that these ports are not used by any other applications and that they are not blocked by a firewall.

Port	Protocol	Application
Outbound		
21	TCP	FTP ¹
22	TCP	SCP ¹
22	TCP	SSH
25	TCP	SMTP
49	TCP	TACACS+
80	TCP	HTTP



Port	Protocol	Application
443	TCP	HTTPS ²
465, 587	TCP	SMTPTS
53	TCP/UDP	DNS
123	UDP	NTP
514	UDP	Audit Log ³
514	UDP	Syslog ³
1812, 1813	UDP	RADIUS ⁴
Inbound		
22	TCP	SSH (optional)
80	TCP	HTTP ⁵ (optional)
443	TCP	HTTPS ⁵

- ¹ FTP and SCP are optional and used as backups to customer-owned servers in the on-prem version of SD-WAN Orchestrator. You can always use the HTTPS port, as it is already allowed. This is not applicable to Orchestrator-as-a-service.
- ² SD-WAN Orchestrator communicates with Cloud Portal over both HTTPS and WebSockets over TLS 1.2.
- ³ Audit log and Syslog ports are configurable.
- ⁴ These ports may differ. Verify the ports are the same as the server during configuration.
- ⁵ Inbound HTTP/HTTPS connections can be restricted to authorized subnets only. EdgeConnect SD-WAN talks on these ports.

Configuration best practices

- If possible, make all configurations to appliances from the SD-WAN Orchestrator, not on the appliances themselves since SD-WAN Orchestrator has a master/slave relationship with the appliances so future changes from SD-WAN Orchestrator can override appliance-made configurations.
- If SD-WAN Orchestrator is added to the network after the appliances have been configured, ensure all pre-existing template data or policy configurations applied to appliances manually are inserted into the SD-WAN Orchestrator templates before pushing out to the appliance.
 - All template-based configurations in SD-WAN Orchestrator will wipe the configurations on the affected appliances first before applying the new configuration.
 - In some cases, customers may have specific configurations already applied to an individual appliance that will be deleted if not added to the template. This is the design of the SD-WAN Orchestrator to ensure that cookie-cutter configurations are consistent across all appliances in an SD-WAN Orchestrator group or managed appliance.
 - If no configuration change is detected, SD-WAN Orchestrator will not make any changes to the appliance configuration.



New features and enhancements from past releases

The following table describes new features and enhancements that have been made in SD-WAN Orchestrator since the original version 9 release.

Feature	Description	Baseline Release
Availability KPI enhancements	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.	9.4.5
Cipher Settings	Cipher Profile settings allow you to restrict the use of certain ciphers for the Orchestrator services that use cryptography, including TLS, Tunnels, SSH, Certificates, SNMP, NTP, and Clusters. This feature set helps meet CSfC standards for data classification and protection.	9.4.5
RMA Wizard enhancements	The RMA Wizard was updated with several improvements, including support for interface mapping on ECOS appliances. This mapping allows an appliance to be replaced with another appliance of a different but equivalent model, configured with different interface count, interface names, and port types.	9.4.5
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
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.	9.4.3
Axis API integration	Connectivity between EdgeConnect appliances and Aruba SSE (Axis Security) is now automated to provide easy, reliable access to cloud-based security services offered by Axis Security. The integration provides faster Orchestration to prevent API bottlenecking, eliminates the need to configure complicated SSE policy manually, and fully automates sublocations based on label, zone, IP range, or address group.	9.4.3
EC-10106/10108 Enhancements	This release contains several enhancements to the UI for the EC-10106 and EC-10108 appliances, including a new PoE filter on the Interfaces tab and support for combo ports in the Type field of the Interfaces table.	9.4.2
Context-Sensitive Clickthrough to Zscaler UXI Portal	Users now have direct browser access to the Zscaler Digital Experience (ZDX) monitoring service through a popout URL on the Zscaler Internet Access tab or in the appliance tree.	9.4.2
Fast Orchestrator WebSocket Failover	With this release, discovery of communication failures and redirection of traffic from direct WebSocket to Portal WebSocket occur in greatly reduced times. You can choose to configure this feature to run in Aggressive, Normal, or Slow mode.	9.4.2
Debugging	This release introduces a "Debug" icon that, when clicked, opens a dialog containing debugging information for a particular feature.	9.4.1
IP Anonymization	Orchestrator can now mask the IP addresses exported in logs so that anyone reading the logs cannot view the full IP addresses. The operator can set the mask length to the values of 0, 8, 16, or 24, with 24 as the default mask length.	9.4.1



Feature	Description	Baseline Release
VXLAN and BGP EVPN Routing Support	Through the Orchestrator UI, you can now specify VXLAN settings for routing segments configured on Aruba CX switches or EdgeConnect appliances. When a VNI is configured for a segment or in a template, the 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
Role-to-ID Mapping	You can now define and map roles that are used throughout the SD-WAN Fabric. For example, you can map a role to Group Policy Identifiers (GPIDs) from Aruba CX Switches to facilitate identity awareness between Aruba Orchestrator and Aruba CX Switches.	9.4.1
Public Key Infrastructure	Previously, Orchestrator web server required importing a CA-signed end entity certificate and a private key, which were both generated externally. In addition, IKE-based IPsec tunnels only supported pre-shared keys for peer authentication. With this release, end entity certificate support includes internally creating a Certificate Signing Request (CSR), generation of public/private key pairs, and using the signed end-entity certificate for Orchestrator web server.	9.4.1
Tiered Subscription Licensing	Aruba Orchestrator now shows AAS licensing type and feature usage (Licensed vs Configured) information, generates AAS licensing-specific alarms and notifications, and allows users to configure features based on the network's AAS license type.	9.4.1
Firewall UI Enhancements	This release includes support for ICMP codes and IPV4/IPV6 options on firewalls in the Service Groups UI.	9.4.1
AppExpress	This feature allows you to monitor the traffic flow for up to 50 applications and leverage synthetic polling and real-time user traffic observations to intelligently steer traffic. AppExpress automatically selects the best path for each of the 50 applications and works for internal and cloud-based applications.	9.4.1
IPsec Tunnel Debugging Enhancements	More informational and additional fields have been added to the Tunnel Troubleshooting dialog box for IPsec UDP tunnels, standard IPsec fabric tunnels, and third-party IPsec passthrough tunnels.	9.4.1
X.509 Certificates	This release includes support for X.509 certificates, including the ability to generate X.509 certificates upon request, parameters to enforce security settings, and audit log generation for certificate validation.	9.4.1
Orchestrator High Availability	Orchestrator High Availability minimizes interruptions to Orchestrator functionality by enabling you to fail over from a primary Orchestrator to a backup (stand-by) Orchestrator.	9.4.1
Secure NTP Authentication on Self-Hosted Orchestrator	Starting in 9.4.x, self-hosted Orchestrators support secure NTP authentication. This fulfills a Common Criteria requirement. Secure NTP authentication only works on an Orchestrator running on Rocky Linux OS. Starting from 9.4.x+ releases, Orchestrator deployment packages are shipped with Rocky Linux. Secure NTP authentication will also work on Orchestrator 9.1.9+, 9.2.10+, and 9.3.3+ on-prem deployments that have been migrated to Rocky Linux.	9.4.1
Pre-Config for IDS/IPS	Users can now apply pre-configurations for IDS/IPS settings in Orchestrator.	9.3.1
All Advanced Security Settings Selected for New Installations	By default, all settings on the Advanced Security Setting dialog box are now selected for new Orchestrator installations. Upgrades retain previous settings.	9.3.1
Dark Mode	Orchestrator provides a new dark theme. You can toggle between light and dark themes by clicking the theme icon in the upper-right corner of the Orchestrator UI.	9.3.1



Feature	Description	Baseline Release
Regional Loopback Orchestration	In Loopback Orchestration, you can now associate a configured region with a loopback interface and change the loopback pool subnet IP for a loopback interface. Using the new reclaim feature, you can also return deleted loopback IP addresses to their original pools so they can be used again.	9.3.1
Business Intent Overlays	You can now set a Session Affinity Timeout for local breakout flows, and there is now a Fixed Order option for ranking links when using Waterfall for Link Selection.	9.3.1
Rest API for RBAC Filter	The REST API now includes RBAC functionality that was previously only available through the Orchestrator UI.	9.3.1
Web UI Enhancements	This release contains improvements to the web user interface (UI), including additional filters on the Profiles page to help with saving, deleting, and editing profiles, as well as updates to support per-VRF DHCP relay and DHCP servers.	9.3.0
IDS/IPS Feature Enhancements	A new Bulk Edit Filtered Rules feature can apply actions to multiple selected IDS/IPS rules. You can now immediately update signatures on appliances or schedule updates to occur when convenient for your organization. The IDS/IPS tab now displays a history of signature versions. You can now create and manage signature profiles you can use to configure rules downloaded from the signature set on Cloud Portal. Orchestrator provides a Default signature profile with default rule settings.	9.3.0
DoS Threshold Management	You can now manage DoS threshold settings at a more granular level, including setting custom thresholds, response actions, and alarms.	9.3.0
Secondary Interfaces for Zscaler Orchestration	Previously, you could select WAN interfaces as primary and backup interfaces for Zscaler internet traffic. You can now specify secondary interfaces as well.	9.3.0
Audit Log Template Comments	The most recent audit log comment (if applicable) now appears at the top of the template group.	9.3.0
Netskope Orchestration	Netskope Orchestration automates the integration of Netskope by creating and deploying IPSec tunnels and IP SLA probes and managing the lifecycle of tunnels and probes.	9.3.0
Updated Orchestrator Help to Improve Usability	Orchestrator help topics now display in a browser window separate from the Orchestrator browser window, allowing you to view the help and Orchestrator application side-by-side. You can also access other help topics from this window's navigation pane.	9.3.0
VRPv3	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
New API Routes for Live Stats	New API routes were added to enhance live stat collection.	9.3.0
Improved BGP Functionality	Numerous improvements were made to BGP capabilities in Orchestrator, including the ability to use IPv6 addresses in BGP peer dialogs, append multiple communities in the route-map rule for a BGP peer, and set new loop detection/loop interval parameters for BGP and OSPF.	9.3.0
Internet Breakout Trends	Orchestrator now shows trends for certain data about internet breakout links, such as latency, loss, and jitter. Metrics are displayed in a separate chart for each overlay.	9.3.0



