

Silver Peak Unity Orchestrator™

Release Notes

Version 9.5.1_40443

Revision E: November 5, 2024

This document provides important information about Orchestrator 9.5.1, including top items, limitations, new features, issues fixed, and upgrade considerations. See [Additional Information](#) for historical features and fixes, information about installation procedures, CLI-only features, port requirements, and configuration best practices.

Top Items for this Release

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 Orchestrator to a supported version. For more information, see [Known Issues/Upgrade Considerations](#).

Because of the migration from CentOS to Rocky Linux, upgrading to Orchestrator 9.4.x and later could cause connectivity issues between the Orchestrator and EdgeConnect Operating System (ECOS) appliances that have not also been upgraded to 9.4.x.x. For more information, see [Known Issues/Upgrade Considerations](#).

In Orchestrator 9.3.0, most of the APIs changed to accommodate API-based RBAC. If you have integrated your IT systems using Orchestrator REST APIs, **be cautious about upgrading** to Orchestrator 9.5.1 until you change your integrations to work with Orchestrator 9.5.1. 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 Orchestrator releases. For a reference to pre-upgrade API endpoints, see [Pre 9.3 Orchestrator API Endpoints](#).

Most of the currently installed, self-hosted EdgeConnect 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 Orchestrators running on CentOS 7. The EdgeConnect 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 Orchestrator application does not change the underlying VM. The procedure requires creating a complete backup of your current Orchestrator, building a new Rocky Linux VM, and loading the backup on the new machine.

NOTE: Self-hosted/on-prem Orchestrators (IaaS AWS) are not affected. EdgeConnect Orchestrator-as-a-Service (OaaS) products are also not affected.

Documentation of detailed procedures for this operation is provided on the [HPE Aruba Networking EdgeConnect SD-WAN documentation site](#).

Top Items for this Release (continued)

■ Prior to upgrading to Orchestrator 9.5.1, all EdgeConnect appliances must be on release 8.3.x.x or greater, or 9.x.x.x release streams. EdgeConnect appliances running a release prior to 8.3.x.x will lose all communications to the 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 Orchestrator periodically, which will claim back the used disk space.

■ In Orchestrator 9.4.1 and later, RADIUS authentication using MSCHAP, MSCHAPv2, and EAP-MSCHAPv2 will fail. These 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 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.

■ If you are upgrading from Orchestrator 9.0.6, you cannot upgrade to the original Orchestrator 9.1.0 release, build 40514. You can only upgrade to release 9.1.0_40516 or newer.

■ Silver Peak 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. Refer to [Release Limitations](#) for more information about these features and other important information. Documentation specific to the Advanced Segmentation feature can be found [here](#).

■ Tunnel Groups are not supported in this release and will be deprecated in a future Orchestrator version. If you are using Tunnel Groups, you should migrate to Business Intent Overlays (BIOs).

■ If you are upgrading from a release prior to 8.9.10 or from 8.10.x prior to 8.10.10, this release sets the default lifetime for IPSec UDP key material to 0 (infinite), which helps to ensure that tunnels in your SD-WAN network do not go down due to key material configuration issues (activation or expiration). Following the upgrade, you should validate your configuration in the Schedule IPSec Key Rotation dialog.

■ If you are upgrading from Orchestrator 8.5.7, or from a release that requires you to upgrade to 8.5.7 before going to 8.10.12, you must delete partitions that are more than three months old. See [Installation and Upgrade](#) for more information.

■ 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 Orchestrator to the new version, install a new Orchestrator VM at the same new version, back up the existing (upgraded) Orchestrator, and then restore the backup on the new Orchestrator VM – new 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 Orchestrator 9.1.x releases. As these limitations are addressed in subsequent builds of this release, this list will be updated in future revisions of the release notes.

Feature Limitations

The following features have these specified limitations:

- When using the Radius snooping feature, source and destination must be collocated.
- IPSec Suite B is not fully supported in Orchestrator 9.5.1.

Feature Limitations when Segmentation is Enabled

The following features are not supported when segmentation is enabled:

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

When segmentation is enabled, Orchestrator removes and reapplies all Overlays on all appliances. Afterward, the Orchestrator tears down and recreates every tunnel again. Any manual tunnels and route policies present on the EdgeConnect are removed and must be recreated by the user manually.

Each EdgeConnect will experience 2-15 minutes of downtime as Overlays are removed and re-added. The 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 Orchestrator in the middle of the enablement process.

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

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:

- 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, 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.

Release Limitations (continued)

- 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 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 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 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.

New Features and Enhancements

The following new features or enhancements are included in Orchestrator 9.5.1.

SNMP Support and Encryption

There is now SNMP support for standard Linux Server MIBs, such as CPU, memory, disk, and other metrics. In addition, SNMPv3 encryption has been upgraded to AES256/SHA256.

IPv6 Router Advertisement (RA) Support

The Deployment Profiles tab now includes support for Router Advertisement settings for IPv6 LAN interfaces.

Flexible LAN-Side Bridge Groups

This feature allows for creation of a bridged (switched) interface while in inline router mode on the LAN side of an EdgeConnect OS. The BVI (Bridged Virtual Interface) allows devices in a bridge group to use the IP address of the BVI as a default gateway to other IP networks. Four new predefined interfaces were added to Orchestrator to support bridge groups.

Role Cache Available in Orchestrator UI

Role-to-IP mapping cache can now be viewed in the Orchestrator user interface. Previously, this information was only available through a tunbug command. The resultant table shows all known MAC addresses and allows for deleting ARP entries.

Select Multiple Segments in VRF Inter-Segment DNAT Rule Configuration

You can now add, update, or delete multiple DNAT rules from different source segments.

Support for Discrete Sub-Options of Option-82 in DHCP Relay

When you configure DHCP, you can now select specific sub-options when you enable Option-82 and select Distinct DHCP server per segment.

Security Issues Fixed

The following table contains security-related issues fixed in Orchestrator 9.5.x releases, organized by the software version that first resolved them.

Issue ID	CVE	CVSS Score	CVSS Vector	Description	First Release to Resolve
ID: 27113	N/A	7.2	CVSS:3.0/AV:N/A C: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.	9.5.0
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.	9.5.0
ID: 26683	CVE-2021-38153	5.9	CVSS:3.1/AV:N/A C:H/PR:N/UI:N/S: U/C:H/I:N/A:N	This release was patched to address CVE-2021-38153.	9.5.0

Issues Fixed

The following known issues have been fixed in Orchestrator 9.5.1.

- ID: 31135 Because of an issue with how encryption keys were stored, SMTP encryption and decryption for Cloud OaaS was not functioning properly in version 9.4.2 and later.
- ID: 30556 A coding error in the AuthenticationResource file prevented the two-factor authentication (2FA) mechanism from working properly.
- ID: 29689 Calling getApplianceById during cluster upgrade resulted in a MySQL exception, preventing the upgrade from completing successfully.
- ID: 29466 Upon upgrade from Orchestrator 9.2.3_40156 to 9.3.2.40150, non-hub appliances were added as hub appliances.
- ID: 29374 Invalid query parameter prevented updates to GCP account.
- ID: 29275 Added new query parameter to support the Netskope API "exact" sourceIdentity enhancement.
- ID: 29164 New HA pair creation continually failed due to a previous HA pair creation that failed in a previous Orchestrator release.
- 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.
- ID: 28993 Address Map selection was not available in Application Definitions.
- ID: 28963 A previous improvement made to the file upload process created an issue that prevented Update Signature IDS/IPS from running successfully.
- 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.
- 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.
- ID: 28329 An issue with API efficiency caused a delay in reflecting successful EdgeHA deployment in the Orchestrator appliance tree.
- ID: 28205 When the time period for collecting data was set to 1 day, Orchestrator response time was slow.
- ID: 28192 The inbound port forwarding pre-configuration file could not convert configured interface labels to the correct IP.

NOTE Issues fixed in past releases can be found [here](#).

API Changes

The following API changes are included in Orchestrator 9.5.1.

Important In Orchestrator 9.3.0, most APIs have changed to accommodate API-based RBAC. If your IT systems are integrated with Orchestrator REST APIs, do not upgrade to Orchestrator 9.3.0 until you modify your integrations to work with 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 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 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 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 Orchestrator 9.1.0

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

Changes from 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

Known Issues/Upgrade Considerations

The following list summarizes considerations that must be addressed when upgrading from any previous version of Orchestrator to 9.5.1.

Risk of failed cryptographic functions in Orchestrator 9.4.x and 9.5.x releases caused by race condition

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:

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."

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.

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.

Slow upgrades to 9.4.x

It is possible to experience slowness when upgrading 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. 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 Orchestrator users migrate to Rocky Linux when possible.

Appliance connectivity issues possible post-9.4.x upgrade

Because of the migration from CentOS to Rocky Linux, upgrading to Orchestrator 9.4.x and later could cause connectivity issues between the Orchestrator and older versions of the EdgeConnect Operating System (ECOS). If your ECOS appliances are also on version 9.4.x.x and later, there should be no connectivity issues. However, if your ECOS appliances are on older versions, you will need to disable FIPS mode on the Orchestrator (enabled by default) before restarting the Orchestrator in order to connect to your appliances.

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

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

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

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

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

Large queries use extra disk space and produce a high volume of stats

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 Orchestrator periodically, which will claim back the used disk space.

Known Issues/Upgrade Considerations (continued)

Admin and gms users now separate users

In Orchestrator 9.4.1 and later, 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.

With this change, `/home/gms/gms/orch-setup -c` and `/home/gms/gms/orch-setup -p` now require a sudo password for the admin user, instead of a root user password. In addition, to perform upgrades, `/home/gms/gms/orch-setup -u` must now be run as `sudo /home/gms/gms/orch-setup -u`.

Check Point CloudGuard Connect disabled with version 9.4.1

Upon upgrade to 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 Orchestrator 9.4.1 and later, RADIUS authentication using MSCHAP, MSCHAPv2, and EAP-MSCHAPv2 will fail. These 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 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.

Orchestrator and Azure/AWS integration support

Orchestrator 9.5.x does not support ECOS 8.3 or earlier for Azure/AWS integration.

MFA required for OaaS starting with version 9.3.0

Starting from 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 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 Orchestrator 9.5.1 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 Orchestrator 9.3.0, as some existing APIs are currently undergoing changes. These changes are planned to be completed in a future Orchestrator release. For more information, see [Top Items for this Release](#).

Known Issues/Upgrade Considerations (continued)

Zscaler integration requires GRE to be enabled

When upgrading to Orchestrator 9.5.1, the Zscaler integration requires the Zscaler account to have GRE enabled. If GRE is not enabled, the upgrade fails. If GRE is disabled on your account, the Zscaler integration will report errors upon upgrade, and you must enable GRE on your Zscaler account.

NOTE: 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.

Internet Breakout Policy on hub appliances

After 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.

IPSec anti-replay window incompatibility

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.

INET tunnel deletion/recreation

After upgrading to version 9.2.2.40302, cross-connected INET tunnels may be deleted or rebuilt, which could lead to intermittent tunnel connectivity.

User names limited to 40 characters

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.

Minor alarm upon upgrading from older ECOS images

An alarm may trigger on Orchestrator version 9.1 or newer under the following conditions:

- A pair of appliances deployed in EdgeHA configuration are upgraded from ECOS version 9.0 or older to ECOS version 9.1 or newer, OR
- A pair of appliances deployed in EdgeHA configuration running ECOS version 9.1 or newer are added and the number of EdgeHA subnets is less than 32.

To clear this alarm, perform the following steps for each EdgeHA pair:

- 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

The Orchestrator^{SP} 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 Orchestrator^{SP}, which is targeted for the October 9th maintenance window. Service providers will not need to upgrade tenants to get this fix.

Known Issues/Upgrade Considerations (continued)

Duplicate routes in EdgeHA with regional routing

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:

1. On the BGP page (Configuration > Networking > Routing > BGP), enable BGP, configure the ASN and Router ID, and then click **Apply**.

NOTE: It is not necessary to configure BGP peers if you are using OSPF on the LAN side.

2. 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**.

Statistics migration for upgrades from 8.8.1 or earlier

If you are upgrading from version 8.8.1 or earlier, except for version 8.5.10, appliance statistics will be migrated in the background following the upgrade to 8.9.4.

Always upgrade to the latest available version

When upgrading from a previous release train (for example, 8.8.x to 8.9.x), you should upgrade to the latest version currently available to prevent upgrade failures and to get the latest security and product updates.

Orchestrator backups have a 2 GB limit over SFTP

The size of Orchestrator backups is limited to 2 GB when using the SFTP protocol. To avoid this issue, users can configure backups to use FTP, SCP, HTTP, or HTTPS.

Direct upgrade from Orchestrator 8.5.3 or earlier is not supported

If you are upgrading from Orchestrator release 8.5.3 or earlier, you must follow a specific upgrade path to Orchestrator 9.5.1. See [Upgrade Path](#) for more information.

Orchestrator backup configuration needs to be redefined

If Orchestrator was ever upgraded to 7.2.0 version and configured the Orchestrator backup (destination host, port, protocol etc.), this will need to be reconfigured after upgrade to 8.6.

Tunnel and application filter in Orchestrator reports

If Orchestrator was ever upgraded to 7.2.1 version and then upgraded to 8.6, tunnel and application filters in the reports will not be preserved.

After upgrading to 8.5, the time zone displayed for scheduled jobs may change

Orchestrator 8.5 shows all schedules in server time zone, but the user can always change the jobs to be shown in the time zone of choice by setting the time zone in the new Orchestrator Administration > Schedule timezone dialog.

