

# Aruba Orchestrator User Guide

Orchestrator 9.2.2

Last updated on November 10, 2022

Revision B

# Copyright and Trademarks

Aruba Orchestrator User Guide

Date: November 2022

© Copyright 2022 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein. Aruba Networks and the Aruba logo are registered trademarks of Aruba Networks, Inc. Third-party trademarks mentioned are the property of their respective owners. To view the end-user software agreement, go to [Aruba EULA](#).

Hewlett Packard Enterprise Company  
6280 America Center Drive  
San Jose, CA 95002  
USA

# Support

For product and technical support, contact Aruba Systems at either of the following:

**1.800.943.4526 (toll-free in USA and Canada)**  
**+1.408.941.4300**  
**[www.silver-peak.com/support](http://www.silver-peak.com/support)**

We are dedicated to continually improving our products and documentation. If you have suggestions or feedback for our documentation, send an e-mail to [sp-techpubs@hpe.com](mailto:sp-techpubs@hpe.com).

# Contents

<b>Copyright and Trademarks .....</b>	<b>2</b>
<b>Support .....</b>	<b>3</b>
<b>What's New .....</b>	<b>10</b>
Orchestrator 9.2.2 .....	10
Orchestration Performance Enhancements .....	10
<b>Getting Started .....</b>	<b>11</b>
Supported Browsers .....	11
Guidelines for Creating Passwords .....	11
Overview of SD-WAN Prerequisites .....	11
<b>Monitoring .....</b>	<b>14</b>
Summary .....	14
Dashboard .....	14
Topology .....	14
Health Map .....	20
Alarms .....	22
Reporting .....	65
Schedule and Run Reports .....	65
View Reports .....	66
Scheduled and Historical Jobs .....	68
Bandwidth .....	69
Overlay-Interface-Transport .....	69
Interface Bandwidth Trends .....	70
Interface Summary .....	72
Application Bandwidth .....	72
Application Pie Charts .....	73
Application Trends .....	74
Top Talkers .....	75
Domains .....	77
Countries .....	77
Ports .....	78
Traffic Behavior .....	79
Appliance Bandwidth .....	80
Appliance Max Bandwidth .....	81
Appliance Bandwidth Utilization .....	82
Appliance Bandwidth Trends .....	83
Appliance Packet Counts .....	83
Tunnels Bandwidth .....	83
Tunnels Pie Charts .....	86
Tunnel Bandwidth Trends .....	86
Tunnel Packet Counts .....	87
DRC Bandwidth Trends .....	88
Flows - Active and Recent .....	90

Appliance Flow Counts .....	95
Appliance Flow Trends .....	95
Tunnel Flow Counts .....	96
DSCP Bandwidth .....	96
DSCP Pie Charts .....	97
DSCP Trends .....	97
Traffic Class Bandwidth .....	98
Traffic Class Pie Charts .....	98
QoS (Shaper) Trends .....	99
Shaper Summary .....	100
Boost Tab .....	101
Firewall Drops .....	103
Tunnel Health .....	104
Live View .....	104
Loss Summary .....	104
Loss Trends .....	105
Jitter Summary .....	106
Jitter Trends .....	107
Latency Summary .....	108
Latency Trends .....	110
Out of Order Packets Summary .....	111
Mean Opinion Score (MOS) Summary .....	113
Mean Opinion Score (MOS) Trends .....	113
Tunnels Summary .....	114
 <b>Configuration .....</b>	 <b>116</b>
Overlays & Security .....	116
Business Intent Overlays .....	116
Apply Overlays .....	121
Interface Labels .....	121
Hubs .....	123
Deployment Profiles .....	124
Deployment - EdgeConnect HA .....	134
Firewall Zones .....	136
Firewall Protection Profiles .....	136
Internet Traffic .....	141
IPSec Pre-Shared Key Rotation .....	142
Intrusion Detection/Prevention System (IDS/IPS) .....	143
SSL Certificates Tab .....	148
SSL CA Certificates Tab .....	149
SSL for SaaS Tab .....	149
Discovered Appliances .....	150
Preconfigure Appliances .....	151
Appliance Configuration Wizard .....	152
EC-Enterprise Licenses .....	155
EC-Metered Licenses .....	156
Cloud Portal .....	158
Networking .....	159
Deployment Tab .....	159
Interfaces Tab .....	165
NAT .....	169

NAT Rules and Pools .....	169
VRRP Tab .....	171
WCCP Tab .....	172
PPPoE Tab .....	175
Loopback Interfaces .....	177
Loopback Orchestration .....	177
Virtual Tunnel Interfaces .....	178
DHCP Server Defaults .....	179
DHCP Leases .....	181
DHCP Failover .....	181
DHCP Failover State .....	182
Link Aggregation .....	183
Regions .....	187
Routing Segmentation .....	189
Management Services .....	193
Inter-Segment Routing and DNAT Exceptions .....	195
Inter-Segment SNAT Exceptions .....	196
BGP Tab .....	196
Prefix Match Criteria .....	201
BGP ASN Global Pool .....	204
Routes Tab .....	205
OSPF Tab .....	213
BFD Tab .....	219
Multicast .....	221
Peer Priority Tab .....	223
Admin Distance Tab .....	224
Management Routes Tab .....	225
Tunnels Tab .....	226
Tunnel Exception .....	242
Schedule Auto MTU Discovery .....	243
Policies .....	243
DNS Proxy Policies .....	243
Route Policies Tab .....	244
QoS Policies Tab .....	249
Schedule QoS Map Activation .....	260
Optimization Policies Tab .....	260
SaaS NAT Policies Tab .....	268
Inbound Port Forwarding .....	276
Security Policies Tab .....	278
Access Lists Tab .....	281
Address Groups .....	283
Service Groups .....	289
Shaper Tab .....	296
SaaS Optimization Tab .....	297
Application Definitions .....	299
Application Groups Tab .....	301
Threshold Crossing Alerts Tab .....	301
IP SLA Tab .....	304
Templates .....	314
Templates Overview .....	314
Template Groups .....	315
System Template .....	316

Auth/Radius/TACACS+ Template .....	318
Flow Export Template .....	320
Logging Template .....	320
Banner Messages Template .....	323
HTTPS Certificate Template .....	324
User Management Template .....	326
DNS Template .....	327
Date/Time Setting .....	327
SNMP Template .....	328
SSL Certificates Template .....	330
SSL CA Certificates Template .....	331
SSL for SaaS Template .....	332
Tunnels Template .....	333
VRRP Template .....	336
Peer Priority Template .....	338
Route Redistribution Maps Template .....	339
Routes Template .....	340
BGP Template .....	341
BFD Template .....	342
OSPF Template .....	343
Admin Distance Template .....	345
Route Policies Template .....	345
QoS Policies Template .....	348
Optimization Policies Template .....	354
SaaS NAT Policies Template .....	359
Threshold Crossing Alerts Template .....	364
SaaS Optimization Template .....	367
Security Policies Template .....	369
DNS Proxy Template .....	370
Shaper Template .....	371
Management Services Template .....	373
CLI Template .....	373
Session Management Template .....	374
Apply Template Groups .....	376
Cloud Services .....	376
AWS Transit Gateway Network Manager .....	376
Microsoft Azure Virtual WAN .....	386
Check Point CloudGuard Connect .....	389
Microsoft Office 365 .....	391
Zscaler Internet Access .....	392
Service Orchestration .....	398
Deploy Cloud Hubs .....	406
Cloud Hubs in AWS .....	407
Cloud Hubs in Azure .....	412
Cloud Hubs in GCP .....	425
 <b>Administration .....</b>	 <b>433</b>
General Settings .....	433
Appliance User Accounts Tab .....	433
Auth/RADIUS/TACACS+ Tab .....	434
Date/Time Tab .....	436

DNS (Domain Name Servers) Tab .....	437
SNMP Tab .....	438
Flow Export Tab .....	440
Logging Tab .....	445
Banners Tab .....	447
HTTPS Certificate Tab .....	448
Orchestrator Reachability Tab .....	449
Custom Appliance Tags .....	450
Software .....	451
System Information .....	451
Software Versions .....	456
Upgrade Appliance Software .....	456
Appliance Configuration Backup .....	457
View Configuration History .....	459
Restore a Backup to an Appliance .....	459
Remove Appliance from Orchestrator .....	460
Remove Appliance from Orchestrator and Account .....	461
Tools .....	462
Synchronize Appliance Configuration .....	462
Put the Appliance in System Bypass Mode .....	463
Broadcast CLI Commands .....	464
Link Integrity Test .....	465
Disk Management .....	470
Erase Network Memory .....	471
Reboot or Shut Down an Appliance .....	472
Schedule an Appliance Reboot .....	473
Active Sessions Tab .....	476
<b>Orchestrator .....</b>	<b>478</b>
Orchestrator Server .....	478
Role Based Access Control .....	478
View Orchestrator Server Information .....	481
Restart, Reboot, or Shutdown .....	482
Manage Orchestrator Users .....	482
API Key .....	487
Remote Authentication .....	487
Cloud Portal .....	495
Audit Logs .....	496
Orchestration Settings .....	497
Maintenance Mode .....	498
Tunnel Settings Tab .....	499
Orchestrator Blueprint Export .....	505
Brand Customization .....	507
Software & Setup .....	507
Upgrade Orchestrator Software .....	507
Check for Orchestrator and Appliance Software Updates .....	509
Back Up on Demand .....	509
Schedule Orchestrator Backup .....	510
Schedule Stats Collector Backup .....	511
SMTP Server Settings .....	513
Proxy Configuration .....	513

Timezone for Scheduled Jobs .....	514
Orchestrator Advanced Properties .....	514
Change the Orchestrator Log Level .....	515
IP Allow List .....	516
Orchestrator Getting Started Wizard .....	517
Statistics Retention .....	518
Stats Collector Configuration .....	519
Notification Banner .....	524
Aruba Central .....	524
Aruba Central Site Mapping .....	524
ClearPass Policy Manager .....	528
 <b>Support</b>	 <b>531</b>
Technical Assistance .....	531
Tech Support - Appliances .....	531
Tech Support - Orchestrator .....	532
Log In to the Support Portal .....	532
Monitor Transfer Progress .....	533
Packet Capture .....	534
Upload Local Files .....	535
Create a Support Case .....	535
Partition Management .....	536
Remote Log Receivers .....	537
Routing Peers Table .....	540
RMA Wizard .....	540
User Documentation .....	542
Alarm Descriptions .....	542
Built-in Policies .....	544
Reporting .....	544
Realtime Charts .....	544
Historical Charts .....	545
Appliance Charts .....	546
Internal Drop Trends .....	547
Appliance Memory Trends .....	549
System Performance .....	550
Appliance CPU Usage .....	551
Orchestrator Debug .....	552
IPSec UDP Status .....	553
Unverified Emails .....	553

## What's New

This page provides a brief description and links to additional information about new features in recent Orchestrator releases.

## Orchestrator 9.2.2

The following enhancements were introduced in Orchestrator 9.2.2:

### Orchestration Performance Enhancements

This release adds a number of performance enhancements to significantly reduce orchestration times for most use cases.

## Getting Started

Orchestrator enables you to globally monitor performance and manage EdgeConnect (EC) appliances, whether you are configuring a WAN Optimization network (NX, VX, or VRX appliances) or an SD-WAN network (EC or EC-V appliances).

## Supported Browsers

Orchestrator and the Appliance Web user interfaces support the following browsers:

- Google Chrome (recommended)
- Microsoft Edge
- Mozilla Firefox
- Opera
- Safari

We recommend that you use the latest version available for your browser.

## Guidelines for Creating Passwords

- Passwords should be a minimum of eight characters.
- There should be at least one lower case letter and one upper case letter.
- There should be at least one digit.
- There should be at least one special character.
- Consecutive letters in the password should not be dictionary words.

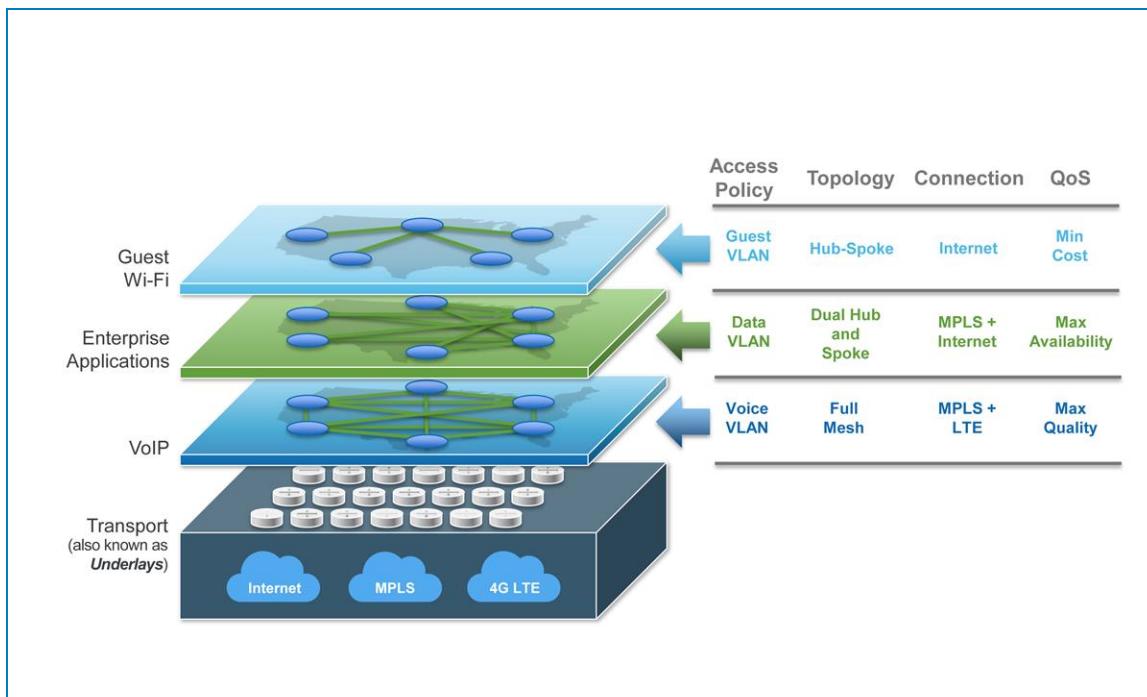
## Overview of SD-WAN Prerequisites

With Orchestrator, you create virtual network overlays to apply business intent to network segments. Provisioning a device is managed by applying profiles.

- **Interface Labels** associate each interface with a use.
  - LAN labels refer to traffic type, such as **VoIP**, **data**, or **replication**.
  - WAN labels refer to the service or connection type, such as **MPLS**, **internet**, or **Verizon**.
- **Deployment Profiles** configure the interfaces and map the labels to them, to characterize the appliance.

- **Business Intent Overlays** use the Labels specified in Deployment Profiles to define how traffic is routed and optimized between sites. These overlays can specify preferred paths and can link bonding policies based on **application**, **VLAN**, or **subnet**, independent of the brand and physical routing attributes of the underlay.

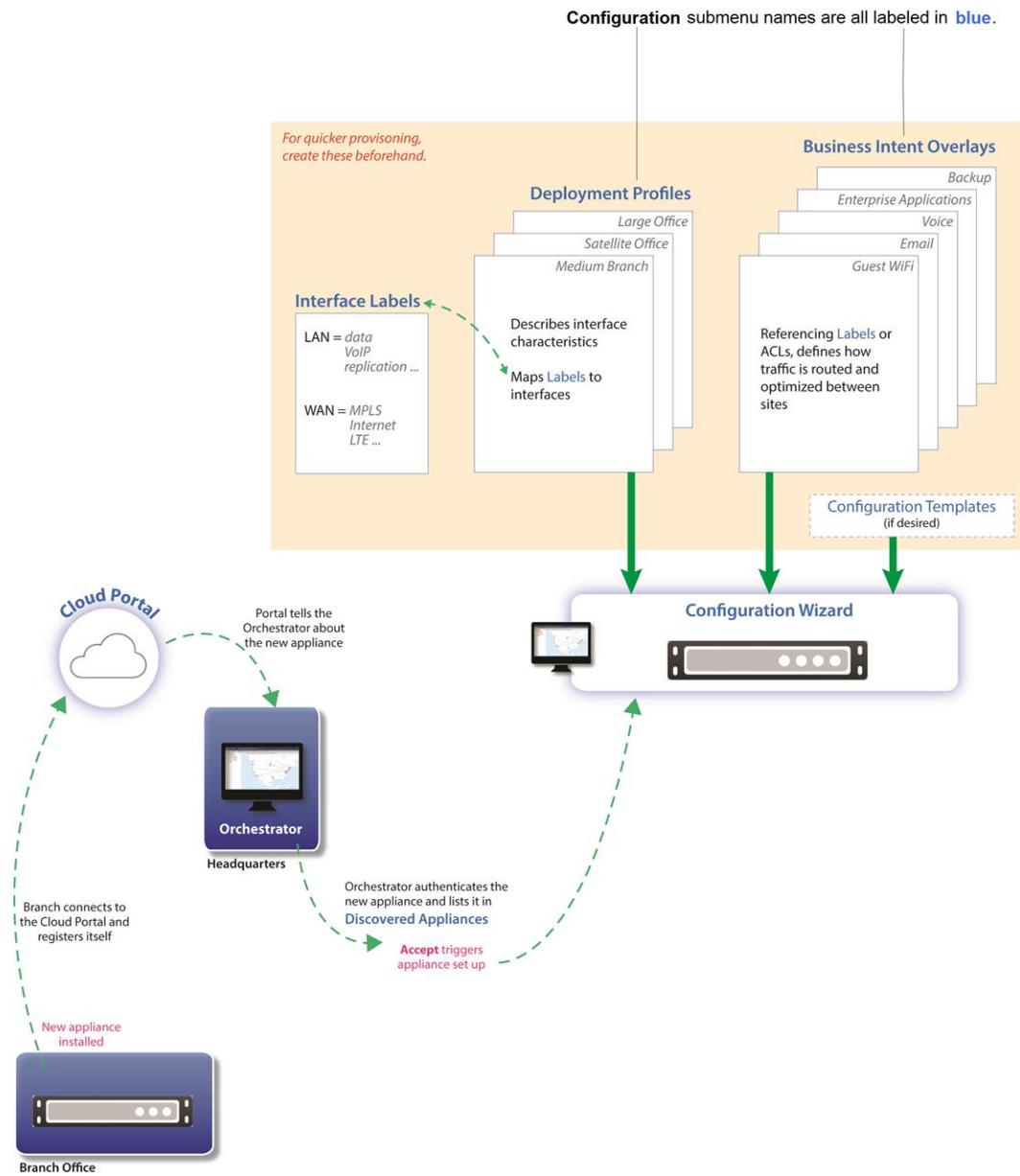
This diagram shows the basic architecture and capabilities of **Overlays**.



Including a new appliance into the SD-WAN fabric consists of two basic steps:

1. **Registration and discovery.** After you **Accept** the discovered appliance, the **Configuration Wizard** opens.
2. **Provisioning.** Because the wizard prompts you to select profiles, it is easier to create these ahead of time.

The following figure shows the process of installing and provisioning an appliance for SD-WAN.



# Monitoring

These topics focus on reports related to performance, traffic, and appliance status. Additionally, [Threshold Crossing Alerts](#) are helpful in monitoring your network.

## Summary

### Dashboard

*Monitoring > Summary > Dashboard*

The Dashboard integrates information from multiple components—or widgets—into a unified display for monitoring your network. It displays appliance license information, topology, health map, top talkers, top domains, and so forth, on one tab. The collection of widgets are customizable and persist for each user account.

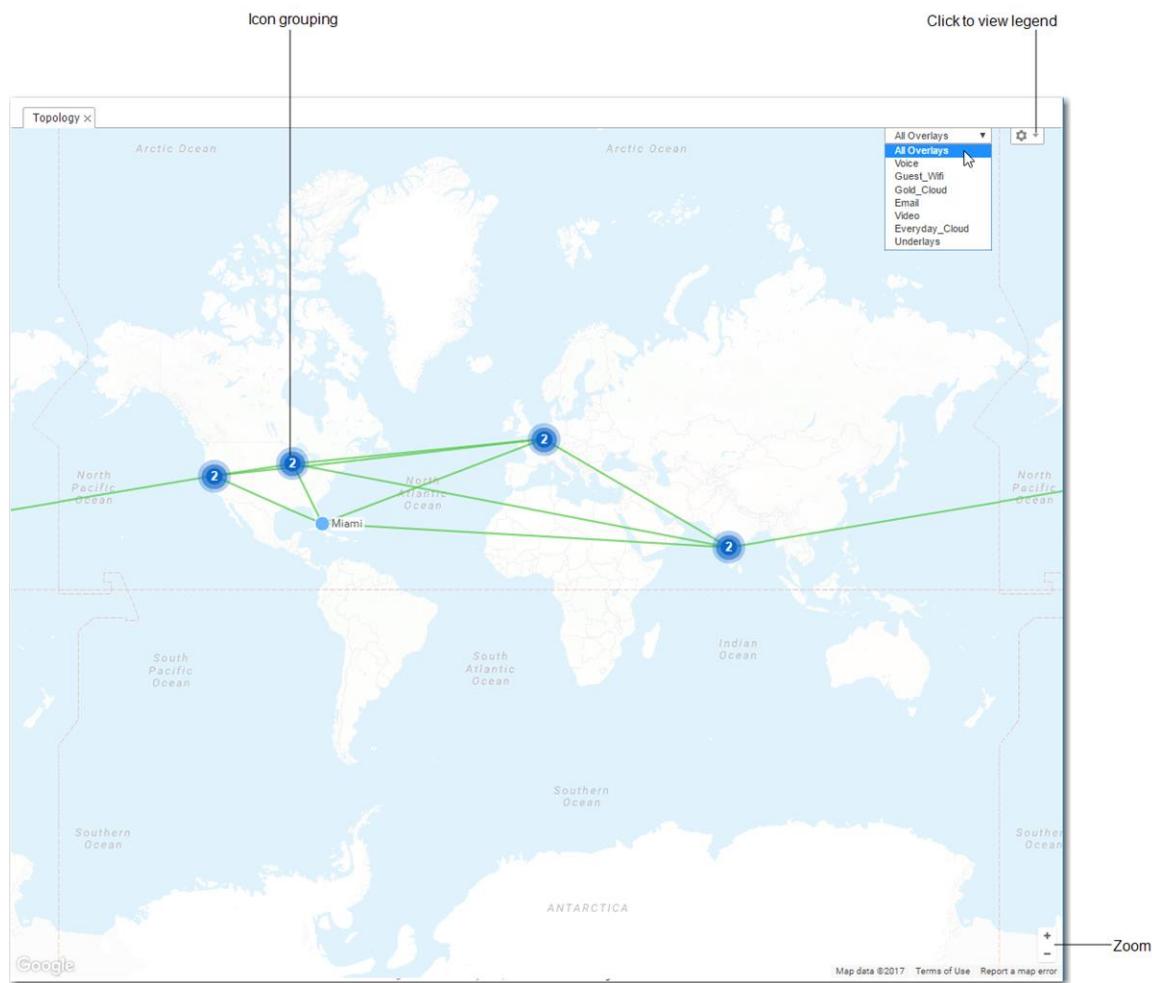
- Click **Settings** [  ] to select the widgets you want to show or hide.
- To move widgets, drag them by title.
- To access more detail in its corresponding tab, click a widget's title.
- To filter on various widgets, select **Src** or **Dest**, **Overlay** or **Underlay**, or **Inbound** or **Outbound**. The filter varies depending on the widget you are selecting.
- You can choose and change the grouping variable for Overlay-Transport and Overlay-Interface by clicking **Flip**.
- The **Appliance Licenses** widget displays an inventory by appliance model, as well as license type, availability, and usage.
- To search for appliances in the tree, enter an appliance name and the tag will be displayed above the tree.
- To filter collections of appliances, select **Show Tags** and select from among the tag options.

### Topology

*Monitoring > Summary > Topology*

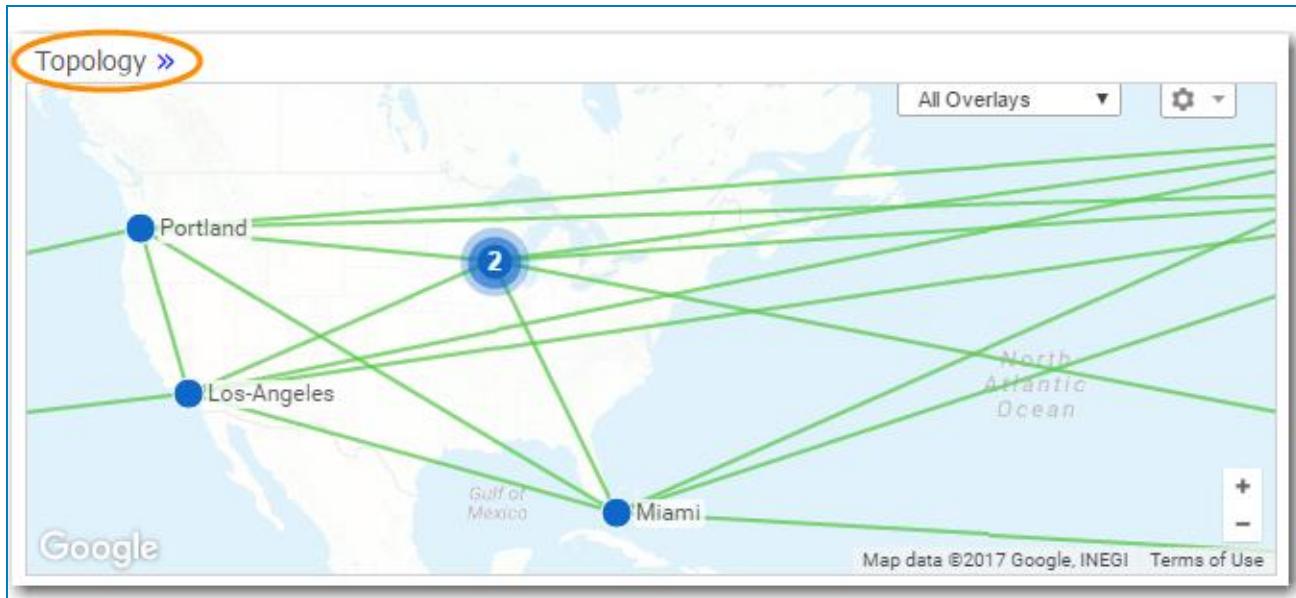
The Topology tab provides a visual summary of your network.

When configuring a software-defined WAN (**SD-WAN**), you can view **All Overlays**, individual **Business Intent Overlays** (BIOS), or the single and bonded **Underlay** tunnels that support them.

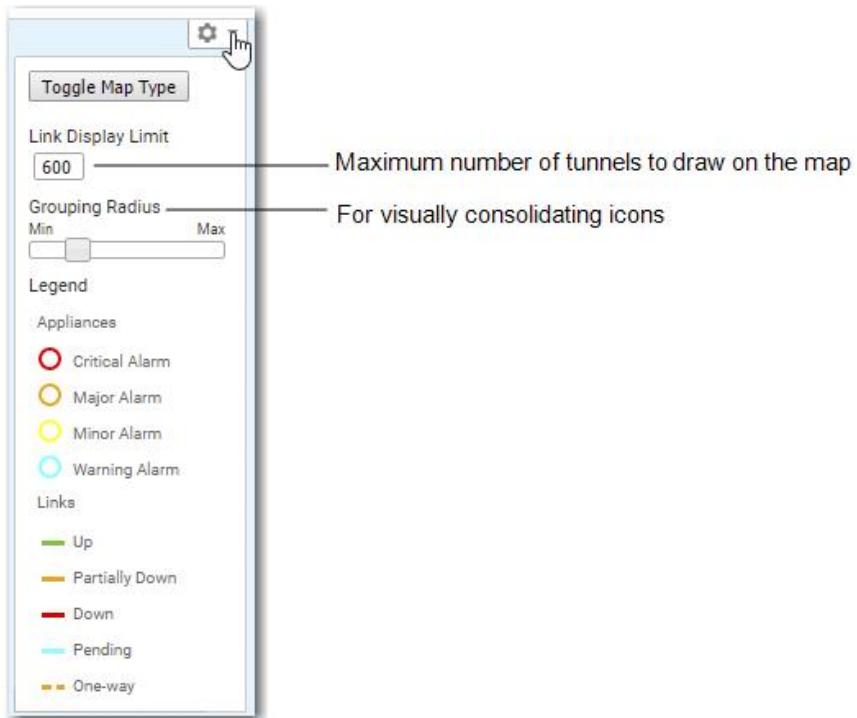


You can access it under **Monitoring** in the menu bar, or by clicking the widget title on the **Dashboard** tab.

*Topology widget on Dashboard tab*

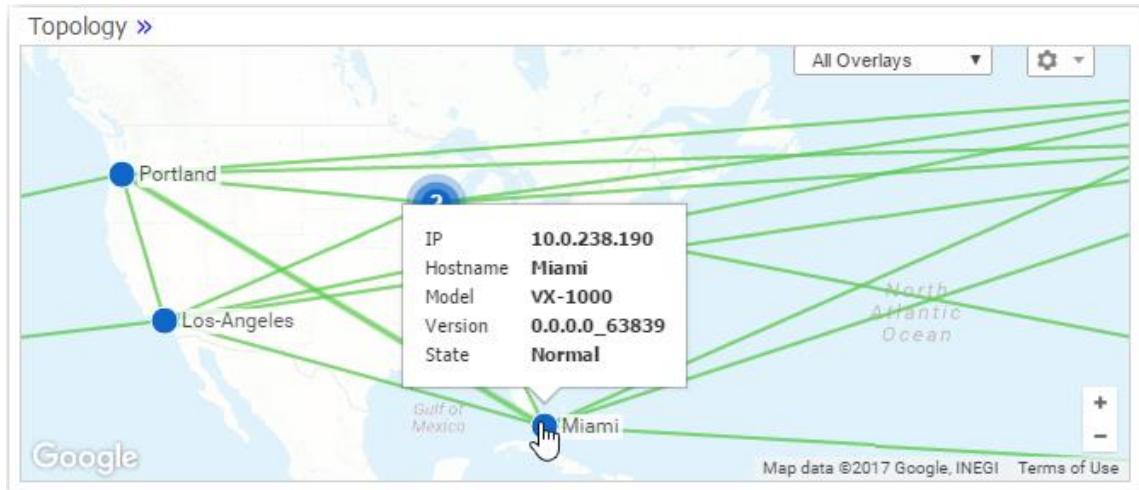


- The Legend details the management and operational states of the appliances.

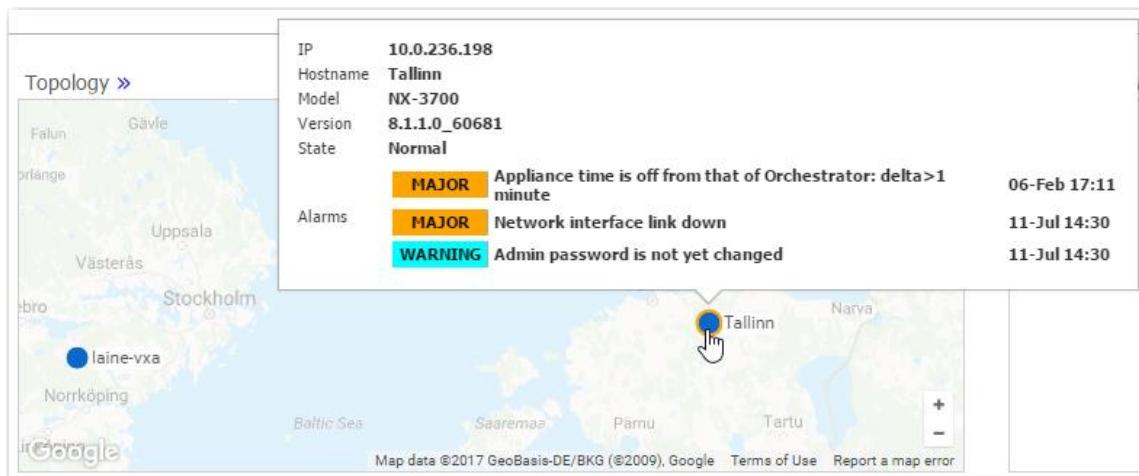


- The **Topology** map can dynamically geolocate an appliance when you enter a location (City, State, Country) in an appliance Configuration Wizard, or when you modify the appliance by right-clicking to access its contextual menu.
- The map tile renders to support variable detail at different zoom levels.

- You can use icon grouping to visually consolidate adjacent appliances. The status bubbles up, and you can configure relative grouping distance in the map's legend. The grouping is also a function of how far you zoom in or out.
- Rolling over an individual appliance's icon displays basic system information.



When the icon is encircled by a ring, indicating an alarm, those also display.



## View Tunnels in the Topology Map

Clicking on a tunnel opens a table with access to information about that link.

The screenshot illustrates the Aruba Orchestrator interface. At the top, a map shows various cities like Portland, Minneapolis, Chicago, and Los Angeles, with green lines representing network connections. A cursor is hovering over the San Francisco area. An orange arrow points from the map down to a detailed table below.

**Topology**

**Tunnels**

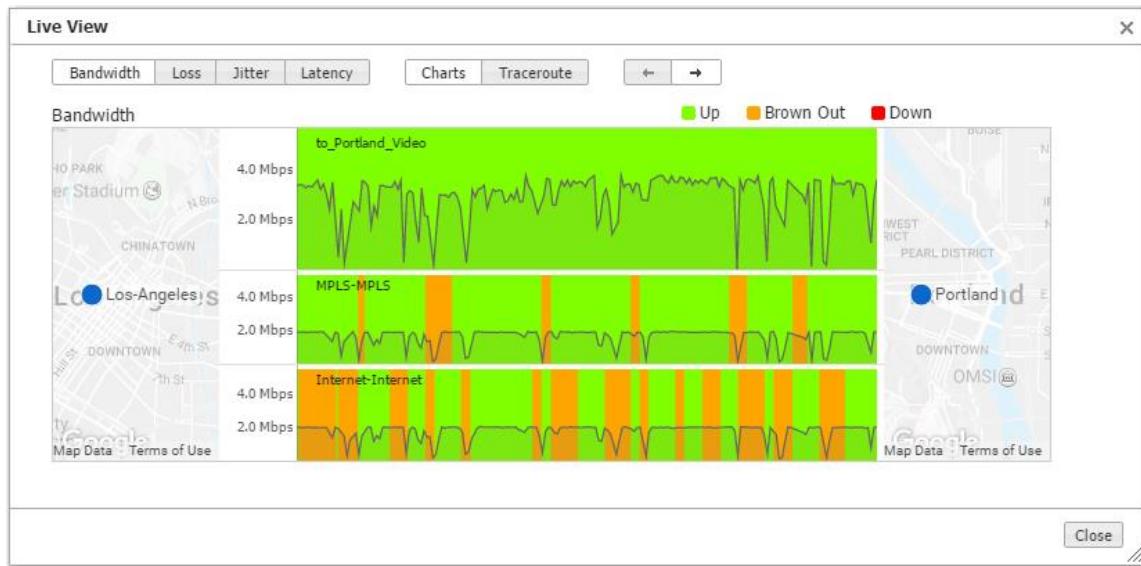
12/36 Rows, 1 Selected

Type	Local Appliance	Remote Appliance	Name	Status	Live View	Historical Charts
Overlay: Gold_Cloud	(6 tunnels)					
Overlay: Everyday_Cloud	(6 tunnels)					
Overlay: Voice	(6 tunnels)					
Overlay: Video	(6 tunnels)					
Overlay: Email	(6 tunnels)					
Overlay: Guest_Wifi	(6 tunnels)					
overlay	Los-Angeles	Portland	to_Portland_Video	up - active	N/A	N/A
underlay	Los-Angeles	Portland	to_Portland_MPLS-MPLS	up - active	N/A	N/A
underlay	Los-Angeles	Portland	to_Portland_Internet-Internet	up - active	N/A	N/A
underlay	Portland	Los-Angeles	to_Los-Angeles_Internet-Internet	up - active	N/A	N/A
underlay	Portland	Los-Angeles	to_Los-Angeles_MPLS-MPLS	up - active	N/A	N/A
overlay	Portland	Los-Angeles	to_Los-Angeles_Video	up - active	N/A	N/A

**Close**

## Live View

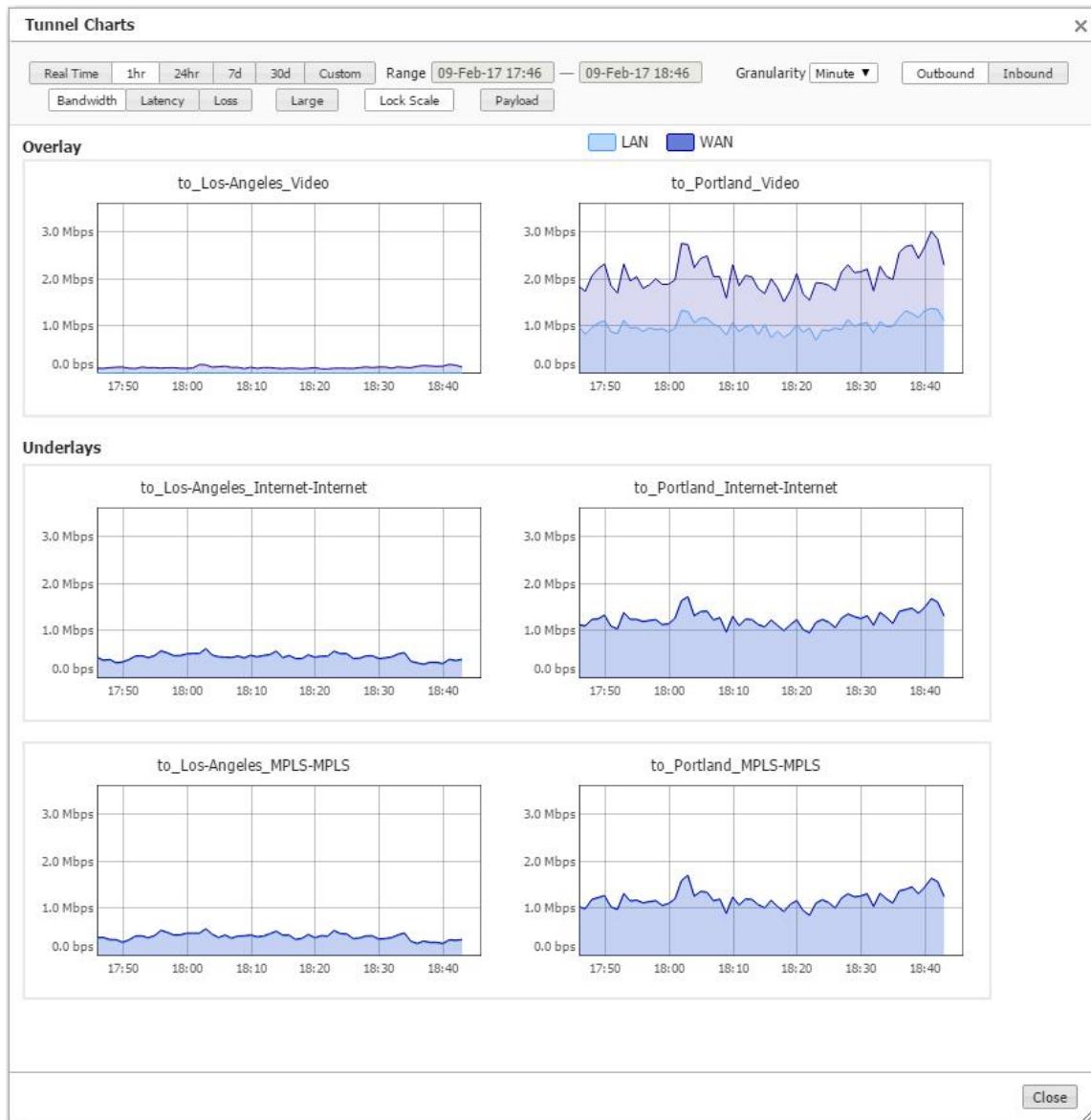
From the table, you can access the link's **Live View** graph.



LiveView shows in real time how synergy is created to maintain coverage. The real-time chart shows the SD-WAN overlay at the top and the underlay networks at the bottom. The overlay is green and delivering consistent application performance while both underlays are in persistent brown-out state.

## Historical Charts

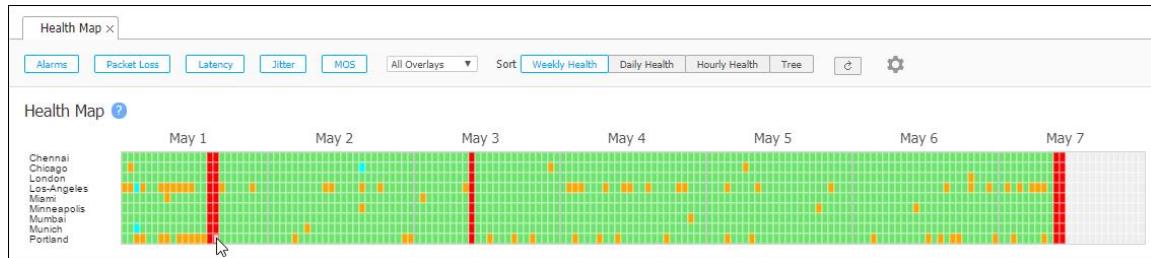
These charts enable you to selectively view the tunnel's components and behavior.



## Health Map

*Monitoring > Summary > Health Map*

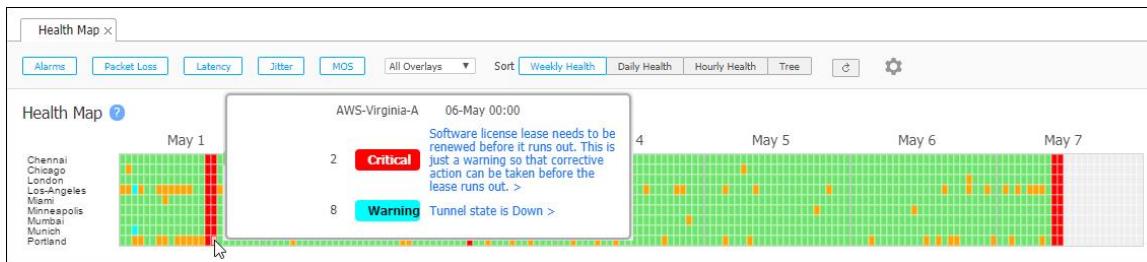
The **Health Map** provides a high-level view of your network's health, based on real-time measurements of network conditions between appliances.



- View filters are available for alarms, packet loss, latency, jitter, MOS (mean opinion score), and Business Intent Overlay.
- The health map can be sorted by weekly, daily, hourly health, or tree (by group, and then alphabetical by hostname).
- Each block represents one hour and uses color coding to display the most severe event among the selected filters. Color codes correspond to alarm severity and thresholds.
  - **Green** - Normal operation.
  - **Red** - Critical. Steps must be taken immediately in order to restore the affected service.
  - **Orange** - Major. Steps must be taken as soon as possible because the affected service has degraded drastically.
  - **Yellow** - Minor. A problem that does not yet affect service, but could if the problem is not corrected.
  - **Aqua** - Warning. A potential problem that could affect service.
  - **Grey** - No data available.
- Thresholds can be configured by clicking on the gear icon .



- Clicking a color block displays a pop-up with specifics about that event, what value triggered it, and any additional threshold breach for that appliance during the same hour.



- While filter and sort order customizations persist for each user account, threshold settings apply globally.
- Threshold settings are not retroactive. Setting new thresholds does not redisplay historical data based on newly edited values.
- Deleting an appliance deletes its data.
- If you are using overlays, note the following:
  - You can view each overlay's health individually.
  - If you remove an individual overlay, its data is not recoverable. However, its historical data remains included in All Overlays.

## Alarms

### *Monitoring > Summary > Alarms*

This tab displays the Alarms table, which provides details about both appliance and Orchestrator alarms.

The screenshot shows the Alarms table with the following columns: Host Name, Alarm Time, Severity, Source, Alarm Description, Recommended Action, Ack, Acked Time, Acked By, and Comments. There are 6 rows listed:

Host Name	Alarm Time	Severity	Source	Alarm Description	Recommended Action	Ack	Acked Time	Acked By	Comments...
Orchestrator	23-Sep-21 11:24	Warning	/orchestration/overlays	At least one hub is not part of any overlay	To add a Hub to an Overlay, either (1) apply the Overlay to a Hub appliance or (2) add the Overlay to an existing Hub.	<input checked="" type="checkbox"/>	05-Oct-21 10:32	Orc rmoir@silver-peal	+Add
Ripponden1-Collier	07-Oct-21 09:43	Warning	system	Could not reach Orchestrator using HTTPS over any interface	Appliance cannot connect to Orchestrator using HTTPS. This connectivity issue may be due to a misconfiguration of the interface or a network problem.	<input type="checkbox"/>			+Add
Thalague-Kainke	04-Oct-21 12:59	Warning	System	NTP servers 185.22.60.71, 185.21.101.59 are unreachable	Check appliance's NTP server IP and version config. Can appliance reach these NTP servers?	<input type="checkbox"/>			+Add
Ripponden1-Collier	07-Oct-21 14:57	Warning	System	NTP servers 91.228.108.123, 77.72.144.59 are unreachable	Check appliance's NTP server IP and version config. Can appliance reach these NTP servers?	<input type="checkbox"/>			+Add
Scaux-Gullet	07-Oct-21 14:10	Major	/orchestrator/connect...	Orchestrator cannot reach this appliance	Check the connection between the appliance and the Orchestrator.	<input type="checkbox"/>			+Add
Orchestrator	26-Jul-21 01:11	Warning	/orchestration	Some appliances are paused from orchestration	Go to Pause Orchestration List to see detail.	<input checked="" type="checkbox"/>	05-Oct-21 10:32	Orc rmoir@silver-peal	+Add

Each entry in the Alarms table represents one current condition that could require human intervention. Because alarms are conditions, they can come and go without management involvement.

While merely acknowledging most alarms does **not** clear them, some alarm conditions are set up to self-clear when you acknowledge them. For example, if you remove a hard disk drive, it generates an alarm; after you replace it and it finishes rebuilding itself, the alarm clears.

You can filter the alarms listed in the Alarms table.

- Time: **1h, 4hr, 1d, 7d**, or **Custom**. **Custom** enables you to specify a range of dates in the **Range** fields.
- **Active** - All uncleared alarms. Acknowledged alarms go to the bottom of this list.
- **History** - Filtered to show only cleared alarms.
- **All** - All uncleared and cleared alarms.

**NOTE** Orchestrator keeps a history of alarms for 7 days. If you are using the on-prem version of Orchestrator you can configure it to keep a history for more than 7 days. If you are using Orchestrator-as-a-service, this cannot be changed.

The Alarms tab also includes the following functionality:

- **Alarm Emails ON** and **Alarm Emails Paused**: You can enable or disable if you want to receive an email if there is an alarm that is on or paused.
- **Alarm Email Recipients**: Each configured recipient can receive emails about either Appliance alarms or Orchestrator alarms. Click **Add Recipient** in the **Alarm Recipients** window. Select the appropriate type of alarm from the **Alarm Type** drop-down list, and then select the check boxes (**Critical, Major, Minor, Warning**) for which you want to receive emails. Click **Save** or **Reload**.
- **Wait to Send Emails**: You can customize the amount of time you want the system to wait to send you an email notifying you of an alarm. Click this button to open the Wait to Send Emails dialog box, and then enter the number of minutes you want the system to wait. Click **Save**.
- **Export**: You can export a CSV file of your alarms.
- **Ack, Acked By, and Acked Time**: These columns in the Alarms table indicate whether an acknowledgment has been received between devices.
  - **Acked By**: The name of the appliance that did the acknowledgment.
  - **Acked Time**: The time when the acknowledgment was received by the appliance.

## Disable Alarms

You can specify which alarms you want to disable by clicking **Customize / Disable Alarms**, which opens the **Alarm Information** dialog box.

To disable alarms:

1. Click **Disable All Alarms on Specific Appliances**.
2. Enter the name of the appliance that has the alarms you want disabled.
3. Click **Disable Alarms**.
4. Click **Save**.

## Customize Alarms

Complete the following steps to customize a pre-existing alarm.

1. Select the edit icon next to the selected appliance in the Alarm Information window.
2. Choose **Enable/Disable**.
3. If selecting **Enable**, specify the **Custom Severity** by choosing from the list: **None, CRITICAL, MAJOR, MINOR, WARNING**.

If selecting **Disable**, the following message will display: \*You are about to disable this alarm. Click **Save**.

## Alarm Severity

Orchestrator has four severity levels for alarms:

- **Critical** (red) - Critical alarms are service-affecting and require immediate attention. They reflect conditions that adversely affect an appliance or indicate the loss of a broad category of service.
- **Major** (orange) - While service-affecting, major alarms are less severe than critical alarms. They reflect conditions that should be addressed in the next 24 hours. An example would be an alarm caused by an unexpected traffic class error.
- **Minor** (yellow) - Minor alarms are not service-affecting and can be addressed at any time. Examples include alarms caused by a user who has not changed their account's default password, a degraded disk, or a software version mismatch.
- **Warning** (blue) - Warning alarms are not service-affecting. They warn of conditions that could become problems over time—for example, an alarm caused by IP SLA being down.

## Alarm Recipients

Complete the following to add alarm recipients to receive an email notifying you of an alarm within your network.

1. Click **Alarm Email Recipients**.
2. Click **Add Recipient**.
3. Enter the following information in the correct fields.

- The Alarm Type is **Orchestrator** for Orchestrator alarms, and **Appliance** for appliance-generated alarms.
- Groups display in a drop-down list, based on the groups configured in the navigation pane.
- By default, alarms are **HTML Formatted**. However, you can choose **Plain Text** or **Both**.
- Plain Text alarms are emailed as pipe-separated data. Users can create a script to parse the email and read the fields.

Example:

```
Hostname|Alarm_Status|Time|Alarm_ID|Type_ID|Source|Severity|Description|Recommended_action

Orchestrator|1|1526341365000|94|6815775|orchestrator|MINOR|Backup configuration not set|


Orchestrator|1|1526341362000|93|6815762|orchestrator|MAJOR|Orchestrator is using the default SMTP settings
```

- The **Alarm ID** is the auto-incremented, primary key in the database.
- **Alarm Status:** 1 - Raised | 2 - Cleared

## Additional Alarm Indications

- A cumulative (Orchestrator + appliances) alarm summary always displays at the right side of the header. Clicking it opens a top-level summary and access to the Alarms tab.
- Appliances are color-coded to indicate their severest alarms on the Topology tab and in the navigation pane.
- **Threshold crossing alerts** are related to alarms. They are preemptive, user-configurable thresholds that declare a Major alarm when crossed. For more information about their configuration and use, see [Threshold Crossing Alerts Template on page 364](#) and [Threshold Crossing Alerts Tab on page 301](#).

## Export Alarm Descriptions

Orchestrator enables you to export to a CSV file a full list of alarms you could potentially receive. This file includes a variety of details about the listed alarms, including alarm descriptions and recommended actions. For details, see [Alarm Descriptions on page 542](#).

To automatically export the CSV file, navigate to **Support > User Documentation > Alarm Descriptions**.

## List of Alarms

This topic provides lists of alarms related to [EdgeConnect appliances](#) and [Orchestrator](#).

**NOTE** The tables in this topic use the decimal numeral system for Alarm ID. You can convert these numbers to the hexadecimal numeral system if you have applications that can do their own filtering, such as SNMP.

## EdgeConnect Appliance Alarms

Appliances can raise alarms based on issues that occur with [tunnels](#), [software](#), [equipment](#), and [Threshold Crossing Alerts \(TCAs\)](#). TCAs are visible on the appliance, but are managed by Orchestrator.

### Tunnels

*System Type 0 (Appliance); Source Type 1 (Tunnel)*

Alarm ID	Alarm Severity	Alarm Text	Source	Service Affecting	Clearable
65537	CRITICAL	<p>Tunnel is down.</p> <p><b>Recommended Action:</b> Tunnel peer is unreachable. Check tunnel configuration. Verify Local &amp; Remote IPs, Admin up, and peer's Mode matches. Check network connectivity.</p>	Appliance	TRUE	TRUE
65539	CRITICAL	<p>Tunnel protocol version mismatch.</p> <p><b>Recommended Action:</b> Tunnel peers are running incompatible software versions. Normal during a software upgrade. Run the same or compatible software releases among the tunnel peers.</p>	Appliance	TRUE	TRUE
65542	CRITICAL	<p>Tunnel peer type mismatch.</p> <p>[For VX-Xpress only]</p> <p><b>Recommended Action:</b> VX-Xpress appliance can only peer with another VX-Xpress appliance. Create a tunnel to another VX-Xpress appliance.</p>	Appliance	TRUE	FALSE
65543	CRITICAL	<p>Duplicate license detected.</p> <p><b>Recommended Action:</b> Duplicate serial numbers detected. Install unique license on all virtual appliances. To check and/or change license:</p> <ul style="list-style-type: none"> <li>• In Appliance Manager: Administration &gt; Basic Settings &gt; License &amp; Registration</li> <li>• In Orchestrator: Configuration &gt; Overlays &amp; Security &gt; Licensing &gt; Licenses</li> </ul>	Appliance	TRUE	TRUE
65544	CRITICAL	<p>Tunnel has invalid source IP address.</p> <p><b>Recommended Action:</b> Delete the tunnel and re-create it with a valid IP address.</p>	Appliance	TRUE	TRUE

Alarm ID	Alarm Severity	Alarm Text	Source	Service Affecting	Clearable
65545	CRITICAL	Tunnel received an unmatched GRE packet. <b>Recommended Action:</b> Check for tunnel encapsulation mismatch. On Configuration > Tunnels page, go to specified tunnel and verify both tunnel peers are using the same encapsulation method.	Appliance	TRUE	TRUE
65536	MAJOR	Tunnel is misconfigured. <b>Recommended Action:</b> System ID is not valid. Was appliance registration completed?	Appliance	TRUE	TRUE
65546	MAJOR	Tunnel is in reduced functionality. <b>Recommended Action:</b> Tunnel peers are not running the same release of software. This results in reduced functionality. Run the same or compatible software releases among the tunnel peers.	Appliance	TRUE	TRUE
65547	MAJOR	Tunnel UDP port conflicts with cluster port. [Deprecated alarm] <b>Recommended Action:</b> Choose another number for UDP Destination Port on local and remote appliances if using the same interface for UDP tunnel and flow redirection.	Appliance	TRUE	TRUE
65541	MINOR	Tunnel software version mismatch. <b>Recommended Action:</b> Tunnel peers are not running the same release of software, but the releases are completely compatible. Normal during an upgrade. Run the same software version to eliminate the alarm.	Appliance	TRUE	TRUE

## Software

*System Type 0 (Appliance); Source Type 4 (Software)*

Alarm ID	Alarm Severity	Alarm Text	Source	Service Affecting	Clearable
262147	CRITICAL	The licensing for this virtual appliance has expired. [For VX series only] <b>Recommended Action:</b> Enter a new license key for the appliance. <b>NOTE</b> The VX appliances are a family of virtual appliances, comprised of the VX-n000 software, an appropriately paired hypervisor and server, and a valid software license.	Appliance	TRUE	FALSE

Alarm ID	Alarm Severity	Alarm Text	Source	Service Affecting	Clearable
262148	CRITICAL	<p>There is no license installed on this virtual appliance.</p> <p>[For VX series only]</p> <p><b>Recommended Action:</b> Enter a valid license key for the appliance.</p> <p><b>NOTE</b> The VX appliances are a family of virtual appliances, comprised of the VX-n000 software, an appropriately paired hypervisor and server, and a valid software license.</p>	Appliance	TRUE	FALSE
262156	CRITICAL	<p>Invalid virtual appliance license.</p> <p>[For VX series only]</p> <p><b>Recommended Action:</b> Enter a valid license key for the appliance.</p>	Appliance	TRUE	FALSE
262166	CRITICAL	<p>Software capability token expired.</p> <p><b>Recommended Action:</b> Portal (30-day token) expired; no communication with Portal in 30 days. You must have HTTPS connectivity to internet to renew the license lease.</p>	Appliance	TRUE	FALSE
262171	CRITICAL	<p>Invalid account name and key.</p> <p><b>Recommended Action:</b> Provide valid account registration information.</p>	Appliance	TRUE	FALSE
262172	CRITICAL	<p>EC Base license not granted.</p> <p><b>Recommended Action:</b> Contact Support to obtain additional EdgeConnect licenses. If you have licenses, approve this appliance from your Orchestrator.</p>	Appliance	TRUE	FALSE
262173	CRITICAL	<p>Orchestrator is unreachable.</p> <p><b>Recommended Action:</b> Appliance cannot connect to Orchestrator using HTTPS. This connectivity is required for Orchestrator to manage the appliance.</p>	Appliance	TRUE	FALSE
262175	CRITICAL	<p>Silver Peak Cloud Portal host name cannot be resolved.</p> <p><b>Recommended Action:</b> Check if appliance has been configured with a reachable DNS server. If there is no DNS server configured, appliance tries to use built-in DNS servers on the Internet to resolve the portal hostname.</p>	Appliance	TRUE	FALSE
262176	CRITICAL	<p>EC Plus license not granted.</p> <p><b>Recommended Action:</b> Contact Support to obtain additional licenses.</p>	Appliance	TRUE	FALSE

Alarm ID	Alarm Severity	Alarm Text	Source	Service Affecting	Clearable
262177	CRITICAL	EC Boost license not granted.  <b>Recommended Action:</b> Contact Support to obtain additional licenses.	Appliance	TRUE	FALSE
262178	CRITICAL	Appliance has not been approved by Orchestrator.  <b>Recommended Action:</b> Approve the appliance from your Orchestrator.	Appliance	TRUE	FALSE
262179	CRITICAL	Software licensing error.  <b>Recommended Action:</b> Failing to get token from Portal. Contact Support.	Appliance	TRUE	FALSE
262180	CRITICAL	No public IP address detected on an interface behind Internet.  [Deprecated alarm]  <b>Recommended Action:</b> Connect the interface to Internet.	Appliance	TRUE	FALSE
262182	CRITICAL	DHCP server misconfiguration.  <b>Recommended Action:</b> DHCP server configuration contains invalid entry that prevented it from running. Check log file for error and verify your configuration.	Appliance	TRUE	FALSE
262185	CRITICAL	Unable to resolve Orchestrator DNS name.  <b>Recommended Action:</b> Could not resolve one or more Orchestrator DNS names. Check DNS server configuration.	Appliance	TRUE	TRUE
262208	CRITICAL	Config DB load partially failed.  <b>Recommended Action:</b> Check configuration and apply again.	Appliance	TRUE	TRUE
262144	MAJOR	Software upgrade process has failed.	Appliance	FALSE	TRUE
262145	MAJOR	System is low on resources.  <b>Recommended Action:</b> The appliance is running low on resources (memory). If this alarm persists, contact Support.	Appliance	TRUE	FALSE
262146	MAJOR	Significant change in time of day has occurred, and might compromise statistics. Please contact TAC.  [Deprecated alarm]  <b>Recommended Action:</b> Appliance time changed. Appliance statistics could be missing for an extended interval. Contact Support.	Appliance	FALSE	TRUE

Alarm ID	Alarm Severity	Alarm Text	Source	Service Affecting	Clearable
262149	MAJOR	<p>A disk self-test has been performed. You must reboot the appliance after the test has been completed.</p> <p><b>Recommended Action:</b> Reboot the appliance. Traffic will not be optimized until this is performed.</p>	Appliance	TRUE	FALSE
262154	MAJOR	<p>Software license will expire in 15 days. [For VX series only]</p> <p><b>Recommended Action:</b> Enter new license key to avoid loss of optimization or potential traffic disruption.</p>	Appliance	FALSE	FALSE
262157	MAJOR	<p>Dual wan-next-hop topology is no longer supported.</p> <p><b>Recommended Action:</b> Reconfigure appliance as single bridge with one next hop, or as dual bridge with two IP addresses and two next hops.</p>	Appliance	TRUE	TRUE
262160	MAJOR	<p>Major inconsistency among tunnel traffic class settings found during upgrade. [Deprecated alarm]</p> <p><b>Recommended Action:</b> Review the WAN shaper traffic class settings.</p>	Appliance	TRUE	TRUE
262161	MAJOR	<p>Tunnel IP header disable setting was discarded during upgrade. [Deprecated alarm]</p> <p><b>Recommended Action:</b> Review the optimization map header compression settings.</p>	Appliance	TRUE	TRUE
262163	MAJOR	<p>A peer name has been specified in the configuration matching no existing remote peer.</p> <p><b>Recommended Action:</b> Correct route-map entry or build tunnel. A route policy peer hostname might have changed.</p>	Appliance	TRUE	FALSE
262165	MAJOR	<p>Software license token needs to be renewed.</p> <p><b>Recommended Action:</b> Software will automatically renew the license lease as long as it has HTTPS connectivity to the internet.</p>	Appliance	FALSE	TRUE
262168	MAJOR	<p>Silver Peak Cloud Portal websocket is down.</p> <p><b>Recommended Action:</b> Appliance cannot connect to Silver Peak portal using HTTPS Websockets.</p>	Appliance	FALSE	TRUE

Alarm ID	Alarm Severity	Alarm Text	Source	Service Affecting	Clearable
262174	MAJOR	Silver Peak Cloud Portal is unreachable for licensing.  <b>Recommended Action:</b> Appliance cannot connect to the Cloud Portal using HTTPS Websockets. Verify the connectivity between the appliance and the portal. This connectivity is needed for licensing.	Appliance	TRUE	FALSE
262184	MAJOR	Subnet table is full.  <b>Recommended Action:</b> Subnet table has reached its maximum allowable size. Additional subnets will not be added unless others are removed.	Appliance	TRUE	TRUE
262188	MAJOR	A BGP peer session is not in Established state.  <b>Recommended Action:</b> A BGP peer session is Down. Verify BGP neighbor, ASN, or next hop IP address is configured correctly.	Appliance	TRUE	TRUE
262190	MAJOR	An OSPF neighbor session is no longer in Full or Two-Way state.  <b>Recommended Action:</b> An OSPF neighbor session is Down. Verify whether OSPF neighbor connectivity still exists on this interface.	Appliance	TRUE	TRUE
262193	MAJOR	DHCP server failover my state communications interrupted.  <b>Recommended Action:</b> DHCP server failover my state communications interrupted. Check for partner reachability and verify your configuration.	Appliance	TRUE	TRUE
262197	MAJOR	Excessive route advertisement updates detected.  <b>Recommended Action:</b> Verify proper configuration or route filtering of the route indicated.	Appliance	TRUE	TRUE
262201	MAJOR	EC Feature License not granted.  <b>Recommended Action:</b> Contact Support.	Appliance	TRUE	FALSE
262205	MAJOR	ACL Groups File Handling Failed.  <b>Recommended Action:</b> Check if valid IP/Port are used for configuration .If issue persists, contact Support with support logs.	Appliance	FALSE	TRUE
262206	MAJOR	ACL Groups Config Memory Limit Exceeded.  <b>Recommended Action:</b> To free up memory, reduce the group name lengths used in the Address/Service groups configuration and try again.	Appliance	FALSE	TRUE

Alarm ID	Alarm Severity	Alarm Text	Source	Service Affecting	Clearable
262207	MAJOR	<p>ACL rule has invalid syntax.</p> <p><b>Recommended Action:</b> Check ACL rules syntax and apply again. Syntax rules:</p> <ul style="list-style-type: none"> <li>Even when using a range or a wildcard, the IPv4 address must be specified in the 4-octet format, separated by the dot notation. For example, <b>A.B.C.D.</b></li> <li>Range is specified using a single dash. For example, <b>128-129</b>.</li> <li>Wildcard is specified as an asterisk (*).</li> <li>Range and Wildcard can both be used in the same address, but an octet can only contain one or the other. For example, <b>10.136-137.*.64-95</b>.</li> <li>A wildcard can only be used to define an entire octet. For example, <b>10.13*.*.64-95</b> is not supported. Use <b>10.130-139.*.64-95</b> to specify this range.</li> <li>The same rules apply to IPv6 addressing.</li> <li>CIDR notation and (Range or Wildcard) are mutually exclusive in the same address. For example, <b>192.168.0.1-127/24</b> is not supported. Use either <b>192.168.0.0/24</b> or <b>192.168.0.1-127</b>.</li> </ul> <p>After fixing the syntax, the alarm does not clear automatically. Clear it manually.</p>	Appliance	TRUE	TRUE
262170	MINOR	<p>Performance is limited by max Boost bandwidth.</p> <p><b>Recommended Action:</b> Recommend subscribing to more Boost bandwidth.</p>	Appliance	FALSE	TRUE
262183	MINOR	<p>Subnet table reached High water mark.</p> <p><b>Recommended Action:</b> Subnet table has reached its maximum level for adding BGP/OSPF-learned routes. Only local subnets added beyond this number.</p>	Appliance	TRUE	TRUE
262194	MINOR	<p>Secure shell challenge-response succeeded.</p> <p><b>Recommended Action:</b> Secure shell authentication succeeded. No action required if authorized personnel are trying to access secure shell.</p>	Appliance	TRUE	TRUE
262195	MINOR	<p>Secure shell challenge-response failed.</p> <p><b>Recommended Action:</b> Secure shell authentication failed. Verify if authorized personnel are trying to access secure shell.</p>	Appliance	TRUE	TRUE

Alarm ID	Alarm Severity	Alarm Text	Source	Service Affecting	Clearable
262199	MINOR	DSCP label is unassigned. <b>Recommended Action:</b> Label is not assigned to interface.	Appliance	TRUE	TRUE
262200	MINOR	Peer interface admin or oper or nh reachability is down. <b>Recommended Action:</b> Peer interface admin or operational or next hop reachability status changed.	Appliance	TRUE	TRUE
262150	WARNING	The SSL private key is invalid. <b>Recommended Action:</b> The key is not an RSA standard key that meets the minimum requirement of 1024 bits. Regenerate a key that meets this minimum requirement.	Appliance	TRUE	FALSE
262151	WARNING	The SSL certificate is not yet valid. <b>Recommended Action:</b> The SSL certificate has a future start date. It will correct itself when the future date becomes current. Otherwise, install a certificate that is current.	Appliance	TRUE	FALSE
262152	WARNING	The SSL certificate has expired. <b>Recommended Action:</b> Reinstall a valid SSL certificate that is current.	Appliance	TRUE	FALSE
262153	WARNING	The NTP server is unreachable. <b>Recommended Action:</b> Check the appliance's NTP server IP and version configuration. Can appliance reach the NTP server? Is UDP port 123 open between the appliance's mgmt0 IP and the NTP server?	Appliance	TRUE	FALSE
262155	WARNING	Software license will expire in 45 days. [For VX series only] <b>Recommended Action:</b> Enter a new license key to avoid loss of optimization or potential traffic disruption.	Appliance	FALSE	TRUE
262158	WARNING	Setting default system wan-next-hop to VLAN next-hop no longer necessary. [Deprecated alarm] <b>Recommended Action:</b> Use the VLAN IP address as tunnel source endpoints instead of bvi0.	Appliance	FALSE	TRUE
262159	WARNING	Minor inconsistency among tunnel traffic class settings found during upgrade. [Deprecated alarm] <b>Recommended Action:</b> Review the WAN shaper traffic class settings.	Appliance	FALSE	TRUE

Alarm ID	Alarm Severity	Alarm Text	Source	Service Affecting	Clearable
262162	WARNING	A very large range has been configured for a local subnet.  <b>Recommended Action:</b> Confirm that you intended to configure such a large local subnet (/8 or larger).	Appliance	FALSE	TRUE
262164	WARNING	Interface shaper max bandwidth exceeds system max bandwidth.  <b>Recommended Action:</b> Review the interface shaper max bandwidth settings. Make sure it does not exceed system max bandwidth.	Appliance	TRUE	TRUE
262167	WARNING	Silver Peak Cloud Portal is unreachable.  <b>Recommended Action:</b> Appliance cannot connect to the Cloud Portal using HTTPS. This connectivity is needed for internet applications classification.	Appliance	FALSE	TRUE
262169	WARNING	SaaS application is no longer supported.  <b>Recommended Action:</b> SaaS application is no longer supported.	Appliance	FALSE	TRUE
262181	WARNING	Admin password is not yet changed.  <b>Recommended Action:</b> Change admin password.	Appliance	FALSE	TRUE
262186	WARNING	Built-in CA certificate was invalid and it has been deleted internally.  <b>Recommended Action:</b> Built-in CA Certificate is invalid, and a new one has been auto-generated. Install the built-in CA certificate on clients as needed.	Appliance	FALSE	TRUE
262187	WARNING	CA Bundle was invalid and it has been deleted internally.  <b>Recommended Action:</b> CA Certificate Bundle is invalid and will be fixed automatically by portal in a couple of hours, or contact Support.	Appliance	FALSE	TRUE
262189	WARNING	An IP SLA monitor is in the Down state.  <b>Recommended Action:</b> An IP SLA monitor has reported Down status. Check and correct the source of the failure.	Appliance	TRUE	TRUE
262191	WARNING	DNS proxy process is in Down state.  <b>Recommended Action:</b> DNS proxy is in down state.	Appliance	TRUE	TRUE
262192	WARNING	EC Licensing Warning.  <b>Recommended Action:</b> Check your EC license.	Appliance	FALSE	TRUE

Alarm ID	Alarm Severity	Alarm Text	Source	Service Affecting	Clearable
262196	WARNING	An IP SLA monitor is not installed.  <b>Recommended Action:</b> An IP SLA monitor is not installed. Check and fix the source of the failure.	Appliance	TRUE	TRUE
262198	WARNING	CPU utilization threshold exceeded.  <b>Recommended Action:</b> CPU utilization reached almost 100%. Ignore if it is intended. Otherwise, take action to reduce CPU utilization.	Appliance	TRUE	TRUE
262202	WARNING	Stats collection slow or incomplete.  <b>Recommended Action:</b> In Orchestrator, go to Orchestrator > Software & Setup > Setup > Stats Collector Configuration and look for the following issues: 1. Stats collection paused due to low disk space. 2. Stats collection failing because the Stats Collector is unreachable. 3. Too many appliances assigned to a single Stats Collector.	Appliance	FALSE	TRUE
262203	WARNING	Unable to resolve Stats Collector DNS name.  <b>Recommended Action:</b> Could not resolve Stats Collector DNS name. Check DNS server configuration.	Appliance	FALSE	TRUE
262204	WARNING	Stats Collector is unreachable.  <b>Recommended Action:</b> Appliance cannot connect to Stats Collector using HTTPS. This connectivity is required for Appliance to upload stats.	Appliance	FALSE	TRUE

## Equipment

*System Type 0 (Appliance); Source Type 3 (Equipment)*

Alarm ID	Alarm Severity	Alarm Text	Source	Service Affecting	Clearable
196608	CRITICAL	RAID array is degraded. [Deprecated alarm]	Appliance	FALSE	TRUE
196611	CRITICAL	Fan failure detected.  <b>Recommended Action:</b> Fan failure. Use the self-service RMA tool on the Silver Peak Support Portal to RMA the failed device.	Appliance	FALSE	FALSE

Alarm ID	Alarm Severity	Alarm Text	Source	Service Affecting	Clearable
196612	CRITICAL	<p>System bypass mode.</p> <p><b>Recommended Action:</b> Normal with factory default configuration, during reboot, and if user has put the appliance in bypass mode. Check the system bypass configuration.</p>	Appliance	FALSE	FALSE
196613	CRITICAL	<p>LAN/WAN fail-to-wire card failure.</p> <p><b>Recommended Action:</b> Fail-to-wire card failure. Use the self-service RMA tool on the Silver Peak Support Portal to RMA the failed device.</p>	Appliance	FALSE	FALSE
196614	CRITICAL	LAN/WAN fail-to-wire card relay failure.	Appliance	FALSE	FALSE
196615	CRITICAL	<p>Encryption card hardware failure.</p> <p>[Deprecated alarm]</p> <p><b>Recommended Action:</b> Disk encryption card failure. Use the self-service RMA tool on the Silver Peak Support Portal to RMA the failed device.</p>	Appliance	FALSE	FALSE
196641	CRITICAL	<p>NIC failure.</p> <p><b>Recommended Action:</b> Network interface card failure. Use the self-service RMA tool on the Silver Peak Support Portal to RMA the failed device.</p>	Appliance	FALSE	FALSE
196644	CRITICAL	<p>Insufficient configured memory size for this virtual appliance.</p> <p>[For VX series only]</p> <p><b>Recommended Action:</b> Assign more memory to the virtual machine and restart the appliance. Traffic will not be optimized until this is resolved.</p>	Appliance	TRUE	FALSE
196645	CRITICAL	<p>Insufficient configured processor count for this virtual appliance.</p> <p>[For VX series only]</p> <p><b>Recommended Action:</b> Assign more processors to the virtual machine and restart the appliance. Traffic will not be optimized until this is resolved.</p>	Appliance	TRUE	FALSE
196646	CRITICAL	<p>Insufficient configured disk storage for this virtual appliance.</p> <p>[For VX series only]</p> <p><b>Recommended Action:</b> Assign more storage to the virtual machine and restart the appliance. Traffic will not be optimized until this is resolved.</p>	Appliance	TRUE	FALSE

Alarm ID	Alarm Severity	Alarm Text	Source	Service Affecting	Clearable
196649	CRITICAL	Bridge loop is detected.  <b>Recommended Action:</b> Make sure bridge ports are connected to different virtual switches and restart the appliance. Traffic will not be optimized until this is resolved.	Appliance	TRUE	FALSE
196650	CRITICAL	Network interface is unassigned.  <b>Recommended Action:</b> Assign the network interface to an existing MAC address, and then restart the appliance. Or, if the network interface is not being used, then set its admin state to down.	Appliance	TRUE	FALSE
196651	CRITICAL	Bridge creation failed.  <b>Recommended Action:</b> Check log messages for more details on the failure.	Appliance	TRUE	FALSE
196609	MAJOR	Disk is failed.  <b>Recommended Action:</b> Disk failure. Use the self-service RMA tool on the Silver Peak Support Portal to RMA the failed hard disk drive.	Appliance	FALSE	FALSE
196617	MAJOR	Network interface link down.  <b>Recommended Action:</b> Is the system in bypass mode? Check cables and interface admin status on the router.	Appliance	TRUE	TRUE
196618	MAJOR	Management interface link down.  <b>Recommended Action:</b> Check cables and interface admin status on the router.	Appliance	TRUE	TRUE
196619	MAJOR	Interface is half duplex.  <b>Recommended Action:</b> Check speed/duplex settings on the router/switch port.	Appliance	TRUE	TRUE
196620	MAJOR	Interface speed is 10 Mbps.  <b>Recommended Action:</b> Check speed/duplex settings. Use a 100/1000 Mbps port on the router/switch.	Appliance	TRUE	TRUE
196621	MAJOR	Config DB disk full. [Deprecated alarm]	Appliance	TRUE	FALSE
196622	MAJOR	Operating System disk full. [Deprecated alarm]	Appliance	TRUE	FALSE
196623	MAJOR	File System disk full. [Deprecated alarm]	Appliance	TRUE	FALSE
196624	MAJOR	Datapath internal loopback test failed. [Deprecated alarm]	Appliance	TRUE	FALSE

Alarm ID	Alarm Severity	Alarm Text	Source	Service Affecting	Clearable
196625	MAJOR	<p>WAN Next-hop unreachable.</p> <p><b>Recommended Action:</b></p> <ul style="list-style-type: none"> <li>Check cables on EdgeConnect appliance and router.</li> <li>Check IP/mask on EdgeConnect appliance and router. Next hop should be only a single IP hop away.</li> <li>To troubleshoot, use:  <code>show cdp neighbor,</code>  <code>show arp,</code>          and  <code>ping -I &lt;appliance IP&gt;</code>  <code>&lt;next-hop IP&gt;</code></li> <li>Packets are sent with ttl=1, so ensure next hop IP has no intermediate routers.</li> </ul> <p><b>NOTE</b> If there is either a LAN Next-Hop Unreachable or WAN Next-Hop Unreachable alarm, resolve the alarm(s) immediately by configuring the gateway(s) to respond to ICMP pings from the EdgeConnect appliance IP Address.</p>	Appliance	TRUE	FALSE
196626	MAJOR	<p>VRRP instance is down.</p> <p><b>Recommended Action:</b> Check the interface. Is the link down?</p>	Appliance	TRUE	TRUE
196628	MAJOR	<p>WAN next-hop router discovered on a LAN port (box is in backwards).</p> <p><b>Recommended Action:</b></p> <ul style="list-style-type: none"> <li>Check WAN next hop IP address.</li> <li>Check lan0 and wan0 cabling (in-line mode only).</li> <li>If not resolved, contact Support.</li> </ul>	Appliance	TRUE	FALSE
196629	MAJOR	<p>Disk is not-in-service.</p> <p><b>Recommended Action:</b> Check if the disks are properly seated. Contact Support for further assistance.</p>	Appliance	FALSE	FALSE
196631	MAJOR	<p>Disk has been removed by operator.</p> <p><b>Recommended Action:</b> Normal during disk replacement. Insert the disk using Appliance Manager or Orchestrator. Contact Support if insertion fails.</p>	Appliance	FALSE	FALSE

Alarm ID	Alarm Severity	Alarm Text	Source	Service Affecting	Clearable
196632	MAJOR	<p>LAN/WAN interfaces have different admin states.</p> <p>[For Bridge mode only]</p> <p><b>Recommended Action:</b> Check interface admin configuration (lan0-wan0, lan1-wan1). Applicable only to in-line mode.</p>	Appliance	TRUE	TRUE
196633	MAJOR	<p>LAN/WAN interfaces have different link carrier states.</p> <p>[For Bridge mode only]</p> <p><b>Recommended Action:</b> Check interface configured speed settings and current values (lan0/wan0, lan1/wan1). Applicable only to in-line mode.</p>	Appliance	TRUE	TRUE
196634	MAJOR	<p>LAN/WAN interface has been shut down due to link propagation of paired interface.</p> <p>[For Bridge mode only]</p> <p><b>Recommended Action:</b> Check cables and connectivity. For example, if lan0 is shut down, check why wan0 is down. Applicable only to in-line mode.</p>	Appliance	TRUE	TRUE
196636	MAJOR	<p>Flow redirection cluster peer is down.</p> <p>[For Boost only]</p> <p><b>Recommended Action:</b> Check Flow Redirection configuration on all applicable appliances and check L3/L4 connectivity between the peers. Open TCP and UDP ports 4164 between the cluster peer IPs if they are blocked.</p>	Appliance	TRUE	FALSE
196637	MAJOR	<p>Bonding members have different speed/duplex.</p> <p><b>Recommended Action:</b> Check interface speed/duplex settings and negotiated values on wan0/wan1 and lan0/lan1 ether-channel groups.</p>	Appliance	TRUE	TRUE
196638	MAJOR	<p>WCCP adjacency(ies) down.</p> <p><b>Recommended Action:</b> Cannot establish WCCP neighbor. Check WCCP configuration on appliance and router. Verify reachability. Enable debugging on router: <code>debug ip wccp packet</code></p>	Appliance	TRUE	TRUE

Alarm ID	Alarm Severity	Alarm Text	Source	Service Affecting	Clearable
196639	MAJOR	<p>WCCP assignment table mismatch.</p> <p><b>Recommended Action:</b> Check WCCP mask/hash assignment configuration on all EdgeConnect appliances and ensure that they match.</p>	Appliance	TRUE	TRUE
196640	MAJOR	<p>Power supply not connected, not powered, or failed.</p> <p>[EC-M, EC-L, and EC-XL only (dual supplies)]</p> <p><b>Recommended Action:</b> Connect to a power outlet. Check power cable connectivity.</p>	Appliance	FALSE	FALSE
196642	MAJOR	<p>LAN next-hop unreachable.</p> <p><b>Recommended Action:</b> Check Appliance configuration: LAN side next hop IP, Appliance IP/Mask, VLAN IP/mask, and VLAN ID.</p> <p><b>NOTE</b> If there is either a LAN Next-Hop Unreachable or WAN Next-Hop Unreachable alarm, resolve the alarm(s) immediately by configuring the gateway(s) to respond to ICMP pings from the EdgeConnect appliance IP Address.</p>	Appliance	TRUE	FALSE
196643	MAJOR	<p>Unexpected system restart.</p> <p><b>Recommended Action:</b> The appliance rebooted unexpectedly. Power issues? Was the appliance shut down ungracefully? Contact Support if the shutdown was not planned.</p>	Appliance	FALSE	TRUE
196647	MAJOR	<p>Interfaces have different MTUs.</p> <p>[For Bridge mode only: lan0/wan0]</p> <p><b>Recommended Action:</b> Check interface MTU settings on lan0/wan0 (pairwise) on dual bridge mode and lan0/lan1/wan0/wan1... on single bridge mode.</p>	Appliance	TRUE	TRUE
196648	MAJOR	<p>Interfaces have different MTUs.</p> <p>[For Bridge mode only: lan1/wan1]</p> <p><b>Recommended Action:</b> Check interface MTU settings on lan1/wan1 or tlan1/twan1 interfaces.</p>	Appliance	TRUE	TRUE
196652	MAJOR	<p>System optimization disabled.</p> <p>[Deprecated alarm]</p> <p><b>Recommended Action:</b> Turn on system optimization.</p>	Appliance	TRUE	FALSE
196656	MAJOR	<p>HASync peer is down.</p> <p><b>Recommended Action:</b> Check HA link connectivity.</p>	Appliance	TRUE	FALSE

Alarm ID	Alarm Severity	Alarm Text	Source	Service Affecting	Clearable
196610	MINOR	Disk is degraded.  <b>Recommended Action:</b> Wait for disk to recover. If it does not recover, contact Support.	Appliance	FALSE	FALSE
196630	MINOR	Disk is rebuilding.  <b>Recommended Action:</b> Normal. Wait for the disk to rebuild. If it does not rebuild, contact Support.	Appliance	FALSE	FALSE
196635	MINOR	Disk SMART threshold exceeded.  <b>Recommended Action:</b> Disk failure. Use the self-service RMA tool on the Silver Peak Support Portal to RMA the failed hard disk drive.	Appliance	FALSE	TRUE
196653	MINOR	Non-optimal configured memory size for this virtual appliance.  [For VX series only]  <b>Recommended Action:</b> Assign more memory to the virtual machine and restart the appliance. Traffic will be sub-optimal until this is resolved.	Appliance	TRUE	TRUE
196654	MINOR	Non-optimal configured processor count for this virtual appliance.  [For VX series only]  <b>Recommended Action:</b> Assign more processors to the virtual machine and restart the appliance. Traffic will be sub-optimal until this is resolved.	Appliance	TRUE	TRUE
196655	MINOR	Non-optimal configured disk storage for this virtual appliance.  [For VX series only]  <b>Recommended Action:</b> Assign more storage to the virtual machine and restart the appliance. Traffic will be sub-optimal until this is resolved.	Appliance	TRUE	TRUE
196616	WARNING	Network interface admin down.  <b>Recommended Action:</b> Check your interface configuration.	Appliance	TRUE	TRUE
196627	WARNING	VRRP state changed from Master to Backup.  <b>Recommended Action:</b> VRRP state has changed from Master to Backup. Check VRRP Master for uptime and connectivity.	Appliance	TRUE	TRUE

## Threshold Crossing Alerts

*System Type 0 (Appliance); Source Type 5 (Threshold Crossing Alerts)*

Alarm ID	Alarm Severity	Alarm Text	Source	Service Affecting	Clearable
327681	WARNING	WAN Tx throughput threshold exceeded. <b>Recommended Action:</b> User configured. Check bandwidth reports for tunnel bandwidth.	Appliance	FALSE	TRUE
327682	WARNING	LAN Rx throughput threshold exceeded. [LAN Rx outbound] <b>Recommended Action:</b> User configured. Check bandwidth reports.	Appliance	FALSE	TRUE
327683	WARNING	Optimized flows count threshold exceeded. <b>Recommended Action:</b> User configured. Check flow and real-time connection reports.	Appliance	FALSE	TRUE
327684	WARNING	Total flows count threshold exceeded. <b>Recommended Action:</b> User configured. Check flow and real-time connection reports.	Appliance	FALSE	TRUE
327685	WARNING	File system utilization threshold exceeded. <b>Recommended Action:</b> Disk is almost full. Under Support > Debug files, delete the old tcpdumps, snapshots sysdumps, and show-tech files.	Appliance	FALSE	TRUE
327686	WARNING	Latency threshold exceeded. <b>Recommended Action:</b> User Configured. Check Latency reports. If latency is too high, check routing between the appliances and QoS policy on upstream routers. Check tunnel DSCP marking. If latency persists, contact Internet Service Provider (ISP) and Support.	Appliance	FALSE	TRUE
327687	WARNING	Pre-FEC loss threshold exceeded. <b>Recommended Action:</b> User configured. Check Loss Reports. Check for loss between EdgeConnect appliances (interface counters on upstream routers). Use network bandwidth measurement tools, such as iperf, to measure loss. Contact Internet Service Provider (ISP).	Appliance	FALSE	TRUE

Alarm ID	Alarm Severity	Alarm Text	Source	Service Affecting	Clearable
327688	WARNING	<p>Post-FEC loss threshold exceeded.</p> <p><b>Recommended Action:</b> User configured. Check Loss Reports. Check for loss between EdgeConnect appliances (interface counters on upstream routers). Use network bandwidth measurement tools, such as iperf, to measure loss. Enable/Adjust Silver Peak Forward Error Correction (FEC). Contact ISP (Internet Service Provider).</p>	Appliance	FALSE	TRUE
327689	WARNING	<p>Out of order packets threshold exceeded.</p> <p><b>Recommended Action:</b> User configured. Check Out-of-Order Packets Reports. Normal in a network with multiple paths and different QoS queues. Normal in a dual-homed router or four port in-line configuration. Contact Support if out-of-order packets are not 100% corrected.</p>	Appliance	FALSE	TRUE
327690	WARNING	<p>Corrected out of order packets threshold exceeded.</p> <p><b>Recommended Action:</b> User configured. Check Out-of-Order Packets Reports. Normal in a network with multiple paths and different QoS queues. Normal in a dual-homed router or four port in-line configuration. Contact Support if out-of-order packets are not 100% corrected.</p>	Appliance	FALSE	TRUE
327691	WARNING	<p>Bandwidth utilization threshold exceeded.</p> <p><b>Recommended Action:</b> User configured. Check bandwidth reports for tunnel bandwidth utilization.</p>	Appliance	FALSE	TRUE
327692	WARNING	<p>Low reduction threshold exceeded. [For Boost]</p> <p><b>Recommended Action:</b> User configured. Check bandwidth reports for dedupe. Check if the traffic is pre-compressed or encrypted.</p>	Appliance	FALSE	TRUE
327693	WARNING	<p>Appliance flow limit threshold exceeded.</p> <p><b>Recommended Action:</b> If this condition persists, a larger appliance will be necessary to fully optimize all flows.</p>	Appliance	FALSE	TRUE

## Orchestrator Alarms

Orchestrator can raise alarms based on issues with [tunnels](#), [software](#), and [equipment](#).