Feature	Description	Baseline Release
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
Secondary Accounts	Orchestrator now supports multiple license end dates for a single Orchestrator using secondary accounts.	9.3.0
Identity-Based Traffic Management	Orchestrator now supports Aruba identity-based traffic management (IBTM). IBTM enables dynamically assigning SD-WAN traffic management policies based on identity match criteria such Role Based Access Control (RBAC) username, user-role, user group, user-mac address, device type and identity context awareness from other sources. For more information, see Aruba SD-WAN Identity-Based Traffic Management User Guide (PDF) .	9.3.0
Branch NAT No-Translate Rules	The restriction of overlapping a translated source/destination subnet with a source/destination subnet has been removed.	9.2.4
Enhanced Logging for Templates, Template Groups, and Routing Segmentation (VRF) Firewall Zone Policies	<p>Users can add Audit Log Comments to track new or modified templates, template groups, and routing segmentation (VRF) firewall zone policies. Templates are also tracked with a time and date stamp and a user ID. Template groups are tracked with a time and date stamp.</p> <p>NOTES</p> <p>The time stamp shown for a template group considers the most recent one among all template timestamps, regardless of whether it is selected. Because users can modify a template and deselect it from active templates, the modification will reflect on the template group.</p> <p>An update to the template modification timestamp is reflected in the template group modification timestamp. In these cases, the username is not shown in the template details on the right-side panel of the UI. Note that sometimes the system updates template policies independently—for example, the SaaS Optimization template is updated periodically when application definitions data is updated from the portal.</p>	9.2.1
Enhanced Packet Capture Filtering and Option to Enable Circular Storage	Orchestrator allows you to capture packets for selected appliances and configure the host, IP, or port to capture, add filter options, and enable circular storage.	9.2.1
New Log Settings Option to Include WAN-Side Stateful Drops	Users can configure Log Settings to include WAN-side stateful drops.	9.2.1
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
Multicast Group Filtering	Users can now allowlist multicast groups, so that EdgeOS processes only the groups matching the defined list.	9.2.0
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
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



Feature	Description	Baseline Release
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
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
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
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 Orchestrator 9.2.0. Full support will be provided in a future version.	9.2.0
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
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
One-Click Deployment on GCP	After creating a Google Cloud Platform account with required permissions for Orchestrator, users can now quickly deploy one or more new EdgeConnect Virtual (EC-V) appliances in GCP by providing some basic configuration and deployment details.	9.2.0
Configuration Limits for EC Appliances	Various configuration limits were defined for EC-model appliances.	9.2.0
Alarm Notification Table Optimization	This release includes scalability enhancements to alarm notification handling to support a larger number of appliances.	9.2.0
Performance Enhancements	This release adds a number of performance enhancements to significantly reduce orchestration times for most use cases.	9.2.0
Zscaler GRE Tunnel Automation	Orchestrator now supports GRE (in addition to IPsec) tunnel automation as the tunnel protocol for a specified WAN interface label. For more information, see the help content under Configuration > Cloud Services > Zscaler Internet Access.	9.1.3
Zscaler Supports Bandwidth Percentage in Gateway Options	In addition to bandwidth control options that use fixed amounts of bandwidth and inherit bandwidth values from parent locations, it is now possible to specify download/upload as percentages of the deployment WAN label's bandwidth. For more information, see the help content under Configuration > Cloud Services > Zscaler Internet Access.	9.1.3
Update Now Button Added to Application Definitions	An Update Now button now provides the ability to force an update of application definitions outside of automatic updates. For more information, see Configuration > Templates & Policies > Applications & SaaS > Application Definitions.	9.1.3



Feature	Description	Baseline Release
Orchestration Performance Enhancements	This release adds a number of performance enhancements to significantly reduce orchestration times for most use cases.	9.1.2
Orchestrator Supports Zscaler Appliance Association	Previously, associating an EdgeConnect appliance to Zscaler required configuration of business intent overlays. Now, it is possible to filter only required appliances and associate to Zscaler directly. For more information, see the help content under Configuration > Cloud Services > Zscaler Internet Access.	9.1.1
Aruba Central Integration	Orchestrator now allows integration of Aruba EdgeConnect devices in Aruba Central. Once integrated, EdgeConnect device alerts can be monitored in the Network Health tab in Aruba Central. For more information, see help content under Orchestrator > Aruba Central > Aruba Central Site Mapping.	9.1.1
Deploy Cloud Hubs in Azure	This release supports deployment of EC-Vs in the Azure cloud from Aruba Orchestrator. For more information, see help content under Configuration > Cloud Services > IaaS > Cloud Hubs in Azure.	9.1.1
End-to-End Encryption	This feature enables end-to-end encryption for all communication paths in the SD-WAN network, between Orchestrator and appliances and from Orchestrator to Cloud Portal to appliance websocket connections.	9.1.0
Intrusion Detection System (IDS)	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. For more information, see the help content under Configuration > Overlays & Security > Security > Intrusion Detection System (IDS).	9.1.0
Aruba ClearPass Policy Manager Integration	Orchestrator now supports association with ClearPass Policy Manager, which provides role-based and secure network access for devices. This integration provides user and role information for an IP address, which you can view on the Flows and Top Talkers tabs of Orchestrator. For more information, see the help content under Orchestrator > Aruba Central > ClearPass Policy Manager.	9.1.0
Remote Statistics Collection	To improve Orchestrator performance, this release includes a new remote stats collector feature that eliminates the use of Orchestrator resources for monitoring appliances. This new architecture allows you to scale your network with greater performance. For more information, see the help content under Orchestrator > Software & Setup > Setup > Stats Collector Configuration.	9.1.0
Support for ACL Group Objects	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. For more information, see the help content under Configuration > Templates & Policies > ACLs > Address Groups and Configuration > Templates & Policies > ACLs > Service Groups.	9.1.0
Support for Non-routing Hub (Stub Hub)	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. For more information, see the help content under Configuration > Overlays & Security > Hubs.	9.1.0
OSPF Template	This release of Orchestrator includes a new template for configuring OSPF. For more information, see the help content under Configuration > Templates & Policies > Templates > OSPF.	9.1.0



Feature	Description	Baseline Release
Separation of Active and Historical Alarms	This release separates active and historical alarms into different database tables. This update will help to address potential deadlock issues in the alarms database and provides support for displaying alarms in the user's own time zone. On the Alarms tab in Orchestrator, you can toggle the alarm view between Active, History, and All.	9.1.0
Zone Name in Routes Dialog	In this release, users can configure a firewall zone when configuring a user-defined route.	9.1.0
Improvements in Denied Devices List	Virtual appliances are no longer displayed on the Denied Devices list, and users now have the option to permanently delete one or more appliances from the list and from Orchestrator.	9.0.5
One-click Cloud EC-V	This feature enables users to quickly deploy one or more EdgeConnect Virtual (EC-V) appliances in supported public cloud providers. In this release, Silver Peak supports one-click EC-Vs in AWS. After creating an AWS Identity and Access Management (IAM) account with required permissions for Orchestrator and an EC2 key pair, users can quickly deploy one or more new EC-Vs by providing some basic configuration and deployment details.	9.0.5
Third-Party Service Orchestration	Service Orchestration automates the integration of third-party services without an API. Service Orchestration automates the creation and deployment of IPSec tunnels and IP SLA probes and manages the lifecycle of the tunnels and probes.	9.0.5
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 > Networking > Link Aggregation.	9.0.4
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).	9.0.4
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.	9.0.4
Configurable Confidence Value for Address Map Definitions	In this release, users can modify the Confidence value for Address Map application definitions under Configuration > Templates & Policies > Applications & SaaS > Application Definitions.	9.0.4
Custom CA Certificate Trust Store	Orchestrator's trust store can be customized by adding and deleting CA certificates under Configuration > Overlays & Security > Security > Custom CA Certificate Trust Store.	9.0.4
Route Map Enhancements	This release includes two changes to rules configuration for Route Redistribution Map templates: 1) Source protocol can be set to "ANY" under match criteria; 2) An OSPF tag can be specified for routes that are sent to the SD-WAN fabric. Both require appliance software 9.0.2.0 or higher.	9.0.3
UI Changes to Support Port Flexibility for Bonding	Updates to the UI now allow users to bond only LAN side interfaces. Previously, when enabling bonding, both LAN and WAN side interfaces were bonded (blan0 and bwan0).	9.0.3
Routes Template Enhancements	This release includes the following changes to the Routes template: 1) Use SD-WAN Fabric Learned Routes and Enable Equal Cost Multi Path (ECMP) can be enabled for all segments; 2) The Allow WAN to WAN routing option has been moved to the Miscellaneous section of the System template.	9.0.3