In Orchestrator 7.2, the user time zone is not stored when the schedule is saved. After upgrade, Orchestrator will default to the server time zone and users can modify it to the time zone of their choice.

When Overlays are applied, default QoS map and Opt map entries are deleted

On an appliance with an empty database, there are QoS map and Opt map entries that get created by default and start from 10000. When Overlays are applied, the priorities are assigned from 20000. These default rules may get hit first and Overlay rules may never get hit. Therefore, these policy maps entries will be deleted when Overlays are applied.

Known Issues/Upgrade Considerations (continued)

When Overlays are applied, user will not be allowed to use the following priorities. Even if a user creates these rules, Overlay Manager will delete them.

- QoS map priorities that will be deleted: 10000, 10010, 10020, 10030
- Opt maps priorities that will be deleted: 10000, 10010, 10020, 10021, 10030, 10040, 10050, 10060, 10070, 10071

Existing policy maps deleted

If overlays are applied to appliances, priority range starting from 20000 to 24999 will be used by Orchestrator to create overlays related rules. If your appliance already has rules in this range, they will be deleted.

Template history will be lost

When templates are applied, we maintain a history of when was the last time a given template was applied on a given appliance. This history will be lost. New history will be built as templates get applied.

Orchestrator Tunnel groups (a.k.a new Tunnel builder) cannot be used with appliance 7.3 or lower

Tunnel groups can be applied to appliances running on 8.0 or higher version. If you had applied tunnel groups on 7.3 appliance while the Orchestrator was on 8.0 or 8.0.1, you will have to remove the appliances from Tunnel Groups before upgrading to 8.5.

Orchestrator RADIUS or TACACS+ template will not allow any html escape characters like "<"

The html sanitizer on Orchestrator will reject it because it looks like start of an html tag. Do not use any html escape characters in the input.

Downgrade procedure from 8.1.5 to a lower version of Orchestrator

- If users switch Orchestrator from a release $\geq 8.1.3$ to $\leq 8.1.2$, the Orchestrator will not be approved. The customer needs to call Silver Peak to get their Orchestrator approved.
- If users switch Orchestrator from a release $\geq 8.1.3$ to $> 8.1.3$, the Orchestrator will remain approved. No need to call Silver Peak

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 Orchestrator, and configuration best practices.

Installation and Upgrade

Starting with release 8.5, Orchestrator supports only Silver Peak appliances running VXOA release 7.3.0 or higher. Refer to the [Orchestrator Getting Started Guide](#) for installation and upgrade procedures. Starting with release 8.6.0, Orchestrator's IP address, DNS, hostname, and NTP must be configured via CLI. Refer to the [Orchestrator Getting Started Guide](#) for more information about configuring these items.

Important If you are upgrading from Orchestrator 8.5.7, or from a release that requires you to upgrade to 8.5.7 before going to 9.5.1, you must do the following **when** your Orchestrator is at version 8.5.7:

1. Log in to Orchestrator and go to Support > Technical Assistance > Partition Management.
2. Delete all partitions that are more than three months old (any statistics older than three months will be removed by the stats retention policy).
3. Back up Orchestrator and proceed with the upgrade when complete.

Upgrade Path

Not all Orchestrator releases support a direct upgrade to version 9.5.1. Follow the appropriate upgrade path below according to your current Orchestrator release:

- Orchestrator 7.1.1 > Orchestrator 7.3.x > Orchestrator 8.5.7 > Orchestrator 9.5.1
- Orchestrator 7.2.x – 8.4.x > Orchestrator 8.5.7 > Orchestrator 9.5.1
- Orchestrator 8.5.0 – 8.5.4 > Orchestrator 8.7.0 > Orchestrator 9.5.1
- Orchestrator 8.5.4+ > Orchestrator 9.5.1

Note: If you are upgrading from version 8.8.1 or earlier, except for version 8.5.10, appliance statistics will be migrated in the background following the upgrade to 9.5.1. Historical statistics will not be available in Orchestrator until the migration is complete. The migration may take a few hours to a few days depending on the amount of stats data you have stored. To see how much data is currently stored, connect to the Orchestrator over SSH as **admin** and type the following command:

```
[gms@silverpeak-gxv:~] $ du -s -h /home/gms/gms/db/data
133G /home/gms/gms/db/data
[gms@silverpeak-gxv:~] $
```

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. Orchestrator will collect new statistics throughout the migration period.

Upgrade Procedure

1. Acquire the Orchestrator installation image from the Silver Peak support site (the image name is Orchestrator 9.5.1.40443.gip).
2. Refer to the [Orchestrator Getting Started Guide](#) for details about the Orchestrator upgrade procedure.

Initial Installation Procedure

For detailed installation instructions, refer to the [Orchestrator Getting Started Guide](#).

Recovering from a Failed Orchestrator Upgrade

Option A: Restore the Previous Version of Orchestrator

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

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

1. Copy the Orchestrator backup file from your backup server to the /home/gms directory on your Orchestrator server, and name it **gms.zip**.
2. SSH into 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 /* <Your_Restore_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 Orchestrator still does not start, contact the Silver Peak Technical Support team for assistance.

Option B: Proceed with the Upgraded Orchestrator Version

If you want to continue upgrading following a failed upgrade, contact the Silver Peak Technical Support team for assistance.

Features only Available Through Orchestrator CLI

Certain Orchestrator operations can only be performed through 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 Orchestrator	For more information about these items, refer to the Orchestrator Getting Started Guide .
Upgrade Orchestrator	<p>If you are already using Orchestrator 8.6.0 or later and want to upgrade to a newer version, refer to the Orchestrator Getting Started Guide.</p> <p>WARNING A failed upgrade can result in Orchestrator being in a corrupt state. Ensure that you back up Orchestrator before you start the upgrade process.</p> <p>NOTE The upgrade process can take several hours to complete. Run the below command as admin via SSH to check if the Orchestrator upgrade is in progress:</p> <pre>ps ax grep "install_orchestrator"</pre> <p>If you see any output, the Orchestrator upgrade is still in progress.</p>
Restore Orchestrator from Backup	<p>This must be performed manually from Orchestrator SSH CLI, as follows:</p> <ol style="list-style-type: none"> 1. Copy the Orchestrator backup file from your backup server to the /home/gms directory of the new Orchestrator server and rename it gms.zip. 2. SSH into 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 Orchestrators that are running on Fedora core Linux 23 and above, refer to the Orchestrator Getting Started Guide for information about updating security patches.</p> <p>Important: Back up Orchestrator before applying any patches. If a kernel or library update corrupts the OS, restore 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 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 Orchestrator

The table below lists the ports used by 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
443	TCP	HTTPS ²
465, 587	TCP	SMTPS
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 Orchestrator. You can always use the HTTPS port, as it is already allowed. This is not applicable to Orchestrator-as-a-service.

² 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 talks on these ports.

Configuration Best Practices

- If possible, make all configurations to appliances from the Orchestrator, not on the appliances themselves since Orchestrator has a master/slave relationship with the appliances so future changes from Orchestrator can override appliance-made configurations.
- If 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 Orchestrator templates before pushing out to the appliance.
 - All template-based configurations in 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 Orchestrator to ensure that cookie-cutter configurations are consistent across all appliances in an Orchestrator group or managed appliance.
 - If no configuration change is detected, 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 Orchestrator since the original version 8 release.

Feature	Description	Baseline Release
Adaptive DDoS	With this feature, users can configure baseline learnings in the Orchestrator UI from the Firewall Protection Profile tab or template. Adaptive DDoS also utilizes existing Stats Collector infrastructure to allow users to configure and report on the baseline computation cycle to a configured duration.	9.5.0
AppExpress Enhancements	Several improvements were made to AppExpress functionality, including the addition of a reporting component, pre-population of values for common applications during portal integration, and additions to the Flow Table and Business Intent Overlay UIs.	9.5.0
Availability KPI	The Availability KPI feature helps distinguish and segregate underlay traffic by service provider, helps determine whether your service providers are meeting their contracted Service Level Agreements (SLAs), and provides insight into your SD-WAN traffic.	9.5.0
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 bottlenecks, eliminates the need to configure complicated SSE policy manually, and fully automates sublocations based on label, zone, IP range, or address group.	9.5.0
Cluster Manager	Users can now sync user sessions on VRRP master appliances with VRRP backup appliances in real time. The Flow Redirection feature uses Cluster Manager infrastructure to sync flow redirection messages, offering secure synchronization of user sessions and flow redirection data. User session sync can happen in both traditional HA and EdgeHA environments.	9.5.0
DDoS Stats for Firewall Protection Profile	This feature provides stats and reporting functionality for the Firewall Protection Profile (FPP) feature in EdgeConnect Orchestrator. Users can now monitor their network behavior based on the DoS Threshold setting, providing visibility into FPP actions and establishing a baseline traffic profile for tuning thresholds, identifying violating sources, and enabling response actions.	9.5.0
IPS Enhancements	Several enhancements were made to Intrusion Prevention System (IPS) functionality, including the ability to preserve default rule actions of signatures in Signature Profiles and control automatic signature updates from Cloud Portal.	9.5.0
IPv6 SLAAC	This feature implements Stateless Address Auto-Config SLAAC IPv6 addressing of ECOS Gateway WAN interfaces, along with Stateless DHCPv6 for learning DNS server IPs. IPv6 SLAAC + Stateless DHCPv6 is the preferred address assignment method globally, offering superior performance vs. IPv4 transport networks.	9.5.0
LAN-Side EC-V Connectivity to AWS Transit Gateway and Cloud WAN	Users can now deploy two or more EC-Vs in Traditional HA mode in a VPC and establish BGP sessions with an AWS Transit Gateway (TGW) or a Core Network Edge (CNE). This feature is designed to extend the SD-WAN fabric to reach workloads and services deployed in AWS, enabling users to quickly establish LAN-side connectivity with their choice of AWS-native service and redirect traffic to the EdgeConnect instances.	9.5.0
Network Access Control (NAC)	Network Access Control (NAC) functionality has been added to the Orchestrator for devices and users, with focus on Layer 2 authentication types—802.1x and MAC—for physical and VLAN interfaces that may benefit from enhanced physical port security.	9.5.0

Feature	Description	Baseline Release
Orchestrator Server Log Viewer	This feature (Support > Reporting > Live Tail Logger) allows users to view live logs in the Orchestrator UI. The viewer opens a secure web socket connection with the server and attaches a custom appender with a log-level threshold filter to the loggers selected by the user. The custom appender sends logs over the web socket session and displays them in the terminal. Developers can link the Live Tail Logger to a feature of their choice by adding a hyperlink (to an existing feature) that redirects users to the Live Tail Logger and automatically starts the utility with the appropriate logs to view.	9.5.0
Stateful SNAT Exceptions	To increase flexibility in how NAT traffic is handled, users can now easily configure a list of prefixes that will not be translated by the WAN-side interface firewall and will be exempted from the Stateful-SNAT process. Users can import a global list of public IP ranges into the EdgeConnect Orchestrator, and these ranges will be applied automatically to all EdgeConnects.	9.5.0
Unified Fabric Orchestration	Aruba Central now orchestrates SD-WAN connectivity between ECOS and AOS devices, with ECOS devices acting as VPNCs (hubs). Users with an existing EdgeConnect SD-WAN deployment with sites that would benefit from the integrated LAN/WAN feature set of SD-Branch and Micro-branch can leverage this feature to deploy, manage, and connect all solutions.	9.5.0
VXLAN UI Enhancements	Several enhancements have been made to the Orchestrator UI to make VXLAN configuration and reporting easier, including fields on the Routes tab to support static VXLAN for local routes and a Details column on the VXLAN tab to provide information on the VXLAN's state.	9.5.0
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 popup 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
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 (GPIs) from Aruba CX Switches to facilitate identity awareness between Aruba Orchestrator and Aruba CX Switches.	9.4.1

Feature	Description	Baseline Release
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
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

Feature	Description	Baseline Release
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
VRRPv3	VRRP version 3 has been added to support IPv6, including the ability to set the advertisement timer in centi-seconds. There is now also the ability to include a free-form description of the VRRP instance.	9.3.0
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
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

Feature	Description	Baseline Release
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	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. NOTES <ul style="list-style-type: none"> 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. 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. 	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
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

Feature	Description	Baseline Release
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
Orchestration Performance Enhancements	This release adds a number of performance enhancements to significantly reduce orchestration times for most use cases.	9.1.2

Feature	Description	Baseline Release
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
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

Feature	Description	Baseline Release
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
Multiple Ranges for DHCP Server	DHCP Settings now support adding multiple IP address ranges under the DHCP Server options.	9.0.3

Feature	Description	Baseline Release
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