## Tunnels

*System Type 100 (Orchestrator); Source Type 1 (Tunnel)*

Alarm ID	Alarm Severity	Alarm Text	Source	Service Affecting	Clearable
6619136	CRITICAL	Interfaces with duplicate IP exists: {0}. <b>Recommended Action:</b> No overlays will be applied to appliances with duplicate IP address.	/orchestrator/interfaces	TRUE	FALSE
6619137	CRITICAL	Interfaces with no public IP exists: {0}. <b>Recommended Action:</b> No overlays will be applied to appliances with duplicate IP address.	/orchestrator/interfaces	TRUE	FALSE
6619138	CRITICAL	Failed to apply overlays. <b>Recommended Action:</b> No overlays will be applied to appliances with duplicate IP address.	/orchestrator/orchestration/overlays	TRUE	FALSE
6619139	CRITICAL	ACL used in an overlay is not defined on the appliance. acl name: {0} overlay name: {1}. <b>Recommended Action:</b> ACLs can be created on the appliance by applying ACL templates.	/orchestrator/orchestration/overlays	TRUE	FALSE
6619140	CRITICAL	Interfaces with duplicate wan label exists: {0}. <b>Recommended Action:</b> Assign unique labels to all WAN interfaces. No overlays will be applied to appliances with duplicate WAN labels.	/orchestrator/interfaces	TRUE	FALSE
6619141	CRITICAL	Interfaces with duplicate public IP exists: {0}. <b>Recommended Action:</b> No overlays will be applied to appliances with duplicate IP addresses.	/orchestrator/interfaces	TRUE	FALSE
6619142	CRITICAL	Failed to apply tunnel group. <b>Recommended Action:</b> Refer to the Audit logs for more details.	/orchestrator/orchestration/tunnelgroups	TRUE	FALSE
6619143	CRITICAL	Interface has bad IP address: {0}. <b>Recommended Action:</b> No overlay tunnels will be built using this interface.	/orchestrator/interfaces	TRUE	FALSE
6619146	CRITICAL	Cannot build tunnel with src IP {0} and dest IP {1}. IP versions mismatch. <b>Recommended Action:</b> Make sure the tunnel source and destination IP address are both ipv4 or are both ipv6 addresses.	/orchestrator/orchestration/tunnels	TRUE	TRUE

Alarm ID	Alarm Severity	Alarm Text	Source	Service Affecting	Clearable
6619147	CRITICAL	<p>Failed to apply labels.</p> <p><b>Recommended Action:</b> Refer to the Audit logs for more details.</p>	/orchestrator/orchestration	TRUE	FALSE
6619148	CRITICAL	<p>Failed to apply internal subnets.</p> <p><b>Recommended Action:</b> Refer to the Audit logs for more details.</p>	/orchestrator/orchestration	TRUE	FALSE
6619149	CRITICAL	<p>Failed to apply application classification data to appliance.</p> <p><b>Recommended Action:</b> Make sure the appliance can connect to Orchestrator. Refer to the Audit logs for more details.</p>	/orchestrator/orchestration/applications	TRUE	FALSE
6619150	CRITICAL	<p>Appliance has the same IPSec UDP port as the other HA peer overlays will not be applied to this appliance. HA Peer: {0}.</p> <p><b>Recommended Action:</b> You can change the IPSec UDP Port of an appliance by editing the System Information from the System Information tab.</p>	/orchestrator/orchestration/tunnels/ha	TRUE	FALSE
6619151	CRITICAL	<p>Both Overlay Manager and Tunnel Group manager are ENABLED.</p> <p><b>Recommended Action:</b> You can enable one or the other. Turn one of them OFF.</p>	/orchestration	TRUE	FALSE
6619152	CRITICAL	<p>Overlay {0} has no hub defined. No tunnels will be built between appliances that are part of this overlay.</p> <p><b>Recommended Action:</b> To add a Hub to an Overlay, either (1) apply the Overlay to a Hub appliance or (2) go to the Hubs tab and make an appliance that is currently in the Overlay a Hub.</p>	/orchestration/overlays	TRUE	FALSE
6619153	CRITICAL	<p>Overlay {0} has no WAN ports defined. No tunnels will be built between appliance that are part of this overlay.</p> <p><b>Recommended Action:</b> At least 1 WAN port needs to be defined in an overlay.</p>	/orchestration/overlays	TRUE	FALSE
6619154	CRITICAL	<p>Tunnel Group {0} has no hub defined. No tunnels will be built between appliances that are part of this tunnel group.</p> <p><b>Recommended Action:</b> To add a Hub to a Tunnel Group, either (1) apply the Tunnel Group to a Hub appliance or (2) go to the Hubs tab and make an appliance that is currently in the Tunnel Group a Hub.</p>	/orchestration/tunnelgroups	TRUE	FALSE

Alarm ID	Alarm Severity	Alarm Text	Source	Service Affecting	Clearable
6619155	CRITICAL	Tunnel Group {0} has no interfaces defined. No tunnels will be built between appliances that are part of this tunnel group.  <b>Recommended Action:</b> Go to Tunnel Groups to configure interfaces.	/orchestration/tunnelgroups	TRUE	FALSE
6619156	CRITICAL	Failed to apply templates.  <b>Recommended Action:</b> One or more templates failed to apply. Refer to the Audit Logs for more details.	/orchestrator/orchestration/templates	TRUE	FALSE
6619157	CRITICAL	Failed to apply port forwarding rules to appliance.  <b>Recommended Action:</b> Make sure appliance can connect to Orchestrator. Refer to the Audit logs for more details.	/orchestrator/orchestration	TRUE	FALSE
6619158	CRITICAL	Overlay {0} is using local breakout without any interfaces selected.  <b>Recommended Action:</b> Go to Business Intent Overlays to configure local break out interface.	/orchestration/overlays	TRUE	FALSE
6619159	CRITICAL	Maximum number of tunnels exceeded. {0}.  <b>Recommended Action:</b> Configure Overlays to create fewer tunnels.	/orchestrator/orchestration/tunnels	FALSE	FALSE
6619160	CRITICAL	At least one region is missing a hub appliance.  <b>Recommended Action:</b> To add a Hub to an Overlay, either (1) apply the Overlay to a Hub appliance or (2) go to the Hubs tab and make an appliance that is currently in the Overlay a Hub.	/orchestration/overlays	TRUE	FALSE
6619161	CRITICAL	Appliance has a duplicate hostname with another appliance in the network. No overlays will be built to this appliance.  <b>Recommended Action:</b> Change the hostname of one of the appliances.	/orchestrator/orchestration/tunnels	FALSE	FALSE
6619166	CRITICAL	Orchestration failed. {0}.  <b>Recommended Action:</b> Go to the Audit Logs for more details.	/orchestrator/orchestration	TRUE	FALSE

Alarm ID	Alarm Severity	Alarm Text	Source	Service Affecting	Clearable
6619168	CRITICAL	<p>Duplicate IPSec UDP Port {0} detected on the following appliances [{1}] that belong to site "{2}". Appliances sharing the same site name must have unique IPSec UDP port numbers. Orchestration for these appliances will be suspended until this is addressed.</p> <p><b>Recommended Action:</b> You can change the IPSec UDP Port of an appliance on the System Information tab.</p>	/orchestrator/orchestration/tunnels	TRUE	FALSE
6619173	CRITICAL	<p>Failed to apply traffic behavior data to appliance.</p> <p><b>Recommended Action:</b> Make sure appliance can connect to Orchestrator. Refer to the Audit logs for more details.</p>	/orchestrator/orchestration	TRUE	FALSE
6619174	CRITICAL	<p>Appliance does not have geo location information. Zscaler ZENs cannot be auto discovered.</p> <p><b>Recommended Action:</b> Update appliance location in Configuration Wizard.</p>	/orchestrator/orchestration/zscaler	TRUE	FALSE
6619175	CRITICAL	<p>Only IPSec UDP tunnel mode is supported on Edge HA devices.</p> <p><b>Recommended Action:</b> Check Tunnel Settings.</p>	/orchestration	TRUE	TRUE
6619177	CRITICAL	<p>Edge HA peer {0} has tunnels with source port {1}. Orchestration will be skipped for this appliance until the conflicting tunnels are deleted.</p> <p><b>Recommended Action:</b> Wait for the conflicting tunnels to tear down.</p>	/orchestrator/orchestration/tunnels	TRUE	FALSE
6619178	CRITICAL	<p>This appliance and appliances [{0}] have been manually configured with same IPSec UDP port {1}. Orchestration will be paused on all the conflicting appliances until unique ports are assigned to the appliance.</p> <p><b>Recommended Action:</b> You can change the IPSec UDP Port of an appliance on the System Information tab.</p>	/orchestrator/orchestration/tunnels	TRUE	FALSE
6619189	CRITICAL	<p>{0} exceeded threshold {1} by {2}% ({3}) at {4}.</p> <p><b>Recommended Action:</b> Check internal LAN.</p>	/orchestrator/internaldrops	FALSE	TRUE
6619172	MAJOR	Failed to create/update Check Point CloudGuard site: {0}.	/orchestrator/integration/checkPoint	FALSE	TRUE

Alarm ID	Alarm Severity	Alarm Text	Source	Service Affecting	Clearable
6619144	MINOR	<p>Appliance does not have any wan labels required for an overlay. No tunnels will be built on this appliance for the overlay.</p> <p>Overlay name: {0} wan labels: {1}.</p> <p><b>Recommended Action:</b> Assign at least one wan label selected for this overlay in the deployment configuration of the appliance.</p>	/orchestrator/orchestration/overlays	TRUE	TRUE
6619145	MINOR	<p>Appliance missing lan label {1} for traffic access policy of overlay. No traffic on this appliance will be routed to the overlay.</p> <p>Overlay name: {0}.</p> <p><b>Recommended Action:</b> Assign a lan port the required lan label selected for this overlay in the deployment configuration of the appliance. If this appliance is in server mode, you should use an ACL instead of selecting a lan label in the overlay configuration.</p>	/orchestrator/orchestration/overlays	TRUE	TRUE
6619163	WARNING	<p>Mesh Overlay - {0} has no hub defined. No tunnels will be built for Hub &amp; Spoke Interface label {1} for this overlay.</p> <p><b>Recommended Action:</b> To add a Hub to an Overlay, either (1) apply the Overlay to a Hub appliance or (2) go to the Hubs tab and make an appliance that is currently in the Overlay a Hub.</p>	/orchestration/overlays	TRUE	FALSE
6619164	WARNING	<p>Mesh Tunnel Group - {0} has no hub defined. No tunnels will be built for Hub &amp; Spoke Interface label {1} for this group.</p> <p><b>Recommended Action:</b> To add a Hub to a Tunnel Group, either (1) apply the Tunnel Group to a Hub appliance or (2) go to the Hubs tab and make an appliance that is currently in the Tunnel Group a Hub.</p>	/orchestration/tunnelgroups	TRUE	FALSE
6619165	WARNING	<p>Appliance does not have public IP for wan label {0} auto discovered Zscaler Service Edges may not be correct.</p> <p><b>Recommended Action:</b> In the Deployment page, toggle the Not Behind NAT flag to NAT, or create a Service Edge Override on the Zscaler tab.</p>	/orchestrator/orchestration/zscaler	FALSE	FALSE

Alarm ID	Alarm Severity	Alarm Text	Source	Service Affecting	Clearable
6619167	WARNING	<p>At least one hub is not part of any overlay.</p> <p><b>Recommended Action:</b> To add a Hub to an Overlay, either (1) apply the Overlay to a Hub appliance or (2) go to the Hubs tab and make an appliance that is currently in the Overlay a Hub.</p>	/orchestration/overlays	TRUE	FALSE
6619169	WARNING	<p>At least one appliance is associated with a region and regional routing is currently disabled.</p> <p><b>Recommended Action:</b> If regional routing is desired and has been authorized, go to Regional Routing and enable the feature.</p>	/orchestration	TRUE	TRUE
6619170	WARNING	<p>{0} is only supported on inline router deployment mode appliances.</p> <p><b>Recommended Action:</b> Choose "Deployment &gt; Router" mode.</p>	/orchestrator	FALSE	TRUE
6619171	WARNING	<p>Regional routing is enabled but {0} not associated with any region, so no tunnel will be built.</p> <p><b>Recommended Action:</b> Associate the appliance with a region or disable regional routing.</p>	/orchestration	TRUE	TRUE
6619176	WARNING	<p>{0} Appliance {1} Bandwidth for {2} interface is below min threshold.</p> <p><b>Recommended Action:</b> In Deployment page, update Inbound/outbound interface Bandwidth to be above the minimum Bandwidth (Orchestrator &gt; Advanced Properties &gt; interfaceBandwidthCheckPerTunnelOverhead).</p>	/orchestrator/interfaceBandwidth	TRUE	FALSE

## Software

*System Type 100 (Orchestrator); Source Type 4 (Software)*

Alarm ID	Alarm Severity	Alarm Text	Source	Service Affecting	Clearable
6815744	CRITICAL	Orchestrator detected possible cloned appliances - cloned: {0} clone: {1}.	/orchestrator/discovery/clone	FALSE	TRUE
6815745	CRITICAL	Appliance backup failed: {0}.	/orchestrator/system/backup	FALSE	TRUE

Alarm ID	Alarm Severity	Alarm Text	Source	Service Affecting	Clearable
6815746	CRITICAL	<p>Appliances with the same serial numbers exist: {0}.</p> <p><b>Recommended Action:</b> If your appliances have duplicate serial numbers you may have applied the same license key on the appliances. They may also be cloned appliances if they are cloned. Contact Support for the correct steps on cloning appliances.</p>	/orchestrator/system	TRUE	TRUE
6815748	CRITICAL	Orchestrator cannot reach this appliance.	/orchestrator/connectivity	TRUE	TRUE
6815749	CRITICAL	Appliance version not supported: {0}.	/orchestrator/system	TRUE	TRUE
6815752	CRITICAL	<p>Appliance is configured with labels to build IPsec UDP tunnels, but the appliance version does not support IPsec UDP tunnels.</p> <p><b>Recommended Action:</b> You can change the tunnel modes for labels in the Overlay Manager Settings.</p>	/orchestrator/orchestration/tunnels	TRUE	FALSE
6815754	CRITICAL	<p>Orchestrator requires a validated portal account name and key (or for NX/VX/VRX, a valid license key).</p> <p><b>Recommended Action:</b> Go to Licensing to provide the required information.</p>	/license	TRUE	FALSE
6815757	CRITICAL	<p>Orchestrator portal account or license expired on {0 date}.</p> <p><b>Recommended Action:</b> Go to Licensing to provide the required information.</p>	/license	TRUE	FALSE
6815758	CRITICAL	<p>Orchestrator cannot connect to Silver Peak portal using HTTPS.</p> <p><b>Recommended Action:</b> Check portal connection and refer to the Audit Logs for more information.</p>	/portal/connectivity	TRUE	TRUE

Alarm ID	Alarm Severity	Alarm Text	Source	Service Affecting	Clearable
6815760	CRITICAL	Orchestrator cannot register with Silver Peak portal using credentials provided. <b>Recommended Action:</b> Go to Licensing to provide the required information.	/portal/registration	TRUE	TRUE
6815766	CRITICAL	CPX license expired on {0 date}. [Deprecated alarm] <b>Recommended Action:</b> Renew your license to avoid service interruption.	/portal/license/cpx	TRUE	TRUE
6815770	CRITICAL	Your EdgeConnect account expired on {0 date}. EdgeConnect devices in your network will stop passing traffic. <b>Recommended Action:</b> Renew your license to avoid service interruption.	/portal/license/ec	TRUE	TRUE
6815774	CRITICAL	SaaS license expired on {0 date}. <b>Recommended Action:</b> Renew your license to avoid service interruption.	/portal/license/saas	TRUE	TRUE
6815778	CRITICAL	Discovered appliances list contains cloned appliances. Clones: {0}. <b>Recommended Action:</b> Contact Support for information on how to correctly clone appliances.	/discovery/clone	FALSE	TRUE
6815779	CRITICAL	Orchestrator backup failed. <b>Recommended Action:</b> Go to Historical Jobs for details.	/system/backup	FALSE	TRUE
6815780	CRITICAL	Orchestrator failed to get update from portal for application definition data. <b>Recommended Action:</b> Check portal connection and refer to the Audit Logs for more information.	/orchestration/applications	FALSE	TRUE

Alarm ID	Alarm Severity	Alarm Text	Source	Service Affecting	Clearable
6815782	CRITICAL	Orchestrator failed to get update from portal for traffic behavior data.  <b>Recommended Action:</b> Check portal connection and refer to the Audit Logs for more information.	/orchestration/applications	FALSE	TRUE
6815790	CRITICAL	Orchestrator is not registered with Silver Peak portal.  <b>Recommended Action:</b> Use your previous Orchestrator to approve this one. If you do not have another Orchestrator, contact Support for assistance.	/portal/registration	TRUE	TRUE
6815791	CRITICAL	Failed to connect to Zscaler.  <b>Recommended Action:</b> Check Zscaler subscription.	/orchestration	TRUE	TRUE
6815792	CRITICAL	Your Orchestrator service will expire on {0 date}.  <b>Recommended Action:</b> Contact the Silver Peak Sales team to order an extension.	/portal/license/cloudorch	FALSE	TRUE
6815796	CRITICAL	Your EdgeConnect Boost expired on {0 date}. EdgeConnect devices in your network will stop using boost.  <b>Recommended Action:</b> Renew your boost license to avoid service interruption.	/portal/license/ec	TRUE	TRUE
6815799	CRITICAL	Failed to connect to Check Point CloudGuard Connect Service. {0}.  <b>Recommended Action:</b> Check Check Point CloudGuard Connect subscription parameters.	/orchestration/checkPoint	TRUE	TRUE
6815800	CRITICAL	Cannot get Azure data. Details : {0}.  <b>Recommended Action:</b> Check Azure subscription. Go to the Audit Logs for more details.	/orchestration/azure	TRUE	TRUE

Alarm ID	Alarm Severity	Alarm Text	Source	Service Affecting	Clearable
6815801	CRITICAL	Cannot download Azure configuration. Details : {0}. <b>Recommended Action:</b> Check Azure subscription.	/orchestration/azure	TRUE	TRUE
6815802	CRITICAL	Cannot create IPSEC Tunnels for Azure VPN Site - {0} for appliance {1} and label {2}. <b>Recommended Action:</b> Associate Hub to Azure VPN Site using Azure Portal. If Hub is already associated, wait for deployment to complete to start Azure Orchestration.	/orchestrator/orchestration/azure	TRUE	TRUE
6815803	CRITICAL	Cannot Orchestrate association to Azure VVwan. <b>Recommended Action:</b> Use VTI IP Pool Dialog to configure the subnet pool.	/orchestration/azure	TRUE	TRUE
6815804	CRITICAL	Cannot connect to Azure. Details : {0}. <b>Recommended Action:</b> Check Azure subscription. Go to the Audit Logs for more details.	/orchestration/azure	TRUE	TRUE
6815808	CRITICAL	Appliance was manually added to Orchestrator. <b>Recommended Action:</b> Remove the appliance from Orchestrator, discover and approve it.	/orchestrator/system	TRUE	TRUE
6815815	CRITICAL	Custom bonding policy or secondary WAN interface configured in overlay but appliance does not support this feature. <b>Recommended Action:</b> Check overlay configuration or upgrade appliance.	/orchestrator/orchestration/overlays	TRUE	FALSE
6815817	CRITICAL	Invalid IPsec UDP Key Material lifetime. Lifetime must be greater than rotation period. <b>Recommended Action:</b> Change IPsec UDP Key Material lifetime.	/ikeless	TRUE	FALSE

Alarm ID	Alarm Severity	Alarm Text	Source	Service Affecting	Clearable
6815820	CRITICAL	Cannot connect to AWS. Details : {0}.  <b>Recommended Action:</b> Check AWS subscription. Go to the Audit Logs for more details.	/orchestration/awstgnm	TRUE	TRUE
6815822	CRITICAL	Cannot Orchestrate association to AWS Transit Gateway.  <b>Recommended Action:</b> Use AWS VTI Subnet Pool Dialog to configure the subnet pool.	/orchestration/awstgnm	TRUE	TRUE
6815825	CRITICAL	Azure VWAN has duplicate ASN in the network. Details : {0}.  <b>Recommended Action:</b> Use Azure Portal to assign unique ASNs to the VPN Sites.	/orchestration/azure	TRUE	TRUE
6815826	CRITICAL	Orchestrator cannot register with Silver Peak Cloud Portal.  <b>Recommended Action:</b> Contact Support.	/portal/registration	TRUE	TRUE
6815827	CRITICAL	Routing Segmentation is only supported in inline-router mode.  <b>Recommended Action:</b> Check the deployment mode.	/orchestrator/routingSegmentation	TRUE	TRUE
6815828	CRITICAL	Cannot Orchestrate association to AWS Transit Gateway. No primary interface configured for AWS TGNM Integration.  <b>Recommended Action:</b> Configure the primary interfaces using Interface Label dialog in AWS Network Manager tab.	/orchestration/awstgnm	TRUE	TRUE
6815829	CRITICAL	Cannot Orchestrate association to Azure VWAN. {0}.  <b>Recommended Action:</b> Configure the interfaces using Interface Label dialog in Microsoft Azure Virtual WAN tab to proceed with the integration.	/orchestration/azure	TRUE	TRUE

Alarm ID	Alarm Severity	Alarm Text	Source	Service Affecting	Clearable
6815830	CRITICAL	<p>Cannot create AWS Customer Gateway for Appliance {0} and label {1}. Reason - No valid interface public ip address found.</p> <p><b>Recommended Action:</b> Ensure interface has public ip address. Refer to deployment page. No AWS Customer Gateway will be created with missing public IP.</p>	/orchestrator/orchestration/awstgnm	TRUE	TRUE
6815833	CRITICAL	<p>Cannot orchestrate AWS Transit Gateway Network Manager. Check the Audit log for more details.</p> <p><b>Recommended Action:</b> Restart Orchestrator to restart AWS TGNM Orchestration.</p>	/orchestration/aws_tgnm	TRUE	TRUE
6815834	CRITICAL	<p>Cannot orchestrate Azure Virtual WAN. Check the Audit log for more details.</p> <p><b>Recommended Action:</b> Restart Orchestrator to restart Azure VWAN Orchestration.</p>	/orchestration/azure	TRUE	TRUE
6815838	CRITICAL	<p>New IPSec UDP Key Material will be activated at {0}.</p> <p><b>Recommended Action:</b> Ensure the appliance is reachable from Orchestrator.</p>	/orchestrator/ikeless	TRUE	TRUE
6815839	CRITICAL	<p>Orchestrator is unable to rotate IPSec UDP key material.</p> <p><b>Recommended Action:</b> Ensure the appliance is reachable from Orchestrator.</p>	/orchestrator/ikeless	TRUE	TRUE
6815841	CRITICAL	<p>Unable to activate IPSec UDP Key Material. IPSec UDP tunnels will go down without activation.</p> <p><b>Recommended Action:</b> Go to the Audit Logs for more details.</p>	/orchestrator/ikeless	TRUE	TRUE
6815842	CRITICAL	<p>Orchestration of the appliance is in-progress for more than 24 hrs.</p> <p><b>Recommended Action:</b> Reboot Orchestrator.</p>	/orchestrator/orchestration/hung	TRUE	TRUE

Alarm ID	Alarm Severity	Alarm Text	Source	Service Affecting	Clearable
6815843	CRITICAL	<p>Orchestrator needs to restart in order to reflect changes to custom cert settings.</p> <p><b>Recommended Action:</b> Restart Orchestrator in order for new custom cert settings to take effect.</p>	/orchestrator/customCerts	TRUE	FALSE
6815846	CRITICAL	<p>Cannot Orchestrate association of Remote Endpoints for {0} service. No primary/backup interfaces configured.</p> <p><b>Recommended Action:</b> Configure the primary/backup interfaces using Interface Label dialog in Service Orchestration tab.</p>	/orchestration/serviceOrchestration	TRUE	TRUE
6815850	CRITICAL	<p>Unable to establish connection with stats collector.</p> <p><b>Recommended Action:</b> Unable to establish connection with stats collector. Check the status of Stats collector. It may not be running.</p>	/connectivity/statsCollector	TRUE	TRUE
6815856	CRITICAL	<p>Cannot connect to Aruba Central. Details : {0}.</p> <p><b>Recommended Action:</b> Check Aruba Central subscription. Go to the Audit Logs for more details.</p>	arubaCentral	TRUE	TRUE
6815747	MAJOR	<p>Appliance time is off from that of Orchestrator: {0}.</p> <p><b>Recommended Action:</b> Check interface speed/duplex settings and negotiated values on wan0/wan1 and lan0/lan1 ether-channel groups.</p>	/orchestrator/system/time	FALSE	TRUE
6815750	MAJOR	<p>Appliance is needed to reboot.</p> <p><b>Recommended Action:</b> You can reboot appliance under Administration &gt; Tools &gt; Reboot &gt; Appliance Reboot / Shutdown.</p>	/orchestrator/system	FALSE	TRUE

Alarm ID	Alarm Severity	Alarm Text	Source	Service Affecting	Clearable
6815751	MAJOR	Appliance configuration changes have not been saved.  <b>Recommended Action:</b> Your can save appliance changes under Administration > Setup > Save Appliance Changes.	/orchestrator/system	FALSE	TRUE
6815756	MAJOR	Orchestrator portal account or license will expire on {0 date}.  <b>Recommended Action:</b> Go to Licensing to provide the required information.	/license	FALSE	TRUE
6815761	MAJOR	Orchestrator does not have a set email address for alarm delivery.  <b>Recommended Action:</b> Go to Alarms to configure email recipient(s).	/email/alarm	FALSE	FALSE
6815762	MAJOR	Orchestrator is using the default SMTP settings.  <b>Recommended Action:</b> Go to SMTP Server Settings to configure SMTP server.	/email/smtp	FALSE	FALSE
6815776	MAJOR	Orchestrator SMTP settings are blank.  <b>Recommended Action:</b> Go to SMTP Server Settings to configure SMTP server.	/email/smtp	FALSE	FALSE
6815777	MAJOR	Failed to deliver an email.  <b>Recommended Action:</b> Check SMTP Server Settings.	/email/smtp	FALSE	FALSE
6815784	MAJOR	Silver Peak diagnostic remote access has been enabled from {0} to {1}.  <b>Recommended Action:</b> You can disable this in the Remote Access Settings.	/system/support	FALSE	FALSE
6815787	MAJOR	Failed to apply appliance preconfiguration.  <b>Recommended Action:</b> Applying preconfiguration to an appliance failed. Refer to the Preconfiguration tab and Audit logs for more details.	/orchestrator/preconfiguration	FALSE	TRUE

Alarm ID	Alarm Severity	Alarm Text	Source	Service Affecting	Clearable
6815788	MAJOR	Changes done on the appliance will not be auto saved. Enable Auto Save in Orchestration Settings.  <b>Recommended Action:</b> Enable Auto Save in Orchestration Settings.	/orchestration	TRUE	FALSE
6815807	MAJOR	Duplicate ASNs found in the network for appliances - {0} with asn - {1}.  <b>Recommended Action:</b> Assign unique ASNs for appliances using Orchestrator BGP menu.	/orchestrator/orchestration/bgp	TRUE	TRUE
6815809	MAJOR	Invalid ASN found in the network for appliance - {0} with asn - {1}.  <b>Recommended Action:</b> Assign unique ASN for the appliance using Orchestrator BGP menu.	/orchestrator/orchestration/bgp	TRUE	TRUE
6815831	MAJOR	Invalid ASN found in the network for appliance - {0} with asn - {1}. Amazon EC2 supports all 2-byte ASN numbers in the range of 1 - 65534, with the exception of 7224, which is reserved in the us-east-1 Region, and 9059, which is reserved in the eu-west-1 Region.  <b>Recommended Action:</b> Assign unique ASN for the appliance using Orchestrator BGP menu.	/orchestrator/orchestration/aws_tgnm	TRUE	TRUE
6815837	MAJOR	Unable to assign ASN for the appliance. All ASNs from ASN Range are reserved.  <b>Recommended Action:</b> Use BGP ASN Global Pool dialog to increase the scope of ASN Range.	/orchestrator/orchestration/bgp	FALSE	TRUE
6815844	MAJOR	Source Interface is not configured in the IP SLA configuration on Zscaler Internet Access.  <b>Recommended Action:</b> Configure the Source Interface for the Zscaler IP SLA configuration.	/orchestration/zscaler/ipsla	TRUE	TRUE

Alarm ID	Alarm Severity	Alarm Text	Source	Service Affecting	Clearable
6815847	MAJOR	<p>Failed to initialize connection with ClearPass Policy Manager. {0}.</p> <p><b>Recommended Action:</b> Check ClearPass Policy Manager server parameters.</p>	/orchestration/clearPass	TRUE	TRUE
6815848	MAJOR	<p>Failed to connect with ClearPass Policy Manager service endpoints. {0}.</p> <p><b>Recommended Action:</b> Check the Audit Logs for details.</p>	/orchestration/clearPass	TRUE	TRUE
6815852	MAJOR	<p>Unable to connect to one or more Stats Collectors.</p> <p><b>Recommended Action:</b> Go to Orchestrator &gt; Software &amp; Setup &gt; Setup &gt; Stats Collector Configuration to identify issues. Take steps to restore connectivity.</p>	/connectivity/statsCollector	FALSE	TRUE
6815753	MINOR	There were {0} failed attempts to login over last 5 minutes.	/authentication	FALSE	TRUE
6815775	MINOR	Backup configuration not set.	/system/backup	FALSE	TRUE
6815835	MINOR	<p>Appliance does not have any wan labels required for Azure VWAN Orchestration. No third party tunnels will be built on this appliance.</p> <p><b>Recommended Action:</b> Use appliance deployment to assign at least one wan label matching Azure VWAN Interface Label list.</p>	/orchestrator/orchestration/azure	TRUE	TRUE
6815836	MINOR	<p>Appliance does not have any wan labels required for AWS TGNM Orchestration. No third party tunnels will be built on this appliance.</p> <p><b>Recommended Action:</b> Use appliance deployment to assign at least one wan label matching AWS Interface Label list.</p>	/orchestrator/orchestration/aws_tgnm	TRUE	TRUE

Alarm ID	Alarm Severity	Alarm Text	Source	Service Affecting	Clearable
6815845	MINOR	<p>Appliance does not have any wan labels required for {0} Orchestration. No third party tunnels will be built on this appliance.</p> <p><b>Recommended Action:</b> Use appliance deployment to assign at least one wan label matching Third party service Interface Label list.</p>	/orchestrator/orchestration/serviceOrchestration	TRUE	TRUE
6815854	MINOR	<p>HA Sync Communication is not enabled.</p> <p><b>Recommended Action:</b> Follow release documents to enable this feature.</p>	/orchestration/deployment	FALSE	TRUE
6815755	WARNING	<p>Orchestrator portal account or license will expire on {0 date}.</p> <p><b>Recommended Action:</b> Go to Licensing to provide the required information.</p>	/license	FALSE	TRUE
6815759	WARNING	<p>Orchestrator cannot connect to Silver Peak portal using HTTPS.</p> <p><b>Recommended Action:</b> Check portal connection and refer to the Audit Logs for more information.</p>	/portal/connectivity	TRUE	TRUE
6815763	WARNING	<p>CPX license will expire on {0 date}.</p> <p>[Deprecated alarm]</p> <p><b>Recommended Action:</b> Renew your license to avoid service interruption.</p>	/portal/license/cpx	FALSE	TRUE
6815764	WARNING	<p>CPX license will expire on {0 date}.</p> <p>[Deprecated alarm]</p> <p><b>Recommended Action:</b> Renew your license to avoid service interruption.</p>	/portal/license/cpx	FALSE	TRUE
6815765	WARNING	<p>CPX license will expire on {0 date}.</p> <p>[Deprecated alarm]</p> <p><b>Recommended Action:</b> Renew your license to avoid service interruption.</p>	/portal/license/cpx	FALSE	TRUE

Alarm ID	Alarm Severity	Alarm Text	Source	Service Affecting	Clearable
6815767	WARNING	Your EdgeConnect account will expire in {0} day(s). EdgeConnect devices in your network will stop passing traffic on {1 date}. <b>Recommended Action:</b> Renew your license to avoid service interruption.	/portal/license/ec	FALSE	TRUE
6815768	WARNING	Your EdgeConnect account will expire in {0} day(s). EdgeConnect devices in your network will stop passing traffic on {1 date}. <b>Recommended Action:</b> Renew your license to avoid service interruption.	/portal/license/ec	FALSE	TRUE
6815769	WARNING	Your EdgeConnect account will expire in {0} day(s). EdgeConnect devices in your network will stop passing traffic on {1 date}. <b>Recommended Action:</b> Renew your license to avoid service interruption.	/portal/license/ec	FALSE	TRUE
6815771	WARNING	SaaS license will expire on {0 date}. <b>Recommended Action:</b> Renew your license to avoid service interruption.	/portal/license/saas	FALSE	TRUE
6815772	WARNING	SaaS license will expire on {0 date}. <b>Recommended Action:</b> Renew your license to avoid service interruption.	/portal/license/saas	FALSE	TRUE
6815773	WARNING	SaaS license will expire on {0 date}. <b>Recommended Action:</b> Renew your license to avoid service interruption.	/portal/license/saas	FALSE	TRUE
6815783	WARNING	Orchestrator deployment size has exceeded the recommended level of {0} appliances. <b>Recommended Action:</b> Contact Support to increase cloud resource allocation.	/system/database	FALSE	TRUE

Alarm ID	Alarm Severity	Alarm Text	Source	Service Affecting	Clearable
6815785	WARNING	Some appliances are paused from orchestration.  <b>Recommended Action:</b> Go to Pause Orchestration List to see detail.	/orchestration	TRUE	FALSE
6815786	WARNING	Apply Overlays is currently disabled.  <b>Recommended Action:</b> Enable Apply Overlays in Orchestration Settings.	/orchestration	TRUE	FALSE
6815789	WARNING	Apply Templates is currently disabled.  <b>Recommended Action:</b> Enable Apply Templates in Orchestration Settings.	/orchestration/templates	TRUE	FALSE
6815793	WARNING	Your EdgeConnect Boost will expire in {0} day(s). EdgeConnect devices in your network will stop using boost on {1 date}.  <b>Recommended Action:</b> Renew your boost license to avoid service interruption.	/portal/license/ec	FALSE	TRUE
6815794	WARNING	Your EdgeConnect Boost will expire in {0} day(s). EdgeConnect devices in your network will stop using boost on {1 date}.  <b>Recommended Action:</b> Renew your boost license to avoid service interruption.	/portal/license/ec	FALSE	TRUE
6815795	WARNING	Your EdgeConnect Boost will expire in {0} day(s). EdgeConnect devices in your network will stop using boost on {1 date}.  <b>Recommended Action:</b> Renew your boost license to avoid service interruption.	/portal/license/ec	FALSE	TRUE
6815798	WARNING	Paused stats collection for some of the appliances.	/orchestration	FALSE	TRUE
6815806	WARNING	Stats Collection is paused and will resume after Orchestrator backup is completed.	/orchestration/backup	FALSE	TRUE
6815810	WARNING	Check Point CloudGuard Connect orchestration is paused.	/orchestration/checkPoint	FALSE	FALSE

Alarm ID	Alarm Severity	Alarm Text	Source	Service Affecting	Clearable
6815811	WARNING	Zscaler Internet Access orchestration is paused.	/orchestration/zscaler	FALSE	FALSE
6815812	WARNING	Microsoft Azure Virtual WAN orchestration is paused.	/orchestration/azure	FALSE	FALSE
6815813	WARNING	Could not allocate IPs from Loopback Pool {0}.  <b>Recommended Action:</b> Change Loopback pool with enough IPs in Loopback Orchestration tag	/orchestrator/orchestration	FALSE	TRUE
6815814	WARNING	Loss and Latency metrics are available for IPSLA monitors with appliance version later than {0}.  <b>Recommended Action:</b> Upgrade appliance to enable loss and latency metrics for IPSLA.	/orchestrator/orchestration/ipsla	FALSE	TRUE
6815816	WARNING	Best internet breakout is configured in overlay, but appliance does not support this feature (Deprecated).  <b>Recommended Action:</b> Check overlay configuration or upgrade appliance.	/orchestrator/orchestration/overlays	TRUE	FALSE
6815818	WARNING	Shell access settings are different on the appliance than on Orchestrator.  <b>Recommended Action:</b> Reconcile shell access setting. Matching Orchestrator policy with appliance setting is recommended.	/orchestrator/orchestration/shellAccessSetting	FALSE	TRUE
6815819	WARNING	Connection not established for websocket receiver: {0}.  <b>Recommended Action:</b> Check websocket receiver configuration.	remoteLogWebSocket	FALSE	TRUE
6815821	WARNING	AWS Transit Gateway Network Manager orchestration is paused.	/orchestration/aws_tgnm	FALSE	FALSE
6815823	WARNING	A new maintenance alert was received from Silver Peak.	/portal/SilverPeakMaintenance	TRUE	TRUE
6815824	WARNING	Stats Collection is lagging behind.	/orchestrator/statistics	FALSE	TRUE

Alarm ID	Alarm Severity	Alarm Text	Source	Service Affecting	Clearable
6815832	WARNING	Inter-Segment Routing & DNAT rules have duplicate ip address with existing Inter-Segment Routing & DNAT Exceptions rules.  <b>Recommended Action:</b> Check the Inter-Segment Routing & DNAT rules and solve the duplicate ip address.	/orchestrator/routingSegmentation	TRUE	TRUE
6815840	WARNING	This appliance does not support Routing Segmentation.  <b>Recommended Action:</b> Upgrade the appliance.	/orchestrator/routingSegmentation	TRUE	TRUE
6815849	WARNING	ClearPass Policy Manager session paused.	/orchestration/clearPass	FALSE	FALSE
6815851	WARNING	Stats Collection is paused and will resume after Orchestrator backup is completed.	/orchestration/backup	FALSE	TRUE
6815855	WARNING	Some of the Aruba Central sites don't have lat and lon. Site Name : {0}.	/arubaCentral/arubaCentral	FALSE	TRUE

## Equipment

System Type 100 (Orchestrator); Source Type 3 (Equipment)

Alarm ID	Alarm Severity	Alarm Text	Source	Service Affecting	Clearable
6750234	CRITICAL	Failed to get database connection. Details: {0}.  <b>Recommended Action:</b> Reserve required Memory and CPU.	/system/resource	TRUE	TRUE
6750209	MAJOR	Disk partition {0} is dangerously full - {1}% used.  <b>Recommended Action:</b> Go to Server Information to see detailed disk usage.	/system/disk	FALSE	FALSE
6750317	MAJOR	One or more Stats Collectors are critically low on disk space.  <b>Recommended Action:</b> Go to Orchestrator > Software & Setup > Setup > Stats Collector Configuration and review disk usage. Increase disk size where needed.	/system/disk/statsCollector	FALSE	FALSE

Alarm ID	Alarm Severity	Alarm Text	Source	Service Affecting	Clearable
6750208	WARNING	Disk partition {0} is more than {1}% used. <b>Recommended Action:</b> Go to Server Information to see detailed disk usage.	/system/disk	FALSE	FALSE

## Reporting

The following tabs enable you to schedule and run reports, view past report content, and see which reports run currently or have been run historically.

### Schedule and Run Reports

*Monitoring > Reporting > Schedule & Run Reports*

Use the Schedule & Run Reports tab to create, configure, run, schedule, and distribute reports. You can specify what you want to include in your report based on appliances, the time range of the report, traffic type, and the types of charts to include. You can also specify email recipients for the report.

Reports and statistics help you bracket a problem, question, or analysis. Orchestrator reports fall into two broad categories:

- Statistics related to network and application performance. These provide visibility into the network, enabling you to investigate problems, address trends, and evaluate your WAN utilization.
- Reports related to status of the network and appliances. For example, alarms, threshold crossing alerts, reachability between Orchestrator and the appliances, scheduled jobs, and so forth.

Configure the following in this tab:

- **Global Report** - By default, Orchestrator emails this preconfigured subset of charts every day. Clicking on a chart's image opens the associated tab in the browser.
  - To access all reports residing on the Orchestrator server, click **View Reports**.
- **Name** of the report.
- **Email Recipients** - Enter the email address to which to send the report.
  - To send a test email or to configure another SMTP server instead, navigate to **Orchestrator > Software & Setup > Setup > SMTP Server Settings**.
  - If a test email does not arrive within minutes, check your firewall.

- Default range of reports - **Daily** = 14 days, **Hourly** = 24 hours. Increasing the scope uses additional memory.
- A Scheduled or Single Report.

Additionally, you can specify the following for a generated report:

- Appliances in Report - Fill in the box or click **Use Tree Selection** to display appliances.
- Amount of Top Reports (10, 25, 50, 100, 1000).
- Traffic Type.
- Select the check boxes next to the following charts to be included in the report:
  - Application Charts
  - Tunnel Charts
  - Appliance Charts
- Lock Scales for Local Trends - Automatically scales graphs for specified scheduled reports.

**TIP** To specify the timezone for scheduled jobs and reports, navigate to **Orchestrator > Software & Setup > Setup > Timezone for Scheduled Jobs**.

## View Reports

*Monitoring > Reporting > View Reports*

Use this tab to **view** and **download** reports in PDF form. Reports can be filtered by keywords or sorted by **name**, **size**, or **date last modified**. These reports can also be emailed depending on the configuration set on the **Schedule & Run Reports** tab.

View Reports X

**View Reports** ?

90 Rows

Report	File Size	Last Modified	Download
08.Dec.16-07.30.03-Daily-Global_Report.pdf	337 KB	07-Dec-16 23:31	
08.Dec.16-07.30.03-Minutes-Global_Report.pdf	334 KB	07-Dec-16 23:33	
08.Dec.16-07.30.03-Hourly-Global_Report.pdf	333 KB	07-Dec-16 23:33	
09.Dec.16-07.30.03-Daily-Global_Report.pdf	336 KB	08-Dec-16 23:31	
09.Dec.16-07.30.03-Minutes-Global_Report.pdf	334 KB	08-Dec-16 23:32	
09.Dec.16-07.30.03-Hourly-Global_Report.pdf	333 KB	08-Dec-16 23:32	
10.Dec.16-07.30.03-Daily-Global_Report.pdf	337 KB	09-Dec-16 23:31	
10.Dec.16-07.30.03-Minutes-Global_Report.pdf	334 KB	09-Dec-16 23:32	
10.Dec.16-07.30.03-Hourly-Global_Report.pdf	333 KB	09-Dec-16 23:33	
11.Dec.16-07.30.03-Daily-Global_Report.pdf	337 KB	10-Dec-16 23:31	
11.Dec.16-07.30.03-Minutes-Global_Report.pdf	334 KB	10-Dec-16 23:33	
11.Dec.16-07.30.03-Hourly-Global_Report.pdf	333 KB	10-Dec-16 23:34	
12.Dec.16-07.30.03-Daily-Global_Report.pdf	337 KB	11-Dec-16 23:31	
12.Dec.16-07.30.03-Minutes-Global_Report.pdf	334 KB	11-Dec-16 23:34	
12.Dec.16-07.30.03-Hourly-Global_Report.pdf	333 KB	11-Dec-16 23:34	
13.Dec.16-07.30.03-Daily-Global_Report.pdf	337 KB	12-Dec-16 23:31	
13.Dec.16-07.30.03-Minutes-Global_Report.pdf	334 KB	12-Dec-16 23:32	
13.Dec.16-07.30.03-Hourly-Global_Report.pdf	333 KB	12-Dec-16 23:36	

\*-Global\_Report.pdf

## Sample Report



## Scheduled and Historical Jobs

*Monitoring > Reporting > Scheduled & Historical Jobs*

This tab has two views:

- It provides a central location for viewing and deleting **scheduled jobs**, such as appliance backup and any custom reports configured for distribution.

Job	Appliances	Description	Schedule	Last Run	Next Run	Status
IPsec Pre-shared Key Rotation	All appliances		First day of the month at 1:00 starting 17-Aug-20 15:47 PDT			
IPsec UDP Key Rotation	All appliances		Every day at 15:20 starting 02-Jul-19 15:20 PDT	06-Oct-21 15:20 ...	07-Oct-21 15:20 P...	Success - 06-Oct-21 15:20 PDT...
Auto MTU Discovery	Network		Every day at 2:00 starting 06-Nov-19 14:37 PST	07-Oct-21 02:00 ...	08-Oct-21 02:00 P...	Success - Job started success...

- It provides a central location for viewing **historical jobs**.

Job	Appliances	Description	Start Time	End Time	Duration	Status
Acure WAN Get Data	Network		07-Oct-21 12:15 EDT	07-Oct-21 12:16 EDT	13s	Success - Finished job
ClearPass Policy Manager Get Data	Network		07-Oct-21 12:15 EDT	07-Oct-21 12:15 EDT	3s	Success - Finished job
Acure WAN Get Data	Network		07-Oct-21 12:10 EDT	07-Oct-21 12:11 EDT	13s	Success - Finished job
Zacaler Internet Access Get Data	All appliances		07-Oct-21 12:10 EDT	07-Oct-21 12:11 EDT	13s	Success - Finished receiving locations f
AVS TGMM Get Data	Network		07-Oct-21 12:10 EDT	07-Oct-21 12:11 EDT	13s	Success - Finished job
Check Point CloudGuard Connect Get Data	All appliances		07-Oct-21 12:10 EDT	07-Oct-21 12:10 EDT	7s	Failed - Failed to run job: ("errors":["
ClearPass Policy Manager Get Data	Network		07-Oct-21 12:10 EDT	07-Oct-21 12:10 EDT	3s	Success - Finished job
Acure WAN Get Data	Network		07-Oct-21 12:05 EDT	07-Oct-21 12:06 EDT	15s	Success - Finished job
AVS TGMM Get Data	Network		07-Oct-21 12:05 EDT	07-Oct-21 12:06 EDT	15s	Success - Finished job
ClearPass Policy Manager Get Data	Network		07-Oct-21 12:05 EDT	07-Oct-21 12:05 EDT	5s	Success - Finished job
AVS TGMM Get Data	Network		07-Oct-21 12:00 EDT	07-Oct-21 12:01 EDT	16s	Success - Finished job
Acure WAN Get Data	Network		07-Oct-21 12:00 EDT	07-Oct-21 12:01 EDT	14s	Success - Finished job

## Bandwidth

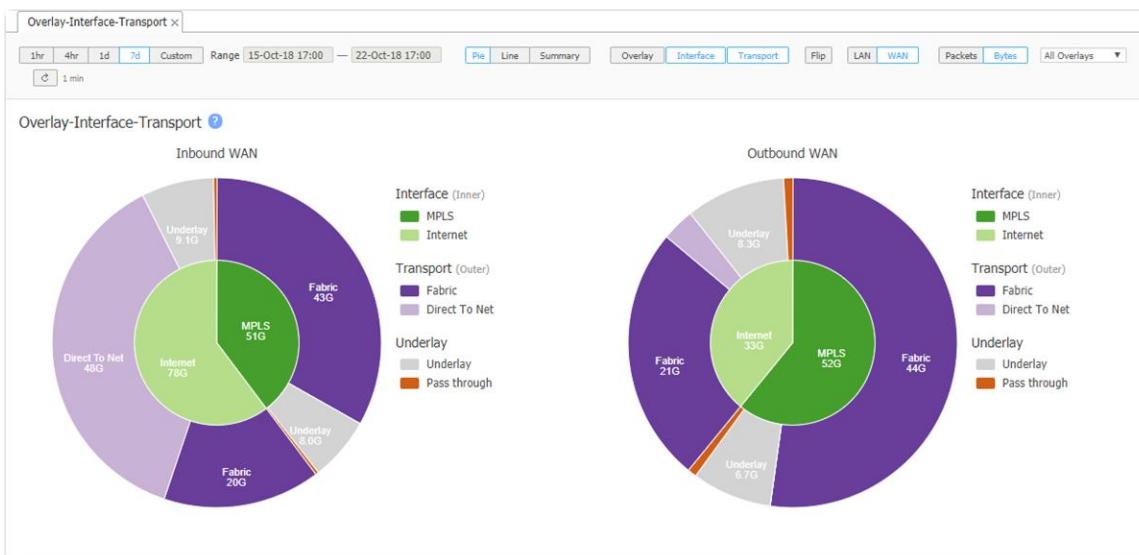
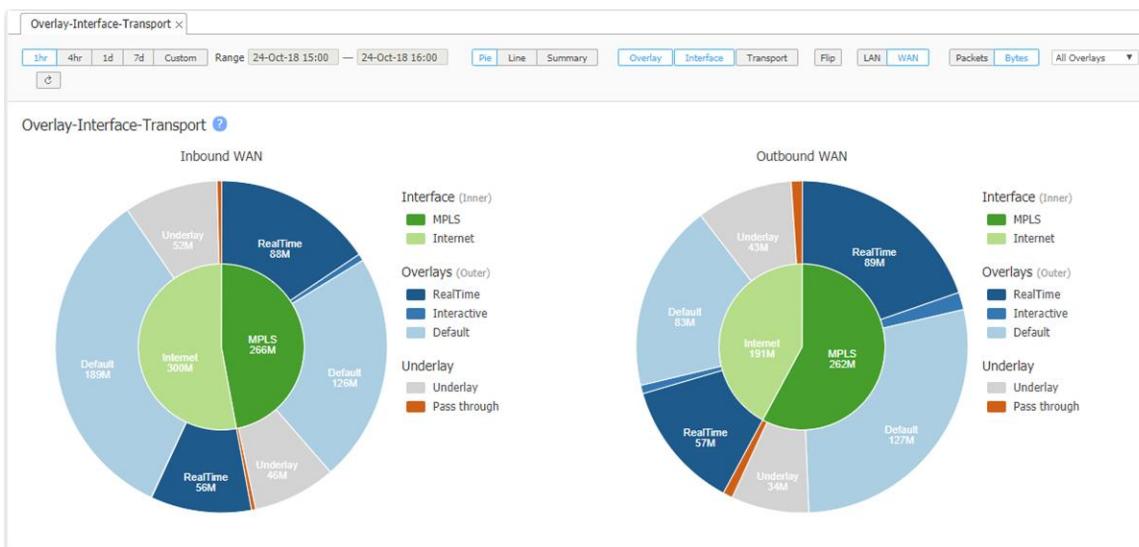
### Overlay-Interface-Transport

*Monitoring > Bandwidth > Overlays & Interfaces > Overlay-Interface-Transport*

These charts display the distribution of traffic across three dimensions—overlays, interfaces, and transport. You can view each option individually, or in relation to another.

For instance, for a given interface, you can see how the overlay traffic is distributed.

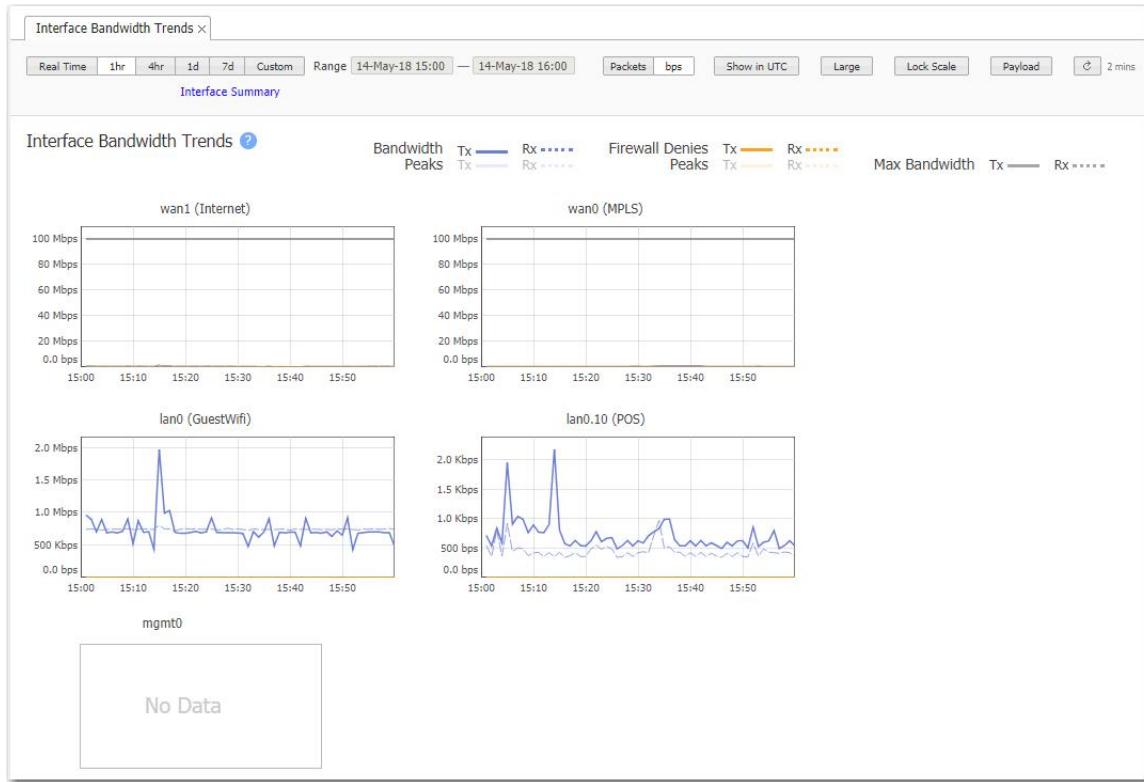
You can also view how much traffic is transported from one EdgeConnect appliance to another on the SD-WAN fabric (Overlays), versus how much is broken out locally, direct to the internet. The Underlay legend displays non-overlay traffic.



## Interface Bandwidth Trends

*Monitoring > Bandwidth > Overlays & Interfaces > Interface Trends*

The Interface Bandwidth Trends tab shows interface statistics for a single selected appliance in real time or for a specific period. Real time charts show the past five minutes of usage and refresh every second. By default, charts display transmit and receive statistics for bandwidth and firewall denies. You can toggle peak statistics or maximum bandwidth statistics on or off by clicking the sample indicator line next to each statistic name.



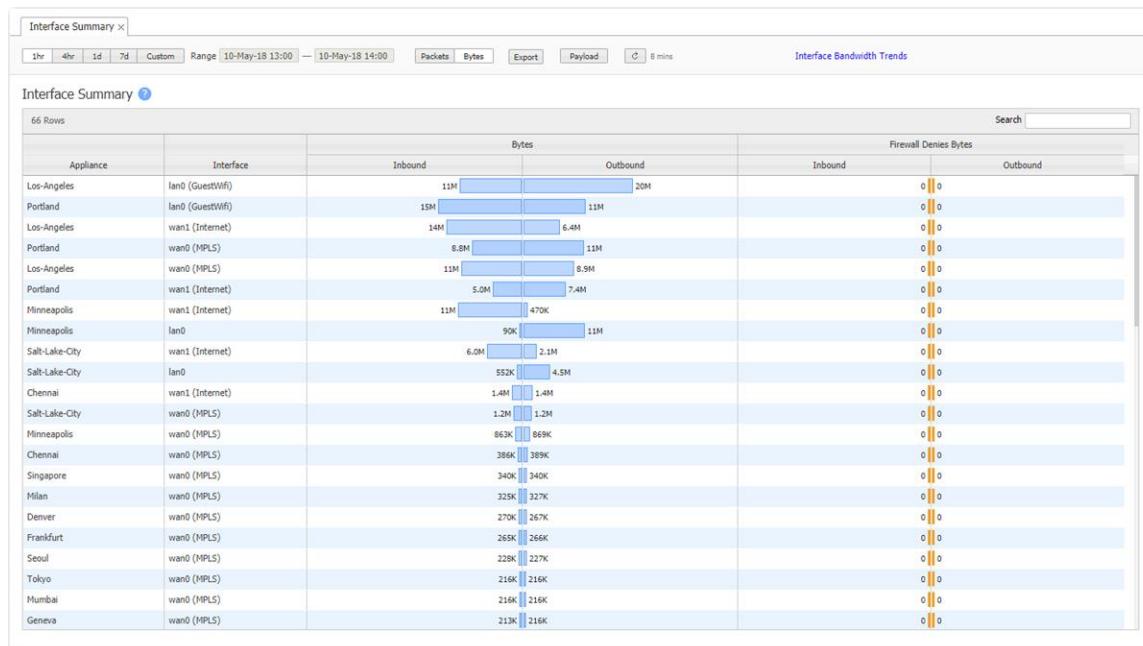
You can customize the chart settings using the controls at the top of the tab, as follows:

Option	Description
<b>Time period</b>	<ul style="list-style-type: none"> <li>Click <b>Real Time</b> to enable live statistics for all available interfaces.</li> <li>Click a predefined time period (<b>1h</b>, <b>4h</b>, <b>1d</b>, <b>7d</b>) to display statistics over the last hour, four hours, day, or seven days.</li> <li>Click <b>Custom</b> and set your own custom time range to display statistics for that time period.</li> </ul>
<b>Packets/bps</b>	<ul style="list-style-type: none"> <li>Click <b>Packets</b> to display statistics according to the number of packets sent and received.</li> <li>Click <b>bps</b> to display statistics for bits per second sent and received.</li> </ul>
<b>Show in UTC</b>	Click this option to toggle chart times between local appliance time or UTC.
<b>Large</b>	Click this option to toggle the size of the charts between smaller (default) and large.
<b>Lock Scale</b>	By default, each chart uses its own scale that is relative to the data displayed. Click this option to apply and lock the same scale to each chart.
<b>Payload</b>	By default, charts show complete bandwidth usage statistics—payload plus all SD-WAN overhead (headers, FEC, and so forth). To see bandwidth usage for payload only, click to enable the <b>Payload</b> button.

## Interface Summary

*Monitoring > Bandwidth > Overlays & Interfaces > Interface Summary*

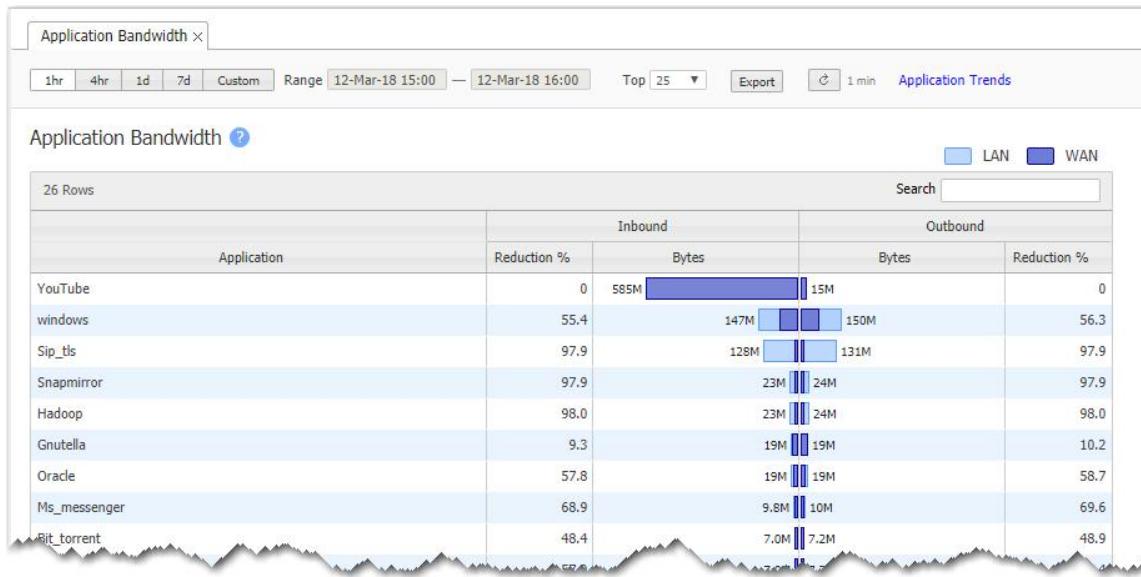
This tab shows interface summary statistics, including inbound and outbound Packets or Bytes per interface, as well as Firewall Denies (Drops). Statistics are summarized for the selected time period.



## Application Bandwidth

*Monitoring > Bandwidth > Applications > Summary*

The **Application Bandwidth** chart shows which applications have sent the most bytes.

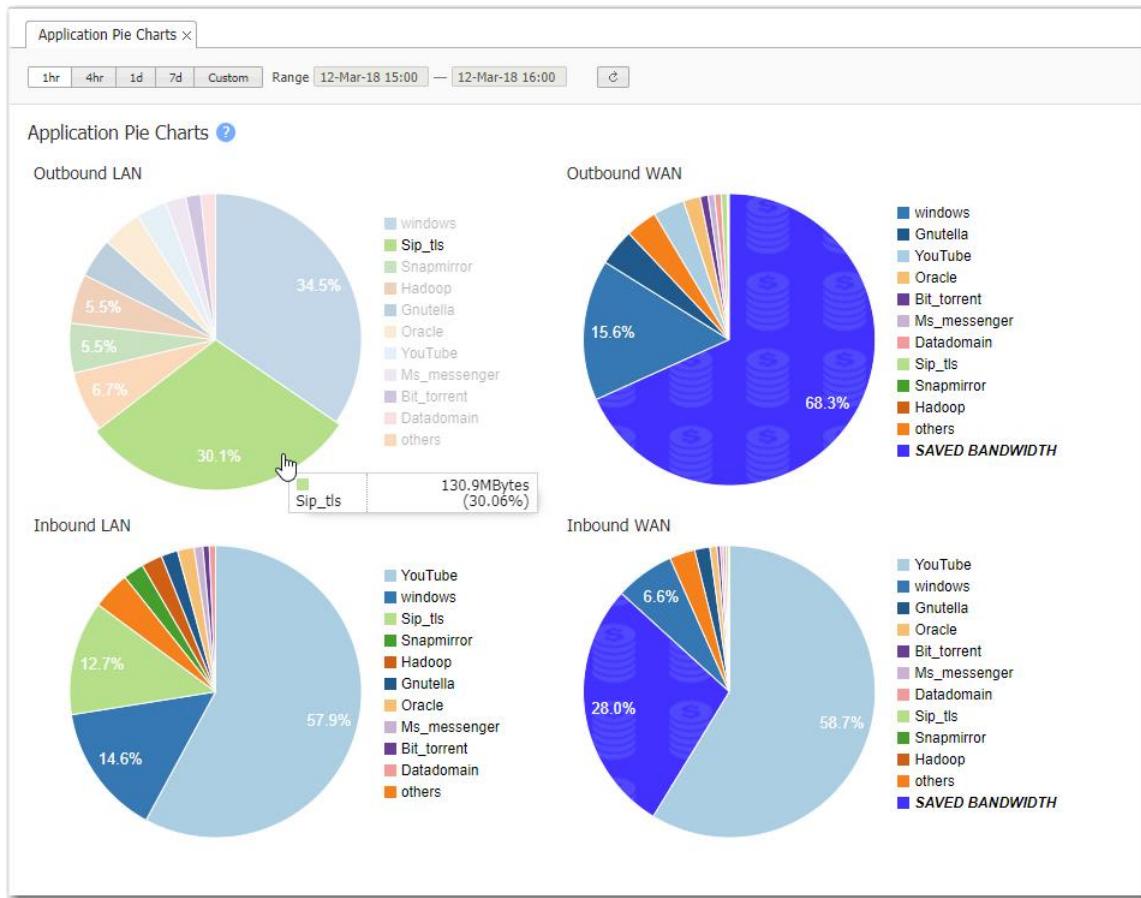


## Application Pie Charts

*Monitoring > Bandwidth > Applications > Pie Charts*

The **Application Pie Charts** show what proportion of the bytes an application consumes on the LAN and on the WAN.

- Mousing over the charts and the legends reveals additional information.
- The WAN charts identify what percentage of the bandwidth the EdgeConnect appliance saved by optimizing the traffic.



## Application Trends

*Monitoring > Bandwidth > Applications > Trends*

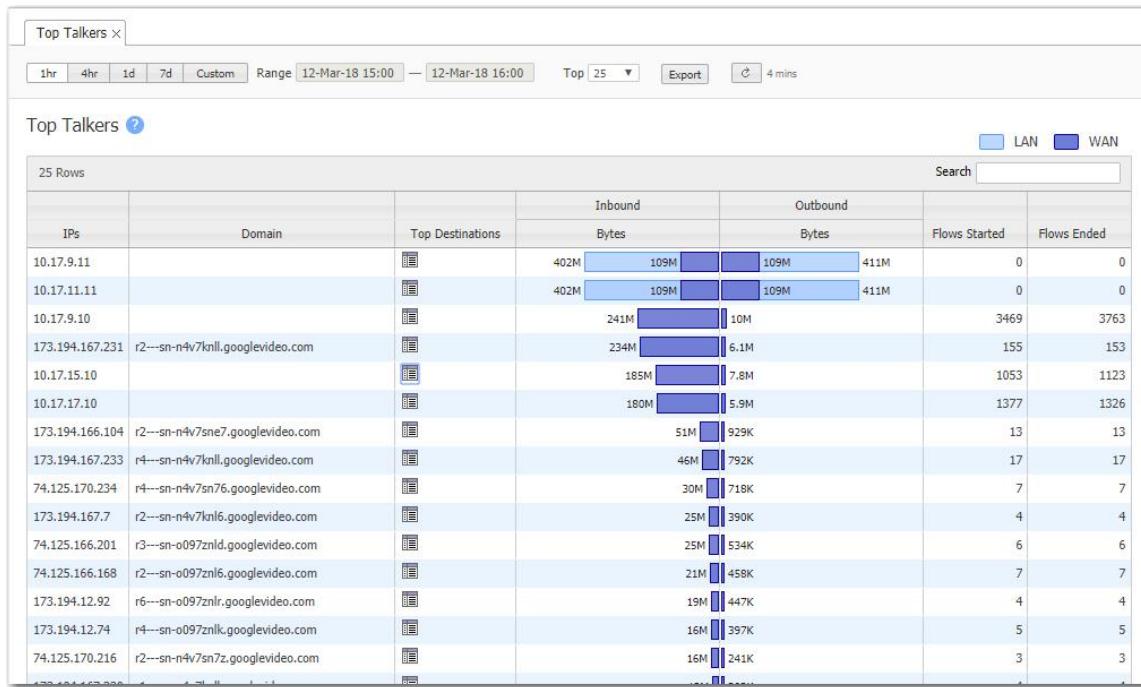
This tab shows application trends over time.



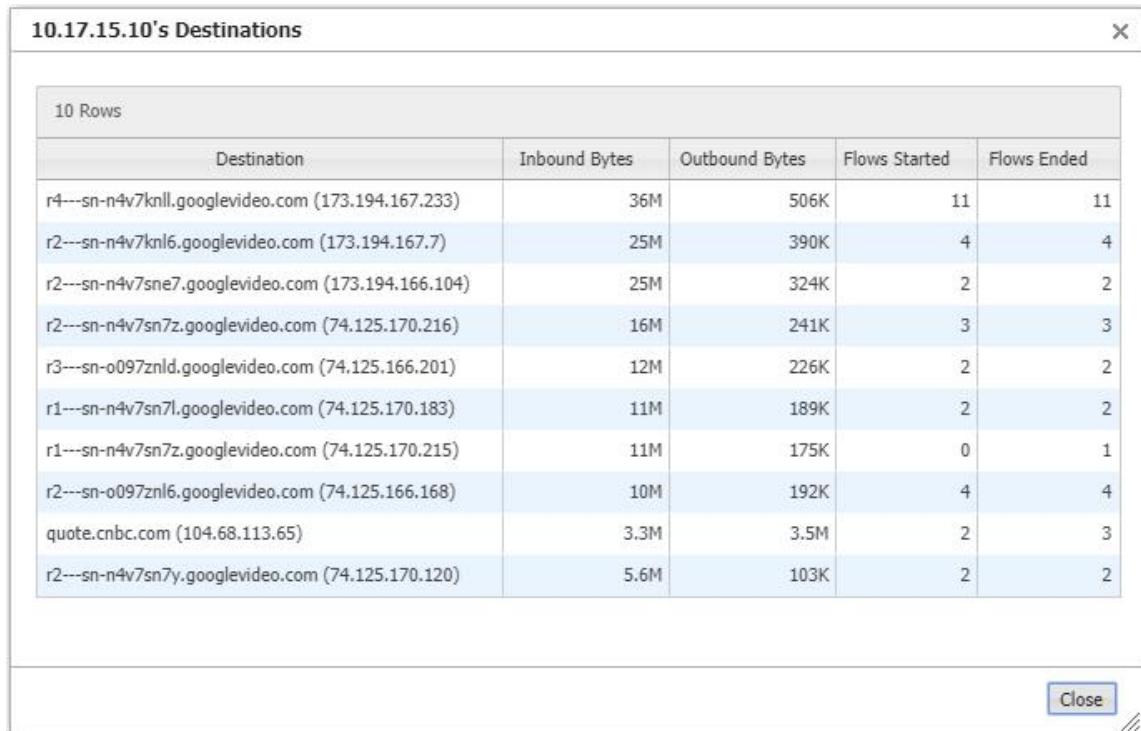
## Top Talkers

*Monitoring > Bandwidth > Identifiers > Top Talkers*

This tab lists the IP addresses that use the most bandwidth.



You can also view each IP's destinations.

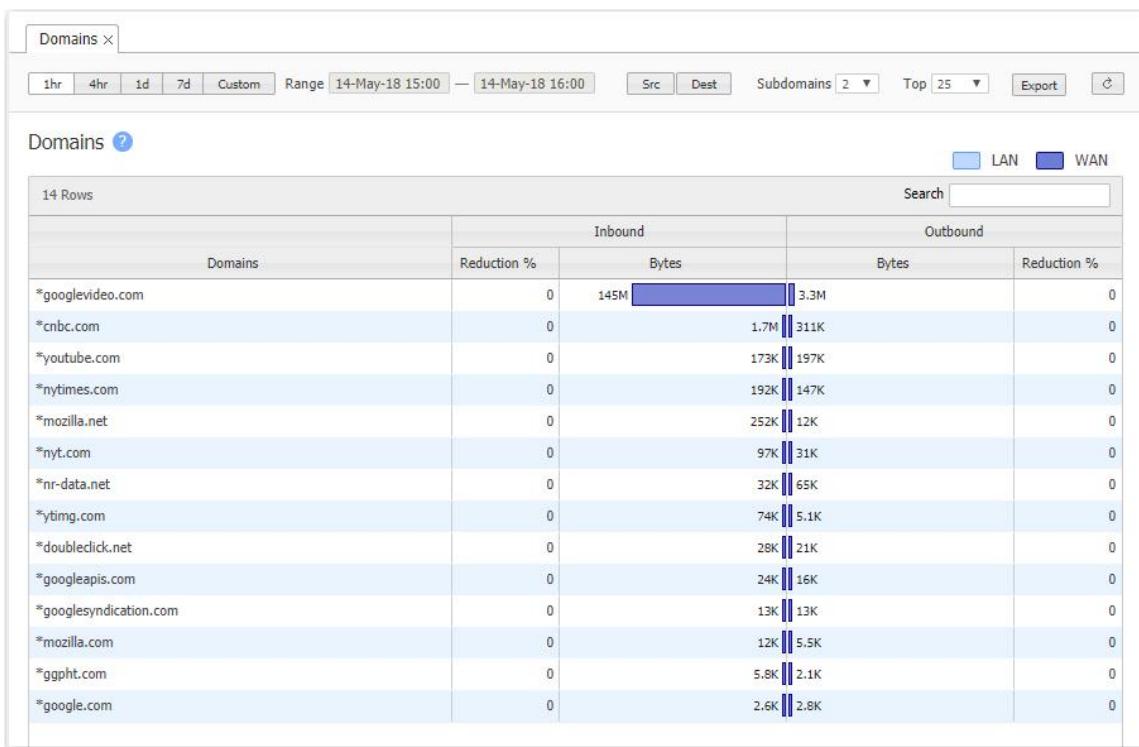


## Domains

*Monitoring > Bandwidth > Identifiers > Domains*

This tab lists the domains that use the most bandwidth.

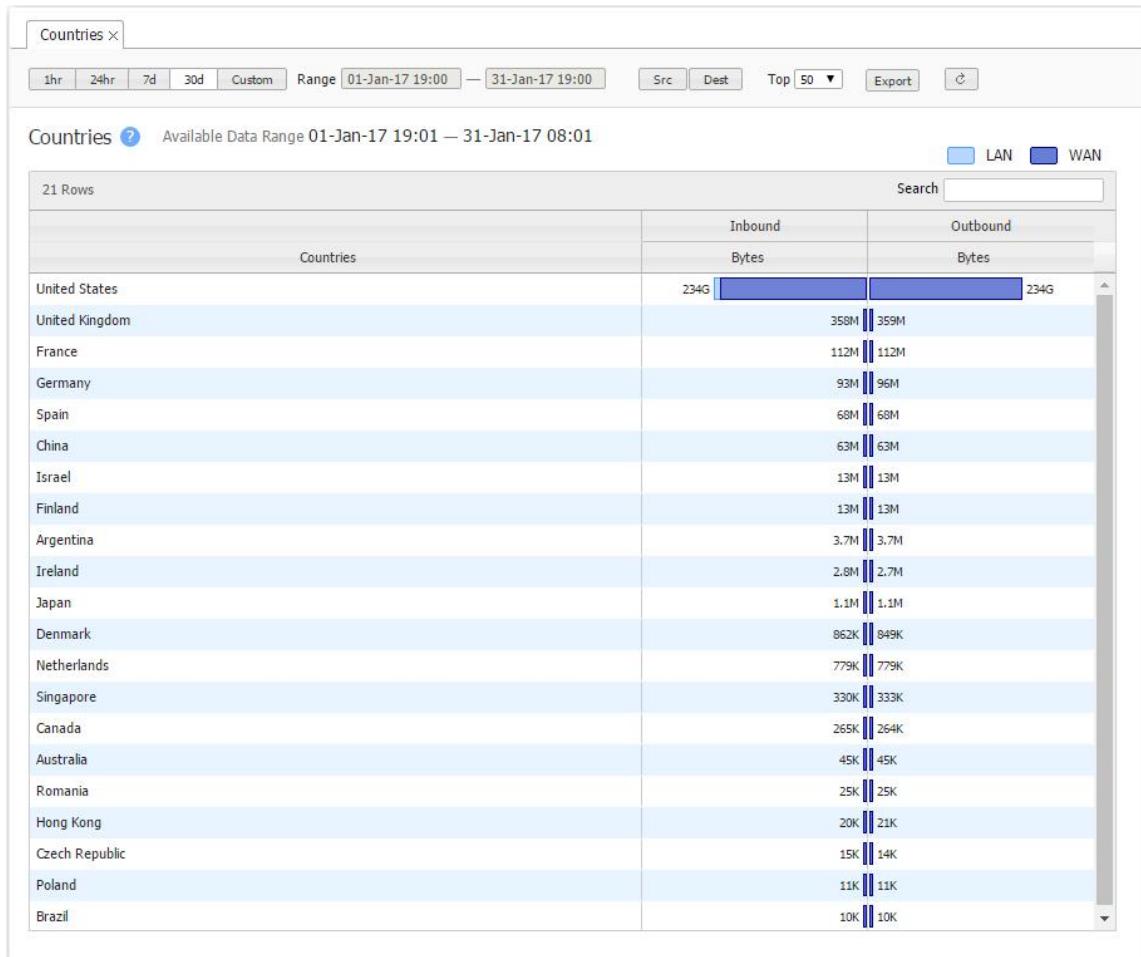
The number of **Subdomains** selected determines how the table aggregates subdomains for display. An asterisk (\*) indicates that more subdomains would be displayed if a higher number were selected. This is not a filter, but rather a grouping convenience.



## Countries

*Monitoring > Bandwidth > Identifiers > Countries*

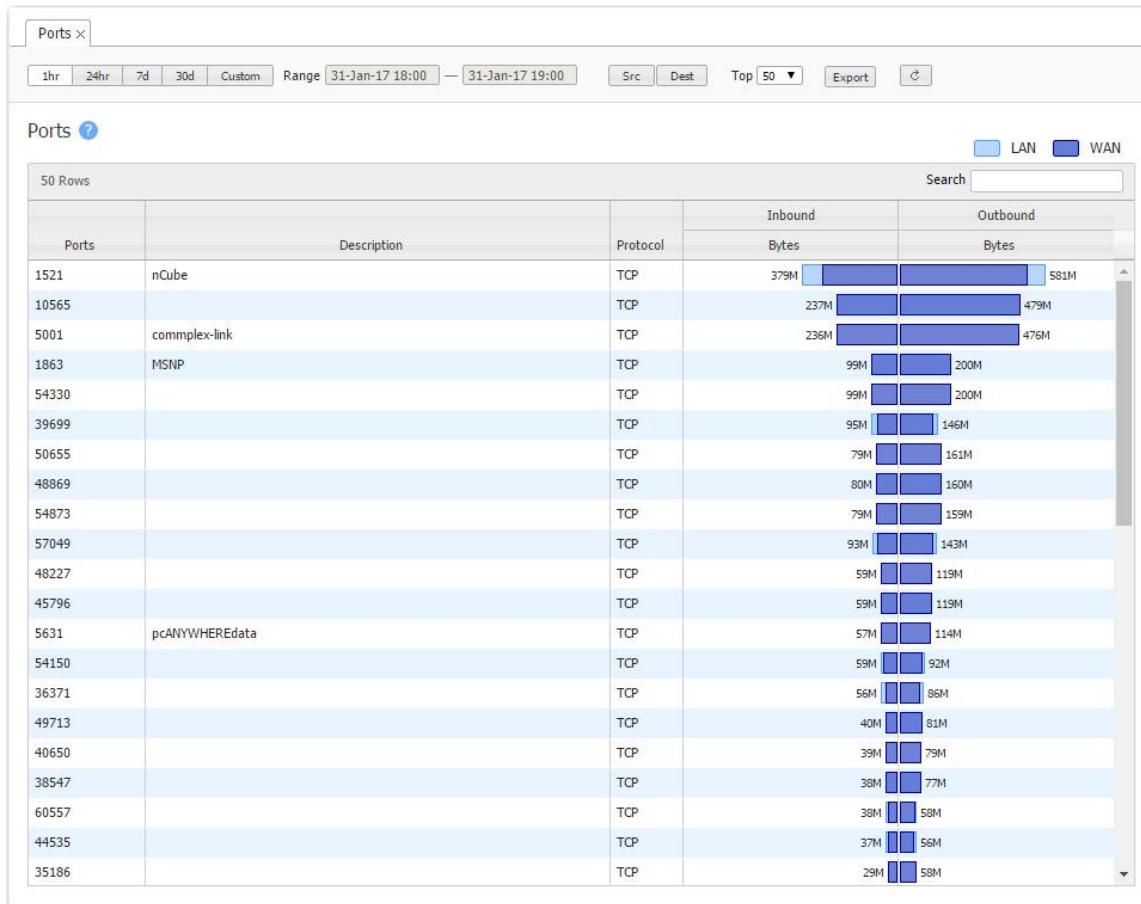
This tab lists the countries that use the most bandwidth.



## Ports

*Monitoring > Bandwidth > Identifiers > Ports*

This tab lists the ports that use the most bandwidth.



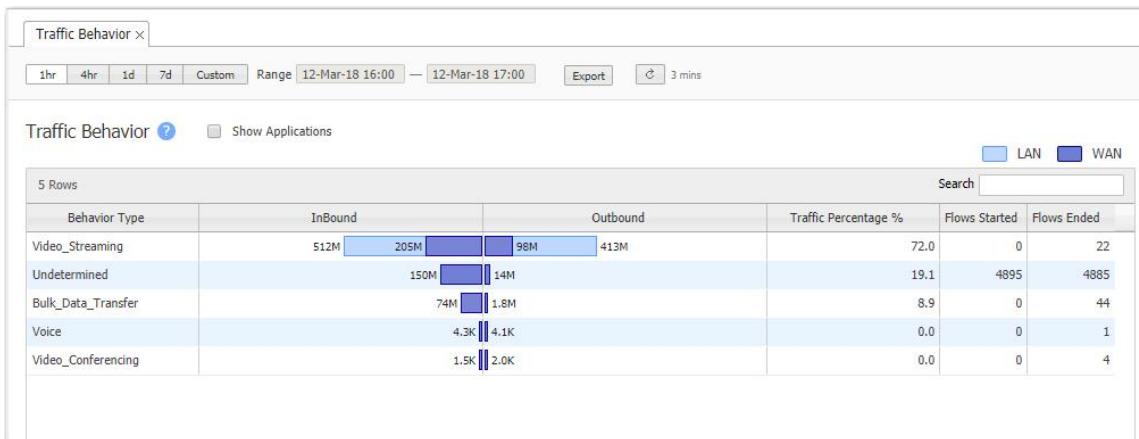
## Traffic Behavior

*Monitoring > Bandwidth > Identifiers > Traffic Behavior*

The **Traffic Behavior** report identifies and categorizes traffic based on low-level characteristics of the data streams. The behavior types are:

- Voice
- Video Conferencing
- Video Streaming
- Bulk Data Transfer
- Interactive
- Undetermined

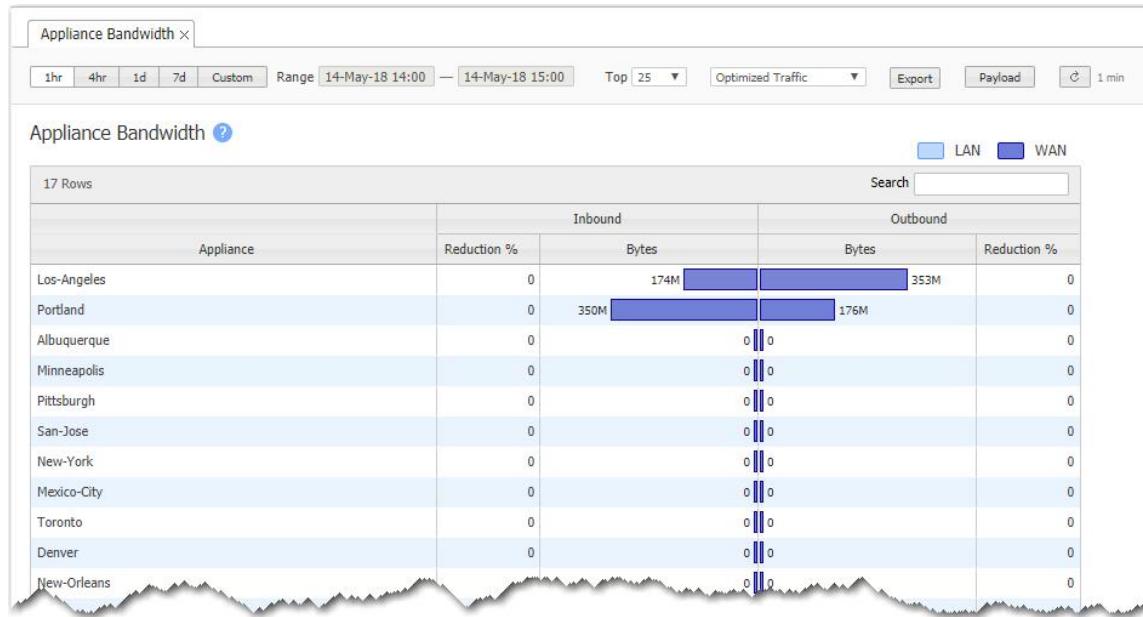
You can also specify these categories as match criteria when creating policies or ACLs (Access Control Lists).



## Appliance Bandwidth

*Monitoring > Bandwidth > Appliances > Summary*

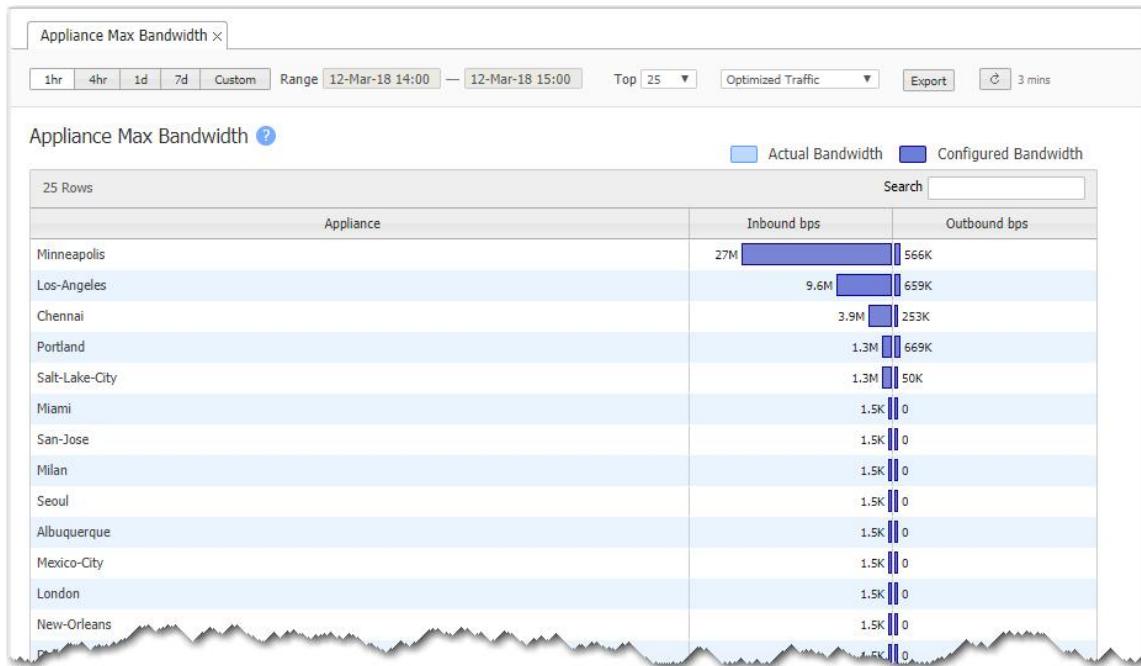
The **Appliance Bandwidth** chart lists the top appliances based on the total volume of inbound and outbound traffic before reduction. It shows how many bytes the EdgeConnect appliance saved when transferring data, aggregated over a selectable time period.



## Appliance Max Bandwidth

*Monitoring > Bandwidth > Appliances > Max*

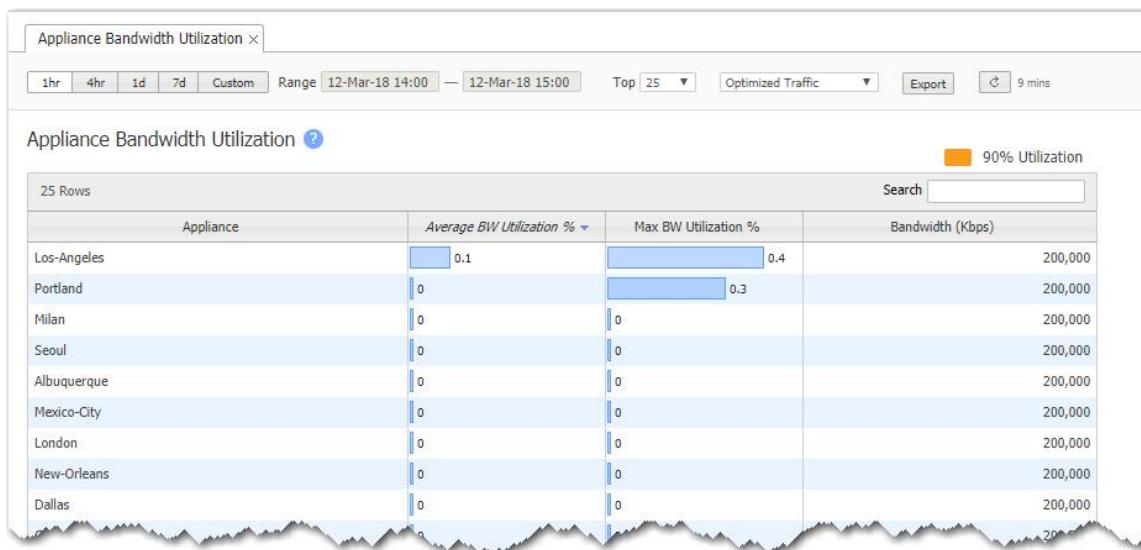
The **Appliance Max Bandwidth** chart lists the top appliances by the peak throughput (in either direction) within a selected time period. It compares the system bandwidth of the appliance to the effective bandwidth it is providing.



## Appliance Bandwidth Utilization

*Monitoring > Bandwidth > Appliances > Utilization*

The **Appliance Bandwidth Utilization** chart lists the top appliances by the average percent of available bandwidth used. This helps you determine whether an appliance that is optimizing traffic is reaching its capacity.



## Appliance Bandwidth Trends

*Monitoring > Bandwidth > Appliances > Trends*

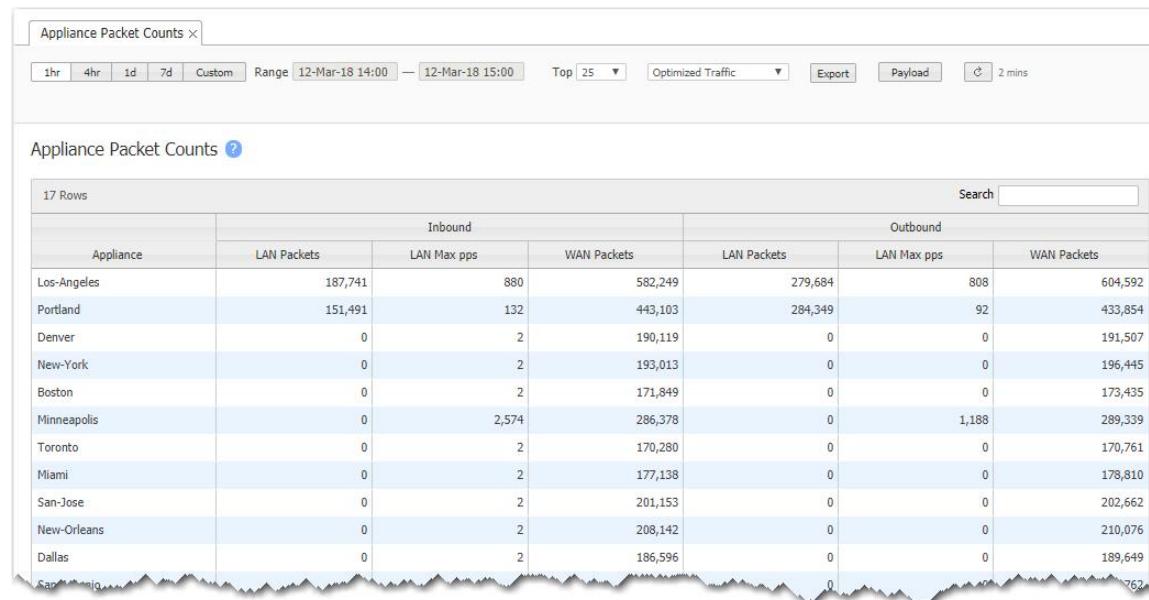
The **Appliance Bandwidth Trends** chart shows bandwidth usage over time.

For each Business Intent Overlay, the Link Bonding Policy specified determines the bandwidth efficiency. To guarantee service quality levels, High Availability requires the most overhead, and High Efficiency requires the least. Charts display the total bandwidth used. The Payload option shows how much raw data is transmitted. At the same time, it exposes the Peaks option, which enables the viewing of peak transmissions.

## Appliance Packet Counts

*Monitoring > Bandwidth > Appliances > Packet Counts*

The **Appliance Packet Counts** chart lists the top appliances according to the sum of the inbound and outbound LAN packets, showing how much traffic was sent.