Feature	Description	Baseline Release
Multiple Ranges for DHCP Server	DHCP Settings now support adding multiple IP address ranges under the DHCP Server options.	9.0.3
Zone Orchestration for AWS TGNM and Azure	This release adds a Zone option to the AWS Network Manager and Microsoft Azure Virtual WAN tabs. Clicking the Zone button opens the Configure Zone dialog, which allows the user to select a zone to be assigned for the VTI interfaces created by these integrations.	9.0.3
Appliance CPU Usage Charts	A new tab containing appliance CPU usage charts can be found under Support > Reporting > Appliance CPU Usage. The page provides real time and historical views for combined CPU usage and individual CPUs for a single selected appliance. Realtime charts show the past five minutes and historical charts show the past few days. Historical charts are only updated when requested by the user.	9.0.3
Updates to BGP Template	In this release, the BGP template contains the following configuration fields. All fields are optional. Two global options are AS Path Propagate and Graceful restart. The following peer level configurations can be applied to all appliance peers: Next-Hop-Self, Keep Alive Timer, Hold Timer, and Enable MD5 Password.	9.0.3
Added Details for Cleared and Acknowledged Alarms	The following new columns are now included in the Alarms table under Monitoring > Summary > Alarms: Cleared By, Acked By, Acked Time, Comments to indicate whether an alarm was cleared/acknowledged by the system or a user. For user cleared alarms, the ID of the user is displayed. Additionally, when a user acknowledges an alarm, a comment dialog is displayed for providing optional details.	9.0.3
Peer-based Subnet Sharing Metric	The Peer Priority configuration has been enhanced to include an Advertise Metric that influences ingress traffic. The values let appliances decide how to receive traffic when a new session is initiated from the SD-WAN fabric to a local destination.	9.0.3
Increased Retention for New Daily Stats	Retention for the following hourly flow stats has been increased to three months: DNS, Flowapp, Top Talkers, Port, and Behavioral.	9.0.2
Advanced Segmentation (VRF)	Orchestrator 9.0 supports 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.	9.0.0
YAML Preconfig Support for Routing Segmentation	Added routing segmentation (VRF) support for all YAML preconfig modules.	9.0.0
YAML Preconfig Supports Custom Tags	YAML preconfig now supports the use of up to eight custom tags to be set on appliances.	9.0.0
Secure Shell Access	New options under Advanced Security Settings allow administrators to set secure shell access or disable shell access on one or more appliances. On a new Orchestrator, the default mode of operation will be secure shell access. In this mode, shell access requires a challenge-response from Silver Peak technical support. On an upgraded Orchestrator, shell access will still be enabled by default.	9.0.0
SAML 2.0 Integration	This Orchestrator release provides support for SAML 2.0 as a remote authentication method.	9.0.0
Live Troubleshooting for Down Tunnels	This release includes a dashboard for troubleshooting down tunnels, available by clicking on a tunnel down alarm in the Alarms tab.	9.0.0



Issues fixed from past releases

The following table describes issues fixed in past releases that are included in this release.

Issue	Earliest Release to Fix
ID: 39248. A discrepancy between values in the login and logout values in audit logs led to the same user being labeled as “admin” or “unknown,” depending on authentication success or failure.	9.4.5
ID: 38559. The appliance was sending non-binary bindings, resulting in inconsistent admin interface statuses across networks.	9.4.5
ID: 38451. An issue with the interface mapping functionality in the RMA wizard resulted in certain interface types displaying as different interface types after upgrade.	9.4.5
ID: 38235. Upon orchestrating GRE tunnels, Zscaler association became stuck in a pending state and failed to validate the Zscaler static IP.	9.4.5
ID: 38032. Upon Cloud Orchestrator upgrade, user-created inbound port forwarding rules were discarded because the peer appliance tried to update rules before the other appliance was yet to sync.	9.4.5
ID: 39506. The IPsec encryption algorithm’s “Auto” option for SD-WAN tunnels was removed, causing modifications to parameters in the Tunnel Settings tab that triggered an unplanned rebuild of IPsec tunnels.	9.4.4
ID: 38160. When upgrading from an Orchestrator version prior to 9.2, appliance subattribute values were null for user-defined Address Group applications, which generated the frequent error: argument “content” is null.	9.4.4
ID: 37834. When the gateway rule appliance was configured as “any” and Zscaler location or sublocation contained stale entries, the upgrader removed the entire rule instead of cleaning up stale entries.	9.4.4
ID: 37796. Daily tunnel availability aggregation was taking a long time to execute because certain query parameters were not optimized.	9.4.4
ID: 36709. If the LAN label provided for sublocations on the Zscaler Gateway Options tab was not configured in the appliance deployment, a missing condition check created an erroneous error log message for overlapping IP addresses. Note that this error is a false positive and does not impact orchestration.	9.4.4
ID: 36390. Inconsistency with whether zone IDs were classified as strings or numbers prevented the appliance Firewall Zone in WAN interfaces to display incorrectly on the Deployment tab of the web UI.	9.4.4
ID: 33461. An error in how partial hours were handled when pulled from user browser data resulted in an incorrect timestamp on the Dashboard Health map in the Orchestrator UI.	9.4.4
ID: 33363. Appliance priority failed to reset when the appliance was put in maintenance mode or in a bad status, which prevented Netskope orchestration for other appliances.	9.4.4
ID: 33182. The RBAC configuration was missing two GET and PUT entries in the REST API, which prevented IDS/IPS functionality from deploying properly in Orchestrator.	9.4.4
ID: 33180. When relay server information was saved using comma-separated values and a deployment profile was created with the “No DHCP” button selected, the Configuration Wizard threw an error and did not apply the deployment as expected.	9.4.4
ID: 33119. A validation issue in the /ValidateApplianceUpgrade API prevented super users from successfully approving discovered appliances.	9.4.4



Issue	Earliest Release to Fix
ID: 32216. If VPN Location, VPN Credential, Static IP Address, and GRE Tunnel settings were manually deleted from Zscaler portal, Zscaler orchestration failed with a "Resource not found" error until the stale entries removed from the Zscaler configuration table.	9.4.4
ID: 31703. An issue with the discard operation through the web UI can cause template group entries to be deleted if users click the "Discard" changes button when configuring template groups.	9.4.4
ID: 29343. Appliances running Zscaler Gateway disassociated from the Orchestrator, preventing users from editing rules in Orchestrator and Zscaler portal.	9.4.4
ID: 27304. An NPE issue in the appliance created an unexpected null value in the Orchestrator database rather than the expected Boolean value, creating a conversion error that prevented orchestration from running successfully.	9.4.4
ID: 22630. A missing configuration in the /getBatch API call prevented the Tunnel Bandwidth tab from loading properly.	9.4.4
ID: 38261. When Orchestrator DB RESOURCE_BASE /gmsRegistration CONFIG_DATA contained an internalManagementIP address not equal to the currently configured IP address on the Orchestrator interface list, Orchestrator randomly alternated between DB gmsRegistration RESOURCE_BASE CONFIG_DATA and the Orchestrator interface IP address, advertised in the Orchestrator reachability configuration applied to appliances. In environments where EdgeConnect appliance portal websocket connectivity was administratively prohibited, this led to appliance isolation from Orchestrator, preventing successful orchestration.	9.4.3
ID: 38245. The actionlog table could not process all of its entries and locked during the sysdump process, preventing sysdump from completing successfully.	9.4.3
ID: 37966. A change in API response format prevented the Orchestrator UI from properly rendering information in the Licenses Used/Avail column of the License Report tab.	9.4.3
ID: 37603. An issue in the web UI prevented some route policy types from being displayed properly in the Route Policies drop-down menu.	9.4.3
ID: 37386. A data type mismatch in interface and interface overlay stats between the appliance and the stats collector database table prevented users from viewing stats.	9.4.3
ID: 37200. When using Branch NAT for many-to-one IP SNAT, a validation error mishandled the "translateNatPoolID" parameter, barring it from the preconfiguration and preventing successful use of Branch NAT.	9.4.3
ID: 36993. A mismatch in expected versus actual parameters in the Delete Endpoint Exception API request caused the request to fail.	9.4.3
ID: 36785. A permissions issue prevented an RBAC user from accessing the addMultiple and deleteMultiple requests in the passthrough API.	9.4.3
ID: 36686. When unreachable HA appliances were removed and then re-onboarded, the legacy HA configuration caused the Appliance Wizard to open, displaying incorrect settings.	9.4.3
ID: 36675. An inefficiency in how the userScreening API call ran through the portal caused a 5-20 second delay in two-factor authentication login on the Cloud Orchestrator.	9.4.3
ID: 36674. Attempting to back up Stats Collector using SCP in an environment where the SFTP subsystem was not enabled prevented the backup job from completing successfully.	9.4.3