Feature	Description	Baseline Release
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
DSCP Marking per Interface	This feature allows the user to configure DSCP marking on tunnel packets, which is normally determined by QoS policy, to be overridden on a per WAN interface basis. You can configure DSCP Marking overrides on a per appliance basis using the QoS Policies tab or in the QoS Policies template.	8.10.15
Disable Cloud Portal Data Collection	This feature allows the user to disable automatic Cloud Portal data collection on all the appliances associated with their account.	8.10.15
Three-step OIDC Authorization for JWT	An optional, three-step authorization method can now be configured with JWT authentication. Admins can now configure an OIDC URL and Client Secret in the JWT authentication dialog. When configured, the browser will send Orchestrator an authorization code and secret, and Orchestrator will use these to retrieve the ID token to authenticate the user.	8.10.15
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.	8.10.15
Improvements in Zscaler ZEN Discovery	In this version, Orchestrator receives three ZEN nodes from the Zscaler API. From this list, Orchestrator will select the nodes that are in the same country as the local appliance.	8.10.15
Enhanced Cloud Portal and Orchestrator Authentication	The initial authentication between Orchestrator and Silver Peak Cloud Portal is now encrypted using the account key provided to Orchestrator, and subsequent communication will be encrypted using a new encryption key provided by the Portal.	8.10.12
IP SLA Enhancements	This version of Orchestrator supports the automatic creation of IP SLA rules for Zscaler tunnels. Additionally, for appliances running ECOS 9.1.x, loss and latency metrics for HTTP/HTTPS IP SLA are supported.	8.10.12
Allowed External IPs in Cloud Orchestrator	Cloud Orchestrator now provides support to allow connections from specific external IP addresses.	8.10.11
Support for Zscaler Sub-Locations	Sub-locations are now supported in the integration with Zscaler. In Orchestrator, sub-locations are LAN-side segments within each branch and can be identified by LAN interfaces, zones, or a collection of LAN subnets.	8.10.10
Integration with AWS Transit Gateway Network Manager (TGNM)	Orchestrator now supports association with AWS Transit Gateway Network Manager (TGNM), enabling you to securely connect your on-premises network or branch office to an Amazon Virtual Private Cloud (VPC).	8.10.10
New Route Redistribution Map Template	This release adds a new Route Redistribution Map template that can be applied to appliance SD-WAN fabric routing configurations.	8.10.10
Intelligent Upgrades via ZTP	When accepting a new appliance, Orchestrator will now verify version compatibility with ECOS software versions before suggesting that users upgrade the appliance.	8.10.0

Feature	Description	Baseline Release
Intelligent Upgrades and Downgrades	When upgrading appliances via Orchestrator, users can quickly see the total number of appliances on which the selected image is compatible, as well as on a per-appliance basis.	8.10.0
CSRF Protection	Changes have been made that greatly reduce or eliminate the possibility of a cross-site forgery request (CSRF) on Orchestrator.	8.10.0
Best Internet Breakout Enhancements	The internet breakout feature has been enhanced, enabling selection of the best quality internet link for local breakout based on user-defined criteria like performance thresholds.	8.10.0
Increased Interface Support on EC-V	Added UI support throughout Orchestrator to coincide with the increase to 32 supported interfaces on EC-V appliances.	8.10.0
Appliance Support for DHCPv6	Added Orchestrator UI support for IPv6 DHCP on WAN interfaces of Silver Peak appliances.	8.10.0
Custom Policy for Link Bonding	A new custom link bonding policy is available for Business Intent Overlays including configuration options based on multiple criteria including physical performance characteristics, link economics, link resiliency characteristics, and custom attributes.	8.10.0
Global Local Breakout IPSLA	A global local breakout IPSLA can now be configured from the BIO page.	8.10.0
Enhanced Local IPSLA Ping	The local IPSLA Ping monitor now supports loss & latency thresholds, and IPSLA Ping can be used to monitor a 3rd party tunnel.	8.10.0
YAML Support for New IPSLA Ping	YAML has been enhanced to support new loss & latency thresholds for IPSLA Ping.	8.10.0
Allowed External IPs in Cloud Orchestrator	Cloud Orchestrator now provides support to allow connections from specific external IP addresses.	8.9.11
Improvements in IPSec UDP Key Material Defaults and Configuration	In this release, to help ensure that tunnels in your SD-WAN network are not adversely affected by a conflicting configuration, the default lifetime for IPSec UDP key material is 0 (infinite).	8.9.10
Default RBAC Role for Full Appliance Access	RBAC users with read-write privileges now have access to Appliance Manager and Appliance CLI through Orchestrator.	8.9.10
JSON Web Token (JWT) Authentication	This Orchestrator release includes support for JWT-based authentication.	8.9.10

Feature	Description	Baseline Release
Websocket API option for Remote Log Receiver	A new websocket option has been added to Remote Log Receiver for streaming alarm or audit log information.	8.9.10
Aggregate Shaper Stats	This release adds a new Shaper Summary tab in Orchestrator for aggregated Shaper statistics, available under Monitoring > Bandwidth > QoS > Shaper Summary.	8.9.10
New Routes and Route Map Templates	This release adds a new Routes template and Route Map template that can be applied to appliance SD-WAN fabric routing configurations.	8.9.10
IKE-less Seed Distribution	To address CVE-2020-12142, the Orchestrator "Schedule IPSec Key Rotation" settings include a new option that lets administrators disable the persistence of key material on appliances.	8.9.2
Disable Self-signed Certificates	To address CVE-2020-12143 and CVE-2020-12144, new options in the Orchestrator "Advanced Security Settings" page let administrators force appliances to verify the certificate for Orchestrator and the Cloud Portal.	8.9.2
Loopback Orchestration	Users can now designate a pool of loopback addresses to be assigned automatically to appliances by Orchestrator.	8.9.0
Portal Migration Wizard	The Orchestrator 8.9.0 UI includes a wizard for helping customers verify connectivity and move to a new Cloud Portal address.	8.9.0
Auto-prune Tunnels from Removed Appliances	As an added level of security, if an appliance is removed from the network, all tunnels to that appliance will be removed.	8.9.0
Improved Response Times for Top 'X' Charts	Data used in Top 'X' charts is fetched in parallel from multiple appliances and loaded in an iterative fashion to enable large performance gains in all size deployments.	8.9.0
Support for New Alarm: Insufficient Bandwidth for Tunnels	In this release, Orchestrator will raise an alarm if an interface does not have enough available bandwidth to bring up tunnels.	8.9.0
OAuth 2.0 Support for Identity Access Management (IAM)	Support has been added for OAuth 2.0 and single sign-on services to use existing enterprise IAM solutions for Orchestrator user management. Additionally, Orchestrator RBAC roles can be associated with IAM users, including those serviced by RADIUS and TACACS+.	8.9.0
Control Auto-scaling in Scheduled Reports	Added a toggle called "Lock Scale for Trends" in the Schedule & Run Reports tab to let users enable or disable auto-scaling for trend graphs.	8.8.4
Check Point Integration	Automatic API-based integration support for service chaining to Check Point CloudGuard Connect cloud security service. You can build, orchestrate, maintain, and troubleshoot secure connectivity from EdgeConnect appliances to the Check Point cloud from the Orchestrator.	8.8.3
Zscaler Orchestration Improvements	Added improvements in Zscaler Orchestration to support load balancing of IPSec tunnels and support for new geo-location APIs in Zscaler ZEN selection.	8.8.3
Microsoft Virtual WAN Orchestration	<i>This feature is currently in Beta:</i> Automatic API-based integration support for connecting to Azure workloads using Azure Virtual WAN cloud service. You can build, orchestrate, maintain, and troubleshoot secure connectivity from EdgeConnect appliances to the Azure cloud from the Orchestrator.	8.8.3

Feature	Description	Baseline Release
Route Map Enhancements	Added support for route redistribution across the SD-WAN fabric, OSPF, and BGP domains with various options to match route attributes and deny or permit by changing the route attributes. Per BGP peer, inbound and outbound route-maps are supported, which allows matching BGP route attributes and deny or permit by setting BGP route attributes in the inbound and outbound direction.	8.8.3
Increased Capacity for Inbound Port Forwarding Rules	The limit for inbound port forwarding has been increased to support up to 100 rules.	8.8.3
IPFIX UI Enhancements	Added UI support to enable the export of IPFIX flow application performance and zone-based firewall information elements.	8.8.3
Bandwidth Tier Licensing	Added support for bandwidth tier licensing.	8.8.1
DHCP Failover	Added DHCP server failover support.	8.8.1
Tunnels to Hubs in other region	Ability to build tunnels from spokes of one region to hub(s) in a different region.	8.8.1
Notification Banner	Users can add a notification message that appears in the header.	8.8.1
Maintenance Mode	This feature adds appliances to maintenance mode. Orchestration and alarms are paused when appliances are in maintenance mode.	8.8.1
ASN and Local communities	Ability to add ASN and locally configured communities to subnet shared routes.	8.8.1
Reset flows confirmation	A confirmation dialog displays which shows the number of flows that are reset when users select Reset All Flows in the Flows tab.	8.8.1
Ikev2 enhancements	Ability to specify local and remote identifier for manually created IPSec tunnel using IKE v2.	8.8.1
Loopback & VRI in preconfig	Added loopback and virtual tunnel interface support in appliance preconfiguration.	8.8.1
PPPoE in preconfig	Added PPPoE support in appliance preconfiguration.	8.8.1
TACACS and RADIUS enhancements	Support "Remote only" and "Local if Remote Unavailable" authentication options.	8.7.0
Alarm Suppression	Orchestrator and Appliance alarms can be suppressed in the alarm tab.	8.7.0
Role based access	The Role Based Access Control feature adds fine-grained role-based authentication and access to features and functions. You can assign roles for every Orchestrator user. You can create a new role, modify an existing one or use one of the default roles. You can also customize appliance access for a user.	8.7.0
Works with Office365	Silver Peak's built-in automation with the Office 365 IP Address and URL Web service ensures that Unity Orchestrator receives continuous updates regarding Office 365 service endpoint domains and IP addresses. This is aligned in real-time with Microsoft's connectivity principles for the Office 365 service.	8.7.0

Feature	Description	Baseline Release
Redesigned BIO and regional overlays	The Business Intent Overlays tab has been redesigned to better support visibility across Overlays, and to allow more efficient work flows. Overlay settings can now be compared simultaneously for all overlays. Specific pending changes are highlighted for confirmation before being saved and applied. Policies for SD-WAN Traffic to Internal Subnets, and Breakout Traffic to the Internet and Cloud Services are now more clearly defined. Finally, Regional Topology differences are now displayed for easy interpretation.	8.7.0
VTI and Loopback Interfaces	Added support to create loopback and VTI interfaces.	8.7.0
Loop back interfaces in Appliance Wizard	Added capability to create loopback interfaces in appliance wizard.	8.7.0
Firewall logging	Added capability to configure the logging level for implicit firewall drop between zones.	8.7.0
Peer role in routes	Display peer role (hub/spoke) in routes.	8.7.0
ACL Policy enhancement	Allow user to match overlay or internet/non-internet in ACL/Policies, in addition to current criteria.	8.7.0
Source address for BGP	Added option to specify source address for BGP connections.	8.7.0
DHCP relay per VLAN	DHCP relay configuration is now per VLAN interface instead of per physical interface.	8.7.0
Branch NAT	Added Branch NAT configuration feature.	8.7.0
Firewall logging	Firewall logging for Security Policies	8.6.1
License Control	License revocation and grant support for metered license model.	8.6.1
Regions Tab	Dedicated tab to assign regions to appliances.	8.6.0
Verify Email Address	The email address verification is optional if Orchestrator is configured with a custom SMTP server.	8.6.0
Support Any Protocol in Inbound Port Forwarding	Accept traffic from any protocol with inbound port forwarding.	8.6.0
Zscaler Orchestration	Automated deployment of the Zscaler Cloud service that inspects web traffic and enforces security policies across appliances.	8.6.0
Flows Tab Improvement	Flows tab has been redesigned to provide a variety of new filters to further specify flows: Overlay and Transport filters, Flow characteristics, IP/Subnet and Port Source and Destination filters, Duration filters, Active/Ended filters, and various other checkboxes.	8.6.0
Routes Tab Filter	Users can now enter a subnet as a route filter when searching for routes from appliances.	8.6.0
Tech Support Tab Improvement	Support for downloading appliance tech support files to Orchestrator and uploading these files from Orchestrator to a Salesforce case. Also, filtered out tunbug files from the sysdump file list.	8.6.0
Firewall Logging	Ability to set the logging level for a firewall rule.	8.6.0

Feature	Description	Baseline Release
Multicast	Ability to configure multicast routing on appliances.	8.6.0
Suppress Tunnel creation	WAN labels can be configured to participate exclusively in a Hub & Spoke or Mesh network. Also, users can restrict tunnels from being built between pairs of appliances using the Tunnel Exceptions tab.	8.5
Zone based Firewall Statistics	Tab that shows zone-based firewall statistics.	8.5
BGP Graceful Restart	Added support for BGP Graceful Restart for 8.1.9.2 or above appliances. When enabled, if a BGP session peer goes down, the appliance will retain routes learned from the peer and use it for forwarding if possible.	8.5
New Route States	New routes states that indicate peer's role as Hub or Spoke.	8.5
Non-accelerated TCP Inactivity Timeout	Non-accelerated TCP inactivity timeout can now be configured from System tab or System template. This specifies how long a non-accelerated TCP connection can remain inactive before the flow is deleted.	8.5
IP Directed Broadcast	Added support for IP Directed Broadcast for 8.1.9.3 or above appliances. This configuration is available in both System tab and System template.	8.5
Preconfiguration Pass-through Tunnels and Flow Redirection	Third party pass-through tunnels and flow redirection configuration are now supported in preconfiguration YAML file.	8.5
Software Versions tab redesigned	Software Versions tab has been redesigned to group appliances by Active and Non-Active partitions.	8.5
Boost Trends	A new tab that shows historical boost usage.	8.5
Notes for interfaces on Deployment page	Users can now add a note to interfaces on deployment page.	8.5
Configurable tunnel alarm aggregation	When more than five tunnel alarms are triggered the Orchestrator aggregates this into a single alarm. This behavior is now configurable.	8.5
Support IPv6 internal subnets	Both IPv4 and IPv6 addresses can be configured as internal subnets.	8.5
Overlapping LAN side subnets	We added capability to specify an interface for route to support overlapping subnets on multiple LAN side interfaces.	8.5
Configurable Statistics Retention	Statistics retention periods are now configurable. An estimate of the disk space required for the retention duration is provided.	8.5
Preferred Routes	The ability to find the preferred route for a specific IP address. This is available via the row edit dialog in the Routes menu.	8.5
Health map sorting	The health map can be sorted by any of the health metrics – alarms/loss/latency.	8.5
Allow ECDSA certificates	Users can upload ECDSA certs for "SSL for SaaS (Custom CA Certificate)" and "SSL Certificates"	8.5