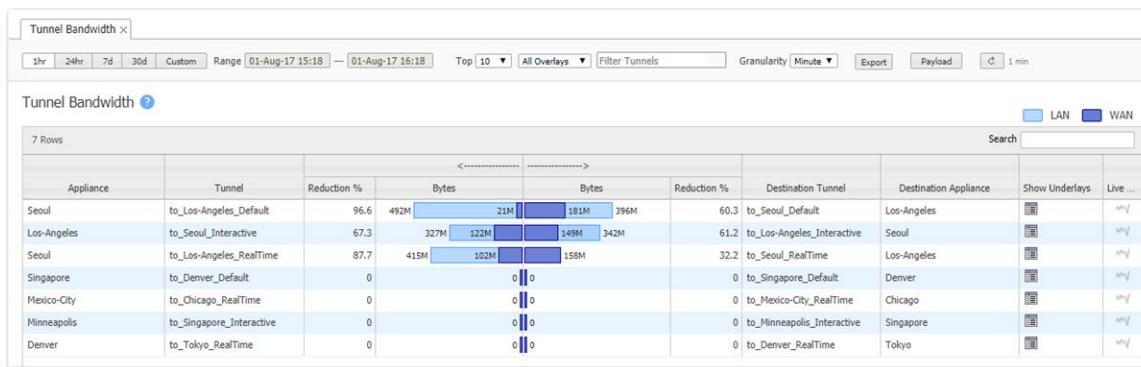
The screenshot shows a table titled "Appliance Packet Counts" with 17 rows. The table has columns for Appliance, Inbound (LAN Packets, LAN Max pps, WAN Packets), and Outbound (LAN Packets, LAN Max pps, WAN Packets). The data is as follows:

Appliance	Inbound			Outbound		
	LAN Packets	LAN Max pps	WAN Packets	LAN Packets	LAN Max pps	WAN Packets
Los-Angeles	187,741	880	582,249	279,684	808	604,592
Portland	151,491	132	443,103	284,349	92	433,854
Denver	0	2	190,119	0	0	191,507
New-York	0	2	193,013	0	0	196,445
Boston	0	2	171,849	0	0	173,435
Minneapolis	0	2,574	286,378	0	1,188	289,339
Toronto	0	2	170,280	0	0	170,761
Miami	0	2	177,138	0	0	178,810
San-Jose	0	2	201,153	0	0	202,662
New-Orleans	0	2	208,142	0	0	210,076
Dallas	0	2	186,596	0	0	189,649
San-Diego	0	2	176,262	0	0	176,262

## Tunnels Bandwidth

*Monitoring > Bandwidth > Tunnels > Summary*

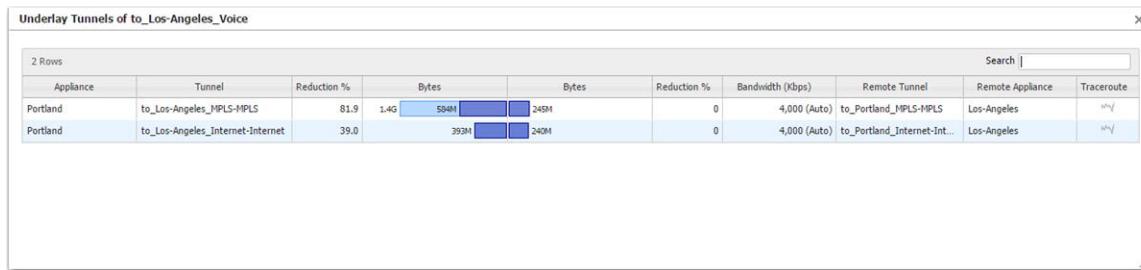
The **Tunnel Bandwidth** chart shows the tunnels that are sending the most bytes—that is, the most active tunnels.



## Show Underlays

Underlays are actual IPSec tunnels and physical paths taken (such as MPLS).

Overlays are logical tunnels created for different traffic types and policies (such as VoIP).



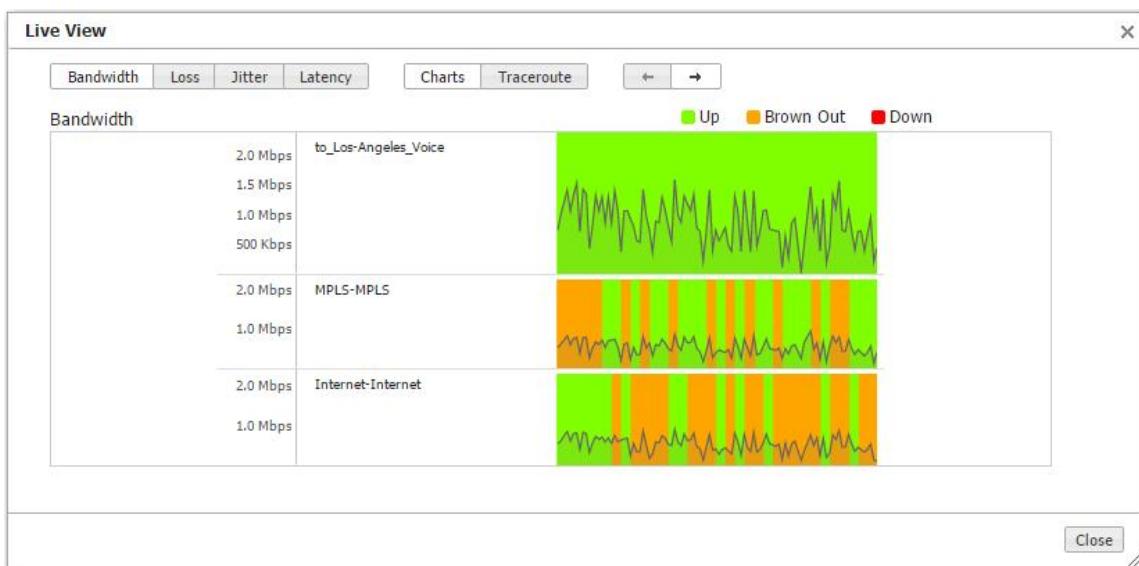
## Traceroute

This shows trace route information between the tunnel source and destination IP addresses. It shows intermediate hops, their IP addresses, and the latency between each hop.



## Live View

Live View shows the live bandwidth, loss, jitter, and latency on all the tunnels. For an overlay, it also shows live tunnel states—**Up**, **Browned Out**, or **Down**.



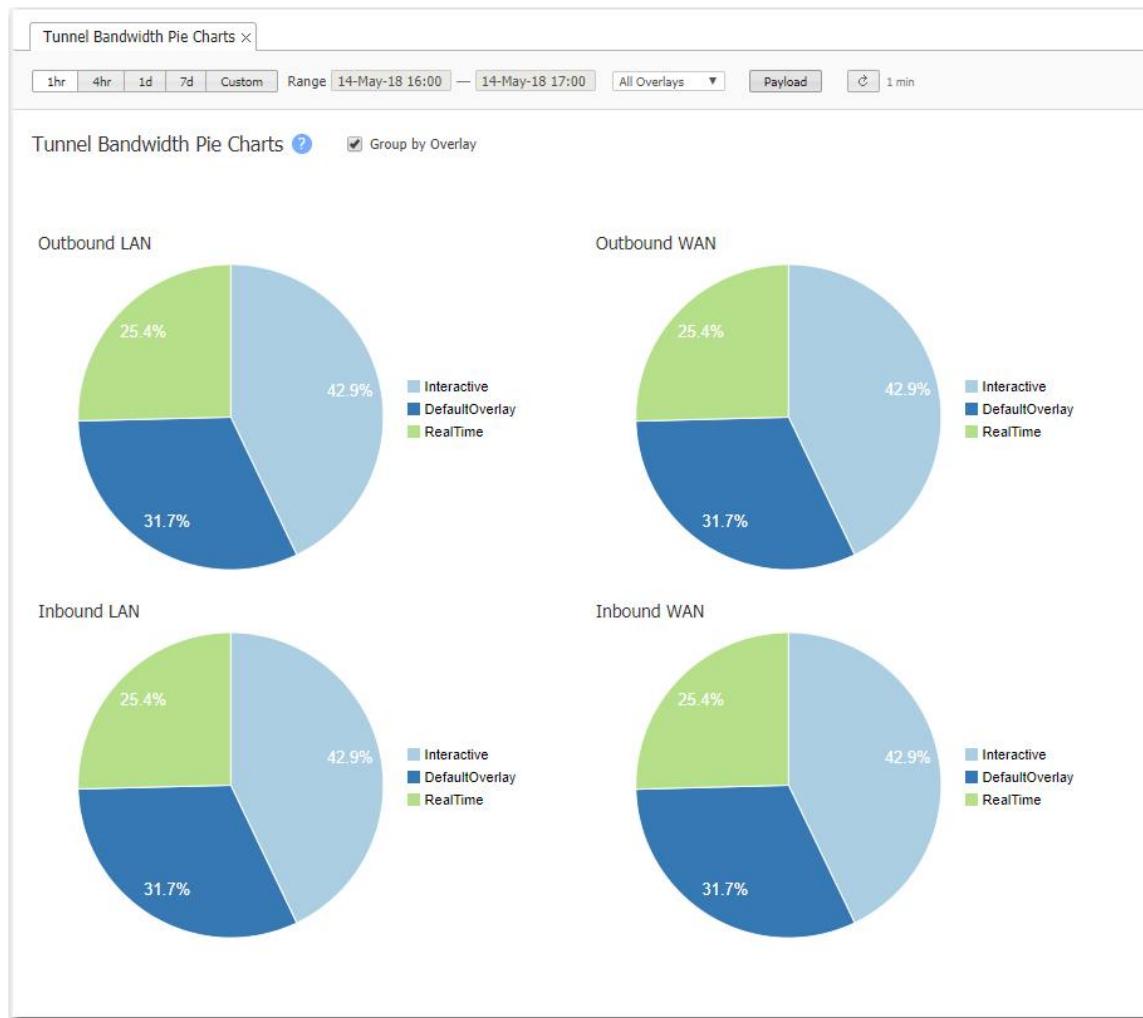
LiveView shows in real time how synergy is created to maintain coverage. The real-time chart shows the SD-WAN overlay at the top and the underlays at the bottom. The overlay is green and is delivering consistent application performance while both underlays are in persistent brown-out state.

## Tunnels Pie Charts

*Monitoring > Bandwidth > Tunnels > Pie Charts*

The **Tunnel Bandwidth Pie Charts** show the proportion of the bytes a tunnel consumes on the LAN and on the WAN.

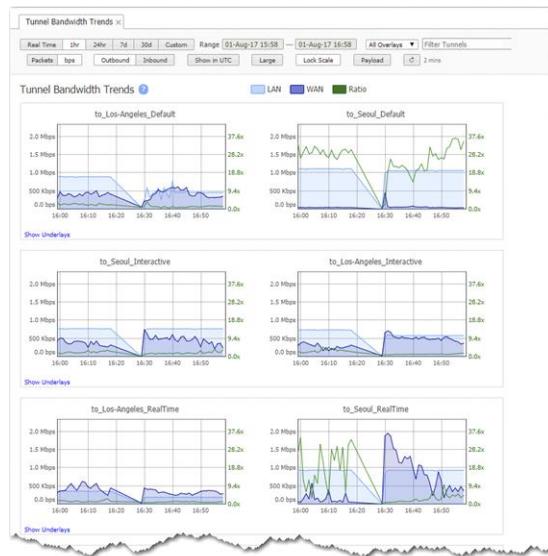
- Hovering over the charts and the legends reveals additional information.
- The WAN charts identify the percentage of the bandwidth the appliance saved by optimizing the traffic.



## Tunnel Bandwidth Trends

*Monitoring > Bandwidth > Tunnels > Trends*

The **Tunnel Bandwidth Trends** chart shows tunnel bandwidth usage over time.



- For each Business Intent Overlay, the specified Link Bonding Policy determines the bandwidth efficiency.
- To guarantee service quality levels, High Availability requires the most overhead and High Efficiency requires the least.
- Charts display the total bandwidth used.
- The Payload option shows how much raw data is transmitted. At the same time, it exposes the Peaks option, which enables the viewing of peak transmissions.

**NOTE** Underlay tunnels are a shared resource among overlays. Therefore, underlay charts display aggregated data.

## Tunnel Packet Counts

*Monitoring > Bandwidth > Tunnels > Packet Counts*

The **Tunnel Packet Counts** chart shows the tunnels that sent the most packets.

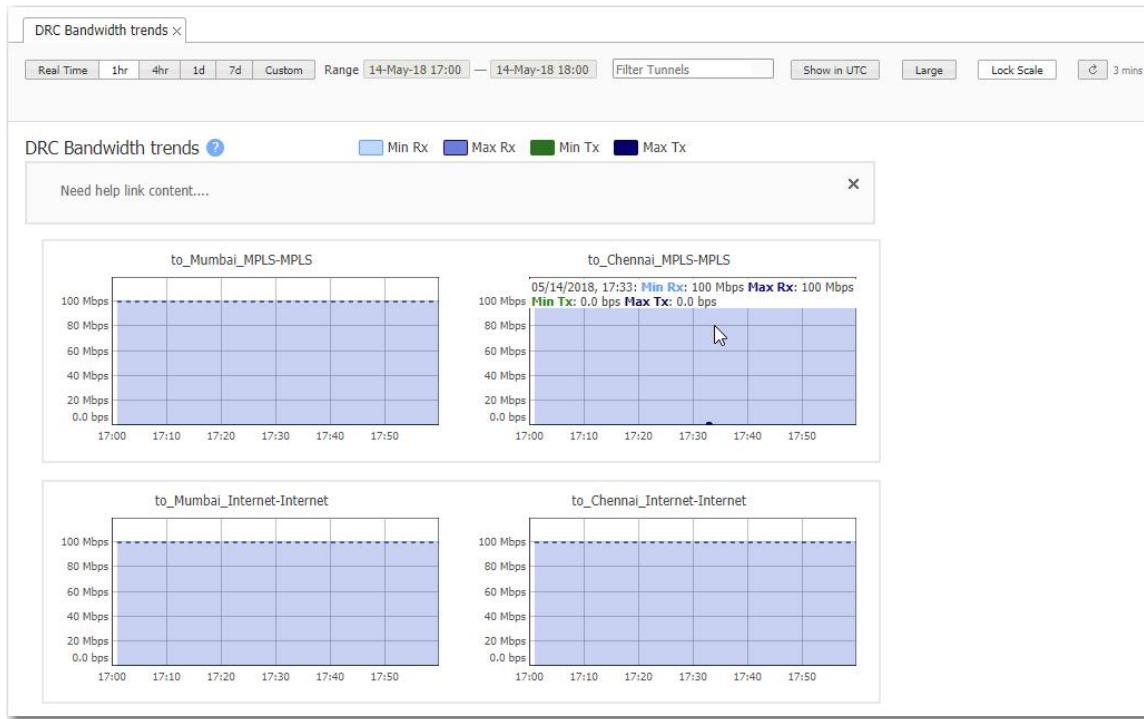
Tunnel Packet Counts							
		Inbound		Outbound			
Appliance	Tunnel	LAN Packets	LAN Max pps	WAN Packets	LAN Packets	LAN Max pps	WAN Packets
Portland	to_Los-Angeles_Interactive	205,482	130	180,494	206,522	142	185,660
Los-Angeles	to_Portland_Interactive	204,394	144	183,705	207,239	134	182,053
Portland	to_Los-Angeles_DefaultOverlay	140,864	114	115,397	163,154	142	155,597
Los-Angeles	to_Portland_DefaultOverlay	161,561	147	154,082	142,017	115	116,386
Portland	to_Los-Angeles_RealTime	128,076	58	119,651	115,782	54	100,504
Los-Angeles	to_Portland_RealTime	114,563	55	99,442	129,121	60	120,640
Mexico-City	to_Osaka_Interactive	0	0	4	0	0	4
Toronto	to_Frankfurt_DefaultOverlay	0	0	4	0	0	4
Dallas	to_Albuquerque_RealTime	0	0	4	0	0	4
Seoul	to_Singapore_Interactive	0	0	4	0	0	4
Pittsburgh	to_Portland_Interactive	0	0	4	0	0	4
Mexico-City	to_San-Jose_Interactive	0	0	4	0	0	4

## DRC Bandwidth Trends

*Monitoring > Bandwidth > Tunnels > DRC Trends*

The **DRC Bandwidth Trends** tab shows Dynamic Rate Control statistics over time.

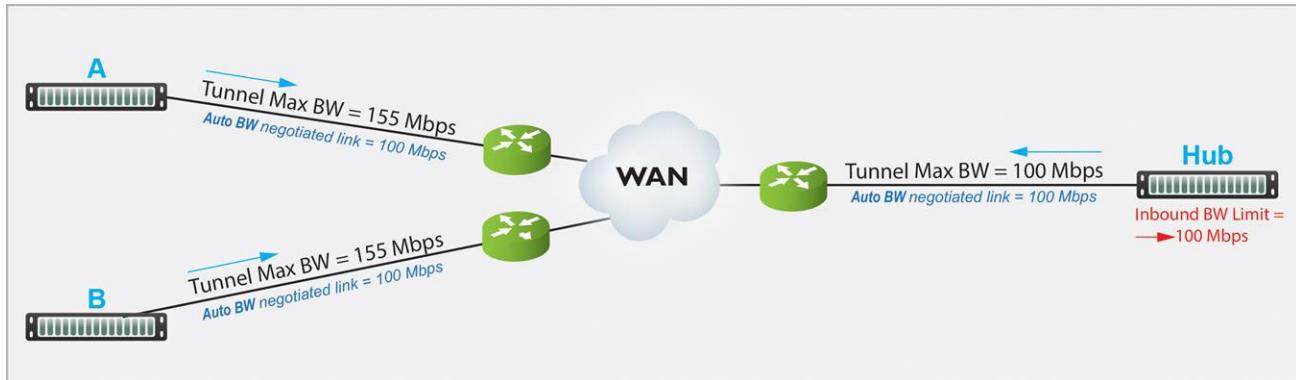
Dynamic Rate Control allows the Hub to regulate the tunnel traffic by lowering each remote appliance's **Tunnel Max Bandwidth**. The smallest possible value is that appliance's **Tunnel Min(imum) Bandwidth**.



## Dynamic Rate Control

**Tunnel Max Bandwidth** is the maximum rate at which an appliance can transmit.

**Auto BW** negotiates the link between a pair of appliances. In this example, the appliances negotiate each link down to the lower value (100 Mbps).



However, if **A** and **B** transmit at the same time, **Hub** could easily be overrun.

If **Hub** experiences congestion:

- **Enable Dynamic Rate Control** allows the Hub to regulate the tunnel traffic by lowering each remote appliance's **Tunnel Max Bandwidth**. The smallest possible value is that appliance's **Tunnel Min (imum) Bandwidth**.
- **Inbound BW Limit** caps how much the appliance can receive.

## Flows - Active and Recent

*Monitoring > Bandwidth > Flows > Active & Recent Flows*

The Flows tab enables you to view, filter, and manage flows for all your appliances. This tab also generates the Active & Recent Flows report, with or without filtering. This report retrieves the maximum number of most recent flows that are evenly distributed among the selected appliances.

The following table describes the fields displayed in the upper portion of the Flows tab.

Field	Description
<b>Application</b>	Includes built-in applications, custom applications, and user-created application groups. Select the text field and a list displays. Choose the application you want to apply to your flow or enter the exact application you want to apply.
<b>App Group</b>	Includes the application group created by the user. Select the text field and a list displays. Choose the application group you want to apply to your flow or enter the exact application group you want to apply.
<b>Role</b>	Specify the user role you want to apply.
<b>User Name</b>	Specify the name of the user you want to apply.
<b>IP/Subnet</b>	This shows the flows that match both SRC IP and DEST IP as the two endpoints if SRC:DEST is enabled. If not enabled, all sources will appear when the filter is applied. You can apply this filter by clicking <b>Enter</b> without selecting the Apply button if you want to do so.
<b>Port</b>	This displays ports with SRC and DEST as the two endpoints if SRC: DEST is enabled. If not enabled, all ports will appear when the filter is applied.
<b>Segment</b>	Displays flows originating in the specified segment. Click the double arrow icon to enable both fields and filter by destination segments as well.
<b>Zone</b>	You can filter flows by zone in the following ways: <ul style="list-style-type: none"> <li>• <b>To filter flows from and to the same firewall zone</b>, clear the <b>From:To</b> check box, and then select the appropriate firewall zone from the <b>Zone</b> drop-down list. Flows will be filtered based on the specified zone, both from and to the zone. Select <b>Any</b> to filter based on all zones.</li> <li>• <b>To filter flows from one firewall zone to another firewall zone</b>, select the <b>From:To</b> check box, and then specify the appropriate <b>From</b> and <b>To</b> firewall zones. Flows will be filtered based on the specified firewall zones.</li> </ul>

Field	Description
<b>VLAN</b>	Identifies the Virtual Local Area Network of a packet. Enter the <b>VLAN ID</b> you want to apply to your flow in the text field. EdgeConnect supports up to 64 VLANs.
<b>DSCP</b>	Select the desired DSCP from the list. You can choose any or a specified DSCP from the list.
<b>Protocol</b>	You can specify the protocol you want to apply to your filter. Select the text field and a list displays. You can select all or specify an individual protocol to apply.
<b>Domain</b>	Includes the domain you can specify to filter your flow. Use the format <code>*.domain.*</code> or <code>*.domain.[com, info, edu, org, net, and so forth.]</code> Select the text field and a list displays. Choose the domain you want to apply.
<b>Overlay</b>	Overlay to which the flow is applied. Overlays are defined on the <b>Business Intent Overlay</b> tab.
<b>Transport</b>	Select any of the three transport types: <b>SD-WAN</b> , <b>Breakout</b> , and <b>Underlay</b> . You can also apply a third-party service in this column if you have one configured.
<b>Flow Characteristics</b>	<p>You can apply any of the following flow characteristics to your flow: <b>Boosted</b>, <b>Directly Attached</b>, <b>IPS Dropped</b>, <b>Pass-Through</b>, <b>Slow Devices</b>, <b>Route Dropped</b>, <b>Firewall Dropped</b>, <b>Embryonic</b>, and <b>Asymmetric</b>.</p> <p><b>NOTE</b> You can select only one flow characteristic at a time.</p> <ul style="list-style-type: none"> <li>• Slow Devices: For debugging. A slow device cannot receive data quickly enough from the EdgeConnect appliance. This causes the appliance to expend too many resources for this device at the expense of accelerating other devices. To counteract this, disable TCP acceleration for the slow devices in the Optimization Policy.</li> <li>• Embryonic: For TCP, this is a flow that is in a state of formation (for example, three-way handshake is not complete). For UDP, ICMP, and other IP protocols, this is a flow for one-way traffic. ICMP Error packets without request are also considered embryonic. Dropped embryonic flows are highlighted in red.</li> <li>• Other drops are also highlighted in red, including firewall policy drops, some system/routing drops, and IPS drops. For the Firewall Protection Profiles feature, some flows could drop because of security errors, such as not complying to strict three-way handshakes. These are highlighted in red as well.</li> </ul>
<b>Include EdgeHA</b>	If not selected, Edge HA flows are excluded (default). If selected, the flows between Edge HA will be included.
<b>Include Built-in</b>	Includes the built-in policy flows. If not selected, they are excluded (default). If selected, they will be included.
<b>Active/Ended</b>	Select to apply an active or ended flow as a filter. If selected, the Started and/or Ended fields become available.
<b>Started/Ended</b>	Select the started or ended time of the flow from the drop-down menu. If <b>Custom</b> is selected, use the provided fields to specify an exact date and time range. These fields are available only if Active or Ended are selected.
<b>Duration</b>	Shows flows that have lasted through a specific time frame. You can select < (less than) or > (greater than), and enter a specific duration (in minutes).

Field	Description
<b>Bytes</b>	You can specify whether you want to filter flows that have transferred their total bytes or within the last five minutes.
<b>Filter</b>	This list has all the saved filters. When selected, the filter configurations are loaded. See more information below about the <b>Filter</b> option.

## Filter

You can configure specific filters in this field. Select the drop-down menu to see a list of default filters you can apply to your flows. When configured, you can add, edit, or delete filters if you select the edit icon.

Complete the following steps to add a filter:

1. Select the **Edit** icon next to the Filter drop down.
2. Create a filter or select one from the list.
3. Select **+Add**.
4. Select **Save**.

You can also select the history tab with the two arrows next to the **Filter** field if you want to go back to a previously applied filter. A maximum of 20 previously applied filters can be saved.

## Reset or Reclassify Flows

- You can **Reclassify** or **Reset** [Selected / All Returned / All] flows:
  - Resetting the flow kills it and restarts it. It is service-affecting.
  - Reclassifying the flow is not service-affecting. When policy changes occur, flow reclassification makes a best-effort attempt to conform the flow to the change. If the flow cannot be successfully "diverted" to this new policy, then an Alert asks if you want to reset.
  - **Selected** flows are individually selected; **All Returned** results from filtering (up to the max number of returnable flows); and **All** refers to all flows, visible or not.
- To export the table as a .csv file, select **Export**.
- Reduction (%) refers to reduced WAN traffic, relative to a specific appliance:
  - Reduction (%) for **Outbound** traffic =  $100(\text{Received from LAN} - \text{Transmitted to WAN})/\text{Received from LAN}$
  - Reduction (%) for **Inbound** traffic =  $100(\text{Transmitted to LAN} - \text{Received from WAN})/\text{Transmitted to LAN}$
- Flow **Details** are provided primarily to assist Support with troubleshooting and debugging.
- To set the column visibility, right-click any header in the Flows table. This will enable you to hide or

unhide any selected fields.

- You can also select, drag, and drop any of the columns in the table to the order you want.

## Additional Information about Flows

Note the following version specific and general information about flows:

### ECOS 9.1 Behavior Changes

All flows in drop state are reset at flow reclassify time, overriding intervals described below.

### ICMP/UDP Flows

- For any non-TCP connection (such as icmp, UDP), a flow is deleted only from inactivity.
- The inactivity timeout is three minutes for this type of flow. For example, after a ping connection is stopped, the flow still appears in the "Current Flows" for three minutes. This setting can be modified by using the system template.

### TCP Non Accelerated Flows

- For a TCP connection, a flow is deleted under different timeouts. A half-open (single SYN) connection stays for two minutes if the connection does not establish correctly. A half-close (single FIN) or unclean-close (RST) deletes the connection after two minutes. A normal close (FIN-FIN) deletes the connection almost immediately.
- A TCP connection also has an inactivity timeout. If no activity is detected on an established TCP connection for 30 minutes (by default), the flow is deleted. This setting can be modified by using the system template.

### TCP Accelerated Flows

- Timeout is determined by the configured Keep Alive Timers.
  - A heartbeat ACK is sent to idle endpoints after ten minutes.
  - If the endpoints have closed, an RST is returned and the connection is deleted after two more minutes due to the unclean-close.
- The timers can be modified per sequence number by using the Optimization Template.
  - Idle Timeout: The period of time that a TCP connection has to be idle before a keep-alive is sent. (Default 600 seconds)
  - Probe Interval: The time in seconds between each keep-alive probe. (Default 30 seconds)
  - Probe Count: The number of times TCP probes the connection to determine whether it is alive after the keep-alive option has been activated. The connection is assumed to be lost after sending this number of keep-alive probes. (Default 8)

- Auto Reset Flows** - Enables or disables the auto-reset of TCP flows. If a connection is seen by an appliance but after the handshake already completed, the connection would normally remain but without TCP Acceleration. If this feature is enabled, and a connection is reclassified in the Flows report, around 30 seconds later, it will be reset. When the endpoints re-establish the flow, it now will be subject to the optimization and route policies it matches. This feature is disabled by default. It can be enabled per sequence number by using the Optimization Template.

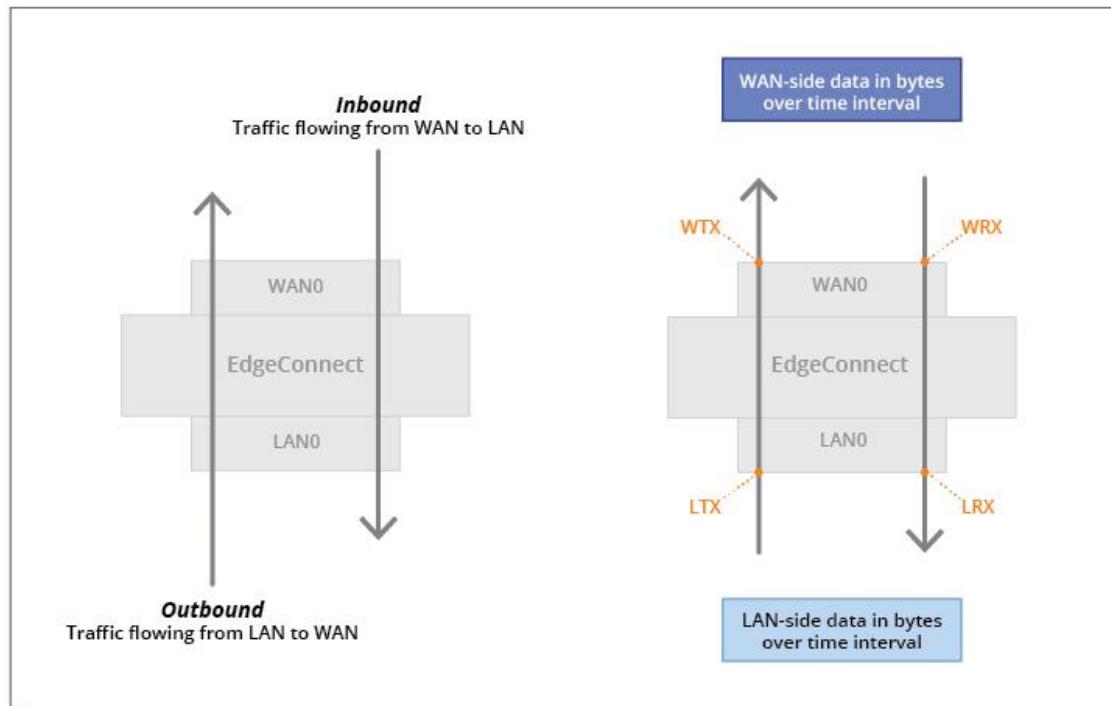
## Outbound and Inbound

*Outbound* and *Inbound* in Aruba EdgeConnect refer to the direction of traffic as it flows from the LAN-side to the WAN-side of an appliance, or from the WAN-side to the LAN-side of an appliance. These are different from actual interface names, such as WAN0 or LAN0.

Description	Counter Type	Traffic Received On	Traffic Forwarded To
<b>Inbound LAN</b>	LAN TX	WAN-side interface	LAN-side interface
<b>Outbound LAN</b>	LAN RX	LAN-side interface	WAN-side interface
<b>Inbound WAN</b>	WAN RX	WAN-side interface	LAN-side interface
<b>Outbound WAN</b>	WAN TX	LAN-side interface	WAN-side interface

WAN optimization data reduction is calculated using the following formula:

$$\text{Data Reduction \%} = (\text{LAN Bytes} - \text{WAN Bytes}) / \text{LAN Bytes}$$



## Appliance Flow Counts

*Monitoring > Bandwidth > Flows > Appliance Counts*

The **Appliance Flow Counts** chart lists the top appliances according to which ones had the most flows within a selected time period.

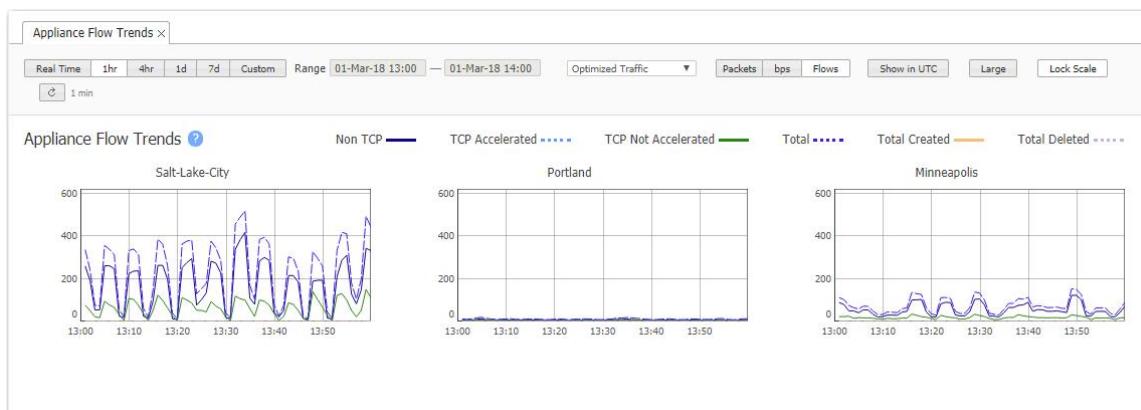
When you filter on **All Traffic**, the **Created** and **Deleted** columns display the number of new and ended flows for that same time period. The **Max** column value is from a one-minute window within the time range.

Appliance	TCP Accelerated				TCP Unaccelerated				Non TCP			
	Max	Avg	Created	Deleted	Max	Avg	Created	Deleted	Max	Avg	Created	Deleted
Los-Angeles	0	0	0	0	322	150	7,527	7,427	497	31	1	1
Minneapolis	0	0	0	0	9	2	0	0	20	5	0	0
Portland	0	0	0	0	165	140	7,475	7,368	2	0	1	2
Salt-Lake-City	0	0	0	0	282	12	0	0	924	31	0	0

## Appliance Flow Trends

*Monitoring > Bandwidth > Flows > Appliance Trends*

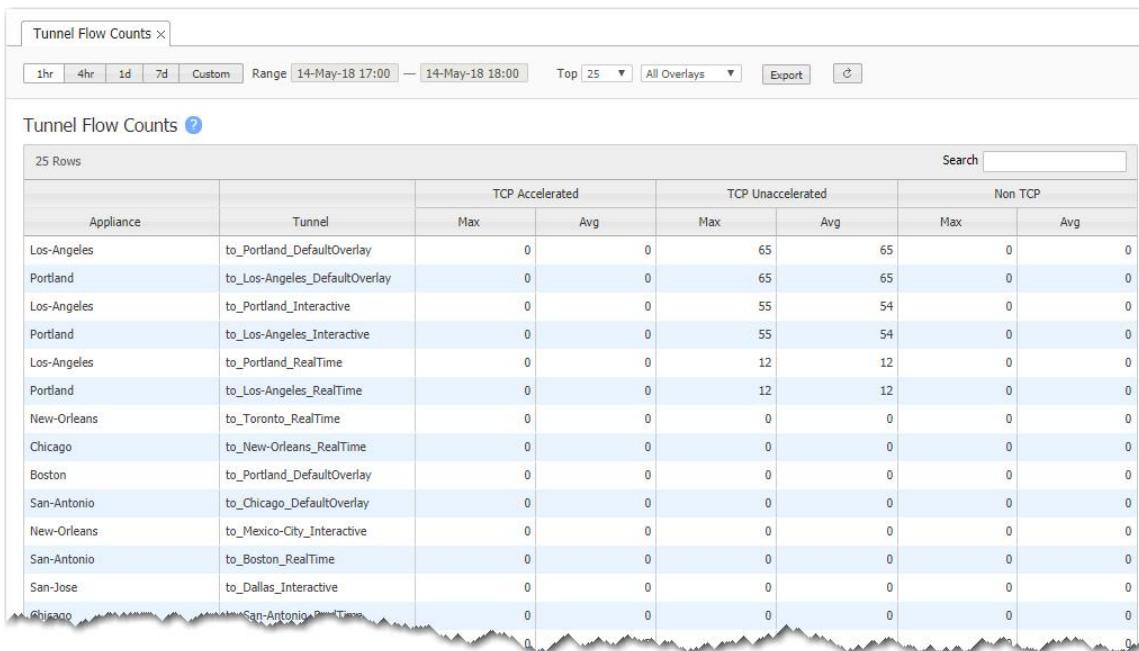
The **Appliance Flow Trends** chart shows the number of flows, packets, and bits/second through the appliance over time. It also differentiates among TCP (accelerated and unaccelerated) flows and non-TCP flows.



## Tunnel Flow Counts

*Monitoring > Bandwidth > Flows > Tunnel Counts*

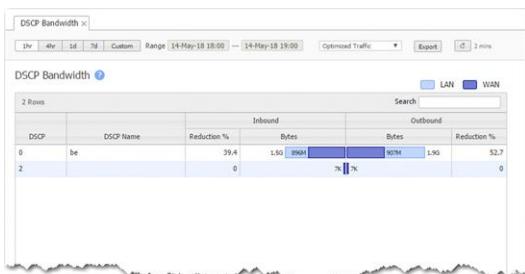
The **Tunnel Flow Counts** chart lists the tunnels with the most flows on average. It differentiates flows into TCP (accelerated and unaccelerated) and non-TCP, and also shows peak values.



## DSCP Bandwidth

*Monitoring > Bandwidth > DSCP > Summary*

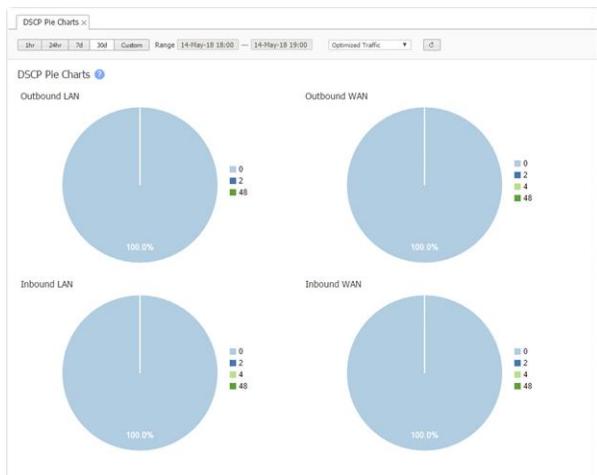
The **DSCP Bandwidth** chart shows the DSCP classes that are sending the most data.



## DSCP Pie Charts

*Monitoring > Bandwidth > DSCP > Pie Charts*

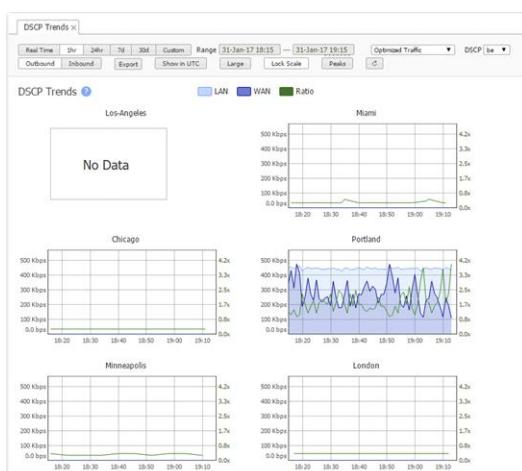
The **DSCP Pie Charts** show the proportion of traffic in each DSCP class. Hovering over the charts and the legends reveals additional information.



## DSCP Trends

*Monitoring > Bandwidth > DSCP > Trends*

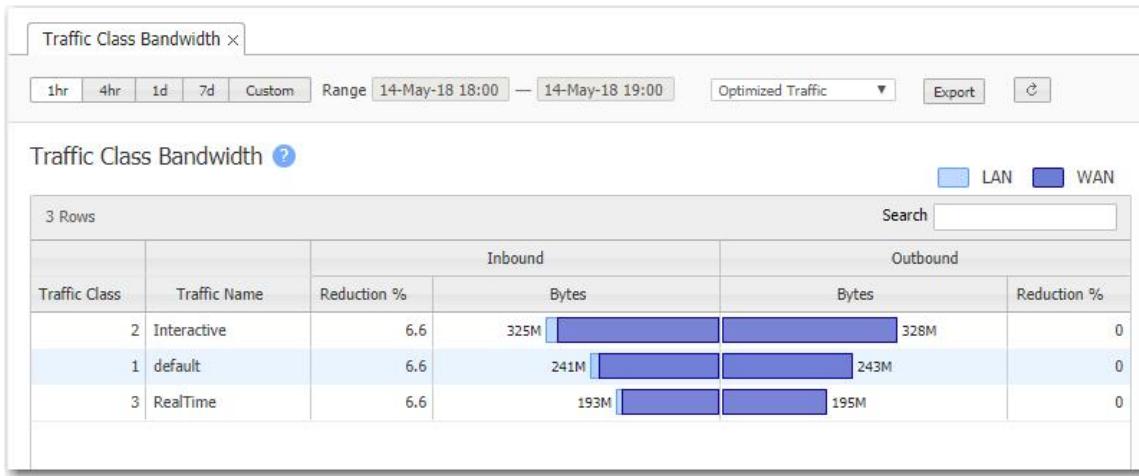
This tab shows DSCP usage over time.



## Traffic Class Bandwidth

*Monitoring > Bandwidth > QoS > Summary*

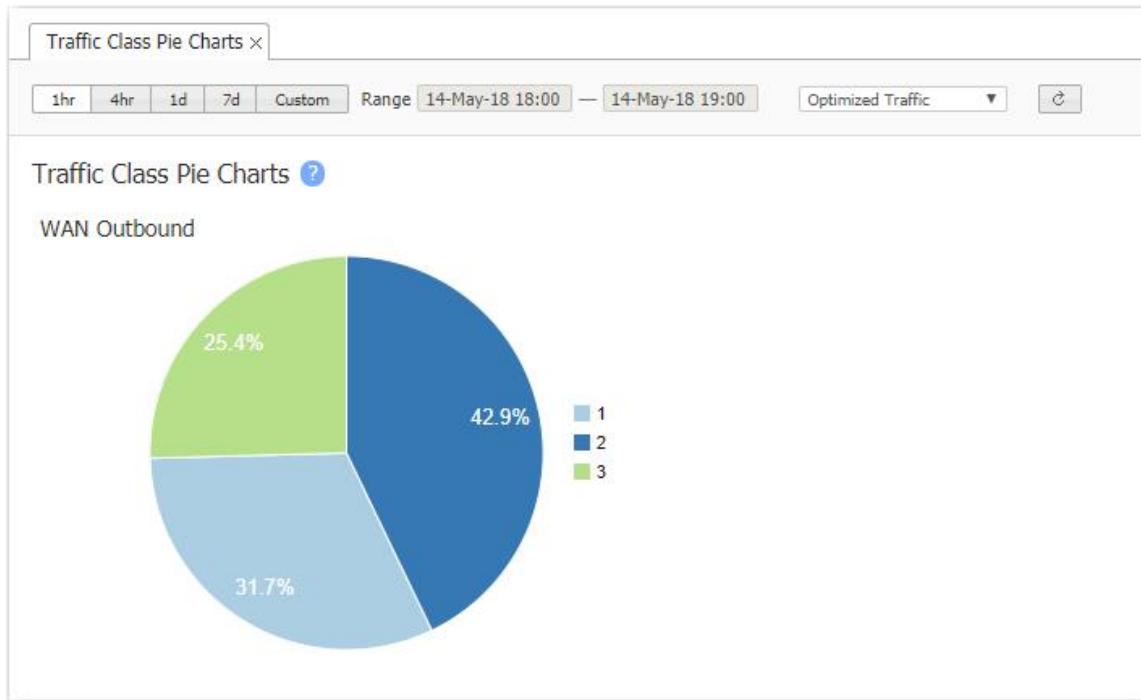
The **Traffic Class Bandwidth** chart shows the QoS traffic classes that are sending the most data.



## Traffic Class Pie Charts

*Monitoring > Bandwidth > QoS > Pie Charts*

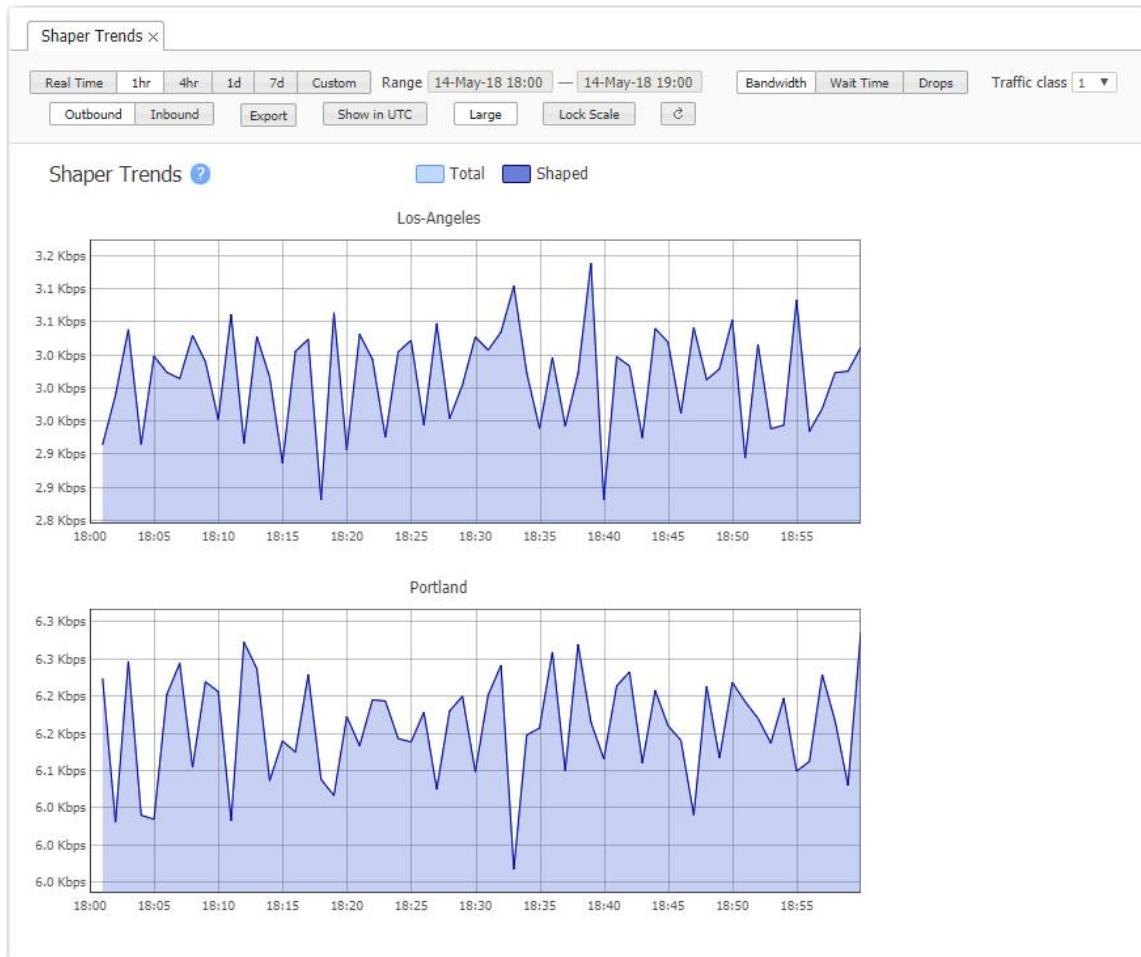
The **Traffic Class Pie Charts** show the proportion of traffic in each Traffic class. Hovering over the charts and the legends reveals additional information.



## QoS (Shaper) Trends

*Monitoring > Bandwidth > QoS > Trends*

This tab shows how much bandwidth any traffic class uses over time.



## Shaper Summary

Use this tab to view the Shaper Summary for all traffic classes on selected appliances. The Shaper delays certain packet types to optimize overall network performance. For more information about shaping, see [Shaper Tab on page 296](#) and [Shaper Template on page 371](#).

- Use the controls above the table to specify how much data—time and date range—you want to see in the summary.
- Use the **Top X** filter to limit data according to top applications by total traffic bytes. You can include the top 10, 25, 50, 100, or 1000 applications.
- Click **Outbound** or **Inbound** to change the summary by traffic direction.

The following information is included in the Shaper Summary:

Field	Description
<b>Appliance</b>	Name of the appliance that is shaping traffic to generate the Shaper Summary.
<b>Traffic Class</b>	Traffic classes defined by Shaper parameters. The following four are pre-configured by Orchestrator: Real-time, Interactive, Default, and Best Effort. The user can configure the remaining six classes.
<b>Total Bytes</b>	Total amount of bytes being shaped.
<b>Shaped Bytes</b>	Amount of bytes used for shaping.
<b>Shaped Packets</b>	Amount of packets used for shaping.
<b>Average Wait Time (ms)</b>	Specified amount of time Orchestrator waits until packets are dropped while shaping is in progress.
<b>Drop Packets</b>	Amount of packets that have been reported as dropped due to expiration in the Shaper queue.
<b>Other Drops</b>	Refers to all other drops besides the expired drop packets.
<b>Trends</b>	Click the graph icon to see the Shaper Bandwidth Trends charts, which show Inbound and Outbound traffic trends in graphs.

## Boost Tab

*Monitoring > Bandwidth > Boost > Summary*

This tab provides a summary of the Boost configuration and usage for selected appliances. You can change the time period for which Boost statistics are displayed by using the **1hr**, **4hr**, **1d**, and **7d** buttons at the top of the tab, or click **Custom** to specify a custom date range and granularity.

The screenshot shows the Boost tab interface. At the top, there are buttons for time ranges: 1hr, 4hr, 1d, 7d (selected), Custom, and a date range selector from 30-Jun-21 09:23 to 07-Jul-21 09:23. There is also an Export button and a refresh icon. Below this, the summary section displays "Boost" status, "EC Boost" usage (7,010,000 Kbps / 10,000,000 Kbps Used | 2,990,000 Kbps Remaining), and a "Configure Boost" button. A search bar is also present. The main area contains a table with two rows of data:

Appliance	Configured Boost (Kbps)	% Time Insufficient Boost	Minutes Insufficient Boost	Total Boost Bytes	Trends
[Redacted]	100000	0	0	3.1M	
[Redacted]	50000	0	0	19.1M	

This tab provides the following details about your Boost configuration:

Field	Description
<b>Appliance</b>	Name of the appliance.
<b>Configured Boost (Kbps)</b>	Boost bandwidth configured on the appliance.

Field	Description
<b>% Time Insufficient Boost</b>	Percentage of time when Boost bandwidth was not available for use.
<b>Minutes Insufficient Boost</b>	Amount of time (in minutes) when Boost bandwidth was not available for use.
<b>Total Boost Bytes</b>	Total amount of Boost bandwidth used over the specified time range.
<b>Trends</b>	Graph displaying detailed Boost trends for the specified appliance.

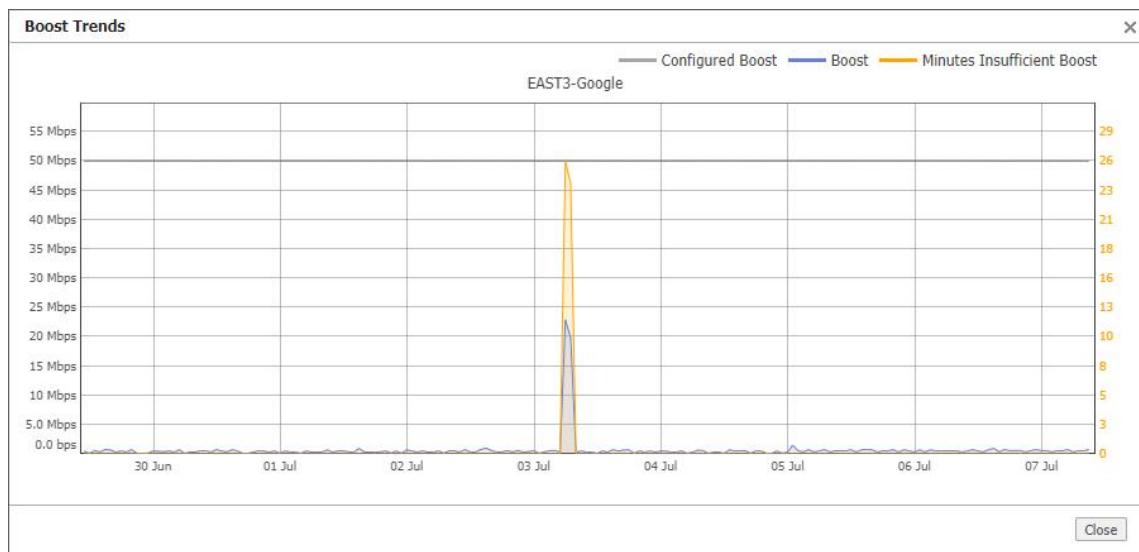
The total Boost bandwidth available to your network is controlled by your license. If necessary, you can purchase additional Boost bandwidth.

If a Boost license is available, you can assign Boost to appliances on the Licenses tab or on an appliance's Deployment page. You can also configure Boost allocation using Business Intent Overlays.

**NOTE** Your network uses a single queue for Boost across all appliances. When that queue is completely utilized, appliances will have insufficient Boost for any additional demands.

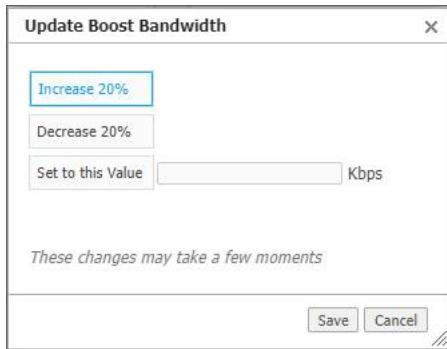
## Boost Trends

To view Boost trends for a specific appliance, click the graph icon in the Trends column. The Boost Trends graph displays Configured Boost, Boost, and Minutes Insufficient Boost over the time period specified on the Boost tab.



## Change Boost Configuration

To change the Boost configuration of one or more appliances selected in the table, click **Configure Boost**. You can increase or decrease Boost bandwidth by 20%, or set the bandwidth to a specific value in Kbps. Click **Save** to apply your changes, or click **Cancel** to not apply your changes and close the dialog box.



## Firewall Drops

*Monitoring > Bandwidth > Firewall Drops > Summary*

You can use the Firewall Drops tab to view the statistics on various flows, packets, and bytes dropped or allowed by a zone-based firewall for a given time range.

- You can select a range of time (in hours and days) to view the firewall drops. You can also select to view in Matrix or Table view.
- Select **Export** to export the report to an excel spreadsheet.

Firewall Drops												
Source Segment: Default Destination Segment: Default												
3 Rows												
Appliance	Src Segment	Dest Segment	From Zone	To Zone	Flows Dropped	Flows Allowed	Packets Dropped	Packets Allowed	Bytes Dropped	Bytes Allowed	Charts	
Teiron-Powers	Default	Default	UNTRUSTED	UNTRUSTED	0	92	0	108	0	8.8K		
Teiron-Powers	Default	MGMT	UNTRUSTED		0	738	0	14.8K	0	8.3M		
Teiron-Powers	Default	MGMT	TRUSTED		0	0	0	0	0	0		

- If segmentation is enabled, you can specify the **Source Segment** and the **Destination Segment** to search for the flows, packets, and firewall drops in that segment.
- In the charts column, you can select the chart icon.
  - In this pop-up, you can see packets, and bytes dropped or allowed by a zone-based firewall for a given time range.

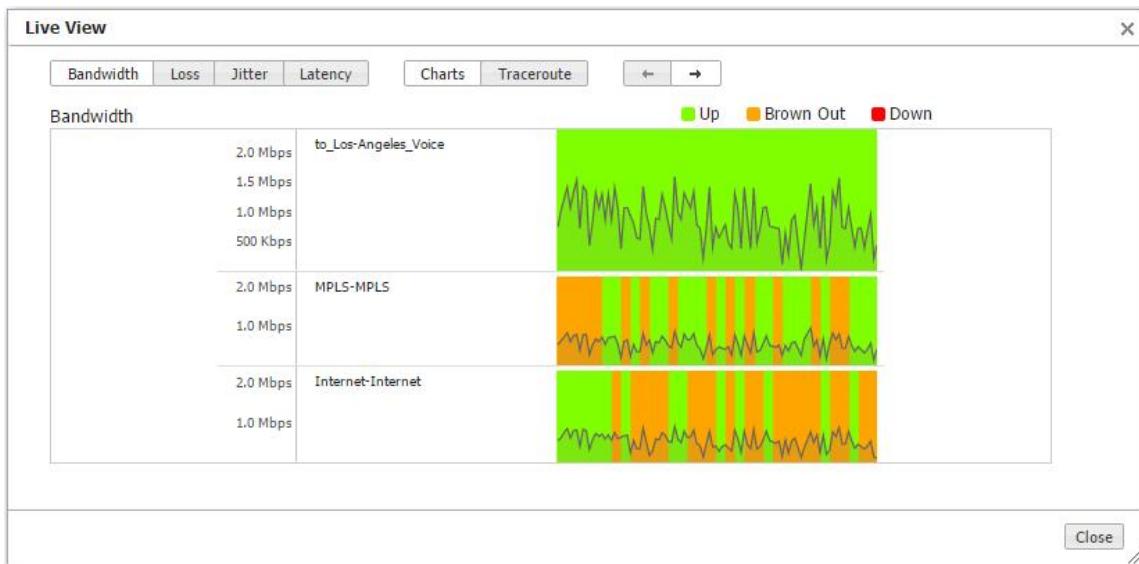


# Tunnel Health

## Live View

*Monitoring > Tunnel Health > Live View*

Live View shows the live bandwidth, loss, latency, and jitter on all tunnels. For an overlay, it also shows live tunnel states—Up, Browned Out, or Down.



LiveView shows in real time how synergy is created to maintain coverage. The real-time chart shows the SD-WAN overlay at the top and the underlay networks at the bottom. The overlay is green and delivering consistent application performance while both underlays are in persistent brown-out state.

## Loss Summary

*Monitoring > Tunnel Health > Loss > Summary*

The **Loss** chart shows tunnels that have the most dropped packets. Statistics are summarized for the selected time period.

The screenshot shows a table titled 'Loss' with various columns including Appliance, Tunnel, <-> WAN Packets, <-> POST-FEC Loss Packets, <-> PRE-FEC Loss Packets, <-> Loss %, Loss %-->, WAN Packets -->, PRE-FEC Loss Packets -->, POST-FEC Loss Packets -->, Remote Tunnel, and Remote Appliance. The table lists several tunnels with their respective statistics. A legend at the top right indicates that green bars represent Pre-FEC Loss and orange bars represent Post-FEC Loss.

Loss											
Appliance	Tunnel	<-> WAN Packets	<-> POST-FEC Loss Packets	<-> PRE-FEC Loss Packets	<-> Loss %	Loss %-->	WAN Packets -->	PRE-FEC Loss Packets -->	POST-FEC Loss Packets -->	Remote Tunnel	Remote Appliance
Edinburgh-Main	to_EMEA4-AWS_REALTIME	6,560	166	559	7.85	3.31	2.71	6.58	7,179	506	208 to_Edinburgh-Main_... EMEA4-AWS
Sussex-Pumpkin-EC-US-Starlink	to_EMEA4-AWS_RECVATIO...	11,635	171	200	1.49	1.62			11,326	175	132 to_Sussex-Pumpkin-EC_... EMEA4-AWS
Sussex-Pumpkin-EC-US-Starlink	to_EMEA4-AWS_REALTIME	8,777	46	89	1	1	1.08		9,508	104	54 to_Sussex-Pumpkin-EC_... EMEA4-AWS
Sussex-Pumpkin-EC-US-Starlink	to_EMEA4-AWS_RECVATIO...	7,773	29	75	0.96	1	1.22		7,802	96	56 to_Sussex-Pumpkin-EC_... EMEA4-AWS
Sussex-Pumpkin-EC-US-Starlink	to_EMEA4-AWS_REALTIME	11,830	42	60	0.5	1	1.17		11,401	257	230 to_Sussex-Pumpkin-EC_... EMEA4-AWS
CH-AI	to_DEFAULT1-AWS_REALTIME	1,891	0	0	0	0			2,273	0	0 to_CH-AI_REALTIME DEFAULT1-AWS
CH-AI	to_DEFAULT2-AWS_REALTIME	355	0	0	0	0			487	0	0 to_CH-AI_REALTIME DEFAULT2-AWS
CH-AI	to_DEFAULT1-AWS_BESTEFORT	0	0	0	0	0			4,898	0	0 to_CH-AI_BESTEFORT DEFAULT1-AWS
CH-AI	to_DEFAULT2-AWS_CASB	0	0	0	0	0			0	0	0 to_CH-AI_CASB DEFAULT2-AWS
CH-AI	to_DEFAULT1-AWS_CASB	0	0	0	0	0			0	0	0 to_CH-AI_CASB DEFAULT1-AWS

Loss percentages, before and after Forward Error Correction (FEC), are determined by data that the local EdgeConnect observes. Two types of loss are measured:

- Pre-FEC Loss % - Percent of data packets lost before applying FEC / Total sent packets. This measure indicates what the packet loss *would be* if FEC were not applied.
- Post-FEC Loss % - Percent of data packets lost after applying FEC / Total sent packets. This measure indicates what the packet loss *is* after FEC is applied.

The total number of sent packets over the link is calculated based on three parameters:

- Total received packets (SUM\_WRX\_PKTS)
- Recovered packets from FEC (CORRECTED\_PACKETS)
- Unrecovered packets after FEC (SUM\_POST\_LOSS)

Calculations are based on the following formulas:

- Total sent packets = SUM\_WRX\_PKTS + CORRECTED\_PACKETS + SUM\_POST\_LOSS
- Packets lost in transmission (SUM\_PRE\_LOSS) = CORRECTED\_PACKETS + SUM\_POST\_LOSS

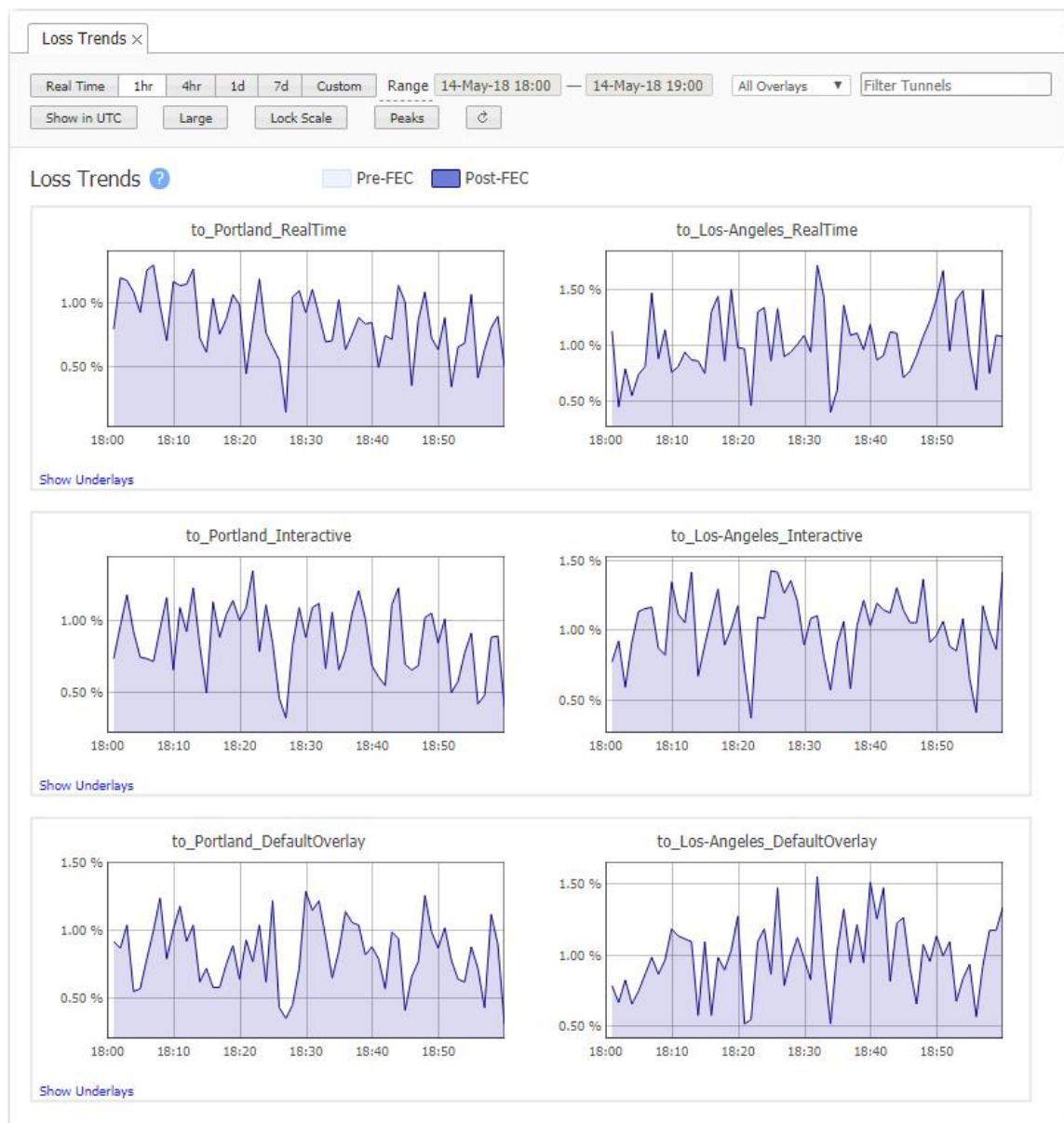
Based on the above information, the Pre-FEC and Post-FEC Loss percentages are calculated as follows:

- Pre-FEC Loss (%) = SUM\_PRE\_LOSS \* 100 / (SUM\_WRX\_PKTS + SUM\_PRE\_LOSS)
- Post-FEC Loss (%) = SUM\_POST\_LOSS \* 100 / (SUM\_WRX\_PKTS + SUM\_PRE\_LOSS)

## Loss Trends

[Monitoring > Tunnel Health > Loss > Trends](#)

The **Loss Trends** chart shows tunnel packet loss over time, before and after Forward Error Correction (FEC).

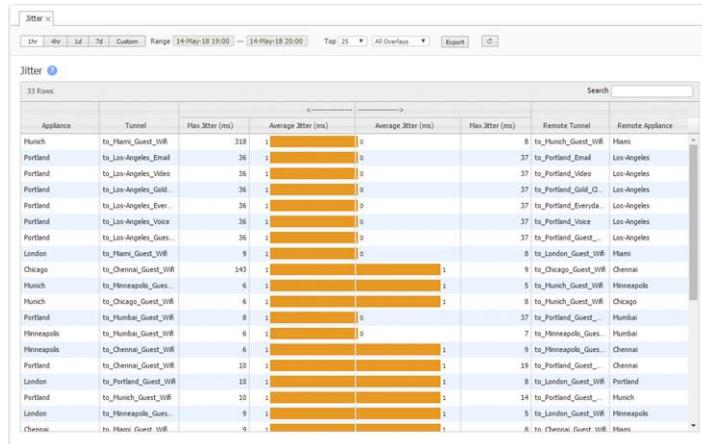


**NOTE** Underlay tunnels are a shared resource among overlays. Therefore, underlay charts display aggregated data.

## Jitter Summary

*Monitoring > Tunnel Health > Jitter > Summary*

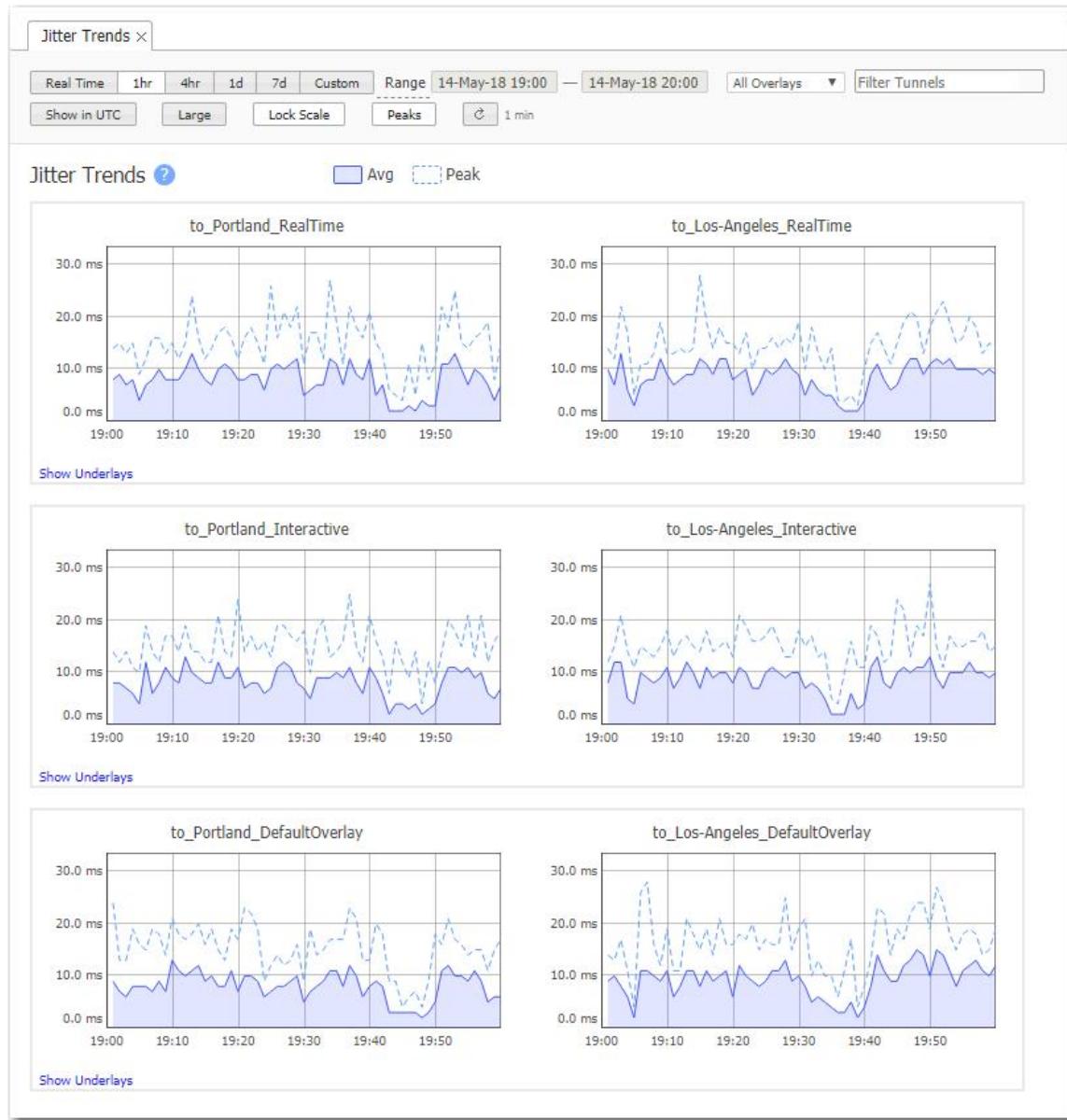
The **Jitter** chart shows the tunnels that have the most Jitter. Statistics are summarized for the selected time period. Jitter can be caused by congestion in the LAN, firewall routers, bottleneck access links, load sharing, route flapping, routing table updates, and timing drifts.



## Jitter Trends

*Monitoring > Tunnel Health > Jitter > Trends*

This tab shows tunnel jitter time.

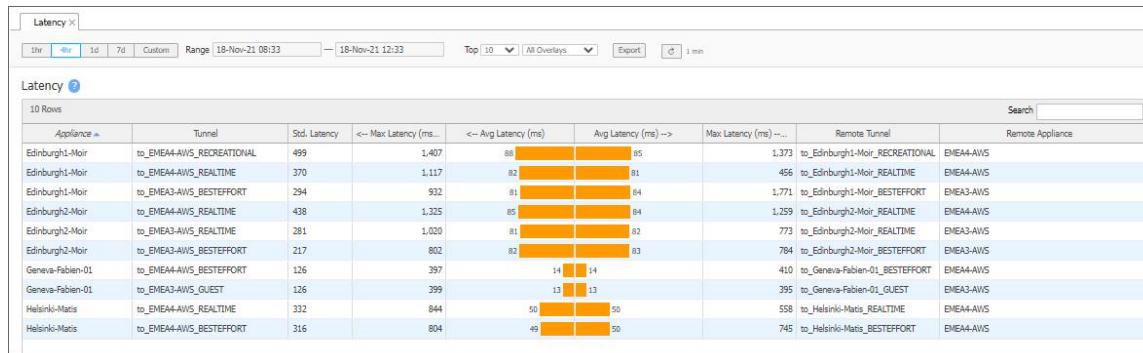


**NOTE** Underlay tunnels are a shared resource among overlays. Therefore, underlay charts display aggregated data.

## Latency Summary

*Monitoring > Tunnel Health > Latency > Summary*

The Latency tab shows summary statistics for latency (transmission delay) on an in-band, end-to-end tunnel basis for the selected time/date range. Either overlay or underlay tunnels can be displayed, and anywhere between the top 10 to top 1000 tunnels are displayed by round-trip time (RTT).



On this tab, latency is a measure of the RTT within a tunnel in milliseconds. Values on the left display RTT as measured by the local appliance. Values on the right display RTT as measured by the appliance at the remote end of the tunnel.

Some column descriptions follow:

- Std. Latency - Standard deviation (in milliseconds) of latency values for the tunnel within the specified period.  
Standard deviation is a measure of the amount of variation in a set of values. Low standard deviation indicates that the values tend to be close to the mean or expected value while a high standard deviation indicates that the values are spread over a wider range.
- Max Latency (ms) - Maximum RTT value (in milliseconds) for the tunnel within the specified range.
- Avg Latency (ms) - Average RTT value (in milliseconds) for the tunnel within the specified range.

High latency can negatively affect throughput in the network, most noticeably for TCP traffic. Physical distance has the most significant impact on latency. For example:

- If data is crossing the United States, you can expect delays from 60 to 120 milliseconds
- International transmissions can normally experience delays up to 200 milliseconds
- Satellite transmissions often have delays of about 1/2 second, and up to several seconds are possible

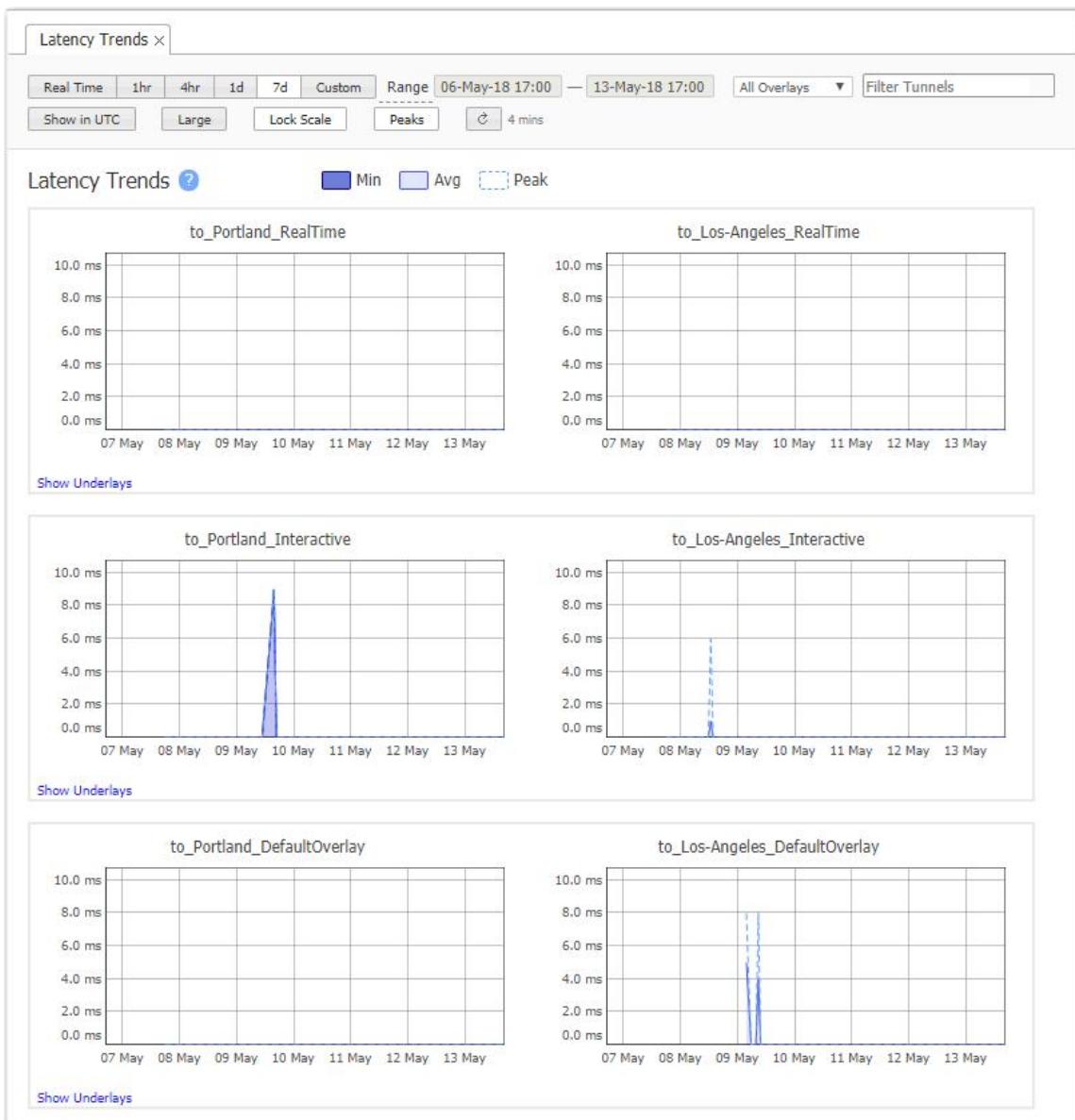
High latency can also be caused by equipment (hop-by-hop delays), or by loss or congestion resulting from lost packets, lost acknowledgments, and necessary retransmissions.

TCP Acceleration (a function of Boost) can mitigate the impact of latency on throughput. In addition, path conditioning and packet re-ordering (a function of Business Intent Overlay link bonding) can mitigate the impact of loss and out-of-order packets on TCP throughput by reducing the number of retransmissions.

## Latency Trends

*Monitoring > Tunnel Health > Latency > Trends*

The **Latency Trends** chart shows tunnel latency over time.



**NOTE** Underlay tunnels are a shared resource among overlays. Therefore, underlay charts display aggregated data.

## Out of Order Packets Summary

*Monitoring > Tunnel Health > Out of Order Packets > Summary*

The **Out of Order Packets** chart shows the tunnels that receive the most packets out of sequence relative to how they were sent.

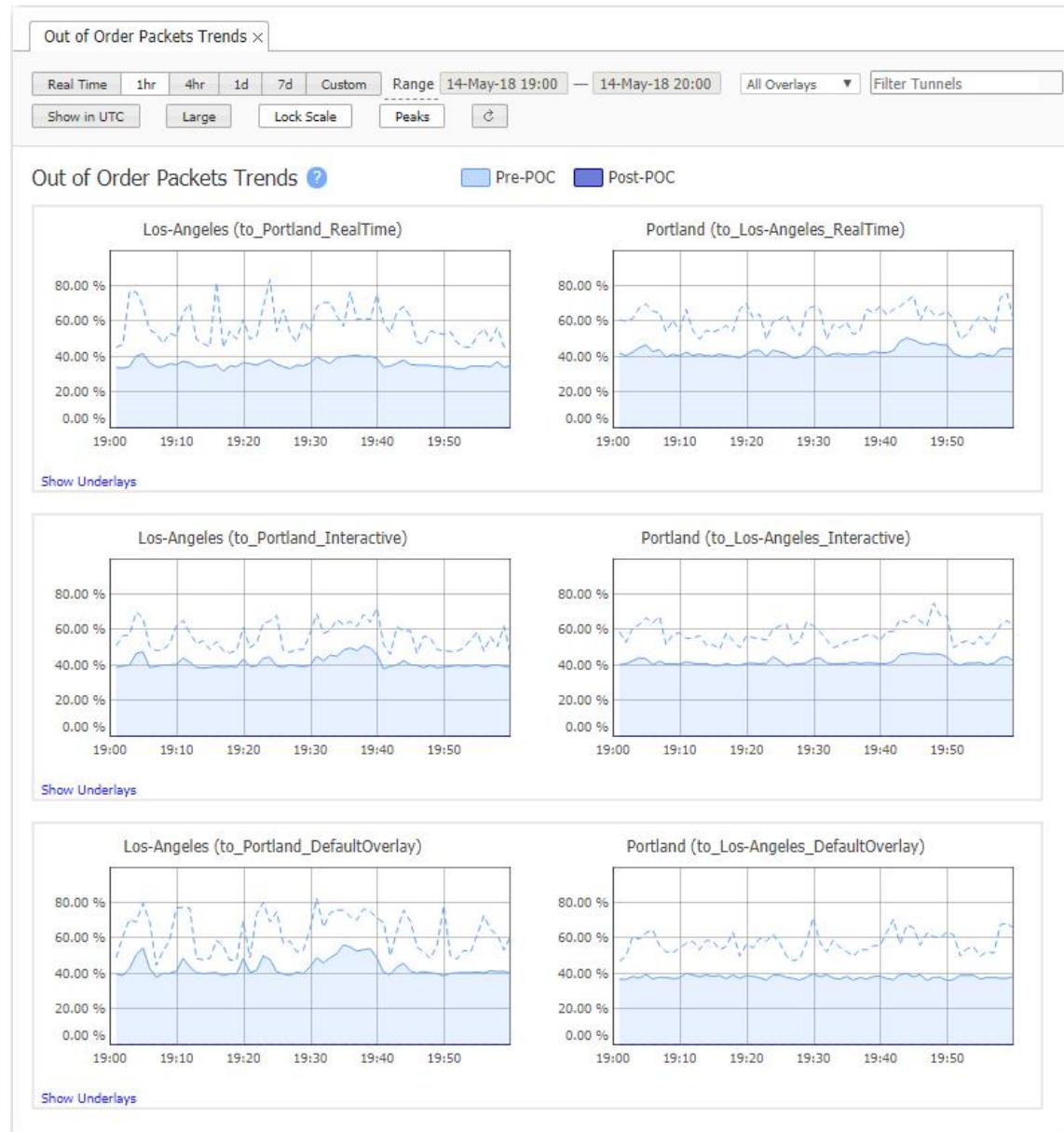
The screenshot shows the 'Out of Order Packets' summary page. At the top, there are time range filters (1hr, 4hr, 1d, 7d, Custom) set to 14-May-18 19:00 — 14-May-18 20:00, and a search bar. Below the filters is a table titled 'Out of Order Packets' with 6 rows. The table has columns for Appliance, Tunnel, Average Out Of Order %, Average Out Of Order % (with a bar chart), Remote Tunnel, and Remote Appliance. A legend at the top right indicates that green bars represent 'Pre-POC Out Of Order' and orange bars represent 'Post-POC Out Of Order'.

Appliance	Tunnel	<----->		Remote Tunnel	Remote Appliance
		Average Out Of Order %	Average Out Of Order %		
Portland	to_Los-Angeles_Interactive	30	0    0	29.5	Los-Angeles
Portland	to_Los-Angeles_DefaultOverlay	28.6	0    0	30.3	Los-Angeles
Los-Angeles	to_Portland_DefaultOverlay	30.3	0    0	28.6	Portland
Portland	to_Los-Angeles_RealTime	30.3	0    0	27.2	Los-Angeles
Los-Angeles	to_Portland_Interactive	29.5	0    0	30	Portland
Los-Angeles	to_Portland_RealTime	27.2	0    0	30.3	Portland

# Out of Order Packets Trends

*Monitoring > Tunnel Health > Out of Order Packets > Trends*

The **Out of Order Packets Trends** chart shows tunnel packets that are out of order over time, before and after Packet Order Correction (POC).

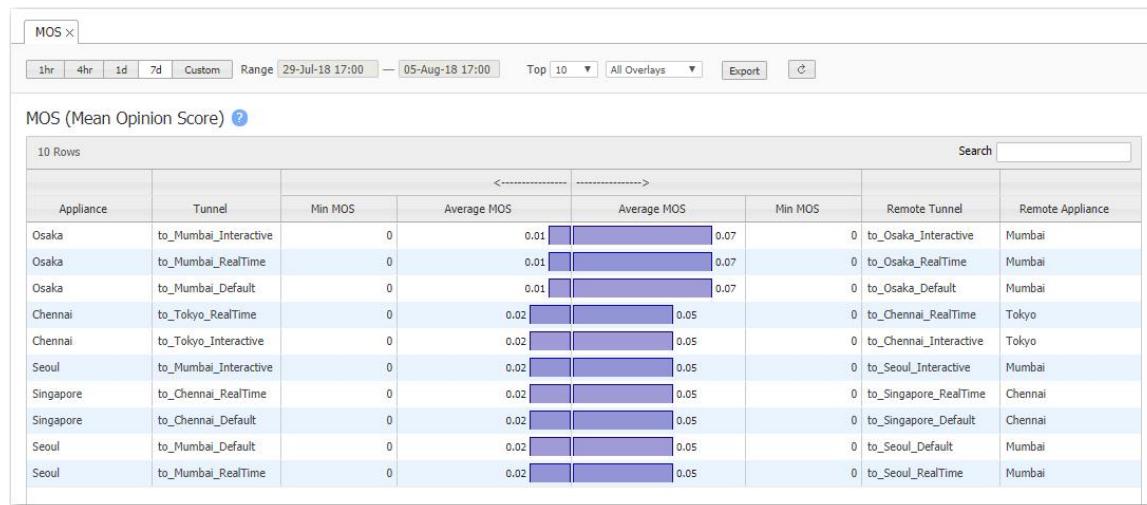


**NOTE** Underlay tunnels are a shared resource among overlays. Therefore, underlay charts display aggregated data.

## Mean Opinion Score (MOS) Summary

*Monitoring > Tunnel Health > MOS > Summary*

The Mean Opinion Score (MOS) is a commonly used measure for video, audio, and audiovisual quality evaluation. Perceived quality is rated on a theoretical scale of 1 to 5; the higher the number, the better the quality.

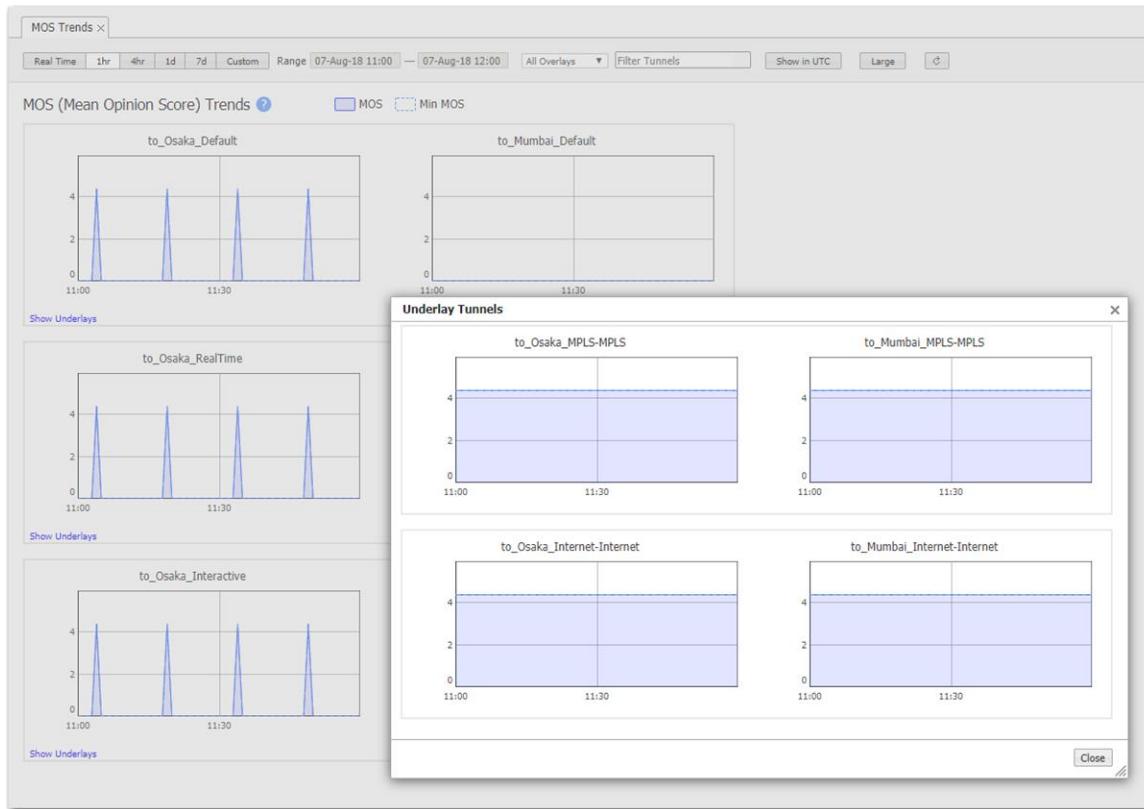


The value can be affected by loss, latency, and jitter. In practice, a value of **4.4** is considered an excellent quality target.

## Mean Opinion Score (MOS) Trends

*Monitoring > Tunnel Health > MOS > Trends*

The Mean Opinion Score (MOS) is a commonly used measure for video, audio, and audiovisual quality evaluation. Perceived quality is rated on a theoretical scale of 1 to 5; the higher the number, the better the quality.



- The value can be affected by loss, latency, and jitter. In practice, a value of **4.4** is considered an excellent quality target.
- The **Min MOS** value reports the worst score within a minute.

## Tunnels Summary

*Monitoring > Tunnel Health > Other Tunnel Statistics > Tunnels Summary*

This tab summarizes tunnel statistics, including reduction, throughput, latency, and packet loss.