Issue	Earliest Release to Fix
ID: 36537. A misconfiguration in KPI settings prevented users from creating multiple reports from the Schedule & Run Reports tab of the Orchestrator UI.	9.4.3
ID: 36452. A missing API endpoint related to RBAC prevented credentialed users from accessing the Licenses tab in the Orchestrator UI.	9.4.3
ID: 36426. An error in the appliance version check code prevented preconfiguration from completing successfully during deployment.	9.4.3
ID: 36330. A lock in the encryption function caused Orchestrator experience slowness when pushing the User Management template.	9.4.3
ID: 36328. An issue on the Interface Labels tab erroneously allowed users to overwrite an interface label that was being used, putting the Orchestrator into an inconsistent state and causing performance issues.	9.4.3
ID: 36258. A connection management issue related to max timeout wait time caused the appliance to enter a pending state for an extended period of time.	9.4.3
ID: 36247. A restriction in validation logic allowed values of only 0 and 1 to be used for TLAN and WLAN interfaces.	9.4.3
ID: 34600. A missing API endpoint related to RBAC prevented credentialed users from modifying configurations on the System Information tab in the Orchestrator UI.	9.4.3
ID: 34402. A newly added property in the HTTPS Certificate template did not properly map to older versions of the template, causing the template to fail when pushed to the new Orchestrator.	9.4.3
ID: 34287. An issue with how SQL query generation logic handled the interfaceName parameter when it was left blank prevented the Distributed Stats Collector from successfully completing /interface API calls.	9.4.3
ID: 33813. Browser incompatibility with self-closing HTML tags prevented Orchestrator's Schedule & Run Reports tab from listing appliance reports that could be scheduled.	9.4.3
ID: 33677. An issue with the request manager caused Orchestrator to display duplicate or triplicate entries in the Deployment Report and Loopback Interfaces tabs.	9.4.3
ID: 33676. Fetching Orchestrator license data from Cloud Portal instead of the license cache created slow loading and other performance issues on the Licenses tab.	9.4.3
ID: 33675. Running Deployment tab API calls through Cloud Portal instead of cached information caused slow loading and other performance issues when using the Deployment Wizard.	9.4.3
ID: 33673. POST body data from performing configuration changes was not shown in audit logs.	9.4.3
ID: 33466. An issue with the year-based wrapping logic in the /systemInfo API endpoint resulted in inconsistent system information being displayed on the UI's System Information tab and the CLI.	9.4.3
ID: 33391. Orchestrator was waiting for end-to-end encryption to complete before applying preconfiguration files, slowing appliance performance during the onboarding process.	9.4.3
ID: 33279. A special character validation check in Orchestrator server prevented upload of Address Groups via bulk import.	9.4.3



Issue	Earliest Release to Fix
ID: 33106. A triggered alarm erroneously claimed that two EdgeHA peer appliances were configured to the same metered account even when they were configured to different metered accounts.	9.4.3
ID: 32222. The maximum number of connections allowed to Cloud Portal from the Orchestrator was set too low and the proxied calls from the appliances were not rate-limited, leading to suboptimal performance for API requests.	9.4.3
ID: 31784. A previous UI fix introduced an issue where the background color of the UI header changed from gray to white, making the text unreadable.	9.4.3
ID: 31729. Lack of a horizontal scroll bar on the Segment (VRF) Firewall Zone Policies table made the page unreadable in the UI.	9.4.3
ID: 31678. Invalid subattribute data triggered an alarm for AVC attributes file-handling even after that alarm had been disabled in the web UI.	9.4.3
ID: 31671. A configuration error in the custom time range on the Alarms tab prevented getting accurate data when the range was configured for the previous day.	9.4.3
ID: 31642. The end-user license agreement (EULA) in OaaS deployments was unclear that the Aruba EULA was governed by the HPE EULA.	9.4.3
ID: 31570. On the Application Groups tab, attempting to edit or create a new Application Group before information on the existing groups was loaded could erase all existing Application Groups.	9.4.3
ID: 31286. A configuration issue caused AVC data to be deleted erroneously, preventing users from creating application groups.	9.4.3
ID: 31135. Because of an issue with how encryption keys are stored, SMTP encryption and decryption for Cloud OaaS is not functioning properly in version 9.4.2 and later. This issue will be addressed in an upcoming release.	9.4.3
ID: 31130. Because the VRF-aware /subnets/all API route was missing in the API documentation, VRF segment routes were not being advertised in API calls.	9.4.3
ID: 31013. An unexpected rest request while fetching results from MySQL queries returned empty responses for some values, leading to different results in Application Summary reports run with the same parameters.	9.4.3
ID: 31006. An API misconfiguration allowed read-only users to make changes to signature profiles.	9.4.3
ID: 30972. Using Orchestrator as a proxy for appliance APIs consumed appliance resources and resulted in OaaS inaccessibility and intermittent 502 gateway errors.	9.4.3
ID: 30963. The request body of the Upgrade Appliance API call was being erroneously checked by the RBAC filter, preventing the upgrade from completing successfully.	9.4.3
ID: 30413. Orchestrator used the incorrect REST API to update BGP peers, causing manually created BGP peers to be deleted erroneously.	9.4.3
ID: 30360. The request body of the RMA wizard API call was being checked by the RBAC filter, preventing the RMA wizard from running properly.	9.4.3
ID: 30306. Header row records were appearing at the end of API response arrays instead of the beginning.	9.4.3



Issue	Earliest Release to Fix
ID: 30175. A missing null pointer exception in the preconfiguration for EdgeHA caused EdgeHA deployment to fail.	9.4.3
ID: 30097. The Orchestrator UI was fetching data in the Deployment tab from the appliance by default, not showing a loading bar, and displaying all the data at once, leading to slowness in the UI on large networks.	9.4.3
ID: 30037. A misconfiguration in RBAC mapping prevented read-only users from successfully loading the System Information page.	9.4.3
ID: 29853. Orchestrator was updating template group association timestamps before database updates had finished, resulting in the Template Shaper not applying the updates to all devices.	9.4.3
ID: 29851. A URL used by the Orchestrator UI was not updated with the correct RBAC predefined permission map for DNAT exceptions, leaving authorized users unable to modify configurations on the Inter-Segment Routing & DNAT Exceptions tab.	9.4.3
ID: 29833. A check performed on revoked licenses incorrectly parsed a null value, preventing the successful upload of license files on the Air-Gap tab.	9.4.3
ID: 29466. Upon upgrade from Orchestrator 9.2.3_40156 to 9.3.2.40150, non-hub appliances were added as hub appliances.	9.4.3
ID: 29374. Invalid query parameter prevented updates to GCP account.	9.4.3
ID: 29275. Added new query parameter to support the Netskope API "exact" sourceidentity enhancement.	9.4.3
ID: 29164. New HA pair creation continually failed due to a previous HA pair creation that failed in a previous Orchestrator release.	9.4.3
ID: 29091. Missing null checks in the appliance access group during apiKey permission checks created a null pointer exception that returned an error in the Orchestrator UI.	9.4.3
ID: 29088. Spaces were accepted in the configuration file for API calls, resulting in a 401 error being thrown when the API calls were run.	9.4.3
ID: 28993. Address Map selection was not available in Application Definitions.	9.4.3
ID: 28959. A UI issue in the Upload to Support feature caused the Monitor Transfer Progress dialog box to appear with a continuously rotating loading indicator.	9.4.3
ID: 28916. An issue with auto-updating cloud portal configurations caused classification data alarms to appear erroneously in the Orchestrator UI.	9.4.3
ID: 28330. A third-party library referenced in the .pom file was incompatible with the version of metrics-core running, making the Cloud Orchestrator unreachable.	9.4.3
ID: 28329. An issue with API efficiency caused a delay in reflecting successful EdgeHA deployment in the Orchestrator appliance tree.	9.4.3
ID: 28320. Orchestrator file upload was not working as expected when legacy API support was enabled.	9.4.3
ID: 28264. A validation error prevented login error to the Orchestrator UI via a protocol-agnostic valid URL without a protocol string ("http://" or "https://").	9.4.3



Issue	Earliest Release to Fix
ID: 28205. When the time period for collecting data was set to 1 day, Orchestrator response time was slow.	9.4.3
ID: 28192. The inbound port forwarding pre-configuration file could not convert configured interface labels to the correct IP.	9.4.3
ID: 27925. Attempting to log in to Orchestrator using non-ASCII characters prevented appliance upgrades from completing successfully.	9.4.3
ID: 27830. Inter-segment DNAT rules were executing add actions even if the previous delete actions had failed, causing segmentation errors that led to tunnel dropping unexpectedly.	9.4.3
ID: 27773. Portal data downloaded for IP intelligence and backups were in conflict, leading to backups not being created as expected.	9.4.3
ID: 27772. Because the cipher list for SFTP/SCP was hardcoded, users could not use or restrict ciphers on the appliance.	9.4.3
ID: 27361. Data in the UI was being aggregated by service type rather than by service and interface type, resulting in errors in Overlay-Interface-Transport graphs.	9.4.3
ID: 27326. Because the two functions queried different databases and used different tunnelid metrics, the statistics displayed in the Loss > Trends and Loss > Summary tabs did not match.	9.4.3
ID: 25544. An information handling error in JavaScript created an issue where filtering by subnet for 0.0.0.0/0 did not filter the default route and the table row count increased erroneously.	9.4.3
ID: 25119. Overlapping IP ranges for a single sublocation resulted in silent failure of the Zscaler API.	9.4.3
ID: 24086. IP Allow List instructions in the UI were incorrect for Orchestrator-as-a-Service deployments.	9.4.3
ID: 23664. APIs for /stats/aggregate/ and /stats/timeseries/ queried tables that no longer existed post-upgrade, throwing a 500 Error (internal server error) and preventing a proper response.	9.4.3
ID: 31902. The syslog proxy service was continuing to run even when there was missing or incorrect information in the configuration, resulting in the root partition logs filling with errors.	9.4.2
ID: 31835. A defect in the cryptographic library updated for Orchestrator 9.4.x could lead to the generation of corrupted cryptographic key material, causing functions reliant on encryption and decryption to fail unexpectedly.	9.4.2
ID: 31524. An error in the path for the reachability API prevented Orchestrator from returning the cached reachability status for appliance portal reachability calls.	9.4.2
ID: 28963. A previous improvement made to the file upload process created an issue that prevented Update Signature IDS/IPS from running successfully.	9.4.2
ID: 27640. Custom logic in the Loss tunnel JavaScript file overrode column names when exporting data to a .csv file.	9.4.2
ID: 27569. An exception handling issue between the appliance and the Cloud Portal prevented pre-configuration from loading successfully.	9.4.2
ID: 27549. When passing an appliance URL containing query parameters through the REST API, the path and query parameters were not separated when creating the appliance URI.	9.4.2