Feature	Description	Baseline Release
Preconfiguration	Providing the capability for per site VXOA appliance preconfiguration, in simple YAML formatted configuration file for rapid on-boarding.	8.5
Scalability & Speed	Speed of Orchestration of Overlays has been significantly improved.	8.5
MOS Statistics	MOS statistics are available for Overlays and Underlay tunnels.	8.5
Define Custom severity for Alarms	Users can override the default severity for Orchestrator and Appliance Alarms. This feature is available on the Alarms tab.	8.5
Delay Alarm Emails	Configure wait time for an alarm to clear before sending an email.	8.5
Backup Orchestrator to HTTPS or SFTP servers	Additional support for Orchestrator backup destinations - SCP FTP SFTP HTTP HTTPS.	8.5
Preconfiguration	Pre-define site-specific configuration using YAML files in Orchestrator before Zero Touch Provisioning occurs. Appliances can be associated with YAML preconfiguration files using a serial number or tag. This allows for Zero Touch Provisioning including automated software upgrade with minimal human involvement.	8.5
Wildcard-Based Prefix Matching in Policies	Adds support for wildcard-based IP/Subnet match criteria in all policies.	8.5
Block Network Orchestration via Cloud Portal	A new configuration item knob has been added to block network orchestration through the cloud portal as a relay. It is not recommended to block this communication.	8.5
Internet Breakout policy per Hub	The ability to breakout internet traffic differently at a hub site versus a spoke site; this is configured in the Business Intent Overlay tab.	8.4
Inbound port forwarding enhancement	Inbound port forwarding allows reachability to LAN-side branch devices from the WAN. Inbound port forwarding rules can be added via Configuration → Inbound Port Forwarding. Inbound port forwarding is limited to ten rules.	8.4
Overlay-Interface distribution chart	A new chart showing the distribution of traffic between: local breakout, overlays, and appliance interfaces. Pairwise combinations of the three dimensions can be viewed on a 'sunburst' chart which displays their interaction. The data can also be viewed in tabular form and in trend line charts.	8.4
Metered Boost	For EC-Metered licensed appliances, this feature allows users to specify Boost bandwidth independent from system maximum bandwidth.	8.4
User Defined SaaS Applications	This feature allows customers to define their own SaaS/Cloud applications that are not currently covered by Silver Peak's definition list by providing SaaS application's domain and a list of IP subnets that are hosting this domain.	8.4
SaaS Ping Interface using Interface Label	For assigning an interface for SaaS Optimization's RTT Pings, customers can now choose interface label besides interface names.	8.4
Overlay ACL	ACLs used in an overlay can now be defined in the Business Intent Overlay Definition tab itself. No need to push the ACLs via template. Overlay ACLs are automatically pushed when overlays are applied.	8.4

Feature	Description	Baseline Release
Maximum Orchestrator backups to retain	Users can configure the maximum number of Orchestrator backups that should be retained.	8.4
RMA Wizard	RMAed appliances can be automatically replaced with the new appliance using RMA Wizard on Orchestrator.	8.4
Upgrade appliances via Configuration Wizard	There is now an option to select the software version to upgrade the appliance to in the appliance wizard. When you finish the wizard, the appliance will first be upgraded and then the rest of the wizard steps will proceed. The list of possible software versions is the same as that in the "Upgrade Appliances" dialog.	8.4
New Tree filters	Unreachable appliances are greyed out in the tree. In addition to that, users can filter appliances in the tree that are unreachable, reachable only via Portal, or reachable via both channels.	8.4
SFP interface support	Added support to show transceiver information for EC-M-B and EC-M-P models' SFP interfaces.	8.4
Admin up/down datapath interfaces	UI support for admin up/down datapath interface.	8.4
Account Key Protection	User can now change EC account key from Orchestrator and apply across all appliances.	8.4
IP/Port wildcard pattern match	Policy match criteria now allows IP addresses to be specified with wildcard, or a range. Port can be specified with a range or a port string.	8.4
IPFIX Flow Export	Flow Exporting UI now includes IPFIX support in both Flow Export tab and templates.	8.4
IPSLA HTTP Ping	HTTP/HTTPS monitoring are now available for IPSLA.	8.4
Enable / Disable Default DNS Lookup	Cloud portal name lookup thru default DNS (8.8.8.8) can now be enabled/disabled thru System Information tab for appliances.	8.4
Auto-MTU Discovery Scheduler	Auto-MTO discovery can now be scheduled in Schedule Auto MTU Discovery dialog box.	8.4
Interface Dynamic Rate Control	Interface Dynamic Rate Control feature can be enabled/disabled in Shaper tab and template.	8.4
Compound Applications	Compound tab is added to Application Definition and user can use it to define more complicated multi-criteria applications. Previously defined UDAs are automatically imported during upgrade.	8.4
IPSec Pass-Through Tunnels	We now support IPSec pass-through tunnels for connecting to third-party appliances. The new "IPSec" mode can be found in Add Passthrough Tunnel dialog.	8.4
Pause Orchestration	Orchestration can be suspended for one or more appliances. This is mainly used for debugging purposes where you don't want Orchestrator to make any changes while the user is also making changes on Appliance. Once Orchestration is reestablished, all intended configuration changes will then be applied by Orchestrator to the appliance.	8.3
Configurable VLAN for Edge HA	The VLAN used to connect two Edge HA pairs can be configured.	8.2

Feature	Description	Baseline Release
SaaS Ping Interface	The interface via which SaaS pings are sent can be configured in the SaaS Optimization dialog and SaaS Optimization template.	8.3
Remove Network Manager role from Orchestrator	Orchestrator has only two privilege levels – Read only, Read-Write. Network Manager and Admin have the same privilege level – Read-Write. Network Monitor has Read-Only. To avoid confusion of having three roles to choose from, Network Manager role has been removed from Orchestrator	8.3
Unreachable Appliance indicator in Tree	Unreachable appliances are greyed out in the Tree.	8.3
OSPF	Orchestrator 8.3 introduces OSPF routing to allow Silver Peak's SD-WAN subnet-sharing protocol to share routes with traditional WAN routers. OSPF can advertise routes to traditional routers as well as learn routes from traditional routers. The primary use-cases supported are: <ol style="list-style-type: none"> Advertisement of Silver Peak SD-WAN subnets into an existing data-center router for the purposes of allowing traditional branch routers to gain reachability to Silver Peak SD-WAN branches. Learning branch routes from an existing large branch router that is subtending many subnets. 	8.3
Interface Bandwidth Summary report	Shows a summary of data across all the interfaces including inbound and outbound packets and bytes per second for each interface, as well as firewall denies.	8.3
Orchestrator in-place upgrade	Orchestrator will upgrade the current version's database. Since there is now only one copy of the database, it is highly recommended that users take a backup of the Orchestrator before initiating upgrade.	8.3
Appliance Flow Trends tab enhancements	Show packets and bps in Appliance Flows Trends tab.	8.3
Authentication protocols for TACACS and RADIUS	The following protocols are supported for RADIUS Server: <ul style="list-style-type: none"> PAP CHAP MSCHAP MSCHAPv2 EAP-MSCHAPv2 TACACS Server: <ul style="list-style-type: none"> PAP CHAP MSCHAP 	8.3
Alarms in CSV format	Alarms can be configured and sent in CSV or HTML format.	8.3
CLI shell from UI	Access appliance CLI from browser.	8.3
Remote assistance	Allow Silver Peak Support to access customer's appliances for a certain window of time.	8.3
TCP MSS clamping	Maximum TCP MSS clamping can be configured via System template.	8.3

Feature	Description	Baseline Release
Overlay Region Support	Users can separate their Overlay topology into different regions, allowing hubs of each region to connect to hubs in other regions.	8.3
Orchestration of Templates	Appliances will now be associated to template groups, and Orchestrator will keep all appliances synchronized with template changes.	8.3
Inbound Port Forwarding Orchestration	Inbound port forwarding allows traffic from the WAN to reach a specific computer or service within a private LAN when Silver Peak's stateful firewall is enabled.	8.3
Cross Connect Grouping	In the Overlay settings, different interfaces can now be split into separate cross connect groups to allow for greater scalability.	8.3
Controlling statistics collection	Users can control the type of appliance statistics they want Orchestrator to collect.	8.2
EdgeConnect High Availability	The EdgeConnect HA mode is a high availability cluster configuration that provides appliance redundancy by pairing two EdgeConnect devices together. Appliances can be put in a HA pair only via Orchestrator using the deployment dialog of either of the appliances. For both EdgeConnect appliances in a high availability cluster to share a common transport connection, you must set the tunnel type to IPSEC over UDP mode. Please see the Overlay Tunnel Settings in the Orchestrator.	8.2
AVC	<p>Application Visibility and Classification</p> <ul style="list-style-type: none"> • A scalable application identification framework which is data driven. It allows identification of new applications without code change. • Ability to customize application and application group definitions using Orchestrator. • Network wide application visibility and statistics. • Intuitive way to map applications and application groups to Business Intent Overlays to provide a specific treatment to application/application group traffic. • Classification of majority of the applications using the first packet of a flow. <p>We added a new page Application Definitions for customizing thousands of applications. For Orchestrator upgrade, we support migration of legacy application groups. You can access this feature by Legacy Groups Migration Wizard. After migration is completed, we provide a new UI for Application Group tab, which is located at Application Groups. Application Group template is no longer supported after migration. For new installations, no migration is needed.</p>	8.2
Tech Support improvements	Tech support tab has been enhanced to provide more robust experience. Appliance and Orchestrator Tech Support functionalities are separated out into dedicated tabs: "Tech Support-Appliances" and "Tech Support-Orchestrator"	8.2
Packets per second trends tab	A new tab that shows packets per second trends for tunnels.	8.2
IPSec UDP overlays	IPSec UDP overlays are more deterministic and reliable than traditional IPSec Overlays. IPSec UDP overlays must be configured via the Orchestrator.	8.2
Save Changes & Reboot required	These two indicators are removed from the Orchestrator header. Orchestrator now automatically saves changes on the appliance at regular intervals (every 5 mins by default). Reboot required can still be seen on the Appliance User Interface.	8.2

Feature	Description	Baseline Release
Cloud Portal template has been removed	Orchestrator automatically pushes the Account name and key to all appliances. A template is no longer required.	8.2
Login improvements	Orchestrator login password requirements have been strengthened to include a special character, a digit, and a minimum of 8 characters or more. Orchestrator now supports application based 2-factor authentication e.g. Google Authenticator	8.2
IP Whitelist	Orchestrator can be configured to restrict access only to a list of IP Addresses or subnets.	8.2
Site Dashboard	Site Dashboard provides a view of the mostly widely used information about the appliance in one single page on the Orchestrator. Some of these include Interface statistics, Overlay statistics, Application statistics, and Top flows. Users can simultaneously view multiple site's dashboards in different browser tabs.	8.2
Interface Charts	A new tab that shows bandwidth trends of all interfaces on the appliance.	8.2
IPSLA Rules for Internet breakout interfaces	Orchestrator automatically creates IPSLA rules on the appliance for all the interfaces used for Internet breakout in an overlay. The rule tells the appliance to ping the host sp-ipsla.silverpeak.cloud in the internet to decide if the internet connectivity via the interface is up/down and admin up/down the passthrough tunnel associated with that interface used to send traffic to internet.	8.1
Internet Gateways in an Overlay	Internet gateways (appliances that can send traffic out to the internet) in a network can be marked in the Business Intent Overlays page by making them hubs (both in Hub and Spoke and Mesh overlays). Other appliances in the network can then backhaul their internet traffic via these gateways.	8.1
Sitewide Dashboard (BETA)	A dashboard specific to an appliance. It shows interface charts, top apps, top overlays, flows etc., for a given appliance.	8.1
Templates editor	Template UI has been enhanced to provide a bit more clarity on which templates are part of template group and which ones are not.	8.1
Site health	The alarm banner in the Orchestrator header that showed alarm counts has been replaced with Site health. One can see how many sites are healthy and how many have alarms.	8.1
Internet Breakout	Overlay traffic can be segregated into internal traffic and internet traffic. Business Intent Overlays can be configured to break out Internet locally at a branch site or backhauled via the overlay or sent to an external site for service chaining.	8.1
Cross Connect selected WAN links	Users can cross connect selected WAN links in the Overlay. To provide redundancy in the event of a problem in the network, you can choose to cross-connect tunnels.	8.1
Non IPsec tunnels in the Overlays	The underlay tunnels inside an overlay can be in a combination of IPsec/gre/udp modes. In addition to that, users can also control various tunnel setting per WAN label. When overlays are in use, tunnel template are disabled. Tunnel properties are controlled in the Overlay Manager settings. Default mode for tunnels built in an overlay is IPsec.	8.1
Auto flow reclassify	Orchestrator controls how often appliances auto reclassify flows. The default is 60 sec. Setting the value to 0 disables auto flow reclassify.	8.1