Tunnels Summary																															
		Tunnels Summary																													
		Tunnels Summary																													
50 Rows																															
Inbound																															
Tunnel	Status	LAN	WAN	Reduction %	LAN Through...	WAN Through...	LAN +	WAN	Reduction %	LAN Through...	WAN Through...	LAN Through...	Packets Loss %	Jitter (ms)	Latency (ms)																
													Avg	Max	Avg	Max	Avg	Max													
Portland to_Los...	up - active	2.5 MB	12 MB	0.00	0	962 bps	0	7.2 kB	0.00	390 kbps	1.6 Mbps	0	0	72.00	32.00	50.02	0.00														
Portland to_Los...	up - active	190 MB	127 MB	35.96	0	0	0	0	0.00	26 kBps	17 kBps	0	0	72.00	32.00	50.02	0.00														
Portland to_Min...	up - active	0	0	0.00	0	0	0	0	0.00	0	0	0	0	53.00	9.00	99.93	0.00														
Minneapolis to_L...	up - active	0	0	0.00	0	0	0	0	0.00	0	0	0	0	6.00	3.00	49.98	0.00														
Portland to_Oh...	up - active	0	0	0.00	0	0	0	0	0.00	0	0	0	0	38.00	11.00	99.92	0.00														
Los Angeles to_S...	up - active	0	0	0.00	0	0	0	0	0.00	0	0	0	0	5.00	3.00	50.00	0.00														
Portland to_Na...	up - active	0	0	0.00	0	0	0	0	0.00	0	0	0	0	51.00	9.00	99.93	0.00														
Minneapolis to_S...	up - active	0	0	0.00	0	0	0	0	0.00	0	0	0	0	59.00	7.00	99.63	0.00														
Portland to_Los...	up - active	0	0	0.00	0	0	0	0	0.00	0	0	0	0	72.00	32.00	50.02	0.00														
Chicago to_Los...	up - active	0	0	0.00	0	0	0	0	0.00	0	0	0	0	0	7.00	17.00	49.97	0.00													
Portland to_Oh...	up - active	0	5.0 kB	0.00	0	516 bps	0	3.9 kB	0.00	0	671 bps	0	0	38.00	11.00	99.92	0.00														
Minneapolis to_O...	up - active	0	4.8 kB	0.00	0	657 bps	0	4.9 kB	0.00	0	646 bps	0	0	6.00	3.00	49.98	0.00														
Portland to_Mia...	up - active	0	5.7 kB	0.00	0	587 bps	0	4.4 kB	0.00	0	760 bps	0	0	51.00	9.00	99.93	0.00														
Portland to_Min...	up - active	0	5.7 kB	0.00	0	587 bps	0	4.4 kB	0.00	0	760 bps	0	0	53.00	9.00	99.93	0.00														
Portland to_Jos...	up - active	0	5.5 kB	0.00	0	645 bps	0	4.8 kB	0.00	0	735 bps	0	0	72.00	32.00	50.02	0.00														
Chemnitz to_Na...	up - active	0	5.7 kB	0.00	0	704 bps	0	5.3 kB	0.00	0	760 bps	0	0	0.00	1.00	0.00	0.00														
Portland to_Los...	up - active	83 kB	27 kB	0.00	0	681 bps	0	5.1 kB	0.00	1.1 kBps	3.6 bps	0	0	72.00	32.00	50.02	0.00														
Minneapolis to_S...	up - active	0	4.8 kB	0.00	0	458 bps	0	3.4 kB	0.00	0	633 bps	0	0	6.00	3.00	49.98	0.00														
London to_Ohe...	up - active	0	5.7 kB	0.00	0	704 bps	0	5.3 kB	0.00	0	760 bps	0	0	0.00	0.00	0.00	0.00														
Chemnitz to_Na...	up - active	0	5.7 kB	0.00	0	704 bps	0	5.3 kB	0.00	0	760 bps	0	0	0.00	5.00	0.00	0.00														
Portland to_Los...	up - active	0	5.4 kB	0.00	0	669 bps	0	5.0 kB	0.00	0	722 bps	0	0	72.00	32.00	50.02	0.00														
Chicago to_Min...	up - active	0	5.7 kB	0.00	0	645 bps	0	4.8 kB	0.00	0	760 bps	0	0	62.00	6.00	99.82	0.00														

For each Business Intent Overlay, the specified Link Bonding Policy determines the bandwidth efficiency. To guarantee service quality levels, High Availability requires the most overhead and High Efficiency requires the least. The table shows the total bandwidth used. The Payload filter removes overhead from the displayed values.

# Configuration

These topics focus on how to configure Orchestrator. The options available under this menu are organized as follows:

- Overlays & Security
- Networking
- Templates & Policies
- Cloud Services

## Overlays & Security

These topics describe the pages related to deploying a WAN optimization network or a software-defined Wide Area Network (SD-WAN).

From a configuration standpoint, an SD-WAN uses Business Intent Overlays (BIOS), whereas a WANop network does not.

### Business Intent Overlays

*Configuration > Overlays & Security > Business Intent Overlays*

Use the **Business Intent Overlays (BIOS)** tab to create separate, logical networks that are individually customized to your applications and requirements within your network. By default, there are several predefined overlays matching a range of traffic within your network.

The overlay summary table is used for easy comparison of values between your various configured overlays. You can select any link in the table and the **Overlay Configuration** dialog box launches. You can also temporarily save your changes before officially applying those changes to your overlay. The pending configuration updates are indicated by an orange box around the edited item. Click **Save and Apply Changes to Overlays** when you are ready to apply the changes and click **Cancel** if you want to delete the changes.

#### Overview

Orchestrator matches traffic to an ACL, progressing down the ordered priority list of overlays until it identifies the first one that matches. The matched traffic is then analyzed against the overlay's Internet Traffic configuration and forwarded within the fabric, or broken out to the internet based on the preferred policy order. If the software determines that the traffic is not destined for the internet, it refers to the **WAN Links & Bonding Policy** configuration and forwards traffic accordingly within the overlay.

## SD-WAN Traffic to Internal Subnets

### Overlay Configuration

You can begin to configure or modify a default overlay in the **Overlay** column. You can also select any icon on the **Business Intent Overlay** page and the selected editor or dialog box opens.

Complete the following steps to configure your overlay.

1. Select the name of the overlay. The **Overlay Configuration** window opens. If you want to edit the default overlay or create a new overlay, enter the new name of the overlay in the **Name** field.
2. Select the **Match** field and choose the match criteria from the menu.
3. Click the **Edit** icon next to the ACL field. To apply default ACLs or create your own, select **Add Rule** in the **Associate ACL** window.
4. Click **Save**.

### Region

To view your associated region within your overlay, select the **Regions** icon in the **Region** column in the overlay summary table. You can modify, remove, or edit overlay settings for a selected region by expanding the list at the right-top of the **Overlay Configuration** window. For more information about **Regions**, refer to the help on the tab.

### Topology

Select the type of topology you want to apply to your overlay and network. You can choose between the following types of topology:

- **Mesh:** Choose **Mesh** if you want to make a local network.
- **Hub & Spoke:** Hubs are used to build tunnels in Hub & Spoke networks and route traffic between regions. If you choose **Hub & Spoke**, any appliance set as a hub will serve as a hub in any overlay applied to it. Hubs in different regions mesh with each other to support regional routing. To configure hubs, select the **Hubs** link at the top of the page.
- **Regional Mesh and Regional Hub & Spoke:** To streamline the number of tunnels created between groups of appliances that are geographically dispersed, you can assign appliances to **Regions** and select **Regional Mesh** or **Regional Hub & Spoke**.

1. At the top of the page, select **Regions**.
2. You can add and remove a region or view the status of each overlay within a selected region.

## Building SD-WAN Using These Interfaces

You can select which WAN interfaces you want to use for each device to connect to the SD-WAN. First, you assign for your traffic to go to the **Primary** interfaces. If the primary interface is unavailable or not meeting the desired Service Level Objectives configured, the **Backup** interfaces are used. Move the desired interfaces between **Primary** and **Backup**. The interfaces are grayed out until moved into the **Primary** or **Backup** boxes.

- **Cross Connect** allows you to define tunnels built between each interface label. Each appliance has a maximum number of tunnels that it can support, and using **Cross Connect** increases the number of tunnels created.
- **Add Backup if Primary Are:** Specifies when the system should use the Backup interfaces.
- **+Secondary:** Click **+Secondary** to enable secondary interfaces. You can specify when you choose Orchestrator to go to Secondary by selecting **Down** or **Not Meeting Service Levels**.

## Service Level Objective

Traffic is routed through the primary interfaces exclusively unless the service level thresholds for **Loss**, **Latency**, or **Jitter** have been exceeded. If this occurs, backup interfaces are added so that the service level objective can be met.

**NOTE** Primary interfaces can still be used to support the overall Service Level Objective.

## Link Bonding Policy

You can select the following Link Bonding Policies when you need to specify the criteria for selecting the best route possible when data is sent between multiple tunnels and appliances. You can also select custom bonding, which enables you to customize link prioritization and traffic steering policies based on multiple criteria.

Field	Description
<b>High Availability</b>	For critical services that cannot accept any interruption at all. For example, call center voice or critical VDI traffic.
<b>High Quality</b>	For typical real-time services, such as VoIP or video conferencing. For example, WebEx or business-quality Skype, VDI traffic.
<b>High Throughput</b>	For anything where maximum speed is more important than quality. For example, data replication, NFS, file transfers, and so forth.
<b>High Efficiency</b>	For everything else. This option sends load balance information on multiple links, with no FEC or overhead.

Field	Description
<b>Custom</b>	<p>Specify the following:</p> <ul style="list-style-type: none"> <li>• FEC Wait Time (in milliseconds)</li> <li>• Exclude links: Overlay or Underlay brownout</li> <li>• Link Reorder Frequency: Aggressive, Moderate, Conservative</li> <li>• Path Conditioning (in percentage)</li> <li>• Packet Reorder Wait Time (in milliseconds)</li> <li>• Link Selection: Waterfall or Balanced</li> </ul>

## QoS, Security, and Optimization

To further customize your overlay configuration, enter the appropriate information for the following fields.

Field	Description
<b>FW Zone</b>	Select the firewall zone you want to restrict traffic to from an overlay.
<b>Boost</b>	Select <b>True</b> or <b>False</b> if you want to apply any purchased Boost to your overlay.
<b>Peer Unavailable Option</b>	Select the following options you want your traffic to go if a peer is unavailable: <b>Use MPLS</b> , <b>Use Internet</b> , <b>Use LTE</b> , <b>Use Best Route</b> , <b>Drop</b> .
<b>Traffic Class</b>	Channels traffic to the desired queue based on the applied service. Select <b>Best Route</b> or <b>Drop</b> .
<b>LAN DSCP</b>	Select the DSCP you want to apply as a filter to the LAN interface.
<b>WAN DSCP</b>	Select the DSCP you want to apply as a filter to the WAN interface.

## Breakout Traffic to Internet and Cloud Services

You can use the **Breakout Traffic to Internet & Cloud Services** to monitor and manage traffic coming to or from the internet.

### Hub Versus Branch Breakout Settings

You can create different breakout policies for hubs. Any hub you select in the **Topology** section also displays at the top of the **Internet Traffic to Web, Cloud Services** tab. When you select an individual hub, the **Use Branch Settings** displays, selected, to the right of the screen. Complete the following steps to create a custom breakout policy for that hub:

1. Clear the check box for **Use Branch Settings**.
2. Configure the now accessible parameters.
3. Click **OK**.

## Preferred Policy Order and Available Policies

- You can move policies back and forth between the **Preferred Policy Order** and the **Available Policies** columns. You can also change their order within a column. The defaults provided are **Backhaul via Overlay**, **Break Out Locally**, and **Drop**.
- When you choose **Break Out Locally**, confirm that any selected interface that is directly connected to the Internet has **Stateful Firewall** specified in the deployment profile.
- You can add services (such as Zscaler, Fortigate, or Palo Alto). The service requires a corresponding Internet-breakout (Passthrough) tunnel for each appliance traffic to that service. To add a service, select the edit icon next to **Available Policies**.
- The **Default** policy you configure for internet breakout is pushed to all appliances that use the selected Overlay. However, you might want to push different breakout rules to your hubs.

### Break Out Locally Using These Interfaces, Available Interfaces, and Link Selection

You can select the best internet breakout links by specifying the type of **Link Selection: Waterfall** or **Balance**. Drag and drop an available interface into **Primary** or **Backup** in the **Break Out Locally Using These Interfaces** and complete the following steps.

1. Select **Waterfall** or **Balanced** under **Link Selection**.
2. If waterfall is chosen, links are ranked on the selected threshold, from best to worst. The best link is chosen first and the next best link is chosen when the current, best link's bandwidth utilization is full. Select one of the following ways you want Orchestrator to first determine which link to use.

Field	Description
<b>Auto</b>	Default threshold if you do not specify the threshold for your links.
<b>MOS</b>	Measure of the voice connect quality.
<b>Loss</b>	Configured amount of loss the primary link is given.
<b>Latency</b>	Configured amount of time you assign to the primary link for latency.
<b>Fixed Order</b>	Always selects the primary interfaces set by the user. No detection of the best set link.

**NOTE** Backup links are used only when **all** primary links are down.

3. If **Balanced** is chosen, enter the amount for the three Performance Thresholds: **Loss**, **Latency**, and **Jitter**. Traffic is dispersed between one or more of the configured top or equally ranked links.
- WARNING** Random links are selected if no brownout thresholds for Loss, Latency, and Jitter have been set.
4. Click the edit icon next to **Break Out Locally Using** these interfaces and complete the dialog box if you choose to set IP SLA Rule destinations.

**NOTE** You can still enable Path Loading even if you do not select any primary links.

If you select **Exclude links That Are Below Performance Thresholds**, the selected policy order is applied.

## Apply Overlays

*Configuration > Overlays & Security > Apply Overlays*

Use this page to **add or remove overlays** from appliances. If you select **Edit Overlays**, you will be redirected to the **Business Intent Overlay** tab for further customization. You can also view the status of the overlays if you select **View Status**.

## Interface Labels

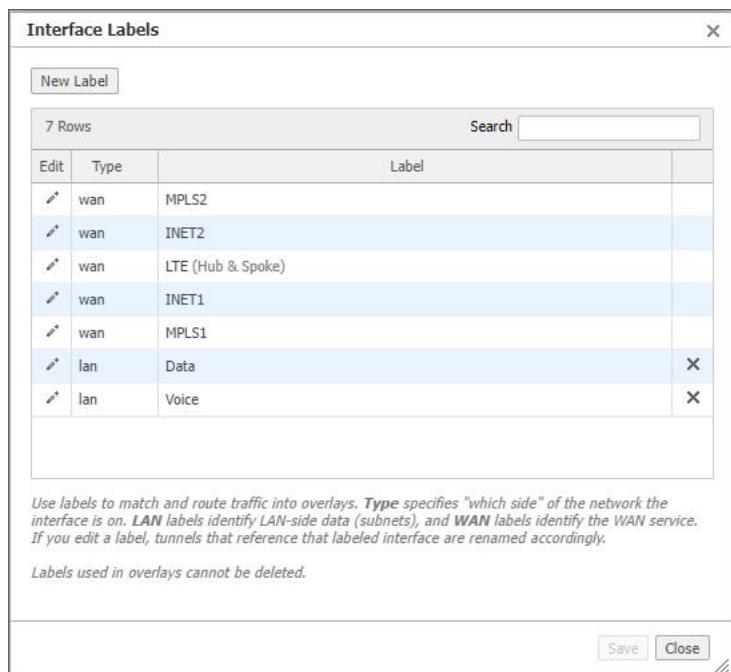
*Configuration > Overlays & Security > Interface Labels*

To make it easier to identify connections, you can create descriptive interface labels for each link type in your environment. Use labels to match and route traffic into overlays. The label type specifies "which side" of the network the interface is on. LAN labels identify LAN-side data (subnets), and WAN labels identify the WAN service, such as MPLS, Internet, or LTE. If you edit a label, tunnels that reference that labeled interface are renamed accordingly.

- LAN labels can be selected for a traffic access policy in a Business Intent Overlay (BIO), which in turn is applied to an appliance with those LAN labels. All traffic matching those interfaces is automatically processed by that BIO. If you use an ACL for a traffic access policy, the LAN label is ignored for that BIO.
- WAN labels are used by Orchestrator and BIOS to determine which interfaces on different appliances should be connected by tunnels built by Orchestrator. Orchestrator automatically pushes interface labels to appliances it manages.

## Manage Labels

Use the Interface Labels dialog box to manage labels in Orchestrator, available under **Configuration > Overlays & Security > Interface Labels**.

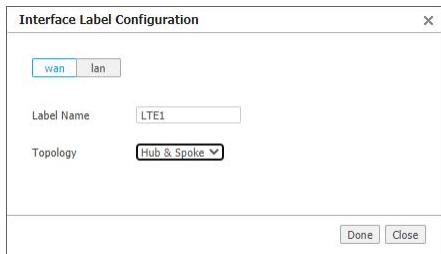


From this dialog box, you can create, edit, or delete labels.

## Create a Label

1. Click **New Label**.

The Interface Label Configuration dialog box opens.



2. Select **wan** or **lan** for the label type.
3. Enter a descriptive name in the **Label Name** field.

**NOTE** For WAN labels, if you want to allow Orchestrator to build tunnels using this label in any topology, leave the Topology selection set to **any**. If you want to override BIO settings and exclude this label in Full Mesh overlays, set Topology to **Hub & Spoke**.

4. Click **Done** to save your changes and close the dialog box. Otherwise, click **Close** to cancel and return to the list of interface labels.

## Edit a Label

1. In the Interface Labels dialog box, click the edit icon to the right of an existing label.
2. Select **wan** or **lan** for the label type—you cannot change the label type if the label is currently in use.
3. If you want to change the label name, modify it in the **Label Name** field.

**NOTE** For WAN labels, if you want to allow Orchestrator to build tunnels using this label in any topology, leave the Topology selection set to **any**. If you want to override BIO settings and exclude this label in Full Mesh overlays, set Topology to **Hub & Spoke**.

4. Click **Done** to save your changes and close the dialog box. Otherwise, click **Close** to cancel and return to the list of interface labels.

## Delete a Label

1. In the Interface Labels dialog box, click the X icon to the left of a label you want to delete.

**NOTE** Labels used in overlays cannot be deleted.

The label is deleted from the list but can be restored by closing the dialog box without saving.

2. To save your changes and permanently delete the label, click **Save**.

**WARNING** When deleting a label, a confirmation message warns you that deleted interface labels will be removed from all policies, interfaces, and deployment profiles that are currently using the label.

3. Click **Save** to confirm the removal. Otherwise, click **Cancel** to return to the Interface Labels dialog box.

## Hubs

### *Configuration > Overlays & Security > Hubs*

On this tab, you can add, remove, and associate hubs to a specified region within the Regional Mesh or Regional Hub-and-Spoke topologies configured on the **Business Intent Overlay** tab.

You can specify whether a hub will re-advertise routes that were previously received from a spoke in the hub's region or a hub in another region.

**NOTE** This feature requires appliance software version 9.1.0 or later.

You can also access the Regions tab and Business Intent Overlay tabs by clicking the links at the top of the page.

Complete the following steps to add a hub:

1. Start typing a name or select the appliance you want make a hub from the list.
2. Select one of the following:
  - **Re-Advertise Routes** - This hub will re-advertise its routes so that other appliances can learn them. This hub will also re-advertise routes learned from other EdgeConnect appliances within its region.
  - **Do Not Re-Advertise Routes (Stub Hub)** - This hub will not re-advertise routes learned from other regions or spokes. All local routes (static, directly connected, BGP, and OSPF) will still be advertised. Hubs that do not re-advertise their routes are stub hubs.
3. Click **Add Hub**.

To delete a hub, select the X icon next to the hub you want to delete.

**NOTE** You must remove all overlays before you can revert a hub back to a spoke.

## Deployment Profiles

*Configuration > Overlays & Security > Deployment Profiles*

Instead of configuring each appliance separately, you can create various **Deployment Profiles** and provision a device by applying the profile you want. For example, you can create a standard format for your branch.

**TIP** For a smoother workflow, complete the DHCP Server Defaults tab (**Configuration > Networking > DHCP Server Defaults**) before creating Deployment Profiles.

You can use Deployment Profiles to simplify provisioning, regardless of whether you choose to create and use **Business Intent Overlays**.

**NOTE** You cannot edit **IP/Mask** fields because they are appliance-specific.

### Map Labels to Interfaces

- On the **LAN** side, labels are optional. They can be used as match criteria for Business Intent Overlay ACLs, such as **data**, **VoIP**, or **replication**.
- On the **WAN** side, labels identify the link type, such as **MPLS** or **Internet**. These labels are mandatory. They are used by Orchestrator to build Business Intent Overlay policies.
- To create or manage a global pool of labels, either:
  - Navigate to **Configuration > Overlays & Security > Deployment Profiles**, click the **Edit** icon next to **Label**, and make the appropriate changes, or

- Navigate to **Configuration > Overlays & Security > Interface Labels**) and make the appropriate changes.
- The change you make to a label propagates automatically. For example, it renames tunnels that use that labeled interface.

## LAN-side Configuration: Segments and Firewall Zones

EdgeConnect Segmentation (VRF) provides orchestrated layer-3 segmentation, Zone Based Firewall, and IDS-end-to-end across the SD-WAN fabric. Segment and zone policies are global in scope. They are managed on the **Configuration > Networking > Routing > Routing Segmentation (VRF)** tab.

Segments and zones are then assigned to LAN-side interfaces for each appliance by using the Deployment dialog box. By default, the Segment and FW Zone fields on LAN interfaces are set to the system-generated Default segment. You can select a different segment and firewall zone from the drop-down lists. These lists reflect the segments and zones that are set up on the Routing Segmentation (VRF) tab.

**NOTE** The segment for WAN interfaces cannot be changed.

## LAN-side Configuration: DHCP

- By default, **each** LAN IP acts as a **DHCP Server** when the appliance is in (the default) Router mode.
- The global defaults are set in **Configuration > Networking > DHCP Server Defaults** and pre-populate this page. The other choices are **No DHCP** and having the appliance act as a **DHCP/BOOTP Relay**.
- Enter the LAN interface from the drop-down. Click **+IP** to add a specific IP address.
- Enter the IP address of the specific LAN interface above the **NO DHCP** link.
- To customize an individual interface on the Deployment Profiles tab, click the DHCP-related link under the IP/Mask field. The DHCP Settings dialog box opens.

The following tables describe the various DHCP settings you can configure.

*DHCP Server*

Field	Description
<b>Subnet Mask</b>	Mask that specifies the default number of IP addresses reserved for any subnet. For example, entering <b>24</b> reserves 256 IP addresses.
<b>Exclude first N addresses</b>	Specifies how many IP addresses are not available at the beginning of the subnet's range.
<b>Exclude last N addresses</b>	Specifies how many IP addresses are not available at the end of the subnet's range.
<b>Default lease, Maximum lease</b>	Specify, in hours, how long an interface can keep a DHCP-assigned IP address.

Field	Description
<b>Default gateway</b>	Indicates whether the default gateway is being used.
<b>DNS server(s)</b>	Specifies the associated Domain Name System servers.
<b>NTP server(s)</b>	Specifies the associated Network Time Protocol servers.
<b>NetBIOS name server(s)</b>	Used for Windows (SMB) type sharing and messaging. It resolves the names when you are mapping a drive or connecting to a printer.
<b>NetBIOS node type</b>	NetBIOS node type of a networked computer relates to how it resolves NetBIOS names to IP addresses. There are four node types: <ul style="list-style-type: none"> <li>• <b>B-node</b> - 0x01 Broadcast</li> <li>• <b>P-node</b> - 0x02 Peer (WINS only)</li> <li>• <b>M-node</b> - 0x04 Mixed (broadcast, then WINS)</li> <li>• <b>H-node</b> - 0x08 Hybrid (WINS, then broadcast)</li> </ul>
<b>DHCP failover</b>	Enables DHCP failover. To set it up, click the <b>Failover Settings</b> link.

#### DHCP/BOOTP Relay

Field	Description
<b>Destination DHCP/BOOTP Server</b>	IP address of the DHCP server assigning the IP addresses. This setting applies to the local interface only.
<b>Enable Option 82</b>	When selected, inserts additional information into the packet header to identify the client's point of attachment. This setting applies to all LAN-side interfaces on this appliance. <b>IMPORTANT:</b> Changing this setting will modify Option 82 settings on all LAN-side interfaces that are enabled as DHCP Relay.
<b>Option 82 Policy</b>	Tells the relay what to do with the hex string it receives. The choices are <b>append</b> , <b>replace</b> , <b>forward</b> , and <b>discard</b> . This setting applies to all LAN-side interfaces on this appliance. <b>IMPORTANT:</b> Changing this setting will modify Option 82 settings on all LAN-side interfaces that are enabled as DHCP Relay.

#### WAN-side Configuration

Select the WAN-side label you want to apply to this deployment. Click the edit icon to add a new interface or delete a previously configured interface.

**Firewall Zone:** Zone-based firewall policies are configured globally on the Orchestrator. A zone is applied to an **Interface**. By default, traffic is allowed between interfaces labeled with the same zone. Any traffic between interfaces with different zones is dropped. You can create exception rules (Security Policies) to allow traffic between interfaces with different zones. The firewall zones you have already configured will be in the list under **FW Zone**. Select the Firewall Zone you want to apply to the WAN you are deploying.

**Firewall Mode:** Four options are available at each WAN interface:

- **Allow All** permits unrestricted communication. Use this option with extreme caution and only if the interface is behind a WAN edge firewall.
- **Stateful only** allows communication from the LAN-side to the WAN-side.  
Use this if the interface is behind a WAN edge router.
- **Stateful with SNAT** applies Source NAT to outgoing traffic.  
Use this if the interface is directly connected to the Internet and you want to enable local internet breakout.
- **Harden**
  - For traffic inbound from the WAN, the appliance accepts **only** IPSec tunnel packets that terminate on an EdgeConnect appliance.
  - For traffic outbound to the WAN, the appliance **only** allows IPSec tunnel packets and management traffic that terminate on an EdgeConnect appliance.

**NAT Settings:** To change the NAT setting, click the NAT-related link under the Next Hop field on the WAN side. The NAT Settings dialog box opens.

Select one of the following options:

- If the appliance is behind a NAT-ed interface, select **NAT**.
- If the appliance is not behind a NAT-ed interface, select **Not behind NAT**.
- Enter an **IP address** to assign a destination IP for tunnels being built from the network to this WAN interface.

**Shaping:** You can limit bandwidth selectively on each WAN interface.

- **Total Outbound** bandwidth is licensed by model. It is the same as max system bandwidth.
- To enter values for shaping inbound traffic (recommended), you must first select **Shape Inbound Traffic**.

**EdgeConnect Licensing:** Only visible on EdgeConnect appliances.

- For additional bandwidth, you can purchase **Plus**, and then select it here for this profile.

- If you have purchased a pool of **Boost** for your network, you can allocate a portion of it in a Deployment Profile. You can also direct allocations to specific types of traffic in the Business Intent Overlays.
- To view how you have distributed **Plus** and **Boost**, navigate to the **Configuration > Overlays & Security > Licensing > Licenses** tab.
- Select the appropriate licensing you have applied to your EdgeConnect appliance from the menu. The licenses will only display depending on the licenses you have for that particular account. You can select the following licensing options:
  - Mini
  - Base
  - Base + Plus
  - 50 Mbps
  - 200 Mbps
  - 500 Mbps
  - 1 Gbps
  - 2 Gbps
  - Unlimited

**NOTE** You must have the correct hardware to support the license selected.

## BONDING

- EdgeConnect supports etherchannel bonding of multiple physical interfaces of the same media type into a single virtual interface. For example, **wan0** plus **wan1** bond to form **bwan0**. This increases throughput on a very high-end appliance and/or provides interface-level redundancy.
- For bonding on a virtual appliance, you would need to configure the host instead of the appliance. For example, on a VMware ESXi host, you would configure NIC teaming to get the equivalent of etherchannel bonding.
- Whether you use a physical or a virtual appliance, etherchannel must also be configured on the directly connected switch/router. Refer to Aruba SD-WAN user documentation.

## A More Comprehensive Guide to Basic Deployments

This section discusses the basics of three deployment modes: **Bridge**, **Router**, and **Server** modes.

It describes common scenarios, considerations when selecting a deployment, redirection concerns, and some adaptations.

For detailed deployment examples, refer to the Aruba EdgeConnect SD-WAN Edge Platform documentation site for various [deployment guides](#).

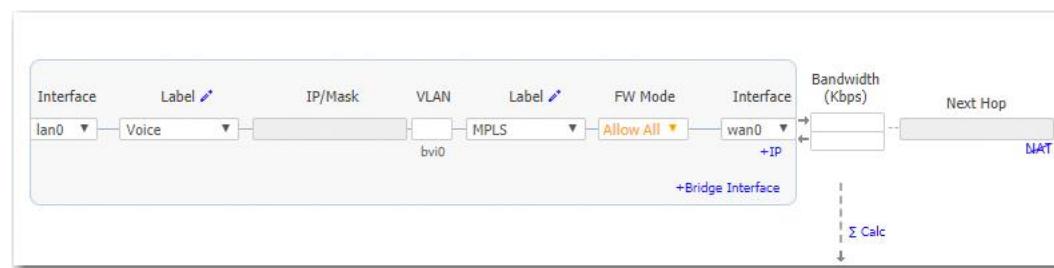
In Bridge Mode and in Router Mode, you can provide security on any WAN-side interface by **hardening the interface**. This means:

- For traffic inbound from the WAN, the appliance accepts **only** IPSec tunnel packets.
- For traffic outbound to the WAN, the appliance **only** allows IPSec tunnel packets and management traffic.

## Bridge Mode

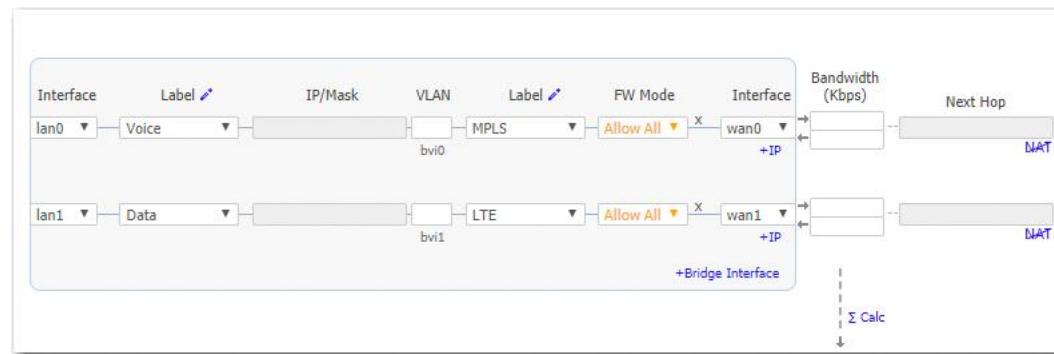
### Single WAN-side Router

In this deployment, the appliance is in-line between a single WAN router and a single LAN-side switch.



### Dual WAN-side Routers

This is the most common 4-port bridge configuration.



- 2 WAN egress routers / 1 or 2 subnets / 1 appliance
- 2 separate service providers or WAN services (MPLS, IPSec VPN, MetroEthernet, and so forth)

### Considerations for Bridge Mode Deployments

- Do you have a physical appliance or a virtual appliance?
- A virtual appliance has no fail-to-wire, so you will need a redundant network path to maintain connectivity if the appliance fails.
- If your LAN destination is behind a router or L3 switch, you need to add a LAN-side route (a LAN next hop).
- If the appliance is on a VLAN trunk, you need to configure VLANs on the EdgeConnect appliance so that the appliance can tag traffic with the appropriate VLAN tag.

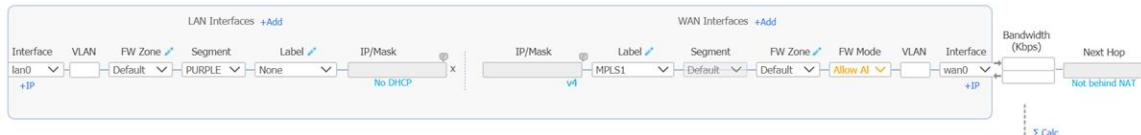
## Router Mode

There are four options to consider:

1. Single LAN interface & single WAN interface
2. Dual LAN interfaces & dual WAN interfaces
3. Single WAN interface sharing LAN and WAN traffic
4. Dual WAN interfaces sharing LAN and WAN traffic

**For best performance, visibility, and control, Options #1 and #2 are recommended because they use separate LAN and WAN interfaces.** And when using NAT, use Options #1 or #2 to ensure that addressing works properly.

### #1 - Single LAN Interface & Single WAN Interface

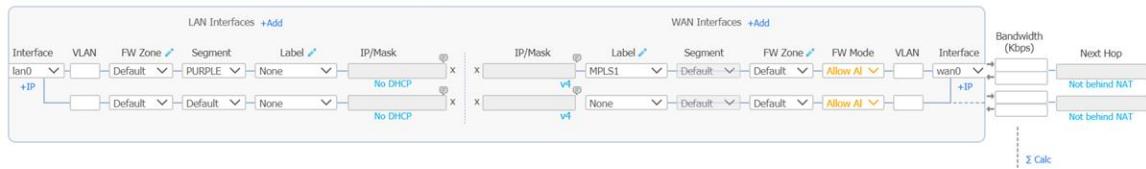


For this deployment, you have two options:

1. You can put EdgeConnect **in-path**. In this case, if there is a failure, you need other redundant paths for high availability.
2. You can put EdgeConnect **out-of-path**. You can redirect LAN-side traffic and WAN-side traffic from a router or L3 switch to the corresponding interface using WCCP or PBR (Policy-Based Routing).

To use this deployment with a single router that has only one interface, you could use multiple VLANs.

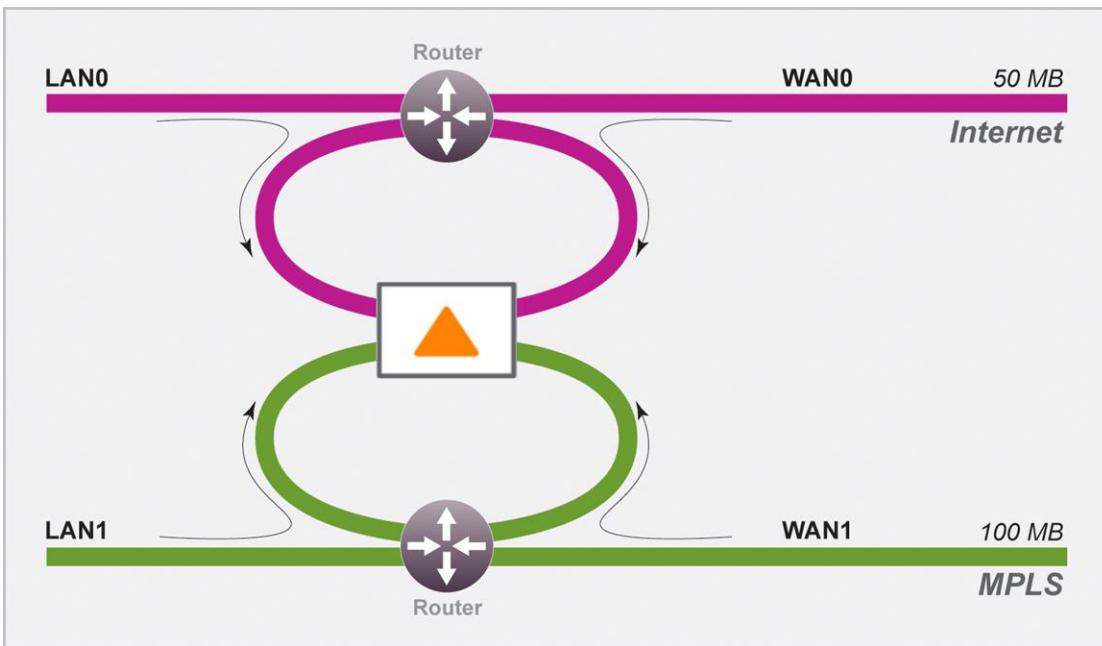
### #2 - Dual LAN Interfaces & Dual WAN Interfaces



This deployment redirects traffic from two LAN interfaces to two WAN interfaces on a single EdgeConnect appliance.

- 2 WAN next-hops / 2 subnets / 1 appliance
- 2 separate service providers or WAN services (MPLS, IPSec VPN, MetroEthernet, and so forth)

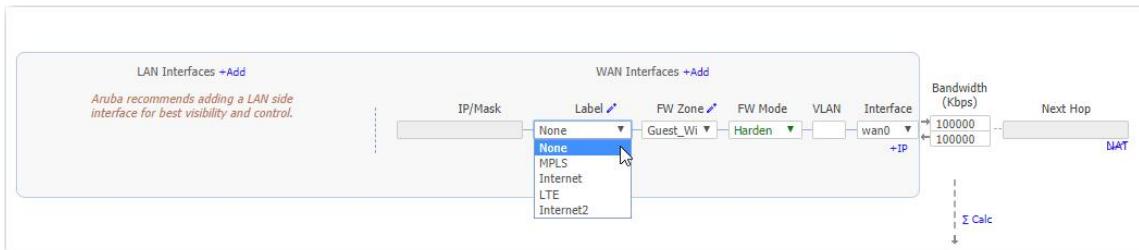
#### Out-of-path dual LAN and dual WAN interfaces



For this deployment, you have two options:

1. You can put EdgeConnect ***in-path***. In this case, if there is a failure, you need other redundant paths for high availability.
2. You can put EdgeConnect ***out-of-path***. You can redirect LAN-side traffic and WAN-side traffic from a router or L3 switch to the corresponding interface using WCCP or PBR (Policy-Based Routing).

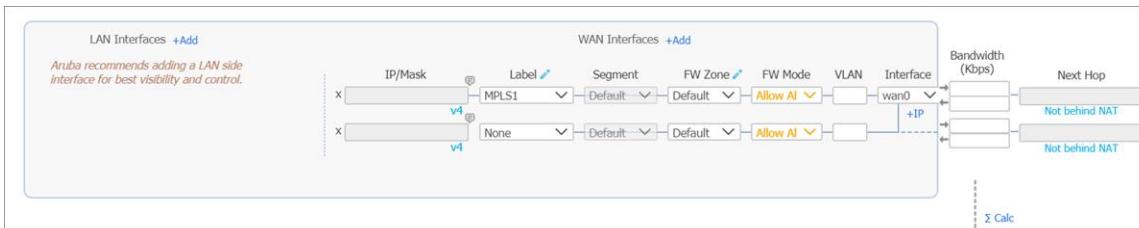
#### #3 - Single WAN Interface Sharing LAN and WAN traffic



This deployment redirects traffic from a single router (or L3 switch) to a single subnet on the EdgeConnect appliance.

- This mode only supports ***out-of-path***.
- When using two EdgeConnects at the same site, this is also the most common deployment for high availability (redundancy) and load balancing.
- For better performance, control, and visibility, Router mode **Option #1** is recommended instead of this option.

#### #4 - Dual WAN Interfaces Sharing LAN and WAN traffic



This deployment redirects traffic from two routers to two interfaces on a single EdgeConnect appliance.

This is also known as **Dual-Homed Router Mode**.

- 2 WAN next-hops / 2 subnets / 1 appliance.
- 2 separate service providers or WAN services (MPLS, IPSec VPN, MetroEthernet, and so forth).
- This mode only supports ***out-of-path***.
- For better performance, control, and visibility, Router mode **Option #2** is recommended instead of this option.

#### Considerations for Router Mode Deployments

- Do you want your traffic to be **in-path** or **out-of-path**? This mode supports both deployments. In-path deployment offers much simpler configuration.

- Does your router support VRRP, WCCP, or PBR? If so, you might want to consider out-of-path Router mode deployment. You can set up more complex configurations, which offer load balancing and high availability.
- Are you planning to use host routes on the server/end station?
- In the rare case when you need to send inbound WAN traffic to a router other than the WAN next hop router, use LAN-side routes.

### Examine the Need for Traffic Redirection

Whenever you place an appliance out-of-path, you must redirect traffic from the client to the appliance.

There are three methods for ***redirecting outbound packets from the client to the appliance*** (known as **LAN-side redirection**, or **outbound redirection**):

- **PBR** (Policy-Based Routing) - Configured on the router. No other special configuration required on the appliance. This is also known as **FBR** (Filter-Based Forwarding).  
If you want to deploy two EdgeConnects at the site for redundancy or load balancing, you also need to use VRRP (Virtual Router Redundancy Protocol).
- **WCCP** (Web Cache Communication Protocol) - Configured on both the router and the EdgeConnect appliance. You can also use WCCP for redundancy and load balancing.
- **Host routing** - The server/end station has a default or subnet-based static route that points to the EdgeConnect appliance as its next hop. Host routing is the preferred method when a virtual appliance is using a single interface, **mgmt0**, for datapath traffic (also known as Server Mode).

To ensure end-to-end connectivity in case of appliance failure, consider using VRRP between the appliance and a router, or the appliance and another redundant EdgeConnect.

How you plan to optimize traffic also affects whether you also need ***inbound redirection from the WAN router*** (known as **WAN-side redirection**):

- If you use **subnet sharing** (which relies on advertising local subnets between EdgeConnect appliances) or **route policies** (which specify destination IP addresses), you only need LAN-side redirection.
- If, instead, you rely on **TCP-based** or **IP-based** auto-optimization (which relies on initial handshaking **outside** a tunnel), you must also set up inbound *and* outbound redirection on the WAN router.
- For TCP flows to be optimized, both directions must travel through the same client and server appliances. If the TCP flows are asymmetric, you need to configure flow redirection among local appliances.

A tunnel must exist before auto-optimization can proceed. There are three options for tunnel creation:

- If you enable **auto-tunnel**, the initial **TCP-based** or **IP-based** handshaking creates the tunnel. This means that the appropriate LAN-side and WAN-side redirection must be in place.

- You can allow the *Initial Configuration Wizard* to create the tunnel to the remote appliance.
- You can create a tunnel manually on the **Configuration > Networking > Tunnels > Tunnels** page.

## Server Mode

This mode uses the **mgmt0** interface for management and datapath traffic.



## ADD DATA INTERFACES

- You can create additional data-plane Layer 3 interfaces to use as tunnel endpoints.
- To add a new logical interface, click **+IP**.

## Deployment - EdgeConnect HA

The EdgeConnect High Availability (HA) mode is a high availability cluster configuration that provides appliance redundancy by pairing two EdgeConnect devices together.

When a deployment profile configures two EdgeConnect appliances in EdgeConnect HA mode, the resilient cluster acts as a single logical system. It extends the robust SD-WAN multipathing capabilities such as Business Intent Overlays seamlessly across the two devices as if they were one entity.

With EdgeConnect HA mode, a WAN uplink is physically plugged into a single one of the EdgeConnect appliances but is available to both in the cluster. For WAN connections that perform NAT (for example, a consumer-grade Broadband Internet connection), it means that only a single Public IP needs to be provisioned in order for both EdgeConnect devices in the EdgeConnect HA cluster to be able to build Business Intent Overlays using that transport resource.

## Enable EdgeConnect HA Mode

1. In the appliance tree, select the appliance, and then right-click to select **Deployment** from the contextual menu. The appliance's Deployment page appears.
2. Select the **EdgeConnect HA** check box.
3. Configure the interfaces (LAN and WAN-side) on both EdgeConnect devices to reflect the WAN connections that are plugged into each one of the respective appliances.

**NOTE** Both EdgeConnect devices will be able to leverage all WAN connections regardless of which chassis they are physically plugged into. It is, however, important to match the deployment profile interface configuration to the actual chassis the WAN connection is physically, directly connected to.

4. Select the physical ports on the respective EdgeConnect appliances that you will connect to each other using an Ethernet cable (RJ-45 twisted pair or SR optical fiber).

**NOTE** You can choose any LAN or WAN port combination for this HA Link that is available on the respective EdgeConnect chassis. You must match the media type and speed for both ends of the HA link. (For example, 1 Gigabit-Ethernet RJ-45 to RJ-45 or 10 Gigabit-Ethernet multimode fiber LC-connector-to-LC-connector). Also, note that you cannot use MGMT ports for the HA Link; only LAN or WAN ports.

## IPSec over UDP Tunnel Configuration

For both EdgeConnect appliances in a high availability cluster to be able to share a common transport connection, you must set the tunnel type to IPSec over UDP mode.

See Tunnel Settings in the Orchestrator (**Orchestrator > Orchestrator Server > Tools > Tunnel Settings**).

**NOTE** *If you are deploying a network with EdgeConnect appliances running VXOA 8.1.6 or higher and Orchestrator 8.2 or higher, the tunnel type is already set to IPSec over UDP mode by default.*

## VRRP Configuration

Typically, in a branch site deployment, you will choose to configure the cluster with a VRRP protocol and assign a VIP (virtual IP) address to the cluster.

- Set the VRRP priority of the preferred LAN-side Primary EdgeConnect to **128**.
- Set the other, Secondary appliance's VRRP priority to **127**.

## LAN-side Monitoring

The IP SLA feature should be configured to monitor the LAN-side VRRP state in order to automatically disable subnet sharing from that appliance in the case of a LAN link failure.

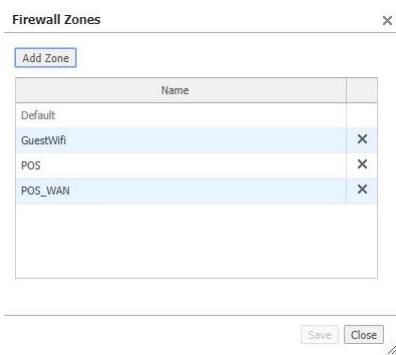
For more information, refer to the IP SLA configuration guide.

## Firewall Zones

*Configuration > Overlays & Security > Security > Firewall Zones*

Zone-based firewalls are created on the Orchestrator.

- A zone is applied to an **Interface**.
- By default, traffic is allowed between interfaces labeled with the same zone.
- Any traffic between interfaces with different zones is dropped.
- Users can create exception rules (Security Policies) to allow or deny traffic between interfaces within the same or different zones.



**NOTE** "Default" will always be the initial default zone. You cannot have another zone named "Default".

**NOTE** The name of your firewall cannot exceed 16 characters and cannot contain any special characters. It can contain alphanumeric characters and underscores only.

## Firewall Protection Profiles

*Configuration > Overlays & Security > Security > Firewall Protection Profiles*

Use the Firewall Protection Profiles tab to add or modify a protection profile on any appliance with a firewall.

### Create a Firewall Protection Profile

1. Select an appliance or group of appliances from the list on the right-side menu.
2. Navigate to **Configuration > Overlays & Security > Security > Firewall Protection Profiles**.

Firewall Protection Profiles <a href="#">?</a>																
3 Rows																
Edit	Appliance ...	Profile Na...	Enabled...	Enforce ...	Discard ...	Allow As...	Enforce ...	Enforce ...	Rapid a...	Block D...	Embryo...	Allowlist	Blocklist	Threshol...	Segm...	Zone
			Yes	true	true	false	true	true	20	900	30			4	Default	Default
			Yes	true	true	false	true	true	20	900	30			4	Default	Default
			Yes	true	true	false	true	true	20	900	30			4	Guest	GUEST

3. Click the edit icon next to the appliance you want to configure a profile for.

The Firewall Protection Profiles - <Appliance Name> dialog box opens.

**Firewall Protection Profiles** - [\[Cancel\]](#) [\[Save\]](#)

Firewall Protection Profiles

Edit	Profile Name	Enabled...	Enforce Str...	Discard No...	Allow Asy...	Enforce I...	Enforce ...	Allowlist	Blocklist	Threshol...	Comment
	Default	Yes	false	true	false	true	true	SEWAN-Loopbac...		4	Default profile for syst...
	Guest	Yes	true	true	false	true	true	SEWAN-Loopbac...		3	Strict profile for Guest...
	Untrusted	Yes	false	true	false	true	true			4	Mapped to UNTRUSTED...
	Trusted	Yes	false	true	false	true	true			4	Mapped to TRUSTED ...

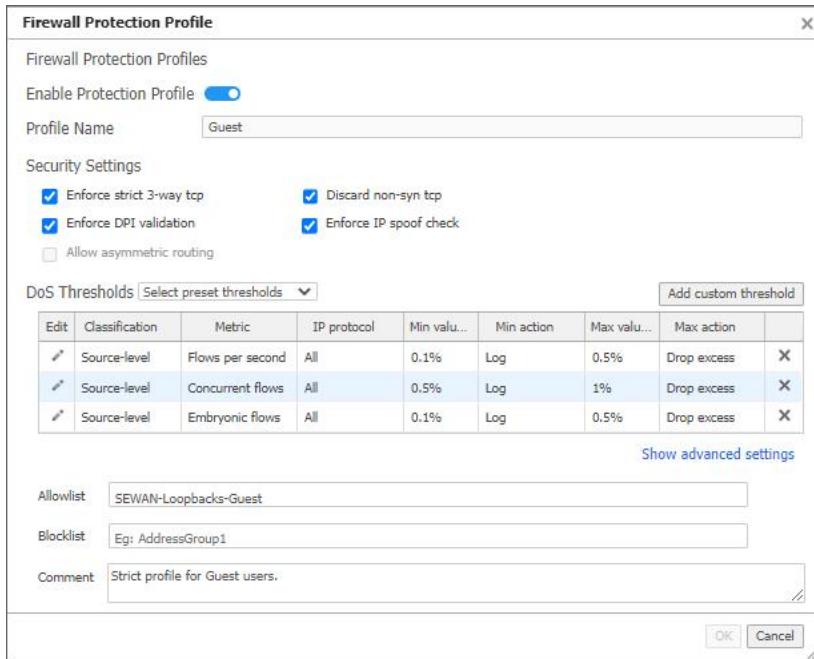
Profile Mappings

Segment	Zone	Profile Name	X
Default	Default	Default	
Default	SOHO	Trusted	
Default	TRUSTED	Trusted	
Default	UNTRUSTED	Untrusted	
Default	MGMT	Trusted	
GuestWiFi	UNTRUSTED	Untrusted	

[Save](#) [Cancel](#)

4. Under the Firewall Protection Profiles header, click **Add**.

The Firewall Protection Profile dialog box opens.



5. Enter a name for the profile.
6. Select or clear any of the Security Settings check boxes.

**NOTE** When asymmetric routing is configured, strict three-way TCP enforcement and deep packet inspection (DPI) validation cannot be performed. To enable these settings, turn off asymmetric routing.

7. In the DoS Thresholds field, select a preset threshold (Lenient, Moderate, or Strict). To further edit a preset threshold, click the edit icon next to the classification you want to edit.

Alternatively, click **Add custom threshold** to define specific threshold values. For more information, see [Set Firewall Protection Profile Thresholds on the next page](#).

8. *(Optional)* Add exceptions to the Allowlist or Blocklist fields.
9. *(Optional)* Click **Show advanced settings** and set the following fields:

Field	Description
<b>Rapid aging</b>	Set a threshold value (in seconds) to enforce the tearing down of TCP connections when the period of inactivity matches the configured value (for example, 30s).
<b>Block duration</b>	Enforce dynamic blocking of flows originating from a source for a specified duration (for example, 300s).
<b>Embryonic timeout</b>	Set this value so that the firewall can tear down half-open TCP connections when the timeout value is reached (for example, 30s). While TCP connection goes through the three-way handshake (SYN, ACK, SYN-ACK), an embryonic connection is a half-open connection that produces (for example) a SYN without the other two parts of the handshake. This is a popular form of denial of service (DoS) attack.

10. Click **OK**.

## Add Profile Mappings

After you create a profile, you can map it to a segment and zone of your firewall to achieve the expected behavior.

To map a profile to a segment:

1. Click **Add** under the Profile Mappings header.
2. Click the box under the Segment field and start typing the segment you want to map to your profile, then click the segment.
3. Click the box under the Zone field and start typing the zone you want to assign to your profile, then click the zone.
4. Click the box under the Profile Name field and select the profile you created earlier.
5. Click **Save**.

## Add Firewall Protection Profile to a Template Group

1. On the Firewall Protection Profiles tab, click **Manage Firewall Protection Profiles with Templates**.
2. Select a template group to add the firewall protection profile to, and then click **Add/Edit**.

Firewall Protection Profile appears as a template under Active Templates > Policies.

Segment	Zone	Profile Name
No Data Available		

## Set Firewall Protection Profile Thresholds

To view the threshold settings on an existing firewall protection profile, click the link in the Thresholds Count column of the Firewall Protection Profiles table.

To change the threshold settings:

1. Click the edit icon next to the appliance you want to configure.

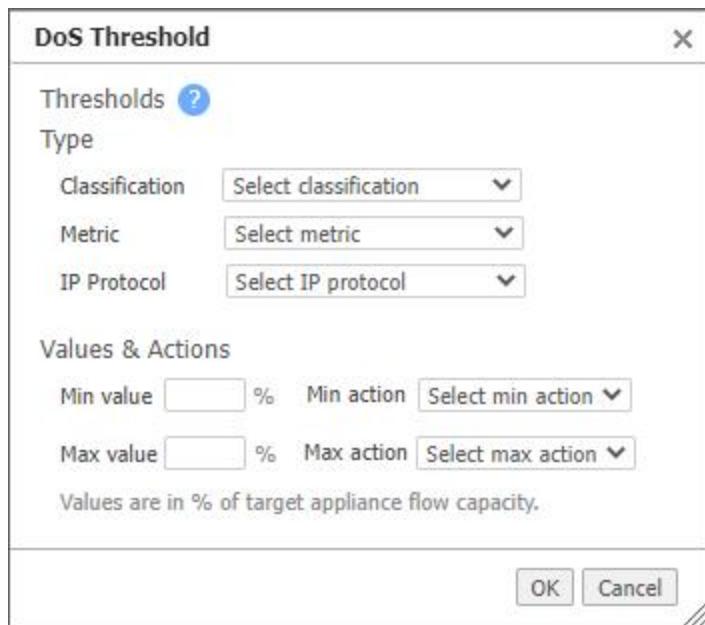
The Firewall Protection Profiles - <Appliance Name> dialog box opens.

2. Click the edit icon next to the profile name whose threshold you want to edit.

The Firewall Protection Profile dialog box opens.

3. Either select a preset threshold from the DoS Thresholds drop-down list, or click **Add custom threshold**.

The DoS Threshold dialog box opens.



4. Set the following parameters:

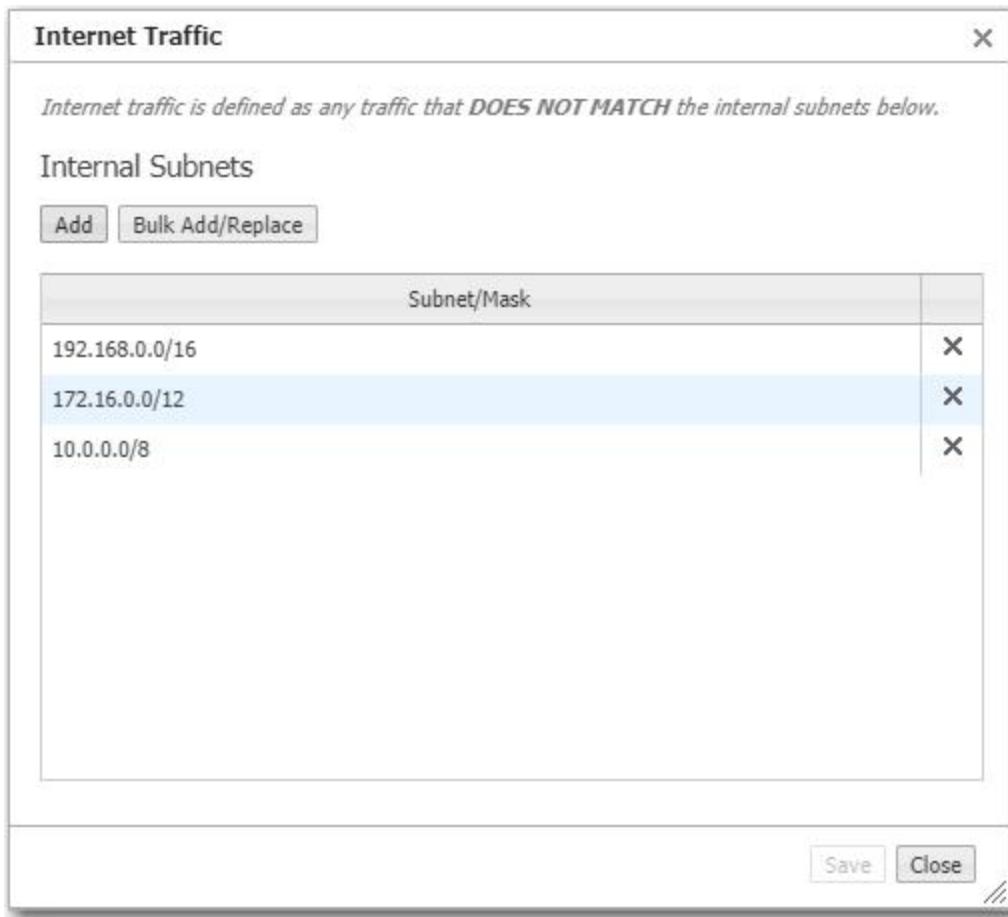
Field	Description
<b>Classification</b>	Classify flows in two ways: <ul style="list-style-type: none"> <li><b>Zone level:</b> Flows originating from multiple endpoints that are part of a single firewall zone.</li> <li><b>Source level:</b> All flows originating from a single endpoint or source device.</li> </ul>
<b>Metric</b>	DoS thresholds can be configured with any or all of the three metrics available in a firewall protection profile: <ul style="list-style-type: none"> <li><b>Flows per second:</b> Rate of flow (fps). A single flow is a unidirectional set of packets containing common attributes (source and destination IP, ports, protocols).</li> <li><b>Concurrent Flows:</b> Number of flows that are active at a given point in time.</li> <li><b>Embryonic Flows:</b> A half-open connection. While TCP connection goes through the three-way handshake (SYN, ACK, SYN-ACK), an embryonic connection is a half-open connection that produces (for example) a SYN without the other two parts of the handshake.</li> </ul>
<b>IP Protocol</b>	Select an IP protocol ( <b>TCP</b> , <b>UDP</b> , <b>ICMP</b> , <b>Others</b> , or <b>All</b> ) for use in threshold settings.
<b>Min value</b>	Minimum threshold value. When this value is breached, the protection profile takes a corresponding minimum action ( <b>Log</b> , <b>Rapid aging</b> , <b>Drop excess</b> , or <b>Block source</b> ).
<b>Max value</b>	Maximum threshold value. When this value is breached, the protection profile takes a corresponding maximum action ( <b>Log</b> , <b>Rapid aging</b> , <b>Drop excess</b> , or <b>Block source</b> ).

5. Click **OK**.

## Internet Traffic

*Configuration > Overlays & Security > Internet Traffic Definition*

Internet traffic is any traffic that **does NOT match** the internal subnets listed in this dialog box.



## IPSec Pre-Shared Key Rotation

*Configuration > Overlays & Security > Security > IPSec Key Rotation*

Use this dialog box to schedule the rotation of auto-generated IPSec pre-shared keys.

### Failure Handling and Orchestrator Reachability

Orchestrator distributes key material to all EdgeConnect appliances in the network. Immediately before the end of a key rotation interval, Orchestrator activates new ephemeral key material for all of the EdgeConnect appliances in the SD-WAN network. For key activation, all the appliances should be reachable to Orchestrator. However, there are two cases of unreachability:

1. **Inactive appliances:** When appliances are inactive, they exist in the Orchestrator, but do not have tunnels configured to any active appliances.
2. **Temporary unreachability:** Temporary unreachability issues occur in cases where an EdgeConnect appliance reboots or if there is a link or communication failure. In this case, Orchestrator will not

activate the new key material until all active appliances are reachable and have received the new key material or if the maximum activation wait time has been exceeded. If the appliance is unreachable for a period longer than the key rotation interval, it will be treated as an inactive appliance.

**Re-authorization:** Inactive appliances that become active at a later point in time will be authorized to receive the current key material. Only then will they be able to download configurations and build tunnels.

## Schedule IPSec Key Rotation Dialog Box

The Schedule IPSec Key Rotation dialog box enables you to schedule your key rotation. The following tables provide details about the two sections in this dialog box.

### *SD-WAN IPSec UDP Key Material Rotation*

Field	Description
<b>Enable Key Rotation</b>	Select this check box to enable key rotation.
<b>Persist Key Material</b>	If enabled, key material is stored on each appliance, ensuring data plane tunnels are built quickly after an appliance reboot (no dependency on Orchestrator). If disabled, new key material from Orchestrator is required after any reboot (Orchestrator reachability is critical).
<b>Max Activation Wait</b>	Maximum time (in hours) Orchestrator must wait before activating the new key material. This wait time applies only when unreachable appliances exist in the network <i>and</i> at least one tunnel is UP from a reachable appliance to an unreachable appliance. This gives you time to fix connectivity issues. After the wait time expires, Orchestrator activates the new key material on all reachable appliances. Generally, it is recommended to set this wait time to half of the rotation period.
<b>Rotation Period</b>	Click the edit icon to set the rotation and the time you want the key material rotation to begin. Click <b>Force Rotate</b> to immediately start a new key material rotation.
<b>Key Material Lifetime</b>	Amount of time a key material lasts. <b>CAUTION</b> The lifetime must be at least three times the amount of the set Rotation Period.

### *SD-WAN IPSec Pre-shared Key Rotation*

Field	Description
<b>Enable</b>	Select this check box to enable.
<b>Period</b>	Click the edit icon to set the time when you want the key rotation to begin.

## Intrusion Detection/Prevention System (IDS/IPS)

*Configuration > Overlays & Security > Security > Intrusion Detection/Prevention System (IDS/IPS)*

The Intrusion Detection/Prevention System (IDS/IPS) can monitor traffic for potential threats and malicious activity and generates threat events based on preconfigured rules. Packets are copied and inspected against signatures downloaded to Orchestrator from Cloud Portal. Orchestrator sends appliances the signature file and any rules that have been added to the allow list. The IDS designates traffic for inspection using matching rules enabled in the zone-based firewall. The IPS protects traffic by matching a signature and then performing a configured action (alert, block, or allow).

Use the Intrusion Detection/Prevention System tab to view status or modify the IDS/IPS configuration for appliances selected in the appliance tree. The following information is displayed for selected appliances:

Field	Description
<b>Appliance</b>	Name of the appliance.
<b>Status</b>	Indicates whether IDS/IPS is enabled on the selected appliance.
<b>IDS/IPS State</b>	Indicates the state of IDS/IPS on the EdgeConnect device.
<b>Eligible</b>	Indicates whether the device is eligible to enable IDS/IPS. For more information, see <a href="#">Prerequisites on the next page</a> .
<b>Licensed</b>	Indicates whether the device is licensed to run IDS/IPS.
<b>Signature Version</b>	Identifies the signature ID running IDS/IPS.
<b>Inspected pkts/sec (last 5 min)</b>	Number of packets inspected in the previous five minutes.
<b>Threats detected (last 5 min)</b>	Number of threats detected in the previous five minutes.
<b>IPS Flow Drops (Cumulative)</b>	Number of dropped flows since IPS has been running. The flow drop count is cumulative and is added to the previous flow drop count.
<b>Events</b>	Click the info icon to see the most recent IDS/IPS events on the selected appliance.
<b>Stats</b>	Click the stats icon to see the following IDS/IPS statistics for the selected appliance: Packets per second sent to the IDS/IPS, IPS Flow Drops (Cumulative), Threats Detected, and Bits per second sent to the IDS/IPS.

Intrusion Detection/Prevention System <a href="#">?</a>										
<input type="button" value="Apply IDS/IPS on Appliances"/> <input type="button" value="IDS/IPS Signatures"/> <input type="button" value="Update Signatures"/> <input type="button" value="43 mins"/>										
3 Rows, 1 Selected										
Appliance	Status	IDS/IPS State	Eligible	Licensed	Signature...	Inspected p...	Threats de...	IPS Flow Drops (Cumulative)	Events	Stats
Protecting	IPS Enabled	Yes	Yes	10015	64	0	0	0	<a href="#">i</a>	<a href="#">n/a</a>
Protecting ...	IPS Enabled	Yes	Yes	10015	437	43	766	766	<a href="#">i</a>	<a href="#">n/a</a>
Protecting ...	IPS Enabled	Yes	Yes	10015	1,382	145	1,436	1,436	<a href="#">i</a>	<a href="#">n/a</a>

## Prerequisites

Note the following requirements about using IDS/IPS:

- IDS/IPS can be enabled only on appliances with a minimum of four cores and 16 GB of RAM.
- IDS/IPS can be enabled only on appliances running ECOS 9.1.0.0 or later. Appliances running an earlier version of ECOS will not be displayed on the Intrusion Detection/Prevention System tab.
- IDS/IPS is a licensed feature and can be enabled only on appliances that have been assigned the Advanced Security license (see help text on the **Configuration > Overlays & Security > Licensing > Licenses** tab).

**NOTE** IDS/IPS alarms are logged in standard syslog format. You can configure a logging facility for IDS and remote log receiver to send logs to a third party for additional review and analytics (see [Advanced Reporting and Analytics](#) on page 147 below).

## Apply IDS/IPS on Appliances

1. To turn on or turn off IDS/IPS on the appliances displayed in the table, click **Apply IDS/IPS on Appliances**.

The Apply IDS/IPS dialog box opens.

2. Apply or remove IDS/IPS:

- To turn off IDS and IPS for all appliances, select **Off**.
- To enable IDS on the appliances, select **IDS Only**.
- To enable IPS on the appliances, select **IPS-Performant**.

The proposed change in state, if any, is displayed for each appliance in the IDS/IPS State column.

3. To apply your changes, click **Save**. Or, to close the dialog box without making any changes, click **Cancel**.

## Associate Actions with IPS Signatures

By default, all rules included in the IDS/IPS Signatures list are enabled on all appliances where IPS is enabled, and the default action is to drop traffic when a rule is triggered. However, for certain traffic or in some specific cases, you might want to specify different actions the IPS takes.

1. To manage IPS rules and actions, click **IDS/IPS Signatures**.

The IDS/IPS Signatures dialog box opens.

**Allow IDS Rules**

Search Rules  By Name, Description, ID

Show Allowed Rules

22513 Rows, 1 Selected

ID	Name ▲	Description	Class Type	Severity	Action
2846003	Android/Hiddad.KN Che...		command-and-control	Major	<input checked="" type="checkbox"/>
2807017	Backdoor.Win32.GF.13...		command-and-control	NA	<input type="checkbox"/>
2018395	Possible Kelihos.F EXE ...		trojan-activity	NA	<input type="checkbox"/>
2812180	Win32/Adware.Convert...		pup-activity	NA	<input type="checkbox"/>
2017249	%Hex Encoded Applet ...		exploit-kit	NA	<input type="checkbox"/>
2014906	.exe File requested ove...		policy-violation	NA	<input checked="" type="checkbox"/>
2020573	.exe download with no ...		bad-unknown	NA	<input type="checkbox"/>
2015674	3XX redirect to data URL		misc-activity	NA	<input type="checkbox"/>
2024930	401TRG Generic Webs...	Alerts on generic web...	web-application-attack	Major	<input type="checkbox"/>
2031318	401TRG Liferay RCE (C...		attempted-admin	Major	<input type="checkbox"/>
2024977	401TRG Perl DDoS IRC...	Alerts on successful w...	trojan-activity	Major	<input type="checkbox"/>
2024942	401TRG Successful Mul...	Emerging Threats phi...	credential-theft	Critical	<input type="checkbox"/>
2842536	404 / Snake Keylogger ...	This will alert on 404K...	trojan-activity	Major	<input type="checkbox"/>

Save Cancel

2. Use the search field at the top of the table to filter the list of rules. You can use the filters below the search bar to view rules by class, severity, or action.
3. Use the drop-down menu in the Action column to set the response for a rule:
  - **Drop:** Drop the traffic when a matching signature condition exists for the source, destination, or both.
  - **Inspect:** Continue the traffic flow to the destination, but inspect the traffic for any anomalies.
  - **Allow:** Pass the traffic from the source.

**NOTE** Reset, quarantine, and packet logging actions will be available in a future release, but are not currently available.
4. To apply your changes, click **Save**. Or, to close the dialog box without making any changes, click **Cancel**.

## Specify Traffic to Be Inspected

You can specify the traffic to be inspected according to source and destination zone, as well as specify detailed match criteria, using Firewall Zone Security Policies (**Configuration > Overlays & Security > Security > Firewall Zone Security Policies**).

From Zone Default to Zone UNTRUSTED			
Source Segment	Denso	Destination Segment	Default
<input type="button" value="Add Rule"/> 2 Rows, 1 Selected			
Priority ▲	Match Criteria	Action	Enabled
20000	Match Everything	<input type="button" value="allow"/> <input type="button" value="allow"/> <input type="button" value="deny"/> <b>inspect</b>	<input checked="" type="checkbox"/>
65535	Match Everything		<input checked="" type="checkbox"/>

With the addition of IDS, firewall actions have the following meanings:

- **allow:** Allow traffic and do not inspect.
- **deny:** Deny traffic and do not inspect.
- **inspect:** Allow traffic and inspect.

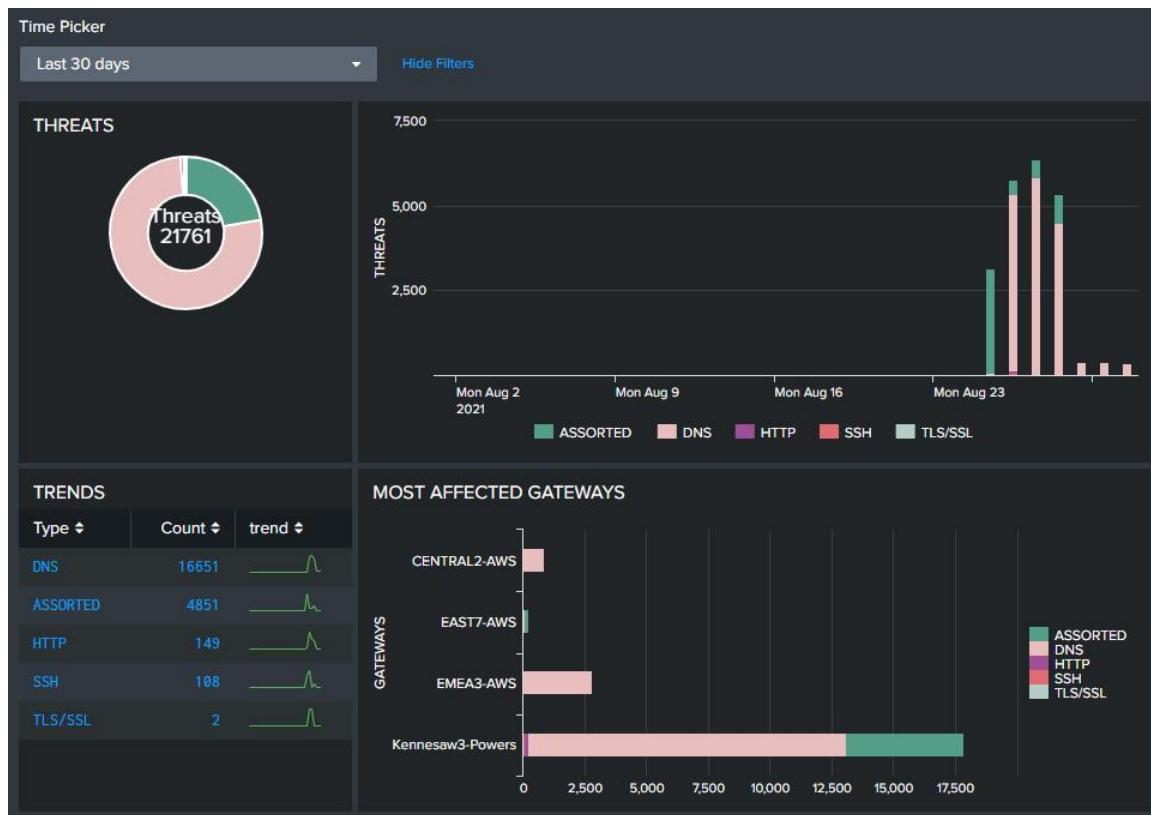
**NOTE** No traffic will be inspected until rules with the inspect action are specified in the security policy.

For more information, see the following tabs in Orchestrator:

- **Templates (Security Policies):** Configuration > Templates & Policies > Templates
- **Routing Segmentation:** Configuration > Networking > Routing > Routing Segmentation (VRF)

## Advanced Reporting and Analytics

For users who are using or trying Splunk, you can install the Aruba EdgeConnect Security App for Splunk application to enable advanced reporting and analytics using the IDS alarms forwarded from EdgeConnect appliances. Search Splunkbase for "EdgeConnect" or click [this link](#) to search in your browser.



Follow the instructions provided to install and configure the application.

## SSL Certificates Tab

*Configuration > Overlays & Security > SSL > SSL Certificates*

EdgeConnect provides deduplication for Secure Socket Layer (SSL) encrypted WAN traffic by supporting the use of SSL certificates and other keys.

The SSL Certificates tab summarizes the SSL certificates installed on appliances for **decrypting non-SaaS traffic**.

- EdgeConnect decrypts SSL data using the configured certificates and keys, optimizes the data, and transmits data over an IPSec tunnel. The peer EdgeConnect appliance uses configured SSL certificates to re-encrypt data before transmitting.
- Peers that exchange and optimize SSL traffic must use the same certificate and key.
- For the SSL certificates to function, the following must also be true:
  - The tunnels are in **IPSec** or **IPSec UDP** mode for both directions of traffic.
  - In the Optimization Policy, **TCP acceleration** and **SSL acceleration** are enabled.

**TIP** For a historical matrix of EdgeConnect and Orchestrator security algorithms, click [here](#).

## SSL CA Certificates Tab

*Configuration > Overlays & Security > SSL > SSL CA Certificates*

This tab lists any installed **Certificate Authorities (CA)** that the browser uses to validate up the chain to the root CA.

If the enterprise certificate that you used for signing substitute certificates is subordinate to higher level **Certificate Authorities (CA)**, you must add those CA certificates. If the browser cannot validate up the chain to the root CA, it will warn you that it cannot trust the certificate.

**TIP** For a historical matrix of EdgeConnect and Orchestrator security algorithms, click [here](#).

## SSL for SaaS Tab

*Configuration > Overlays & Security > SSL > SSL for SaaS*

This tab lists the signed substitute certificates for the appliances.

To fully compress SSL traffic for a SaaS service, the appliance must decrypt it and then re-encrypt it.

To do so, the appliance generates a substitute certificate that must then be signed by a Certificate Authority (CA). There are two possible signers:

For a **Built-In CA Certificate**, the signing authority is Silver Peak.

- The appliance generates it locally, and each certificate is unique. This is an ideal option for Proof of Concept (POC) and when compliance is not a big concern.
- To avoid browser warnings, follow up by importing the certificate into the browser from the client-side appliance.

For a **Custom CA Certificate**, the signing authority is the Enterprise CA.

- If you already have a subordinate CA certificate (for example, an SSL proxy), you can upload it to Orchestrator and push it out to the appliances. If you need a copy of it later, just download it from [here](#).
- If this substitute certificate is subordinate to a root CA certificate, also install the higher-level **SSL CA certificates** (into the **SSL CA Certificates** template) so that the browser can validate up the chain to the root CA.

- If you do not already have a subordinate CA certificate, you can access any appliance's Configuration > Templates & Policies > Applications & SaaS > SaaS Optimization page and generate a Certificate Signing Request (CSR).

**TIP** For a historical matrix of EdgeConnect and Orchestrator security algorithms, click [here](#).

## Discovered Appliances

*Configuration > Overlays & Security > Discovery > Discovered Appliances*

This tab lists each appliance that Orchestrator discovers.

Discovered Appliances												
Discovery Email Recipients [redacted] Save												
Show Denied Devices												
Search												
Serial Number	Appliance	IP Address	Public IP Address	Location	Tag	Discovered Time	Reachability	Approve	Deny	Software Version	Model	
00188C1C07CBA	DFW-[redacted]	[redacted]	[redacted]	Irving, Texas, US	[redacted]	22-Jun-22 09:48	Reachable	Approve	Deny	9.1.1.3_91743	EC-XS	
00188C123690	Colorado-[redacted]	[redacted]	[redacted]	Greenwood Village, CO	Unassigned	22-Jun-22 09:48	Unreachable	Approve	Deny	9.2.0.0_93600	EC-XS	
00188C1F1746	Aberdeen-[redacted]	[redacted]	[redacted]	Middletown, New Jersey	Aberdeen-[redacted]	22-Jun-22 09:43	Unreachable	Approve	Deny	9.1.1.3_91743	EC-V	
00188C13A7FE	SanJose-[redacted]	[redacted]	[redacted]	Cupertino, California	Unassigned	22-Jun-22 09:43	Reachable	Approve	Deny	9.1.1.3_91743	EC-US	
00188C1C0DE0	WEST4-[redacted]	[redacted]	[redacted]	San Francisco, California	sp-automated-ecv-[redacted]	15-Jun-22 14:27	Unreachable	Approve	Deny	9.2.0.0_93600	EC-V	
00188C1F266F	Indianapolis-[redacted]	[redacted]	[redacted]	Greencastle, Indiana	Unassigned	20-May-22 09:37	Unreachable	Approve	Deny	9.1.1.3_91743	EC-V	
00188C132EF2	silverpeak-[redacted]	[redacted]	[redacted]	Edinburgh, Scotland	Unassigned	10-May-22 07:14	Unreachable	Approve	Deny	8.1.4.5_84465	EC-XS	
00188C16E5F2	SFBayArea-[redacted]	[redacted]	[redacted]	Los Angeles, California	Unassigned	06-May-22 09:39	Unreachable	Approve	Deny	9.1.1.2_91733	EC-XS	
00188C1F2FCC	Alibaba-[redacted]	[redacted]	[redacted]	Hangzhou, Zhejiang, China	alibaba_china	04-May-22 08:39	Unreachable	Approve	Deny	9.1.1.3_91743	EC-V	
00188C1F2048	WEST6-[redacted]	[redacted]	[redacted]	San Francisco, California	idtest	29-Apr-22 10:14	Unreachable	Approve	Deny	9.1.1.2_91733	EC-V	
00188C1F2E95	Taka-[redacted]	[redacted]	[redacted]	Singapore, Singapore	Unassigned	24-Apr-22 08:46	Unreachable	Approve	Deny	9.0.3.3_89697	EC-V	

- To enable Orchestrator to manage an appliance after you verify its credentials, click **Approve**.
- If the appliance does not belong in your network, click **Deny**. If you want to include it later, click **Show Denied Devices**, locate it in the table, and click **Discover**.

Denied Devices												
Discovery Email Recipients [redacted] Save												
Show Discovered Devices												
Search												
Serial Number	Hostname	IP Address	Public IP Address	Location	Tag	Discovered Time	Discover	Software Version	Model	Comment		
00188C1F3A98	[redacted]	[redacted]	[redacted]	Dubai, Dubai, AE	sp-automated-ecv-7...	13-Jul-22 10:33	Discover	8.3.0.19_85161	EC-V		X	
00188C1CP995	Pittsgrove-[redacted]	[redacted]	[redacted]	Camden, New Jersey, US	Unassigned	22-Jun-22 10:03	Discover	9.1.1.3_91743	EC-V	OLD	X	
00188C1F3142	Atlanta-[redacted]	[redacted]	[redacted]	Alpharetta, Georgia, US	Unassigned	01-Jul-22 14:12	Discover	9.2.0.0_93713	EC-V		X	
0000000000000000	setteam-sewan-orch...	[redacted]	[redacted]	[redacted]	Unassigned	10-Jun-22 11:23	Discover	9.2.0.40293	OGE	DO NOT APPROVE ...	X	
00188C160702	H-CT-EC1	[redacted]	[redacted]	Yokohama, Kanagawa, JP	Unassigned	24-Apr-22 17:59	Discover	9.0.3.3_89697	EC-XS		X	
00188C164EDE	ECOS-1	[redacted]	[redacted]	Anaheim, California, US	Unassigned	09-May-22 17:30	Discover	9.0.6.0_90160	EC-XS		X	
00188C1F2F90	[redacted]	[redacted]	[redacted]	Frankfurt am Main, Hessen, DE	alibaba	29-Apr-22 00:38	Discover	9.0.6.0_90160	EC-V	test	X	
00188C131E78	H-CT-EC2	[redacted]	[redacted]	Yokohama, Kanagawa, JP	Unassigned	24-Apr-22 18:35	Discover	9.0.2.6_88624	EC-XS		X	
00188C1F2D3A	Anaheim-[redacted]	[redacted]	[redacted]	Anaheim, California, US	Unassigned	15-Apr-22 11:19	Discover	9.0.5.1_90052	EC-V		X	
0000000000000000	orchestrator.localdo...	[redacted]	[redacted]	[redacted]	Unassigned	14-Apr-22 18:51	Discover	9.0.6.4_90158	ORCH		X	
0000000000000000	orchestrator.localdo...	[redacted]	[redacted]	[redacted]	Unassigned	14-Apr-22 18:34	Discover	9.0.6.4_90158	ORCH		X	

- As a security measure to prevent unauthorized management of your network, any Orchestrator with your Account Name and Account Key must be approved by the originally deployed Orchestrator.

## Preconfigure Appliances

*Configuration > Overlays & Security > Discovery > Preconfiguration*

Use this page to prepopulate flat data files that are matched with appliances as you add them to your network.

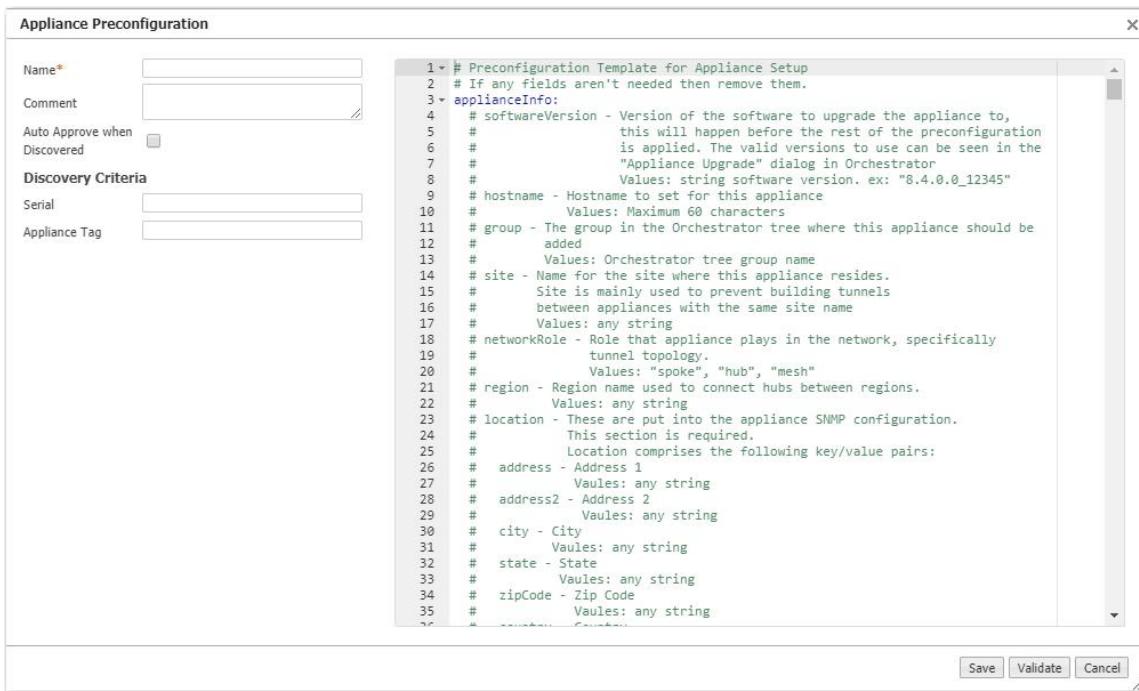
The screenshot shows a web-based application window titled "Preconfigure Appliances". At the top, there are buttons for "New" and "Clone from Existing". Below is a table with one row, labeled "1 Rows". The table has columns: Edit, Name, Discovery Criteria, Comment, Status, Modified On, Applied On, and Applied Appliance. The first row contains the value "site-A" in the Name column, "Pending Discovery" in the Status column, and the date "09-May-18 16:06" in the Modified On column. A search bar is located at the top right of the table area.

The information in the files is a combination of items found in the Appliance Configuration Wizard, along with site-specific information such as BGP, OSPF, IP SLA rules, VRRP, interfaces, and addressing.

You can create a new file or clone (and rename) an existing one. Make any changes with the built-in editor.

After the appliance is discovered and approved, software upgrade and configuration push are done automatically.

## New or Clone



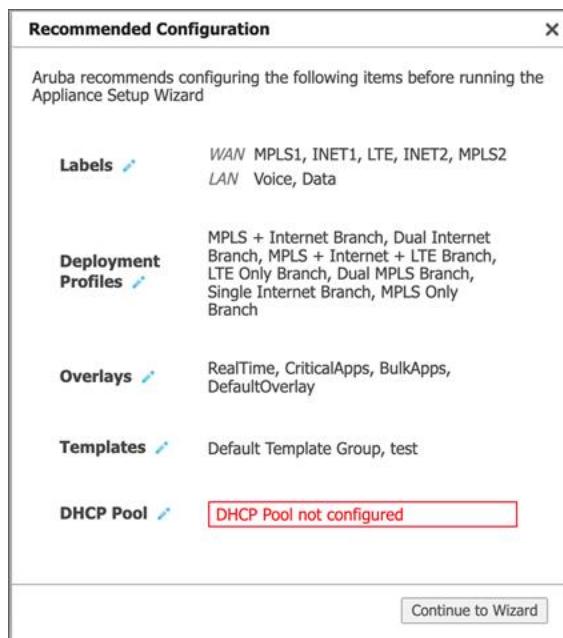
Field	Description
<b>Name</b>	Assigns a name to the preconfiguration file.
<b>Comment</b>	Optional descriptive field.
<b>Auto Approve when Discovered</b>	When <b>selected</b> , Orchestrator finds the appliance that matches the Discovery Criteria and automatically loads it without needing user intervention. When <b>deselected</b> , the user will be prompted to manually approve the association of the preconfiguration file to the appliance.
<b>Serial</b>	Serial number associated with the appliance that is to receive this configuration.
<b>Appliance Tag</b>	Free-form text or unique identifier that an administrator can associate with the appliance. Available as a discovery criteria for EC-Vs.

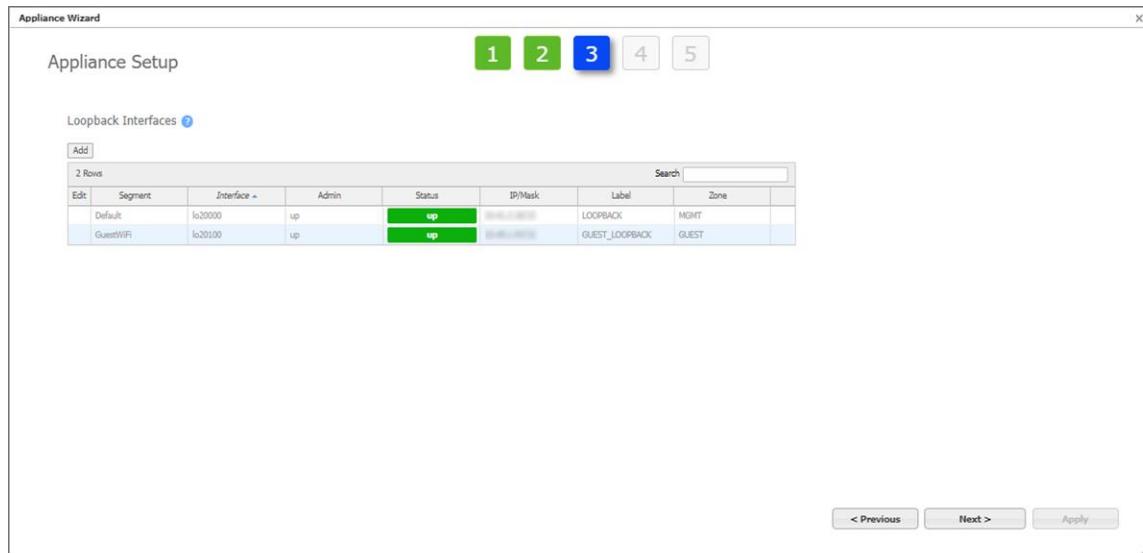
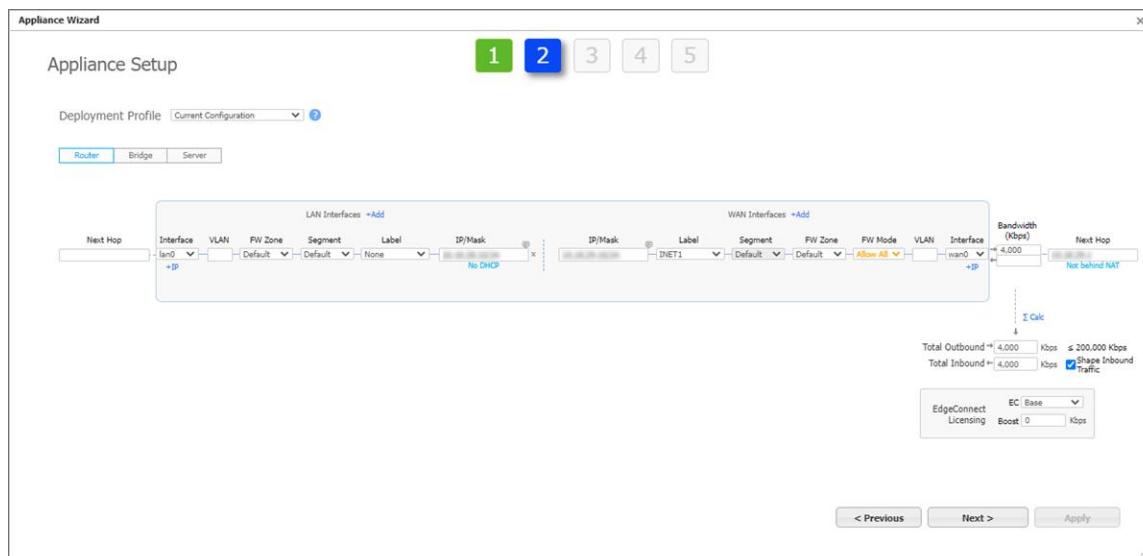
## Appliance Configuration Wizard

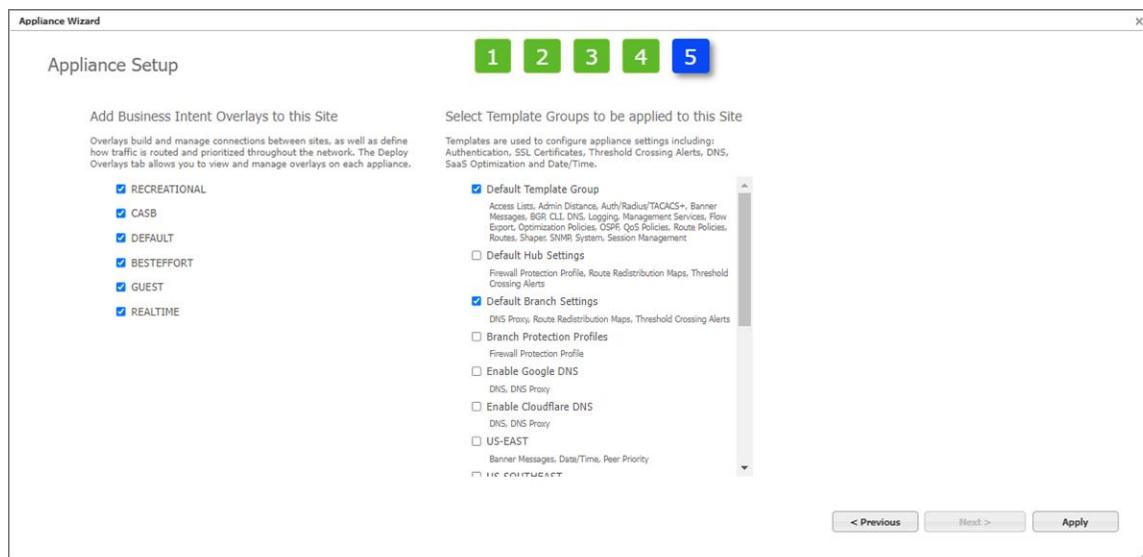
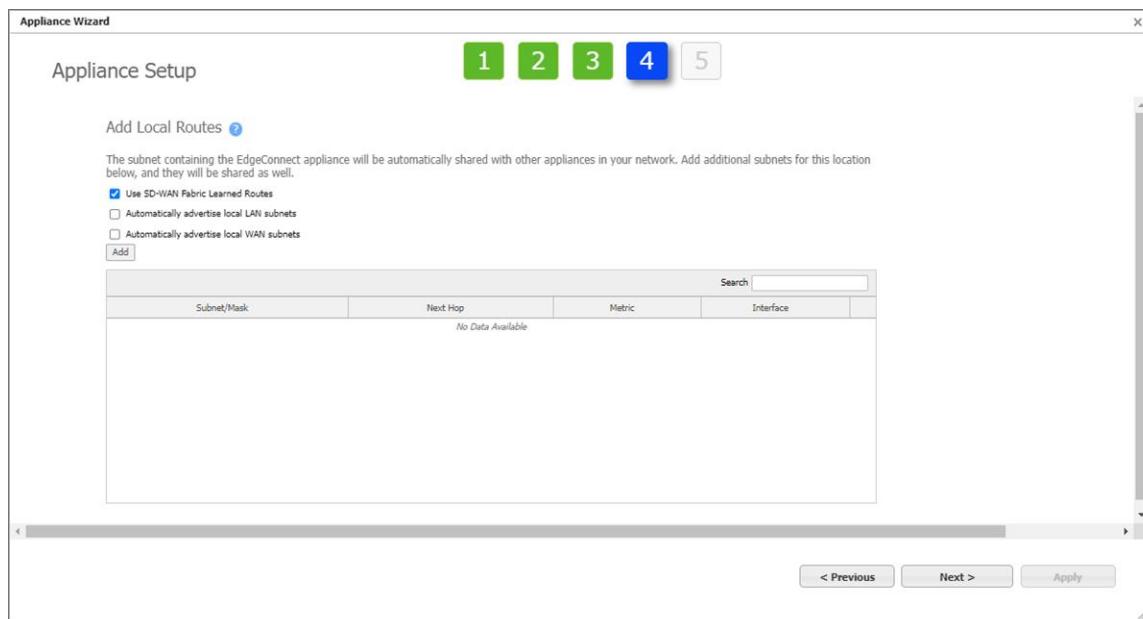
*Configuration > Overlays & Security > Discovery > Configuration Wizard*

Use this wizard to set up a newly added appliance or to reconfigure an appliance that is already in your network.