Issue	Earliest Release to Fix
ID: 27538. An issue with the value fetched during the appliance reachability check resulted in pre-configuration not completing during auto-discovery.	9.4.2
ID: 27505. A missing field in the request body for the /users/resetPassword API route prevented users from completing the password reset process successfully.	9.4.2
ID: 27364. A mapping issue prevented a SuperAdmin user from deleting a template group via the UI, though it could be deleted via API.	9.4.2
ID: 27358. An issue in the UI prevented purging the stats table in Orchestrator.	9.4.2
ID: 27315. A data validation error caused orchestration issues when pushing orchestrated inter-segment DNAT rules.	9.4.2
ID: 27224. An error in the remote auth API added whitespace between items in authorizationScopes, causing configuration issues.	9.4.2
ID: 27208. A null pointer exception was causing the IP allow list to block source IPs when IPv6 was added to the allow list.	9.4.2
ID: 27136. A third-party app that created and deleted additional partitions raised alarms which the Orchestrator was unable to clear.	9.4.2
ID: 27113. A prototype pollution vulnerability created the possibility for remote code execution or a denial-of-service attack.	9.4.2
ID: 27098. Java plugins were erroneously reporting security vulnerabilities from previous versions that no longer existed in the current version.	9.4.2
ID: 27035. When attempting to upgrade the appliance from the Discovered Appliances page, download using portal FQDN could not complete if the resolved portal IP and the IP resolved in SAMAP policy were different.	9.4.2
ID: 26996. An issue in certain POST API functions presented an "insufficient privileges" error to users trying to make changes using the SuperAdmin role.	9.4.2
ID: 26951. Passthrough APIs had duplicate Accept-Encoding headers, and certain APIs were missing from the passthrough API hashmap, creating compatibility issues between appliances.	9.4.2
ID: 26917. The /applicationTrends API was not returning application statistics as expected for versions of the appliance later than 8.1.6.x.	9.4.2
ID: 26906. A validation error in the API allowed rules with invalid VRF and Zone ID to be pushed to the Orchestrator. The erroneous rules could not be deleted via the UI.	9.4.2
ID: 26882. An issue with converting and sorting integer strings caused Orchestrator to delete the latest Stats Collector backup after reaching the "Max backups to retain" threshold.	9.4.2
ID: 26850. The Service Orchestration - Remote Endpoint Configuration tab was not properly validating certain special characters.	9.4.2
ID: 26717. A configuration issue prevented Cloud Orchestrator from retrieving or displaying portal licenses.	9.4.2



Issue	Earliest Release to Fix
ID: 26683. This release was patched to address CVE-2021-38153.	9.4.2
ID: 26677. License information was not available on the Deployment tab.	9.4.2
ID: 26656. A validation issue in a pre-config setting prevented the appliance from being properly onboarded.	9.4.2
ID: 26623. The query parameter groupByNe was improperly passed to the DAO layer, resulting in a query that failed to pull all appliance stats.	9.4.2
ID: 26524. In Orchestrator 9.3.0, you cannot back up Stats Collector to an HTTP server.	9.4.2
ID: 26523. Proper data validation for an empty data set was not occurring for the /config/maps POST request, which caused the appliance to save empty data.	9.4.2
ID: 26426. Missing subattribute parameters in the Address Map API triggered AVC alarms in Orchestrator.	9.4.2
ID: 26331. A validation issue prevented the appliance from deploying in certain new AWS regions.	9.4.2
ID: 25684. Certain UI functions truncated y-axis values in the Loss Trends chart, resulting in usability issues.	9.4.2
ID: 25541. When configuring SAML authentication, the Remote Authentication Server dialog box did not retain the X.509 certificate each time the dialog box was opened.	9.4.2
ID: 26662. Upon upgrade, some IP addresses were not properly whitelisted, preventing successful login to Orchestrator.	9.4.1
ID: 26511. In the deployment UI, the DHCP lease timer could only be configured in hours instead of seconds.	9.4.1
ID: 25759. Changes to and additions of address groups were not captured in audit logs.	9.4.1
ID: 25734. In the Modify User dialog box, the Phone field did not accept international formats.	9.4.1
ID: 25575. The DNS Proxy template did not accept "loopback" as an interface label.	9.4.1
ID: 25574. An issue with order of operations and match criteria during search resulted in some searches not producing the expected or most relevant results.	9.4.1
ID: 25431. During SMTP server settings configuration, when the Enable Authentication check box was not selected and an SMTP User was not provided, the UI generated an error message indicating that the SMTP User cannot be empty.	9.4.1
ID: 25154. A soft reset of the appliance could not be performed when the Soft Reconfiguration feature was enabled.	9.4.1
ID: 24804. Users were unable to populate the custom CA certificate store with certificates from the AVC dataset.	9.4.1
ID: 24193. Upon upgrade, a configuration issue caused stats collection to lag on some appliances.	9.4.1
ID: 24004. The POST /routes/preferredRoute API function was running a route query instead of making changes, which was potentially misleading for users.	9.4.1



Issue	Earliest Release to Fix
ID: 22997. If Legacy Stats Collector was discontinued and Advanced Stats Collector was enabled, API calls from the Orchestrator UI were unable to fetch data related to the Domains tab.	9.4.1
ID: 26612. The Refresh button on the Modify User dialog did not generate an MFA QR code.	9.3.1
ID: 26303. An API call using the groupByNe parameter returned unexpected results.	9.3.1
ID: 26274. When a zone name was modified in Orchestrator, a discrepancy between zone map data and config tables prevented the edited zone name from being applied.	9.3.1
ID: 25680. A SAML authentication issue prevented successful SSO login to Orchestrator.	9.3.1
ID: 25553. A key rotation issue led to an incorrect Key Material Activation Time on the Orchestrator.	9.3.1
ID: 25501. When upload of the backup config file from Orchestrator to the SFTP server failed, the local backup file created inside the home directory was not deleted properly, resulting in increased disk utilization.	9.3.1
ID: 25421. A validation issue in Cloud Portal resulted in the Orchestrator's IP being blocked and the export check failing unexpectedly.	9.3.1
ID: 25377. An issue with scrolling in the web UI caused certain UI elements to not appear as expected on screen.	9.3.1
ID: 25161. Route redistribution map templates set to merge unexpectedly deleted locally configured route maps.	9.3.1
ID: 25005. A validation issue in the SAML Remote Authentication Server created the potential for a cross-site scripting vulnerability.	9.3.1
ID: 25004. A validation issue on the Alarms page created the potential for a cross-site scripting vulnerability.	9.3.1
ID: 24884. The RMA wizard successfully replaced an appliance, but the cache did not update and the appliance was unavailable.	9.3.1
ID: 24882. The "Orchestrator cannot reach this appliance" notification was not triggered when the appliance was unreachable.	9.3.1
ID: 24869. This release was patched to address CVE-2023-2650 (OpenSSL vulnerability).	9.3.1
ID: 24828. A partitioning issue resulted in historical alarms not loading as expected.	9.3.1
ID: 24814. An issue with alarm IDs prevented some alarm emails from being sent.	9.3.1
ID: 24778. It was not possible to back up Stats Collector to an HTTP server.	9.3.1
ID: 24666. An issue with time sync while using MFA authenticator codes prevented users from logging in to Orchestrator.	9.3.1
ID: 24657. A certificate verification issue caused Stats Collector to become unreachable on the appliance.	9.3.1
ID: 24196. An input validation issue in the audit log comment dialog box caused the server to block requests that contained multiple consecutive spaces.	9.3.1