Feature	Description	Baseline Release
Dashboard	Aims to integrate information from multiple components into a unified display. Shows license information, topology, health dashboard, top talkers, top domains etc., in one tab. Users can also customize the dashboard.	8.1
Dynamic Topology geo map	We've built a new dynamic topology map featuring: <ul style="list-style-type: none"> • Address lookup for geolocation of appliances • Map tile rendering to support variable detail at different zoom levels • Icon grouping to consolidate adjacent appliances (status is bubbled up, and grouping distance is configurable) 	8.1
Live View	Shows live bandwidth, loss, latency and jitter on all the tunnels. For an overlay, it also shows live tunnel states - up/brown/down. Live view can be accessed by clicking on a tunnel on the topology tab, as well as from the Monitoring > Tunnels and Configuration > Tunnels tabs.	8.1
Traceroute	Shows trace route information between the tunnel source and destination IP addresses. It shows intermediate hops, their IPs and latency between each hop. Traceroute view can be accessed by clicking on a tunnel on the topology tab, as well as from the Monitoring > Tunnels and Configuration > Tunnels tabs. For a given tunnel, trace route information is shown from both tunnel source and destination	8.1
Policy maps enhancements	8.1 greatly enhances application visibility with IP intelligence, domain name classification, and automatic classification of RTP traffic. VXOA 8.1 also adds wild-card matching (e.g. "*Netflix*") in match criteria.	8.1
BGP	Use this tab to configure BGP (Border Gateway Protocol) for appliances, and to add their BGP neighbors.	8.1
Flows tab enhancement	Flows can be filtered on domain matching.	8.1
Top talkers	This tab lists the IP addresses that use the most bandwidth.	8.1
Top Domains	This tab lists the domains that use the most bandwidth.	8.1
Top Countries	This tab lists the countries that use the most bandwidth.	8.1
Top Ports	This tab lists the ports that use the most bandwidth.	8.1
Tunnel Bandwidth Pie Charts	The Tunnel Bandwidth Pie Charts show what proportion of the bytes a tunnel consumes on the LAN and on the WAN. It shows traffic distribution across different overlays.	8.1
Appliance Flow Trends	The Appliance Flow Trends charts shows the number of flows through the appliance, over time. It also differentiates among TCP (accelerated and unaccelerated) flows and non-TCP flows.	8.1
DSCP Pie charts	The DSCP Pie charts show what proportion of the bytes are consumed by the top 10 DSCP markings on the LAN and on the WAN.	8.1
DSCP Trends	This tab shows DSCP usage over time.	8.1
QOS Summary	The Traffic Class Bandwidth chart shows which QoS traffic classes are sending the most data.	8.1
Traffic class Pie chart	The Traffic Class Pie charts show what proportion of the bytes are consumed by top 10 traffic classes on the LAN and on the WAN.	8.1

Feature	Description	Baseline Release
QOS drops/Shaper Trends	This tab shows traffic usage by a traffic class over time. It also shows the average wait time of packets in the shaper queue and packets drops associated with that shaper.	8.1
Enhanced Jitter Reporting feature	The Jitter chart shows which tunnels have the most Jitter. Jitter can be caused by congestion in the LAN, firewall routers, bottleneck access links, load sharing, route flapping, routing table updates and timing drifts. Jitter trends tab shows tunnel jitter over time. Jitter max and average tab shows max and average jitter in a given time range	8.1
HTTPS Certificates Upload template	The VXOA software includes a self-signed certificate that secures the communication between the browser and the appliance. You also have the option to install your own custom certificate, acquired from a CA certificate authority using this template to multiple appliances at once.	8.1
Customer SSL Certificate for Orchestrator	Orchestrator includes a self-signed certificate that secures the communication between the browser and the appliance. You also have the option to install your own custom certificate, acquired from a CA certificate authority using the "SSL Certificate Upload" dialog.	8.1
Discovered appliances tab enhancements	The Discovered Appliances tab now shows Geo Location information of the discovered appliance.	8.1
Deployment configuration tab	This report summarizes the appliance Deployment settings. The user can also edit the deployment configuration of any appliance managed by Orchestrator.	8.1
DHCP Leases by Appliance	This page lists which IP addresses are currently being leased from the DHCP pool.	8.1
Built-in Applications	A new tab that shows built in applications defined on appliance.	8.1
Overlay Manager controls	Several knobs have been added to control the behavior of Overlay Manager. <ul style="list-style-type: none"> • Auto Flow Re-Classify timeout – Default 60 sec • Polling interval – Default 5 mins • Reset all Flows upon applying overlays 	8.1
Overlay boost behavior	The boost button on the Overlay configuration page no longer creates a single optimization map entry for the overlay. If Overlay is enabled, the system will simply instruct the appliance to consult the optimization map. However, this behavior is not present on appliances running 8.0 with Orchestrator 8.1 installed. In this scenario, the boost button will appear to do nothing. We now require that you to obtain a boost license and create the required optimization maps. The main difference between 8.0 and 8.1 appliances is the optimization maps are looked up per overlay if boost is set in 8.1 but in 8.0, if an appliance has a boost license, optimization maps are always looked up. The Orchestrator will delete any optimization map entries it previously created for overlays (priority 20000+) when it synchronizes with appliances, but no longer deletes other optimization map entries. A template defining your optimization policy requirements should be created and pushed out to your appliances to engage the boost feature correctly.	8.1
Disabled Rediscovery of Deleted Appliances	Appliances that are deleted from Orchestrator will be not rediscovered. The appliance will be moved under denied list.	8.1

Feature	Description	Baseline Release
Orchestrator license key is optional	Orchestrator license key is optional for Orchestrators registered with Silver Peak Cloud Portal with a valid an account having valid Edge Connect license	8.1
Second Orchestrator	<p>Second Orchestrator to be used during migrating Orchestrator. This is not for Orchestrator redundancy. At any given time, only one Orchestrator should be active except during approving the second Orchestrator.</p> <p>First Orchestrator for a given account is auto approved to discover appliances. Second Orchestrator using the same account will be discovered as a device on the first Orchestrator. It won't discover appliances until it is approved on the first Orchestrator. This provides protection against a malicious user trying to bring up a second orchestrator and take over the network.</p>	8.1
Enhance Applicable Charts to include Overhead Traffic	Overhead bytes are Silver Peak tunnel headers that go along with actual payload. All charts now show the actual data on the wire (payload + overhead bytes) by default.	8.1
Labels	WAN and LAN labels will be applied to all the appliances whether Business Intent Overlays are applied or not.	8.1
Orchestrator backup failure alarm	Orchestrator raises an alarm when backup fails	8.1
Orchestrator reachability	<p>Appliances connect to Orchestrator differently based on the characteristics of the interface they're using to communicate (for example, via internal or external networks). You can specify how each type of appliance interface (using its Label) should connect to the Orchestrator.</p> <p>This is supported on appliances v8.1.2 and above</p>	8.1
Flows are categorized based on Domain, Location	Flows tab shows domain, location and IP Intelligence for flows	8.1
Session timeout and max user sessions	<p>Users login sessions can be configured to timeout after a certain period.</p> <p>The number of Orchestrator users that can be simultaneously logged in can be configured.</p>	8.1
Two-factor authentications	Two-factor Authentication can be enabled on user accounts. Two-factor passcodes will be sent by email.	8.1
User-Resettable Password	Users can reset their passwords from the login page.	8.1
Schedulable Alarm Email Notifications	Orchestrator emails appliance alarms. Send these appliance alarms in Orchestrator's scheduled timezone.	8.1
Search Menu items	A search bar to search menu items	8.1
Show user sessions	A new tab on Orchestrator that shows existing Appliance and Orchestrator user sessions. You can see view all logged-in Orchestrator and Appliance users at any given time	8.1
Appliance Routes	A new tab on Orchestrator that shows Appliance routes	8.1
Turn ON/OFF Alarm notification	Alarms tab has an ON/OFF button to control sending alarm emails.	8.1

Feature	Description	Baseline Release
Allow non-default users in User template	Enhance 'Default users' template in Orchestrator to allow users to add new users for appliance	8.1
Tree search	Appliances can be filtered in Tree based on hostname or IP address.	8.1
Default Overlays	Newly installed Orchestrator now comes with 3 default overlays.	8.1
Simplified Shaper Template	Shaper template is now meant to be used only to apply traffic class changes. Max bandwidth, Dynamic Rate Control and Passthrough shaped bandwidth have been removed from the template	8.1
Configurable SMTP port	Orchestrator can be configured to talk to a SMTP server on any port.	8.1
Google maps	The existing map has been replaced with Google maps on Orchestrator. Topology, Live view and all other places which displayed information on a map now utilizes Google maps.	8.1
Jitter max and average	A new tab on Orchestrator that show max and average jitter in a given time range	8.1
Configurable Security Communication	Cipher suites and SSL protocols that Orchestrator web server will listen to can be configured in Advanced Properties menu. This allows the user to configure the Orchestrator to only listen on TLS 1.2. Please note that disabling TLS 1.0 on Orchestrator versions prior to 8.1.12 will prevent the Orchestrator from being able to upgrade the appliances. To work around this, either upgrade appliances individually or temporarily re-enable TLS 1.0.	8.1
Business Intent Overlays	Business Intent Overlays virtualize all underlying transports and segment the WAN allowing for different policies to be applied per application or application group. Business Intent Overlays are described at a high-level and are applied enterprise wide. The components of the Overlays include the access policy, logical topology, link bonding and QoS policies.	8.0
Health Dashboard	The Health Dashboard provides a high-level view of your network's health, based on the filter thresholds you configure. If you are using overlays, you can view each overlay's health individually.	8.0
Deployment Profiles	Deployment Profiles to abstract the personality of EdgeConnect devices. Deployment Profiles assign labels with global (SD-WAN fabric-wide) semantics to the underlying physical transports (for example, "MPLS" and "Internet"). Deployment Profiles can be applied at the time a new EdgeConnect device is Zero Touch Provisioned and ensure consistent configuration of network policies without configuration drift due to manual box-by-box configuration.	8.0
Overlay Topology	Topology tab can show topology of appliances per overlay/all overlays/all underlays.	8.0
Tunnel charts can be viewed per overlay	All the tunnel trends and aggregate charts can show top tunnels per overlay/all overlays/all underlays.	8.0
Reporting enhancements	All the time series charts in Orchestrator can be included in reports. Reports can be run per overlay. Health dashboard can also be included in the reports.	8.0
Labels	Labels can be created and assigned globally (SD-WAN fabric-wide) to the underlying physical transports (for example, "MPLS" and "Internet").	8.0

Feature	Description	Baseline Release
Tunnel Groups	<p>Orchestrator 8.0 replaces Tunnel builder with Tunnel Group</p> <p>A Tunnel Group consists of a set of appliances, paired with a configuration that defines how to build tunnels among them. Orchestrator automatically builds these tunnels in the background. Tunnel groups are self-healing. If a change is made to an IP address (as with DHCP) or to a Label, those changes propagate appropriately through the tunnel groups.</p> <p>If you're not using Overlays, then you can use this page to create Tunnel Groups.</p> <p>All tunnels built by Orchestrator for a tunnel group will only be IPSec tunnels.</p>	8.0
Shaper template	Shaper template supports both inbound and outbound shapers.	8.0
Policy templates (route maps, opt maps, qos maps, nat maps)	All the policy maps (route map, qos map, opt map, and nat map) rules can be matched on a label.	8.0
ACL template	ACLs can be created with label as the match criteria.	8.0
Cloud portal template	Orchestrator has been enhanced to auto push Cloud portal registration information to all appliances hence the registration information has been removed from Cloud Portal template.	8.0
VRRP Template	Use this template to distribute common parameters for appliances deployed with Virtual Router Redundancy Protocol (VRRP).	8.0
Tunnel template fast fail thresholds	Tunnels template has been enhanced with additional fast fail threshold parameters – latency, loss, jitter.	8.0
Shaper report	Use this tab to create and view both inbound and outbound shapers of appliances.	8.0
Audit Log tab	This is a new tab in Orchestrator which shows all the audit logs. It also lists all the changes being performed by Orchestrator on appliances when applying Overlays.	8.0
Appliance Configuration history	All the appliance's configuration will be backed up every day in Orchestrator. You can view the configuration or compare any two configurations.	8.0
Deployment Report	A new report that shows deployment configuration of each appliance managed by Orchestrator.	8.0
Bulk import subnets from CSV file	Orchestrator now allows for subnets to be imported from a .csv file and applied to a branch site.	8.0

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: 28916. An issue with auto-updating cloud portal configurations caused classification data alarms to appear erroneously in the Orchestrator UI.	9.5.0
ID: 28320. Orchestrator file upload was not working as expected when legacy API support was enabled.	9.5.0
ID: 27773. Portal data downloaded for IP intelligence and backups were in conflict, leading to backups not being created as expected.	9.5.0
ID: 27772. Because the cipher list for SFTP/SCP was hardcoded, users could not use or restrict ciphers on the appliance.	9.5.0
ID: 27505. A missing field in the request body for the /users/resetPassword API route prevented users from completing the password reset process successfully.	9.5.0
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.	9.5.0
ID: 26903. Orchestrator's syslog client module was not removing control characters before sending to the syslog server, resulting in formatting errors in the log output.	9.5.0
ID: 26898. A redundant checkbox in the Routes template UI caused conflicts with route maps.	9.5.0
ID: 26728. An updated query on historicaljob2 timed out, causing systemd to restart the gms server every 30 minutes.	9.5.0
ID: 26529. A UI typo on the Built-in Policies page was corrected.	9.5.0
ID: 26309. The upper limit validation for the "max bw:absolutely" shaper setting was set too low.	9.5.0
ID: 25779. Duplicate AVC domain entries caused traffic to behave unexpectedly.	9.5.0
ID: 25616. Orchestrator could not verify custom firewall certificates from AWS.	9.5.0
ID: 25540. Hint text on the Remote Authentication Server configuration page in the UI caused issues when attempting to log in via SAML.	9.5.0
ID: 24086. IP Allow List instructions in the UI were incorrect for Orchestrator-as-a-Service deployments.	9.5.0
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
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: 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

Issue	Earliest Release to Fix
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
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 sub-attribute 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