**NOTE** Orchestrator assumes you will push many of the same configuration items to each appliance. To that end, it surveys the templates and Overlay prerequisite items and displays the **Recommended Configuration** list, showing what comprehensive items you have and have not yet configured.







## EC-Enterprise Licenses

*Configuration > Overlays & Security > Licensing > Licenses*

- This page lists the appliance model, serial number, appliance name, feature licenses, and license terms for the appliances selected in the appliance tree.
- You can add, edit, or revoke EdgeConnect (EC) licenses from an appliance.

- A license summary including the number of used licenses and total number of available licenses is displayed above the table. The expiration date of the Boost license and each feature license is also listed.

**NOTE** EdgeConnect stops passing traffic when a license expires.

## Assign a License to an Appliance

1. In the appliance tree, select one or more appliances to display in the table.
2. Do one of the following:
  - To assign licenses to one appliance, click the **Edit** icon next to that appliance.
  - To assign licenses in bulk (to all appliances in the table), click **Assign Licenses to Appliances**.

**NOTE** To assign licenses in bulk, all appliances must be on the same software version.

The **Assign Licenses to Appliances** dialog box opens.

3. Complete the following elements as needed:

Field	Description
<b>EC</b>	Select the <b>Add/Replace</b> check box, and then select the EC size from the list: <b>Mini</b> , <b>Base</b> , <b>Base + Plus</b> , <b>50 Mbps</b> , <b>200 Mbps</b> , <b>500 Mbps</b> , <b>1 Gbps</b> , <b>2 Gbps</b> , or <b>Unlimited</b> .
<b>Boost</b>	Select the <b>Add/Replace</b> check box, and then enter the amount of Boost to apply to the EC.
<b>Feature licenses</b>	<ol style="list-style-type: none"> <li>1. To add a feature license, select the <b>Add/Replace</b> check box.</li> <li>2. If required, select a license option from the list and specify a quantity, such as amount of bandwidth.</li> </ol>

4. To revoke a license or Boost, select the **Revoke** check box next to the license or Boost you want to revoke.

**NOTE** If you revoke an EC license from an appliance, Silver Peak will revoke the Boost license and all feature licenses from that appliance.

**NOTE** You must revoke the license from an appliance before you can RMA it. For more information on how to RMA an appliance, see [RMA Wizard on page 540](#).

5. Click **Apply**.

## EC-Metered Licenses

*Configuration > Overlays & Security > Licensing > Licenses*

To filter the list, click one of the following buttons:

Button	Description
<b>EC-Metered License</b>	<p>Display the EC-metered licenses for all appliances selected in the appliance tree.</p> <p>To filter the list, click one of the following buttons:</p> <ul style="list-style-type: none"> <li>• <b>All</b> – Display all appliances.</li> <li>• <b>Boost</b> – Display appliances with Boost licenses granted.</li> <li>• <b>Feature license</b> – Display appliances with this feature license granted.</li> </ul>
<b>Bandwidth Usage Report</b>	<p>Display the bandwidth usage report for all appliances selected in the appliance tree. To aggregate the usage report, click <b>Summary</b>, <b>Appliance</b>, or <b>Daily</b>, and then select a month and year.</p>
<b>Feature License Usage Report</b>	<p>Display the feature license usage report for all appliances selected in the appliance tree. To aggregate the usage report, click <b>Summary</b>, <b>Appliance</b>, or <b>Daily</b>, and then select a month and year.</p>

- This page lists the appliance model, serial number, appliance name, and feature licenses for the appliances selected in the appliance tree.
- You can add, edit, or revoke EdgeConnect (EC) licenses from an appliance.

**NOTE** EdgeConnect stops passing traffic when a license expires.

## Assign a License to an Appliance

1. In the appliance tree, select one or more appliances to display in the table.
2. Do one of the following:
  - To assign licenses to one appliance, click the **Edit** icon next to that appliance.
  - To assign licenses in bulk (to all appliances in the table), click **Assign Licenses to Appliances**.

**NOTE** To assign licenses in bulk, all appliances must be on the same software version.

The **Assign Licenses to Appliances** dialog box opens.

3. Complete the following elements as needed:

Field	Description
<b>EC</b>	Select the <b>Add/Replace</b> check box to apply the EC-metered license.
<b>Boost</b>	Select the <b>Add/Replace</b> check box, and then enter the amount of Boost to apply to the EC.
<b>Feature licenses</b>	<ol style="list-style-type: none"> <li>1. To add a feature license, select the <b>Add/Replace</b> check box.</li> <li>2. If required, select a license option from the list and specify a quantity, such as amount of bandwidth.</li> </ol>

- To revoke a license or Boost, select the **Revoke** check box next to the license or Boost you want to revoke.

**NOTE** If you revoke an EC license from an appliance, Silver Peak will revoke the Boost license and all feature licenses from that appliance.

**NOTE** You must revoke the license from an appliance before you can RMA it. For more information on how to RMA an appliance, see [RMA Wizard on page 540](#).

- Click **Apply**.

## Bandwidth Usage Report

This page lists the maximum outbound bandwidth usage, maximum inbound bandwidth usage, and Boost bandwidth for the account.

To aggregate the usage report, click **Summary**, **Appliance**, or **Daily**, and then select a month and year.

## Feature License Usage Report

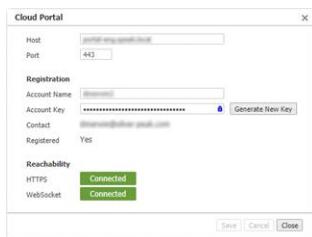
This page lists the feature license usage report for the account.

To aggregate the usage report, click **Summary**, **Appliance**, or **Daily**, and then select a month and year.

## Cloud Portal

*Configuration > Overlays & Security > Licensing > Cloud Portal  
Orchestrator > Orchestrator Server > Licensing > Cloud Portal*

The **Cloud Portal** is used to register cloud-based features and services, such as **SaaS optimization** and **EdgeConnect**.



- When you purchase one of these services, an **Account Name** and instructions to obtain your **Account Key** are sent to you. You will use these to register your appliances.
- The cloud portal populates the **Contact** field from information included in your purchase order.
- Use of these services requires that your appliances can access the cloud portal via the Internet.

# Networking

These topics describe the pages related to configuring and managing the network.

## Deployment Tab

*Configuration > Networking > Deployment*

This tab provides summary and detailed views of the selected appliance's deployment settings.

To change an appliance's deployment settings, click the **Edit** icon next to the name of the desired appliance.

The following table describes the fields on the Summary view of this tab.

Field	Description
<b>Appliance</b>	Name of the deployed appliance.
<b>HA</b>	Name of the appliance with which this appliance is paired for EdgeConnect High Availability (HA).
<b>Mode</b>	Indicates the deployment mode for the appliance: <ul style="list-style-type: none"> <li><b>Inline Router</b> – Uses separate LAN and WAN interfaces to route data traffic.</li> <li><b>Bridge</b> – Uses a virtual interface, <b>bvi</b>, created by binding the WAN and LAN interfaces.</li> <li><b>Server</b> – Both management and data traffic use the mgmt0 interface.</li> </ul>
<b>Outbound Bandwidth</b>	Deployment's total outbound bandwidth in Kbps.
<b>Inbound Bandwidth</b>	Deployment's total inbound bandwidth in Kbps.
<b>WAN Labels Used</b>	Identify the service, such as <b>MPLS</b> or <b>Internet</b> .
<b>LAN Labels Used</b>	Identify the data, such as <b>data</b> , <b>VoIP</b> , or <b>replication</b> .
<b>Segment</b>	Names of the segments used for this appliance deployment.
<b>Details</b>	Select the <b>information</b> icon to view further deployment details of an appliance.

The following table describes the fields on the Details view of this tab.

Field	Description
<b>Appliance</b>	Name of the deployed appliance.
<b>Interface</b>	Name of the LAN or WAN interface.

Field	Description
<b>Label</b>	Label mapped to the interface. LAN labels refer to traffic type, such as VoIP, data, or replication. WAN labels refer to the service or connection type, such as MPLS, internet, or Verizon.
<b>Zone</b>	Firewall zone applied to the interface.
<b>Segment</b>	Name of the segment used for this interface.
<b>IP/Mask</b>	Interface's IP address and subnet mask.
<b>WAN/LAN Side</b>	Indicates that the interface is WAN-side or LAN-side.
<b>Next Hop</b>	Deployment interface's next hop router address.
<b>Public IP</b>	Public IP address.
<b>Inbound</b>	Interface's inbound bandwidth in Kbps.
<b>Outbound</b>	Interface's outbound bandwidth in Kbps.
<b>NAT</b>	Indicates whether the appliance is behind a NAT-ed interface.
<b>Firewall Mode</b>	Indicates the firewall mode for the appliance's WAN-side interface: <ul style="list-style-type: none"> <li><b>Allow All</b> – Permits unrestricted communication.</li> <li><b>Stateful</b> – Only allows communication from the LAN-side to the WAN-side. Used if the interface is behind the WAN edge router.</li> <li><b>Stateful+SNAT</b> – Applies Source NAT to outgoing traffic. Used if the interface is directly connected to the Internet.</li> <li><b>Harden</b> – For traffic inbound from the WAN, the appliance accepts <b>only</b> IPSec tunnel packets that terminate on an EdgeConnect appliance. For traffic outbound to the WAN, the appliance <b>only</b> allows IPSec tunnel packets and management traffic that terminate on an EdgeConnect appliance.</li> </ul>
<b>DHCP</b>	Indicates whether the interface's IP address is obtained from the DHCP server.
<b>HA Interface</b>	Indicates whether the interface is part of an EdgeConnect High Availability (HA) link.
<b>Comment</b>	Additional information for this deployment interface.

## Deployment Dialog Box

The three deployment modes are **Bridge**, **Router**, and **Server**.

**WARNING** ALWAYS use Router mode unless you have a legacy, WAN Optimization-specific use case and are well-acquainted with the requirements of Bridge or Server mode deployments.

## Enable EdgeConnect HA

EdgeConnect High Availability (HA) mode is a high availability cluster configuration that provides appliance redundancy by pairing two EdgeConnect devices together.

When you configure two EdgeConnect appliances in EdgeConnect HA mode, the resilient cluster acts as a single logical system for orchestrated WAN functions. It extends the robust SD-WAN multipathing capabilities, such as Business Intent Overlays, seamlessly across the two devices as though they were one entity.

With EdgeConnect HA mode, a WAN uplink is physically plugged into a single one of the EdgeConnect appliances but is available to both in the cluster. For WAN connections that perform NAT (for example, a consumer-grade Broadband Internet connection), it means that only a single Public IP needs to be provisioned in order for both EdgeConnect devices in the EdgeConnect HA cluster to be able to build Business Intent Overlays using that transport resource. The same is true for orchestrated tunnels to third-party cloud services, such as Zscaler and AWS Transit Gateway.

**NOTE** EdgeConnect HA mode provides clustering for WAN-side functions only. You must select and configure an appropriate LAN-side redundancy mechanism for a given business location. Available options are VRRP+IP SLA, BGP, and OSPF.

To enable EdgeConnect HA:

1. Select the **EdgeConnect HA** check box.
2. Configure the interfaces (LAN-side and WAN-side) on both EdgeConnect devices to reflect the WAN connections that are plugged into each one of the respective appliances.

**NOTE** Both EdgeConnect devices will be able to leverage all WAN connections regardless of which chassis they are physically plugged into. It is, however, important to match the interface configuration displayed on the Deployment dialog box to the actual chassis the WAN connection is physically and directly connected to.

3. Select the physical ports on the respective EdgeConnect appliances that you will connect to each other using an Ethernet cable (RJ-45 twisted pair or SR optical fiber).

**NOTE** You can choose any LAN or WAN port combination for this HA Link that is available on the respective EdgeConnect chassis. You must match the media type and speed for both ends of the HA link. (For example, 1 Gigabit-Ethernet RJ-45 to RJ-45 or 10 Gigabit-Ethernet multimode fiber LC-connector-to-LC-connector). Also, note that you cannot use MGMT ports for the HA Link; only LAN or WAN ports.

## IPSec over UDP Tunnel Configuration

For both EdgeConnect appliances in a high availability cluster to be able to share a common transport connection, you must set the tunnel type to IPSec over UDP mode. This is the default tunnel mode for all deployments running ECOS 8.1.6/Orchestrator 8.2 or later.

**NOTE** For SD-WAN fabrics upgraded from earlier releases, see Tunnel Settings in Orchestrator (**Orchestrator > Orchestrator Server > Tools > Tunnel Settings**) to change to IPSec over UDP mode.

You must configure the same site name for both appliances in the EdgeConnect HA pair so that Orchestrator assigns a unique IPSec UPD port number for each appliance.

## LAN-side High Availability

Typically, in a branch site deployment, you will choose to configure the cluster with VRRP+IP SLA to modify priority and subnet sharing metrics based on VRRP and WAN interface status. For more advanced deployments with Layer 3 routers or switching on the LAN side, BGP or OSPF can be configured. For details, refer to the *EdgeHA High Availability Deployment Guide*.

## LAN-side Monitoring

The IP SLA feature should be configured to monitor the LAN-side VRRP state in order to automatically disable subnet sharing from that appliance in the case of a LAN link failure.

For more information, refer to the IP SLA configuration guide.

## Map Labels to Interfaces

- On the **LAN** side, labels are optional. You can use them as match criteria for Business Intent Overlay ACLs, such as **data**, **VoIP**, or **replication**.
- On the **WAN** side, labels identify the link type, such as **MPLS** or **Internet**. These labels are mandatory. Orchestrator uses them to build Business Intent Overlay policies.
- To create or manage a global pool of labels, either:
  - Navigate to **Configuration > Overlays & Security > Deployment Profiles**, click the **Edit** icon next to Label, and make the appropriate changes, or
  - Navigate to **Configuration > Overlays & Security > Interface Labels**) and make the appropriate changes.
- The change you make to a label propagates automatically. For example, it renames tunnels that use that labeled interface.

## LAN-side Configuration: Segments and Firewall Zones

EdgeConnect Segmentation (VRF) provides orchestrated Layer 3 segmentation, Zone Based Firewall, and IDS-end-to-end across the SD-WAN fabric. Segment and zone policies are global in scope. They are managed on the **Configuration > Networking > Routing > Routing Segmentation (VRF)** tab.

Segments and zones are then assigned to LAN-side interfaces for each appliance by using the Deployment dialog box. By default, the Segment and FW Zone fields on LAN interfaces are set to the system-generated Default segment. You can select a different segment and firewall zone from the drop-down lists. These lists reflect the segments and zones that are set up on the Routing Segmentation (VRF) tab.

**NOTE** The segment for WAN interfaces cannot be changed.

## LAN-side Configuration: DHCP

- By default, **each** LAN IP acts as a **DHCP Server** when the appliance is in (the default) Router mode.
- The global defaults are set in **Configuration > Networking > DHCP > DHCP Server Defaults** and pre-populate this page. The other choices are **No DHCP** and having the appliance act as a **DHCP/BOOTP Relay**.
- To customize an individual interface on the Deployment screen, click the DHCP-related link under the IP/Mask field. The DHCP Settings dialog box opens.

The following tables describe the various DHCP settings you can configure.

*DHCP Server*

Setting	Description
<b>Subnet Mask</b>	Mask that specifies the default number of IP addresses reserved for any subnet. For example, entering <b>24</b> reserves 256 IP addresses.
<b>IP Range</b>	You can designate one or more IP address ranges available for use. Specify <b>Start IP</b> and <b>End IP</b> addresses. To add another IP address range, click <b>Add</b> . <b>IMPORTANT:</b> Multiple IP ranges cannot overlap.
<b>Default lease, Maximum lease</b>	Specify, in hours, how long an interface can keep a DHCP-assigned IP address.
<b>Gateway IP</b>	Specifies the IP address for the gateway to use.
<b>DNS server(s)</b>	Specifies the associated Domain Name System servers.
<b>NTP server(s)</b>	Specifies the associated Network Time Protocol servers.
<b>NetBIOS name server(s)</b>	Used for Windows (SMB) type sharing and messaging. It resolves the names when you are mapping a drive or connecting to a printer.
<b>NetBIOS node type</b>	<b>NetBIOS node type</b> of a networked computer relates to how it resolves NetBIOS names to IP addresses. There are four node types: <ul style="list-style-type: none"> <li>• <b>B-node</b> = 0x01 Broadcast</li> <li>• <b>P-node</b> = 0x02 Peer (WINS only)</li> <li>• <b>M-node</b> = 0x04 Mixed (broadcast, then WINS)</li> <li>• <b>H-node</b> = 0x08 Hybrid (WINS, then broadcast)</li> </ul>
<b>DHCP failover</b>	Enables DHCP failover. To set it up, click the <b>Failover Settings</b> link.

### DHCP/BOOTP Relay

Setting	Description
<b>Destination DHCP/BOOTP Server</b>	IP address of the DHCP server assigning the IP addresses. This setting applies to the local interface only.
<b>Enable Option 82</b>	When selected, inserts additional information into the packet header to identify the client's point of attachment. This setting applies to all LAN-side interfaces on this appliance. <b>IMPORTANT:</b> Changing this setting will modify Option 82 settings on all LAN-side interfaces that are enabled as DHCP Relay.
<b>Option 82 Policy</b>	Tells the relay what to do with the hex string it receives. The choices are <b>append</b> , <b>replace</b> , <b>forward</b> , and <b>discard</b> . This setting applies to all LAN-side interfaces on this appliance. <b>IMPORTANT:</b> Changing this setting will modify Option 82 settings on all LAN-side interfaces that are enabled as DHCP Relay.

### WAN-side Configuration

**Firewall Zone:** Zone-based firewall policies are configured globally on the Orchestrator. A zone is applied to an **Interface**. By default, traffic is allowed between interfaces labeled with the same zone. Any traffic between interfaces with different zones is dropped. You can create exception rules (Security Policies) to allow traffic between interfaces with different zones.

**Firewall Mode:** Four options are available at each WAN interface:

- **Allow All** permits unrestricted communication.

**WARNING** Use this option with extreme caution and only if the interface is behind a WAN edge firewall.

- **Stateful only** allows communication from the LAN-side to the WAN-side.

Use this option if the interface is behind a WAN edge router.

- **Stateful with SNAT** applies Source NAT to outgoing traffic.

Use this option if the interface is connected directly to the Internet and you want to enable local internet breakout.

- **Harden**

- For traffic inbound from the WAN, the appliance accepts **only** IPSec tunnel packets that terminate on an EdgeConnect appliance.
- For traffic outbound to the WAN, the appliance **only** allows IPSec tunnel packets and management traffic that terminate on an EdgeConnect appliance.

**NAT Settings:** To change the NAT setting, click the NAT-related link under the Next Hop field on the WAN side. The NAT Settings dialog box opens.

Select one of the following options:

- If the appliance is behind a NAT-ed interface, select **NAT**.
- If the appliance is not behind a NAT-ed interface, select **Not behind a NAT**.
- To assign a destination IP address for tunnels being built from the network to this WAN interface, select the last option and enter the IP address.

**Shaping:** You can limit bandwidth selectively on each WAN interface.

- **Total Outbound** bandwidth is licensed by model. It is the same as max system bandwidth.
- To enter values for shaping inbound traffic (recommended), you first must select **Shape Inbound Traffic**.

**EdgeConnect Licensing:** Only visible on EdgeConnect appliances.

- You can change the bandwidth allotted for this appliance by selecting the appropriate option from the **EC** drop-down list. Your options are based on the licensing you have purchased.
- If you have purchased a pool of **Boost** for your network, you can allocate a portion of it on the Deployment dialog box. You can also direct allocations to specific types of traffic in the Business Intent Overlays.
- To view the licensing and distribution of EdgeConnect and Boost bandwidth for your appliances, navigate to the **Configuration > Overlays & Security > Licensing > Licenses** tab.

## BONDING

- EdgeConnect supports etherchannel bonding of multiple physical interfaces of the same media type into a single virtual interface. For example, **wan0** plus **wan1** bond to form **bwan0**. This increases throughput on a very high-end appliance and/or provides interface-level redundancy.
- For bonding on a virtual appliance, you would need to configure the host instead of the appliance. For example, on a VMware ESXi host, you would configure NIC teaming to get the equivalent of etherchannel bonding.
- Whether you use a physical or a virtual appliance, etherchannel must also be configured on the directly connected switch/router. Refer to Aruba SD-WAN user documentation.

## Interfaces Tab

*Configuration > Networking > Interfaces*

The Interfaces tab lists the interfaces for appliances selected in the appliance tree.

Interfaces																				
		Link Aggregation		Export		2 mins														
Interfaces																				
<a href="#">All</a> <a href="#">Hardware</a> <a href="#">Dynamic</a>														Search						
35 Rows	Edit	Appliance	Name	Status	LACP Status	IP Address/Mask	Public IP	Segment	DHCP	Speed	Duplex	MTU	MAC Address	SNMP IfIndex						
		appliance-0001	wan5	up					No	1000Mb/s (auto)	full (auto)	1500	Unassigned	1						
		appliance-0001	lan2	up					No	1000Mb/s (auto)	full (auto)	1500	Unassigned	3						
		appliance-0001	wan0	up		20.100.200.200/24		Default	No	1000Mb/s (auto)	full (auto)	1500	Unassigned	6						
		appliance-0001	lan12	up					No	1000Mb/s (auto)	full (auto)	1500	Unassigned	7						
		appliance-0001	lan3	up					No	1000Mb/s (auto)	full (auto)	1500	Unassigned	8						
		appliance-0001	wan13	up					No	1000Mb/s (auto)	full (auto)	1500	Unassigned	9						
		appliance-0001	lan1	up					No	1000Mb/s (auto)	full (auto)	1500	Unassigned	10						
		appliance-0001	lan4	up					No	1000Mb/s (auto)	full (auto)	1500	Unassigned	11						
		appliance-0001	blan0	up					No	N/A	N/A	1500	Unassigned	14						
		appliance-0001	wan2	up					No	1000Mb/s (auto)	full (auto)	1500	Unassigned	15						
		appliance-0001	lan15	up					No	1000Mb/s (auto)	full (auto)	1500	Unassigned	16						

The All button displays all hardware and dynamic interfaces for the selected appliances.

Descriptions of the fields on this tab follow:

Field	Description
<b>Appliance</b>	Name of the appliance for the interface.
<b>Name</b>	Name of the interface.
<b>Status</b>	Status of the interface (up or down).
<b>LACP Status</b>	Link aggregation status of the interface (up or down). This status applies only to bonded interfaces (blan0, blan1, bwan0, and bwan1). This field is displayed only if the channel group is in LACP mode.
<b>IP Address/Mask</b>	IP address for the interface.
<b>Public IP</b>	Public IP address for the interface.
<b>Segment</b>	Name of the configured segment being used.
<b>DHCP</b>	Indicates whether this interface's IP address is obtained from the DHCP server. Displays as <b>Yes</b> , <b>No</b> , <b>No data</b> (not configured), or <b>Invalid data</b> (error condition).
<b>Speed</b>	Current interface speed state and setting.
<b>Duplex</b>	Current interface duplex state and setting.
<b>MTU</b>	Maximum number of packets being transmitted.
<b>MAC Address</b>	MAC address applied to the interface.
<b>SNMP IfIndex</b>	Index number of the network interface.

- Best practice is to assign static IP addresses to management interfaces to preserve their reachability.
- **Duplex** should never display as **half duplex** after auto-negotiation. If it does, performance issues and dropped connections will occur on the appliance. To resolve, check the cabling on the appliance and the ports on the adjacent switch or router.

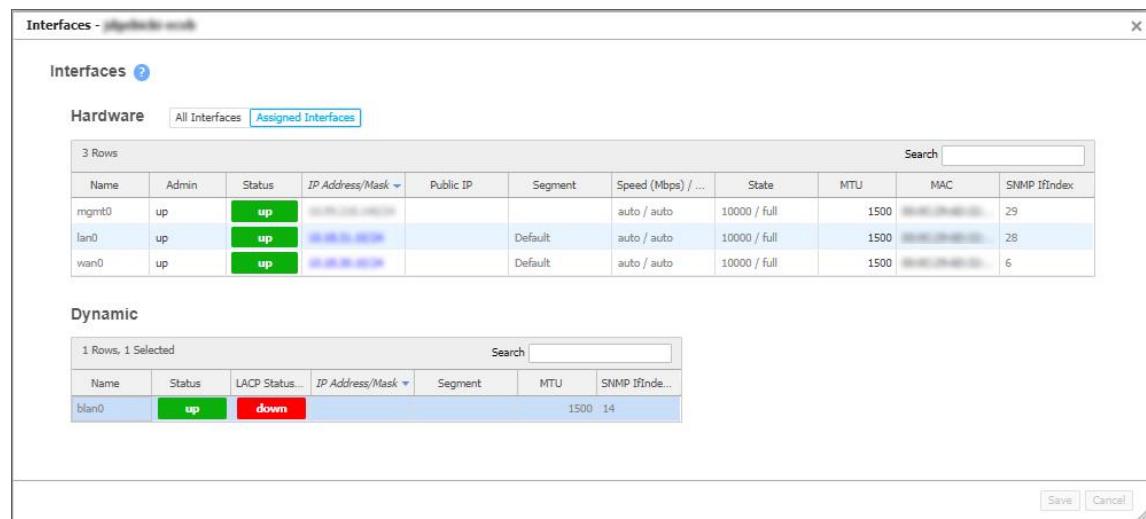
- To directly change interface parameters for a particular appliance, click the corresponding edit icon, which opens the Interfaces dialog box for the appliance.
- To change the IP address for a **lan** or **wan** interface, either use the Appliance Manager **Configuration > System & Networking > Deployment** page or the CLI (Command Line Interface).
- To change the IP address for **mgmt0**, either use the Appliance Manager **Administration > Basic Settings > Hostname/IP** page or the CLI.

## Terminology

Interface	Description
<b>blan</b>	Bonded LAN interfaces (as in <b>lan0 + lan1</b> ).
<b>bvi0</b>	Bridge Virtual Interface. When the appliance is deployed in-line (Bridge mode), it is the routed interface that represents the bridging of <b>wan0</b> and <b>lan0</b> .
<b>bwan</b>	Bonded WAN interfaces (as in <b>wan0 + wan1</b> ).
<b>tlan</b>	10-Gbps fiber LAN interface.
<b>twan</b>	10-Gbps fiber WAN interface.

## Interfaces Edit Row

Use this dialog box to change interface configurations for the appliance.



The All Interfaces button displays all interfaces for the appliance, including both assigned and unassigned hardware interfaces. MAC addresses indicate assigned interfaces.

Descriptions of the fields on this dialog box follow:

## Hardware

Field	Description
<b>Name</b>	Name of the interface.
<b>Admin</b>	Admin status of the interface (up or down). Click this field to change the value.
<b>Status</b>	Status of the interface (up or down).
<b>IP Address/Mask</b>	IP address for the interface. If the address is blue, you can click it to open the Deployment dialog box, from which you can change IP addresses/masks.
<b>Public IP</b>	Public IP address for the interface.
<b>Segment</b>	Name of the configured segment being used.
<b>Speed (Mbps) / Duplex</b>	Current interface speed and duplex settings. <b>auto</b> means auto-negotiation, which is the process by which terminating devices automatically negotiate for maximum bandwidth.
<b>State</b>	Current interface speed and duplex states.
<b>MTU</b>	Maximum number of packets being transmitted. Click this field to change the value.
<b>MAC</b>	MAC address applied to the interface. To unassign the MAC address, click the field and select <b>Unassigned</b> .
<b>SNMP IfIndex</b>	Index number of the network interface.

## Dynamic

Field	Description
<b>Name</b>	Name of the interface.
<b>Status</b>	Status of the interface (up or down).
<b>LACP Status</b>	Link aggregation status of the interface (up or down). This status applies only to bonded interfaces (blan0, blan1, bwan0, and bwan1). This field is displayed only if the channel group is in LACP mode.
<b>IP Address/Mask</b>	IP address for the interface. If the address is blue, you can click it to open the Deployment dialog box, from which you can change IP addresses/masks.
<b>Segment</b>	Name of the configured segment being used.
<b>MTU</b>	Maximum number of packets being transmitted.
<b>SNMP IfIndex</b>	Index number of the network interface.

- As a best practice, assign static IP addresses to management interfaces to preserve their reachability.

- **Speed (Mbps) / Duplex** should never display as **half duplex** after auto-negotiation. If it does, performance issues and dropped connections will occur on the appliance. To resolve, check the cabling on the appliance and the ports on the adjacent switch or router.
- To change the IP address for a **lan** or **wan** interface, either use the Appliance Manager **Configuration > System & Networking > Deployment** page or the CLI (Command Line Interface).
- To change the IP address for **mgmt0**, either use the Appliance Manager **Administration > Basic Settings > Hostname/IP** page or the CLI.

## NAT

NAT allows for multiple sites with overlapping IP addresses to connect to a single SD-WAN fabric. You can configure SNAT (Source Network Address Translation), DNAT (Destination Network Address Translation), destination TCP, and UDP port translation rules to LAN to SD-WAN fabric traffic in the ingress and egress direction. The following address translation options are supported:

- 1:1 source and destination IP address translation
- 1:1 subnet to subnet source and destination IP address translation
- Many to one IP source address translation
- NAT pools for translated source IP address

You can view both NAT Rules and NAT Pools within your network by selecting **NAT Rule** or **NAT Pools** at the top of the page. You can also export a CSV file of your branch NAT traffic. Select the **Edit** icon to add rules to your NAT and NAT Pools.

## NAT Rules and Pools

You can add NAT rules by completing all the values in the table shown below. Each NAT rule has a directional field or value. Outbound rules are applied to the traffic flows initiated from the LAN, destined to the SD-WAN fabric. Inbound rules are applied to the traffic flows initiated from the SD-WAN fabric destined to the LAN. Return traffic for a given flow does not require an additional rule. The destination IP address must be configured for each rule.

**NOTE** You must disable advertisements of local, static routes on the LAN side at the site so the routes are completely unique. Additionally, you must configure announce-only static routes for your NAT pools and advertise them to the SD-WAN fabric by allowing those routes in your "Redistribute routes to SD-WAN fabric" route map.

Complete the following steps to add a rule to your NAT:

1. Select **Add Rule**.
2. Complete the following values in the table by selecting any of the columns.

Field	Description
<b>Priority</b>	Order in which the rules are executed; the lower the priority, the higher the chance your NAT rule will be applied.
<b>LAN Interface</b>	Name of the LAN interface the NAT rule is using. This is configurable for an outbound NAT rule only.
<b>Segment</b>	Name of the segment being used.
<b>Direction</b>	Select the direction the traffic is going: <input type="checkbox"/> <b>Outbound (LAN to Fabric)</b> <input type="checkbox"/> <b>Inbound (Fabric to LAN)</b>
<b>Protocol</b>	Type of protocol being used for each NAT.
<b>Source</b>	Original source IP address of the IP packet.
<b>Destination</b>	Address of the LAN/WAN interface where the traffic is going to.
<b>Translated Source</b>	Translated source IP address when the NAT rule is applied.
<b>Translated Destination</b>	Translated destination IP address when the NAT rule is applied.
<b>Enabled</b>	Select this check box to enable your customized NAT rule. Direction can be both inbound or outbound.
<b>Comment</b>	Any comment you want to add pertaining to your NAT rule.
<b>Criteria</b>	<b>Match:</b> LAN interface, direction, source, destination <b>Set:</b> Translated source, translated destination

## NAT Pools

You also have the option to configure a NAT pool. Complete the following steps to create a NAT pool:

1. Select the **Edit** icon on the NAT tab. The **NAT** window opens.
2. Select the **NAT Pools** icon. The **NAT Pools** window opens.
3. Select **Add**.
4. Select the columns in the table, starting with **Name**, to enter information about your Pool.

Field	Description
<b>Name</b>	Name of your pool.
<b>Direction</b>	Whether the traffic is outbound or inbound.
<b>Subnet</b>	IP address of the subnet.
<b>Translate Ports</b>	Enable source port address translation if the NAT pool is too small to accommodate multiple, flows simultaneously with 1:1 IP address translation.

## VRRP Tab

*Configuration > Networking > VRRP*

This tab summarizes the configuration and state for appliances deployed with **Virtual Router Redundancy Protocol (VRRP)**.

In an out-of-path deployment, one method for redirecting traffic to the EdgeConnect appliance is to configure VRRP on a common virtual interface. Possible scenarios are:

- When no spare router port is available, a single appliance uses VRRP to peer with a router (or Layer 3 switch). This is appropriate for an out-of-path deployment in which no redundancy is needed.
- A pair of active, redundant appliances use VRRP to share a common, virtual IP address at their site. This deployment assigns one appliance a higher priority than the other, thereby making it the **Master** appliance, and the other the **Backup**.

### VRRP Edit Row

Click **Add** to begin completing the fields in the following table.

### VRRP Tab Settings

Field	Description
<b>Admin</b>	Options are up (enable) and <b>down</b> (disable).
<b>Advertisement Timer</b>	Default is <b>1 second</b> .
<b>Group ID</b>	Value assigned to the two peers. Depending on the deployment, the group can consist of an appliance and a router (or L3 switch), or two appliances. The valid range is 1 to 255.
<b>Interface</b>	Interface that VRRP is using for peering.
<b>Segment</b>	Name of the segment, if enabled.
<b>IP Address Owner</b>	An EdgeConnect appliance cannot use one of its own IP addresses as the VRRP IP, so this will always be <b>No</b> .
<b>Master IP</b>	Current VRRP Master's Interface or local IP address.
<b>Master State Transitions</b>	Number of times the VRRP instance went from Master to Backup and vice versa. A high number of transitions indicates a problematic VRRP configuration or environment. In this case, check the configuration of all local appliances and routers, and then review the log files.
<b>Preemption</b>	Leave this selected/enabled so that after a failure, the appliance with the highest priority comes back online and again assumes primary responsibility.
<b>Priority</b>	The greater the number, the higher the priority. The appliance with the higher priority is the VRRP Master.
<b>State Uptime</b>	Time elapsed since the VRRP instance entered the state it is in.

Field	Description
<b>State</b>	The VRRP instance has three options: <ul style="list-style-type: none"> <li><b>Backup</b> - Instance is in VRRP backup state.</li> <li><b>Init</b> - Instance is initializing, it is disabled, or the interface is down.</li> <li><b>Master</b> - Instance is the current VRRP master.</li> </ul>
<b>Virtual IP</b>	IP address of the VRRP instance. VRRP instances can run between two or more appliances, or an appliance and a router.
<b>Virtual MAC address</b>	MAC Address that the VRRP instance is using. On an NX Appliance, this is in 00-00-5E-00-01-{VRID} format. On virtual appliances, the VRRP instance uses the interface's assigned MAC Address (for example, the MAC address that the hypervisor assigned to <b>wan0</b> ).

## WCCP Tab

*Configuration > Networking > WCCP*

Use this tab to view, edit, and delete WCCP Service Groups.

Appliance	Group ID	Oper Status	Admin	Router IP	Protocol	Interface	Compatibility	Forwarding Method	Advanced Settings
appliance-wan0									
appliance-wan0									

Web Cache Communications Protocol (WCCP) supports the redirection of any TCP or UDP connections to appliances participating in WCCP Service Groups. The appliance intercepts only those packets that have been redirected to it. The appliance optimizes traffic flows that the Route Policy tunnelizes. The appliance forwards all other traffic as pass-through or pass-through-unshaped, as per the Route Policy.

Refer to the [Network Deployment Guide](#) and the [SD-WAN Deployment Guide](#) for examples, best practices, and deployment tips.

### WCCP Edit Row

Use this page to **view**, **edit**, and **delete** WCCP Service Groups. For the Service Groups to be active, you must select **Enable WCCP**. Additionally, the appliance should always be connected to an interface/VLAN that does not have redirection enabled—preferably a separate interface/VLAN would be provided for the appliance. If the appliance uses **auto-optimization**, WCCP redirection must also be applied on the uplinks of the router or L3 switch to the core/WAN.

## WCCP Settings

Field	Description
<b>Admin</b>	Values are up and down. The default is up.
<b>Advanced Settings</b>	You can only configure these options directly on the appliance. For more information and best practices, refer to the <a href="#">Network Deployment Guide</a> .
<b>Compatibility Mode</b>	Select the appropriate option for your router. If a WCCP group is peering with a router running <b>Nexus</b> OS, the appliance must adjust its WCCP protocol packets to be compatible. By default, the appliance is <b>IOS</b> -compatible.
<b>Forwarding Method</b>	<p>Also known as the <i>Redirect Method</i>. Packet redirection is the process of forwarding packets from the router or L3 switch to the appliance. The router or L3 switch intercepts the packet and forwards it to the appliance for optimization. The two methods of redirecting packets are <b>Generic Route Encapsulation (GRE)</b> and <b>L2 redirection</b>.</p> <ul style="list-style-type: none"> <li>• <b>either</b> allows the appliance and the router to negotiate the best option. You always should select <b>either</b>. During protocol negotiation, if the router offers both GRE and L2 as redirection methods, the appliance will automatically select L2.</li> <li>• <b>GRE</b> (Layer 3 Generic Routing Encapsulation) allows packets to reach the appliance even if there are other routers in the path between the forwarding router and the appliance. At high traffic loads, this option might cause high CPU utilization on some Cisco platforms.</li> <li>• <b>L2</b> (Layer-2) redirection takes advantage of internal switching hardware that either partially or fully implements the WCCP traffic interception and redirection functions at Layer 2. Layer-2 redirection requires that the appliance and router be on the same subnet. It is also recommended that the appliance be given a separate subnet to avoid pass-through traffic from being redirected back to the appliance and causing a redirection/Layer-3 loop.</li> </ul>
<b>Group ID</b>	Refers to the Service Group ID.
<b>Interface</b>	Default value is <b>wan0</b> .
<b>Oper Status</b>	<p>Common states:</p> <ul style="list-style-type: none"> <li>• <b>INIT</b> - Initializing or down.</li> <li>• <b>ACTIVE</b> - This indicates that the protocol is established and the router has assigned hash/mask buckets to this appliance.</li> <li>• <b>BACKUP</b> - This indicates that the protocol is established, but the router has not assigned any hash/mask buckets to this appliance. This might be caused by using a Weight of 0.</li> <li>• <b>Designated</b> - This state (in addition to Active/Backup) indicates that the appliance is the designated web-cache for the group. The designator communicates with the router(s) to assign hash/mask assignments. When there is more than one appliance in a group, the appliance with the lowest IP becomes the designator for that group.</li> </ul>

Field	Description
<b>Protocol</b>	Although many more protocols are supported, generally <b>TCP</b> and <b>UDP</b> are the focus. For troubleshooting, you might consider adding a group for <b>ICMP</b> as well.
<b>Router IP</b>	IP address of the WCCP router. For Layer 2 redirection, use the physical IP address of the interface that is directly connected to the appliance. For Layer 3 redirection, consider using a loopback IP. It is not recommended to use VRRP or HSRP IPs as router IPs.

### Service Group Advanced Settings

Field	Description
<b>Assignment Detail</b>	<ul style="list-style-type: none"> <li>This field can be used to customize hash or mask values. If you have only one appliance, or if you are using route-map or subnet sharing to tunnelize, use the default <b>LAN-ingress</b> setting.</li> <li><b>WAN-ingress</b> and <b>LAN-ingress</b> are not applicable if there is only one active appliance.</li> <li><b>WAN-ingress</b> and <b>LAN-ingress</b> are also not applicable if you are using route-map or subnet sharing to tunnelize.</li> <li>If there is more than one active appliance and you are using <b>TCP-IP auto-optimization</b>: <ul style="list-style-type: none"> <li>Use <b>LAN-ingress</b> for WCCP groups that are used to redirect outbound traffic.</li> <li>Use <b>WAN-ingress</b> for WCCP groups that are used to redirect inbound traffic.</li> </ul> </li> <li>This ensures that a connection will go through the same appliance in both inbound and outbound directions and avoid asymmetry.</li> <li><b>custom</b> provides granular control of the distribution of flows. Contact Support for assistance.</li> </ul>
<b>Assignment Method</b>	Determines how redirected packets are distributed between the devices in a Service Group, effectively providing load balancing among the devices. The options are: <ul style="list-style-type: none"> <li><b>either</b>, which enables the appliance and router to negotiate the best method for assignment. This is preferred. If the router offers both <b>hash</b> and <b>mask</b> methods, the appliance will select the <b>mask</b> assignment method.</li> <li><b>hash</b>, for hash table assignment.</li> <li><b>mask</b>, for mask/value sets assignment.</li> </ul>
<b>Force L2 Return</b>	Generally is not selected. Normally, all Layer-3 redirected traffic that is not optimized (that is, it is pass-through) is returned back to the WCCP router as GRE (L3 return). Processing returned GRE traffic can create additional CPU overhead on the WCCP router. <b>Force L2 Return</b> can be used to override default behavior and route pass-through traffic back to the appliance's next hop router, which might or might not be the WCCP router. Use caution, as this could create a Layer 3 loop, if L2 returned traffic gets redirected back to the appliance by the WCCP router.

Field	Description
<b>Password</b>	This field is <i>optional</i> .
<b>Priority</b>	The lowest priority is <b>0</b> , and the default value is <b>128</b> . Only change this setting from the default if an interface has multiple WCCP service groups defined for the same protocol (for example, TCP) and you wish to specify which service group to use.
<b>Weight</b>	The default value is <b>100</b> . You can use this to influence WCCP hash/mask assignments for individual appliances when more than one appliance is in a cluster. For Active/Backup appliance configuration, use a Weight of <b>0</b> on the backup appliance.

The **Hash** and **Mask** areas are accessible only when you select **custom** in the **Assignment Detail** field.

## PPPoE Tab

*Configuration > Networking > PPPoE*

Point-to-Point Protocol over Ethernet (**PPPoE**) is a network protocol for encapsulating PPP frames inside Ethernet frames. It is used mainly with DSL services where individual users connect to a DSL modem over Ethernet.

Edit	Appliance	PPPoE Name	Ethernet Device	Details
#	Madrid-[redacted]	ppp0	lan1	(i)
#	Melbourne-[redacted]	ppp0	lan1	(i)
#	[redacted]			

When configuring a PPPoE connection, complete the following fields:

Field	Description
<b>Ethernet Device</b>	Specifies the physical interface to use for sending the protocol. Generally, this is a WAN-side interface.
<b>Password</b>	This is set up with your Internet Service Provider (ISP).
<b>PPPoE Name</b>	Name is <b>ppp</b> followed by a numerical suffix from <b>0</b> to <b>9</b> .
<b>User Name</b>	This is set up with your Internet Service Provider (ISP).

Generally, this is all the configuration required. If your ISP is fine-tuning the access, you might be asked to configure some of the **Optional Fields**, below.

**Add PPPoE - Paris**

PPPoE Name	ppp 0 ▾		
User Name	<input type="text"/>		
Password	<input type="password"/> ⚡		
Ethernet Device	wan0 ▾		
<b>Optional Fields</b>			
UNIT	0	Connect Timeout	30
LCP Failure	3	Connect Poll	2
LCP Interval	20	Service Name	<input type="text"/>
DNS Type	NOCHANGE ▾	ACNAME	<input type="text"/>
DNS1	0.0.0.0	Default Route	<input type="checkbox"/>
DNS2	0.0.0.0		

**Add** **Cancel**

Field	Description
<b>ACNAME</b>	Access Concentrator Name. Provided by the ISP.
<b>Connect Poll</b>	Specifies how many times to try to establish the link. The default value is <b>2</b> .
<b>Connect Timeout</b>	When trying to establish the link, this specifies how many seconds until the effort times out. The default value is <b>30</b> seconds.
<b>Default Route</b>	If the check box is selected, the connection uses the default gateway provided by the ISP.
<b>DNS Type</b>	This specifies the resolver to use: <ul style="list-style-type: none"> <li>• <b>NOCHANGE</b> - Do not accept or configure the ISP's Domain Name Server (DNS). Use the DNS configured on the <b>Administration &gt; General Settings &gt; Setup &gt; DNS</b> tab.</li> <li>• <b>SERVER</b> - Accept the ISP's DNS. This then overrides the EdgeConnect DNS configuration.</li> <li>• <b>SPECIFY</b> - Use <b>DNS1</b> and <b>DNS2</b> to resolve domain names.</li> </ul>
<b>LCP Failure</b>	<i>Link Control Protocol Failure.</i> Specifies the number of times the keep-alive can fail before the link goes down. The default value is <b>3</b> .
<b>LCP Interval</b>	The default value for this keep-alive interval is <b>20</b> seconds.
<b>Service Name</b>	Provided by the ISP.

## Loopback Interfaces

*Configuration > Networking > Loopback Interfaces*

The loopback feature enhances reliability and security by enabling you to access your network using a single static IP address. If one interface goes down, you can access all interfaces through the single static IP address.

To add a loopback interface to your network:

1. Navigate to **Configuration > Networking > Loopback Interfaces**.

The Loopback tab opens.

2. Click the edit icon next to the appliance to which you want to add a loopback interface.

The Loopback Interfaces dialog box opens.

3. Click **Add**.

The Add Interface dialog box opens.

4. Configure the following elements as needed:

Field	Description
<b>Segment</b>	Name of the segment, if enabled.
<b>Interface</b>	Name of the loopback interface.
<b>IP/Mask</b>	IP address for the loopback interface.
<b>Admin</b>	Select whether the admin status is up or down.
<b>Label</b>	Label of the loopback interface.
<b>Zone</b>	Zone you want to apply to your loopback interface.

5. Click **Add**.

## Loopback Orchestration

*Configuration > Networking > Loopback Orchestration*

You can create a pool of loopback addresses for Orchestrator to automatically create one or more loopback interfaces. You can also assign IP addresses from the pool to each appliance in the network. Complete the following steps to create the range for your loopback interfaces.

1. Select **+Add Loopback Interface**. The **Loopback Interface** window opens.
2. Specify the **Label** from the drop-down menu. This is optional. If no label is selected, "None" is assigned. Additionally, **Label** only displays the LAN side interface labels configured on the **Interface Labels** tab.
3. Specify the firewall zone if you want the loopback interface to be part of a specific firewall zone.
4. Select the management check box if you want the interface to be used by management applications running on the appliance.

**NOTE** You can only select one loopback interface as management if you configure multiple loopbacks.

5. Click **Add**.

The following table represents the fields for loopback orchestration.

Field	Description
<b>Segment</b>	Associated segment that has loopback orchestration applied.
<b>Label</b>	Label of the LAN interface being used.
<b>Zone</b>	Firewall zone associated with the loopback interface.
<b>Management IP</b>	Loopback interface selected as the management interface.
<b>Loopback Pool</b>	Pool of loopback addresses representing each device.
<b>Allocated / Total</b>	Number of loopback IP addresses allocated from the pool out of the total number of IP addresses in the pool.
<b>Deleted</b>	Number of loopback interfaces deleted. <b>NOTE</b> You can only delete an interface from an appliance in the Appliance Manager.

## Virtual Tunnel Interfaces

*Configuration > Networking > Virtual Tunnel Interfaces (VTI)*

A Virtual Tunnel Interface (VTI) is a tunneling protocol that does not require a static mapping of IPSec sessions to a physical interface. The tunnel endpoint is associated with a tunnel interface that enables a constant secure and stable connection throughout your network.

Click the **Edit** icon to get started configuring your VTIs.

### VTI Dialog Box

Complete the following steps to configure a VTI with an associated tunnel in Orchestrator.

1. Click **Add**.

The Add VTI Interface dialog box opens.

2. Complete the following fields with the appropriate information.

Field	Description
<b>Segment</b>	Name of the segment, if enabled.
<b>Interface</b>	ID of the VTI. <b>NOTE</b> IDs 20000 through 30000 are reserved for Orchestrator.
<b>Admin</b>	Select whether the interface is up or down.
<b>Status</b>	Status of the VTI tunnel.
<b>IP/Mask</b>	IP address and subnet mask of the VTI.
<b>Passthrough Tunnel</b>	Name of the passthrough tunnel associated with the VTI.
<b>Interface Type</b>	Interface type (lan or wan).
<b>Label</b>	If you want to apply a label to the VTI, select one from the list of those available.
<b>Zone</b>	Select the firewall zone to which the VTI should apply from the drop-down list.

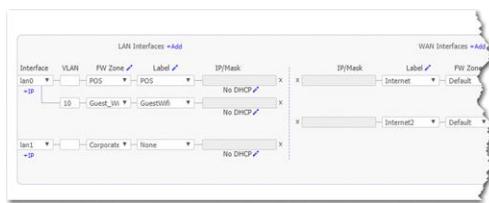
3. Click **Add**.

## DHCP Server Defaults

### *Configuration > Networking > DHCP Server Defaults*

You can reduce your workload by using this tab to configure global defaults for Dynamic Host Configuration Protocol (DHCP).

- These defaults apply to the LAN interfaces in **Deployment Profiles** that specify **Router** mode.
- There are three choices:
  - **No DHCP**.
  - Each LAN interface acts as a **DHCP Server**.
  - The EdgeConnect appliance acts as a **DHCP/BOOTP Relay** between a DHCP server at a data center and clients needing an IP address.
- On the **Configuration > Overlays & Security > Deployment Profiles** tab, the selected default displays consistently under each LAN-side IP/Mask field.



For any LAN-side interface, you can override the global default by clicking the DHCP-related link under the IP/Mask field and changing the values or selection.

- Changes you save to the global default only apply to new configurations.
- To view or revise the list of reserved subnets, select **Monitoring**.

## DHCP Settings

### DHCP Server

Field	Description
<b>DHCP Pool Subnet/Mask</b>	Enter the DHCP pool subnet and mask IP addresses.
<b>Subnet Mask</b>	Mask that specifies the default number of IP addresses reserved for any subnet. For example, entering <b>24</b> reserves 256 IP addresses.
<b>Exclude first N addresses</b>	Specifies how many IP addresses are not available at the beginning of the subnet's range.
<b>Exclude last N addresses</b>	Specifies how many IP addresses are not available at the end of the subnet's range.
<b>Default lease, Maximum lease</b>	Specify, in hours, how long an interface can keep a DHCP-assigned IP address.
<b>Default gateway</b>	Indicates whether the default gateway is being used.
<b>DNS server(s)</b>	Specifies the associated Domain Name System servers.
<b>NTP server(s)</b>	Specifies the associated Network Time Protocol servers.
<b>NetBIOS name server(s)</b>	Used for Windows (SMB) type sharing and messaging. It resolves the names when you are mapping a drive or connecting to a printer.
<b>NetBIOS node type</b>	NetBIOS node type of a networked computer relates to how it resolves NetBIOS names to IP addresses. There are four node types: <ul style="list-style-type: none"> <li>• <b>B-node</b> - 0x01 Broadcast</li> <li>• <b>P-node</b> - 0x02 Peer (WINS only)</li> <li>• <b>M-node</b> - 0x04 Mixed (broadcast, then WINS)</li> <li>• <b>H-node</b> - 0x08 Hybrid (WINS, then broadcast)</li> </ul>
<b>DHCP failover</b>	Enables DHCP failover. To set it up, click the <b>Failover Settings</b> link.

## DHCP/BOOTP Relay

Field	Description
<b>Destination DHCP/BOOTP Server</b>	IP address of the DHCP server assigning the IP addresses.
<b>Enable Option 82</b>	When selected, inserts additional information into the packet header to identify the client's point of attachment. This setting applies to all LAN-side interfaces on this appliance. <b>IMPORTANT:</b> Changing this setting will modify Option 82 settings on all LAN-side interfaces that are enabled as DHCP Relay.
<b>Option 82 Policy</b>	Tells the relay what to do with the hex string it receives. The choices are <b>append</b> , <b>replace</b> , <b>forward</b> , and <b>discard</b> . This setting applies to all LAN-side interfaces on this appliance. <b>IMPORTANT:</b> Changing this setting will modify Option 82 settings on all LAN-side interfaces that are enabled as DHCP Relay.

## DHCP Leases

*Configuration > Networking > DHCP Leases*

This tab lists the IP addresses that are currently being leased from the DHCP pool.

The screenshot shows the 'DHCP Leases' interface with the following details:

- Header: Dashboard, DHCP Leases (highlighted), DHCP Failover State, Export, Filter dropdown.
- Title: DHCP Leases ?
- Subtitle: 3 Rows
- Search bar: Search [ ]
- Table Headers: Appliance, Hostname, IP Address, Current State, MAC, Start Time, End Time.
- Table Data:
 

Appliance	Hostname	IP Address	Current State	MAC	Start Time	End Time
Woodstock-[redacted]	[redacted]	[redacted]	free	[redacted]	06-Sept-18 13:05	07-Sept-18 13:05
Woodstock-[redacted]	[redacted]	[redacted]	free	[redacted]	06-Sept-18 14:08	07-Sept-18 14:08
Woodstock-[redacted]	[redacted]	[redacted]	free	[redacted]	06-Sept-18 20:01	07-Sept-18 20:01

## DHCP Failover

On the DHCP Failover dialog box, configure the following settings to apply to your DHCP failover servers.

**NOTE** The DHCP Failover dialog box is accessed by clicking the **Failover Settings** link on the DHCP Server Defaults tab.

1. Select the **DHCP Failover** check box to enable the DHCP Failover feature.
2. Select whether you are configuring the failover settings for either the Primary or Secondary server.
3. Configure the remaining settings in the table below.

#### DHCP Failover Fields

Field	Description
<b>My IP</b>	IP address of the LAN interface.
<b>My Port</b>	Port number of the LAN interface.
<b>Peer IP</b>	IP address of the DHCP peer.
<b>Peer Port</b>	Port number of the DCHP peer.
<b>MLCT</b>	Optional. If selected, the default is 60 minutes. This field cannot be zero.
<b>SPLIT</b>	Optional. If selected, determines which peer (primary/secondary) should process the DHCP requests.
<b>Max Response Delay</b>	Optional. If selected, determines how many seconds the DHCP server can pass without receiving a message from its failover peer before it assumes the connection has failed.
<b>Max Unacked Updates</b>	Tells the remote DHCP server how many BNDUPD messages it can send before it receives a BNDACK from the local system.
<b>Load Balance Max Seconds</b>	Optional. Allows you to configure a cutoff after which load balancing is disabled. The cutoff is based on the number of seconds since the client sent its first DHCPDISCOVER or DHCPREQUEST message. It only works with clients that correctly implement the secs field.

## DHCP Failover State

*Configuration > Networking > DHCP Failover State*

EdgeConnect appliances can act as a DHCP server for clients on the LAN side. DHCP failover allows redundancy by creating failover groups when two appliances are combined in an HA configuration. DHCP failover also provides stability if one EdgeConnect appliance dies by allowing the other EdgeConnect HA pair to take over as the DHCP server. To do so, the primary and secondary servers must be completely synchronized so that each server can reply on the other if one fails.

This tab displays the DHCP failover peer states of each server for troubleshooting purposes.

### DHCP Failover State Fields

Field	Description
<b>Appliance</b>	Name of the EdgeConnect appliance that is part of the DHCP failover configuration.
<b>Failover Group Name</b>	Failover group name that is the same for all the tagged and untagged interfaces corresponding to one physical interface.
<b>My State</b>	Failover endpoint state of the selected primary appliance. The states are: <b>Normal, Communications-Interrupted, Partner-Down, Recover, Recover-wait, Recover-done</b> .
<b>My State Time</b>	Date and time when the selected appliance's DHCP server entered the specified state in the table.
<b>Partner State</b>	Failover endpoint state of the partner appliance. The states are: <b>Normal, Communications-Interrupted, Partner-Down, Recover, Recover-wait, Recover-done</b> .
<b>Partner State Time</b>	Date and time when the partner appliance entered the specified state in the table.
<b>MCLT</b>	Maximum client lead time: the maximum amount of time that one server can extend a lease for a client's binding beyond the time known by the partner.

## Link Aggregation

*Configuration > Networking > Link Aggregation*

The Link Aggregation tab displays channel group and link aggregation details for appliances selected in the appliance tree.

Appliance	Channel Groups	Channel Groups Status	Interfaces	MTU	LACP Mode	LACP Rate	LACP System Priorit...	Comment	State Details
appliance-one		down	lan1, lan2	1500	yes	slow	65535		
appliance-two	blan0	up							

Link aggregation combines data from multiple physical or virtual interfaces into a channel group, which provides a single high-speed link. Configuring link aggregation adds failover redundancy to the interfaces in the channel group.

**IMPORTANT:** If you aggregate interfaces that are currently in use, those interfaces are removed from deployment before aggregation occurs. When attempting to apply channel group additions or changes on the Link Aggregation dialog box, a confirmation dialog box opens that gives you the choice to proceed with aggregating the interfaces or to cancel your link aggregation changes.

The table on the Link Aggregation tab displays the following information:

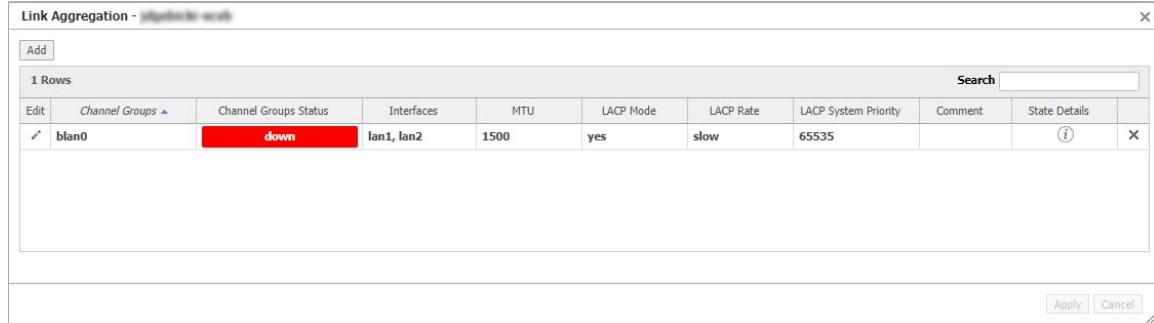
Column	Description
<b>Appliance</b>	Name of the EdgeConnect appliance.
<b>Channel Groups</b>	If any channel groups are configured for the appliance, the names of the channel groups are listed in this column. <b>NOTE</b> You can create up to four channel groups (bonded interfaces) for each appliance; two for the LAN side (blan0, blan1) and two for the WAN side (bwlan0, bwlan1).
<b>Channel Groups Status</b>	Status of the channel group (up or down). For dynamic mode (LACP mode), this status combines the LACP and link statuses. For static mode, it combines the link statuses of the underlying ports.
<b>Interfaces</b>	Physical or virtual interfaces included in the channel group. A channel group consists of one, two, three, or four interfaces. <b>NOTE</b> An interface can be part of only one channel group.
<b>MTU</b>	Maximum transmission unit (MTU) size (in bytes) configured for the channel group. The configured MTU overrides any existing MTU settings when the channel group is deployed. The default size is 1500 bytes.
<b>LACP Mode</b>	Indicates whether Link Aggregation Control Protocol (LACP) is enabled for the channel group (yes or no).
<b>LACP Rate</b>	Affects the timeout and the rate at which the LACP partner (switch) is requested to send LACPDU packets. <ul style="list-style-type: none"> <li>• For slow, one packet per 30 seconds, and timeout after 90 seconds. This is the default rate.</li> <li>• For fast, one packet per second, and timeout after three seconds.</li> </ul>
<b>LACP System Priority</b>	Priority number used to break ties with the LACP partner. This value can be set from 1 to 65535 with the lowest number having the highest priority. The default value is 65535.
<b>Comment</b>	Additional information about the channel group.

Column	Description
<b>State Details</b>	<p>Provides status information on the channel group, including details about the channel group (bonded interface) state and port (interface) states. Click the info icon to open a dialog box that displays this status information.</p> <ul style="list-style-type: none"> <li>The Channel group state tab on the dialog box includes three status indicators: Link status, LACP status, and Channel group status. (LACP status is displayed only in dynamic mode [LACP mode].) The Channel group status reflects the Link status and LACP status. If either is down, the Channel group status will be down. The LACP status reflects the LACP statuses on the Port states tab. If the LACP statuses of all interfaces are down, the LACP status on the Channel group state tab will be down.</li> <li>To refresh the status information on this dialog box, click <b>Refresh</b>.</li> <li>The State Details icon is also displayed in the table on the Link Aggregation dialog box. The same dialog box opens if you click it there.</li> </ul>

## Configure Link Aggregation

To add, change, or delete channel groups for an appliance, click the edit icon in the appropriate table row on the Link Aggregation tab.

The Link Aggregation dialog box opens.



The Channel Groups Status column displays the current status of the channel group (up, down, or pending). Pending status indicates that the link aggregation configuration has not yet been applied, and the state of the link aggregation is not known at this time.

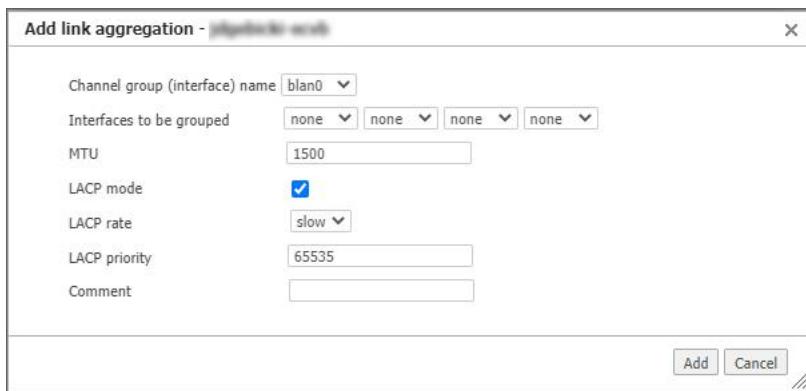
## Add or Modify a Channel Group

To add a channel group, perform the following steps:

**NOTE** To modify a channel group, click the edit icon next to the channel group. The Modify link aggregation dialog box opens. Change the fields as described below, and then click **Apply**. You cannot modify an existing channel group name, but you can change the other settings.

1. Click **Add** on the Link Aggregation dialog box.

The Add link aggregation dialog box opens.



2. Complete the following fields:

Field	Description
<b>Channel group (interface) name</b>	Select a name for the channel group from the drop-down list ( <b>blan0</b> , <b>blan1</b> , <b>bwan0</b> , or <b>bwan1</b> ).
<b>Interfaces to be grouped</b>	From the drop-down lists, select one, two, three, or four interfaces to include in the channel group. <b>IMPORTANT:</b> If you aggregate interfaces that are currently in use, those interfaces are removed from deployment before aggregation occurs. When you click the Apply button on the Link Aggregation dialog box, a confirmation dialog box opens that gives you the choice to proceed with aggregating the interfaces or to cancel your link aggregation changes.
<b>MTU</b>	Specify the MTU size (in bytes) to be applied to all interfaces in the group. The default size is 1500 bytes.
<b>LACP mode</b>	Select this check box to enable LACP for the channel group. By default, this check box is not selected.
<b>LACP rate</b>	Select <b>slow</b> or <b>fast</b> from the drop-down list. The default is slow. This field is available only if LACP mode is selected.
<b>LACP priority</b>	Specify a priority number from 1 to 65535. Priority number is used to break ties with the LACP partner. The lower the number, the higher the priority. The default is 65535. This field is available only if LACP mode is selected.
<b>Comment</b>	(Optional) Provide additional information about the channel group.

3. Click **Add**.

## Delete a Channel Group

To delete a channel group listed in the table on the Link Aggregation dialog box, click the corresponding delete icon (X) in the last column.

## Apply Your Changes

To apply your link aggregation configurations:

1. On the Link Aggregation dialog box, click **Apply**.

A confirmation dialog box opens.

**IMPORTANT:** If you aggregate interfaces that are currently in use, those interfaces are removed from deployment before aggregation occurs. This confirmation dialog box gives you the choice to proceed with aggregating the interfaces or to cancel your link aggregation changes.

2. Click **Aggregate Interfaces** to proceed. Otherwise, click **Cancel**.

## Regions

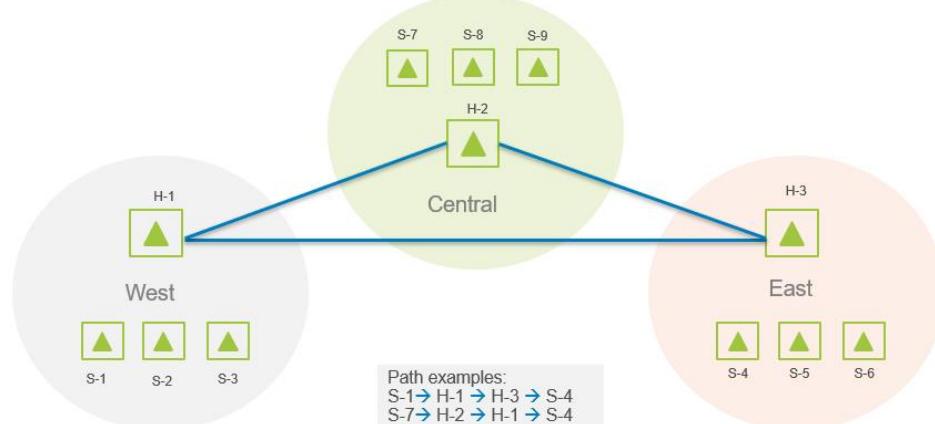
*Configuration > Overlays & Security > Regions*

Use this tab to add or remove regions from the SD-WAN fabric and configure regional routing. The regions within your SD-WAN fabric can represent geographical regions, administrative regions, or a set of sites in the network that have common business goals.

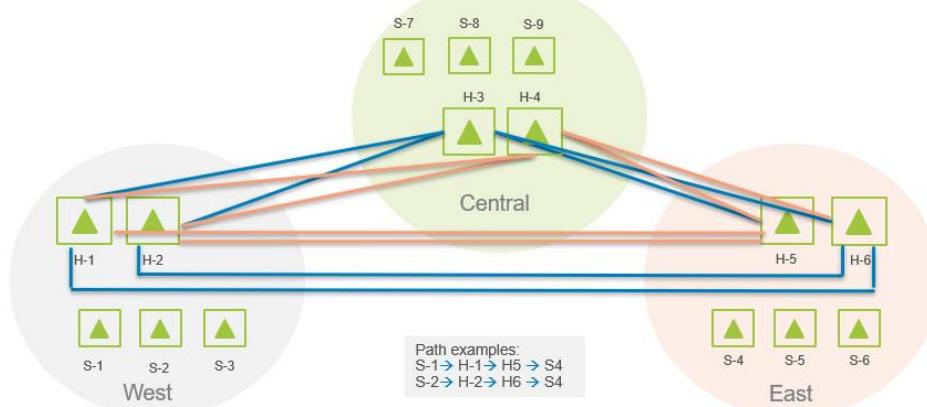
### Regional Routing

When enabled, regional routing enables you to manage your SD-WAN fabric by regions. It involves intra-region and inter-region route distribution across the SD-WAN fabric. The regions within your network can represent geographical regions, administrative regions, or a set of sites in the network that have common business goals. You can provide different Business Intent Overlay for each region by enabling regional routing and customizing BIOs per region. The following diagrams show examples of different regional network topologies you can build by enabling regional routing.

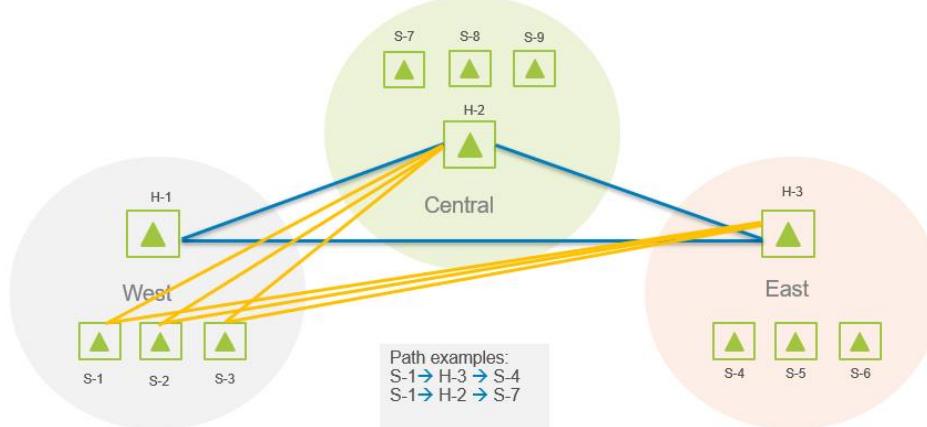
### REGIONAL BIO TOPOLOGY



## REGIONAL MULTI-HUB BIO TOPOLOGY



## OPTIMIZED REGIONAL BIO TOPOLOGY



You can enable regional routing within your Orchestrator UI. Navigate to the Regions tab and click **Enable Regional Routing**. The Regional Routing dialog box displays. Move the toggle to enable regional routing.

### View Status

Click **View Status** to view the status of the added or updated appliances to regions.

### Edit Regions

Complete the following steps to add a region or edit existing regions that you want to add to your overlays.

1. Click **Edit Regions**.
2. Click **New Region**.

3. Enter the name of your new region in the **Region Configuration** dialog box.
4. Click **Save**.

You can also edit an existing region.

1. Click the **Edit** icon next to the region you want to edit.
2. Enter the region name.
3. Click **Save**.

Navigate to the **Business Intent Overlay** tab to make further customizations to your regions and overlays.

## Routing Segmentation

*Configuration > Networking > Routing > Routing Segmentation (VRF)*

Use this tab to enable and disable routing segmentation across your network and apply unique configuration to your segments. Routing segmentation allows for the configuration of VRF (Virtual Routing and Forwarding)-style Layer 3 segmentation in your SD-WAN deployments. Note the following before configuring routing segmentation in Orchestrator:

- You must upgrade all EdgeConnect appliances and Orchestrator to version 9.0.
- All EdgeConnects must be configured to Inline Router mode.
- If a new appliance has been added to your network, or if an existing appliance has been replaced, you need to upgrade the appliance software to the appropriate version running in the network.
- After upgrading, segmentation is **disabled** by default. You will have to enable it on this tab.
- Regardless of whether segmentation is enabled or disabled, a **Default** segment is automatically created when you upgrade to 9.0.
- The system-generated Default segment cannot be deleted.
- After you enable routing segmentation, all existing configuration across your network is associated with the Default segment.

### Add a New Segment

Before adding a segment, you must enable segmentation by moving the toggle at the top of the page. If Routing Segmentation is not enabled, you cannot make any modifications to the Default segment or add any new segments.

To add a new segment, click **+Add Segment** and enter a **Segment Name**. You can make further specifications by clicking the edit icon or by selecting the **+Add** icon in any of the columns in the table.

## Segment Configuration

You can uniquely configure your segments by specifying the following on this page:

- Overlays & Breakout Policies
- Firewall Zone Policies
- Inter-Segment Routing & DNAT
- Inter-Segment SNAT
- Loopback

**NOTE** **Inter-Segment Routing & DNAT** and **Inter-Segment SNAT** are applicable only if you are using different segments.

The following sections provide more details.

### Overlays & Breakout Policies for Segments

Use this dialog box to configure overlays and breakout policies for your segments. This configuration determines the overlays used by each segment when traffic is originating from that segment and sent over the SD-WAN fabric to other sites. This configuration is also used when traffic breaks out locally to the Internet and Cloud Services using the Preferred Policy Order on the **Business Intent Overlay** (BIO) tab. For traffic to match what is on the specified BIO tab, ensure the following two conditions are true:

- BIO must include the defined segment policy
- The BIO match criteria must match the new flow

The overlays are arranged by priority defined in the **Match** field in the **Overlay Configuration** dialog box on the **BIO** page. You can specify if you want to include or skip the segment for each overlay by clicking **Include** or **Skip** icon in the table cell. By default, all overlays are included for all configured segments.

#### Include and Skip

If you want to skip an overlay, click the enabled **Include** icon and **Skip** appears grayed out. The segment will not be applied to the specified overlay. Click **Skip** again to include the segment; it will turn back to green. If an overlay is set to Skip, traffic will not match that overlay and moves to the next prioritized BIO. Additionally, if no BIOS match, traffic is dropped.

**TIP** If overlay is set to **Skip**, Flow Details on the **Flows** tab displays the list of skipped overlays.

### Firewall Zone Policies

Use this dialog box to enable and associate firewall zones to your segments. With segmentation enabled, firewall zone security policies are orchestrated and there is no need for Firewall Security Templates. After migration, deactivate the Security Policies Template in all Template Groups. If left active, the template will override any default-default segment security policies configured on this dialog box.

Before you begin Firewall Zone configuration, note the following:

- Review your existing security policies.
- Create a new security templates group with the new firewall zoning policies that only includes zones associated with LAN and WAN interfaces.
- Delete all rules in your previous Security Policy Template on the **Apply Template Groups** tab.
- Ensure you have selected the **Replace** option in the previous Security Policy Template.
- Save the previously used Security Policy Template. This deletes the security policy rules on your appliances.

Complete the following steps to set a rule or policy to your firewall zones within your segment.

1. Select the cell of the segment you want to update in the Matrix View. The **From Zone To Zone** dialog box opens.

**NOTE** If you are already in Table View, click **Add Rule**.

2. Enter the Source Segment in the **Source Segment** field. This is the segment that the firewall is starting from.
3. Enter the Destination Segment in the **Destination Segment** field. This is the segment where the firewall is going to.
4. Select **Add Rule**.
5. Complete the content in the table.

Field	Description
<b>Priority</b>	Enter the priority amount.
<b>Match Criteria</b>	Click the edit icon in this column to modify and create the match criteria for each zone.
<b>Action</b>	Select <b>Allow</b> or <b>Deny</b> to determine whether this zone will apply the selected segment.
<b>Enabled</b>	Select the check box to enable or clear it to disable.
<b>Logging</b>	Determines the filter for the zone-based firewall drop logging levels. You can select one of the following levels to apply: <b>None</b> , <b>Emergency</b> , <b>Alert</b> , <b>Critical</b> , <b>Error</b> , <b>Warning</b> , <b>Notice</b> , <b>Info</b> , or <b>Debug</b> .
<b>Tag</b>	Use tags to categorize or identify the purpose of a rule.
<b>Comment</b>	Any additional details about the firewall zone.

6. Click **Save**. The Save Segment Firewall Zone Policies dialog box opens.
7. Enter a comment (optional) in the **Audit Log Comment** field, and then click **Save**. Any text entered in the **Audit Log Comment** field appears on the Audit Logs tab.

**NOTE** Firewall zones are unique to each segment. For example, the default zone in Segment X will not be the same default zone in Segment Y.

## Inter-Segment Routing & DNAT

Use this dialog box to configure inter-segment routing and DNAT rules when traffic is crossing between segments. Click **+Add** and the **Inter-Segment Routing & DNAT** dialog box opens. Click **+Add Rule** and select any rule in the table to modify the following:

Field	Description
<b>Source Segment</b>	Name of the segment traffic is initiating from.
<b>Matches</b>	IP address got the source segment. This is used to match the packet destination IP address before the packet goes through DNAT.
<b>Destination IP</b>	
<b>Send to Segment</b>	Name of the segment the packets are translated to from the matched destination IP address.
<b>Translated Destination</b>	IP address of the DNAT IP address when the segment is translated.
<b>Enabled</b>	Whether or not this is enabled or disabled within your segment.
<b>Comment</b>	Any additional information.

## Inter-Segment SNAT

This dialog box enables you to enable source network address translation to your segments.

**NOTE** The default setting for SNAT is enabled for inter-segment traffic.

Field	Description
<b>Source</b>	Name of the segment that the SNAT is starting from.
<b>Destination</b>	Name of the segment that SNAT is translated to.
<b>SNAT</b>	Whether SNAT is enabled or disabled.

## Loopback

Click **+Add** and you are redirected to the **Loopback Orchestration** tab. Select the segment you want to apply a loopback interface from the table, and then click **+Add Loopback Interface**.

## Appliances

This column represents the amount of appliances the selected segment is enabled on.

## Comment

Click the cell in the **Comment** column to add a comment including any additional information for that particular segment.

## Delete a Segment

**WARNING** Segmentation involves drastic changes to your physical network. Deleting segments can be service affecting. Carefully read this section before deleting any of your segments.

Deleting a segment removes all the segmentation configuration from all the appliances within your network. When you delete a segment, Orchestrator automatically deletes the following:

- The segment's association with the overlay and break-out policies
- The intra-segment and inter-segment firewall zone policies
- The inter-segment routing & DNAT rules
- The inter-segment SNAT rule
- The loopback interfaces associated with the segment
- The VTI interfaces associated with the segment
- All the interface and VLAN interfaces

### **Manual Tasks to Complete Before Deleting a Segment**

The following configuration is disassociated from the segment and you need to manually delete the following:

- Any manual created tunnels
- BGP peers in the segment
- Internal subnet table rules
- Overlay ACL rules associated to the deleted segment

To delete a segment, click the **X** in the last column in the table. A Delete Routing Segment warning appears. Click **Delete** or **Cancel**.

### **Disable a Segment**

To disable routing segmentation across your network, you need to delete all configured segments in the network, except the default segment (which cannot be deleted). After all the segments are deleted, navigate to this tab and move the toggle at the top of the page to disable.

## **Management Services**

*Configuration > Networking > Routing > Management Services*

Use this tab to configure management services. You can configure them regardless of whether routing segmentation is enabled or disabled.

- When enabled, management services are functional in the associated segment based on the selected interface.
- When disabled, all the interfaces are available for configuration.

**NOTE** Management services still function if routing segmentation is not enabled in Orchestrator. In this case, you will be able to use the default configuration **only**; that is, **any** interface with the **Default** segment.

Starting with version 9.0, Orchestrator provides two tabs from which you can configure management services:

- Management Routes - Use this tab to configure static routes for management services traffic from an EdgeConnect appliance (egress traffic).
- Management Services - Use this tab to specify the source IP address of the interface used for each management service.

While it is recommended that you now use the Management Services tab to configure services, you can continue to use the Management Routes tab if you are not required to specify source IP addresses for management services.

The Management Services tab displays the following fields:

Field	Description
<b>Appliance</b>	Name of the appliance selected.
<b>Management Service</b>	Management service used by your appliance.
<b>Interface for Source IP Address</b>	IP address of the interface used by the management service. By default, management services are configured to use <b>any</b> source IP address. You can modify the interface for the Source IP address by updating this field for the corresponding management service.
<b>Source Segment</b>	Name of the associated segment applied to the management service when your source IP address is selected.

Click the edit icon associated with the management service you want to configure.

## Management Services Dialog Box

To configure a management service listed in this dialog box:

1. Click twice in the **Interface for Source IP Address** field associated with that service.

A drop-down list of all the interfaces configured for your appliance appears.

2. Select an interface.

The Source Segment field updates automatically with the associated segment.

3. Click **Save**.

If the Interface for Source IP Address field is set to **any**, there is no control over which source IP address will be used for management services egress packets. Depending on the route lookup, the corresponding source IP configured in the Management Routes table is used as the source IP of the packet. If the Source IP is not configured (0.0.0.0) in the Management Routes table for the selected route, the egress interface's IP address is used as the source IP address.

Descriptions of management service behaviors follow:

Service	Behavior
<ul style="list-style-type: none"> <li>• <b>HTTP(S)</b></li> <li>• <b>Cloud Portal</b></li> <li>• <b>Orchestrator</b></li> </ul>	<p>These services use the selected interface's Interface for Source IP Address as the source address to establish reachability and WebSocket connections to the Cloud Portal and Orchestrator. HTTP/HTTPS uses the Interface for Source IP Address for connection as well.</p> <p><b>CAUTION</b> If routing segmentation is enabled, make sure to provide Internet connectivity from the segment to the Interface for Source IP Address associated with the segment.</p>
<ul style="list-style-type: none"> <li>• <b>DHCP Relay</b></li> <li>• <b>NTP</b></li> <li>• <b>NetFlow</b></li> <li>• <b>RADIUS/TACACS+</b></li> <li>• <b>SNMP</b></li> <li>• <b>SSH</b></li> <li>• <b>Syslog</b></li> </ul>	<p>Each of these management services use Interface for Source IP Address as the source IP address. The source interface configured from the management route table is ignored if the Interface for Source IP Address is not "any".</p>

## Inter-Segment Routing and DNAT Exceptions

*Configuration > Networking > Routing > Inter-Segment Routing & DNAT Exceptions*

Use this tab to configure inter-segment routing and Destination NAT (DNAT) rules when traffic is crossing between segments. Click the edit icon to open the **Inter-Segment Routing & DNAT** dialog box. Click **+Add Rule** and select any rule in the table to modify or define the following:

Field	Description
<b>Source Segment</b>	Name of the segment that traffic is initiating from.
<b>Matches Destination IP</b>	IP address that matches the destination segment IP address, before DNAT. The IP address is included in the defined policy match criteria.
<b>Send to Segment</b>	Name of the segment the packets are translated to from the matched destination IP address. This is included in the set criteria.
<b>Translated Destination IP</b>	IP address of the DNAT IP address when the segment is translated. <b>NOTE</b> If DNAT is not needed, this field is empty.
<b>Enabled</b>	Indicates whether inter-segment DNAT is enabled or disabled within your segment.
<b>Comment</b>	Any additional information.

This only pushes the inter-segment DNAT exceptions to one appliance, selected in the Orchestrator appliance tree.

## Inter-Segment SNAT Exceptions

*Configuration > Networking > Routing > Inter-Segment SNAT Exceptions*

Use this tab to enable source network address translation to your segments. Select an appliance or group of appliances in the Orchestrator appliance tree to apply your Source NAT (SNAT) exceptions.

**NOTE** The default setting for SNAT is enabled for inter-segment traffic.

Field	Description
<b>Appliance</b>	Name of the appliance that the SNAT exception is being applied to.
<b>Source</b>	Name of the segment that the SNAT is starting from.
<b>Destination</b>	Name of the segment that the SNAT is translated to and going to.
<b>SNAT</b>	Indicates whether SNAT is enabled or disabled for the specified segment.
<b>Comment</b>	Any additional information.

## BGP Tab

*Configuration > Networking > Routing > BGP*

On this tab, you can configure **BGP (Border Gateway Protocol)** for appliances and add their BGP peers (also known as BGP "neighbors"). You can also add and modify peer-based advertisement and redistribution rules. EdgeConnect has the following behaviors relative to **communities**:

- Although EdgeConnect does not configure BGP communities, it propagates existing communities.
- Appliances can display up to ten communities per route.
- Appliances subnet-share communities with their EdgeConnect peers.
- Appliances advertise communities to remote peers, if learned from EdgeConnect peers.
- Appliances advertise communities to BGP neighbors.
- All BGP-learned subnets also appear in the appliance Routes table, displayed on the Routes configuration page. In addition, any AS Path or BGP Community information learned with a particular subnet will also be displayed with that subnet entry in the table.
- BGP route updates are not refreshed unless the peer specifically asks for it. To update the BGP routes, go to the **Peers** table and select **Soft Reset** in the desired row.
- BGP Equal-cost multi-path (ECMP) is supported for eBGP and iBGP. Multiple next-hops will be installed for the same prefix if all BGP path attributes are the same, enabling BGP to load balance egress traffic across multiple peers.

- A maximum of 64 BGP peers and 64 OSPF neighbors is supported per appliance, with 200 next-hops supported per interface.
- A small set of community numbers are used as internal communities that represent the source domain of a particular route:

Value	Description
100	Locally configured
101	Subnet shared (learned from another appliance)
102	Local BGP
103	Remote BGP (learned from another appliance)
104	Local OSPF
105	Remote OSPF (learned from another appliance)

These internal community values only use the appliance's local ASN in the ASN portion of the community. When the ASN portion of an attached community exactly matches the local ASN and the community portion exactly matches one of these internal values, they are flagged as internal communities only and stripped when advertising the route to BGP peers.

Click the **Summary** button on the BGP tab to display configuration details associated with the local appliance, such as its local AS number and router ID. Click the icon in the **BGP State Details** column to display a summary, including the number of routes learned and advertised via BGP by this appliance.

Click the **Peers** button on the BGP tab to display information about all configured peers for the appliances selected in the appliance tree. Click the icon in the **Peer Details** column to display the connection status of each peer that is configured for the appliance.

### Filter by Segment

To filter the rows displayed in the BGP table by segment:

- Select **Default** from the **Segment** drop-down list to display for the system-supplied default segment, or
- Select one of the other listed segments, which reflect the custom segments defined using Routing Segmentation (Configuration > Networking > Routing > Routing Segmentation (VRF)).

Select **All** to display for all segments, which is the default setting.

The table below describes the fields displayed for the BGP configuration.

Field	Description
<b>Appliance</b>	Name of the appliance.
<b>Segment</b>	Name of the segment being used, if enabled.
<b>Peer IP</b>	IP address of the EdgeConnect peer.

Field	Description
<b>Local Interface</b>	A list of the interfaces that can be chosen: <b>Any</b> , <b>lan0</b> , <b>wan0</b> , or <b>wan1</b> .
<b>Peer ASN</b>	Peer's Autonomous System Number.
<b>Peer State</b>	State of the peer. A peer state of <b>Established</b> indicates that full adjacency has been established and routes can be advertised to and learned from that peer.
<b>Soft Reset</b>	Click this button to manually request a route update from the BGP peer without resetting the session. This feature is available if you have enabled Soft Reconfiguration for this BGP peer.
<b>Soft Reconfiguration</b>	Indicates whether Soft Reconfiguration is enabled for this BGP peer.
<b>Established Time</b>	Final peer state that indicates neighbor connection as complete.
<b>Type</b>	Governs what kinds of routes the appliance is allowed to advertise to this BGP peer. These routes are itemized as Route Export Policies.
<b>Inbound Route Map</b>	Route map being used for the inbound traffic.
<b>Outbound Route Map</b>	Route map being used for the outbound traffic.
<b>Local Preference</b>	Local preference is the first attribute an EdgeConnect appliance looks at to determine which route towards a certain destination is the “best” one. This value is not exchanged between external BGP routers. Local preference is a discretionary BGP attribute. Default value is 100. The path with the highest local preference is preferred.
<b>MED</b>	<i>Multi Exit Discriminator.</i> When BGP chooses the best route to reach a certain destination, it first looks at the local preference and AS path attributes. When the local preference and AS path length are the same for two or more routes towards a certain prefix, the Multi Exit Discriminator (MED) attribute is chosen. With MED, the lowest value is preferred. <b>NOTE</b> If you configured the Metric Delta parameter in an earlier version of our software, this value has been translated into a MED value.
<b>Input Metric</b>	Metric that is advertised with the route when shared.
<b>Enable Imports</b>	Allows the learning of routes from this specific BGP peer.
<b>AS Prepend Count</b>	Learned path from an external prepend between a remote BGP site to local BGP peers.
<b>Next-Hop-Self</b>	Advertised route connected to a CE router that an EdgeConnect appliance learns from the eBGP with a PE router.
<b>Override ASN</b>	Indicates whether routes are advertised to the BGP peer where the BGP peer's own ASN is in the AS-Path.
<b>Keep Alive Timer</b>	Interval, in seconds, between keep alive signals to a peer.