Issue	Earliest Release to Fix
ID: 24079. Session IDs were being improperly attached to redirect responses, resulting in issues logging in to Orchestrator.	9.3.1
ID: 23949. The appliance's approved status was not updated from false to true in the Orchestrator database upon replacement, resulting in the appliance erroneously not being marked as approved.	9.3.1
ID: 23924. Orchestrator was not clearing alarms upon system start, leaving legacy alarms in the system after upgrade.	9.3.1
ID: 23912. Disk usage alarms on the appliance did not properly resolve even after appliance disk space was expanded.	9.3.1
ID: 23733. An issue with user tokens created the potential for a cross-site scripting vulnerability.	9.3.1
ID: 23704. The web UI did not recognize a change in license tier from base to 200 Mbps.	9.3.1
ID: 23596. An issue within the sys dump process created the potential for a remote code execution vulnerability.	9.3.1
ID: 23164. The Azure library did not recognize the Orchestrator when it was behind an authenticated proxy, preventing proper integration.	9.3.1
ID: 21975. A critical alarm was erroneously thrown when the WAN interface was acquiring an IP address through DHCP.	9.3.1
ID: 24030. Upon upgrade, SMTP server settings did not properly set the email alarm format, resulting in Orchestrator not sending email alarms when appliances met alarm thresholds.	9.3.0
ID: 23957. A command issue created the potential for an unauthenticated user to execute a command injection vulnerability.	9.3.0
ID: 23909. When a template was created from an existing template group, the template group priority was not being updated, resulting in templates being applied in the improper order.	9.3.0
ID: 23699. An error in calculating the Y- and Y2-axis bounds of the Appliance Flow Trends chart created issues with correctly viewing the line graph.	9.3.0
ID: 23438. Because of the asynchronous nature of the collector and reader on an appliance, the Underlay value on the Availability page could sometimes present an erroneous percentage (less than 1%).	9.3.0
ID: 23297. An issue with end-to-end encryption caused unexpectedly high CPU usage on the Orchestrator.	9.3.0
ID: 23128. An issue with ciphers in Orchestrator created the potential for an unauthenticated user to manipulate user sessions or cookies.	9.3.0
ID: 22845. The Speed and Duplex columns in the Interfaces table were incorrectly displaying configuration settings in the Orchestrator UI, even if they were correct in the CLI.	9.3.0
ID: 22803. An issue in the passwordreset table meant that admin account usernames could not contain more than 40 characters.	9.3.0
ID: 22352. ACLs in route maps were not being applied successfully due to a misconfiguration in certain templates.	9.3.0



Issue	Earliest Release to Fix
ID: 22208. In the Orchestrator UI, the loss charts scale was not being properly updated when the Lock Scale option was selected.	9.3.0
ID: 22096. On the Schedule & Run Reports page, reports that were run produced an error when only "CPU Usage Stats" was selected.	9.3.0
ID: 20230. Continuous diffing of Zscaler artifacts and use of location/sublocation download state as an orchestration parameter caused some performance issues with Zscaler Orchestration.	9.3.0
ID: 20148. Outdated JavaScript libraries were in use in some versions of Orchestrator.	9.3.0
ID: 24884. The RMA wizard successfully replaced an appliance but the cache did not update and the appliance was unavailable.	9.2.5
ID: 24672. The Orchestrator alarm email service could not fetch the correct parent groups when nested appliance groups were configured.	9.2.5
ID: 24663. A WAN label was deleted when it was used in hub breakout policy, resulting in the web UI rebooting unexpectedly.	9.2.5
ID: 24603. Upon upgrade, Orchestrator updated the appliance's software version and applied new configurations even if the appliance upgrade failed, resulting in node process restarting unexpectedly and other performance issues.	9.2.5
ID: 23850. After changing the Configuration Polling Interval, the Zscaler IP SLA address reverted to the default URL.	9.2.5
ID: 24210. An error in the SameSite attribute incorrectly removed a session token, which caused users to appear unauthenticated and be redirected back to the Orchestrator login page.	9.2.4
ID: 24061. Setting the appliance in maintenance mode with Pause Orchestration enabled caused performance issues with Zscaler Orchestration.	9.2.4
ID: 23975. A query syntax issue caused Stats Collector to reboot unexpectedly.	9.2.4
ID: 23904. A configuration issue caused the HASync peer to become unreachable from the appliance.	9.2.4
ID: 23895. Addresses CVE-2022-4304, CVE-2022-4450, CVE-2023-0215, and CVE-2023-0286.	9.2.4
ID: 23858. The remote log service was not sending alarms with customized severity.	9.2.4
ID: 23849. A validation error in Zscaler Gateway was thrown if the Idle Time to Dissociation parameter was set to 99 minutes or less.	9.2.4
ID: 23710. An issue with the alarm debounce module created a filtering error that prevented some alarms from being sent.	9.2.4
ID: 23694. The hostname of the appliance that triggered an alarm was missing from syslog messages.	9.2.4
ID: 23667. A missing source menu in the exportTemplate API request caused Orchestrator Blueprint Export to throw an error.	9.2.4



Issue	Earliest Release to Fix
ID: 23648. An error in how appliance models are reported to Orchestrator prevented the Boost tab of the web UI from loading properly.	9.2.4
ID: 23630. Users were unable to apply a license preconfiguration value without a feature license on an appliance that supported a feature license.	9.2.4
ID: 23445. The security response header was missing the Referrer-Policy header.	9.2.4
ID: 23304. A JavaScript error in how time zones are classified prevented graphs from loading in bandwidth trends reporting.	9.2.4
ID: 22919. Appliance preconfiguration settings did not contain fields for branch NAT rules and NAT pools.	9.2.4
ID: 22913. A session management issue caused a 504 Gateway Time Out error when trying to connect to the web UI.	9.2.4
ID: 23927. An upgrade of the Zscaler web services to fix security issues included a change in the session cookie format that caused the Orchestrator to lose connectivity to Zscaler.	9.2.3
ID: 23893. A duplicate record was being created during appliance configuration, preventing Zscaler association from forming successfully.	9.2.3
ID: 23709. A validation error prevented an "@" symbol from being used in Orchestrator RADIUS login.	9.2.3
ID: 23671. Errors in filtering caused API requests to be serialized, resulting in slower than expected Orchestrator UI performance.	9.2.3
ID: 23573. A configuration issue in HA appliances caused orchestration to fail in HA devices.	9.2.3
ID: 23559. A configuration issue prevented backup of the Stats Collector if the username or password contained a backslash character (\).	9.2.3
ID: 23468. When an API call was made for /rest/stats/aggregate/topTalkers, the source IP address was incorrectly returned in the internal encoding.	9.2.3
ID: 23392. Stats Collector was running backup jobs even when the "Advanced Stats Collection" option was not enabled.	9.2.3
ID: 23316. Adding location details in Orchestrator caused the SNMP configuration to be deleted unexpectedly.	9.2.3
ID: 23302. A caching issue caused time information to fall out of sync on the appliance, even when NTP was enabled.	9.2.3
ID: 23280. IP Forwarding was not enabled by default when using Azure or AWS One-Click automation.	9.2.3
ID: 23229. A validation error prevented successful upgrade if the appliance had an IPv6 address.	9.2.3
ID: 23222. A validation issue regarding the Packet Reorder Wait Time value prevented the Orchestrator from upgrading successfully.	9.2.3
ID: 23204. An RBAC filtering issue affected the UI so that certain roles could access D-NAT and S-NAT menus when they were supposed to be disabled.	9.2.3



Issue	Earliest Release to Fix
ID: 23117. The Orchestrator was not sending alarm emails in cases where no appliance alarms were raised.	9.2.3
ID: 23114. Orchestrator was not sending alarms to the remote server when the alarm stream was at a paused state.	9.2.3
ID: 22962. An authentication issue prevented successful bulk upload of files to Service Groups in Orchestrator.	9.2.3
ID: 22955. A database query error prevented cleared appliance alarms from being sent.	9.2.3
ID: 22861. An issue with PPPoE links dropping unexpectedly prompted Orchestrator to delete key route policy entries for EdgeHA, causing packets to be sent over the wrong interface.	9.2.3
ID: 22603. Certain preconfiguration settings were being overwritten by the appliance and reset to default values.	9.2.3
ID: 23163. To address CVE-2022-43528, the /gms/rest/authentication/login endpoint was removed from the Orchestrator API regardless of whether two-factor authentication (2FA) was enabled. In this release, the API endpoint was restored for the case where 2FA is disabled.	9.2.2
ID: 22987. An issue caused Zscaler locations to be downloaded incorrectly, resulting in incomplete appliance information and dropped tunnels.	9.2.2
ID: 22567. Upon upgrade, syslog alarm messages contained an incorrect hostname and systemId.	9.2.2
ID: 22387. Orchestrator was incorrectly sending frequent alarm alerts via email.	9.2.2
ID: 22363. Upon upgrade, authorization and network roles were inconsistent on some appliances.	9.2.2
ID: 22343. Unreachable HA appliances could not be removed from Orchestrator.	9.2.2
ID: 22328. On some appliances, orchestration stopped unexpectedly after enabling segmentation.	9.2.2
ID: 22317. A configuration issue led to templates being applied in a different order than expected.	9.2.2
ID: 22153. A confirmation pop-up now confirms when the replace function is being used on the Templates tab.	9.2.2
ID: 22102. User roles were not being shown for users on the Active Sessions tab.	9.2.2
ID: 21901. The backup file was being generated on the appliance several times a day, increasing disk usage to a high level.	9.2.2
ID: 22451. A database error caused the cloud instance of Stats Collector to reboot unexpectedly.	9.2.1
ID: 22308. SMTP credentials for Cloud Orchestrator were not being saved correctly.	9.2.1
ID: 22296. Users were not receiving emails containing two-factor authentication code after upgrade to Cloud Orchestrator 9.2.1.	9.2.1
ID: 22065. Deleted appliances persisted in some tables, causing an upgrade failure.	9.2.1
ID: 22027. Application search by IP failed on Application Definitions tab.	9.2.1