Issue	Earliest Release to Fix
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
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: 22790. CVE-2022-42889 does not affect the Orchestrator because Orchestrator does not use the affected code. However, Orchestrator has been patched for this vulnerability.	9.4.1
ID: 21430. The autocomplete attribute in Orchestrator was not disabled for passwords.	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
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

Issue	Earliest Release to Fix
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: 23834. A field validation issue created a potential cross-site scripting vulnerability.	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: 23569. An issue in the /gms/rest/stats/debugStats path created the potential for an SQL injection vulnerability.	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: 23315. A validation issue on the Orchestrator login page created the potential for a cross-site scripting vulnerability.	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: 22793. This release was patched to address CVE-2020-36518, CVE-2022-42003, and CVE-2022-42004.	9.3.0
ID: 22618. Addresses a security vulnerability. Customers are urged to upgrade to this version. Details of this vulnerability will be published at a later time.	9.3.0
ID: 22352. ACLs in route maps were not being applied successfully due to a misconfiguration in certain templates.	9.3.0
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: 21795. A validation error allowed a user session to continue even after the user's password had been changed.	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

Issue	Earliest Release to Fix
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
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

Issue	Earliest Release to Fix
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
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

Issue	Earliest Release to Fix
ID: 22027. Application search by IP failed on Application Definitions tab.	9.2.1
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
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

Issue	Earliest Release to Fix
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
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

Issue	Earliest Release to Fix
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
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
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

Issue	Earliest Release to Fix
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
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

Issue	Earliest Release to Fix
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
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

Issue	Earliest Release to Fix
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
ID: 19839. On some HA tunnels, DSCP markings were being overwritten when viewed on the partner appliance.	8.10.17
ID: 19721. Accounts were not being locked out as expected after too many failed authentication attempts.	8.10.17
ID: 19720. An application was returning passwords in HTTP server responses in RADIUS and TACACS+ API calls.	8.10.17
ID: 19636. An issue in the UI was causing a specific device to not show up in Orchestrator's Security Policies tab.	8.10.17
ID: 19629. On some appliances, the "Failed to apply overlay ACLs" alarm was constantly being logged, though no error seemed to be present.	8.10.17
ID: 19620. When logged in with RBAC, users were unable to upload an appliance image file in the Upgrade Appliances tab.	8.10.17
ID: 19601. An existing address map was overwritten by a new address map, causing a network outage. In this and future releases, Orchestrator will display a warning message if a new address map will overwrite an existing one.	8.10.17
ID: 19336. In some cases, monthly maintenance alerts were being logged almost hourly.	8.10.17
ID: 18895. Manually resetting all flows in the SD-WAN fabric caused a brief outage that was hard to troubleshoot since flow reset actions were not recorded in the audit log. In this and future releases, details such as user, number of flows, and flow operation are saved in the audit log.	8.10.17
ID: 19676. Orchestrator was running out of threads and unable to deploy Zscaler tunnels, and the operation continued to fail each time Orchestrator tried again.	8.10.16
ID: 19633. DHCP failover settings were being cleared and not saved after being applied on the appliance or Orchestrator deployment page.	8.10.16
ID: 19582. The connection to Cloud Portal was getting closed after registration, resulting in timeouts on certain appliances when trying to apply preconfig templates.	8.10.16
ID: 19490. In some cases, Orchestrator was taking too long to display any information when opening the Schedule & Run Reports tab.	8.10.16
ID: 19487. Cloud Orchestrator was no longer sending alerts to an external collector, even though the same configuration had been working previously.	8.10.16
ID: 19365. This release fixes a known issue with using the QoS Policies template for DSCP Marking Override.	8.10.16
ID: 19276. Orchestrator reachability details and server information were not being restored properly following a backup and restore.	8.10.16
ID: 19233. In rare cases, unreachable appliances were not being displayed in the tree view for a local admin user but were showing up for other local users.	8.10.16
ID: 19230. IPSec UDP key activation was failing on some appliances because key rotation and forced activation were happening at the same time. Additional information was added to the Orchestrator UI to help avoid these issues in the future.	8.10.16
ID: 19123. Configured email recipients for alarm notifications had gotten corrupted, so Orchestrator notifications stopped being sent.	8.10.16
ID: 18854. An issue with an empty string in in a YAML preconfiguration file was causing Orchestrator to match the wrong file for an appliance.	8.10.16
ID: 18806. The Max Bandwidth line was missing from interface bandwidth trend charts only when the reporting period was set to seven days (7d).	8.10.16
ID: 19220. Preconfiguration was failing because no value had been entered for the password field. This was converted to a null value, and the appliance did not accept it.	8.10.15

Issue	Earliest Release to Fix
ID: 19158. In the case where there are many appliances in the denied appliances list, some appliances discovered by ZTP were showing a reachability status of "UNKNOWN" on Orchestrator.	8.10.15
ID: 19118. Orchestrator would not push an overlay configuration to an EdgeHA appliance that was using an LTE interface and did not have a public IP.	8.10.15
ID: 18931. A change in advanced security settings was causing the upgrade from Orchestrator 8.9.11 to fail. Orchestrator 8.9.11 can only be upgraded to 8.10.15+ or 9.0.4+.	8.10.15
ID: 18930. Orchestrator was reusing NAT pool IDs when deleting and adding new pools, which could cause an appliance to reboot unexpectedly.	8.10.15
ID: 18871. When the Zscaler response for activation requests was failing with a "401 password expired," Orchestrator was continuing to retry with the same request and eventually failed because the payload was too large.	8.10.15
ID: 18858. When running a single report with a custom time range under the Schedule & Run Reports tab, the page did not refresh, and the report eventually timed out without completing.	8.10.15
ID: 18845. The /appliance API was returning an incorrect HA peer.	8.10.15
ID: 18838. Due to a version incompatibility issue, BGP peers could not be added from the Add Peer dialog in Orchestrator and had to be added from the Appliance UI.	8.10.15
ID: 18829. In some cases, enabling Source and Destination NAT was causing appliances to lose connectivity and reboot unexpectedly.	8.10.15
ID: 18828. When LTE backup links were shared by more than one appliance, the appliances shared the same public IP. Attempting to push overlay changes to these appliances was failing with a duplicate IP error.	8.10.15
ID: 18730. In some cases, the link integrity test could not be run from the Orchestrator UI because Orchestrator thought the test was already running, but it was not.	8.10.15
ID: 18718. When attempting to upgrade an appliance from Orchestrator, the "Upgrade" button was greyed out. This was due to a previous appliance upgrade job that had an incomplete status.	8.10.15
ID: 18558. In some cases, Orchestrator's WebSocket connection to Cloud Portal was going down after the registration service stopped. The only way to restore the connection was to reboot Orchestrator.	8.10.15
ID: 18373. Following the upgrade to Orchestrator 8.10.11, empty entries in the preconfiguration file were causing preconfig to fail.	8.10.15
ID: 18681. As a result of the authentication mechanism used by Orchestrator tenants when signing in via Orchestrator-SP, some components of the UI were becoming extremely slow.	8.10.14
ID: 18661. In rare cases, adding or renaming a hub site caused all tunnels to go down and need to be rebuilt.	8.10.14
ID: 18618. Following the upgrade to 8.9.12, Orchestrator was trying to connect to appliances via web proxy, if configured.	8.10.14
ID: 18579. In some cases, users were unable to add or delete rules in the Zscaler Gateway Options dialog. Orchestrator was failing with the "Failed to update Zscaler location config: Appliance is required" error.	8.10.14
ID: 18555. Some values for metric and comment did not match what was specified in pre-config after being pushed to the appliance.	8.10.14
ID: 18512. On rare occasions, after changing the IP on a WAN interface, orchestration was getting stuck in a pending state without finishing changes across the network. Restarting Orchestrator was the only workaround.	8.10.14
ID: 18461. Wildcards for subnets were not supported in the match criteria for Zscaler sub-locations (Gateway Options).	8.10.14
ID: 18409. When exporting the Loss Summary report to CSV, Post-FEC Loss statistics were not being included.	8.10.14
ID: 18391. Users were unable to add an application definition using a domain that included a wildcard (*).	8.10.14
ID: 18555. Some values for metric and comment did not match what was specified in pre-config after being pushed to the appliance.	8.10.13

Issue	Earliest Release to Fix
ID: 18512 On rare occasions, after changing the IP on a WAN interface, orchestration was getting stuck in a pending state without finishing changes across the network. Restarting Orchestrator was the only workaround.	8.10.13
ID: 18397. Following the upgrade to 8.9.11, logins via RADIUS authentication were failing.	8.10.12
ID: 18396. When providing an HTTPs URL for Orchestrator backups, parameters were not supported in the URL.	8.10.12
ID: 18384. After upgrading Cloud Orchestrator to 8.10.11, appliance upgrades were failing with a generic "internal server error."	8.10.12
ID: 18379. Orchestrator was generating an empty Application Bandwidth report.	8.10.12
ID: 18352. When attempting to add a new SaaS application definition, the application definition pop up dialog was failing with a console error.	8.10.12
ID: 18339. Orchestrator was raising alarms for appliance features that were not configured or not supported in a specific appliance software version.	8.10.12
ID: 18299. Zscaler tunnels were not building to new devices following the upgrade to Orchestrator 8.10.11.	8.10.12
ID: 18205. When configuring an appliance with a region without enabling regional overlays, an alarm recommended that users turn on regional routing. This alarm description has been modified to help ensure users understand the potential impact of enabling regional routing.	8.10.12
ID: 18189. Zscaler tunnels were taking too long to build unless users manually resubmitted subscription credentials.	8.10.12
ID: 18186. On occasion, ACLs for the realtime overlay fail to load in the Business Intent Overlays window.	8.10.12
ID: 18139. When using tunnel groups instead of Overlays, IPsec UDP seed orchestration was generating an exception.	8.10.12
ID: 18112. Ended flows were not showing up in the Flows table if a custom filter within the last 24 hours was applied, but they were showing up when filtered for the last 24 hours.	8.10.12
ID: 18069. When expanding the list of available templates, the list appears offscreen if its contents are long enough that users would have to scroll through them.	8.10.12
ID: 18031. Following a reboot, some appliances did not appear as online in Orchestrator for approximately 20 minutes, even though appliance uptime was approximately 15 minutes.	8.10.12
ID: 17985. Orchestrator was failing to connect to Zscaler, and users were forced to manually enter account credentials again to restore the connection.	8.10.12
ID: 17866. If an HTTPs log receiver was configured on Orchestrator prior to adding Okta as an OAuth provider, OAuth logins were failing with an invalid client_id value.	8.10.12
ID: 17748. On rare occasions, users were unable to approve an appliance because its status was "Upgrading," even after upgrading locally and rebooting.	8.10.12
ID: 18150: In previous releases, it was possible to expose Orchestrator's internal IP address while accessing its translated IP.	8.10.11
ID: 18147: Removed an API route that could allow an authorized user to make MySQL database queries.	8.10.11
ID: 18146: The implementation of an API route exposed Orchestrator to a potential path traversal vulnerability.	8.10.11
ID: 18145: Fixed an issue that could allow the subversion of Orchestrator authentication.	8.10.11
ID: 17745. If the appliance tree was filtered for a single appliance in a group, that single appliance could no longer be selected individually because the group to which the appliance belonged was automatically selected.	8.10.10
ID: 17580. The field length for email addresses and user names had been limited to 40 characters. This has been expanded to 512 characters.	8.10.10
ID: 17488. The Interface Summary table did not include data for inbound/outbound average and maximum bandwidth utilization. These have now been added.	8.10.10
ID: 17474. If a new appliance was approved from the Silver Peak Cloud Portal, the same appliance was not being marked as "Approved" in Orchestrator.	8.10.10

Issue	Earliest Release to Fix
ID: 17118. Some tenant daily bandwidth reports with HA were not reporting correctly, and the data in some daily bandwidth reports for a tenant did not match the parent-level daily bandwidth report.	8.10.10
ID: 17908. IPSec UDP key material lifetime on a new Orchestrator was not long enough. This lifetime has been increased to three months.	8.10.2
ID: 17883. Even though Boost was enabled in the Business Intent Overlay, traffic matching that overlay was not getting boosted.	8.10.2
ID: 17774. Resource limit errors were getting logged during the upgrade to 8.10.0, and the Orchestrator service would not start following the upgrade.	8.10.1
ID: 17003. Access to the Orchestrator UI was lost after applying SSL certificates on the Orchestrator host.	8.10.1
ID: 17472. IPSec UDP key material was not available when a new Orchestrator was first initialized, causing tunnels to go down when key material rotation is enabled.	8.10.0
ID: 17222. In some cases, Cloud Orchestrator was not sending email alerts for alarms.	8.10.0
ID: 16944. If an IP change disrupts Portal connectivity during provisioning or preconfiguration of an appliance, the wizard will try to reapply the configuration before abandoning the process with an error.	8.10.0
ID: 16879. When using the Date/Time template in the Default Template Group, date/time was not being set as expected and the list of NTP servers in the template was empty.	8.10.0
ID: 16878. When outbound bandwidth was summed to a value that exceeded the MINI license (50M), the license was changing to BASE+Plus instead of BASE.	8.10.0
ID: 16796. A read only user assigned the predefined monitor role was unable to export the Appliance Bandwidth Trend report, but other reports could be exported as expected.	8.10.0
ID: 16769. Deleting an unused template was causing all default templates to be applied unexpectedly.	8.10.0
ID: 16679. Selecting the Appliance -> Synchronize option for an appliance selected in the device tree, only a "No Data Available" message was being displayed.	8.10.0
ID: 16510. In some cases, the REST API was returning data from renamed or deleted appliances.	8.10.0
ID: 17882. Flows matching an allow rule were getting denied after matching the default rule, which denied them.	8.9.10
ID: 17856. Following the upgrade to 8.3.0.5, changes in IPSec UDP key material settings caused the current seed to expire before Orchestrator generated a new one, causing tunnels to go down.	8.9.10
ID: 17855. Application charts were reporting smaller values when using a custom period of 24 hours versus when using the built in one day option.	8.9.10
ID: 17803. An overlay that is not present in the BIO is available when applying overlays.	8.9.10
ID: 17718. Following the upgrade to 8.3.0.5, the new IPSec UDP seed was not getting activated, causing tunnels to go down at some sites. Tunnels came back up following an appliance reboot.	8.9.10
ID: 17691. Orchestrator was generating an "Only IPSEC UDP tunnel mode is supported on Edge HA devices," even though only IPSec UDP tunnels were in use.	8.9.10
ID: 17659. Remote authentication methods did not include a default role.	8.9.10
ID: 17656. Cloud Orchestrator was unresponsive when trying to establish a database connection. The connection method did not utilize a timeout, so Orchestrator needed to be restarted.	8.9.10
ID: 17603. In some cases, OAuth users with read-write access were getting access denied errors for some operations or getting logged out of Orchestrator automatically after a short period of time.	8.9.10
ID: 17567. In Template Groups, when setting the match criteria in a security policy rule to an interface, the specified interface was changing to "Everything" after the template group is saved and refreshed.	8.9.10
ID: 17538. Following the upgrade to Orchestrator 8.9.x, RADIUS users were being asked to manually select the RADIUS option at every login attempt.	8.9.10
ID: 17501. In some cases, appliance upgrades were failing because the image could not be verified. Some logs were showing a successful download before 100%, and some image installs were failing.	8.9.10