Field	Description
<b>Hold Timer</b>	When availability to a peer is lost, this specifies how long to wait before dropping the session.
<b>BFD</b>	Indicates whether BFD is enabled for the BGP peer. This field is set to N/A if BFD is not supported on the appliance.
<b>Adjacency</b>	Indicates the adjacency of the BGP peer (Single-Hop or Multi-Hop). This field is set to N/A if BFD is not supported on the appliance.
<b>Peer Details</b>	Additional details about the peer or its state.

To edit the BGP configuration for one of the listed appliances, click the edit icon in the left column of the table.

## BGP Information

Use this window to enable BGP for your appliances and to configure BGP peers. Complete the following steps to start BGP configuration.

1. Move the toggle to **Enable BGP**.
2. Complete the following fields.

Field	Description
<b>Autonomous System Number (ASN)</b>	Configure this number as needed for your network.
<b>Router ID</b>	This router identifier is the IPv4 address by which the remote peer can identify this appliance for purposes of BGP.
<b>Graceful Restart</b>	<p>Enable receiver-side graceful restart capability. EdgeConnect retains routes learned from the peer and continues to use it for forwarding (if possible) if/when a BGP peer goes down. The retained routes are considered stale routes. They will be deleted and replaced with newly received routes.</p> <ul style="list-style-type: none"> <li>• <b>Max Restart Time</b> – Specifies the maximum time (in seconds) to wait for a Graceful Restart capable peer to come back after a peer restart or peer session failure.</li> <li>• <b>Stale Path Time</b> – Specifies maximum time (in seconds) following a peer restart that EdgeConnect waits before removing stale routes associated with that peer.</li> </ul>
<b>AS Path Propagate</b>	Select this check box to enable this appliance to send the full AS path, associated with a prefix to other routers and appliances, avoiding routing loops. This will provide the learned path from an external prepend between a remote BGP site to local BGP peers.

To add a BGP peer, select **Add**. The Add Peer dialog box opens.

## Add Peer

Complete the following fields to add a BGP peer.

Field	Description
<b>Peer IP</b>	IP address of the EdgeConnect peer.
<b>Peer Adjacency</b>	To specify the adjacency of the BGP peer, click <b>Single-Hop</b> or <b>Multi-Hop</b> . Single-Hop is the default selection. This field is not displayed if BFD is not supported on the appliance.
<b>Local Interface</b>	You can specify the source address or interface for a specific BGP peer. Select the interface from the drop-down list: <b>any</b> , <b>lan0</b> , <b>wan0</b> , or <b>wan1</b> .
<b>Peer ASN</b>	Replace all ASNs in the AS-Path of routes advertised to this peer with the appliance ASN.
<b>Override ASN</b>	Select this check box to advertise routes to the BGP peer where the BGP peer's own ASN is in the AS-Path. All instances of the BGP peer ASN are replaced with the local ASN of the appliance in all routes advertised to the BGP peer.
<b>Peer Type</b>	Select the type of peer from the drop-down list: <b>Branch</b> or <b>PE-router</b> .
<b>Admin Status</b>	Select whether you want the Admin Status <b>UP</b> or <b>DOWN</b> .
<b>Soft Reconfiguration</b>	Select this check box to prevent the appliance from sending a route-refresh message to the BGP peer when a policy is changed. When enabled, the appliance will apply policy changes against BGP peer learned routes stored in memory. To request a route update from the peer, click the <b>Soft Reset</b> button for the peer on the BGP tab.
<b>Next-Hop-Self</b>	Select this check box to enable the next-hop-self.
<b>Inbound route map</b>	Route map for inbound traffic. Select the edit icon to load or configure inbound route maps.
<b>Outbound route map</b>	Route map for outbound traffic. Select the edit icon to load or configure outbound route maps.
<b>BFD</b>	Select this check box to enable BFD for the BGP peer. This field is not displayed if BFD is not supported on the appliance. <b>NOTE</b> Before you select this check box, enable and configure BFD from the BFD tab.
<b>Keep Alive Timer</b>	Interval, in seconds, between keep alive signals to a peer.
<b>Hold Timer</b>	Specified time to wait before dropping the session when the reachability to a peer is lost.
<b>Enable MD5 Password</b>	Select this check box to add a password to authenticate the TCP session with the peer.

## BGP Inbound and Outbound Route Redistribution Maps

Route Maps are policies applied to IP routes during redistribution between routing protocols. They have **Match Criteria** and **Set Actions** that allow for filtering routes or modifying metrics and attributes for routes that meet the criteria defined in the match statement. Route-map rules follow a top-down order based on the sequence number defined for each entry.

EdgeConnect Enterprise supports applying Route Maps inbound from and outbound to BGP peers and outbound to OSPF neighbors and the SD-WAN Fabric. It is best practice to use Orchestrator to apply Route Maps using templates.

You can specify up to 20 BGP inbound route maps, 20 BGP outbound route maps, and 128 rules per route map.

You can specify up to 6 comma separated prefixes for each rule applied to a route map.

You can add, delete, rename, or clone route maps using this window. You can add rules to your route map by clicking **Add Rule**. A route map without any enabled rules is treated as a default deny all.

## Prefix Match Criteria

The default for prefix match criteria is exact-match + greater-than. Both the specified prefix and any subnets of that prefix will be matched, up to a length of 32 for IPv4 or 128 for IPv6 (subnet sharing route maps only).

Less-than-or-equal-to (LE) and greater-than-or-equal-to (GE) clauses can also be applied to specify the inclusion of certain subnets.

To match a default-route, deny 0.0.0.0/1, deny 128.0.0.0/1, and then permit any.

### GE Clause

If a GE clause is applied, the rule will also include all prefixes that have a prefix length greater than or equal to the GE value and less than or equal to 32 or 128 (for IPv6).

Example: A.B.C.D/X GE Y

In this example the following will be included:

- The exact match to A.B.C.D/X
- All the prefixes that belong to the subnet A.B.C.D/X that have a length greater than or equal to Y and less than or equal to 32

## LE Clause

If an LE clause is applied, the rule will also include all prefixes that have a prefix length less than or equal to the LE value.

Example: A.B.C.D/X LE Y

In this example the following will be included:

- The exact match to A.B.C.D/X
- All the prefixes that belong to the subnet A.B.C.D/X that have a length greater than or equal to X and less than or equal to 32
- All the prefixes that belong to the subnet A.B.C.D/X that have a length less than or equal to Y

## Combining LE and GE Clauses

Example: A.B.C.D/X LE Y GE Z

In this example the following will be included:

- The exact match to A.B.C.D/X
- All the prefixes that belong to the subnet A.B.C.D/X that have a length less than or equal to Y
- All the prefixes that belong to the subnet A.B.C.D/X that have a length greater than or equal to Z and less than or equal to 32

## Exact Match

If both GE and LE clauses are specified and are equal, the rule will result in an exact match.

Example: A.B.C.D/X LE Y GE Y

In this example, the following will be included:

- The exact match to A.B.C.D/X
- The exact match to the subnet A.B.C.D/X that has a length equal to Y

You can specify the following fields in each rule for the selected route map.

### *Priority (Inbound and Outbound)*

Field	Description
<b>Priority</b>	<ul style="list-style-type: none"> <li>If you are using Orchestrator templates to add rules, Orchestrator will delete all entries from <b>1000 - 9999</b> before applying its policies.</li> <li>You can create rules with higher priority than Orchestrator rules (<b>1 - 999</b>) and rules with lower priority (<b>10000 - 19999</b> and <b>25000 - 65534</b>).</li> </ul> <p><b>NOTE</b> The priority range from <b>20000</b> to <b>24999</b> is reserved for Orchestrator.</p> <ul style="list-style-type: none"> <li>When adding a rule, the priority is incremented by 10 from the previous rule. The priority can be changed, but this default behavior helps to ensure you can insert new rules without having to change subsequent priorities.</li> </ul>

### *Select Match Criteria (Inbound)*

Source Protocol	Complete the Following Fields (based on protocol selected)
<b>BGP</b>	<ul style="list-style-type: none"> <li>Prefix + optional LE/GE parameters</li> <li>BGP Communities</li> </ul>

### *Select Match Criteria (Outbound)*

Source Protocol	Complete the Following Fields (based on protocol selected)
<b>Local/Static</b>	<ul style="list-style-type: none"> <li>Prefix + optional LE/GE parameters</li> </ul>
<b>SD-WAN (Local/Static)</b>	<ul style="list-style-type: none"> <li>Prefix + optional LE/GE parameters</li> <li>BGP Communities</li> </ul>
<b>BGP</b>	<ul style="list-style-type: none"> <li>Prefix + optional LE/GE parameters</li> <li>BGP Communities</li> </ul>
<b>OSPF</b>	<ul style="list-style-type: none"> <li>Prefix + optional LE/GE parameters</li> <li>OSPF Tag</li> </ul>
<b>SD-WAN (BGP)</b>	<ul style="list-style-type: none"> <li>Prefix + optional LE/GE parameters</li> <li>BGP Communities</li> </ul>
<b>SD-WAN (OSPF)</b>	<ul style="list-style-type: none"> <li>Prefix + optional LE/GE parameters</li> <li>OSPF Tag</li> <li>BGP Communities</li> </ul>

### *Set Actions (Inbound and Outbound)*

Field	Description
<b>Permit</b>	Enable or disable. This setting allows or denies the route map.
<b>BGP Local Preference</b>	Best BGP destination. The default value is 100.
<b>Metric</b>	Metric for the route.
<b>BGP Communities</b>	Label of extra information that is added to one or more prefixes advertised to BGP neighbors. There are three options for how this information is added: <b>Append</b> – Click to add this information to the prefix when the route is advertised to BGP neighbors. <b>Override</b> – Click to replace the communities in the route with the community specified. <b>Remove</b> – Click to remove this information from the prefix when the route is advertised to BGP neighbors.
<b>Nexthop</b>	Advertised route connected to a CE router that an EdgeConnect appliance learns from the eBGP with a PE router.
<b>ASN Prepend Count</b>	Original route path that was used. <b>NOTE</b> This field is displayed only for the Outbound redistribution map.
<b>Comment</b>	Comment you want to include.

The following table describes the redistribution commands supported in the BGP routing protocol.

Command	Redistribution Support
<b>Match prefix</b>	Yes
<b>Set metric</b>	Yes
<b>Set tag</b>	Yes

## BGP ASN Global Pool

### *Configuration > Networking > Routing > BGP ASN Global Pool*

Use this dialog box to configure the ASN Range to assign Autonomous System Numbers (ASNs) for new appliances. Note the following before configuration:

- ASNs are applied only to new appliances. The ASNs configured in this dialog box do not impact or change any previous or manually configured ASNs.
- ASN Range is configured for Default Segment and cannot be changed.
- ASN Orchestration assigns the same ASN to EdgeHA appliances.
- ASN Orchestration assigns the same ASN to appliances with same site name.

Enter the start and end ranges for the ASNs. Click the **+Add Reserved ASN** to exclude any ASNs from being applied to an appliance. You can reassign ASNs manually by using the BGP tab.

## Routes Tab

*Configuration > Networking > Routing > Routes*

Each appliance builds a route table with entries that are added automatically by the system, added manually by a user, or learned from a routing protocol (SD-WAN Fabric Subnet Sharing, BGP, or OSPF).

### Route Maps

Route Maps are policies applied to IP routes during redistribution between routing protocols. They have **Match Criteria** and **Set Actions** that allow for filtering routes or modifying metrics and attributes for routes that meet the criteria defined in the match statement. Route-map rules follow a top-down order based on the sequence number defined for each entry.

EdgeConnect Enterprise supports applying Route Maps inbound from and outbound to BGP peers and outbound to OSPF neighbors and the SD-WAN Fabric. It is best practice to use Orchestrator to apply Route Maps using templates.

Route mapping is supported for the following protocols and the direction of those protocols:

- Local, static to SD-WAN fabric
- BGP, OSPF to SD-WAN fabric
- SD-WAN fabric to BGP Outbound peers
- Local, BGP, OSPF to BGP outbound peers
- Local BGP Peers to EdgeConnect BGP sessions

The following table lists the routing protocols and the associated commands supported.

Command	Redistribution Support	BGP	OSPF	SD-WAN	Local/Static
<b>Match prefix</b>	Yes	Yes	Yes	Yes	Yes
<b>Set metric</b>	Yes	Yes	Yes	Yes	Yes
<b>Set tag</b>	Yes	Yes	Yes	Yes	Yes

You can filter the type of routes displayed by clicking **All**, **Local / Static**, **SD-WAN Fabric**, **BGP**, or **OSPF**.

### Import

Click **Import** to import route details from a CSV file into the selected appliance. Each row in the CSV file should contain values for the following fields in the exact order specified with commas to separate values:

- Subnet
- Mask Length
- Metric
- Is Local (*no longer used; leave this value blank*)
- Advertise to Silver Peak Peers (*no longer used; leave this value blank*)
- Advertise to BGP Peers (*no longer used; leave this value blank*)
- Next Hop
- Advertise to OSPF Neighbors (*no longer used; leave this value blank*)
- Interface Name
- Segment

**NOTE** Do not include a header row in the CSV file. Also, do not add spaces after commas in rows.

The following lines illustrate what two rows in a CSV import file might look like:

```
10.1.0.0,16,50,,,10.1.0.1,,lan0,Default  
10.2.0.0,16,50,.....
```

## Export

Click **Export** to save the contents of the Routes table to a CSV file.

### Filter by Subnet

To filter the routes displayed in the Routes table by subnet, enter the subnet in the **Filter by subnet** field, and then click **Apply**.

### Filter by Segment

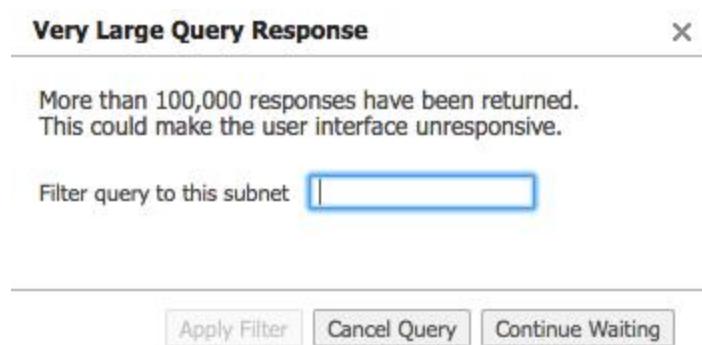
To filter the routes displayed in the Routes table by segment:

- Select **Default** from the **Segment** drop-down list to display for the system-supplied default segment, or
- Select one of the other listed segments, which reflect the custom segments defined using Routing Segmentation (Configuration > Networking > Routing > Routing Segmentation (VRF)).

Select **All** to display for all segments, which is the default setting.

A **Very Large Query Response** pop-up will display if the number of the routes filtered exceeds 500,000. You can filter by subnet and/or segment, or you can cancel or continue waiting to help mitigate this issue.

**NOTE** If the number of the routes filtered is greater than 500,000 the following pop-up will display.



## Segment

The segments you have configured on the Routing Segmentation tab are listed in the Segment field. After you specify the segment, the Routes table displays only the routes belonging to that segment.

The following information is displayed for each route listed in the table:

Field	Description
<b>Appliance</b>	Name of the appliance.
<b>Segment</b>	Routes displayed belonging to this segment.
<b>Subnet/Mask</b>	Actual subnet to be shared or learned.
<b>Next Hop</b>	Next hop IP address for the route. A maximum of 200 next-hops are supported per logical interface.
<b>Interface</b>	Interface for outgoing traffic. Display only.
<b>Zone</b>	Firewall zone associated with the route.
<b>State</b>	Shows whether the route is up or down.
<b>Metric</b>	Metric of the subnet. Value must be between 0 and 100. When a peer has more than one tunnel with a matching subnet (for example, in a high availability deployment), it chooses the tunnel with the lower numerical value.
<b>Advertise to Peers</b>	Select to share subnet information with categories of peers. Select from the following options: <ul style="list-style-type: none"> <li>• <b>Advertise to Silver Peak Peers</b></li> <li>• <b>Advertise to BGP Peers</b></li> <li>• <b>Advertise to OSPF Peers</b></li> </ul> Peers then learn the subnets. To add a subnet to the table without divulging it to peers, clear this option.

Field	Description
Type	<p>Indicates one of the following route types:</p> <ul style="list-style-type: none"> <li>• <b>Auto (System)</b> – Automatically added subnets of interfaces on this appliance.</li> <li>• <b>Auto (SaaS)</b> – Automatically added subnets from SaaS services.</li> <li>• <b>Added by user</b> – Subnets manually added or configured on this appliance.</li> <li>• <b>SP: Hostname</b> – Subnets added by exchanging information with peer appliances. If the peer has learned the subnet from a remote BGP or OSPF peer, that information is appended.</li> <li>• <b>&lt;BGP peer Type&gt;: &lt;BGP peer ip&gt;</b> – Subnets added by exchanging information with local BGP peers.</li> <li>• <b>OPSF: OSPF neighbor IP</b> – Subnets added by exchanging information with local OSPF peers.</li> </ul>
Additional Info	<p>Indicates any tags for restricting route lookups:</p> <ul style="list-style-type: none"> <li>• <b>Tag FROM LAN</b> – Used to restrict route lookups to traffic arriving on a LAN-side interface.</li> <li>• <b>Tag FROM WAN</b> – Used to restrict route lookups to traffic arriving on a WAN-side interface.</li> </ul>
Comment	Any additional information you would like to include.

To edit a route, select the edit icon in the Routes table.

### Route Table Lookup Criteria

Each Route table has lookup criteria that is used in the following order:

- Longest Prefix Match
- Route Table admin distance of the source protocol (lower the better)
- Metric (lower the better)
- Use peer priority (if configured) as a tie-breaker

If there are two or more routes that match all the above criteria, use multiple routes.

### Admin Distance Configuration

You can configure the admin distance by using the Admin Distance template on the **Templates** tab. The default settings in this template determine the most reliable route with the use of admin distance. See the table below for the various default admin distances per route type.

Route Type	Default Admin Distance
Local	1
SD-WAN Fabric - Static	10
SD-WAN Fabric - BGP	15
SD-WAN Fabric - OSPF	15
eBGP	20

Route Type	Default Admin Distance
OSPF	110
iBGP	200

Navigate to the **BGP** and **OSPF** tabs for more information about applying or configuring your route maps.

## Edit or Add Routes

The following table describes the elements in the Routes dialog box. They represent various features you can apply to your route.

Field	Description
<b>Automatically advertise local LAN subnets</b>	Indicates whether the system-created LAN subnets of your appliance should be advertised to your peers.
<b>Automatically advertise local WAN subnets</b>	Indicates whether the system-created local WAN subnets of your appliance should be advertised to your peers.
<b>Metric for automatically added routes</b>	Metric assigned to subnets of interfaces on this appliance. Specify a value from 0 to 100. The default value is 50. When a peer has more than one tunnel with a matching subnet (for example, in a high-availability deployment), it chooses the tunnel with the lower metric value.
<b>Redistribute routes to SD-WAN fabric</b>	Route redistribution map for the SD-WAN fabric. Click the edit icon next to this field and specify the appropriate route redistribution map.
<b>Filter routes from SD-WAN fabric with matching local ASN</b>	Indicates whether to filter routes from the SD-WAN fabric with matching local Autonomous System Number (ASN).
<b>Include BGP local ASN to routes sent to SD-WAN fabric</b>	Indicates whether all routes must carry local ASN over subnet sharing to remote EdgeConnect peers.
<b>Tag BGP communities to routes</b>	<p>Send the specified communities with routes that are advertised to both SD-WAN fabric peers and BGP peers, if the routes are learned from any of the following source protocols:</p> <ul style="list-style-type: none"> <li>• Local/Static</li> <li>• SD-WAN (Local/Static)</li> <li>• SD-WAN (BGP)</li> <li>• SD-WAN (OSPF)</li> </ul> <p>If you select this option, enter the BGP communities you want to be tagged in the field.</p>
<b>Communities</b>	BGP communities to share. A community must be a combination of two numbers (0 to 65535) separated by a colon. For multiple communities, use a comma to separate them. You can have up to nine communities per route shared with subnet sharing. <i>Subnet sharing</i> is the protocol used to exchange routes between EdgeConnect appliances across the SD-WAN fabric.
<b>Use SD-WAN fabric learned routes</b>	Indicates whether to use SD-WAN fabric learned routes.

Field	Description
<b>Enable Equal Cost Multi Path (ECMP)</b>	Indicates whether you want to enable Equal Cost Multi-Path routing support.

## Add Routes

Use the Add Routes dialog box to add a user-defined route to an appliance's route table.

1. In the Routes dialog box, click **Add Routes**.

The Add Route dialog box opens.

2. Configure the following elements as needed.

Field	Description
<b>Subnet/Mask</b>	Subnet IP address and mask (for example, 4.4.4.4/32).
<b>Next Hop</b>	Next hop IP address for the route. If you specify a next hop, you cannot select a zone for the route. (Optional)
<b>Interface</b>	Interface for outgoing traffic. Click in the field and select the appropriate interface. If you specify an interface, you cannot select a zone for the route. (Optional)
<b>Zone</b>	Firewall zone to apply to the route. Select the appropriate firewall zone from the drop-down list. Initially, this field is set to Default. If you specify a next hop or an interface, you cannot select a zone for the route; the field automatically sets to None and cannot be changed. (Optional)
<b>Metric</b>	Metric for the subnet. Specify a value from 0 to 100. When a peer has more than one tunnel with a matching subnet (for example, in a high-availability deployment), it chooses the tunnel with the lower metric value. The default value is 50.
<b>Tag</b>	Tag for restricting route lookups. It is primarily used to filter routes from being redistributed in a routing loop. Select one of the following options from the drop-down list: <ul style="list-style-type: none"> <li>• <b>ANY</b> – Allows route lookups for traffic arriving on a LAN-side or WAN-side interface.</li> <li>• <b>FROM_LAN</b> – Restricts route lookups to traffic arriving on a LAN-side interface.</li> <li>• <b>FROM_WAN</b> – Restricts route lookups to traffic arriving on a WAN-side interface.</li> </ul>
<b>Comments</b>	Additional information you want to provide about this route. (Optional)

3. Click **Add**.

## Import Subnets

Do the following to import route details from a CSV file into the selected appliance.

1. Click **Choose File**.
2. Locate and select the CSV file on your local machine, and then click **Open**.
3. Click **Import**.

Orchestrator imports the information from the selected file and the Routes table displays new or updated route details.

## SD-WAN Fabric Route Redistribution Maps

Route Maps are policies applied to IP routes during redistribution between routing protocols. They have **Match Criteria** and **Set Actions** that allow for filtering routes or modifying metrics and attributes for routes that meet the criteria defined in the match statement. Route-map rules follow a top-down order based on the sequence number defined for each entry.

EdgeConnect Enterprise supports applying Route Maps inbound from and outbound to BGP peers and outbound to OSPF neighbors and the SD-WAN Fabric. It is best practice to use Orchestrator to apply Route Maps using templates.

You can specify up to 20 SD-WAN route maps and 128 rules per route map.

You can specify up to 6 comma separated prefixes for each rule applied to a route map.

You can add, delete, rename, or clone route maps using this window. You can add rules to your route map by clicking **Add Rule**. A route map without any enabled rules is treated as a default deny all.

### Prefix Match Criteria

The default for prefix match criteria is exact-match + greater-than. Both the specified prefix and any subnets of that prefix will be matched, up to a length of 32 for IPv4 or 128 for IPv6 (subnet sharing route maps only).

Less-than-or-equal-to (LE) and greater-than-or-equal-to (GE) clauses can also be applied to specify the inclusion of certain subnets.

To match a default-route, deny 0.0.0.0/1, deny 128.0.0.0/1, and then permit any.

### GE Clause

If a GE clause is applied, the rule will also include all prefixes that have a prefix length greater than or equal to the GE value and less than or equal to 32 or 128 (for IPv6).

Example: A.B.C.D/X GE Y

In this example the following will be included:

- The exact match to A.B.C.D/X
- All the prefixes that belong to the subnet A.B.C.D/X that have a length greater than or equal to Y and less than or equal to 32

## LE Clause

If an LE clause is applied, the rule will also include all prefixes that have a prefix length less than or equal to the LE value.

Example: A.B.C.D/X LE Y

In this example the following will be included:

- The exact match to A.B.C.D/X
- All the prefixes that belong to the subnet A.B.C.D/X that have a length greater than or equal to X and less than or equal to 32
- All the prefixes that belong to the subnet A.B.C.D/X that have a length less than or equal to Y

## Combining LE and GE Clauses

Example: A.B.C.D/X LE Y GE Z

In this example the following will be included:

- The exact match to A.B.C.D/X
- All the prefixes that belong to the subnet A.B.C.D/X that have a length less than or equal to Y
- All the prefixes that belong to the subnet A.B.C.D/X that have a length greater than or equal to Z and less than or equal to 32

## Exact Match

If both GE and LE clauses are specified and are equal, the rule will result in an exact match.

Example: A.B.C.D/X LE Y GE Y

In this example, the following will be included:

- The exact match to A.B.C.D/X
- The exact match to the subnet A.B.C.D/X that has a length equal to Y

You can specify the following fields in each rule for the selected route map.

*Priority*

Field	Description
<b>Priority</b>	<ul style="list-style-type: none"> <li>If you are using Orchestrator templates to add rules, Orchestrator will delete all entries from <b>1000 - 9999</b> before applying its policies.</li> <li>You can create rules with higher priority than Orchestrator rules (<b>1 - 999</b>) and rules with lower priority (<b>10000 - 19999</b> and <b>25000 - 65534</b>).</li> </ul> <p><b>NOTE</b> The priority range from <b>20000</b> to <b>24999</b> is reserved for Orchestrator.</p> <ul style="list-style-type: none"> <li>When adding a rule, the priority is incremented by 10 from the previous rule. The priority can be changed, but this default behavior helps to ensure you can insert new rules without having to change subsequent priorities.</li> </ul>

*Select Match Criteria*

Source Protocol	Complete the Following Fields (based on protocol selected)
<b>Local/Static</b>	<ul style="list-style-type: none"> <li>Prefix + optional LE/GE parameters</li> </ul>
<b>BGP</b>	<ul style="list-style-type: none"> <li>Prefix + optional LE/GE parameters</li> <li>BGP Communities</li> </ul>
<b>OSPF</b>	<ul style="list-style-type: none"> <li>Prefix + optional LE/GE parameters</li> <li>OSPF Tag</li> </ul>

**NOTE** The above fields in the right column will change depending on the source protocol chosen.

*Set Actions*

Field	Description
<b>Permit</b>	Enable or disable. This setting allows or denies the route map.
<b>OSPF Tag</b>	Value of OSPF tag to set in routing information sent to destination. <b>NOTE</b> This field is displayed only if Source Protocol is set to OSPF.
<b>Metric</b>	Metric for the route.
<b>Comment</b>	Comment you want to include.

## OSPF Tab

*Configuration > Networking > Routing > OSPF*

This tab manages **OSPF (Open Shortest Path First)** on LAN and WAN interfaces.

OSPF learns routes from routing peers, and then subnet shares them with EdgeConnect peers and/or BGP neighbors.

A route tag is applied to a route to better identify the source of the network it originated from. It is primarily used to filter routes from being redistributed in a routing loop.

A maximum of 64 OSPF neighbors and 64 BGP peers is supported per appliance, with 200 next-hops supported per interface.

- For BGP, only 64 peers can be added. For OSPF, more than 64 neighbors can be added, though an error will be logged.
- If more than 64 OSPF neighbors are added, the active OSPF neighbors are chosen in a deterministic manner. All OSPF neighbors that are added are queried in a sorted order using segment ID as the primary index and the neighbor IP address as the secondary index. For example, if there are 65 OSPF neighbors, the peer in the highest segment and with the highest IP address will be the one that is always dropped. It will not drop a random OSPF neighbor.
- Also, if there are 60 OSPF neighbors in the default segment, which always has ID:0, and 10 OSPF neighbors in segment 1, the 60 neighbors in the default segment will always be included, as well as the 4 neighbors in segment 1 with the lowest IP addresses.

## Filter by Segment

To filter the rows displayed in the OSPF table by segment:

- Select **Default** from the **Segment** drop-down list to display for the system-supplied default segment, or
- Select one of the other listed segments, which reflect the custom segments defined using Routing Segmentation (Configuration > Networking > Routing > Routing Segmentation (VRF)).

Select **All** to display for all segments, which is the default setting.

The table below describes the fields displayed for the OSPF configuration.

Field	Description
<b>Appliance</b>	Name of the appliance.
<b>Segment</b>	Name of the segment being used, if enabled.
<b>Enable</b>	[Route Metric] Cost associated with a route. The higher the value, the less preferred.
<b>Router ID</b>	This router identifier is the IPv4 address by which the remote peer can identify this appliance for purposes of OSPF.
<b>Redistribute Routes to OSPF</b>	Redistribution map being used to redistribute routes to OSPF.
<b>Details</b>	Additional details about the route.

Select the edit icon in the OSPF table to edit and enable OSPF.

## OSPF Edit Row

Use this dialog box to manage **OSPF (Open Shortest Path First)** on LAN and WAN interfaces.

OSPF learns routes from routing peers, and then subnet shares them with EdgeConnect peers and/or BGP neighbors.

Field	Description
<b>Enable OSPF</b>	When enabled, the appliance has access to use the OSPF protocol.
<b>Router ID</b>	IPv4 address of the router that the remote peer uses to identify the appliance for purposes of OSPF.
<b>Redistribute routes to OSPF</b>	Redistributing routes into OSPF from other routing protocols or from <b>static</b> will cause these routes to become OSPF external routes. Select the edit icon to the left of this field and select the OSPF route redistribution maps you would like to select.

To add an additional interface to an OSPF route, click **Add** in the **Interfaces** section.

**NOTE** The BFD field in the Interfaces table on the OSPF dialog box is set to N/A if BFD is not supported on the appliance.

To configure or modify an OSPF route map, select the edit icon next to the Redistribute routes to OSPF field.

## Add Interface

Complete the following fields to add an interface to OSPF.

Field	Description
<b>Interface</b>	Indicates whether a Backup Designated Router (BDR) is specified for the Designated Router (DR). Options are <b>Yes</b> or <b>No</b> .
<b>Area ID</b>	Number of the area in which to locate the interface. The Area ID is the same for all interfaces. It can be an integer between 0 and 4294967295, or it can take a form similar to an IP address, A.B.C.D.
<b>Cost</b>	The cost of an interface in OSPF is an indication of the overhead required to send packets across a certain interface. It is used in the OSPF path calculation to determine link preference.
<b>Priority</b>	Router priority. (If two or more best routes are subnet shared, peer priority is used as the tiebreaker.)
<b>Admin Status</b>	Indicates whether the interface is set to admin <b>UP</b> or <b>DOWN</b> .

Field	Description
<b>Hello Interval</b>	Specifies the length of time, in seconds, between the hello packets that a router sends on an OSPF interface.
<b>Dead Interval</b>	Number of seconds that a router's Hello packets have not been seen before its neighbors declare the OSPF router down.
<b>Transmit Delay</b>	Number of seconds required to transmit a link state update packet. Valid values are 1 to 65535.
<b>Retransmit Interval</b>	Amount of time (in seconds) the router will wait to send retransmissions if the router receives no acknowledgment.
<b>BFD</b>	Select this check box to enable BFD for the OSPF interface. This field is not displayed if BFD is not supported on the appliance. <b>NOTE</b> Before you select this check box, enable and configure BFD from the BFD tab.
<b>Authentication</b>	<ul style="list-style-type: none"> <li>• <b>None</b> - No authentication.</li> <li>• <b>Text</b> - Simple password authentication allows a password (key) to be configured per area.</li> <li>• <b>MD5</b> - Message Digest authentication is a cryptographic authentication. A key (password) and key-id are configured on each router. The router uses an algorithm based on the OSPF packet, the key, and the key-id to generate a "message digest" that gets appended to the packet.</li> </ul>
<b>Comment</b>	Any information you want to include for your own use.

## OSPF Route Redistribution Maps

Route Maps are policies applied to IP routes during redistribution between routing protocols. They have **Match Criteria** and **Set Actions** that allow for filtering routes or modifying metrics and attributes for routes that meet the criteria defined in the match statement. Route-map rules follow a top-down order based on the sequence number defined for each entry.

EdgeConnect Enterprise supports applying Route Maps inbound from and outbound to BGP peers and outbound to OSPF neighbors and the SD-WAN Fabric. It is best practice to use Orchestrator to apply Route Maps using templates.

You can specify up to 20 OSPF route maps and 128 rules per route map.

You can specify up to 6 prefixes for each rule applied to a route map.

You can add, delete, rename, or clone route maps using this window. You can add rules to your route map by clicking Add Rule. A route map without any enabled rules is treated as a default deny all.

## Prefix Match Criteria

The default for prefix match criteria is exact-match + greater-than. Both the specified prefix and any subnets of that prefix will be matched, up to a length of 32 for IPv4 or 128 for IPv6 (subnet sharing route maps only).

Less-than-or-equal-to (LE) and greater-than-or-equal-to (GE) clauses can also be applied to specify the inclusion of certain subnets.

To match a default-route, deny 0.0.0.0/1, deny 128.0.0.0/1, and then permit any.

### GE Clause

If a GE clause is applied, the rule will also include all prefixes that have a prefix length greater than or equal to the GE value and less than or equal to 32 or 128 (for IPv6).

Example: A.B.C.D/X GE Y

In this example the following will be included:

- The exact match to A.B.C.D/X
- All the prefixes that belong to the subnet A.B.C.D/X that have a length greater than or equal to Y and less than or equal to 32

### LE Clause

If an LE clause is applied, the rule will also include all prefixes that have a prefix length less than or equal to the LE value.

Example: A.B.C.D/X LE Y

In this example the following will be included:

- The exact match to A.B.C.D/X
- All the prefixes that belong to the subnet A.B.C.D/X that have a length greater than or equal to X and less than or equal to 32
- All the prefixes that belong to the subnet A.B.C.D/X that have a length less than or equal to Y

## Combining LE and GE Clauses

Example: A.B.C.D/X LE Y GE Z

In this example the following will be included:

- The exact match to A.B.C.D/X

- All the prefixes that belong to the subnet A.B.C.D/X that have a length less than or equal to Y
- All the prefixes that belong to the subnet A.B.C.D/X that have a length greater than or equal to Z and less than or equal to 32

## Exact Match

If both GE and LE clauses are specified and are equal, the rule will result in an exact match.

Example: A.B.C.D/X LE Y GE Y

In this example, the following will be included:

- The exact match to A.B.C.D/X
- The exact match to the subnet A.B.C.D/X that has a length equal to Y

You can specify the following fields in each rule for the selected route map.

### *Priority*

Field	Description
<b>Priority</b>	<ul style="list-style-type: none"> <li>• If you are using Orchestrator templates to add rules, Orchestrator will delete all entries from <b>1000 - 9999</b> before applying its policies.</li> <li>• You can create rules with higher priority than Orchestrator rules (<b>1 - 999</b>) and rules with lower priority (<b>10000 - 19999</b> and <b>25000 - 65534</b>).</li> </ul> <p><b>NOTE</b> The priority range from <b>20000 to 24999</b> is reserved for Orchestrator.</p> <ul style="list-style-type: none"> <li>• When adding a rule, the priority is incremented by 10 from the previous rule. The priority can be changed, but this default behavior helps to ensure you can insert new rules without having to change subsequent priorities.</li> </ul>

### *Select Match Criteria*

Source Protocol	Complete the Following Fields (based on protocol selected)
<b>Local/Static</b>	<ul style="list-style-type: none"> <li>• Prefix + optional LE/GE parameters</li> </ul>
<b>BGP</b>	<ul style="list-style-type: none"> <li>• Prefix + optional LE/GE parameters</li> <li>• BGP Communities</li> </ul>
<b>SD-WAN Routes</b>	<ul style="list-style-type: none"> <li>• Prefix + optional LE/GE parameters</li> <li>• BGP Communities</li> <li>• OSPF Tag</li> </ul>

**NOTE** The above fields in the right column will change depending on the source protocol chosen.

#### Set Actions

Field	Description
<b>Permit</b>	Enable or disable. This setting allows or denies the route map.
<b>OSPF Tag</b>	Value of OSPF tag to set in routing information sent to destination.
<b>OSPF Metric Type</b>	Filters redistributed routes to OSPF.
<b>Metric</b>	Metric for the route.
<b>Comment</b>	Comment you want to include.

## BFD Tab

*Configuration > Networking > Routing > BFD*

Bidirectional Forwarding Detection (BFD) is a networking protocol that detects faults between devices. The EdgeConnect appliance supports BFD for both BGP and OSPF.

- Single and multi-hop BFD configurations are supported.
- BFD asynchronous mode is supported.
- BFD can be configured for up to 20 segments with a maximum of 100 simultaneous BFD sessions across all segments.

Configuring BFD for BGP or OSPF is a two-step process:

1. Click the edit icon for an appliance listed in the BFD table on the BFD tab, and then enable and configure BFD on the BFD dialog box. For details, see [BFD Dialog Box on the next page](#).
2. Enable BFD for each BGP peer or OSPF interface.
  - a. For BGP, navigate to **Configuration > Networking > Routing > BGP**. Click the edit icon for an appliance listed in the BGP table, and then click **Add** to add a BGP peer or click the edit icon for an existing BGP peer listed in the BGP Peers table. Select the **BFD** check box, make other changes as appropriate, and then click **Add** or **Save**.
  - b. For OSPF, navigate to **Configuration > Networking > Routing > OSPF**. Click the edit icon for an appliance listed in the OSPF table, and then click **Add** in the Interfaces area to add an interface or click the edit icon for an existing interface listed in the Interfaces table. Select the **BFD** check box, make other changes as appropriate, and then click **Add** or **Save**.

The BFD tab provides two views of BFD information:

- Click the **Summary** button on the BFD tab to display configuration details associated with the local appliance. For field descriptions, see [BFD Dialog Box below](#).
- Click the **Sessions** button to display currently active BFD sessions. BFD establishes a session between two endpoints over a particular link. If more than one link exists between two systems, multiple BFD sessions can be established to monitor each of them.

### Filter by Segment

To filter the rows displayed in the BFD table by segment:

- Select **Default** from the **Segment** drop-down list to display for the system-supplied default segment, or
- Select one of the other listed segments, which reflect the custom segments defined using Routing Segmentation (Configuration > Networking > Routing > Routing Segmentation (VRF)).

Select **All** to display for all segments, which is the default setting.

The following table describes the fields displayed in the Sessions view of the BFD tab.

Field	Description
<b>Appliance</b>	Name of the appliance.
<b>Segment</b>	Name of the segment. This field displays only if Routing Segmentation is enabled.
<b>Local address</b>	IP address of the local endpoint.
<b>Remote address</b>	IP address of the remote endpoint.
<b>Local Interface</b>	Name of the local interface (lan0, wan0, wan1).
<b>State</b>	Session state (UP or DOWN).
<b>Uptime</b>	Session up time.
<b>Details</b>	Additional details about the BFD session.

### BFD Dialog Box

Use this dialog box to enable and configure BFD for your appliances, as follows:

- Move the toggle to **Enable BFD**.
- Complete the following fields.

Field	Description
<b>Min Tx Interval</b>	Minimum transmit interval in milliseconds (ms). Specify a value from 300 to 5000. The default setting is 300.
<b>Min Rx Interval</b>	Minimum receive interval in milliseconds (ms). Specify a value from 300 to 5000. The default setting is 300.

Field	Description
<b>Detection Multiplier</b>	Detection time multiplier. In BFD, the detection time is the transmit interval multiplied by the detection multiplier. If BFD data is not received within the detection time, a failure occurs. Specify a value from 3 to 10. The default setting is 3.

## Multicast

*Configuration > Networking > Routing > Multicast*

Orchestrator supports multicast routing, a method of sending data from a single IP address to a larger group of recipients.

- Up to 60 multicast routes are supported, including up to 30 (S,G) and 30 (\*,G) groups.
- Up to 1000 sites can participate in the same multicast stream. Aruba recommends up to 200 sites.
- All versions of IGMP are supported (IGMPv1, IGMPv2, and IGMPv3).
- Multicast routing is supported in Inline Router mode only.

Orchestrator provides four views of multicast status, each accessible by one of the corresponding buttons at the top of the Multicast tab: **Summary**, **Interfaces**, **Neighbors**, and **Routes**.

Descriptions of fields on the Summary view follow:

Field	Description
<b>Appliance</b>	Name of the appliance (also selected in the left menu) associated with the multicast configuration.
<b>Enable</b>	Indicates whether multicast is enabled.
<b>Rendezvous Point IP</b>	IP address of the centralized, source router distributing the packet of traffic to each router involved in multicast.
<b>Allowed Group</b>	Only IP addresses included in the specified address group can multicast. If no address group is specified, any IP address can multicast. The message <i>Feature is not supported for the appliance</i> displays in this field if the appliance does not support the Allowed Group feature.

Click the edit icon to enable or disable multicast, add an interface for multicast, or edit an existing interface.

## Multicast Dialog Box

From the Summary, Interfaces, Neighbors, or Routes view on the Multicast tab:

1. Click the edit icon next to the appliance for which you want to set up multicast.  
The Multicast dialog box opens.
2. Move the **Enable Multicast** toggle to the right to enable multicast.

3. In the **Rendezvous Point IP Address** field, enter the appropriate IP address.
4. In the **Allowed Group** field, select an available address group from the drop-down list or enter a new address group. All IP addresses included in the specified address group will be allowed to multicast. This field is not displayed if the appliance does not support the Allowed Group feature. Address group names can include letters, numbers, periods, underscores, or hyphens.

**IMPORTANT:** The address group you specify in the Address Group field must be valid. If you enter a new address group, ensure that you also create and set it up on the Address Groups tab (Configuration > Templates & Policies > ACLs > Address Groups). If the new address group remains invalid, no IP addresses will be allowed to multicast.

#### Interfaces

Field	Description
<b>Interface</b>	Name of the interface you want to connect.
<b>PIM Enabled</b>	Indicates whether Protocol Independent Multicast is enabled. This allows routers to communicate through the unidirectional shared trees within multicast through the shortest path.
<b>IGMP Enabled</b>	Indicates whether Internet Group Management Protocol is enabled. This establishes the other routers in the multicast group.
<b>DR Priority</b>	Designated router priority of the given interface.
<b>DR Router IP</b>	IP address of the designated router within your network.

To add an interface:

1. Click **Add**.
- The Add Interface dialog box opens.
2. Select the desired interface from the **Interface** drop-down list.
3. Select the **Enable PIM** check box if you want to enable it.
4. Select the **Enable IGMP** check box if you want to enable it.
5. Click **Add**.

#### Neighbors

Field	Description
<b>Interface</b>	Name of the interfaces you want to connect.
<b>Neighbor DR Priority</b>	Designated router priority of the neighbor.
<b>Neighbor IP</b>	IP address of the neighbor.

## Routes

Field	Description
<b>Source</b>	Transmitter of the multicast data.
<b>Group</b>	IP address of the multicast group.
<b>Incoming Interface</b>	Interface that receives inbound traffic.
<b>Outgoing Interfaces</b>	Interface that receives outbound traffic.

On the Multicast tab, you can click **Export CSV** to export a spreadsheet of the multicast report. You can also click the refresh button to update information displayed on the tab.

## Peer Priority Tab

*Configuration > Networking > Routing > Peer Priority*

When an appliance receives a **Subnet** with the same **Metric** from multiple remote/peer appliances, it uses the Peer Priority list as a tie-breaker.

- If a **Peer Priority** is not configured, the appliance randomly distributes flows among multiple peers.
- The lower the number, the higher the peer's priority.

Click the edit icon to configure a peer and its peer priority.

Edit	Appliance	Peer Name	Peer Priority	Advertise Metric
#	Oslo-[REDACTED]	APJ3-Azure	90	preserve existing
#	Oslo-[REDACTED]	AUS1-AWS	80	preserve existing
#	Oslo-[REDACTED]	CENTRAL2-AWS	60	preserve existing
#	Oslo-[REDACTED]	EAST2-AWS	40	preserve existing
#	Oslo-[REDACTED]	EAST9-AWS	40	preserve existing
#	Oslo-[REDACTED]	EMEA3-AWS	10	preserve existing
#	Oslo-[REDACTED]	EMEA4-AWS	10	preserve existing
#	Oslo-[REDACTED]	EMEA5-Google	30	preserve existing
#	Oslo-[REDACTED]	WEST2-AWS	70	preserve existing

**NOTE** By default, the peer priority range starts at 1.

## Peer Priority Edit Row

This dialog box displays a list of configured peers. The peer priority and advertise metric are displayed for each peer.

- Peer priority controls the peer to which traffic is sent when route ties occur. It acts similar to BGP's local preference.
- Advertise metric controls the return path of a flow back toward the local appliance. It adjusts the metric of all routes sent to Peer Name. Advertise metric announces different metrics to different fabric peers. It acts similar to BGP's Multi Exit Discriminator (MED). The default setting is *preserve existing* (do nothing).

Both peer priority and advertise metric impact all routes sent and received from Peer Name.

To add a peer:

1. Click **Add Peer**.
2. In the new row that is added to the table, enter the peer name, peer priority, and advertise metric.
3. To delete a peer, click the X in the far-right column of the peer's row.
4. When finished, click **Apply**.

## Admin Distance Tab

*Configuration > Networking > Routing > Admin Distance*

This tab shows values associated with various types of **Admin Distance**. Admin Distance (AD) is the route preference value assigned to dynamic routes, static routes, and directly connected routes. When the appliance's Routes table has multiple routes to the same destination, the appliance uses the route with the lowest administrative distance.

The following table displays the values associated with various types of **Admin Distance**.

Field	Description
<b>Appliance</b>	Name of the appliance.
<b>Local</b>	Manually configured route, or one learned from locally connected subnets.
<b>EBGP</b>	External BGP: exchanging routing information with a router outside the company-wide network.
<b>IBGP</b>	Internal BGP: exchanging routing information with a router inside the company-wide network.
<b>Subnet Shared - Static Routes</b>	Route learned from an EdgeConnect peer.
<b>Subnet Shared - BGP Remote</b>	Route shared from an EdgeConnect peer in an external network.

Field	Description
<b>OSPF</b>	Route learned from an OSPF (Open Shortest Path First) neighbor.
<b>Subnet Shared - OSPF Remote</b>	Route learned from an EdgeConnect peer.

To edit these fields, click the edit icon.

## Admin Distance Edit Row

Use this dialog box to edit the admin distances for each type in the table. Click any cell in the Distance column to begin modifying the values. When finished, click **Save**.

## Management Routes Tab

*Configuration > Networking > Routing > Management Routes*

Use this tab to configure **next-hops** for management interfaces.

The screenshot shows a software interface titled "Management Routes". At the top left is a close button (X). Below it is a toolbar with a "Management Routes" label, a help icon (?), and a refresh/circular arrow icon. A "Add new route" button is located on the left side of the main area. The main area contains a table with the following data:

Subnet	Next-hop IP	Interface	Source IP	Metric
10.17.46.0/24	0.0.0.0	wan0	0.0.0.0	100
10.17.45.0/24	0.0.0.0	lan0	0.0.0.0	100
10.0.185.0/24	0.0.0.0	mgmt0	10.0.185.43	
10.0.184.0/24	0.0.0.0	wan1	0.0.0.0	100
0.0.0.0/0	10.17.46.1	wan0	0.0.0.0	253
0.0.0.0/0	10.0.185.1	mgmt0	0.0.0.0	252

- Management routes specify the **default gateways** and local IP subnets for the management interfaces.
- In a Dual-Homed Router Mode configuration, you might need to add a static management route for flow redirection between appliances paired for redundancy at the same site.

- The management routes table shows the configured static routes and any dynamically created routes. If you use **DHCP**, the appliance automatically creates appropriate dynamic routes. A user cannot delete or add dynamic routes.
- If the **Source IP** is listed as **0.0.0.0**, packets sent using this route use the **Interface's IP address** as the Source IP address. If the **Source IP** lists a specific IP address, that IP address is used instead.

## Tunnels Tab

*Configuration > Networking > Tunnels > Tunnels*

EdgeConnect tunnels are the foundation of your SD-WAN fabric. This tab displays details about tunnels in your network. It includes the following three subtabs:

- Overlay - Displays SD-WAN bonded tunnels. Specifically, overlay tunnels consist of bonded underlay tunnels.
- Underlay - Displays IPSec tunnels that map to discrete transports.
- Passthrough - Displays third-party (IPSec) tunnels for service chaining to cloud security services, such as Zscaler and Symantec, and tunnels for local breakouts to trusted SaaS applications, such as Office 365.

If you have deployed an SD-WAN network, Business Intent Overlays (BIOs) govern tunnel creation and properties.

### Filter by Tunnel Status

To filter the rows displayed in the Tunnels table by tunnel status, select **Up** or **Down** from the Status drop-down list. Select **All** to display for all statuses, which is the default setting.

### Subtab Field Descriptions

The following tables describe the fields displayed on the Overlay, Underlay, and Passthrough subtabs. Field descriptions are not repeated if they appear on more than one subtab and have the same description.

#### Overlay Subtab

Field	Description
<b>Appliance</b>	Name of the appliance.
<b>Overlay Tunnel</b>	Designated overlay tunnel.
<b>Overlay</b>	Designated overlay to which the overlay tunnel is applied.
<b>Admin Status</b>	Indicates whether the tunnel has been set to admin <b>up</b> or <b>down</b> .

Field	Description
Status	<p>Indications are as follows:</p> <ul style="list-style-type: none"> <li>• <b>Down</b> – Tunnel is down. This can be because the tunnel administrative setting is down or the tunnel cannot communicate with the appliance at the other end. Possible causes are:           <ul style="list-style-type: none"> <li>• Lack of end-to-end connectivity / routability (test with <i>iperf</i>).</li> <li>• Intermediate firewall is dropping the packets (open the firewall).</li> <li>• Intermediate QoS policy (<b>be</b> packets are being starved; change control packet DSCP marking).</li> <li>• Mismatched tunnel mode (udp / gre / ipsec / ipsec_udp).</li> <li>• IPSec is misconfigured: (1) enabled on one side (see <i>show int tunnel configured</i>), or mismatched pre-shared key.</li> </ul> </li> <li>• <b>Down - In progress</b> – Tunnel is down. Meanwhile, the appliance is exchanging control information with the appliance at the other end, trying to bring up the tunnel.</li> <li>• <b>Down - Misconfigured</b> – Two appliances are configured with the same System ID (see <i>show system</i>).</li> <li>• <b>Up - Active</b> – Tunnel is up and active. Traffic destined for this tunnel will be forwarded to the remote appliance.</li> <li>• <b>Up - Active - Idle</b> – Tunnel is up and active, but it has not had recent activity in the past five minutes, and it has slowed the rate of issuing keep-alive packets.</li> <li>• <b>Up - Reduced Functionality</b> – Tunnel is up and active, but the two endpoint appliances are running mismatched software releases that give no performance benefit.</li> <li>• <b>UNKNOWN</b> – Tunnel status is unknown. This can be because the appliance is unable to retrieve the current tunnel status. Try again later.</li> </ul>
MTU	<i>Maximum Transmission Unit.</i> The largest possible unit of data that can be sent on a given physical medium. MTUs up to 9000 bytes are supported. <b>Auto</b> allows the tunnel MTU to be discovered automatically. It overrides the MTU setting.
Uptime	Length of time the tunnel has been up.
Underlay Tunnels	Designated underlay tunnels.
Live View	Click the chart icon to display a live view of the status of your selected tunnel. You can view by bandwidth, loss, jitter, latency, MOS, chart, traceroute, inbound or outbound, and lock the scale.
Historical Charts	Click the chart icon to display historical charts for the selected overlay and underlay tunnels.

#### Underlay Subtab

Field	Description
Segment	Name of the segment. This field displays only if Routing Segmentation is enabled.

Field	Description
<b>Underlay Tunnel</b>	Designated underlay tunnel.
<b>Overlays</b>	Overlays to which the tunnels for the appliance are applied.
<b>Admin Status</b>	Indicates whether the tunnel has been set to admin <b>up</b> or <b>down</b> . To change the admin status for the underlay tunnel, click the menu icon and select <b>Admin Up</b> or <b>Admin Down</b> .
<b>Status</b>	Status indications are described above in field descriptions for the Overlay subtab. Click the status indicator in this field to display detailed troubleshooting information for this tunnel.
<b>Local IP:Port</b>	Local IP address and port number.
<b>Remote IP:Port</b>	Remote IP address and port number.
<b>Discovered IP:Port</b>	Discovered IP address and port number.
<b>Max BW (Kbps)</b>	Maximum bandwidth for the tunnel in kilobits per second (Kbps).
<b>Mode</b>	Indicates whether the tunnel protocol is <b>IPSec</b> , <b>IPSec UDP</b> , <b>UDP</b> , or <b>GRE</b> .
<b>Advanced Options</b>	Click the info icon to open the Tunnel Advanced Options dialog box, which displays details about the tunnel's settings.
<b>Traceroute</b>	Click the chart icon to display a traceroute chart for the selected appliance.
<b>Historical Charts</b>	Click the chart icon to display historical charts for the selected underlay tunnel.

#### Passthrough Subtab

Field	Description
<b>Passthrough Tunnel</b>	Designated passthrough tunnel.
<b>Charts</b>	Click the chart icon to display historical charts for the selected passthrough tunnel.
<b>Local IP</b>	IP address of the local endpoint.
<b>Remote IP</b>	IP address of the remote endpoint.
<b>Mode</b>	Indicates whether the tunnel protocol is <b>GRE</b> , <b>IPSec</b> , or <b>No Encap</b> .
<b>NAT</b>	Indicates whether Network Address Translation (NAT) has been applied.
<b>Peer/Service</b>	Peer or service being used.

To add, modify, or delete tunnels for an appliance, click the edit icon in the appropriate table row on the Tunnels tab.

#### Troubleshooting

1. *Have you created and applied the Overlay to all the appliances on which you are expecting tunnels to be built?*

Verify this on the **Apply Overlays** tab.

2. *Are the appliances on which you are expecting the Overlays to be built using Release 8.0 or later?*

View the active software releases on **Administration > Software > Upgrade > Software Versions**.

3. *Do you have at least one WAN Label selected as a Primary port in the Overlay Policy?*

Verify this on the Business Intent Overlay tab in the **WAN Links & Bonding Policy** section.

4. *Are the same WAN labels selected in the Overlay assigned to the WAN interfaces on the appliances?*

Verify that at least one of the *Primary Labels* selected in the Business Intent Overlay is identical to a Label assigned on the appliance's Deployment page. Tunnels are built between matching Labels on all appliances participating in the overlay.

5. *Do any two (or more) appliances have the same Site Name?*

We **only** assign the same Site Name if we **do not** want those appliances to connect directly. To view the list of Site Names, navigate to the **Configuration > Networking > Tunnels > Tunnels** tab, and then click **Sites** at the top.

## Tunnels Dialog Box

This dialog box enables you to add, modify, or delete underlay and passthrough tunnels for an appliance. If you have deployed an SD-WAN network, Business Intent Overlays (BIOS) govern tunnel creation and properties. Overlay tunnels consist of bonded underlay tunnels.

The Tunnels dialog box includes the following three subtabs:

- Overlay - Displays SD-WAN bonded tunnels. Specifically, overlay tunnels consist of bonded underlay tunnels.
- Underlay - Displays IPSec tunnels that map to discrete transports.
- Passthrough - Displays third-party (IPSec) tunnels for service chaining to cloud security services, such as Zscaler and Symantec, and tunnels for local breakouts to trusted SaaS applications, such as Office 365.

## Use Passthrough Tunnels

Use passthrough tunnels in the following situations:

- For internet breakout to a trusted SaaS application, like Office 365
- For service chaining to a cloud security service, like Zscaler or Symantec
  - This requires building secure and compatible third-party IPSec tunnels from EdgeConnect devices to non-EdgeConnect devices in the data center or cloud.
  - When you create the tunnel, the Service Name in the Business Intent Overlay's Internet Traffic Policies must exactly match the Peer/Service specified in the Passthrough tunnel configuration.

- To load balance, create two or more passthrough IPSec tunnels and, in the Business Intent Overlay, ensure that they all specify the same Service Name in the Internet Traffic Policies.

## IPSec Suite B Presets

As of version 9.2, Orchestrator provides you with four IPSec Suite B presets, as follows:

- GCM-128
- GCM-256
- GMAC-128
- GMAC-256

Each preset includes a predetermined set of IKE and ESP (IPSec) cryptographic algorithms. By selecting an IPSec Suite B preset, you can streamline the algorithm aspect of your tunnel setup rather than selecting individual algorithms. However, you can select individual algorithms if you want to. To select a preset, use the **IPSec Suite B Preset** drop-down field on the Add Tunnel or Modify Tunnel dialog box.

The following tables show the IPSec Suite B presets in the header row and provide the associated algorithm setups for the IKEv2 and ESP (IPSec) stages.

### *IKEv2 Stage*

	GCM-128	GCM-256	GMAC-128	GMAC-256
<b>Encryption (Note)</b>	AES-128-CBC	AES-256-CBC	AES-128-CBC	AES-256-CBC
<b>Pseudo Random Function</b>	HMAC-SHA-256	HMAC-SHA-384	HMAC-SHA-256	HMAC-SHA-384
<b>Integrity (IKE Data Authentication)</b>	HMAC-SHA-256-128	HMAC-SHA-384-192	HMAC-SHA-256-128	HMAC-SHA-384-192
<b>Key Exchange (NIST Elliptic Curve Groups)</b>	DH-19 256-bit Prime Size	DH-20 384-bit Prime Size	DH-19 256-bit Prime Size	DH-20 384-bit Prime Size

### *ESP (IPSec) Stage*

	GCM-128	GCM-256	GMAC-128	GMAC-256
<b>Encryption</b>	AES-128-GCM with 16 octet ICV	AES-256-GCM with 16 octet ICV	NULL	NULL
<b>Integrity (Data Authentication)</b>	NULL	NULL	AES-128-GMAC	AES-256-GMAC

Notice in the second table that the encryption and data authentication is done in one step for GCM. For GMAC, there is no encryption.

## Add or Modify a Tunnel

To add an underlay or passthrough tunnel, perform the following steps:

**NOTE** To modify a tunnel, click the edit icon next to the tunnel. The Modify Tunnel dialog box (for underlay tunnels) or the Modify Passthrough Tunnel dialog box opens. Change fields as described below, and then click **Save**.

1. Select Underlay or Passthrough.
2. Select Add Tunnel.

The Add Tunnel dialog box (for underlay) or the Add Passthrough Tunnel dialog box opens.

3. Complete the following fields as appropriate for either underlay or passthrough tunnels.

### *Add Tunnel dialog box (for underlay)*

The Add Tunnel dialog box displays a General tab. If you set the Mode field on this tab to IPSec, the IKE and IPSec tabs are also displayed.

#### **General tab (for underlay)**

Access the following fields by clicking the General tab on the Add Tunnel dialog box.

##### *General*

Field	Description
<b>Alias</b>	Alias name of the tunnel.
<b>Mode</b>	Indicates whether the tunnel protocol is <b>UDP</b> , <b>GRE</b> , <b>IPSec</b> , or <b>IPSec UDP</b> . If you select IPSec, you can specify the IKE version on the IKE tab.  <b>NOTE</b> If this field is set to IPSec UDP, it is recommended that you use the AES_256_GCM_16 algorithm, which performs both encryption and authentication, resulting in better performance.
<b>IPSec Suite B Preset</b>	This field is available only if the Mode field is set to IPSec. Select an IPSec Suite B preset if required by the security service ( <b>GCM-128</b> , <b>GCM-256</b> , <b>GMAC-128</b> , or <b>GMAC-256</b> ). The default setting is None. <ul style="list-style-type: none"> <li>• If IPSec Suite B Preset is set to None, no preset is selected, but GCM and GMAC algorithms are available to set independently.</li> <li>• If an IPSec Suite B preset is selected, various settings on the IKE and IPSec tabs are configured automatically based on the selected preset.</li> </ul>
<b>Admin</b>	Indicates whether the tunnel has been set to admin <b>up</b> or <b>down</b> .
<b>Local IP</b>	IP address of the local endpoint.
<b>Remote IP</b>	IP address of the remote endpoint.

*General*

Field	Description
<b>Auto discover MTU enabled</b>	When enabled, allows the appliances to auto-negotiate the maximum tunnel bandwidth. Enabled by default.
<b>MTU</b>	Maximum Transmission Unit (MTU) is the largest possible unit of data that can be sent on a given physical medium. For example, the MTU of Ethernet is 1500 bytes. MTUs up to 9000 bytes are supported. Auto allows the tunnel MTU to be discovered automatically, and it overrides the MTU setting. This field is not available if the Auto discover MTU enabled check box is selected.
<b>Auto max BW enabled</b>	When enabled, allows the appliances to auto-negotiate the maximum tunnel bandwidth. Enabled by default.
<b>Max BW Kbps</b>	Maximum amount of bandwidth in kilobits per second. This field is not available if the Auto max BW enabled check box is selected.
<b>UDP destination port</b>	Used in UDP mode. Accept the default value unless the port is blocked by a firewall.
<b>UDP flows</b>	Used in UDP mode. Number of flows over which to distribute tunnel data.
<b>Min BW Kbps</b>	Minimum amount of bandwidth in kilobits per second.

*Packet*

**NOTE** FEC settings do not apply when overlays are used. FEC settings only apply when routing directly to an underlay via Route Policy.

Field	Description
<b>Reorder wait</b>	Maximum time (in milliseconds) the appliance holds an out-of-order packet when attempting to reorder. <b>100</b> ms is the default value and should be adequate for most situations. FEC can introduce out-of-order packets if the reorder wait time is not set high enough.
<b>FEC</b>	Set Forward Error Correction (FEC) to <b>enable</b> , <b>disable</b> , or <b>auto</b> .
<b>FEC ratio</b>	When FEC is set to <b>auto</b> , FEC will range dynamically from off to 1:10 based on detected loss. The options are <b>1:1</b> , <b>1:2</b> , <b>1:5</b> , <b>1:10</b> , and <b>1:20</b> . This field is available only if FEC is set to enable.

*Tunnel Health*

Field	Description
<b>Retry count</b>	Number of failed keep-alive messages allowed before the appliance brings the tunnel down.

*Tunnel Health*

Field	Description
<b>DSCP</b>	Determines the DSCP marking that the keep-alive messages should use.

---

### FastFail Thresholds

**NOTE** FastFail thresholds do not apply when overlays are used. FastFail only applies when routing directly to an underlay via Route Policy.

Field	Description
<b>Fastfail enabled</b>	When multiple tunnels are carrying data between two appliances, this feature determines how quickly to disqualify a tunnel from carrying data.

The Fastfail connectivity detection algorithm for the wait time from receipt of last packet before declaring a **brownout** is:

$$T_{wait} = \text{Base} + N * RTT_{avg}$$

where **Base** is a value in milliseconds, and **N** is the multiplier of the average Round Trip Time over the past minute.

For example, if:

$$\text{Base} = 200\text{ms}$$

$$N = 2$$

Then,

$$RTT_{avg} = 50\text{ms}$$

The appliance declares a tunnel to be in brownout if it does not see a reply packet from the remote end within 300 ms of receiving the most recent packet.

In the Tunnel Advanced Options, **Base** is expressed as **Fastfail wait-time base offset (ms)**, and **N** is expressed as **Fastfail RTT multiplication factor**.

**Fastfail enabled** – This option is triggered when a tunnel's keep-alive signal does not receive a reply. The options are **disable**, **enable**, and **continuous**. If the disqualified tunnel subsequently receives a keep-alive reply, its recovery is instantaneous.

- For disable, keep-alives are sent every second, and 30 seconds elapse before failover. In that time, all transmitted data is lost.
- For enable, keep-alives are sent every second, and a missed reply increases the rate at which keep-alives are sent from one per second to ten per second. Failover occurs after one second.
- For continuous, keep-alives are continuously sent at ten per second. Therefore, failover occurs after one tenth of a second.

### *FastFail Thresholds*

**NOTE** FastFail thresholds do not apply when overlays are used. FastFail only applies when routing directly to an underlay via Route Policy.

Field	Description
<b>Latency</b>	Amount of latency in milliseconds. Thresholds for Latency, Loss, or Jitter are checked once every second. <ul style="list-style-type: none"> <li>Receiving three successive measurements in a row that exceed the threshold puts the tunnel into a brownout situation and flows will attempt to fail over to another tunnel within the next 100 ms.</li> <li>Receiving three successive measurements in a row that drop below the threshold will drop the tunnel out of brownout.</li> </ul>
<b>Loss</b>	Amount of data lost as a percentage.
<b>Jitter</b>	Amount of jitter in milliseconds.
<b>Fastfail wait-time base offset</b>	Fastfail basic timeout time in milliseconds.
<b>Fastfail RTT multiplication factor</b>	Amount of RTT (Round Trip Time) added to the basic timeout.

### **IKE tab (for underlay)**

Access the following fields by clicking the IKE tab on the Add Tunnel dialog box. This tab is displayed only if the Mode field on the General tab is set to IPSec.

#### *IKE*

Field	Description
<b>Pre-shared key</b>	Pre-shared key used for IKE authentication.
<b>Authentication Algorithm</b>	Authentication algorithm used for IKE security association (SA). <ul style="list-style-type: none"> <li>If the IPSec Suite B Preset field on the General tab is set to None, you can select <b>SHA1</b>, <b>SHA2-256</b>, <b>SHA2-384</b>, or <b>SHA2-512</b>. The default setting is SHA1.</li> <li>If the IPSec Suite B Preset field is set to any other setting, this field is automatically set to the appropriate algorithm.</li> </ul> <b>NOTE</b> With IKEv2 and the Encryption algorithm field set to auto, AES-GCM will probably be negotiated, which includes encryption and authentication. In this case, this field might show a SHA setting that is not actually used. <ul style="list-style-type: none"> <li>If the Encryption algorithm field is set to AES-GCM-128 or AES-GCM-256, this field is not applicable.</li> </ul>

Field	Description
<b>Encryption Algorithm</b>	<p>Encryption algorithm used for IKE security association (SA).</p> <ul style="list-style-type: none"> <li>If the IPSec Suite B Preset field on the General tab is set to None, and the IKE Version field is set to IKE v1, you can select <b>AES-CBC-128</b>, <b>AES-CBC-256</b>, or <b>auto</b>. The default setting is auto.</li> <li>If the IPSec Suite B Preset field is set to None, and the IKE Version field is set to IKE v2, you can select <b>AES-CBC-128</b>, <b>AES-CBC-256</b>, <b>AES-GCM-128</b>, <b>AES-GCM-256</b>, or <b>auto</b>. The default setting is auto.</li> <li>If the IPSec Suite B Preset field is set to any other setting, this field is automatically set to the appropriate algorithm.</li> </ul>
<b>Pseudo Random Function</b>	<p>This field is displayed only if the IKE Encryption Algorithm field is set to AES-GCM-128 or AES-GCM-256.</p> <ul style="list-style-type: none"> <li>For AES-GCM-128, you can select <b>SHA2-256</b>, <b>SHA2-384</b>, or <b>SHA2-512</b>.</li> <li>For AES-GCM-256, you can select <b>SHA-384</b> or <b>SHA-512</b>.</li> </ul>
<b>Diffie-Hellman Group</b>	<p>Diffie-Hellman Group used for IKE security association (SA) negotiation.</p> <ul style="list-style-type: none"> <li>If the IPSec Suite B Preset field on the General tab is set to None, you can select the appropriate group. Available groups are 14 through 21, 26, and 31.</li> <li>If the IPSec Suite B Preset field is set to any other setting, this field is automatically set to the appropriate group.</li> </ul>
<b>Rekey interval/lifetime</b>	<p>Rekey interval/lifetime of IKE security association (SA) in minutes. The default is 360 minutes.</p>
<b>Dead peer detection</b>	<p><b>Delay time:</b> The interval (in seconds) to check the lifetime of the IKE peer.  <b>Retry count:</b> Number of times to retry the connection before determining that the connection is dead. This field is not editable.</p>
<b>IKE identifier</b>	<p>Identifier of the IKE tunnel. This field is displayed only if the IKE Version field is set to IKE v1. Select the type of identifier from the drop-down list:</p> <ul style="list-style-type: none"> <li><b>IP ADDRESS</b> – Specify the local public IP address, <i>not</i> the remote endpoint address.</li> <li><b>FQDN</b> – Specify the fully qualified domain name (also known as absolute domain name).</li> <li><b>USER_FQDN</b> – Specify an email address that contains an email domain.</li> </ul>
<b>Local IKE identifier</b>	<p>Specify the local IKE identifier. This field is displayed only if the IKE Version field is set to IKE v2.</p>

Field	Description
<b>Remote IKE identifier</b>	Specify the remote IKE identifier. This field is displayed only if the IKE Version field is set to IKE v2.
<b>Phase 1 mode</b>	Exchange mode for the IKE security association (SA) negotiation. <ul style="list-style-type: none"> <li>If the IKE Version field is set to IKE v1, you can select <b>Main</b> or <b>Aggressive</b>.</li> <li>If the IKE Version field is set to IKE v2, this field is automatically set to Aggressive.</li> </ul>
<b>IKE version</b>	<ul style="list-style-type: none"> <li>If the IPSec Suite B Preset field on the General tab is set to None, you can select <b>IKE v1</b> or <b>IKE v2</b>.</li> <li>If the IPSec Suite B Preset field is set to any other setting, this field is automatically set to IKE v2.</li> </ul>

### IPSec tab (for underlay)

Access the following fields by clicking the IPSec tab on the Add Tunnel dialog box. This tab is displayed only if the Mode field on the General tab is set to IPSec.

#### IPSec

Field	Description
<b>Authentication algorithm</b>	Authentication algorithm used for the IPSec security association (SA). <ul style="list-style-type: none"> <li>If the IPSec Suite B Preset field on the General tab is set to None, you can select <b>SHA1</b>, <b>SHA2-256</b>, <b>SHA2-384</b>, <b>SHA2-512</b>, <b>AES-GMAC-128</b>, or <b>AES-GMAC-256</b>. The default setting is SHA1.</li> <li>If the IPSec Suite B Preset field is set to GMAC-128 or GMAC-256, this field is automatically set to the appropriate algorithm.</li> <li>If the IPSec Suite B Preset field is set to GCM-128 or GCM-256, this field is not applicable.</li> </ul>
<b>Encryption algorithm</b>	Encryption algorithm used for the IPSec security association (SA). <ul style="list-style-type: none"> <li>If the IPSec Suite B Preset field on the General tab is set to None, and the IPSec Authentication algorithm field is set to SHA1, SHA2-256, SHA2-384, or SHA2-512, you can select <b>AES-CBC-128</b>, <b>AEC-CBC-256</b>, <b>AES-GCM-128</b>, <b>AES-GCM-256</b>, <b>NULL</b>, or <b>Auto</b>. The default setting is auto.</li> <li>If the IPSec Suite B Preset field is set to None, and the IPSec Authentication algorithm field is set to AES-GMAC-128 or AES-GMAC-256, this field is automatically set to NULL.</li> </ul>

Field	Description
<b>IPSec anti-replay window</b>	Select a size from the drop-down list or <b>Disable</b> to disable the IPSec anti-replay window. If a size is selected, protection is provided against an attacker duplicating encrypted packets by assigning a unique sequence number to each encrypted packet.
<b>Rekey interval/lifetime</b>	Rekey interval/lifetime of the IPSec security association (SA) in minutes. The default is 360 minutes.
<b>Perfect forward secrecy group</b>	Diffie-Hellman group used for IPSec security association (SA) negotiation. Based on the setting of the IPSec Suite B Preset field on the General tab, this field is set to the following Diffie-Hellman group: <ul style="list-style-type: none"> <li>• For None: 14 (by default)</li> <li>• For GCM-128 or GMAC-128: 19</li> <li>• For GCM-256 or GMAC-256: 20</li> </ul>

### Add Passthrough Tunnel dialog box

The Add Passthrough Tunnel dialog box displays a General tab. If you set the Mode field on this tab to IPSec, the IKE and IPSec tabs are also displayed.

#### General tab (for passthrough)

Access the following fields by clicking the General tab on the Add Passthrough Tunnel dialog box.

##### General

Field	Description
<b>Alias</b>	Alias name of the tunnel.
<b>Mode</b>	Indicates whether the tunnel protocol is <b>GRE</b> , <b>No Encap</b> , <b>IPSec</b> , or <b>IPSec UDP</b> . <b>NOTE</b> If this field is set to IPSec UDP, it is recommended that you use the <b>AES_256_GCM_16</b> algorithm, which performs both encryption and authentication.
<b>IPSec Suite B Preset</b>	This field is available only if the Mode field is set to IPSec. Select an IPSec Suite B preset if required by the security service ( <b>GCM-128</b> , <b>GCM-256</b> , <b>GMAC-128</b> , or <b>GMAC-256</b> ). The default setting is None. <ul style="list-style-type: none"> <li>• If IPSec Suite B Preset is set to None, no preset is selected, but GCM and GMAC algorithms are available to set independently.</li> <li>• If an IPSec Suite B preset is selected, various settings on the IKE and IPSec tabs are configured automatically based on the selected preset.</li> </ul>

*General*

Field	Description
<b>Admin</b>	Indicates whether the tunnel has been set to admin <b>up</b> or <b>down</b> .
<b>Local IP</b>	IP address of the local endpoint.
<b>Remote IP</b>	IP address of the remote endpoint.
<b>NAT</b>	Whether Network Address Translation (NAT) has been applied.
<b>Peer/Service</b>	Enter the peer or service being used.
<b>Auto max BW enabled</b>	When enabled, allows the appliances to auto-negotiate the maximum tunnel bandwidth. Enabled by default.
<b>Max BW Kbps</b>	Maximum amount of bandwidth in kilobits per second. This field is not available if the Auto max BW enabled check box is selected.

**IKE Tab (for passthrough)**

Access the following fields by clicking the IKE tab on the Add Passthrough Tunnel dialog box. This tab is displayed only if the Mode field on the General tab is set to IPSec.

*IKE*

Field	Description
<b>Pre-shared key</b>	Pre-shared key used for IKE authentication.
<b>Authentication Algorithm</b>	<p>Authentication algorithm used for IKE security association (SA).</p> <ul style="list-style-type: none"> <li>If the IPSec Suite B Preset field on the General tab is set to None, you can select <b>SHA1</b>, <b>SHA2-256</b>, <b>SHA2-384</b>, or <b>SHA2-512</b>. The default setting is SHA1.</li> <li>If the IPSec Suite B Preset field is set to any other setting, this field is automatically set to the appropriate algorithm.</li> </ul> <p><b>NOTE</b> With IKEv2 and the Encryption algorithm field set to auto, AES-GCM will probably be negotiated, which includes encryption and authentication. In this case, this field might show a SHA setting that is not actually used.</p> <ul style="list-style-type: none"> <li>If the Encryption algorithm field is set to AES-GCM-128 or AES-GCM-256, this field is not applicable.</li> </ul>

Field	Description
<b>Encryption Algorithm</b>	<p>Encryption algorithm used for IKE security association (SA).</p> <ul style="list-style-type: none"> <li>If the IPSec Suite B Preset field on the General tab is set to None, and the IKE Version field is set to IKE v1, you can select <b>AES-CBC-128</b>, <b>AES-CBC-256</b>, or <b>auto</b>. The default setting is auto.</li> <li>If the IPSec Suite B Preset field is set to None, and the IKE Version field is set to IKE v2, you can select <b>AES-CBC-128</b>, <b>AES-CBC-256</b>, <b>AES-GCM-128</b>, <b>AES-GCM-256</b>, or <b>auto</b>. The default setting is auto.</li> <li>If the IPSec Suite B Preset field is set to any other setting, this field is automatically set to the appropriate algorithm.</li> </ul>
<b>Pseudo Random Function</b>	<p>This field is displayed only if the IKE Encryption Algorithm field is set to AES-GCM-128 or AES-GCM-256.</p> <ul style="list-style-type: none"> <li>For AES-GCM-128, you can select <b>SHA2-256</b>, <b>SHA2-384</b>, or <b>SHA2-512</b>.</li> <li>For AES-GCM-256, you can select <b>SHA-384</b> or <b>SHA-512</b>.</li> </ul>
<b>Diffie-Hellman Group</b>	<p>Diffie-Hellman Group used for IKE security association (SA) negotiation.</p> <ul style="list-style-type: none"> <li>If the IPSec Suite B Preset field on the General tab is set to None, you can select the appropriate group. Available groups are 1, 2, 5, 14 through 21, 26, and 31. For increased security, 14 or higher is recommended.</li> <li>If the IPSec Suite B Preset field is set to any other setting, this field is automatically set to the appropriate group.</li> </ul>
<b>Rekey interval/lifetime</b>	<p>Rekey interval/lifetime of IKE security association (SA) in minutes. The default is 360 minutes.</p>
<b>Dead peer detection</b>	<p><b>Delay time:</b> The interval (in seconds) to check the lifetime of the IKE peer.  <b>Retry count:</b> The number of times to retry the connection before determining that the connection is dead. This field is not editable.</p>
<b>IKE identifier</b>	<p>Identifier of the IKE tunnel. This field is displayed only if the IKE Version field is set to IKE v1. Select the type of identifier from the drop-down list:</p> <ul style="list-style-type: none"> <li><b>IP ADDRESS</b> – Specify the local public IP address, <i>not</i> the remote endpoint address.</li> <li><b>FQDN</b> – Specify the fully qualified domain name (also known as absolute domain name).</li> <li><b>USER_FQDN</b> – Specify an email address that contains an email domain.</li> </ul>

Field	Description
<b>Local IKE identifier</b>	Specify the local IKE identifier. This field is displayed only if the IKE Version field is set to IKE v2.
<b>Remote IKE identifier</b>	Specify the remote IKE identifier. This field is displayed only if the IKE Version field is set to IKE v2.
<b>Phase 1 mode</b>	Exchange mode for the IKE security association (SA) negotiation. <ul style="list-style-type: none"> <li>If the IKE Version field is set to IKE v1, you can select <b>Main</b> or <b>Aggressive</b>.</li> <li>If the IKE Version field is set to IKE v2, this field is automatically set to Aggressive.</li> </ul>
<b>IKE Version</b>	<ul style="list-style-type: none"> <li>If the IPSec Suite B Preset field on the General tab is set to None, you can select <b>IKE v1</b> or <b>IKE v2</b>.</li> <li>If the IPSec Suite B Preset field is set to any other setting, this field is automatically set to IKE v2.</li> </ul>

### IPSec tab (for passthrough)

Access the following fields by clicking the IPSec tab on the Add Passthrough Tunnel dialog box. This tab is displayed only if the Mode field on the General tab is set to IPSec.

#### IPSec

Field	Description
<b>Authentication algorithm</b>	Authentication algorithm used for the IPSec security association (SA). <ul style="list-style-type: none"> <li>If the IPSec Suite B Preset field on the General tab is set to None, you can select <b>SHA1</b>, <b>SHA2-256</b>, <b>SHA2-384</b>, <b>SHA2-512</b>, <b>AES-GMAC-128</b>, or <b>AES-GMAC-256</b>. The default setting is SHA1.</li> <li>If the IPSec Suite B Preset field is set to GMAC-128 or GMAC-256, this field is automatically set to the appropriate algorithm.</li> <li>If the IPSec Suite B Preset field is set to GCM-128 or GCM-256, this field is not applicable.</li> </ul>
<b>Encryption algorithm</b>	Encryption algorithm used for the IPSec security association (SA). <ul style="list-style-type: none"> <li>If the IPSec Suite B Preset field on the General tab is set to None, and the IPSec Authentication algorithm field is set to SHA1, SHA2-256, SHA2-384, or SHA2-512, you can select <b>AES-CBC-128</b>, <b>AEC-CBC-256</b>, <b>AES-GCM-128</b>, <b>AES-GCM-256</b>, <b>NULL</b>, or <b>Auto</b>. The default setting is Auto.</li> <li>If the IPSec Suite B Preset field is set to None, and the IPSec Authentication algorithm field is set to AES-GMAC-128 or AES-GMAC-256, this field is automatically set to NULL.</li> </ul>

Field	Description
<b>IPSec anti-replay window</b>	Select a size from the drop-down list or <b>Disable</b> to disable the IPSec anti-replay window. If a size is selected, protection is provided against an attacker duplicating encrypted packets by assigning a unique sequence number to each encrypted packet.
<b>Rekey interval/lifetime</b>	Rekey interval/lifetime of the IPSec security association (SA) in minutes. The default is 360 minutes.
<b>Perfect forward secrecy group</b>	Diffie-Hellman group used for IPSec security association (SA) negotiation. Based on the setting of the IPSec Suite B Preset field on the General tab, this field is set to the following Diffie-Hellman group: <ul style="list-style-type: none"> <li>For None: 14 (by default)</li> <li>For GCM-128 or GMAC-128: 19</li> <li>For GCM-256 or GMAC-256: 20</li> </ul>

#### 4. Click **Save**.

### Delete a Tunnel

To delete a tunnel listed in the table on the Underlay or Passthrough subtab of the Tunnels dialog box, click the corresponding delete icon (X) in the last column.

## Tunnel Exception

*Configuration > Networking > Tunnels > Tunnel Exception*

Orchestrator includes a tunnel exception feature that enables you to specify tunnel transactions between overlays. There are two ways you can enable this feature in Orchestrator.

You can configure tunnel exceptions through the Tunnel Exception tab.

1. Select the two appliances that you do not want connected via a tunnel.
2. Enter the Interface Labels.



The interface label can be any type of connection, such as **any**, **MPLS**, **Internet**, or **LTE**. Specifying the label excludes appliances within a given network to communicate with that particular appliance.

**NOTE** Use the description field to add a comment if you want to indicate why you are adding an exception.

## Schedule Auto MTU Discovery

*Configuration > Networking > Tunnels > Auto MTU Discovery*

Use this dialog box to schedule when to discover Auto MTU.



## Policies

These topics describe the pages related to managing access lists and policies.

### DNS Proxy Policies

*Configuration > Networking > DNS Proxy*

The DNS (Domain Name Server) Proxy stores public IP addresses with their associated domain name. Server A is used primarily as a private DNS to backhaul traffic and Server B is used to match all other domains that are not included under Server A. Server B is also used for public (cloud services) to breakout traffic. See the table below for the field descriptions on this tab.

Field	Description
Appliance	Name of the appliance associated with DNS proxy.
Segment	Name of the segment applied to your appliances, if enabled.
<b>DNS Proxy Enabled</b>	Whether the DNS Proxy is enabled. Select <b>True</b> or <b>False</b> .

Field	Description
<b>Interface</b>	Name of the interface associated with the DNS proxy.
<b>Server A Addresses</b>	IP addresses of Server A.
<b>Server A Domains</b>	Domain addresses of Server A.
<b>Server A Caching</b>	Whether you configured the server to be cached.
<b>Server B Addresses</b>	IP addresses of Server B.
<b>Server B Domains</b>	Domain addresses of Server B.
<b>Server B Caching</b>	Whether you configured the server to be cached.

## Configure DNS Proxy Policies

Complete the following steps to configure and define your DNS Proxy policies.

**NOTE** This feature is only configurable if you have loopback interfaces configured.

1. Choose whether you want to enable the DNS Proxy by selecting **ON** or **OFF**.
2. Select the name of the loopback interface or the LAN-side label associated with your DNS proxy.
3. Enter the IP addresses for Server A in the **Server A Addresses** field.
4. Choose whether you want caching to be **ON** or **OFF**. If selected, the domain name to the IP address mapping is cached. By default, caching is **ON**.
5. Enter the domain names of the Server A for the above IP addresses.
6. Enter Server B IP addresses in the **Server B Addresses** field. Server B will be used if there are no matches to the Server A domains.

**NOTE** You can **Clear DNS Cache**. This will erase the domain name to the IP address mapping you had cached for both Server A and B.

## Route Policies Tab

*Configuration > Templates & Policies > Policies > Route Policies*

The **Route Policies** report displays the route policy entries that exist on the appliance(s).

This includes the appliance-based defaults, entries applied manually (via the Appliance Manager or CLI), and entries that result from applying an Orchestrator Route Policies template, or applying Business Intent Overlays (if you are deploying an SD-WAN).

Each appliance's default behavior is to auto-optimize all IP traffic, automatically directing flows to the appropriate tunnel. **Auto-optimization** strategies reduce the need to create explicit route map entries for optimization. The three strategies provided are **TCP-based** auto-opt, **IP-based** auto-opt, and **subnet sharing**. By default, all three are enabled on the **Templates** tab, under **System**.

The Route Policy only requires entries for flows that are to be:

- Sent pass-through (shaped or unshaped)
- Dropped
- Configured for a specific high-availability deployment
- Routed based on application, VLAN, DSCP, or ACL (Access Control List)

You might also want to create a Route Policy entry when multiple tunnels exist to the remote **peer**, and you want the appliance to dynamically select the best path based on one of these criteria:

- Load balancing
- Lowest loss
- Lowest latency
- Specified tunnel

Manage these instances on the **Templates** tab, or select the **Edit** icon to manage Routing policies directly for a particular appliance.

If you are deploying an SD-WAN network and setting up Internet breakout from the branch, you must create manual route policy entries for sanctioned SaaS applications or Guest WiFi.

## Priority

- If you are using Orchestrator templates to add rules, Orchestrator will delete all entries from **1000 - 9999** before applying its policies.
- You can create rules with higher priority than Orchestrator rules (**1 - 999**) and rules with lower priority (**10000 - 19999** and **25000 - 65534**).

**NOTE** The priority range from **20000** to **24999** is reserved for Orchestrator.

- When adding a rule, the priority is incremented by 10 from the previous rule. The priority can be changed, but this default behavior helps to ensure you can insert new rules without having to change subsequent priorities.

## Match Criteria

- These are universal across all policy maps—**Route**, **QoS**, **Optimization**, **NAT** (Network Address Translation), and **Security**.

- If you expect to use the same match criteria in different maps, you can create an **ACL** (Access Control List), which is a named, reusable set of rules. For efficiency, create them in **Configuration > Templates & Policies > ACLs > Access Lists**, and apply them across appliances.
- The available parameters are **Application**, **Address Map** (for sorting by country, IP address owner, or SaaS application), **Domain**, **Geo Location**, **Interface**, **Protocol**, **DSCP**, **IP/Subnet**, **Port**, **Traffic Behavior Overlay**, **Fabric or Internet**, and **User Role** (the User Role as specified in the authentication exchange with the ClearPass RADIUS server).

**NOTE** User Role options include the RADIUS User Role, User Name, User Group, User Device, or User MAC. Configuring User Role match criteria enables an EdgeConnect to automatically assign traffic steering and firewall zone policies.

**NOTE** Additional attributes under the Address Map parameter can be used as match criteria. These attributes are secondary parameters to the address map, so the attributes are evaluated for a policy match only when the configured address map parameter matches the flow. To configure these attributes, click **+Attributes**.

- To specify different criteria for inbound versus outbound traffic, select the **Source:Dest** check box.

**NOTE** Source and destination role-based policies can be configured when both source and destination users are in the same network.

## Source or Destination

- An IP address can specify a subnet; for example, 10.10.10.0/24 (IPv4) or fe80::204:23ff:fed8:4ba2/64 (IPv6).
- To allow **any IP address**, use 0.0.0.0/0 (IPv4) or ::/0 (IPv6).
- Ports are available only for the protocols **tcp**, **udp**, and **tcp/udp**.
- To allow **any port**, use **0**.

## Wildcard-based Prefix Matching Rules

- Even when using a range or a wildcard, the IPv4 address must be specified in the 4-octet format, separated by the dot notation. For example, **A.B.C.D**.
- Range is specified using a single dash. For example, **128-129**.
- Wildcard is specified as an asterisk (\*).
- Range and Wildcard can both be used in the same address, but an octet can only contain one or the other. For example, **10.136-137.\*.64-95**.
- A wildcard can only be used to define an entire octet. For example, **10.13\*.\*.64-95** is not supported. Use **10.130-139.\*.64-95** to specify this range.
- The same rules apply to IPv6 addressing.
- CIDR notation and (Range or Wildcard) are mutually exclusive in the same address. For example, **192.168.0.1-127/24** is not supported. Use either **192.168.0.0/24** or **192.168.0.1-127**.

- These prefix-matching rules apply to the following policies only: Route, QoS, Optimization, NAT, Security, and ACLs.

## Route Policies Edit Row

The **Route Policies** report displays the route policy entries that exist on the appliance(s).

This includes the appliance-based defaults, entries applied manually (via the Appliance Manager or CLI), and entries that result from applying an Orchestrator Route Policies template, or applying Business Intent Overlays (if you are deploying an SD-WAN).

Each appliance's default behavior is to auto-optimize all IP traffic, automatically directing flows to the appropriate tunnel. **Auto-optimization** strategies reduce the need to create explicit route map entries for optimization. The three strategies provided are **TCP-based** auto-opt, **IP-based** auto-opt, and **subnet sharing**. By default, all three are enabled on the **Templates** tab, under **System**.