Issue	Earliest Release to Fix
ID: 21885. AVC attributes were not shown in address map and not available for ACL configuration.	9.2.1
ID: 21882. The Appliance filter was displaying inconsistent results.	9.2.1
ID: 21869. Upgrade appliance feature displays a blank screen.	9.2.1
ID: 21732. Addresses a security vulnerability. Customers are urged to upgrade to this version. Details of this vulnerability will be published at a later time.	9.2.1
ID: 21647. A preconfiguration issue in Orchestrator prevented the Link Aggregation feature from working as expected.	9.2.1
ID: 21433. ZIA tunnel taking over 20 minutes to form.	9.2.1
ID: 22026. The syslog receiver was incorrectly processing alarm information from the appliance.	9.2.0
ID: 21992. If a requested alarm history sequence ID was not in its database, the appliance was not returning an error message stating the alarm was not available.	9.2.0
ID: 21798. The Packet Reorder Wait Time minimum value has been raised to 5ms to address transient loss experienced by AppNeta users when viewing the data path measurement type.	9.2.0
ID: 21615. A source parameter error in the UI prevented custom images from being uploaded.	9.2.0
ID: 21506. There was no preconfigured YAML file available for Zscaler association.	9.2.0
ID: 21440. A validation error was preventing users from changing values on the TCP Accel Options template page.	9.2.0
ID: 21403. YAML preconfiguration failed to configure inbound port forwarding properly.	9.2.0
ID: 21323. Audit logs were not generated for Application Groups configuration changes.	9.2.0
ID: 21309. A UI issue was causing duplicate certificates to be inserted into DB, resulting in unexpected restart of the node process.	9.2.0
ID: 21293. Preconfiguration validation was failing when bwan0 and blan0 were configured independently.	9.2.0
ID: 21094. Non-admin users were unable to scan the QR code to access multifactor authentication.	9.2.0
ID: 21062. The actionlog table was not partitioned on queued time.	9.2.0
ID: 21049. A UI issue kept the relative position of Pause/Resume Orchestration button from being adjusted to the browser window size.	9.2.0
ID: 21002. Preconfiguration incorrectly declared proper interface names as invalid.	9.2.0
ID: 20944. Orchestrator was failing to push the overlay route map policy to an online EC-HA appliance when the partner appliance was offline.	9.2.0
ID: 20909. A UI issue was preventing users from editing security policy templates after they were pushed and incorrectly letting users edit it from the appliance UI.	9.2.0



Issue	Earliest Release to Fix
ID: 20893. The IPSec UDP Status page was not sorting by Key Status as expected.	9.2.0
ID: 20838. A validation error was causing the REST API to return an incorrect status code.	9.2.0
ID: 20794. A validation error caused SNMP v3 passwords containing special characters to not be accepted in the SNMP v3 template.	9.2.0
ID: 20774. AWS One-Click was not populating Instance Type for some regions.	9.2.0
ID: 20601. An invalid value in an alarm configuration was causing issues with delivering alarm notification emails.	9.2.0
ID: 20583. An input error was causing customers to create unintended compound application definitions.	9.2.0
ID: 20496. A certificate issue caused Oauth to return an unexpected handshake error.	9.2.0
ID: 20424. The help text for Max Activation Wait Time was misleading. It should have applied only to cases when either an appliance was not reachable or it was reachable but its tunnels were down.	9.2.0
ID: 20299. A UI issue was causing the MOS overlay calculation to be too low, throwing an unexpected alarm.	9.2.0
ID: 20251. Certain roles partitioned using RBAC were not appearing as active sessions.	9.2.0
ID: 20103. On some appliances, the Appliance Bandwidth Utilization chart was erroneously showing 100% utilization.	9.2.0
ID: 19721. Accounts were not being locked out as expected after too many failed authentication attempts.	9.2.0
ID: 19647. After adding or renaming a group in Orchestrator, pressing the Enter key unexpectedly refreshed the page.	9.2.0
ID: 19630. A UI issue prevented some interface boxes from scrolling properly, which would not allow users to add labels.	9.2.0
ID: 19099. The REST API operation POST /appliance/discovered/approve/{applianceId} was returning an invalid JSON in its response.	9.2.0
ID: 18570. The Schedule & Run Reports tab was not generating reports without an associated email address.	9.2.0
ID: 16299. The /gmsConfig REST API was removed to address an issue with resource storage.	9.2.0
ID: 25094. When the state or IP address of an interface in an EdgeHA setup changes, Orchestrator occasionally resets all flows. With this fix, the Reset all flows field on the Orchestration Settings dialog can be used to control this behavior.	9.1.8
ID: 24214. When clearing a local appliance alarm, the Orchestrator incorrectly set the clear time to 0.	9.1.7
ID: 24099. Addresses a security vulnerability. Customers are urged to upgrade to this version. Details of this vulnerability will be published at a later time.	9.1.7
ID: 23912. Disk usage alarms on the appliance did not properly resolve even after appliance disk space was expanded.	9.1.7



Issue	Earliest Release to Fix
ID: 21855. Addresses a security vulnerability. Customers are urged to upgrade to this version. Details of this vulnerability will be published at a later time.	9.1.3
ID: 21766. Upon Orchestrator upgrade, Zscaler passthrough tunnels were incorrectly deleted.	9.1.3
ID: 21733. Addresses a security vulnerability. Customers are urged to upgrade to this version. Details of this vulnerability will be published at a later time.	9.1.3
ID: 21598. BGP configuration was causing route maps to behave unexpectedly after upgrade.	9.1.3
ID: 21419. Zscaler tunnels were being formed to countries that were not always in line with the selected preference.	9.1.3
ID: 21411. Some appliances were unable to establish SD-WAN tunnels on NAT interfaces.	9.1.3
ID: 21385. A UI issue improperly displayed the status of the Redistribute OSPF routes to SD-WAN fabric setting.	9.1.3
ID: 21365. Appliances running in maintenance mode were preventing underlay tunnels from resolving correctly.	9.1.3
ID: 21153. Orchestrator was not properly provisioning due to an error in the Blueprint.	9.1.3
ID: 21295. A validation change in Azure library caused issues with backward appliance compatibility.	9.1.3
ID: 21153. Orchestrator was not properly provisioning due to an error in the Blueprint.	9.1.3
ID: 21098. Fixes for the log4j2 vulnerability introduced an issue that prevented proper logging in the cloud Orchestrator.	9.1.3
ID: 21041. Alarm event timestamps were being sent to the remote web socket out of order.	9.1.3
ID: 20943. Orchestrator was applying and then mistakenly deleting ACLs applied via template.	9.1.3
ID: 20926. When enabling Zscaler Gateway, a validation error sometimes prevented users from entering valid refresh time and idle time on the Authentication menu.	9.1.3
ID: 20906. Upgrades of Orchestrator could fail if the Orchestrator had old IPSec UDP key material in the database.	9.1.3
ID: 20790. An appliance deleted from Orchestrator appeared as queued for deletion but was stuck in a pending state and still collecting stats.	9.1.3
ID: 20764. AWS URLs were not being successfully saved to the Domain field on the Application Definition page.	9.1.3
ID: 20754. The number of lost packets reported by Loss Summary and Loss Trends did not match.	9.1.3
ID: 20722. Scheduled Orchestrator backups were failing even when manual backups were working.	9.1.3
ID: 20701. Libraries were updated to address the log4j2 vulnerability (CVE-2021-44832).	9.1.3
ID: 18667. Setting the IKE identifier on an appliance to "IP ADDRESS" instead of "FQDN" caused an unexpected failure.	9.1.3



Issue	Earliest Release to Fix
ID: 20946. Orchestrator Blueprint Export failed to download in select browsers.	9.1.2
ID: 20817. When removing an appliance, Orchestrator timed out while marking the task as complete.	9.1.1
ID: 20785. After a reboot, Orchestrator continuously made erroneous modifications to Zscaler node location/sublocation.	9.1.1
ID: 20681. Orchestrator was selecting Zscaler VPN endpoints that were not always in the same country as the appliance.	9.1.1
ID: 20677. Orchestrator was not affected by CVE-2021-45105 but was upgraded to include log4j 2.17.0.	9.1.1
ID: 20649. This release addresses the Apache Log4j vulnerability as described in CVE 2021-44228 and CVE-2021-45046.	9.1.1
ID: 20585. Removing an appliance was causing the orchestration task to time out while marking the task as complete.	9.1.1
ID: 20580. The Orchestrator overlay applier deleted ACLs that were applied via template due to a type difference between Orchestrator and appliance VRF ACL rule criteria.	9.1.1
ID: 20522. Orchestrator mistakenly created a new WAN IP for an HA appliance without a label, resulting in out-of-range error when assigning a new IP.	9.1.1
ID: 20483. System Information could not be updated from within Orchestrator.	9.1.1
ID: 20443. DNS classification failed to apply on ECOS 9.0.3.2 appliances.	9.1.1
ID: 20406. RMA Wizard failed to restore configuration when replacing an EC-M-P on 8.3.4.0 with an EC-M-H running the same ECOS version.	9.1.1
ID: 20383. Preconfiguration file allowed duplicate interface labels causing issues with HA pair devices.	9.1.1
ID: 20320. In specific instances, existing Zscaler tunnels were getting deleted, and Orchestrator was trying to send ZEN IP addresses as 0.0.0.0.	9.1.1
ID: 20297. The default Maximum TCP MSS value on the Orchestrator Default Template caused errors on some third-party IPsec tunnels.	9.1.1
ID: 20294. Orchestrator erroneously set ikeVersion to null, which resulted in failure to build Zscaler tunnels.	9.1.1
ID: 20286. An ownership issue with the /home/gms/gms/backup directory was causing backups to fail.	9.1.1
ID: 20275. Exported Excel flow file was not showing data properly.	9.1.1
ID: 20274. The System Information tab was coming up blank if 10 or more appliances were selected.	9.1.1
ID: 20226. Orchestrator failed to apply registration information because a blank space was allowed after the IP address on the Orchestrator Reachability dialog.	9.1.1