Issue	Earliest Release to Fix
ID: 17491. The Role Based Access Control (RBAC) screen did not include a refresh button.	8.9.10
ID: 17472. IPSec UDP key material was not available when a new Orchestrator was first initialized, causing tunnels to go down when key material rotation is enabled.	8.9.10
ID: 17295. Sorting by Avg. Boost Bytes was not working in the table on the Boost summary page.	8.9.10
ID: 17222. In some cases, Cloud Orchestrator was not sending email alerts for alarms.	8.9.10
ID: 16796. A read only user assigned the predefined monitor role was unable to export the Appliance Bandwidth Trend report, but other reports could be exported as expected.	8.9.10
ID: 16769. Deleting an unused template was causing all default templates to be applied unexpectedly.	8.9.10
ID: 16510. In some cases, the REST API was returning data from renamed or deleted appliances.	8.9.10
ID: 16067. When trying to enable EdgeHA from Orchestrator via the appliance deployment option in the tree view, an error indicated that Orchestrator was unable to get the appliance license state.	8.9.10
ID: 17882. Flows matching an allow rule were getting denied after matching the default rule, which denied them.	8.9.10
ID: 17856. Following the upgrade to 8.3.0.5, changes in IPSec UDP key material settings caused the current seed to expire before Orchestrator generated a new one, causing tunnels to go down.	8.9.10
ID: 17855. Application charts were reporting smaller values when using a custom period of 24 hours versus when using the built in one day option.	8.9.10
ID: 17803. An overlay that is not present in the BIO is available when applying overlays.	8.9.10
ID: 17718. Following the upgrade to 8.3.0.5, the new IPSec UDP seed was not getting activated, causing tunnels to go down at some sites. Tunnels came back up following an appliance reboot.	8.9.10
ID: 17691. Orchestrator was generating an "Only IPSEC UDP tunnel mode is supported on Edge HA devices," even though only IPSec UDP tunnels were in use.	8.9.10
ID: 17659. Remote authentication methods did not include a default role.	8.9.10
ID: 17656. Cloud Orchestrator was unresponsive when trying to establish a database connection. The connection method did not utilize a timeout, so Orchestrator needed to be restarted.	8.9.10
ID: 17603. In some cases, OAuth users with read-write access were getting access denied errors for some operations or getting logged out of Orchestrator automatically after a short period of time.	8.9.10
ID: 17567. In Template Groups, when setting the match criteria in a security policy rule to an interface, the specified interface was changing to "Everything" after the template group is saved and refreshed.	8.9.10
ID: 17538. Following the upgrade to Orchestrator 8.9.x, RADIUS users were being asked to manually select the RADIUS option at every login attempt.	8.9.10
ID: 17501. In some cases, appliance upgrades were failing because the image could not be verified. Some logs were showing a successful download before 100%, and some image installs were failing.	8.9.10
ID: 17491. The Role Based Access Control (RBAC) screen did not include a refresh button.	8.9.10
ID: 17472. IPSec UDP key material was not available when a new Orchestrator was first initialized, causing tunnels to go down when key material rotation is enabled.	8.9.10
ID: 17295. Sorting by Avg. Boost Bytes was not working in the table on the Boost summary page.	8.9.10
ID: 17222. In some cases, Cloud Orchestrator was not sending email alerts for alarms.	8.9.10
ID: 16796. A read only user assigned the predefined monitor role was unable to export the Appliance Bandwidth Trend report, but other reports could be exported as expected.	8.9.10
ID: 16769. Deleting an unused template was causing all default templates to be applied unexpectedly.	8.9.10
ID: 16510. In some cases, the REST API was returning data from renamed or deleted appliances.	8.9.10
ID: 16067. When trying to enable EdgeHA from Orchestrator via the appliance deployment option in the tree view, an error indicated that Orchestrator was unable to get the appliance license state.	8.9.10

Issue	Earliest Release to Fix
ID: 17425. In larger networks, the browser was freezing or becoming unresponsive while the Dashboard tab loaded.	8.9.4
ID: 17408. Upgrades or migrations were prone to issues if the Blueprint Export was taken when Orchestrator was not idle or stopped.	8.9.4
ID: 17431. If IPSec UDP key material had been rotated since taking an Orchestrator backup, restoring that backup was causing tunnels to go down temporarily.	8.9.3
ID: 17317. Some websocket messages were not being parsed correctly, resulting in deserialization errors in Orchestrator logs and temporary issues with appliance reachability.	8.9.3
ID: 17281. Template history was not getting cleared completely, resulting in increased CPU usage by MySQL over time.	8.9.3
ID: 17327. In some cases, users were getting an authentication failed message even after resetting the password.	8.9.2
ID: 17003. Access to the Orchestrator UI was lost after applying SSL certificates on the Orchestrator host.	8.9.2
ID: 17029. On rare occasions, an exception in TaskDispatcher or StatsTaskManager was causing Orchestrator to restart unexpectedly.	8.9.1
ID: 16997. In certain deployments, an exception was being thrown if tunnel settings were not enabled for an interface label.	8.9.1
ID: 16960. Searching the appliance tree using the full group name was failing to return results.	8.9.1
ID: 16949. In some cases, if an appliance was generating an excessive amount of alarms, a queueing exception could close the connection to the appliance, which then became unreachable.	8.9.1
ID: 16922. In large networks, there was a significant delay in presenting trend graph data in the Orchestrator UI.	8.9.1
ID: 16744. Tunnel bandwidth graphs were unresponsive or freezing because the API call from Orchestrator was fetching too much data.	8.9.1
ID: 16704. On Cloud Orchestrator, scheduled reports were failing to run or were taking several hours to complete.	8.9.1
ID: 16606. In rare instances, changes to interface labels could cause issues with Zscaler orchestration and potentially disconnect the Zscaler subscription.	8.9.1
ID: 16643. Fixed an issue that was causing performance in the Orchestrator UI to degrade when the Microsoft Azure Virtual WAN integration was enabled.	8.9.0
ID: 16594. On occasion, config-only Orchestrator backups were failing with a "2013. Lost connection to MySQL server during query when using LOCK TABLES" error.	8.9.0
ID: 16589. An Orchestrator OS and MySQL incompatibility issue was causing a severe performance issue in the Orchestrator UI. Additional memory has been allocated to MySQL to address this issue.	8.9.0
ID: 16584. In some cases, searching application definitions with the "Search Millions of Applications" field was producing the following error: "Uncaught TypeError: Cannot read property 'toLowerCase' of null"	8.9.0
ID: 16210. The "Tunnels" button has been removed from the Threshold Crossing Alerts page as its current functionality is no longer supported.	8.9.0
ID: 16129. In large network deployments, the Health Map tab was hanging while appliance data was being loaded.	8.9.0
ID: 15980. The Orchestrator UI would not permit port 65535, which was a valid port, to be configured in ACLs or policies.	8.9.0
ID: 15968. The audit log contained numerous "Failed to apply application classification data to appliance" entries, even though no updates or changes had been made.	8.9.0
ID: 15900. Chart results were showing incomplete data on the Overlay Interface Transport tab.	8.9.0
ID: 15804. Verified that user input is scanned to prevent cross-site scripting (XSS) exploits when using potential vulnerable libraries.	8.9.0
ID: 15748. DHCP server option 150 was not supported, causing issues for certain devices that required it.	8.9.0

Issue	Earliest Release to Fix
ID: 15702. Made some UX/UI improvements by changing the display defaults for various charts and reports and setting the Grouping Radius on the Topology page to default to the minimum.	8.9.0
ID: 15691. Fixed an issue that was showing "NaN% of 0.0" in the dashboard License panel, even though no Boost was assigned for the deployment.	8.9.0
ID: 15576. A critical alarm is now generated if a site is completely down and unreachable from the Cloud Portal or Orchestrator.	8.9.0
ID: 15289. If the Alarms tab was pinned and the user clicked "View All Alarms" in the Alarm summary, the pinned tab was unpinned and a new Alarms tab was opened.	8.9.0
ID: 15271. Fixed an issue in the UI that was causing a vertical scrollbar to appear in the Overlay Configuration page.	8.9.0
ID: 15098. The packet values on the vertical axis of the Appliance Bandwidth Trends chart were not formatted correctly.	8.9.0
ID: 14990. Chart results were showing incomplete data on the Overlay Interface Transport tab.	8.9.0
ID: 14841. Many Orchestrator alarm syslog messages did not indicate the name of the source appliance where the event/alarm originated.	8.9.0
ID: 17408 Upgrades or migrations were prone to issues if the Blueprint Export was taken when Orchestrator was not idle or stopped.	8.8.8
ID: 17029. On rare occasions, an exception in TaskDispatcher or StatsTaskManager was causing Orchestrator to restart unexpectedly.	8.8.7
ID: 16997. In certain deployments, an exception was being thrown if tunnel settings were not enabled for an interface label.	8.8.7
ID: 16960. Searching the appliance tree using the full group name was failing to return results.	8.8.7
ID: 16949. In some cases, if an appliance was generating an excessive amount of alarms, a queueing exception could close the connection to the appliance, which then became unreachable.	8.8.7
ID: 16922. In large networks, there was a significant delay in presenting trend graph data in the Orchestrator UI.	8.8.7
ID: 16744. Tunnel bandwidth graphs were unresponsive or freezing because the API call from Orchestrator was fetching too much data.	8.8.7
ID: 16606. In rare instances, changes to interface labels could cause issues with Zscaler orchestration and potentially disconnect the Zscaler subscription.	8.8.7
ID: 16825. Multiple duplicate entries for a single appliance were showing up in the Tunnel Exception tab.	8.8.6
ID: 16823. The search field at the top of the table in the Tunnel Exception tab was not working.	8.8.6
ID: 16710. When applying overlays in Cloud Orchestrator, NullPointerException errors were showing up in the log files, caused by ACL templates with empty rules.	8.8.6
ID: 16594. On occasion, config-only Orchestrator backups were failing with a "2013: Lost connection to MySQL server during query when using LOCK TABLES" error.	8.8.6
ID: 16589. An Orchestrator OS and MySQL incompatibility issue was causing a severe performance issue in the Orchestrator UI. Additional memory has been allocated to MySQL to address this issue.	8.8.6
ID: 16584. In some cases, searching application definitions with the "Search Millions of Applications" field was producing the following error: "Uncaught TypeError: Cannot read property 'toLowerCase' of null"	8.8.6
ID: 16579. Following the upgrade to 8.8.5, orchestration tasks were hanging and could only be resolved with an Orchestrator reboot.	8.8.6
ID: 16576. In some deployments, the default retention policy of six months for historical alarms could eventually slow down alarm queries. The retention period is now configurable.	8.8.6
ID: 16570. In some deployments, after upgrading to Orchestrator 8.8.5, tunnel refresh was delayed by 10 to 15 minutes following a reboot.	8.8.6