The Route Policy, then, only requires entries for flows that are to be:

- Sent pass-through (shaped or unshaped)
- Dropped
- Configured for a specific high-availability deployment
- Routed based on application, VLAN, DSCP, or ACL (Access Control List)

You might also want to create a Route Policy entry when multiple tunnels exist to the remote **peer**, and you want the appliance to dynamically select the best path based on one of these criteria:

- Load balancing
- Lowest loss
- Lowest latency
- Specified tunnel

Manage these instances on the **Templates** tab, or click the **Edit** icon to manage Route policies directly for a particular appliance.

If you are deploying an SD-WAN network and setting up Internet breakout from the branch, you must create manual route policy entries for sanctioned SaaS applications or Guest WiFi.

## Priority

- If you are using Orchestrator templates to add rules, Orchestrator will delete all entries from **1000 - 9999** before applying its policies.
- You can create rules with higher priority than Orchestrator rules (**1 - 999**) and rules with lower priority (**10000 - 19999** and **25000 - 65534**).

**NOTE** The priority range from **20000** to **24999** is reserved for Orchestrator.

- When adding a rule, the priority is incremented by 10 from the previous rule. The priority can be changed, but this default behavior helps to ensure you can insert new rules without having to change subsequent priorities.

## Match Criteria

- These are universal across all policy maps—**Route**, **QoS**, **Optimization**, **NAT** (Network Address Translation), and **Security**.
- If you expect to use the same match criteria in different maps, you can create an **ACL** (Access Control List), which is a named, reusable set of rules. For efficiency, create them in **Configuration > Templates & Policies > ACLs > Access Lists**, and apply them across appliances.
- The available parameters are **Application**, **Address Map** (for sorting by country, IP address owner, or SaaS application), **Domain**, **Geo Location**, **Interface**, **Protocol**, **DSCP**, **IP/Subnet**, **Port**, **Traffic Behavior Overlay**, **Fabric or Internet**, and **User Role** (the User Role as specified in the authentication exchange with the ClearPass RADIUS server).

**NOTE** User Role options include the RADIUS User Role, User Name, User Group, User Device, or User MAC. Configuring User Role match criteria enables an EdgeConnect to automatically assign traffic steering and firewall zone policies.

**NOTE** Additional attributes under the Address Map parameter can be used as match criteria. These attributes are secondary parameters to the address map, so the attributes are evaluated for a policy match only when the configured address map parameter matches the flow. To configure these attributes, click **+Attributes**.

- To specify different criteria for inbound versus outbound traffic, select the **Source:Dest** check box.

**NOTE** Source and destination role-based policies can be configured when both source and destination users are in the same network.

## Source or Destination

- An IP address can specify a subnet; for example, 10.10.10.0/24 (IPv4) or fe80::204:23ff:fed8:4ba2/64 (IPv6).
- To allow **any IP address**, use 0.0.0.0/0 (IPv4) or ::/0 (IPv6).
- Ports are available only for the protocols **tcp**, **udp**, and **tcp/udp**.
- To allow **any port**, use 0.

## Wildcard-based Prefix Matching Rules

- Even when using a range or a wildcard, the IPv4 address must be specified in the 4-octet format, separated by the dot notation. For example, A.B.C.D.
- Range is specified using a single dash. For example, **128-129**.
- Wildcard is specified as an asterisk (\*).
- Range and Wildcard can both be used in the same address, but an octet can only contain one or the other. For example, **10.136-137.\*.64-95**.

- A wildcard can only be used to define an entire octet. For example, **10.13\*.\*.64-95** is not supported. Use **10.130-139.\*.64-95** to specify this range.
- The same rules apply to IPv6 addressing.
- CIDR notation and (Range or Wildcard) are mutually exclusive in the same address. For example, **192.168.0.1-127/24** is not supported. Use either **192.168.0.0/24** or **192.168.0.1-127**.
- These prefix-matching rules apply to the following policies only: Route, QoS, Optimization, NAT, Security, and ACLs.

## QoS Policies Tab

*Configuration > Templates & Policies > Policies > QoS Policies*

QoS Policy determines how flows are queued and marked.

The **QoS Policies** tab displays the QoS policy entries that exist on the appliances. This includes the appliance-based defaults, entries applied manually (via the Appliance Manager or CLI), and entries that result from applying an Orchestrator QoS Policy template or Business Intent Overlay.

Use the **Shaper** to define, prioritize, and name traffic classes.

Think of it as the Shaper **defines** and the QoS Policy **assigns**.

Use the **Templates** tab to create and manage QoS policies for multiple appliances, or click the **Edit** icon to manage QoS Policies directly for a particular appliance.

Appliance	Map	Priority	Match Criteria	Traffic Class	LAN QoS	WAN QoS	Comment
map1 (active)	20000	Overlay	RealTime	1 - RealTime	trust-lan	trust-lan	Generated by system for overlay: RealTime
map1 (active)	20001	Overlay	CriticalApps	2 - CriticalApps	trust-lan	trust-lan	Generated by system for overlay: CriticalApps
map1 (active)	20002	Overlay	BulkApps	3 - BulkApps	trust-lan	trust-lan	Generated by system for overlay: BulkApps
map1 (active)	20003	Overlay	DefaultOverlay	4 - Default	trust-lan	trust-lan	Generated by system for overlay: DefaultOverlay
map1 (active)	20004	ACL	Overlay_Overlay	1 - RealTime	trust-lan	trust-lan	RealTime overlay
map1 (active)	20005	ACL	Overlay_CriticalApps	2 - CriticalApps	trust-lan	trust-lan	CriticalApps overlay
map1 (active)	20006	ACL	Overlay_BulkApps	3 - BulkApps	trust-lan	trust-lan	BulkApps overlay
map1 (active)	20007	ACL	Overlay_DefaultOverlay	4 - Default	trust-lan	trust-lan	DefaultOverlay overlay
map1 (active)	65535	Protocol	ip	1 - RealTime	trust-lan	trust-lan	
map1 (active)	20000	Overlay	RealTime	1 - RealTime	trust-lan	trust-lan	Generated by system for overlay: RealTime

The QoS Policy's SET actions determine two things:

- To what traffic class a shaped flow—optimized or pass-through—is assigned
- Whether to trust incoming DSCP markings for LAN QoS and WAN QoS, or to remark them as they leave for the WAN

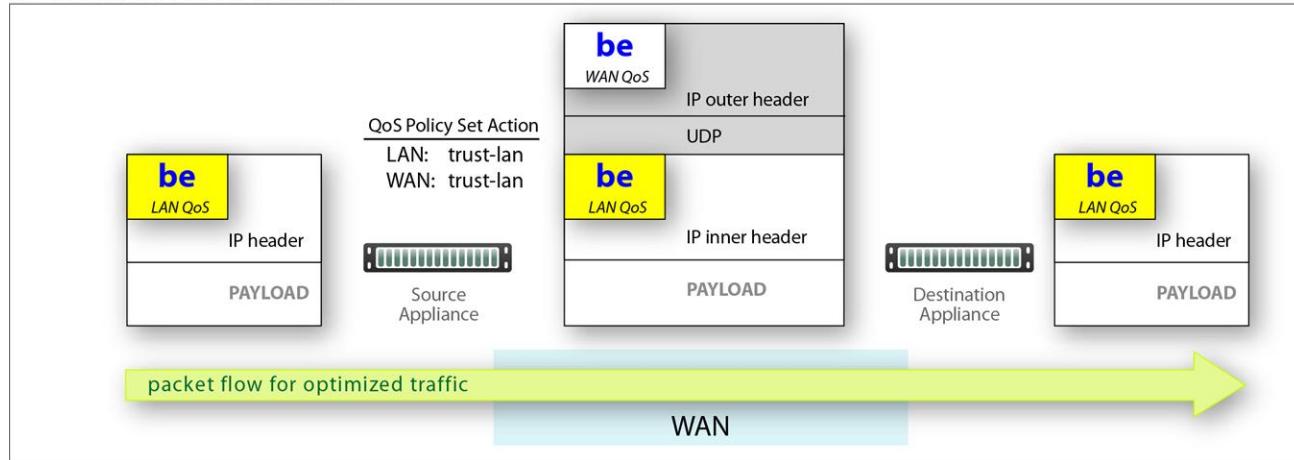
## Handle and Mark DSCP Packets

- DSCP markings specify end-to-end QoS policies throughout a network.
- The default values for **LAN QoS** and **WAN QoS** are **trust-lan**.

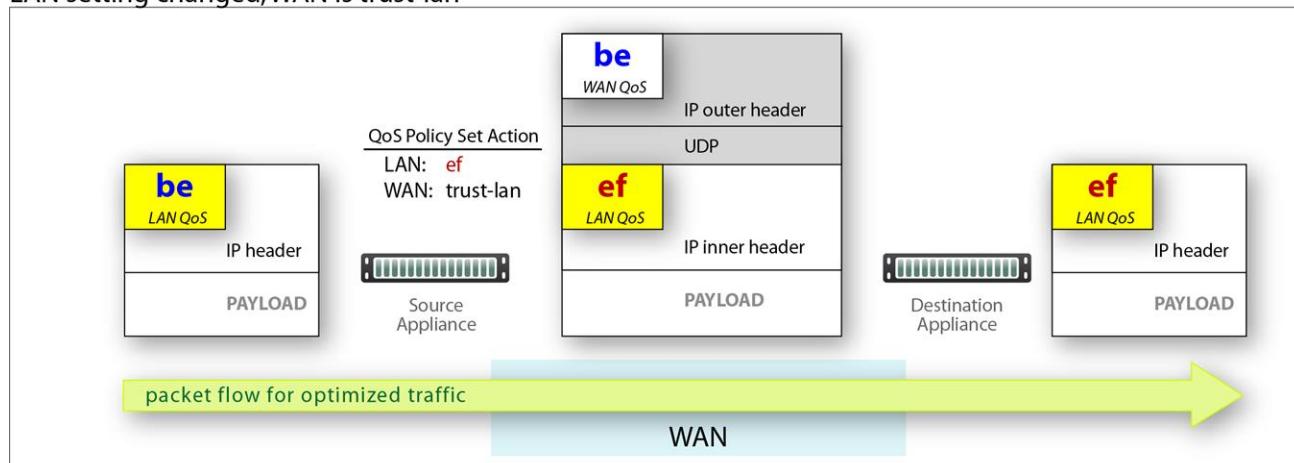
### Apply DSCP Markings to Optimized (Tunnelized) Traffic

- The appliance encapsulates optimized traffic. This adds an IP outer header to packets for travel across the WAN. This outer header contains the **WAN QoS** DSCP marking.
- **LAN QoS** - The DSCP marking applied to the IP header before encapsulation.
- **WAN QoS** - The DSCP marking in the encapsulating outer IP header. The remote appliance removes the outer IP header.

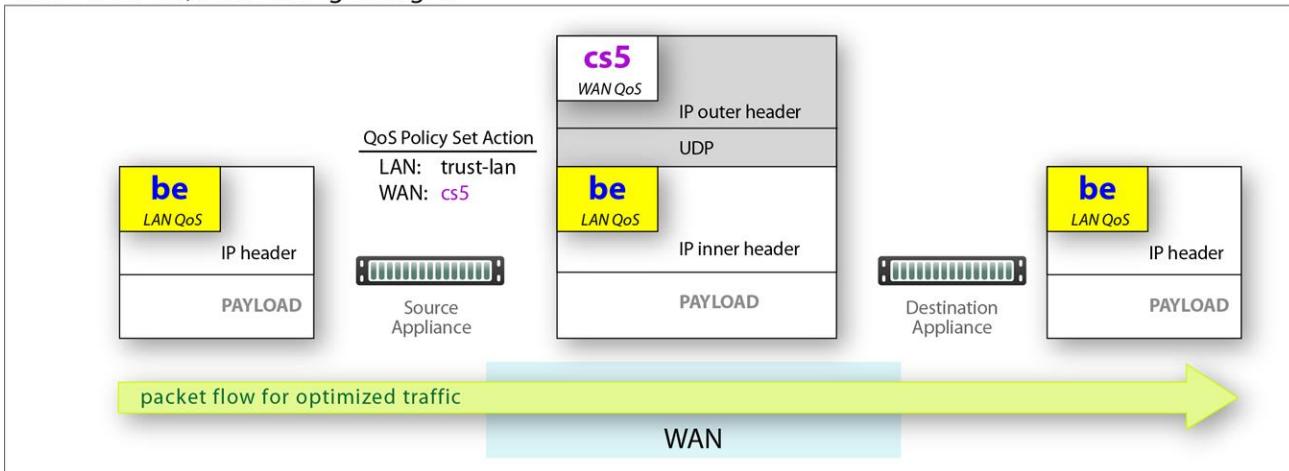
#### LAN and WAN set to trust-lan



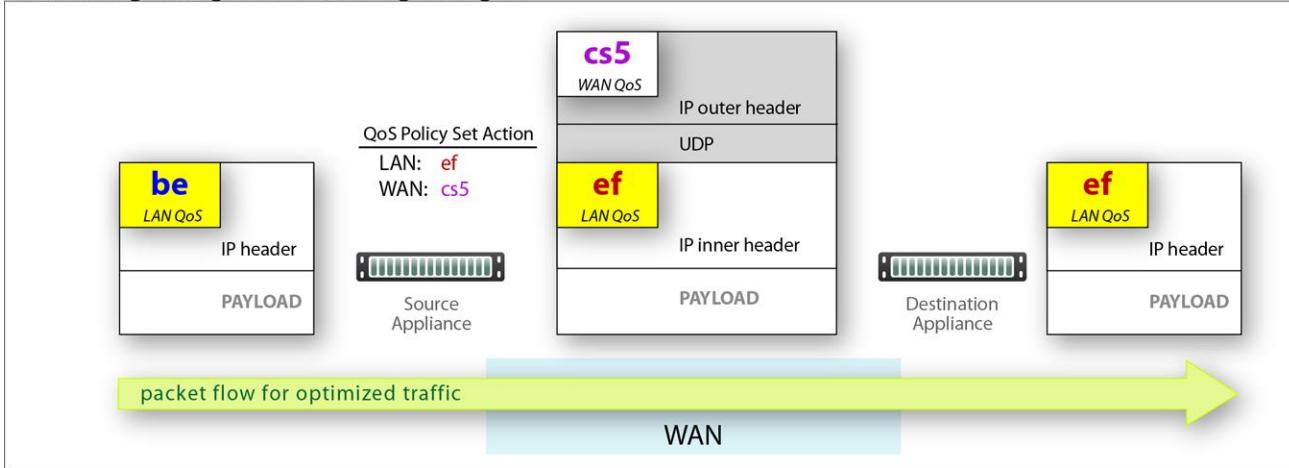
#### LAN setting changed, WAN is trust-lan



### LAN is trust-lan, WAN setting changed



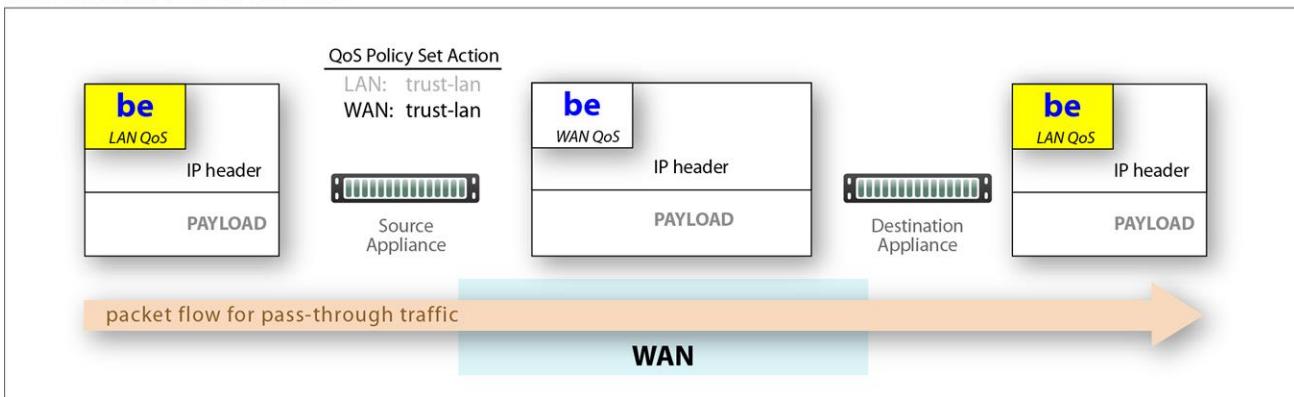
### LAN setting changed, WAN setting changed



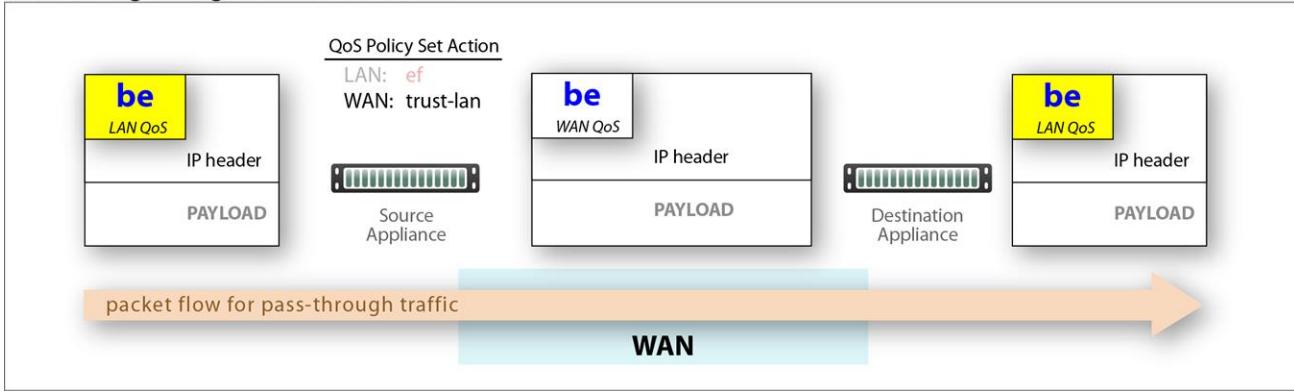
### Apply DSCP Markings to Pass-through Traffic

- The appliance applies the QoS Policy's DSCP markings to all pass-through flows—shaped and unshaped.
- Pass-through traffic does not receive an additional header, so it is handled differently:
  - The Optimization Policy's **LAN QoS** Set Action is ignored.
  - The specified **WAN QoS** marking replaces the packet's existing **LAN QoS** DSCP marking.
  - When the packet reaches the remote appliance, it retains the modified QoS setting as it travels to its destination.

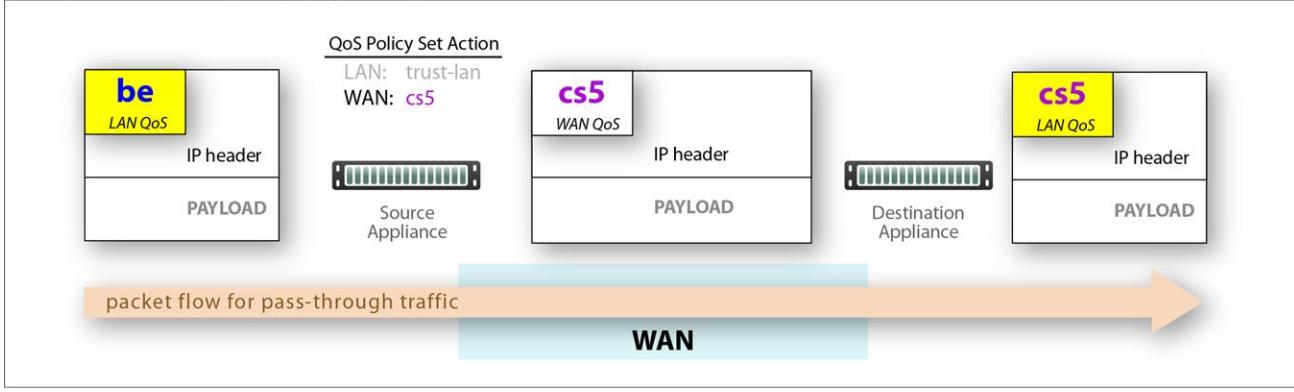
### LAN and WAN set to trust-lan



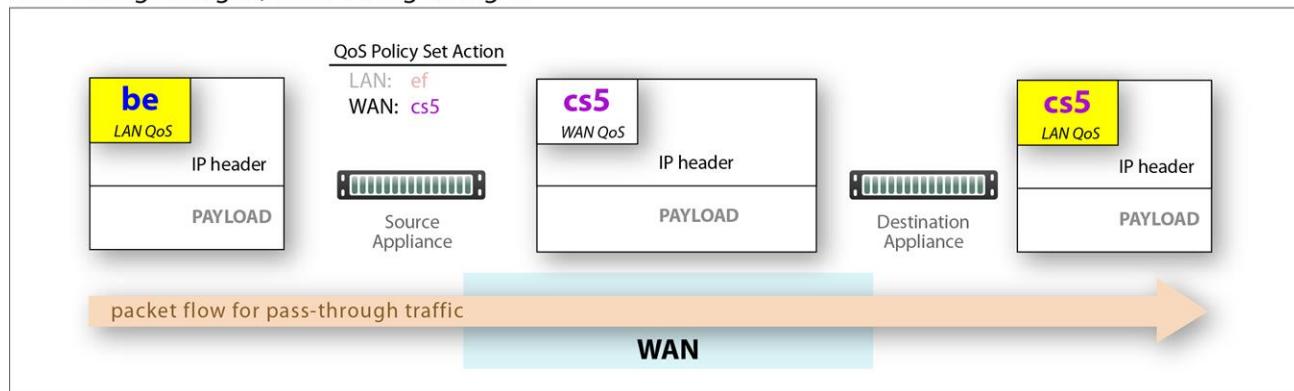
### LAN setting changed, WAN is trust-lan



### LAN is trust-lan, WAN setting changed



## LAN setting changed, WAN setting changed



## Priority

- If you are using Orchestrator templates to add rules, Orchestrator will delete all entries from **1000 - 9999** before applying its policies.
- You can create rules with higher priority than Orchestrator rules (**1 - 999**) and rules with lower priority (**10000 - 19999** and **25000 - 65534**).

**NOTE** The priority range from **20000** to **24999** is reserved for Orchestrator.

- When adding a rule, the priority is incremented by 10 from the previous rule. The priority can be changed, but this default behavior helps to ensure you can insert new rules without having to change subsequent priorities.

## Match Criteria

- These are universal across all policy maps—**Route**, **QoS**, **Optimization**, **NAT** (Network Address Translation), and **Security**.
- If you expect to use the same match criteria in different maps, you can create an **ACL** (Access Control List), which is a named, reusable set of rules. For efficiency, create them in **Configuration > Templates & Policies > ACLs > Access Lists**, and apply them across appliances.
- The available parameters are **Application**, **Address Map** (for sorting by country, IP address owner, or SaaS application), **Domain**, **Geo Location**, **Interface**, **Protocol**, **DSCP**, **IP/Subnet**, **Port**, **Traffic Behavior Overlay**, **Fabric or Internet**, and **User Role** (the User Role as specified in the authentication exchange with the ClearPass RADIUS server).

**NOTE** User Role options include the RADIUS User Role, User Name, User Group, User Device, or User MAC. Configuring User Role match criteria enables an EdgeConnect to automatically assign traffic steering and firewall zone policies.

**NOTE** Additional attributes under the Address Map parameter can be used as match criteria. These attributes are secondary parameters to the address map, so the attributes are evaluated for a policy match only when the configured address map parameter matches the flow. To configure these attributes, click **+Attributes**.

- To specify different criteria for inbound versus outbound traffic, select the **Source:Dest** check box.

**NOTE** Source and destination role-based policies can be configured when both source and destination users are in the same network.

## Source or Destination

- An IP address can specify a subnet; for example, 10.10.10.0/24 (IPv4) or fe80::204:23ff:fed8:4ba2/64 (IPv6).
- To allow **any IP address**, use 0.0.0.0/0 (IPv4) or ::/0 (IPv6).
- Ports are available only for the protocols **tcp**, **udp**, and **tcp/udp**.
- To allow **any port**, use **0**.

## Wildcard-based Prefix Matching Rules

- Even when using a range or a wildcard, the IPv4 address must be specified in the 4-octet format, separated by the dot notation. For example, **A.B.C.D**.
- Range is specified using a single dash. For example, **128-129**.
- Wildcard is specified as an asterisk (\*).
- Range and Wildcard can both be used in the same address, but an octet can only contain one or the other. For example, **10.136-137.\*.64-95**.
- A wildcard can only be used to define an entire octet. For example, **10.13\*.\*.64-95** is not supported. Use **10.130-139.\*.64-95** to specify this range.
- The same rules apply to IPv6 addressing.
- CIDR notation and (Range or Wildcard) are mutually exclusive in the same address. For example, **192.168.0.1-127/24** is not supported. Use either **192.168.0.0/24** or **192.168.0.1-127**.
- These prefix-matching rules apply to the following policies only: Route, QoS, Optimization, NAT, Security, and ACLs.

## QoS Policies Edit Row

QoS Policy determines how flows are queued and marked.

The **QoS Policies** tab displays the QoS policy entries that exist on the appliances. This includes the appliance-based defaults, entries applied manually (via the Appliance Manager or CLI), and entries that result from applying an Orchestrator QoS Policy template or Business Intent Overlay.

Use the **Shaper** to define, prioritize, and name traffic classes. Think of it as the Shaper **defines** and the QoS Policy **assigns**.

Use the **Templates** tab to create and manage QoS policies for multiple appliances, or click the **Edit** icon to directly manage QoS Policies for a particular appliance.

The QoS Policy's SET actions determine two things:

- To what traffic class a shaped flow—optimized or pass-through—is assigned
- Whether to trust incoming DSCP markings for LAN QoS and WAN QoS, or to remark them as they leave for the WAN

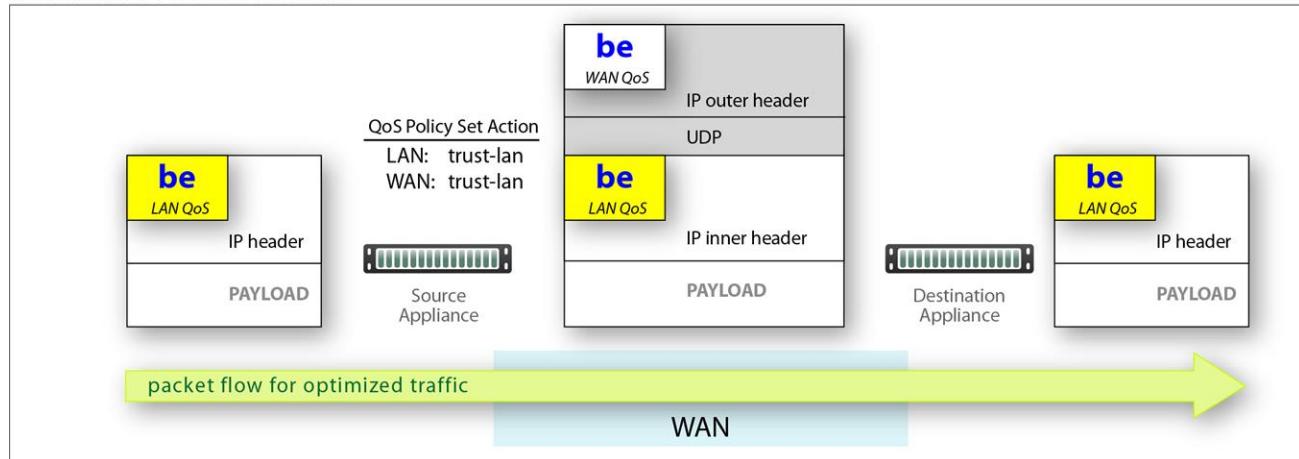
## Handle and Mark DSCP Packets

- DSCP markings specify end-to-end QoS policies throughout a network.
- The default values for **LAN QoS** and **WAN QoS** are **trust-lan**.

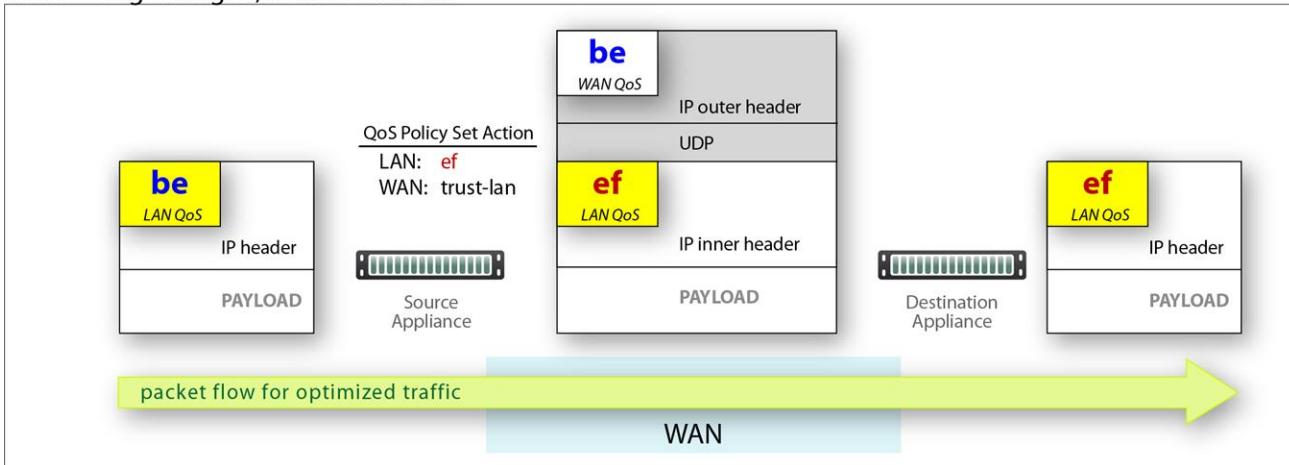
## Apply DSCP Markings to Optimized (Tunnelized) Traffic

- The appliance encapsulates optimized traffic. This adds an IP outer header to packets for travel across the WAN. This outer header contains the **WAN QoS** DSCP marking.
- **LAN QoS** - The DSCP marking applied to the IP header before encapsulation.
- **WAN QoS** - The DSCP marking in the encapsulating outer IP header. The remote appliance removes the outer IP header.

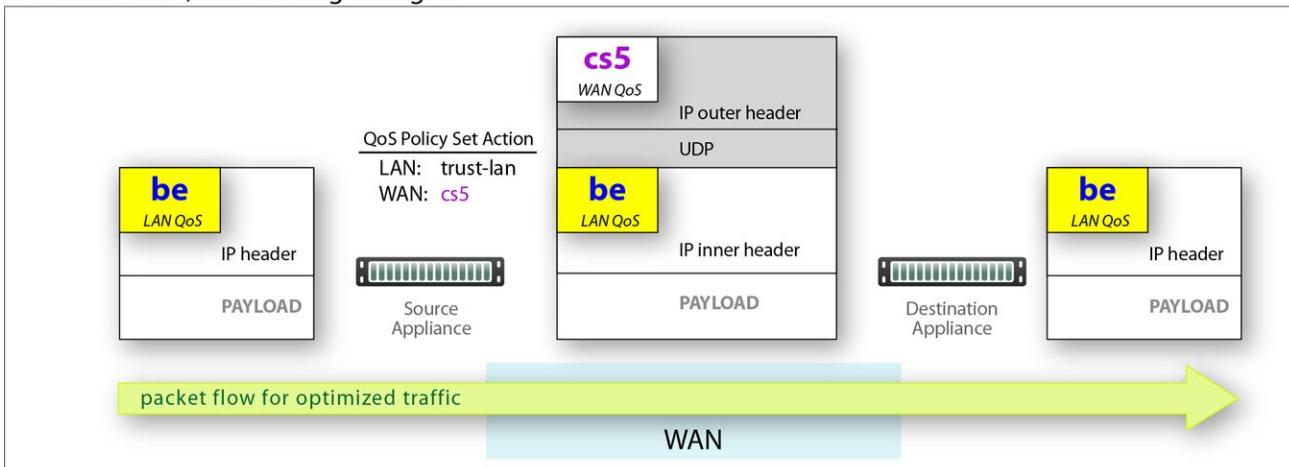
### LAN and WAN set to trust-lan



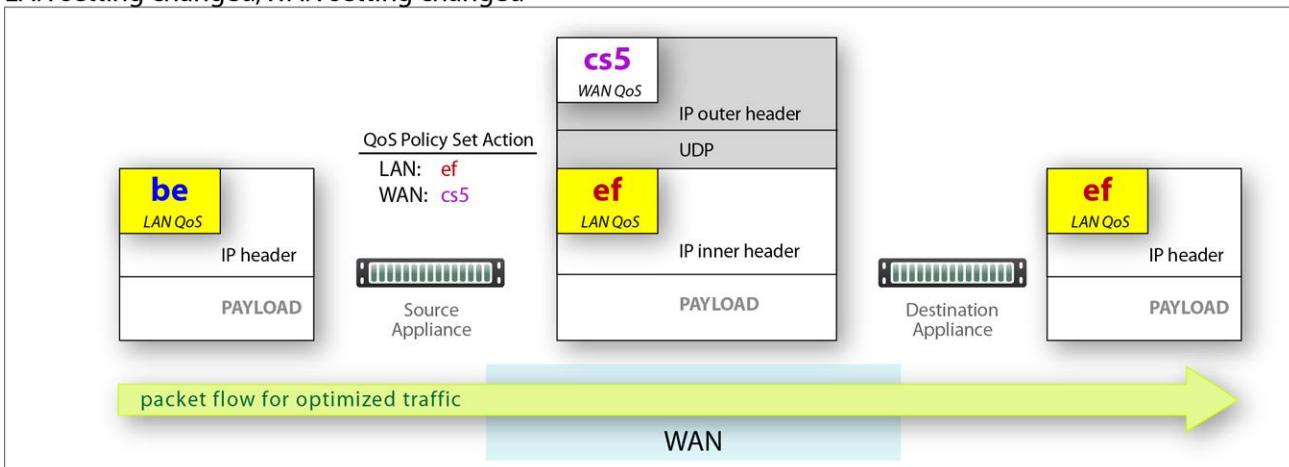
## LAN setting changed, WAN is trust-lan



## LAN is trust-lan, WAN setting changed



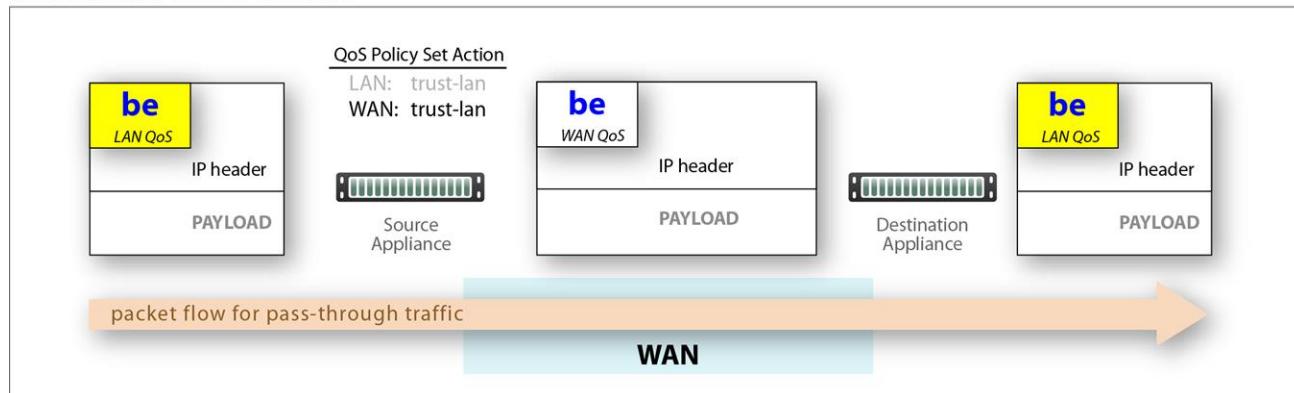
## LAN setting changed, WAN setting changed



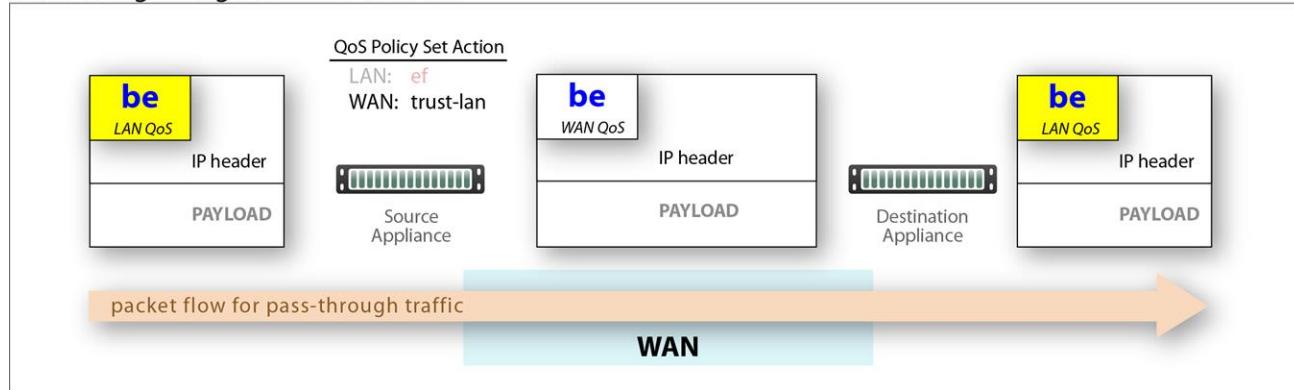
## Apply DSCP Markings to Pass-through Traffic

- The appliance applies the QoS Policy's DSCP markings to all pass-through flows—shaped and unshaped.
- Pass-through traffic does not receive an additional header, so it is handled differently:
  - The Optimization Policy's **LAN QoS** Set Action is ignored.
  - The specified **WAN QoS** marking replaces the packet's existing **LAN QoS** DSCP marking.
  - When the packet reaches the remote appliance, it retains the modified QoS setting as it travels to its destination.

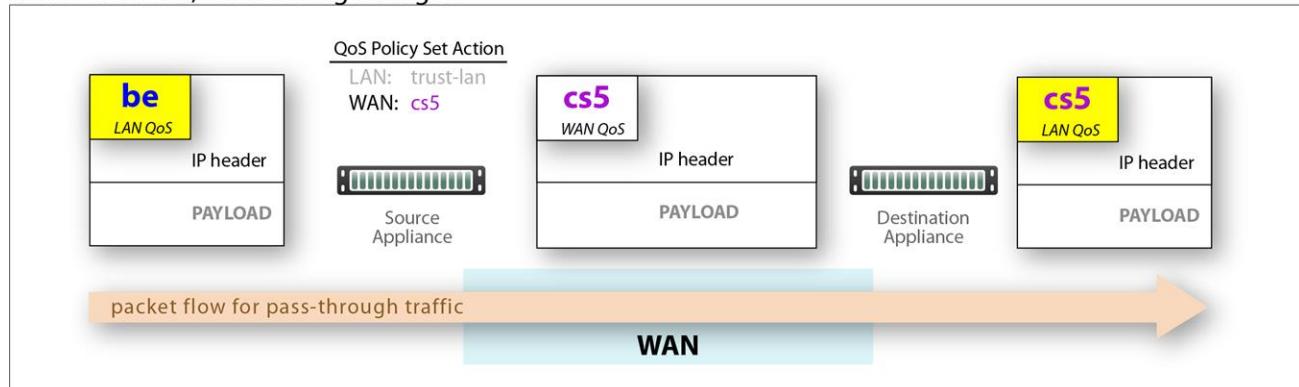
LAN and WAN set to trust-lan



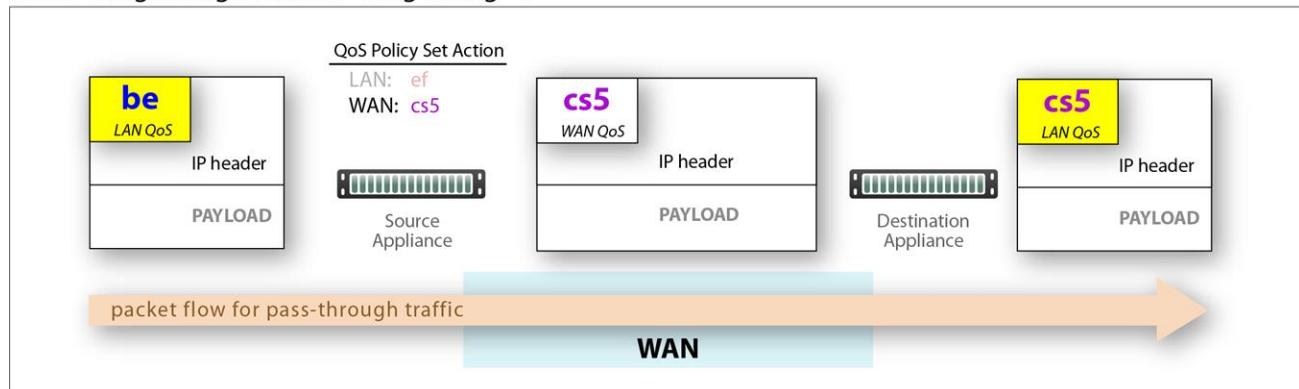
LAN setting changed, WAN is trust-lan



### LAN is trust-lan, WAN setting changed



### LAN setting changed, WAN setting changed



## Priority

- If you are using Orchestrator templates to add rules, Orchestrator will delete all entries from **1000 - 9999** before applying its policies.
- You can create rules with higher priority than Orchestrator rules (**1 - 999**) and rules with lower priority (**10000 - 19999** and **25000 - 65534**).

**NOTE** The priority range from **20000** to **24999** is reserved for Orchestrator.

- When adding a rule, the priority is incremented by 10 from the previous rule. The priority can be changed, but this default behavior helps to ensure you can insert new rules without having to change subsequent priorities.

## Match Criteria

- These are universal across all policy maps—**Route**, **QoS**, **Optimization**, **NAT** (Network Address Translation), and **Security**.

- If you expect to use the same match criteria in different maps, you can create an **ACL** (Access Control List), which is a named, reusable set of rules. For efficiency, create them in **Configuration > Templates & Policies > ACLs > Access Lists**, and apply them across appliances.
- The available parameters are **Application**, **Address Map** (for sorting by country, IP address owner, or SaaS application), **Domain**, **Geo Location**, **Interface**, **Protocol**, **DSCP**, **IP/Subnet**, **Port**, **Traffic Behavior Overlay**, **Fabric or Internet**, and **User Role** (the User Role as specified in the authentication exchange with the ClearPass RADIUS server).

**NOTE** User Role options include the RADIUS User Role, User Name, User Group, User Device, or User MAC. Configuring User Role match criteria enables an EdgeConnect to automatically assign traffic steering and firewall zone policies.

**NOTE** Additional attributes under the Address Map parameter can be used as match criteria. These attributes are secondary parameters to the address map, so the attributes are evaluated for a policy match only when the configured address map parameter matches the flow. To configure these attributes, click **+Attributes**.

- To specify different criteria for inbound versus outbound traffic, select the **Source:Dest** check box.

**NOTE** Source and destination role-based policies can be configured when both source and destination users are in the same network.

## Source or Destination

- An IP address can specify a subnet; for example, 10.10.10.0/24 (IPv4) or fe80::204:23ff:fed8:4ba2/64 (IPv6).
- To allow **any IP address**, use 0.0.0.0/0 (IPv4) or ::/0 (IPv6).
- Ports are available only for the protocols **tcp**, **udp**, and **tcp/udp**.
- To allow **any port**, use 0.

## Wildcard-based Prefix Matching Rules

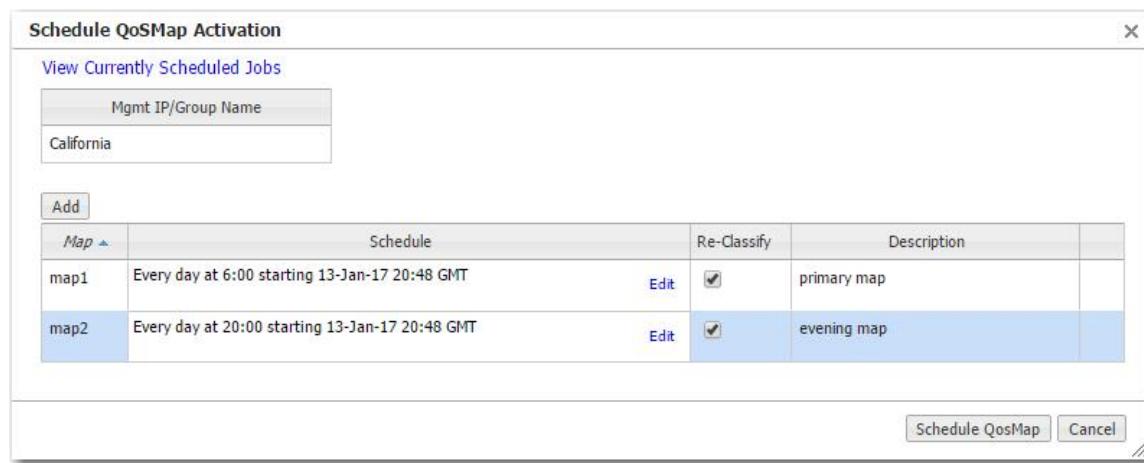
- Even when using a range or a wildcard, the IPv4 address must be specified in the 4-octet format, separated by the dot notation. For example, A.B.C.D.
- Range is specified using a single dash. For example, 128-129.
- Wildcard is specified as an asterisk (\*).
- Range and Wildcard can both be used in the same address, but an octet can only contain one or the other. For example, 10.136-137.\*.64-95.
- A wildcard can only be used to define an entire octet. For example, 10.13\*.\*.64-95 is not supported. Use 10.130-139.\*.64-95 to specify this range.
- The same rules apply to IPv6 addressing.
- CIDR notation and (Range or Wildcard) are mutually exclusive in the same address. For example, 192.168.0.1-127/24 is not supported. Use either 192.168.0.0/24 or 192.168.0.1-127.

- These prefix-matching rules apply to the following policies only: Route, QoS, Optimization, NAT, Security, and ACLs.

## Schedule QoS Map Activation

*Configuration > Templates & Policies > Policies > Schedule QoSMap Activation*

You can schedule appliances to apply different QoS maps at different times.



Before using this option, verify the following:

- The desired Template Group has the QoS maps you need.
- You have applied the Template Group to the appliances you want to schedule.

**TIP** To specify the timezone for scheduled jobs and reports, use the Schedule Timezone window (**Orchestrator > Software & Setup > Setup > Timezone for Scheduled Jobs**).

## Optimization Policies Tab

*Configuration > Templates & Policies > Policies > Optimization Policies*

The **Optimization Policies** tab displays the Optimization policy entries that exist on the appliances. This includes the appliance-based defaults, entries applied manually (via the Appliance Manager or CLI), and entries that result from applying an Orchestrator Optimization Policy template or Business Intent Overlay.

Use the **Templates** tab to create and manage Optimization policies, or click the edit icon to manage Optimization policies directly for a particular appliance.

Edit	Appliance	Map	Priority	Match Criteria	Network Memory	IP Header Compression	Replied Compression	TCP Accel	TCP Accel Details	Protocol Accel	Comment
✓	Hamburg-Bill	PRODUCTION (active)	1005	User Role IoT	disabled	Yes	No	(i)	none	disable boost for IoT	
✓	Hamburg-Bill	PRODUCTION (active)	1008	Application CIFS_verb_Ether_BTSolver	balanced	Yes	Yes	(i)	none	WAN Optimization Demo	
✓	Hamburg-Bill	PRODUCTION (active)	1009	Ether_BTSolver	monocle latency	Yes	Yes	(i)	none	apply test web application test	
✓	Hamburg-Bill	PRODUCTION (active)	1013	Ether_Address_Group	disabled	Yes	No	(i)	none	Handle APPLA Input	
✓	Hamburg-Bill	PRODUCTION (active)	1013	Ether_BTSolver	disabled	Yes	No	(i)	none	allow APPLA application traffic	
✓	Hamburg-Bill	PRODUCTION (active)	1017	Application group_sports	disabled	Yes	No	(i)	none	enable sport	
✓	Hamburg-Bill	PRODUCTION (active)	1018	Application group_Cards	disabled	Yes	No	(i)	none	allow game events	
✓	Hamburg-Bill	PRODUCTION (active)	1019	Application Silverleaf_gwF	disabled	Yes	No	(i)	none	enable MTR for link integrity tests	
✓	Hamburg-Bill	PRODUCTION (active)	1021	Application_SportT2	disabled	Yes	No	(i)	none	enable MTR for link sportT default port	
✓	Hamburg-Bill	PRODUCTION (active)	1040	Application group_Speedtest	disabled	Yes	No	(i)	none	remove speedtest site	
✓	Hamburg-Bill	PRODUCTION (active)	1070	Application_SilverleafOrch	disabled	Yes	No	(i)	none	allow CloudOrch	
✓	Hamburg-Bill	PRODUCTION (active)	1123	Application group_RTP	disabled	Yes	No	(i)	none	allow RTP + ARPTA	
✓	Hamburg-Bill	PRODUCTION (active)	1221	Application_Netflow	monocle latency	Yes	Yes	No	(i)	none	Netflow and DPD override - RUEK
✓	Hamburg-Bill	PRODUCTION (active)	1228	Application_System	monocle latency	Yes	No	(i)	none	syslog override - SPLASH	
✓	Hamburg-Bill	PRODUCTION (active)	1601	Port 23	disabled	Yes	No	(i)	none	enable telnet	
✓	Hamburg-Bill	PRODUCTION (active)	1602	Port 133	disabled	Yes	No	(i)	none	enable ssh	
✓	Hamburg-Bill	PRODUCTION (active)	1612	Overlay_REALTIME	disabled	Yes	No	(i)	none	REALTIME override	
✓	Hamburg-Bill	PRODUCTION (active)	1627	Overlay_GUEST	disabled	Yes	No	(i)	none	GUEST override	
✓	Hamburg-Bill	PRODUCTION (active)	1632	Overlay_BESTPORT	disabled	Yes	No	(i)	none	BESTPORT override	
✓	Hamburg-Bill	PRODUCTION (active)	1640	Overlay_RECREATIONAL	monocle latency	Yes	Yes	(i)	none	RECREATIONAL override	
✓	Hamburg-Bill	PRODUCTION (active)	1672	Overlay_CASB	disabled	Yes	No	(i)	none	CASB override	
✓	Hamburg-Bill	PRODUCTION (active)	1675	Overlay_DEFAULT	monocle latency	Yes	Yes	(i)	none	DEFAULT override	
			6535	Match Everything	balanced	Yes	Yes	(i)	none		

## Priority

- If you are using Orchestrator templates to add rules, Orchestrator will delete all entries from **1000 - 9999** before applying its policies.
- You can create rules with higher priority than Orchestrator rules (**1 - 999**) and rules with lower priority (**10000 - 19999** and **25000 - 65534**).

**NOTE** The priority range from **20000** to **24999** is reserved for Orchestrator.

- When adding a rule, the priority is incremented by 10 from the previous rule. The priority can be changed, but this default behavior helps to ensure you can insert new rules without having to change subsequent priorities.

## Match Criteria

- These are universal across all policy maps—**Route**, **QoS**, **Optimization**, **NAT** (Network Address Translation), and **Security**.
- If you expect to use the same match criteria in different maps, you can create an **ACL** (Access Control List), which is a named, reusable set of rules. For efficiency, create them in **Configuration > Templates & Policies > ACLs > Access Lists**, and apply them across appliances.
- The available parameters are **Application**, **Address Map** (for sorting by country, IP address owner, or SaaS application), **Domain**, **Geo Location**, **Interface**, **Protocol**, **DSCP**, **IP/Subnet**, **Port**, **Traffic Behavior Overlay**, **Fabric or Internet**, and **User Role** (the User Role as specified in the authentication exchange with the ClearPass RADIUS server).

**NOTE** User Role options include the RADIUS User Role, User Name, User Group, User Device, or User MAC. Configuring User Role match criteria enables an EdgeConnect to automatically assign traffic steering and firewall zone policies.

**NOTE** Additional attributes under the Address Map parameter can be used as match criteria. These attributes are secondary parameters to the address map, so the attributes are evaluated for a policy match only when the configured address map parameter matches the flow. To configure these attributes, click **+Attributes**.

- To specify different criteria for inbound versus outbound traffic, select the **Source:Dest** check box.

**NOTE** Source and destination role-based policies can be configured when both source and destination users are in the same network.

## Source or Destination

- An IP address can specify a subnet; for example, 10.10.10.0/24 (IPv4) or fe80::204:23ff:fed8:4ba2/64 (IPv6).
- To allow **any IP address**, use 0.0.0.0/0 (IPv4) or ::/0 (IPv6).
- Ports are available only for the protocols **tcp**, **udp**, and **tcp/udp**.
- To allow **any port**, use **0**.

## Wildcard-based Prefix Matching Rules

- Even when using a range or a wildcard, the IPv4 address must be specified in the 4-octet format, separated by the dot notation. For example, **A.B.C.D**.
- Range is specified using a single dash. For example, **128-129**.
- Wildcard is specified as an asterisk (\*).
- Range and Wildcard can both be used in the same address, but an octet can only contain one or the other. For example, **10.136-137.\*.64-95**.
- A wildcard can only be used to define an entire octet. For example, **10.13\*.\*.64-95** is not supported. Use **10.130-139.\*.64-95** to specify this range.
- The same rules apply to IPv6 addressing.
- CIDR notation and (Range or Wildcard) are mutually exclusive in the same address. For example, **192.168.0.1-127/24** is not supported. Use either **192.168.0.0/24** or **192.168.0.1-127**.
- These prefix-matching rules apply to the following policies only: Route, QoS, Optimization, NAT, Security, and ACLs.

## Set Actions

Set Action	Description
<b>Network Memory</b>	<p>Addresses limited bandwidth. This technology uses advanced fingerprinting algorithms to examine all incoming and outgoing WAN traffic. Network Memory localizes information and transmits only modifications between locations.</p> <ul style="list-style-type: none"> <li>• <b>Maximize Reduction</b> – Optimizes for maximum data reduction at the potential cost of slightly lower throughput and/or some increase in latency. It is appropriate for bulk data transfers such as file transfers and FTP, where bandwidth savings are the primary concern.</li> <li>• <b>Minimize Latency</b> – Ensures that Network Memory processing adds no latency. This might come at the cost of lower data reduction. It is appropriate for extremely latency-sensitive interactive or transactional traffic. It is also appropriate when the primary objective is to fully utilize the WAN pipe to increase the LAN-side throughput, as opposed to conserving WAN bandwidth.</li> <li>• <b>Balanced</b> – Is the default setting. It dynamically balances latency and data reduction objectives and is the best choice for most traffic types.</li> <li>• <b>Disabled</b> – Turns off Network Memory.</li> </ul>
<b>IP Header Compression</b>	Process of compressing excess protocol headers before transmitting them on a link and uncompressing them to their original state at the other end. It is possible to compress the protocol headers due to the redundancy in header fields of the same packet, as well as in consecutive packets of a packet stream.
<b>Payload Compression</b>	Uses algorithms to identify relatively short byte sequences that are repeated frequently. These are then replaced with shorter segments of code to reduce the size of transmitted data. Simple algorithms can find repeated bytes within a single packet; more sophisticated algorithms can find duplication across packets and even across flows.
<b>TCP Acceleration</b>	<p>Uses techniques such as selective acknowledgments, window scaling, and maximum segment size adjustment to mitigate poor performance on high-latency links.</p> <p>The slow LAN alert goes off when the loss has fallen below 80% of the specified value configured in the <b>TCP Accel Options</b> dialog box.</p> <p>For more information, see <a href="#">TCP Acceleration Options</a>.</p>
<b>Protocol Acceleration</b>	Provides explicit configuration for optimizing CIFS, SSL, SRDF, Citrix, and iSCSI protocols. In a network environment, it is possible that not every appliance has the same optimization configurations enabled. Therefore, the site that initiates the flow (the <b>client</b> ) determines the state of the protocol-specific optimization.

## Optimization Policies Edit Row

The **Optimization Policies** tab displays the Optimization policy entries that exist on the appliances. This includes the appliance-based defaults, entries applied manually (via the Appliance Manager or CLI), and entries that result from applying an Orchestrator Optimization Policy template or Business Intent Overlay.

Use the **Templates** tab to create and manage Optimization policies, or click the edit icon to directly manage Optimization policies for a particular appliance.

## Priority

- If you are using Orchestrator templates to add rules, Orchestrator will delete all entries from **1000 - 9999** before applying its policies.
- You can create rules with higher priority than Orchestrator rules (**1 - 999**) and rules with lower priority (**10000 - 19999** and **25000 - 65534**).

**NOTE** The priority range from **20000** to **24999** is reserved for Orchestrator.

- When adding a rule, the priority is incremented by 10 from the previous rule. The priority can be changed, but this default behavior helps to ensure you can insert new rules without having to change subsequent priorities.

## Match Criteria

- These are universal across all policy maps—**Route**, **QoS**, **Optimization**, **NAT** (Network Address Translation), and **Security**.
- If you expect to use the same match criteria in different maps, you can create an **ACL** (Access Control List), which is a named, reusable set of rules. For efficiency, create them in **Configuration > Templates & Policies > ACLs > Access Lists**, and apply them across appliances.
- The available parameters are **Application**, **Address Map** (for sorting by country, IP address owner, or SaaS application), **Domain**, **Geo Location**, **Interface**, **Protocol**, **DSCP**, **IP/Subnet**, **Port**, **Traffic Behavior Overlay**, **Fabric or Internet**, and **User Role** (the User Role as specified in the authentication exchange with the ClearPass RADIUS server).

**NOTE** User Role options include the RADIUS User Role, User Name, User Group, User Device, or User MAC. Configuring User Role match criteria enables an EdgeConnect to automatically assign traffic steering and firewall zone policies.

**NOTE** Additional attributes under the Address Map parameter can be used as match criteria. These attributes are secondary parameters to the address map, so the attributes are evaluated for a policy match only when the configured address map parameter matches the flow. To configure these attributes, click **+Attributes**.

- To specify different criteria for inbound versus outbound traffic, select the **Source:Dest** check box.

**NOTE** Source and destination role-based policies can be configured when both source and destination users are in the same network.

## Source or Destination

- An IP address can specify a subnet; for example, 10.10.10.0/24 (IPv4) or fe80::204:23ff:fed8:4ba2/64 (IPv6).
- To allow **any IP address**, use 0.0.0.0/0 (IPv4) or ::/0 (IPv6).
- Ports are available only for the protocols **tcp**, **udp**, and **tcp/udp**.
- To allow **any port**, use 0.

## Wildcard-based Prefix Matching Rules

- Even when using a range or a wildcard, the IPv4 address must be specified in the 4-octet format, separated by the dot notation. For example, A.B.C.D.
- Range is specified using a single dash. For example, 128-129.
- Wildcard is specified as an asterisk (\*).
- Range and Wildcard can both be used in the same address, but an octet can only contain one or the other. For example, 10.136-137.\*.64-95.
- A wildcard can only be used to define an entire octet. For example, 10.13\*.\*.64-95 is not supported. Use 10.130-139.\*.64-95 to specify this range.
- The same rules apply to IPv6 addressing.
- CIDR notation and (Range or Wildcard) are mutually exclusive in the same address. For example, 192.168.0.1-127/24 is not supported. Use either 192.168.0.0/24 or 192.168.0.1-127.
- These prefix-matching rules apply to the following policies only: Route, QoS, Optimization, NAT, Security, and ACLs.

## Set Actions

Set Action	Description
<b>Network Memory</b>	<p>Addresses limited bandwidth. This technology uses advanced fingerprinting algorithms to examine all incoming and outgoing WAN traffic. Network Memory localizes information and transmits only modifications between locations.</p> <ul style="list-style-type: none"> <li><b>Maximize Reduction</b> – Optimizes for maximum data reduction at the potential cost of slightly lower throughput and/or some increase in latency. It is appropriate for bulk data transfers such as file transfers and FTP, where bandwidth savings are the primary concern.</li> <li><b>Minimize Latency</b> – Ensures that Network Memory processing adds no latency. This might come at the cost of lower data reduction. It is appropriate for extremely latency-sensitive interactive or transactional traffic. It is also appropriate when the primary objective is to fully utilize the WAN pipe to increase the LAN-side throughput, as opposed to conserving WAN bandwidth.</li> <li><b>Balanced</b> – Is the default setting. It dynamically balances latency and data reduction objectives and is the best choice for most traffic types.</li> <li><b>Disabled</b> – Turns off Network Memory.</li> </ul>
<b>IP Header Compression</b>	<p>Process of compressing excess protocol headers before transmitting them on a link and uncompressing them to their original state at the other end. It is possible to compress the protocol headers due to the redundancy in header fields of the same packet, as well as in consecutive packets of a packet stream.</p>

Set Action	Description
<b>Payload Compression</b>	Uses algorithms to identify relatively short byte sequences that are repeated frequently. These are then replaced with shorter segments of code to reduce the size of transmitted data. Simple algorithms can find repeated bytes within a single packet; more sophisticated algorithms can find duplication across packets and even across flows.
<b>TCP Acceleration</b>	Uses techniques such as selective acknowledgments, window scaling, and maximum segment size adjustment to mitigate poor performance on high-latency links. The slow LAN alert goes off when the loss has fallen below 80% of the specified value configured in the <b>TCP Accel Options</b> dialog box. For more information, see <a href="#">TCP Acceleration Options</a> .
<b>Protocol Acceleration</b>	Provides explicit configuration for optimizing CIFS, SSL, SRDF, Citrix, and iSCSI protocols. In a network environment, it is possible that not every appliance has the same optimization configurations enabled. Therefore, the site that initiates the flow (the <b>client</b> ) determines the state of the protocol-specific optimization.

## TCP Acceleration Details

**CAUTION** Because changing these settings can affect service, it is recommended that you **do not modify** these without direction from Support.

### *TCP Acceleration Options*

Option	Description
<b>Adjust MSS to Tunnel MTU</b>	Limits the TCP MSS (Maximum Segment Size) advertised by the end hosts in the SYN segment to a value derived from the Tunnel MTU (Maximum Transmission Unit). This is $TCP\ MSS = Tunnel\ MTU - Tunnel\ Packet\ Overhead$ . This feature is enabled by default so that the <b>maximum value</b> of the end host MSS is always coupled to the Tunnel MSS. If the end host MSS is smaller than the tunnel MSS, the end host MSS is used instead. A use case for disabling this feature is when the end host uses Jumbo frames.
<b>Auto Reset Flows</b>	<b>NOTE</b> Whether this feature is enabled or not, the default behavior when a tunnel goes Down is to automatically reset the flows. If enabled, it resets all TCP flows that are not accelerated, but should be (based on policy and on internal criteria like a Tunnel Up event). The internal criteria can also include: <ul style="list-style-type: none"> <li>• Resetting all TCP accelerated flows on a Tunnel Down event.</li> <li>• Resetting <ul style="list-style-type: none"> <li>• TCP acceleration is enabled.</li> <li>• SYN packet was not seen (so this flow was either part of WCCP redirection, or it already existed when the appliance was inserted in the data path).</li> </ul> </li> </ul>

Option	Description
<b>Enable TCP SYN option exchange</b>	<p>Controls whether or not the proprietary TCP SYN option is forwarded on the LAN side. Enabled by default, this feature detects if there are more than two EdgeConnect appliances in the flow's data path, and optimizes accordingly. Disable this feature if there is a LAN-side firewall or a third-party appliance that would drop a SYN packet when it encounters an unfamiliar TCP option.</p>
<b>End to End FIN Handling</b>	<p>This feature helps to fine tune TCP behavior during a connection's graceful shutdown event. When this feature is <b>ON</b> (Default), TCP on the local appliance synchronizes this graceful shutdown of the local LAN side with the LAN side of the remote appliance. When this feature is <b>OFF</b> (Default TCP), no such synchronization happens and the two LAN segments at the ends gracefully shut down, independently.</p>
<b>IP Black Listing</b>	<p>If selected and if the appliance does not receive a TCP SYN-ACK from the remote end within five seconds, the flow proceeds without acceleration and the destination IP address is blacklisted for one minute.</p>
<b>Keep Alive Timer</b>	<p>Allows us to change the Keep Alive timer for the TCP connections.</p> <ul style="list-style-type: none"> <li>• <b>Probe Interval</b> - Time interval in seconds between two consecutive Keep Alive Probes.</li> <li>• <b>Probe Count</b> - Maximum number of Keep Alive probes to send.</li> <li>• <b>First Timeout (Idle)</b> - Time interval until the first Keep Alive timeout.</li> </ul>
<b>LAN Side Window Scale Factor Clamp</b>	<p>This setting allows the appliance to present an artificially lowered Window Scale Factor (WSF) to the end host. This reduces the need for memory in scenarios where there are many out-of-order packets being received from the LAN side. These out-of-order packets cause much buffer utilization and maintenance.</p>
<b>Per-Flow Buffer</b>	<p><b>(Max LAN to WAN Buffer and Max WAN to LAN Buffer)</b> This setting clamps the maximum buffer space that can be allocated to a flow, in each direction.</p>
<b>Persist timer Timeout</b>	<p>Allows the TCP to terminate connections that are in Persist timeout stage after the configured number of seconds.</p>
<b>Preserve Packet Boundaries</b>	<p>Preserves the packet boundaries end to end. If this feature is disabled, the appliances in the path can coalesce consecutive packets of a flow to use bandwidth more efficiently. It is enabled by default so that applications that require packet boundaries to match do not fail.</p>
<b>Route Policy Override</b>	<p>Tries to override asymmetric route policy settings. It emulates auto-opt behavior by using the same tunnel for the returning SYN+ACK as it did for the original SYN packet. Disable this feature if the asymmetric route policy setting is necessary to correctly route packets. In that case, you might need to configure flow redirection to ensure optimization of TCP flows.</p>

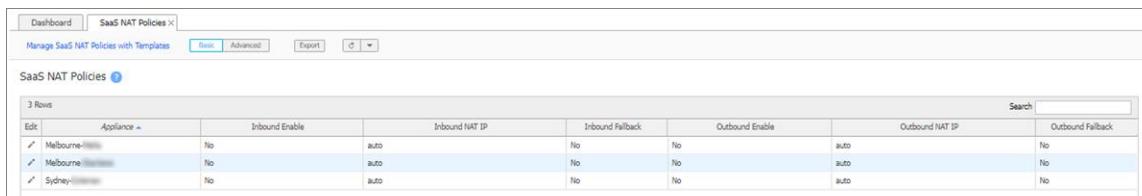
Option	Description
<b>Slow LAN Defense</b>	Resets all flows that consume a disproportionate amount of buffer and have a very slow throughput on the LAN side. Owing to a few slower end hosts or a lossy LAN, these flows affect the performance of all other flows so that no flows see the customary throughput improvement gained through TCP acceleration. This feature is enabled by default. The number relates indirectly to the amount of time the system waits before resetting such slow flows.
<b>Slow LAN Window Penalty</b>	This setting ( <b>OFF</b> by default) penalizes flows that are slow to send data on the LAN side by artificially reducing their TCP receive window. This causes less data to be received and helps to reach a balance with the data sending rate on the LAN side.
<b>WAN Congestion Control</b>	Selects the internal Congestion Control parameter: <ul style="list-style-type: none"> <li><b>Optimized</b> - This is the default setting. This mode offers optimized performance in almost all scenarios.</li> <li><b>Standard</b> - In some unique cases, it might be necessary to downgrade to Standard performance to better inter-operate with other flows on the WAN link.</li> <li><b>Aggressive</b> - Provides aggressive performance and should be used with caution. Recommended mostly for Data Replication scenarios.</li> </ul>
<b>WAN Window Scale</b>	This is the WAN-side TCP Window scale factor that is used internally for WAN-side traffic. This is independent of the WAN-side factor advertised by the end hosts.

## SaaS NAT Policies Tab

*Configuration > Templates & Policies > Policies > SaaS NAT Policies*

This report has two views that show the SaaS NAT policies configured on appliances:

- The **Basic** view shows whether NAT is enabled on all **Inbound** and **Outbound**.



The screenshot shows a table titled "SaaS NAT Policies" with the following columns: Appliance, Inbound Enable, Inbound NAT IP, Inbound Fallback, Outbound Enable, Outbound NAT IP, and Outbound Fallback. There are three rows of data:

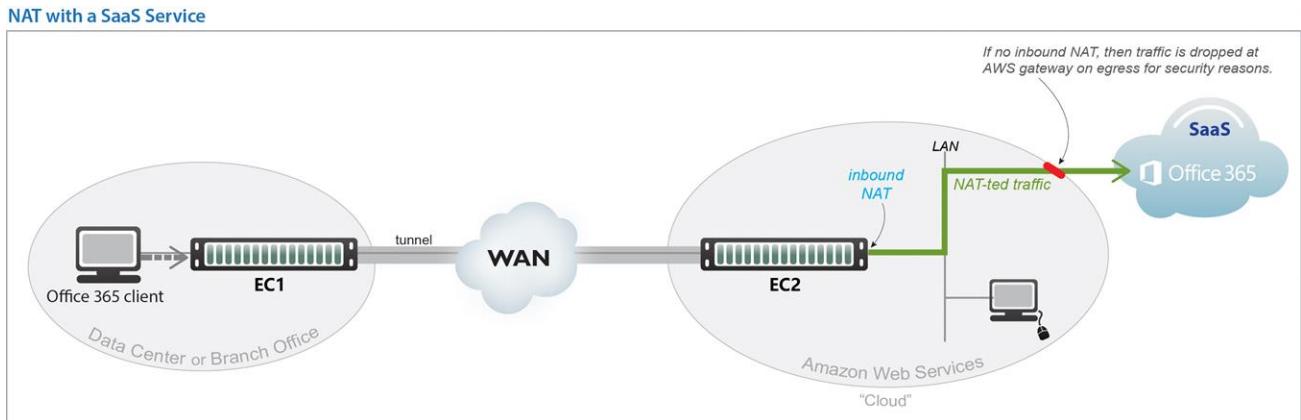
Edit	Appliance	Inbound Enable	Inbound NAT IP	Inbound Fallback	Outbound Enable	Outbound NAT IP	Outbound Fallback
<input checked="" type="checkbox"/>	Melbourne-[REDACTED]	No	auto	No	No	auto	No
<input checked="" type="checkbox"/>	Melbourne-[REDACTED]	No	auto	No	No	auto	No
<input checked="" type="checkbox"/>	Sydney-[REDACTED]	No	auto	No	No	auto	No

- The Advanced view displays all the NAT map rules.

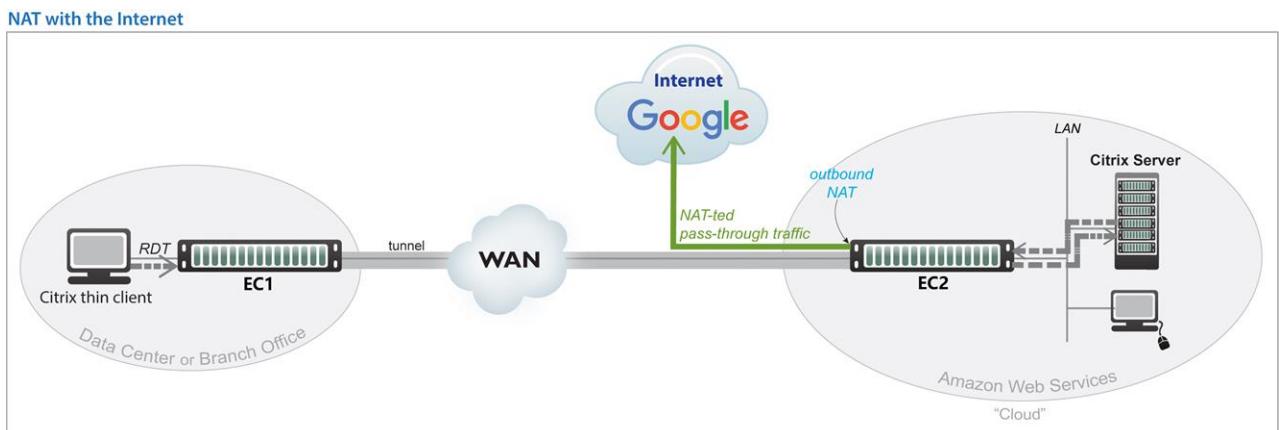
Appliance	Map	Priority	Match Criteria	NAT Type	NAT Direction	NAT IP	Fallback	Comment
Melbourne	map1 (active)	65535	Match Everything	no-nat	none	auto	No	
Melbourne	map1 (active)	65535	Match Everything	no-nat	none	auto	No	
Sydney	map1 (active)	1000	Protocol ip	no-nat	none	auto	No	
Sydney	map1 (active)	65535	Match Everything	no-nat	none	auto	No	

Two use cases illustrate the need for NAT:

- Inbound NAT.** The appliance automatically creates a source NAT (Network Address Translation) map when retrieving subnet information from the Cloud Portal. This ensures that traffic destined to SaaS servers has a return path to the appliance from which that traffic originated.



- Outbound NAT.** The appliance and server are in the cloud, and the server accesses the internet. As in the example below, a Citrix thin client accesses its cloud-based server, and the server accesses the internet.



For deployments in the cloud, **best practice is to NAT all traffic**—either inbound (WAN-to-LAN) or outbound (LAN-to-WAN), depending on the direction of initiating request. This avoids black-holing that can result from cloud-specific IP addressing requirements.

- Enabling **NAT all** applies NAT policies to pass-through traffic as well as optimized traffic, ensuring that black-holing does not occur. **NAT all** on outbound only applies pass-through traffic.
- If **Fallback** is enabled, the appliance moves to the next IP (if available) when ports are exhausted on the current NAT IP.

In general, when applying NAT policies, configure separate WAN and LAN interfaces to ensure that NAT works properly. You can do this by deploying the appliance in Router mode in-path with two (or four) interfaces.

## Advanced Settings

The appliance can perform **source network address translation** (Source NAT or SNAT) on inbound or outbound traffic.

There are two types of NAT policies:

- **Dynamic** - Created automatically by the system for inbound NAT when the **SaaS Optimization** feature is enabled and SaaS service(s) are selected for optimization. The appliance polls the Cloud Intelligence Service for a directory of SaaS services, and NAT policies are created for each of the subnets associated with selected SaaS service(s), ensuring that traffic destined for servers in use by those SaaS services has a return path to the appliance.
- **Manual** - Created by the administrator for specific IP addresses / ranges or subnets. When assigning priority numbers to individual policies within a NAT map, first view **dynamic policies** to ensure that the manual numbering scheme does not interfere with dynamic policy numbering (that is, the manually assigned priority numbers cannot be in the range: 4000-5000). The default (**no-NAT**) policy is numbered 65535.

The NAT policy map has the following criteria and **Set Actions**:

## Match Criteria

- These are universal across all policy maps—**Route**, **QoS**, **Optimization**, **NAT** (Network Address Translation), and **Security**.
- If you expect to use the same match criteria in different maps, you can create an **ACL** (Access Control List), which is a named, reusable set of rules. For efficiency, create them in **Configuration > Templates & Policies > ACLs > Access Lists**, and apply them across appliances.
- The available parameters are **Application**, **Address Map** (for sorting by country, IP address owner, or SaaS application), **Domain**, **Geo Location**, **Interface**, **Protocol**, **DSCP**, **IP/Subnet**, **Port**, **Traffic Behavior Overlay**, **Fabric or Internet**, and **User Role** (the User Role as specified in the authentication exchange with the ClearPass RADIUS server).

**NOTE** User Role options include the RADIUS User Role, User Name, User Group, User Device, or User MAC. Configuring User Role match criteria enables an EdgeConnect to automatically assign traffic steering and firewall zone policies.

**NOTE** Additional attributes under the Address Map parameter can be used as match criteria. These attributes are secondary parameters to the address map, so the attributes are evaluated for a policy match only when the configured address map parameter matches the flow. To configure these attributes, click **+Attributes**.

- To specify different criteria for inbound versus outbound traffic, select the **Source:Dest** check box.

**NOTE** Source and destination role-based policies can be configured when both source and destination users are in the same network.

## Source or Destination

- An IP address can specify a subnet; for example, 10.10.10.0/24 (IPv4) or fe80::204:23ff:fed8:4ba2/64 (IPv6).
- To allow **any IP address**, use 0.0.0.0/0 (IPv4) or ::/0 (IPv6).
- Ports are available only for the protocols **tcp**, **udp**, and **tcp/udp**.
- To allow **any port**, use 0.

## Wildcard-based Prefix Matching Rules

- Even when using a range or a wildcard, the IPv4 address must be specified in the 4-octet format, separated by the dot notation. For example, A.B.C.D.
- Range is specified using a single dash. For example, **128-129**.
- Wildcard is specified as an asterisk (\*).
- Range and Wildcard can both be used in the same address, but an octet can only contain one or the other. For example, **10.136-137.\*.64-95**.
- A wildcard can only be used to define an entire octet. For example, **10.13\*.\*.64-95** is not supported. Use **10.130-139.\*.64-95** to specify this range.
- The same rules apply to IPv6 addressing.
- CIDR notation and (Range or Wildcard) are mutually exclusive in the same address. For example, **192.168.0.1-127/24** is not supported. Use either **192.168.0.0/24** or **192.168.0.1-127**.
- These prefix-matching rules apply to the following policies only: Route, QoS, Optimization, NAT, Security, and ACLs.

## Set Actions

### NAT Type

Option	Description
<b>no-nat</b>	Is the <i>default</i> . No IP addresses are changed.

Option	Description
<b>source-nat</b>	Is the <i>default</i> . No IP addresses are changed.

#### NAT Direction

Option	Description
<b>inbound</b>	NAT is on the LAN interface.
<b>outbound</b>	NAT is on the WAN interface.
<b>none</b>	Only option if the NAT type is <b>no-nat</b> .

#### NAT IP

Option	Description
<b>auto</b>	Select if you want to NAT <b>all</b> traffic. The appliance then picks the first available NAT IP/Port.
<b>tunnel</b>	Select if you want to NAT <b>tunnel</b> traffic only. Applicable only for inbound NAT, as outbound does not support NAT on tunnel traffic.
<b>[IP address]</b>	Select if you want to make NAT use this IP address during address translation.

For **Fallback**, if the IP address is full, the appliance uses the next available IP address.

When you select a specific IP, ensure that the routing is in place for NAT-ed return traffic.

#### Merge / Replace

At the top of the page, choose

**Merge** to use the values in the template, but keep any values set on the appliance as is (producing a mix of template and appliance rules),

-OR-

**Replace** (recommended) to replace all values with those in the template.

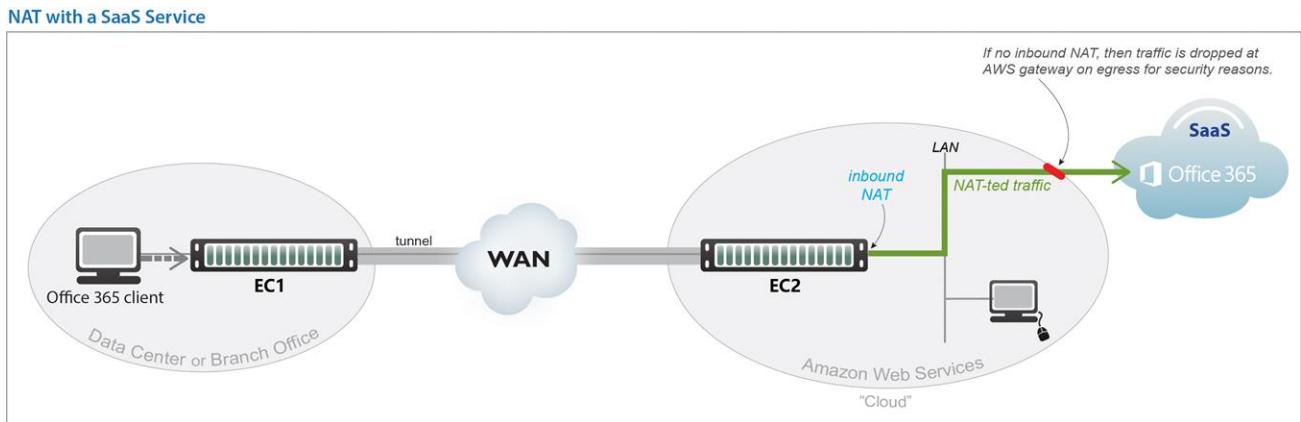
#### SaaS NAT Policies Edit Row

This report has two views that show the SaaS NAT policies configured on appliances:

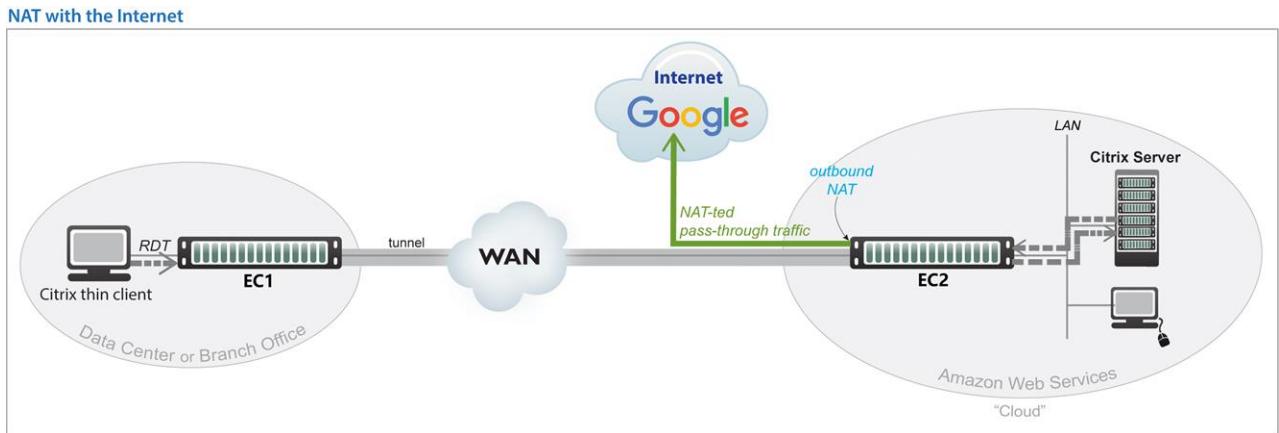
- The **Basic** view shows whether NAT is enabled on all **Inbound** and **Outbound**.
- The **Advanced** view displays all the NAT map rules.

Two use cases illustrate the need for NAT:

- **Inbound NAT.** The appliance automatically creates a source NAT (Network Address Translation) map when retrieving subnet information from the Cloud Portal. This ensures that traffic destined to SaaS servers has a return path to the appliance from which that traffic originated.



- **Outbound NAT.** The appliance and server are in the cloud, and the server accesses the internet. As in the example below, a Citrix thin client accesses its cloud-based server, and the server accesses the internet.



For deployments in the cloud, **best practice is to NAT all traffic**—either inbound (WAN-to-LAN) or outbound (LAN-to-WAN), depending on the direction of initiating request. This avoids black-holing that can result from cloud-specific IP addressing requirements.

- Enabling **NAT all** applies NAT policies to pass-through traffic as well as optimized traffic, ensuring that black-holing does not occur. **NAT all** on outbound only applies pass-through traffic.
- If **Fallback** is enabled, the appliance moves to the next IP (if available) when ports are exhausted on the current NAT IP.

In general, when applying NAT policies, configure separate WAN and LAN interfaces to ensure that NAT works properly. You can do this by deploying the appliance in Router mode in-path with two (or four) interfaces.

## Advanced Settings

The appliance can perform **source network address translation** (Source NAT or SNAT) on inbound or outbound traffic.

There are two types of NAT policies:

- **Dynamic** - Created automatically by the system for inbound NAT when the **SaaS Optimization** feature is enabled and SaaS service(s) are selected for optimization. The appliance polls the Cloud Intelligence Service for a directory of SaaS services, and NAT policies are created for each of the subnets associated with selected SaaS service(s), ensuring that traffic destined for servers in use by those SaaS services has a return path to the appliance.
- **Manual** - Created by the administrator for specific IP addresses / ranges or subnets. When assigning priority numbers to individual policies within a NAT map, first view **dynamic policies** to ensure that the manual numbering scheme does not interfere with dynamic policy numbering (that is, the manually assigned priority numbers cannot be in the range: 4000-5000). The default (**no-NAT**) policy is numbered 65535.

The NAT policy map has the following criteria and **Set Actions**:

### Match Criteria

- These are universal across all policy maps—**Route**, **QoS**, **Optimization**, **NAT** (Network Address Translation), and **Security**.
- If you expect to use the same match criteria in different maps, you can create an **ACL** (Access Control List), which is a named, reusable set of rules. For efficiency, create them in **Configuration > Templates & Policies > ACLs > Access Lists**, and apply them across appliances.
- The available parameters are **Application**, **Address Map** (for sorting by country, IP address owner, or SaaS application), **Domain**, **Geo Location**, **Interface**, **Protocol**, **DSCP**, **IP/Subnet**, **Port**, **Traffic Behavior Overlay**, **Fabric or Internet**, and **User Role** (the User Role as specified in the authentication exchange with the ClearPass RADIUS server).

**NOTE** User Role options include the RADIUS User Role, User Name, User Group, User Device, or User MAC. Configuring User Role match criteria enables an EdgeConnect to automatically assign traffic steering and firewall zone policies.

**NOTE** Additional attributes under the Address Map parameter can be used as match criteria. These attributes are secondary parameters to the address map, so the attributes are evaluated for a policy match only when the configured address map parameter matches the flow. To configure these attributes, click **+Attributes**.

- To specify different criteria for inbound versus outbound traffic, select the **Source:Dest** check box.

**NOTE** Source and destination role-based policies can be configured when both source and destination users are in the same network.

## Source or Destination

- An IP address can specify a subnet; for example, 10.10.10.0/24 (IPv4) or fe80::204:23ff:fed8:4ba2/64 (IPv6).
- To allow **any IP address**, use 0.0.0.0/0 (IPv4) or ::/0 (IPv6).
- Ports are available only for the protocols **tcp**, **udp**, and **tcp/udp**.
- To allow **any port**, use 0.

## Wildcard-based Prefix Matching Rules

- Even when using a range or a wildcard, the IPv4 address must be specified in the 4-octet format, separated by the dot notation. For example, **A.B.C.D**.
- Range is specified using a single dash. For example, **128-129**.
- Wildcard is specified as an asterisk (\*).
- Range and Wildcard can both be used in the same address, but an octet can only contain one or the other. For example, **10.136-137.\*.64-95**.
- A wildcard can only be used to define an entire octet. For example, **10.13\*.\*.64-95** is not supported. Use **10.130-139.\*.64-95** to specify this range.
- The same rules apply to IPv6 addressing.
- CIDR notation and (Range or Wildcard) are mutually exclusive in the same address. For example, **192.168.0.1-127/24** is not supported. Use either **192.168.0.0/24** or **192.168.0.1-127**.
- These prefix-matching rules apply to the following policies only: Route, QoS, Optimization, NAT, Security, and ACLs.

## Set Actions

### NAT Type

Option	Description
<b>no-nat</b>	Is the <i>default</i> . No IP addresses are changed.
<b>source-nat</b>	Is the <i>default</i> . No IP addresses are changed.

### NAT Direction

Option	Description
<b>inbound</b>	NAT is on the LAN interface.
<b>outbound</b>	NAT is on the WAN interface.
<b>none</b>	Only option if the NAT type is <b>no-nat</b> .

## NAT IP

Option	Description
<b>auto</b>	Select if you want to NAT <b>all</b> traffic. The appliance then picks the first available NAT IP/Port.
<b>tunnel</b>	Select if you want to NAT <b>tunnel</b> traffic only. Applicable only for inbound NAT, as outbound does not support NAT on tunnel traffic.
<b>[IP address]</b>	Select if you want to make NAT use this IP address during address translation.

For **Fallback**, if the IP address is full, the appliance uses the next available IP address.

When you select a specific IP, ensure that the routing is in place for NAT-ed return traffic.

## Inbound Port Forwarding

*Configuration > Overlays & Security > Security > Inbound Port Forwarding*

Inbound port forwarding allows traffic from the WAN to reach computers or services within a private LAN when you have a stateful firewall. It helps define and manage inbound traffic, remap a destination IP address and port number to an internal host, and create policies to manage branch devices from the WAN. Use this tab to define the desired inbound traffic.

Inbound Port forwarding is available in two modes when you add or edit a rule, depending on whether the translate mode is enabled or disabled.

The first operating mode for inbound port forwarding is when translate mode is disabled with inbound port forwarding. The LAN-side subnet with private IP addresses is allowed access through an inbound port forwarding rule (defined by you in the following steps) and exposes any external services. This requires LAN side private addresses to be routed on the WAN side. This represents the process of DMZ (Demilitarized Zone).

**NOTE** This mode is not common unless the port forwarding source is directly connected to the EdgeConnect or if the LAN side device address is routed from the WAN side. Additionally, inbound port forwarding does not support TFTP servers.

To establish a DMZ connection, complete the following steps:

1. Go to the **Inbound Port Forwarding** tab.
2. Select the **Edit** icon next to **Appliance**.
3. Select **Add Rule**.
4. Complete each field with the appropriate information.

Field	Description
<b>Source IP/Subnet</b>	Source of the WAN device managing the LAN device(s) specified in the destination.
<b>Destination IP/Subnet</b>	Address of the LAN device(s) managed remotely.

The second mode is when translate mode is enabled. When enabled, the EdgeConnect WAN interface performs destination NAT to reach LAN side device(s) from an external network.

Complete the following steps to enable the translate mode. This represents the process of DNAT (Destination Network Translation).

1. Go to the **Inbound Port Forwarding** tab.
2. Select the **Edit** icon.
3. Select **Add Rule**.
4. Select the **Translate** check box to enable Translate mode.
5. Complete each field with the appropriate information.