Issue	Earliest Release to Fix
ID: 20225. A registration issue was causing Orchestrator to send a reachability IP address that was different from its public IP address to appliances, resulting in loss of connectivity from many appliances to Orchestrator.	9.1.1
ID: 20215. Interface labels without a value in the preconfiguration file caused deployment to fail.	9.1.1
ID: 20190. After adding new EC-V appliances, tunnels were not getting configured on a regional mesh overlay, but those on a regional hub and spoke overlay were configured as expected.	9.1.1
ID: 19716. Orchestrator WebSocket services were vulnerable to cross-site WebSocket hijacking.	9.1.1
ID: 19624. A buffer overrun caused the Orchestrator syslog to stop generating and sending messages.	9.1.1
ID: 19144. Added orchestration for Country/State/Time Zone for existing and new Zscaler Locations/Sub Locations. Zscaler has an API rate limit of 400 calls/hr and might take a while to complete amending Country/State/Time Zone to existing Zscaler Locations/Sub locations.	9.1.1
ID: 20649. This release addresses the Apache Log4j vulnerability as described in CVE 2021-44228 and CVE-2021-45046.	9.1.0
ID: 20443. In a network with appliances running ECOS 9.1.0.0 and 9.0.3.2, DNS classification was failing to be applied on the 9.0.3.2 appliances.	9.1.0
ID: 20153. In some cases, the Reclaim Deleted Loopback IPs dialog box was unresponsive and not working as expected.	9.1.0
ID: 20120. In certain deployments, the partition management table was erroneously showing a size of 0 for all rows.	9.1.0
ID: 20044. In rare cases, Orchestrator tenants did not report EdgeHA data to Cloud Portal, fixed only by restarting the tenant.	9.1.0
ID: 20018. Preconfiguration was generating an error indicating that WAN3 and LAN3 were invalid interface names.	9.1.0
ID: 20001. 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
ID: 19834. When adding multiple appliances to the network, a duplicate device was showing up in the appliance tree and the duplicate device could not be removed.	9.1.0
ID: 19789. A remote IP that had been updated by Check Point was not getting updated in Orchestrator until pausing and restarting Check Point orchestration.	9.1.0
ID: 19756. In a BIO configured to drop internet breakout traffic, local internet traffic was getting sent to passthrough INET per the branch policy.	9.1.0
ID: 19315. On rare occasions, a backup Orchestrator instance was assuming active status without approval. The restore command now includes the "new" option to explicitly control this behavior.	9.1.0
ID: 19235. The bandwidth trends report was showing the number of FEC packets on an underlay, as reported by loss trends, as higher than the total number of packets.	9.1.0
ID: 18677. The preconfiguration syntax validation tool was not checking for an underscore in host names, resulting in failures when preconfig was applied.	9.1.0



Issue	Earliest Release to Fix
ID: 18600. In some cases, Zscaler entries were stuck in pending state, and sublocation information was not showing up in the summary screen.	9.1.0
ID: 17951. When clicking any of the "manage with templates" links in Orchestrator, users will be prompted to confirm the template group to which the template should be added. This change will help avoid inadvertently adding a template to the default group and pushing the change to all appliances.	9.1.0
ID: 19886. Preconfiguration was failing when trying to apply the OSPF system configuration.	9.0.5
ID: 19767. Orchestrator memory utilization was growing over time, eventually causing the server to become unresponsive.	9.0.5
ID: 19515. In some cases, the Top Talkers report was displaying incorrect data for Flows Started and Flows Ended.	9.0.5
ID: 19294. The Loss Summary report was showing an average loss that was higher than it should have been. This was due to a mis-labeling of columns since the data shows actual loss calculated as packets lost/total packets received during the monitoring period. The "Avg Loss %" column labels have been changed to "Loss %."	9.0.5
ID: 19646. On a Cloud Orchestrator that was created from a blueprint, not all applications were available under application match criteria.	9.0.4
ID: 19591. Applying the inbound port forwarding configuration via preconfig was failing if sourceInterface was set to "any."	9.0.4
ID: 19405. When running the manual configuration wizard, existing LAN subnets available on the appliance were not getting populated automatically, which was causing static routes to be removed.	9.0.4
ID: 19312. In a specific configuration, the WebSocket connection between appliances and Cloud Portal/tenant Cloud Orchestrator was failing to establish if backhauled via overlay.	9.0.4
ID: 19310. On some appliances, the appliance wizard was failing to apply the configuration for a loopback interface because segmentation configuration was being pushed, but segmentation was not enabled.	9.0.4
ID: 19112. Following the upgrade from Orchestrator 8.x, the Top Talkers report was no longer getting included in daily reports.	9.0.4
ID: 19093. Users were unable to create an API Key when using Firefox because an extra "-" character was being added in the date field.	9.0.4
ID: 19061. Appliance Memory Trends were showing No Data for the 1hr and 4hr graphs.	9.0.4
ID: 19050. After manually entering the name for a new label that was not available to pick in the Management Services template, the appliance was failing to connect to Orchestrator or Cloud Portal via WebSocket.	9.0.4
ID: 18884. Tunnel Charts for Overlay and Underlay were showing Y-axis values of 15 Gbps, but the appliance was only configured for 2 Gbps up/down.	9.0.4
ID: 18818. In some cases, interface bandwidth statistics would not load with a "Failed to get data" error.	9.0.4
ID: 18809. Total bytes for Zscaler were different or missing when flipping the Overlay-Interface-Transport pie charts.	9.0.4



Issue	Earliest Release to Fix
ID: 18739. In some cases, the default partition in Orchestrator's database was getting too full and backups were failing with a "database partitioning is in progress" error.	9.0.4
ID: 18443. Users were able to successfully log in when using the /authentication/login API. All further requests, however, were coming back with a 401 'Unable to validate CSRF token' error.	9.0.4
ID: 17977. When viewing realtime overlay traffic in the Overlay-Interface-Transport pie charts, the line graph did not match the displayed TX value.	9.0.4
ID: 17756. A new Orchestrator that was restored from a blueprint was incorrectly inheriting the list of discovered appliances from the source Orchestrator.	9.0.4
ID: 18863. Orchestrator was allowing SNMP v3 passwords that were less than 20 characters long.	9.0.3
ID: 18751. BGP preconfiguration was failing to apply the same configuration to two appliances, failing on one or both at times.	9.0.3
ID: 18589. The reserved priority range for Orchestrator (20000 to 24999) had been missed in some online help topics.	9.0.3
ID: 18566. The RMA wizard would not restore a denied appliance, and it had to be restored manually.	9.0.3
ID: 18526. After enabling advanced segmentation, some EdgeConnect appliances did not show the default segment configuration, and orchestration of new tunnels would not start.	9.0.3
ID: 18469. The Top 'X' tunnel graphs were including passthrough tunnels while some latency and loss graphs did not, creating confusion when comparing the two.	9.0.3
ID: 18176. The "Configure Boost" button was visible to read-only users in the Boost summary report, indicating that those users could make changes.	9.0.3
ID: 18129. When using the RMA wizard to replace an appliance, some portion of the previous configuration had not been pushed to the new device.	9.0.3
ID: 18054. When removing and re-applying overlays, the orchestration process remained stuck in a pending state for a single appliance even though there were no apparent issues with connectivity or traffic.	9.0.3
ID: 18006. In previous releases, the RMA wizard was replacing interface MAC address assignments on a replacement EC-V. The wizard will now preserve the assignments from the EC-V being replaced.	9.0.3
ID: 18076. An empty ACL template group configuration was causing the BIO page to fail to return the configuration or allow users to make changes.	9.0.2
ID: 17892. If an appliance was in maintenance mode with orchestration paused and its IPSec UDP port is empty, the appliance was stuck in a continuous synchronizing state when trying to build tunnels.	9.0.2
ID: 17639. On Cloud Orchestrator, spaces in a query field were causing errors on the Flows page.	9.0.0
ID: 15255. The RMA Wizard did not support EdgeConnect Virtual (EC-V) appliances.	9.0.0



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.

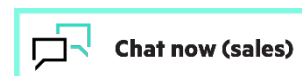
- <https://community.arubanetworks.com/home>



SD-WAN Orchestrator 9.4.6 Release Notes
DISCLOSURE STATEMENT

Learn more at

hpe.com



© 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.