Issue	Earliest Release to Fix
ID: 16211. Some of the filters used in in the Boost summary report were causing some entries in the report to show "No data available."	8.8.6
ID: 16524. The main Orchestrator process was stopping due to a memory error, resulting from an Orchestrator job that was trying to retain too much information about older appliance backups.	8.8.5
ID: 16438. When configuring Internet breakout for an overlay and selecting services for available policies, the Orchestrator UI was not displaying more than six service names.	8.8.5
ID: 16429. The migration from Cloud Orchestrator to on-prem was failing if customers had applied any brand customization.	8.8.5
ID: 16426. In emails from Orchestrator regarding new releases, the download URL displayed the internal Orchestrator IP address instead of Orchestrator's reachability IP/FQDN.	8.8.5
ID: 16412. If the IPSec UDP port was set manually on more than one appliance belonging to the same site/HA pair, Orchestrator was failing to build HA tunnels. An alarm will now be raised if this is the case.	8.8.5
ID: 16059. Cloud Orchestrator was failing to build IPSec UDP tunnels on a specific appliance if the port assignment had been deleted by the user.	8.8.5
ID: 15481. Using the "Try it out!" button for the gmsConfig REST API's GET method was consistently failing with a "can't parse JSON" error.	8.8.5
ID: 16271. Following the upgrade to 8.8.2, Orchestrator backups were failing due to a stats cleanup job that was trying to run during the backup.	8.8.4
ID: 16220. Fixed some issues with Blueprint exports that were causing orchestration and general Orchestrator failures after restoring from those exports.	8.8.4
ID: 16122. Free OS memory was not parsed correctly on older versions of Fedora.	8.8.4
ID: 16015. Orchestrator 8.8.2 backups were failing because stats migration was still in progress. Backups will no longer run if stats migration is running.	8.8.4
ID: 15904. In rare cases, if a newly added appliance became unreachable immediately after it was approved, the Orchestrator UI could hang or become unresponsive.	8.8.4
ID: 15899. The Tunnel Exception page was failing to load because Orchestrator was looking for deployment data for a decommissioned appliance.	8.8.4
ID: 15878. Users can now create an Internet Breakout-only overlay without having to associate an interface and build a tunnel.	8.8.4
ID: 15813. When viewing historical charts for tunnels, configuring the time range to Custom and viewing one minute of data was yielding empty charts.	8.8.4
ID: 15731. Fixed an issue that was preventing new appliances connected to the Cloud Portal from being discovered by Orchestrator.	8.8.4
ID: 15701. Fixed an API issue that was preventing a valid user with read/write privileges from downloading a file from Orchestrator.	8.8.4
ID: 15658. Added guidance to the Orchestrator UI regarding schedules for IPSec Pre-shared Key Rotation. It is recommended that rotation be scheduled during maintenance windows because tunnels may go down briefly during the rotation.	8.8.4
ID: 15569. Uptime information is no longer displayed in Cloud Orchestrator.	8.8.4
ID: 15955. Added support for redistribution of OSPF to fabric via yaml config.	8.8.3
ID: 15827. Duplicate authentication requests were being sent to the RADIUS server for monitor users, causing a 'bad password' login failure.	8.8.3
ID: 15686. Attempting to modify a label type that was in use was causing the BIO page to become unresponsive. Label types can no longer be modified until any active associations have been removed.	8.8.3
ID: 15662. Passthrough tunnels that carry HA traffic will no longer be shaped.	8.8.3

Issue	Earliest Release to Fix
ID: 15574. In the VRRP tab, the 'Authentication String' field was being auto-populated with the Orchestrator username if it had been saved previously in the browser. This issue has been fixed, but it is possible that a specific browser implementation may not honor the instruction from the Orchestrator UI.	8.8.3
ID: 15568. In some cases, applications could not be added to or removed from an application group due to an issue with case sensitivity.	8.8.3
ID: 15567. Orchestration of an appliance in an HA group was being blocked because of an invalid IP address on a peer appliance.	8.8.3
ID: 15553. In the Routes dialog, the "Tag BGP communities to routes sent to SD-WAN fabric" flag was changed to "Tag BGP communities to routes" to help clarify that this tagging applied to both outbound and inbound routes.	8.8.3
ID: 15549. Fixed an issue with using preconfig with HA deployments.	8.8.3
ID: 15535. Added an Export option and a summary of appliance statuses to the Preconfigure Appliances tab to help simplify large network deployments.	8.8.3
ID: 15506. Added validation for hostname in DHCP server's static IP assignment configuration to avoid potential DHCP server failure.	8.8.3
ID: 15822. In some cases, data gaps were present in hourly reports for tunnel bandwidth trends (inbound and outbound), latency trends, and jitter trends.	8.8.2
ID: 15325. Alter query is blocked by Select query pausing stats collection.	8.8.2
ID: 14108. Orchestrator crashes when it is assigned a large heap size.	8.8.2
ID: 15598. Third party IPsec tunnel charts fail to start from the tunnel configuration page	8.8.2
ID: 15584. List of hubs on the business intent overlay page is not rendered properly when multiple hubs are present in a given region.	8.8.2
ID: 15354. Modifying the address of an appliance by right clicking on the appliance and selecting "modify appliance" results in locked browser window.	8.8.2
ID: 15272. Changing a WAN interface IP address may result in tunnels associated with the old IP address being stuck in the down state until node is restarted.	8.8.2
ID: 15262. Only first port of an ACL with multiple ports is matched	8.8.1
ID: 15330. Stats Collection pauses for extended periods of time	8.8.1
ID: 15196. Remote syslog log receiver stop receiving audit log message after a while	8.8.1
ID: 15130. Some appliances not building dynamic Zscaler tunnels	8.8.1
ID: 14820. Restrict certain special characters in User management template	8.8.1
ID: 14433. Appliance wizard throws "Failed to apply appliance subnets: The requested URL is no longer available - use /subnets3/configured instead" error while approving	8.8.1
ID: 14521. Show both estimated and real loss charts in the UI	8.8.1
ID: 15108. Default tunnel MTU incorrectly set	8.8.1
ID: 14510. YAML support for pass through shaped bandwidth setting	8.8.1
ID: 14889. Add full URL in the email verification emails for SMS clients	8.8.1
ID: 15113. Allow RBAC users access to Appliance Charts	8.8.1
ID: 14668. EdgeHA underlay tunnels bounce when adding WAN Interfaces to Deployment	8.8.1
ID: 14492. Orchestrator falls behind in appliance stats collection	8.5.8
ID: 14903. Delay in bringing up the underlay tunnels when adding an interface to HA pair	8.7.0
ID: 14979. Swagger rest api POST for /applicationDefinition/dnsClassification/{domain} Not Working	8.7.0
ID: 14897. Cloud Orch Internal server error when clicking link in password reset email	8.7.0

Issue	Earliest Release to Fix
ID: 14670. Failed to get data from appliance when appliance has no boost configured	8.7.0
ID: 13371. Audit Logs user login failures	8.7.0
ID: 14672. After Orch upgrade from 8.5.6 to 8.6.0, BIO page is not loading	8.7.0
ID: 14716. License changes automatically from BASE+PLUS to BASE	8.7.0
ID: 14896. Underlay tunnels didn't come up for 2-3 hours after a power cycle	8.7.0
ID: 14639. Manual ZTP takes over 20 minutes for the appliance to join the network.	8.7.0
ID: 14778. Appliance list not listed in scheduled appliance reboot	8.7.0
ID: 14513. SNMP Configuration removed when appliance is modified	8.7.0
ID: 14741. Orchestrator link Integrity test not working	8.7.0
ID: 14754. Pausing Orchestration on an appliance will stop new IPSec UDP key from getting activated	8.7.0
ID: 14324. IPSec UDP ports assigned by Orchestrator got changed without user intervention	8.7.0
ID: 14156. Orchestrator route import documentation needs an update - attributes should be listed horizontally	8.7.0
ID: 14264. Sort Orchestrator group names in Configuration Wizard	8.7.0
ID: 14782. Orch monitoring>Flow>Active-UDP is not showing expected result	8.7.0
ID: 14399. Search menu loses focus	8.7.0
ID: 14522. Check boost only if there is boost license applied	8.7.0
ID: 14263. Handling of IPSec authentication and encryption algorithm changes	8.7.0
ID: 14279. Health Map incorrect tile color returned	8.7.0
ID: 14328. New Orchestrator Crash - Java Out of Memory Crash	8.7.0
ID: 14676. SSL CN doesn't match the SSL cert added in Orchestrator	8.7.0
ID: 14366. Internet access down at remote sites after Orchestrator upgrade to 8.5.4.4004	8.7.0
ID: 14579. Appliance discovery - Orchestrator should warn when there is no matching preconfig file	8.7.0
ID: 14289. Orchestrator continuously pushing Overlay Config to appliance	8.7.0
ID: 14533. Daily granularity isn't displaying stats/graphs beyond 7 days	8.7.0
ID: 14537. Google maps does not display the location of the appliances	8.7.0
ID: 14467. Max loss is zero when average is a non-zero value in tunnel summary tab	8.7.0
ID: 14276. After upgrade to Orchestrator 8.5.3, trend charts load slowly	8.7.0
ID: 13987. Test Email address shouldn't be asked to verify	8.7.0
ID: 13784. User accounts created before the upgrade doesn't show the topology page	8.7.0
ID: 14324. IPSec UDP ports assigned by Orchestrator got changed without user intervention	8.6.1
ID: 14366. An empty internal subnets list would be reset to defaults on upgrade	8.6.1
ID: 14676. SSL CN doesn't match the SSL cert added	8.6.1
ID: 14399. Focus is lost randomly from menu search input midway during search	8.6.1
ID: 14279. Health map tile incorrectly colored	8.6.1
ID: 14522. Boost license expiry alarm raised although not using boost	8.6.1
ID: 14263. Tunnels don't come up if IPSec authentication & encryption algorithm is modified	8.6.1
ID: 14328. Orchestrator crashed with out of memory error pushing AVC data	8.6.1
ID: 13384. Stop supporting tunnel and application filter in Scheduled reports	8.6.0
ID: 13977. After upgrading HUB to 8.1.9.2 IPSEC tunnels wont come up (spoke sites are 8.1.5.15)	8.6.0
ID: 13344. Qualys scan. Add Content-Security-Policy HTTP header	8.6.0

Issue	Earliest Release to Fix
ID: 14021. Download orch and appliance debug files from orchestrator to local computer	8.6.0
ID: 13378. Default OK/Cancel selection for creating new groups	8.6.0
ID: 13392. Zero overlay latency value in appliance chart	8.6.0
ID: 12849. Invalid configuration : Not allowed - IP addresses on the same subnet	8.6.0
ID: 14235. Orchestrator crashed with out of memory error while browsing Site Dashboard	8.6.0
ID: 14270. Orchestrator upgrade fails with out of memory error	8.5.6
ID: 14201. Orchestrator crashes if there is an error in Orchestration of any appliance.	8.5.6
ID: 14222. User configured ACLs that have Overlay_ as part of their name will be deleted by Orchestrator.	8.5.6
ID: 14072. Orchestrator crashed during boot up after successfully upgrading from 8.0.x to 8.5.x	8.5.5
ID: 14170. Port forwarding rules not applied if one of the interfaces on the appliance has invalid IP Address	8.5.5
ID: 14137. Orchestrator upgrade to 8.5.4 fails because of missing libnuma library. Install the library as part of upgrade.	8.5.5

Need Help?

If you have any questions, contact your Silver Peak sales representative.

For product and technical support, contact Silver Peak Systems using any of the methods below:

- 1.877.210.7325 (toll-free in USA)
- +1.408.935.1850
- www.silver-peak.com/support

Revision History

Jul 18, 2024	Rev A: Initial document revision.
Sep 17, 2024	Rev B: <ul style="list-style-type: none">• Added a note about connectivity between Orchestrator and ECOS appliances post-9.4.x upgrade to Top Items for this Release and Known Issues/Upgrade Considerations.• Added a note about SMTP encryption/decryption in Cloud OaaS to Top Items for this Release and Known Issues/Upgrade Considerations.• Amended notes about API integration post-9.3.x in Top Items for this Release, API Changes, and Known Issues/Upgrade Considerations.• Added a note about large queries using extra disk space and generating a high volume of stats to Top Items for this Release and Known Issues/Upgrade Considerations.• Added a note about the admin and gms users becoming separate users to Known Issues/Upgrade Considerations.• Added a note about deprecation of Check Point CloudGuard Connect to Known Issues/Upgrade Considerations.
Sep 30, 2024	Rev C: Added a note about potentially slow upgrades to Known Issues/Upgrade Considerations and added ID: 27505 to Issues Fixed from Past Releases .
Oct 14, 2024	Rev D: <ul style="list-style-type: none">• Updated the version to 9.5.1_40443.• Removed the note about SMTP encryption/decryption from Top Items for this Release and Known Issues/Upgrade Considerations.• Added ID: 30556 and ID: 31135 to the list of Issues Fixed for this release.• Revised a note about connectivity between Orchestrator and ECOS appliances post-9.4.x upgrade to include CLI commands to enable, disable, and view status of FIPS mode.
Nov 5, 2024	Rev E: Added a note about the risk of failed cryptographic functions in Orchestrator 9.4.x and 9.5.x to Top Items for this Release and Known Issues/Upgrade Considerations.

Copyright

Copyright © 2024 Silver Peak Systems, Inc. All rights reserved. Information in this document is subject to change at any time. Use of this documentation is restricted as specified in the End User License Agreement. No part of this documentation can be reproduced, except as noted in the End User License Agreement, in whole or in part, without the written consent of Silver Peak Systems, Inc.

Trademark Notification

Silver Peak, the Silver Peak logo, and all Silver Peak product names, logos, and brands are trademarks or registered trademarks of Silver Peak Systems, Inc. In the United States and/or other countries. All other product names, logos, and brands are property of their respective owners.

Warranties and Disclaimers

This documentation is provided "as is" without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. Silver Peak Systems, Inc. assumes no responsibility for errors or omissions in this documentation or other documents which are referenced by or linked to this documentation. References to corporations, their services and products, are provided "as is" without warranty of any kind, either expressed or implied. In no event shall Silver Peak Systems, Inc. be liable for any special, incidental, indirect or consequential damages of any kind, or any damages whatsoever, including, without limitation, those resulting from loss of use, data or profits, whether or not advised of the possibility of damage, and on any theory of liability, arising out of or in connection with the use of this documentation. This documentation may include technical or other inaccuracies or typographical errors. Changes are periodically added to the information herein; these changes will be incorporated in new editions of the documentation. Silver Peak Systems, Inc. may make improvements and/or changes in the product(s) and/or the program(s) described in this documentation at any time.