Field	Description
<b>Source IP/Subnet</b>	Source of the WAN device managing the LAN device(s) specified in the destination.
<b>Destination IP/Subnet</b>	Address of the WAN interface IP.
<b>Destination Port/Range</b>	Port/range of the LAN device(s) that are managed remotely.
<b>Protocol</b>	Select the protocol you want to apply: <b>UDP</b> , <b>TCP</b> , <b>ICMP</b> , <b>Any</b> . If you select <b>Any</b> , the Destination and Translated Ports have a default value that need to be between 0-100. If the value exceeds, 100 a warning appears.
<b>Translated IP</b>	IP address of the LAN device accessed inside your network.
<b>Translated Port/Range</b>	Port/range of the LAN device accessed inside your network.
<b>Source Interface</b>	Source interface name.
<b>Segment</b>	Name of the segment being used.
<b>Comment</b>	Any additional details.

## Additional Information

- **Interface Modes**

Port forwarding is used only when you have 'stateful' or 'stateful+snat' configured on interfaces. It does not apply when you have 'Allow All' or 'Harden' configured.

- **Security Policies**

\*If 'security policies' are configured, make sure they allow the traffic specified in the port forwarding rules.

- You can also reorder the appliances associated with inbound port forwarding by selecting **Reorder** when adding a rule.

**NOTE** 'Any' is a protocol option only on versions 8.1.9.4 and later.

## Security Policies Tab

*Configuration > Overlays & Security > Security > Firewall Zone Security Policies*

This tab displays the Security Policies, which manage traffic between firewall zones.

- Zones are created on the Orchestrator. A zone is applied to an **Interface**.
- By default, traffic is allowed between interfaces labeled with the same zone. Any traffic between interfaces with different zones is dropped. Users can create exception rules (Security Policies) to allow traffic between interfaces with different zones.
- When Routing Segmentation (VRF) is enabled, by default, traffic is allowed between interfaces labeled with the same zone and the same segment. Any traffic between different zones or between different segments is dropped.
- When segmentation is enabled, define your security policies from the Routing Segmentation (VRF) tab.
- When segmentation is enabled, do not use templates. If a security policy template is applied while segmentation is enabled, it will only apply within the default segment. It will override the default-default security policy defined on the Routing Segmentation (VRF) tab. This behavior is designed to prevent a disruption in traffic when segmentation is enabled for the first time, and during a migration to segments. After the migration process is complete, the security policy template should be removed.
- If segments are disabled, define your security policies by creating templates. You can then apply template groups to appliances.
- Clicking the edit icon opens the Security Policy that has been applied. Any changes made here are local to that appliance. Making changes from this tab is not recommended.
- Logging: In table view, you can specify the log level when adding and editing a rule. Select the appropriate level from the options in the list.
- Define your Security Policies by creating **templates**. You can then apply templates to Interfaces or Overlays.
- Clicking the edit icon opens the Security Policy that has been applied. Any changes made here are **local** to that appliance.

- Click **Firewall Drops** to see statistics on various flows, packets, and bytes dropped or allowed by a zone-based firewall for a given time range.
- Click **Manage Security Policies with Templates** to define policies on all appliances within your network. You can use the matrix and table view to further specify your policies. If segmentation is enabled, do not use templates. Manage from the Routing Segmentation (VRF) tab instead.

## Wildcard-based Prefix Matching Rules

- Even when using a range or a wildcard, the IPv4 address must be specified in the 4-octet format, separated by the dot notation. For example, **A.B.C.D**.
- Range is specified using a single dash. For example, **128-129**.
- Wildcard is specified as an asterisk (\*).
- Range and Wildcard can both be used in the same address, but an octet can only contain one or the other. For example, **10.136-137.\*.64-95**.
- A wildcard can only be used to define an entire octet. For example, **10.13\*.\*.64-95** is not supported. Use **10.130-139.\*.64-95** to specify this range.
- The same rules apply to IPv6 addressing.
- CIDR notation and (Range or Wildcard) are mutually exclusive in the same address. For example, **192.168.0.1-127/24** is not supported. Use either **192.168.0.0/24** or **192.168.0.1-127**.
- These prefix-matching rules apply to the following policies only: Route, QoS, Optimization, NAT, Security, and ACLs.

## Security Policies Edit Row

This dialog box displays the Security Policies, which manage traffic between segments and their firewall zones.

Complete the following steps to add or modify rules in your security policies:

1. Select the default logging level to be applied to all "Deny All" events.
2. Select the Source and Destination Segment.
3. Click the cell for the source and destination zone to open the rule editor.
4. Click **Add Rule** to create a new rule.
5. Modify the following fields in a new or existing rule:

Field	Description
<b>Priority</b>	Priority of the rule.
<b>Match Criteria</b>	Click the edit icon to add or modify match criteria for the rule.
<b>Action</b>	Select the action to apply to traffic matching the rule: <input type="checkbox"/> <b>allow</b> – Matching traffic will be allowed. <input type="checkbox"/> <b>deny</b> – Matching traffic will be denied. <input type="checkbox"/> <b>inspect</b> – Matching traffic will be inspected by the Intrusion Detection System (IDS).
<b>Enabled</b>	Select the check box to enable the rule or clear the check box to disable the rule.
<b>Logging</b>	Select the logging level to be applied when logging matches for the specific rule. If you do not want to log matching traffic, select <b>None</b> .
<b>Tag</b>	Use this field to specify a tag to be logged with matching events.
<b>Comment</b>	Use this field to add comments or additional information about the rule.

- Zones are created on the Orchestrator. A zone is applied to an **Interface**.
- By default, traffic is allowed between interfaces labeled with the same zone. Any traffic between interfaces with different zones is dropped. Users can create exception rules (Security Policies) to allow traffic between interfaces with different zones or between their segments and firewall zones.
- Define your Security Policies by creating **templates**. You then can apply templates to Interfaces or Overlays.
- Clicking the Edit icon opens the Security Policy that has been applied. Any changes made here are **local** to that appliance.

## Wildcard-based Prefix Matching Rules

- Even when using a range or a wildcard, the IPv4 address must be specified in the 4-octet format, separated by the dot notation. For example, **A.B.C.D**.
- Range is specified using a single dash. For example, **128-129**.
- Wildcard is specified as an asterisk (\*).
- Range and Wildcard can both be used in the same address, but an octet can only contain one or the other. For example, **10.136-137.\*.64-95**.
- A wildcard can only be used to define an entire octet. For example, **10.13\*.\*.64-95** is not supported. Use **10.130-139.\*.64-95** to specify this range.
- The same rules apply to IPv6 addressing.
- CIDR notation and (Range or Wildcard) are mutually exclusive in the same address. For example, **192.168.0.1-127/24** is not supported. Use either **192.168.0.0/24** or **192.168.0.1-127**.
- These prefix-matching rules apply to the following policies only: Route, QoS, Optimization, NAT, Security, and ACLs.

## Access Lists Tab

*Configuration > Templates & Policies > Policies > ACLs > Access Lists*

This tab lists the configured **Access Control List** (ACL) rules. An **ACL** is a reusable MATCH criteria for filtering flows. It is associated with an action: **permit** or **deny**. An ACL can be a MATCH condition in more than one policy—Route, QoS, or Optimization.

Field	Description
<b>Appliance</b>	Name of the appliance selected.
<b>ACLs</b>	Access Control Lists. A list of one or more ordered access control rules. <b>NOTE</b> An ACL only becomes active when it is used in a policy.
<b>Priority</b>	For ACL rules, you can set the priority to a value within the range 1 to 65535. When adding a rule, the priority is incremented by ten from the previous rule. You can change the priority, but this default behavior helps ensure that you can insert new rules without having to change subsequent priorities.
<b>Match Criteria</b>	Configured ACL match criteria associated to the appliance. See below for more information about Match Criteria.
<b>Permit</b>	Whether the ACL is set to <b>Permit</b> or <b>Deny</b> . <ul style="list-style-type: none"> <li>• <b>Permit</b> allows the matching traffic flow to proceed to the policy entry's associated SET actions.</li> <li>• <b>Deny</b> prevents further processing of the flow by <b>that ACL, specifically</b>. The appliance continues to the next entry in the policy.</li> </ul>
<b>Comment</b>	Any additional information about the ACL.

Click the edit icon to make add, delete, or modify rules to your ACLs.

### Match Criteria

- These are universal across all policy maps—**Route**, **QoS**, **Optimization**, **NAT** (Network Address Translation), and **Security**.
- If you expect to use the same match criteria in different maps, you can create an **ACL** (Access Control List), which is a named, reusable set of rules. For efficiency, create them in **Configuration > Templates & Policies > ACLs > Access Lists**, and apply them across appliances.
- The available parameters are **Application**, **Address Map** (for sorting by country, IP address owner, or SaaS application), **Domain**, **Geo Location**, **Interface**, **Protocol**, **DSCP**, **IP/Subnet**, **Port**, **Traffic Behavior Overlay**, **Fabric or Internet**, and **User Role** (the User Role as specified in the authentication exchange with the ClearPass RADIUS server).

**NOTE** User Role options include the RADIUS User Role, User Name, User Group, User Device, or User MAC. Configuring User Role match criteria enables an EdgeConnect to automatically assign traffic steering and firewall zone policies.

**NOTE** Additional attributes under the Address Map parameter can be used as match criteria. These attributes are secondary parameters to the address map, so the attributes are evaluated for a policy match only when the configured address map parameter matches the flow. To configure these attributes, click **+Attributes**.

- To specify different criteria for inbound versus outbound traffic, select the **Source:Dest** check box.

**NOTE** Source and destination role-based policies can be configured when both source and destination users are in the same network.

## Wildcard-based Prefix Matching Rules

- Even when using a range or a wildcard, the IPv4 address must be specified in the 4-octet format, separated by the dot notation. For example, A.B.C.D.
- Range is specified using a single dash. For example, 128-129.
- Wildcard is specified as an asterisk (\*).
- Range and Wildcard can both be used in the same address, but an octet can only contain one or the other. For example, 10.136-137.\*.64-95.
- A wildcard can only be used to define an entire octet. For example, 10.13\*.\*.64-95 is not supported. Use 10.130-139.\*.64-95 to specify this range.
- The same rules apply to IPv6 addressing.
- CIDR notation and (Range or Wildcard) are mutually exclusive in the same address. For example, 192.168.0.1-127/24 is not supported. Use either 192.168.0.0/24 or 192.168.0.1-127.
- These prefix-matching rules apply to the following policies only: Route, QoS, Optimization, NAT, Security, and ACLs.

## Access Lists Edit Row

The Access Lists dialog box lists the configured **Access Control List** (ACL) rules.

You can add, delete, or rename an ACL by clicking the buttons at the top of this dialog box. You can also add rules to an ACL.

1. Click **Add Rule**.
2. Enter a priority value.
3. Click the edit icon to configure the match criteria. The **Match Criteria** dialog box opens and you can specify the match criteria. Click **More Options** to apply more rules.
4. Select if you want to **Permit** or **Deny** traffic in the ACL.
5. Enter any comments if you decide to do so.

## Address Groups

*Configuration > Templates & Policies > ACLs > Address Groups*

Use the Address Groups tab to view and manage address groups in your SD-WAN network. An address group is a logical collection of IP hosts or subnets that can be referenced in source or destination matching criteria in the zone based firewall and security policies (route, QOS, optimization, and so forth).

**NOTE** Orchestrator supports up to 500 address groups.

The screenshot shows the 'Address Groups' page with the following details:

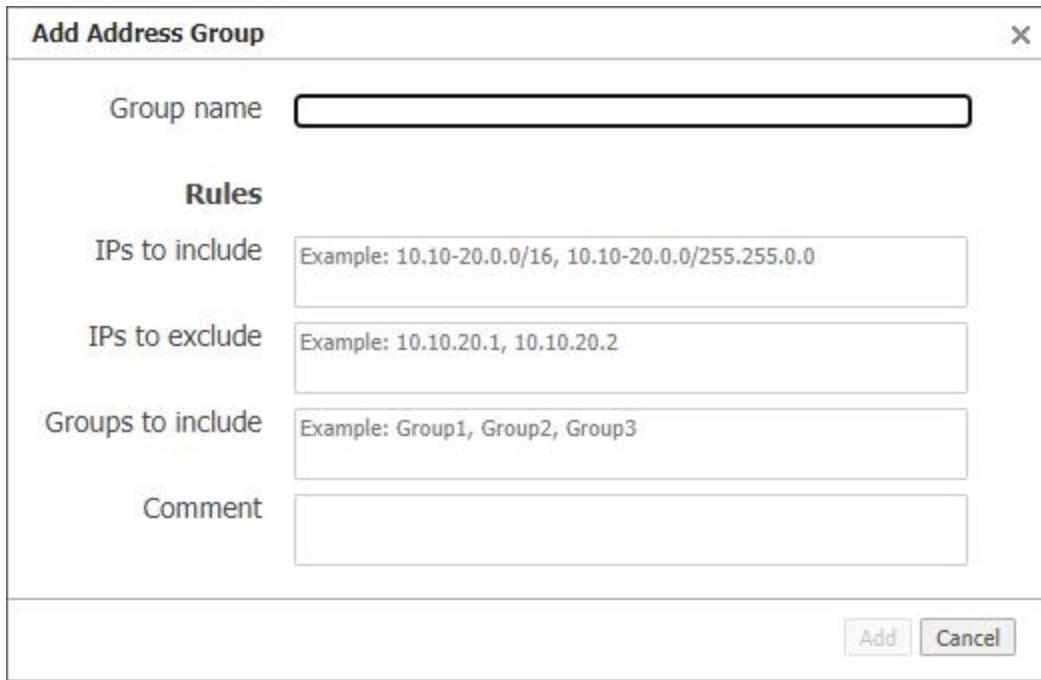
- Header: 'Address Groups' with a help icon, a timer showing '4 mins', and buttons for 'Add Group', 'Delete Group', 'Bulk Import', and 'Export CSV'.
- Buttons: 'Add Rule' and 'Search'.
- Text: 'Memory Consumed: 30 bytes'.
- Table: A grid showing two rows of address groups.

Edit	Name	Includes	Excludes	Comment
*	AuthorizedDNS	8.8.8.8, 8.8.4.4, 1.1.1.1, 1.1.0.0		Firewall denies all but these endpoints
*	Loopbacks-Default	128.41.0.0/16		Pool for loopback orchestration

### Add an Address Group

Follow the steps below to create a new address group:

1. Click **Add Group** to open the Add Address Group dialog box.



2. Provide the following details in the fields provided:

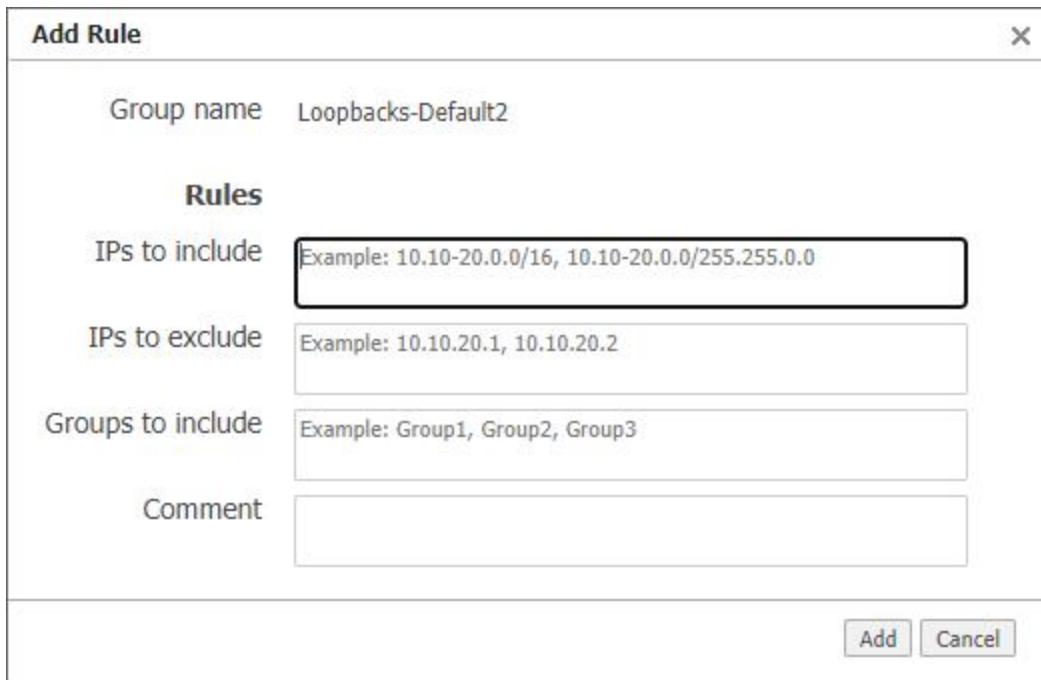
Field	Description
<b>Group name</b>	Enter a unique name for the group, up to 64 characters long. <b>NOTE</b> Group names can only contain uppercase and lowercase letters, numbers, dots, underscores, and hyphens.
<b>IPs to include</b>	Enter one or more IP addresses or subnets to include in the group (see <b>Address Group Formats</b> below).
<b>IPs to exclude</b>	Enter one or more IP addresses to exclude, in the case where you are including an IP range.
<b>Groups to include</b>	Enter the name of one or more address groups to include. <b>NOTE</b> Group inclusion only supports two levels of nesting. For example, if Group1 includes Group2 and Group2 includes Group3, you could not include Group1 anywhere because it already contains two levels of nested groups.
<b>Comment</b>	Enter an optional comment that describes the address group and how it might be used.

3. Click **Add** to create the address group or click **Cancel** to close the dialog box without making any changes.

## Add a Rule to an Address Group

Follow the steps below to add a rule to an existing address group:

1. Select the address group to which you want to add a rule from the drop-down list above the table.
2. Click **Add Rule** to open the Add Rule dialog box.



3. Provide the details for the new rule in the fields provided (see field descriptions in [Add an Address Group](#)).
4. Click **Add** to create the rule or click **Cancel** to close the dialog box without making any changes.

## Delete an Address Group

Follow the steps below to delete an address group:

1. Select the address group you want to delete from the drop-down list above the table.
2. Click **Delete Group**.

A confirmation dialog box opens.

3. Click **Delete** to confirm your choice and permanently remove the selected group and all of its rules. Otherwise, click **Cancel** to return to the list without deleting the group.

## Export Address Groups

You can export the current address groups to a CSV file as a backup to make bulk modifications outside of the Orchestrator UI.

To export address groups:

1. Click **Export CSV**.
2. In the save dialog box, browse to the location where you want to save the file, provide a name for the file, and then click **Save**.
3. Open the saved file in Excel or another program to view or modify its contents.

	A	B	C	D	E
1	Name	IncludedIPs	ExcludedIPs	IncludedGroups	Comment
2	AuthorizedDNS	8.8.8.8,8.4.4,1.1.1,1.1.0.0			Firewall denies all but these endpoints
3	Loopbacks-Default	128.41.0.0/16			Pool for loopback orchestration
4					

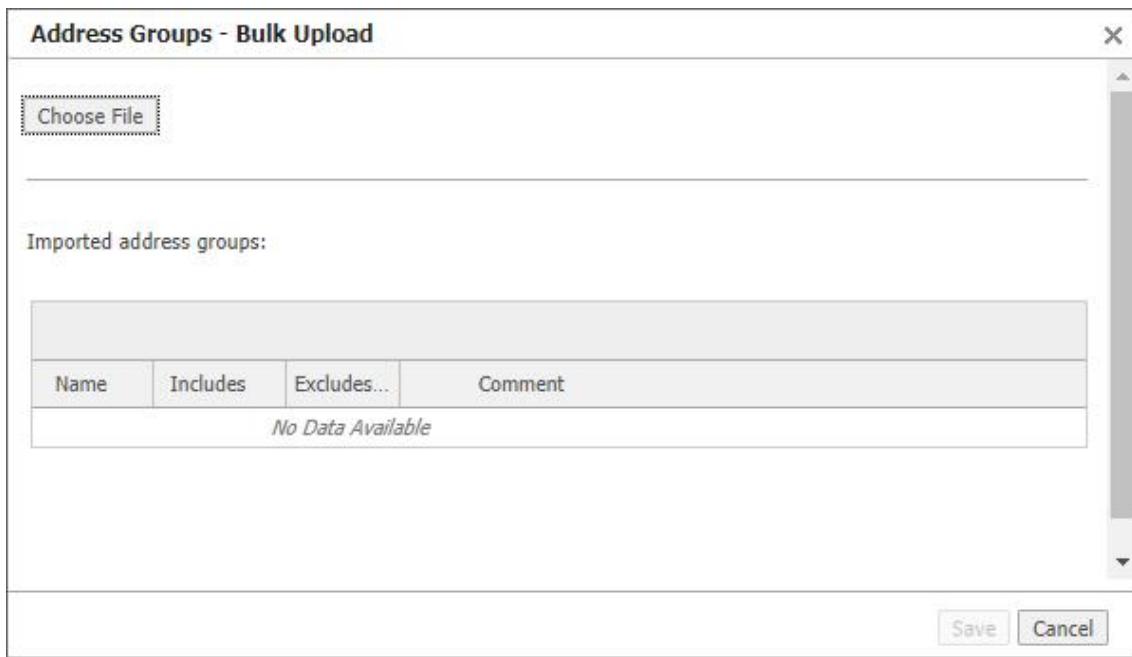
**NOTE** When editing exported rules and address groups, you can modify the included or excluded IPs, included groups, or comments to overwrite the same rule when imported. If you modify the group name on a rule, however, it will create a new rule when imported.

## Import Address Groups

To import address groups from a CSV file:

**NOTE** You can import a file that was exported and modified, or a new file that contains data in the same rows and columns as the exported file. Columns are ordered as Name, Included IPs, Excluded IPs, Included Groups, and Comment. The first row of the import file will be ignored.

1. Click **Bulk Import** to open the Address Groups - Bulk Upload dialog box.



2. Click **Choose File**, locate and select the CSV file to be imported, and then click **Open**.
3. Review the groups and rules to be imported.
4. Click **Save** to import the file and merge with or replace the existing address groups, or click **Cancel** to close the dialog box without making any changes.

## View a Single Address Group

By default, all address groups are displayed in the table on the Address Groups tab. To filter the table to a single address group, select the group from the drop-down list above the table.

**NOTE** You can only add rules to an existing group when viewing a single address group. You cannot add a group with the same name as an existing group.

## Edit or Delete a Rule

To edit or delete an existing rule, click the edit icon to the right of the rule. The Edit Rule dialog box opens.

**Edit Rule**

Group name    Loopbacks-Default2

**Rules**

IPs to include    128.41.0.0/24

IPs to exclude    Example: 10.10.20.1, 10.10.20.2

Groups to include    Example: Group1, Group2, Group3

Comment    Pool for loopback orchestration

**Save** **Delete** **Cancel**

- To edit the rule, modify the available fields, and then click **Save**.
- To delete the rule, click **Delete**.

## Using Address Groups in Match Criteria

When specifying match criteria for IP/Subnet, you can use an address group by enabling the **Src:Dest** and **Groups** options.

**Segment**  **Type to select**  **Source:Dest**

**IP/Subnet**  **Source** **Dest**

**Src:Dest**  **IPs**  **Groups**  **IPs**  **Groups**

**Port**  **Example: 80 or 20-30 or 4|8|10**  **Src:Dest**

## Address Group Formats

An address group can include IP addresses, subnets, address groups, or any combination thereof. For IPs and subnets, the following formats are allowed:

- One or more IP addresses: 10.10.10.1 or 10.10.10.2, 10.10.10.2, 10.10.10.3
- IP subnet: 10.10.0.0/16 or 10.10.0.0/255.255.0.0
- IP range: 10.10.10.10-20
- IP range and subnet: 10.10-20.0.0/16, 10.10-20.0.0/255.255.0.0
- IP wildcard: 10.10.10.\* (you can use the wildcard in any octet)
- Wildcard and mask: 10.\*.0.0/16, 10.\*.0.0/255.255.0.0

## Service Groups

*Configuration > Templates & Policies > ACLs > Service Groups*

Use the Service Groups tab to view and manage service groups in your SD-WAN network. A service group is a logical collection of protocols and ports that can be referenced in source or destination matching criteria in the zone based firewall and security policies (route, QOS, optimization, and so forth).

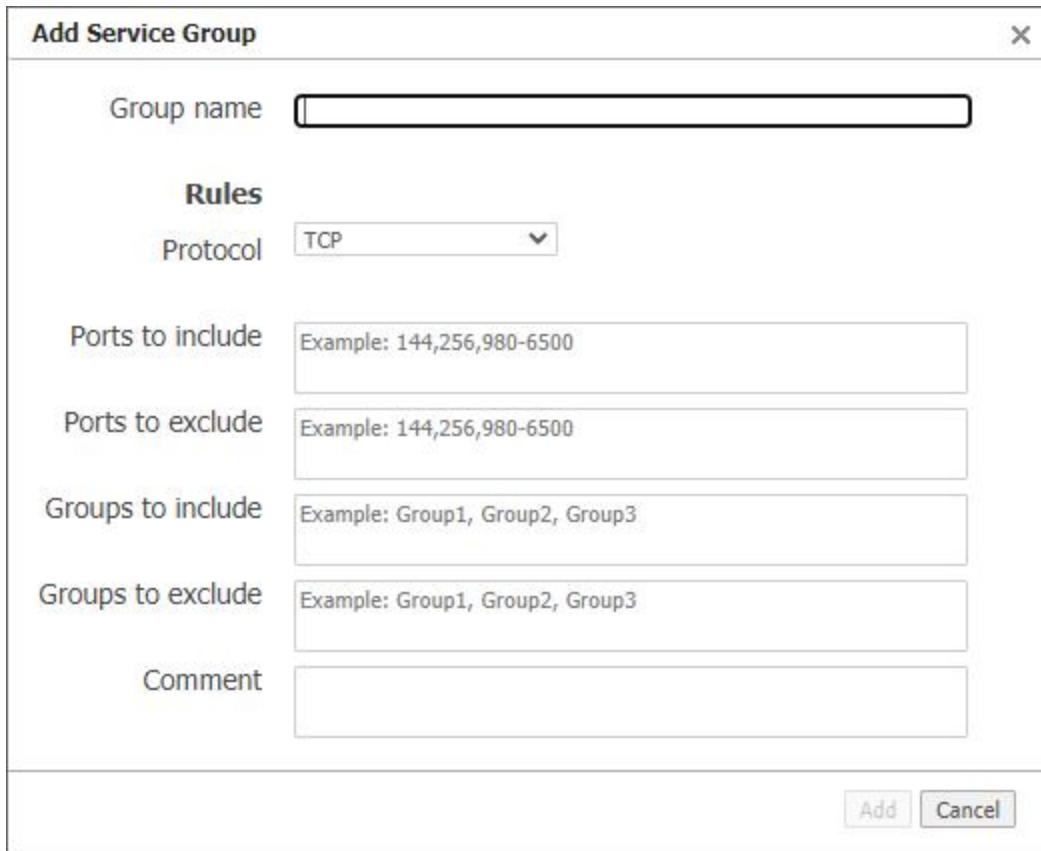
**NOTE** Orchestrator supports up to 500 service groups.

Edit	Name	Protocol	Includes	Excludes	Comment
<a href="#">Edit</a>	ICMP-Echo	ICMP	8		ping request
<a href="#">Edit</a>	ICMP-EchoReply	ICMP	0		ping reply
<a href="#">Edit</a>	ICMP-DestinationUnreacha...	ICMP	3		destination unreachables
<a href="#">Edit</a>	ICMP-TTLExceeded	ICMP	11		TTL Expired in Transit (traceroute, routing loops,...)
<a href="#">Edit</a>	ICMP-Redirect	ICMP	5		redirect messages for better gateway
<a href="#">Edit</a>	SystemPorts-UDP	UDP	1-1023		system, well-known, privileged ports
<a href="#">Edit</a>	SystemPorts-TCP	TCP	1-1023		system, well-known, privileged ports
<a href="#">Edit</a>	EphemeralPorts-TCP	TCP	49152-65535		ephemeral ports
<a href="#">Edit</a>	EphemeralPorts-UDP	UDP	49152-65535		ephemeral ports
<a href="#">Edit</a>	RegisteredPorts-TCP	TCP	1024-49151		registered and unprivileged ports
<a href="#">Edit</a>	RegisteredPorts-UDP	UDP	1024-49151		registered and unprivileged ports
<a href="#">Edit</a>	Unidirectional-UDP	UDP	514, 2055, 67, 162		apps that continuously send in only one direction
<a href="#">Edit</a>	multi-services	TCP	1, 2, 3-5, ICMP-Echo	100-200, SystemPorts-TCP	
<a href="#">Edit</a>	multi-services	GRE			
<a href="#">Edit</a>	multi-services	UDP	512	123	

## Add a Service Group

Follow the steps below to create a new service group:

1. Click **Add Group**. The Add Service Group dialog box opens.



2. Provide the following details in the fields provided:

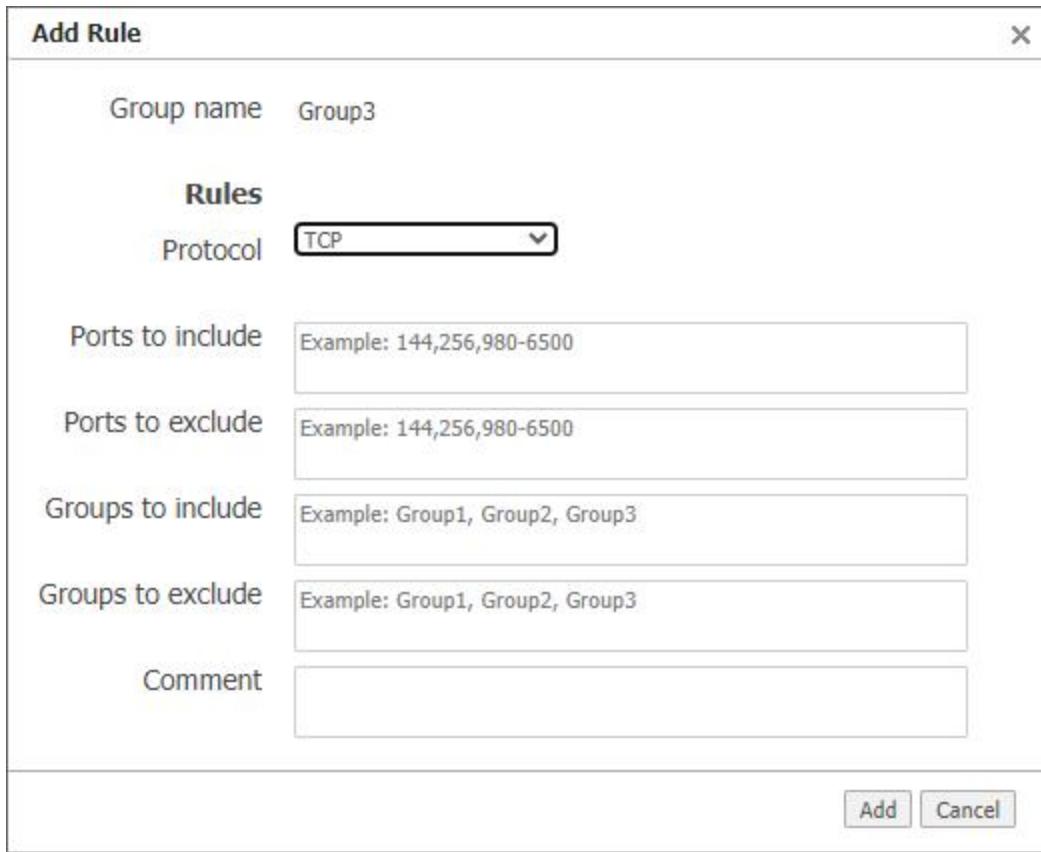
Field	Used in	Description
<b>Group name</b>	All	Enter a unique name for the group, up to 64 characters long. <b>NOTE</b> Group names can only contain uppercase and lowercase letters, numbers, dots, underscores, and hyphens.
<b>Protocol</b>	All	Select a protocol from the list of those available.
<b>Ports to include</b>	TCP, UDP	Enter one or more ports to include in the group. A single port, multiple comma-separated ports, and a range of ports are supported (e.g., 20, 22, 24-30).
<b>Ports to exclude</b>	TCP, UDP	Enter one or more ports to exclude from the group, in the case where you are including a range of ports. A single port, multiple comma-separated ports, and a range of ports are supported (e.g., 20, 22, 24-30).
<b>Groups to include</b>	TCP, UDP	Enter the name of one or more service groups to include. <b>NOTE</b> Group inclusion only supports two levels of nesting. For example, if Group1 includes Group2 and Group2 includes Group3, you could not include Group1 anywhere because it already contains two levels of nested groups.
<b>Groups to exclude</b>	TCP, UDP	Enter the name of one or more service groups to exclude, in the case where you are already including a group that includes multiple groups.
<b>ICMP types</b>	ICMP	For ICMP, add one or more message types to include. Multiple types and ranges are supported (e.g., 1, 2, 4-8).
<b>Comment</b>	All	Enter an optional comment that describes the service group and how it might be used.

- Click **Add** to create the service group or click **Cancel** to close the dialog box without making any changes.

## Add a Rule to a Service Group

Follow the steps below to add a rule to an existing service group:

- Select the service group to which you want to add a rule from the drop-down list above the table.
- Click **Add Rule**. The Add Rule dialog box opens.



3. Provide the details for the new rule in the fields provided (see field descriptions in [Add a Service Group](#)).
4. Click **Add** to create the rule or click **Cancel** to close the dialog box without making any changes.

### Delete a Service Group

Follow the steps below to delete a service group:

1. Select the service group you want to delete from the drop-down list above the table.
2. Click **Delete Group**.

A confirmation dialog box opens.

3. Click **Delete** to confirm your choice and permanently remove the selected group and all of its rules. Otherwise, click **Cancel** to return to the list without deleting the group.

## Export Service Groups

You can export the current service groups to a CSV file as a backup to make bulk modifications outside of the Orchestrator UI. Follow the steps below to export service groups.

1. Click **Export CSV**.
2. In the save dialog box, browse to the location where you want to save the file, provide a name for the file, and then click **Save**.
3. Open the saved file in Excel or another program to view or modify its contents.

A	B	C	D	E	F	G	H
Name	Protocol	IncludedPorts	ExcludedPorts	IncludedGroups	ExcludedGroups	IcmpTypes	Comment
1 ICMP-Echo	ICMP					8 ping request	
3 ICMP-EchoReply	ICMP					0 ping reply	
4 SystemPorts-UDP	UDP	1-1023				system, well-known, privileged ports	
5 SystemPorts-TCP	TCP	1-1023				system, well-known, privileged ports	
6 EphemeralPorts-TCP	TCP	49152-65535				ephemeral ports	
7 EphemeralPorts-UDP	UDP	49152-65535				ephemeral ports	
8 RegisteredPorts-TCP	TCP	1024-49151				registered and unprivileged ports	
9 RegisteredPorts-UDP	UDP	1024-49151				registered and unprivileged ports	
10 Unidirectional-UDP	UDP	514,2055,67,162				apps that continuously send in only one direction	

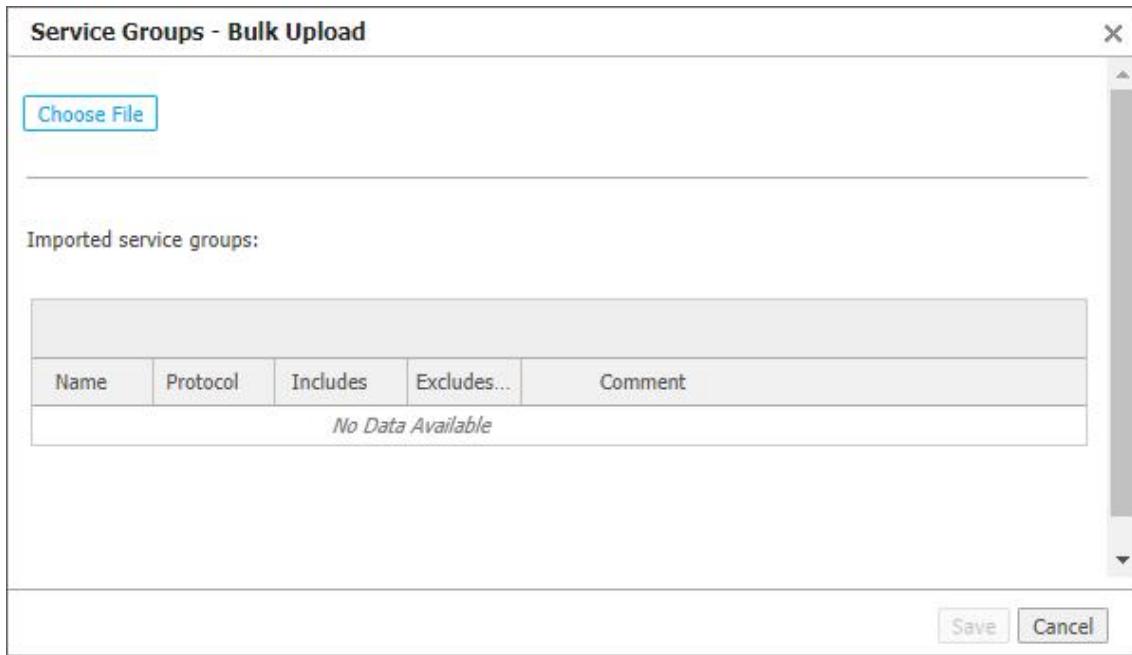
**NOTE** When editing exported rules and service groups, you can modify the protocol, inclusions, exclusions, ICMP types, or comments to overwrite the same rule when imported. If you modify the group name on a rule, however, it will create a new rule when imported.

## Import Service Groups

Follow the steps below to import service groups from a CSV file:

**NOTE** You can import a file that was exported and modified, or a new file that contains data in the same rows and columns as the exported file. Columns are ordered as Name, Protocol, Included Ports, Excluded Ports, Included Groups, Excluded Groups, ICMP types, and Comment. The first row of the import file will be ignored.

1. Click **Bulk Import**. The Service Groups - Bulk Upload dialog box opens.



2. Click **Choose File**, locate and select the CSV file to be imported, and then click **Open**.
3. Review the groups and rules to be imported.
4. Click **Save** to import the file and merge with or replace the existing service groups, or click **Cancel** to close the dialog box without making any changes.

## View a Single Service Group

By default, all service groups are displayed in the table on the Service Groups tab. To filter the table to a single service group, select the group from the drop-down list above the table.

**NOTE** You can only add rules to an existing group when viewing a single service group. You cannot add a group with the same name as an existing group.

## Edit or Delete a Rule

To edit or delete an existing rule, click the edit icon to the right of the rule and the Edit Rule dialog box opens.

**Edit Rule**

Group name SystemPorts-TCP

**Rules**

Protocol

Ports to include

Ports to exclude

Groups to include

Groups to exclude

Comment

- To edit the rule, modify the available fields, and then click **Save**.
- To delete the rule, click **Delete**.

### Using Service Groups in Match Criteria

When specifying match criteria for Port, you can use a service group by enabling the **Src:Dest** and **Groups** options.

IP/Subnet  Example: 1.1.1.1/32 or 1.1.1.1-220 or fe80::204:23ff:fe08:4ba2/128  
 Src:Dest

Port <input checked="" type="checkbox"/>	Source ICMP-EchoReply	Dest ICMP-EchoReply
<input checked="" type="checkbox"/> Src:Dest	<input type="radio"/> Ports	<input checked="" type="radio"/> Groups
	<input type="radio"/> Ports	<input checked="" type="radio"/> Groups

## Shaper Tab

*Configuration > Templates & Policies > Shaping > Shaper*

This report provides a view of the Shaper settings.

The **Shaper** provides a simplified way to globally configure QoS (Quality of Service) on the appliances.

The table for inbound settings is shown below (outbound is similar):

Shaper																
Manage Shaper settings with Templates																
Import   Export   12 rows																
Search																
Edit	Appliance	Interface S...	Min Wan BW (Mbps)	Recalc on IF State...	Traffic ID	Traffic Name	Priority	Min BW %	Min BW Absolute (Mbps)	Min BW Actual (Mbps)	Excess Weighting	Max BW %	Max BW Absolute (Mbps)	Max Wait Time (ms)	Rate Limit (Mbps)	Enable
✓	Edinburgh-Mon	van	220,000	Yes	1	REALTIME	1	5	0	11,000	200	100	10,000,000	220,000	250	0 Yes
✓	Edinburgh-Mon	van	220,000	Yes	2	CASHE	2	5	0	11,000	200	100	10,000,000	220,000	500	0 Yes
✓	Edinburgh-Mon	van	220,000	Yes	3	RECREATIONAL	3	5	0	11,000	400	100	10,000,000	220,000	500	0 Yes
✓	Edinburgh-Mon	van	220,000	Yes	4	GUEST	4	0	0	0	1	50	10,000,000	110,000	500	0 Yes
✓	Edinburgh-Mon	van	220,000	Yes	5	BESTEFFORT	5	5	0	11,000	50	100	10,000,000	220,000	500	0 Yes
✓	Edinburgh-Mon	van	220,000	Yes	6	DEFAULT	6	0	0	0	100	100	10,000,000	220,000	500	0 Yes
✓	Edinburgh-Mon	van	220,000	Yes	7		7	0	0	0	1	100	10,000,000	220,000	500	0 Yes
✓	Edinburgh-Mon	van	220,000	Yes	8		8	5	0	11,000	1	100	10,000,000	220,000	500	0 Yes
✓	Edinburgh-Mon	van	220,000	Yes	9	CLIQUEW	9	0	0	0	1	1	10,000,000	2,200	100	1 Yes

- It shapes traffic by allocating bandwidth as a percentage of the **system bandwidth**.
- The Shaper's parameters are organized into ten traffic classes. Four traffic classes are preconfigured and named **real-time**, **interactive**, **default**, and **best effort**.
- The system applies these QoS settings globally after compressing (deduplicating) all the outbound tunnelized and pass-through-shaped traffic, shaping it as it exits to the WAN.
- To manage Shaper settings for an appliance's system-level **WAN Shaper**, access the Shaper template.
- For minimum and maximum bandwidth, you can configure traffic class values as a percentage of total available system bandwidth and as an absolute value. The appliance always provides the larger of the minimum values and limits bandwidth to the lower of the maximum values.
- Max** overrides **Min** if you set **Min Bandwidth** to a value greater than **Max Bandwidth**.

### Shaper Tab Settings

Field	Description
<b>Appliance</b>	Name of the appliance.
<b>Interface Shaper</b>	<p>Enables a separate shaper for a specific WAN interface.</p> <ul style="list-style-type: none"> <li>For WAN optimization, the interface shaper can be used, but it is not recommended.</li> <li>For SD-WAN, it should never be used because overlay traffic is not directed to an interface shaper; traffic is always shaped by the default WAN shaper.</li> </ul>

Field	Description
<b>Recalc on IF State Changes</b>	When an interface state changes to UP or DOWN, selecting this recalculates the total bandwidth based on the configured bandwidth of all UP interfaces. For example, when <b>wan0</b> goes down, <b>wan0</b> bandwidth is removed from the total bandwidth when recalculating.
<b>Traffic ID</b>	The number assigned to the traffic class.
<b>Traffic Name</b>	The name assigned to a traffic class, either prescriptively or by the user.
<b>Priority</b>	Determines the order in which to allocate each class' minimum bandwidth - <b>1</b> is first, <b>10</b> is last.
<b>Min BW %</b>	Refers to the percentage of bandwidth guaranteed to each traffic class, allocated by priority. However, if the sum of the percentages is greater than 100%, lower-priority traffic classes might not receive their guaranteed bandwidth if it is all consumed by higher-priority traffic.  <b>Max</b> overrides <b>Min</b> if you set <b>Min Bandwidth</b> to a value greater than <b>Max Bandwidth</b> .
<b>Min BW Absolute (kbps)</b>	This guarantees a specific level of service when total system bandwidth declines. This is useful for maintaining the quality of VoIP, for example.
<b>Excess Weighting</b>	If there is bandwidth left over after satisfying the minimum bandwidth percentages, the excess is distributed among the traffic classes in proportion to the weightings specified in the <b>Excess Weighting</b> column. Values range from 1 to 10,000.
<b>Max BW %</b>	This limits the maximum bandwidth that a traffic class can use to a percentage of total available system bandwidth.
<b>Max BW Absolute (kbps)</b>	This limits the maximum bandwidth that a traffic class can use to an absolute value (kbps). You can specify a maximum absolute value to cap the bandwidth for downloads and streaming.
<b>Max Wait Time (ms)</b>	Any packets waiting longer than the specified <b>Max Wait Time</b> are dropped.
<b>Rate Limit (kbps)</b>	You can set per-flow rate limit that a traffic class uses by specifying a number in the Rate Limit column. For no limit, use <b>0</b> (zero).

## SaaS Optimization Tab

*Configuration > Templates & Policies > Applications & SaaS > SaaS Optimization*

When SaaS optimization is enabled, the SaaS Optimization tab provides a view of the information retrieved from the Cloud Intelligence Service.

Appliance	Application Name	Optimize	Advertise	RTT Threshold	Domains
<i>No SaaS Optimization defined for this appliance.</i>					
HongKong-[REDACTED]	Adobe	No	No	10 ms	
Osaka-[REDACTED]	AirWatch	No	No	10 ms	
Osaka-[REDACTED]	AthenaHealth	No	No	10 ms	
Osaka-[REDACTED]	BlueJeans	No	No	10 ms	
Osaka-[REDACTED]	Box	No	No	10 ms	
Osaka-[REDACTED]	CCcone	No	No	10 ms	
Osaka-[REDACTED]	CCeskype	No	No	10 ms	
Osaka-[REDACTED]	ConstantContact	No	No	10 ms	
Osaka-[REDACTED]	CornerstoneOnDemand	No	No	10 ms	
Osaka-[REDACTED]	Dropbox	No	No	10 ms	
Osaka-[REDACTED]	Dynamics	No	No	10 ms	
Osaka-[REDACTED]	Eloqua	No	No	10 ms	
Osaka-[REDACTED]	GoToAssist	No	No	10 ms	
Osaka-[REDACTED]	GoToMeeting	No	No	10 ms	
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

This tab displays the following three buttons:

- **Configuration** - Displays a table of SaaS optimization configurations for the listed appliances.
- **Monitoring** - Displays a table of monitoring information related to SaaS optimization for the listed appliances that have been configured for SaaS optimization.
- **Export** - Exports the displayed table as a .csv file. The exported file depends on whether the SaaS Optimization Configuration table or the SaaS Optimization Monitoring table is displayed when you click this button.

## Configure for SaaS Optimization

To directly access an appliance, configure the SaaS applications or services you want to optimize, and enable SaaS optimization for the appliance, click the edit icon next to that appliance. The SaaS Optimization dialog box opens.

## SaaS Optimization Dialog Box

Use the SaaS Optimization dialog box to optimize your SaaS applications. Descriptions of the three options at the top of the dialog box follow:

- **Enable SaaS Optimization** - Select this check box to enable the appliance to contact the Cloud Intelligence Service and download information about SaaS services.
- **RTT Calculation Interval** - Enter a value to specify how frequently Orchestrator recalculates the Round Trip Time for the enabled applications.
- **RTT Ping Interface** - Select the interface to use to ping the enabled SaaS subnets for Round Trip Times. The default interface is **wan0**.

Descriptions for table columns displayed in the dialog box follow:

Field	Description
<b>Application Name</b>	Name of the SaaS application to optimize.
<b>Optimize</b>	Select this check box to enable SaaS Optimization.
<b>Advertise</b>	If <b>Advertise</b> is selected for a service (for example, SFDC), the appliance will: <ul style="list-style-type: none"> <li>Ping active SaaS subnets to determine RTT/metric</li> <li>Add subnet sharing entries locally for subnets within RTT threshold</li> <li>Advertise subnets and their metric (within threshold) via subnet sharing to client-side appliances</li> </ul> <ul style="list-style-type: none"> <li>Upon seeing an SFDC flow, generate a substitute certificate for an SFDC SSL domain (one substitute certificate per domain)</li> <li>Auto-generate dynamic NAT rules for SFDC (but not for unchecked services)</li> </ul>
<b>RTT Threshold</b>	Amount of time (in ms) allotted that specifies how often Orchestrator will recalculate the Round Trip Time for the enabled applications. <b>NOTE</b> You might want to set a higher RTT Threshold value to see a broader scope of reachable data servers for any given SaaS application. As best practice, production RTT Threshold values should not exceed 50 ms.
<b>Domains</b>	Domain names where the SaaS is applied.
<b>SaaS ID</b>	Unique identifier assigned to the SaaS application (for use in SaaS Optimization).

For more detailed information about SaaS optimization, navigate to the [SaaS Optimization template](#).

## Application Definitions

*Configuration > Templates & Policies > Applications & SaaS > Application Definitions*

This tab provides application visibility and control. You can search to determine whether a definition exists for a specific application and, if so, how it is defined.

The screenshot shows the 'Application Definitions' and 'IP Protocol' sections of the Aruba Orchestrator interface.

**Application Definitions:**

Type	Name	Notes	Confid.	Detail	Edit
Domain Name	Google		75	Domain *.cobraresearch.com	✓
Domain Name	EligoG		75	Domain *.com.google	✓
Domain Name	Contactsgoo...		75	Domain *.contacts.google.com	✓
Domain Name	GoogleDocs		75	Domain *.docs.google.com	✓
Domain Name	GoogleDomains		75	Domain *.domains.google	✓
Domain Name	Doubleclick		75	Domain *.doubleclickbygoogle.com	✓
Domain Name	GoogleDrive		75	Domain *.drive.google.com	✓
Domain Name	Google		75	Domain *.duck.com	✓
Domain Name	GoogleFonts		75	Domain *.fonts.google.com	✓
Domain Name	Google		75	Domain *.foofie.com	✓
Domain Name	GoogleForms		75	Domain *.forms.google.com	✓
Domain Name	Gg-google		75	Domain *.gg.google.com	✓
Domain Name	Google		75	Domain *.google.com	✓

**IP Protocol:**

Protocol	Name	Notes	Confidence	Edit
0	Hopopt	IPv6 Hop-by-Hop Option	50	✓
1	Icmp	Internet Control Message Protocol	50	✓
2	Igmp	Internet Group Management Protocol	50	✓
3	Gpp	Gateway-to-Gateway Protocol	50	✓
4	Ipv4	IPv4 encapsulation	50	✓
5	St	Internet Stream Protocol	50	✓
6	Tcp	Transmission Control Protocol	50	✓
7	Cbt	Core-based trees	50	✓
8	Egp	Exterior Gateway Protocol	50	✓
9	Igp	Interior Gateway Protocol (any private interior gateway (used by cisco for their igps))	50	✓
10	Bbn-rcc-mon	bnn rcc monitoring	50	✓
11	Nvp-ii	Network Voice Protocol	50	✓
12	Pup	Xerox PUP	50	✓
13	Argus	argus	50	✓
14	Emcon	emcon	50	✓

Orchestrator uses the following eight dimensions to identify and define applications:

- **IP Protocol**
- **UDP Port**
- **TCP Port**
- **Domain Name**
- **Address Map** - (Formerly known as *IP Intelligence*). Given a range of IP addresses, the Address Map reveals the organization that owns the segment, along with the country of origin.
- **DPI** - Deep Packet Inspection. An expanded list of Orchestrator legacy built-in applications.
- **Compound** - Created by user from multiple criteria.
- **SaaS** - Created by user. If any components of the definition change, the user must manually update the definition.

You can use any of these dimensions to define a new application, and you can modify or disable an existing application.

Orchestrator automatically checks the Cloud Portal for updated application definitions every 24 hours by default (**Auto updates** set to ON). Application definition data on the Cloud Portal is updated generally once per month. If new definitions are discovered, Orchestrator downloads the data, merges it with the applications, and pushes the changes to appliances in the network. You can also force an update at any time by clicking the **Update Now** button.

## Application Groups Tab

*Configuration > Templates & Policies > Applications & SaaS > Application Groups*

Application groups associate applications into a common group you can use as a MATCH criteria. The applications can be built-in, user-defined, or a combination of both.

Applications		
Application	Groups	Edit Group Membership
Adobe	Computer_and_Electronics, Interactive, SaaS, Software, Video	
Airs	Interactive	
Ammyy	Interactive	
Aol	Email, Interactive, Internet_and_Telecom	
Apple-remote-desktop	Interactive	
Af-micp	Interactive, Network_Services	
Avira	Computer_and_Electronics, Computer_Security, Interactive	
Bluejeans	Interactive, SaaS	
Bluestacks	Computer_and_Electronics, Interactive, Software	
Brocade	Encrypted, Interactive	
Cddbp	Interactive	
Cisco	Computer_and_Electronics, Encrypted, Interactive, Network_Services, Networking, Real-Time, Vide...	
Cisco-aon-amc	Interactive	
Citadel	Interactive	
Citrix-ica	Citrix, File_Sharing, Interactive	
Codengen	Interactive	
Dart	Interactive, Network_Services	
Dcn-meas	Interactive	
Default-port	Interactive	
Dtspcd	Interactive	
Farming	Interactive	

- The **Group Name** cannot be blank.
- Group names are case-insensitive.
- An application group cannot contain another application group.
- A group name followed by \* indicates a group defined by a user.
- You cannot change the name of a group provided by Orchestrator, but you can modify the applications those groups contain.

**NOTE** To avoid performance issues, it is strongly recommended that you assign an application to no more than three groups.

## Threshold Crossing Alerts Tab

*Configuration > Templates & Policies > TCAs > Threshold Crossing Alerts*

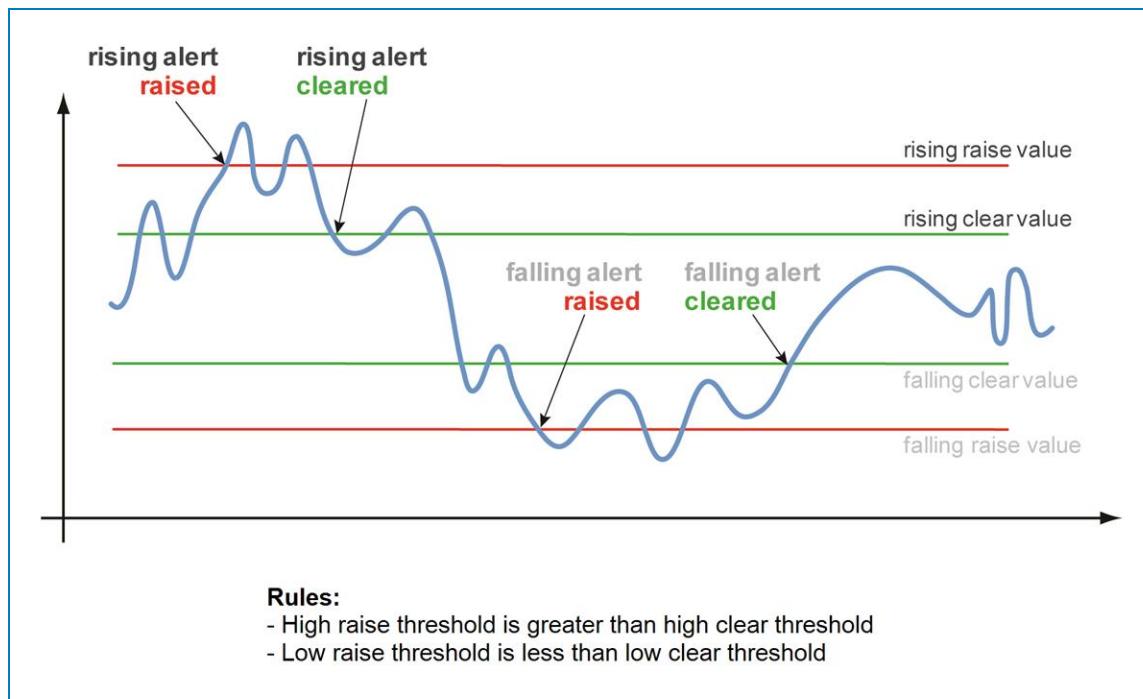
**Threshold Crossing Alerts (TCAs)** are pre-emptive, configurable alarms triggered when specific thresholds are crossed.

The screenshot shows a table titled 'Threshold Crossing Alerts' with 24 rows. The columns include 'Edit', 'Appliance', 'Name', 'Rising: Raise', 'Rising: Clear', 'Rising: Times to Trigger', 'Rising: Enabled', 'Falling: Raise', 'Falling: Clear', 'Falling: Times to Trigger', and 'Falling: Enabled'. Some rows have a checkmark in the 'Edit' column. The 'Name' column includes entries like 'File-system utilization', 'LAN-side receive throughput', 'Total number of flows', 'Total number of optimized flows', 'Tunnel OOP post-POC', 'Tunnel OOP pre-POC', 'Tunnel latency', and 'Tunnel loss post-FEC'. The 'Rising: Raise' and 'Falling: Raise' columns show percentage values (e.g., 90%, 100%), while 'Clear' columns show bandwidth values (e.g., 1000000 kbps, 1000 ms). The 'Enabled' columns show 'Yes' or 'No'.

The alerts are triggered with rising and falling threshold crossing events (that is, floor and ceiling levels). For both levels, one value raises the alarm while another value clears it.

- When you configure appliance and tunnel TCAs with an Orchestrator template, all alerts apply globally, so all of an appliance's tunnels have the same alerts.
- To create a tunnel-specific alert, navigate to **Configuration > Networking > Tunnels > Tunnels**, select the tunnel, click the edit icon to access the tunnel directly, and then click the icon in the **Alert Options** column. Make your changes, and then click **OK**.

**Times to Trigger** - A value of 1 triggers an alarm on the first threshold crossing instance.



## ON by Default

- **Appliance Capacity** - Triggers when an appliance reaches 95% of its total flow capacity. It is not configurable and can be cleared only by an operator.
- **File-system utilization** - Percent of non-Network Memory disk space filled by the appliance. This TCA cannot be disabled.
- **Tunnel latency** - Measured in milliseconds, the maximum latency of a one-second sample within a 60-second span.

## OFF by Default

- **LAN-side receive throughput** - Based on a one-minute average, the LAN-side receive **TOTAL** for all interfaces.
- **WAN-side transmit throughput** - Based on a one-minute average, the WAN-side transmit **TOTAL** for all interfaces.
- **TCAs based on an end-of-minute count:**
  - Total number of flows
  - Total number of optimized flows
- **TCAs based on a one-minute average:**
  - Tunnel loss post-FEC
  - Tunnel loss post-FEC
  - Tunnel OOP post-POC
  - Tunnel OOP post-POC
  - Tunnel reduction
  - Tunnel utilization (based on percent of configured maximum [system] bandwidth)

## Threshold Crossing Alerts Edit Row

Click any cell in the table to edit and configure the Threshold Crossing Alerts.

This table lists the **defaults** of each type of threshold crossing alert:

*Defaults Values for Threshold Crossing Alerts*

TCA Name	Default [ON, OFF]	Default Values [Rising Raise, Rising Clear, Falling Raise, Falling Clear]	allow rising	allow falling
Appliance Level				
WAN-side transmit throughput	OFF	1 Gbps; 1 Gbps; 0; 0	4	4

TCA Name	Default [ON, OFF]	Default Values [Rising Raise, Rising Clear, Falling Raise, Falling Clear]	allow rising	allow falling
<b>LAN-side receive throughput</b>	OFF	1 Gbps; 1 Gbps; 0; 0	4	4
<b>Total number of optimized flows</b>	OFF	256,000, 256,000; 0; 0	4	4
<b>Total number of flows</b>	OFF	256,000, 256,000; 0; 0	4	4
<b>File-system-utilization</b>	<b>ON</b> (cannot be disabled)	95%; 85%; 0%; 0%	4	--
<b>Tunnel Level</b>				
<b>Tunnel latency</b>	<b>ON</b>	1000; 850; 0; 0	4	--
<b>Tunnel loss pre-FEC</b>	OFF	100%; 100%; 0%; 0%	4	--
<b>Tunnel loss post-FEC</b>	OFF	100%; 100%; 0%; 0%	4	--
<b>Tunnel OOP pre-POC</b>	OFF	100%; 100%; 0%; 0%	4	--
<b>Tunnel OOP post-POC</b>	OFF	100%; 100%; 0%; 0%	4	--
<b>Tunnel utilization</b>	OFF	95%; 90%; 0%; 0%	4	4
<b>Tunnel reduction</b>	OFF	100%; 100%; 0%; 0%	--	4

## IP SLA Tab

*Configuration > Templates & Policies > TCAs > IP SLA*

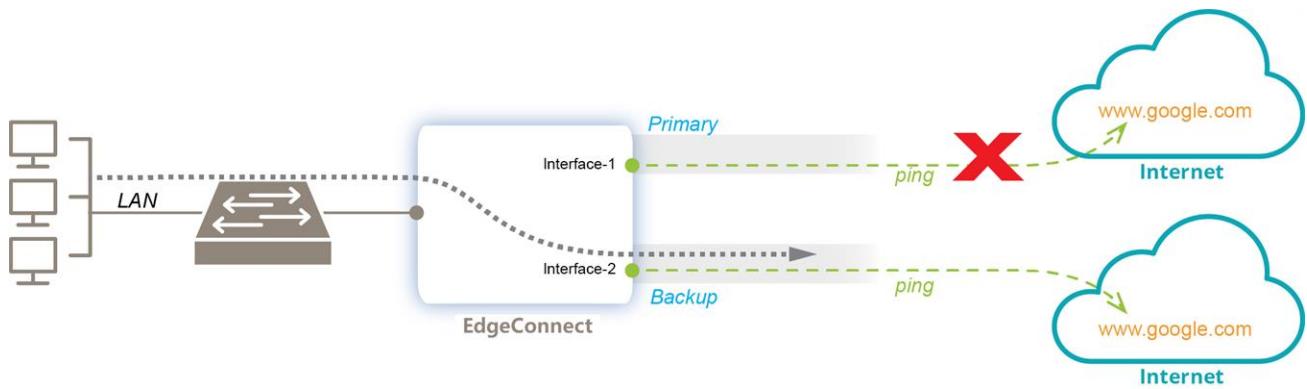
Using a polling process, **IP SLA** (Internet Protocol Service Level Agreement) tracking provides the ability to generate specific actions in the network that are completely dependent on the state of an IP interface or tunnel. The goal is to prevent black-holed traffic. For example, associated IP subnets could be removed from the subnet table, and also from subnet sharing, if the LAN-side interfaces on an appliance go down.

This tab displays all of the IP SLA rules configured on the selected appliances. To add or modify rules, click the **Edit** icon to the left of any row in the table.

### IP SLA Monitor Use Cases

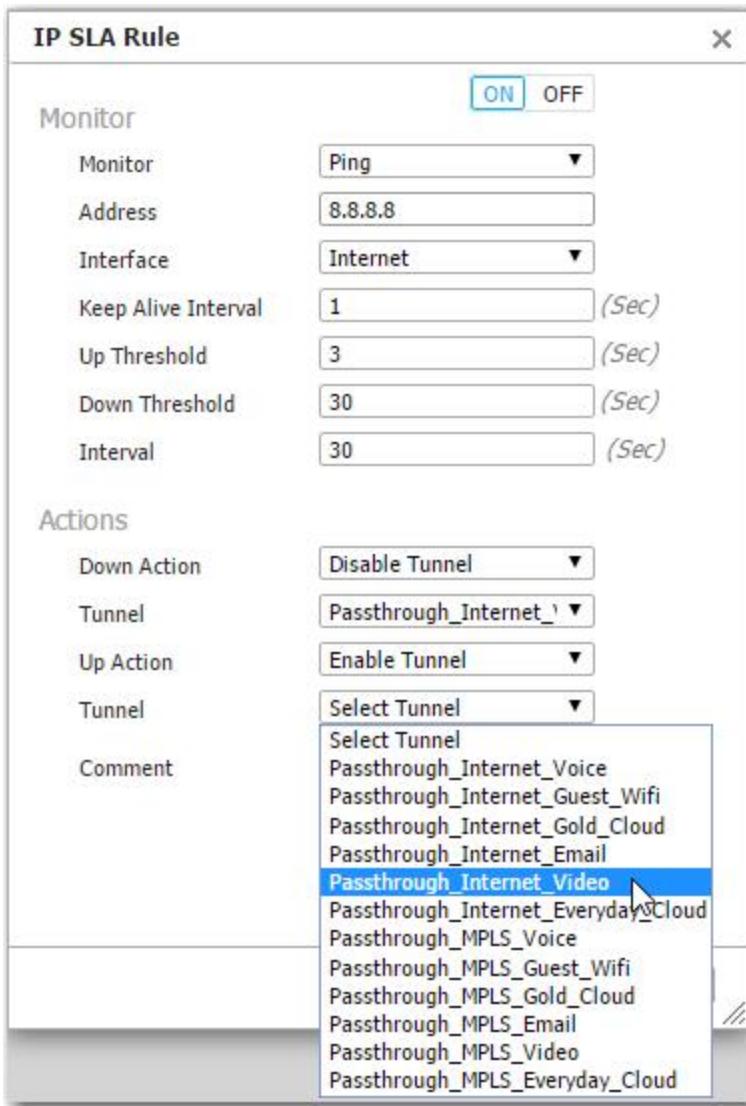
The following examples describe five basic use cases for IP SLA monitoring.

#### Example #1 - Ping via Interface

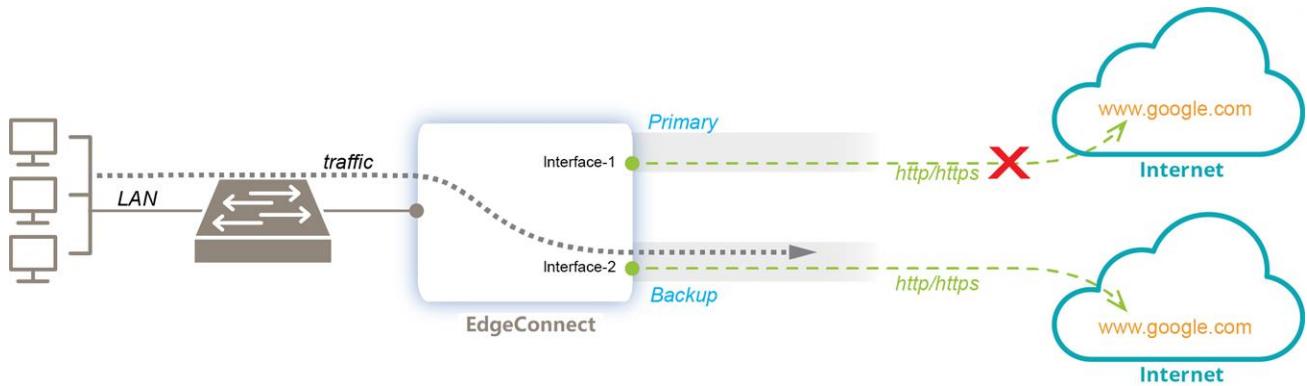


- Two passthrough tunnels configured for Internet breakout and High Availability.
- If the Primary passthrough tunnel goes down, traffic goes to Backup tunnel.

- The IP SLA Rule would look like this, with the same tunnel specified for the Down and Up Actions.



## Example #2 - HTTP/HTTPS via Interface



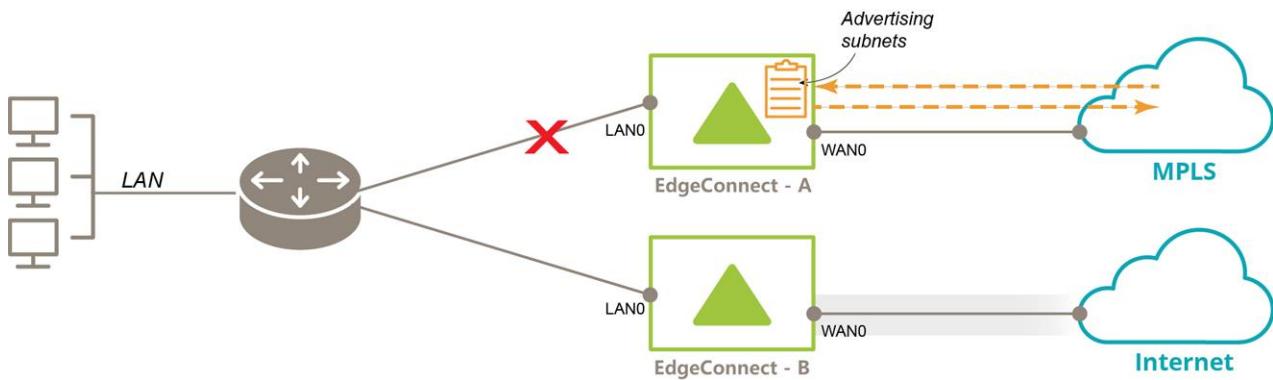
- Two passthrough tunnels configured for Internet breakout and High Availability.
- If the Primary passthrough tunnel goes down, traffic goes to Backup tunnel.
- The **IP SLA Rule** would look like this, with the same tunnel specified for the **Down** and **Up Actions**.

**IP SLA Rule**

		ON OFF
<b>Monitor</b>		
Monitor	HTTP/HTTPS ▾	
URL(s)	www.google.com ▾	
Proxy Address	optional	
Proxy Port	(0..65535)	
User Agent	optional ▾	
HTTP Request Timeout	60	Sec
Interface	Internet ▾	
Keep Alive Interval	90	Sec
Mark Up after X Succeed	2	
Mark Down after X Failed	3	
Monitor Sampling Interval	60	Sec
<b>Actions</b>		
Down Action	Disable Tunnel ▾	
Tunnel	Passthrough_Internet_Interactive ▾	
Up Action	Enable Tunnel ▾	
Tunnel	Select Tunnel ▾	
Comment	Select Tunnel Passthrough_MPLS_RealTime Passthrough_Internet_RealTime Passthrough_MPLS_Interactive Passthrough_MPLS_Default <b>Passthrough_Internet_Default</b> <span style="background-color: #0070C0; color: white; padding: 2px;"> </span> Passthrough_Internet_Interactive	
<input type="button" value="Add"/> <input type="button" value="Close"/>		

- In the **URL(s)** field, the protocol identifier is required only when specifying HTTPS, as in <https://www.google.com>.

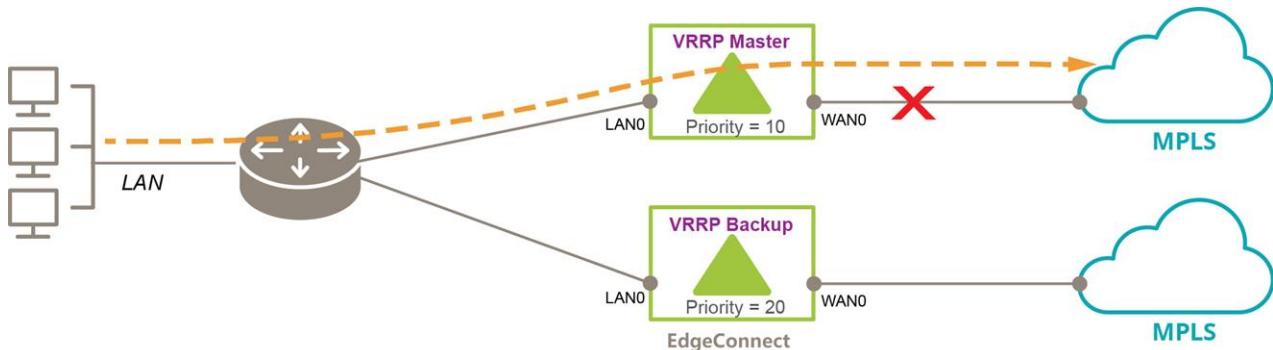
### Example #3 - Monitor Interface (LAN0)



- On **EdgeConnect - A**, we want subnet advertising to be conditional on **LAN0** being up.
- Its **IP SLA Rule** would look like this, with the **Default Subnet Action** being to resume advertising subnets.



#### Example #4 - Monitor Interface (WAN0) to Ensure High Availability



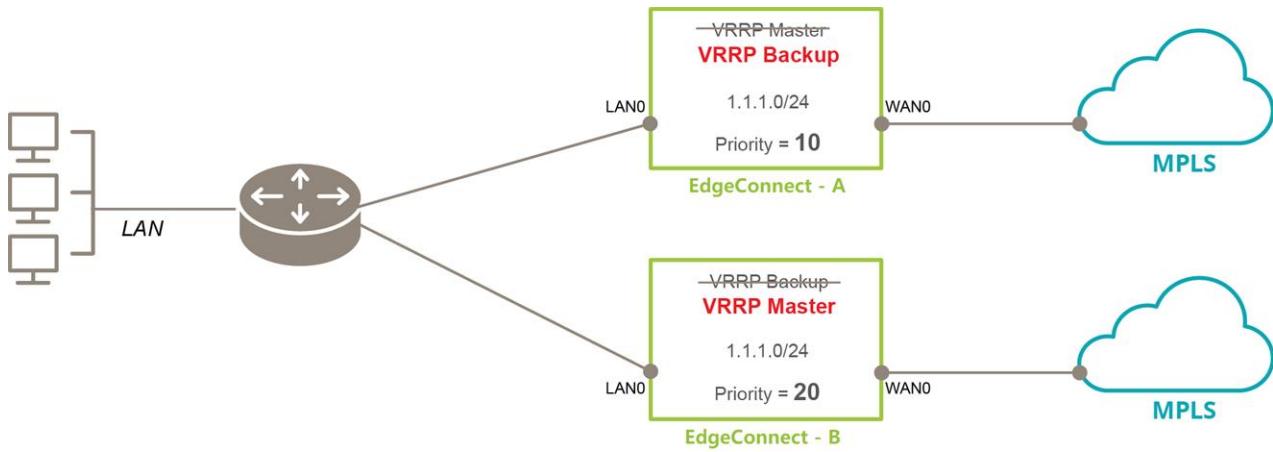
- If **WAN0** goes down on the **VRRP Master**, we want to decrease its Priority so that traffic goes to the **VRRP Backup**.

- Its IP SLA Rule would look like this, with the Default Subnet Action being to revert to the original Priority.

The screenshot shows the 'IP SLA Rule' configuration dialog box. It has two main sections: 'Monitor' and 'Actions'. In the 'Monitor' section, the 'ON' button is selected. The 'Interface' dropdown is set to 'Interface' and the 'MPLS' label is selected. The 'Interval' field is set to '30 (Sec)'. In the 'Actions' section, the 'Down Action' is set to 'Decrease VRRP Priority' and the 'Interface' is 'lan0'. The 'Priority' field is set to '30'. The 'Up Action' is set to 'VRRP Default'. There is also a 'Comment' text area which is empty. At the bottom right of the dialog are 'Add' and 'Close' buttons.

**NOTE** In this instance, the **WAN0** interface was given the label **MPLS** to match the service to which it connected.

## Example #5 - Monitor VRRP



- To monitor the VRRP router state, use **VRRP Monitor** and specify the interface on which the VRRP instance is configured.

In this example, it is **LAN0**.

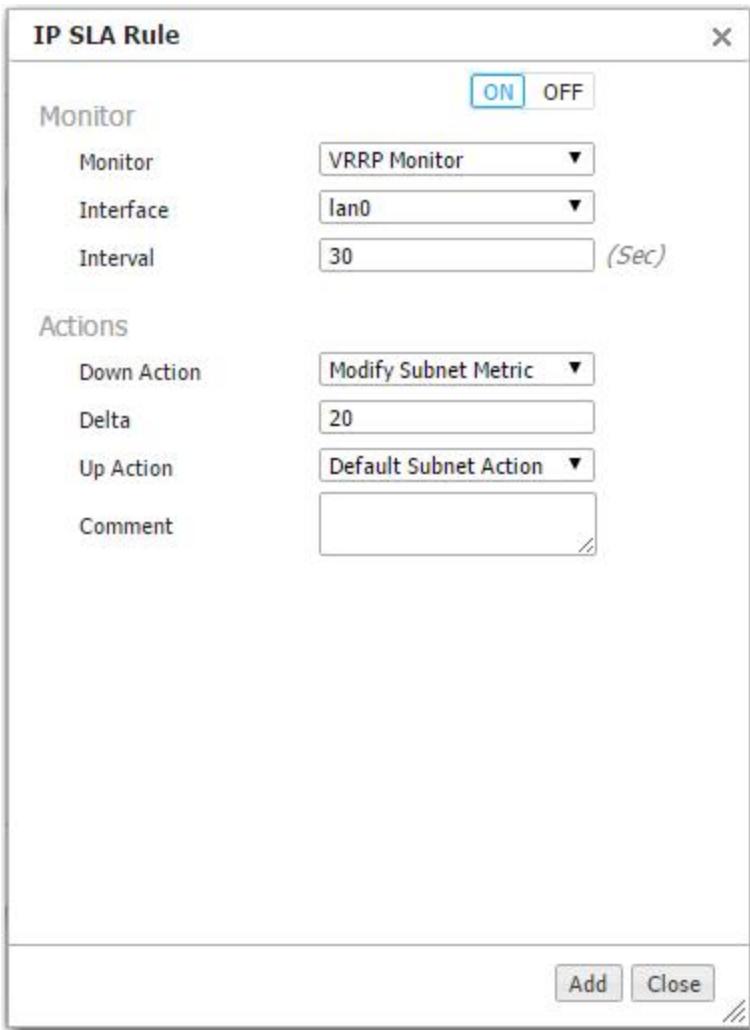
- Here we are looking at an instance where the VRRP role changes, but priority does not, for whatever reason.
- Its **IP SLA Rule** would look like this, with the **Default Subnet Action** being to revert to the original Priority.



**NOTE** In this instance, the **WAN0** interface was given the label **MPLS** to match the service to which it connected.

- Another option would be to specify **Down Action = Modify Subnet Metric**. The Web UI automatically produces another field in which you can add a positive value to the current subnet metric. **Up Action**

= Default Subnet Action would return the subnet metric to its original value.



## IP SLA Edit Row

Use this dialog box to set rules to your IP SLA. Define the Monitor and Actions by completing the following steps.

### Monitor

There are four options to choose from for a Monitor:

Option	Description
Interface	Monitors the operational status of a specific local interface.
Ping	Monitors the reachability of a specific IPv4 address.

Option	Description
<b>HTTP/HTTPS</b>	Monitors the reachability of an HTTP/HTTPS endpoint.
<b>VRRP Monitor</b>	Monitors the VRRP router state (TRUE if Master; FALSE if Backup) for a VRRP instance(s) on an interface.

Based on the Monitor chosen, the Web UI displays the appropriate fields and options.

## Actions

There are eight available **Down Actions**:

Down Action	Description
<b>Remove Auto Subnet</b>	Remove from the subnet table an auto subnet for a port (including all VLAN and subinterface subnets).
<b>Increase VRRP Priority</b>	Increase the configured VRRP router priority by a delta amount.
<b>Decrease VRRP Priority</b>	Decrease the configured VRRP router priority by a delta amount.
<b>Enable Tunnel</b>	Enable a passthrough (internet breakout) tunnel Up for IP Tracking (SLA) purposes.
<b>Disable Tunnel</b>	Disable a passthrough (internet breakout) tunnel Up for IP Tracking (SLA) purposes. The tunnel no longer can be used for load balancing purposes (when load balancing traffic between multiple passthrough tunnels), although it still can be used as a last resort for traffic forwarding.
<b>Disable Subnet Sharing</b>	Disable subnet sharing of subnets to other EdgeConnect peers on the appliance.
<b>Modify Subnet Metric</b>	Add a metric delta to the metric of all subnets shared with EdgeConnect peers.
<b>Advertise Subnets</b>	Advertise subnets to EdgeConnect peers.

There are two default **Up Actions**:

Up Action	Description
<b>Default Subnet Action</b>	This reverts whatever was the <b>Down Action</b> back to the normal state. Examples: <ul style="list-style-type: none"> <li><b>If Down Action = Disable Subnet Sharing</b>, the Up Action re-enables Subnet Sharing.</li> <li><b>If Down Action = Remove Auto Subnets</b>, the Up Action re-adds the auto subnet.</li> <li><b>If Down Action = Modify Subnet Metric</b>, the Up Action restores subnet metrics to their original values.</li> </ul>
<b>VRRP Default</b>	Reverts the VRRP priority back to the configured value.

**NOTE** If a default **Up Action** is used, it must match the **Down Action**.

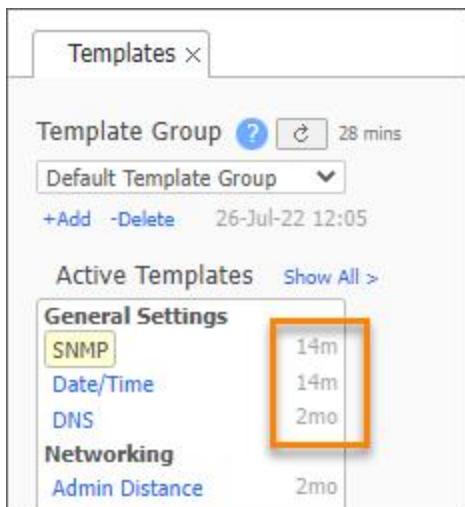
# Templates

This section describes templates and how to use them to manage and assign common configuration parameters to appliances.

## Templates Overview

**CAUTION** After saving, templates are applied automatically and replace all settings on an appliance with those configured in the template. Some templates support a MERGE option. Refer to the Help for more information.

- Each template that appears under Active Templates includes a timestamp that indicates the amount of time that has passed since it was last edited, and the most recently edited templates appear at the top of each template section in the list.



- You can edit only a template that appears under Active Templates.
- Click **Show All >** to view available templates that are not part of the selected template group.
- To add a template to Active Templates, double-click it or drag it from Available Templates.
- To copy and save the current Active Templates as a new template group, click **Save As**.

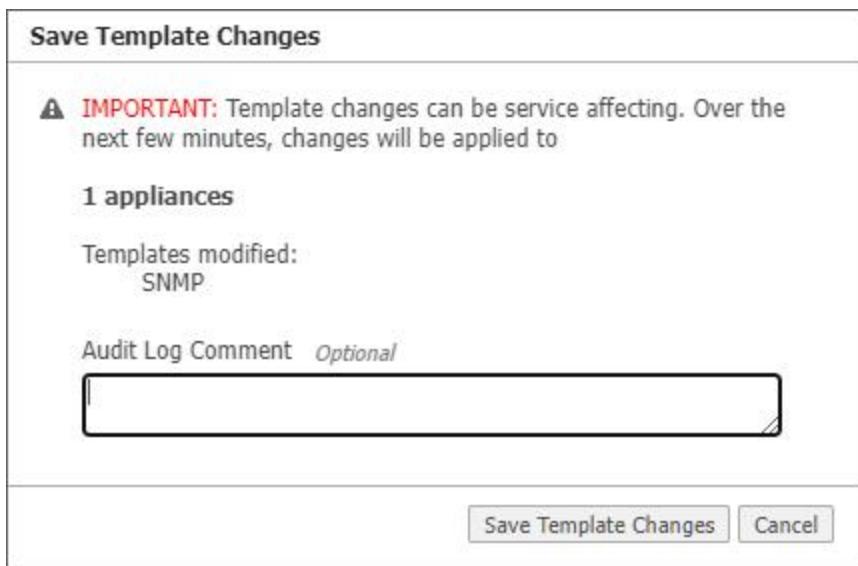
## Modifying a Template

1. Click a template under Active Templates to modify it.

The template has a timestamp that indicates when it was last modified and the user who made the changes. The timestamp appears in the format "DD-month-YY HH:MM by [user]" and the time is expressed in a 24-hour format.



2. To save the changes you made, click **Save**. The Save Template Changes dialog box opens.

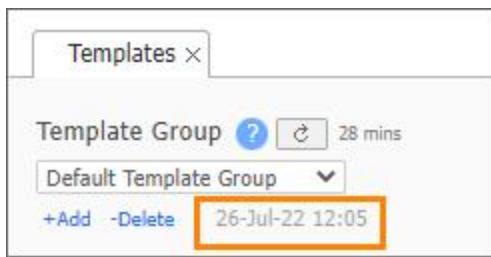


3. Enter a comment (optional) in the **Audit Log Comment** field, and then click **Save Template Changes**. Any text entered in the **Audit Log Comment** field appears on the Audit Logs tab.

## Template Groups

A Template Group contains one or more templates you can assign to some or all of the appliances in your network.

- A timestamp for the selected template group appears below the template group drop-down list and it indicates when one of the templates in the template group was last modified. The timestamp appears in the format "DD-month-YY HH:MM" and the time is expressed in a 24-hour format.



- To create a template group, click **+Add** below the template group drop-down list.
- To delete the selected template group, click **-Delete** below the template group drop-down list.
- When you apply a template group to an appliance, Orchestrator automatically keeps the templates in the group in sync with the appliance.
- To apply template groups, click **Apply Template Groups** at the bottom of the page. This will bring you to the Apply Templates tab where you can permanently associate appliances with specific template groups.
- When returning to the Templates page, Orchestrator displays the last template group viewed.

## System Template

Use this template to configure system-level features.

### *Optimization*

Field	Description
<b>IP ID auto optimization</b>	Enables any IP flow to automatically identify the outbound tunnel and gain optimization benefits. Enabling this option reduces the number of required static routing rules (route map policies).
<b>TCP auto optimization</b>	Enables any TCP flow to automatically identify the outbound tunnel and gain optimization benefits. Enabling this option reduces the number of required static routing rules (route map policies).
<b>Flows and tunnel failure</b>	If there are parallel tunnels and one fails, <b>Dynamic Path Control</b> determines where to send the flows. There are three options: <ul style="list-style-type: none"> <li><b>fail-stick</b> – When the failed tunnel comes back up, the flows do not return to the original tunnel. They stay where they are.</li> <li><b>fail-back</b> – When the failed tunnel comes back up, the flows return to the original tunnel.</li> <li><b>disable</b> – When the original tunnel fails, the flows are not routed to another tunnel.</li> </ul>

### *Network Memory*

Field	Description
<b>Encrypt data on disk</b>	Enables encryption of all the cached data on the disks. Disabling this option is not recommended.

### *Excess Flow Handling*

Field	Description
<b>Excess flow policy</b>	Specifies what happens to flows when the appliance reaches its maximum capacity for optimizing flows. The default is to <b>bypass</b> flows. Or, you can choose to <b>drop</b> the packets.

### *NextHop Health Check*

Field	Description
<b>Enable Health check</b>	Activates pinging of the next hop router.
<b>Retry count</b>	Specifies the number of ICMP echoes to send without receiving a reply before declaring that the link to the WAN next hop router is down.
<b>Interval</b>	Specifies the number of seconds between each ICMP echo sent.
<b>Hold down count</b>	If the link has been declared down, this specifies how many successful ICMP echoes are required before declaring that the link to the next hop router is up.

### *Miscellaneous*

Field	Description
<b>SSL optimization for non-IPSec tunnels</b>	Specifies whether the appliance should perform SSL optimization when the outbound tunnel for SSL packets is not encrypted (for example, a GRE or UDP tunnel). To enable Network Memory for encrypted SSL-based applications, you must provision server certificates by using the Orchestrator. This activity can apply to the entire distributed network of EdgeConnect appliances or just to a specified group of appliances.
<b>Bridge Loop Test</b>	Only valid for virtual appliances. When enabled, the appliance can detect bridge loops. If it detects a loop, the appliance stops forwarding traffic and raises an alarm. Appliance alarms include recommended actions.
<b>Always send pass-through traffic to original sender</b>	If the tunnel goes down when using WCCP and PBR, traffic that was intended for the tunnel is sent back the way it came.
<b>Enable default DNS lookup</b>	Enables the default DNS server to be included with other configured DNS servers for associating cloud portal domain names to network IP addresses.
<b>Enable HTTP/HTTPS snooping</b>	Enables a more granular application classification of HTTP/HTTPS traffic by inspection of the HTTP/HTTPS header, Host. This is enabled by default.

Field	Description
<b>Quiescent tunnel keep alive time</b>	Specifies the rate at which to send keep alive packets after a tunnel has become idle (quiescent mode). The default is 60 seconds.
<b>UDP flow timeout</b>	Specifies how long to keep the UDP session open after traffic stops flowing. The default is 120 seconds (2 minutes).
<b>Non-accelerated TCP Flow Timeout</b>	Specifies how long to keep the TCP session open after traffic stops flowing. The default is 1800 seconds (30 minutes).
<b>Maximum TCP MSS</b>	Maximum Segment Size. The default value is 9000 bytes. This ensures that packets are not dropped for being too large. You can adjust the value (500 to 9000) to lower a packet's MSS.
<b>NAT-T keep alive time</b>	If a device is behind a NAT, this specifies the rate at which to send keep alive packets between hosts to keep the mappings in the NAT device intact.
<b>Tunnel Alarm Aggregation Threshold</b>	Specifies the number of alarms to allow before alerting the tunnel alarm.
<b>Maintain end-to-end overlay mapping</b>	Enforces the same overlay to be used end-to-end when traffic is forwarded on multiple nodes.
<b>IP Directed Broadcast</b>	Allows an entire network to receive data that only the target subnet initially receives.
<b>Allow WAN to WAN routing</b>	Redirects inbound LAN traffic back to the WAN.

## Auth/Radius/TACACS+ Template

EdgeConnect appliances support user **authentication** and **authorization** as a condition of providing access rights.

- **Authentication** is the process of validating that the end user, or a device, is who they claim to be.
- **Authorization** is the action of determining what a user is allowed to do. Generally, authentication precedes authorization.
- **Map order** refers to the order in which the authorization servers are queried.
- The configuration specified for authentication and authorization **applies globally** to all users accessing that appliance.
- If a logged-in user is inactive for an interval that exceeds the inactivity time-out, the appliance logs them out and returns them to the login page. You can change that value, as well as the maximum number of sessions, in the **Session Management template**.

### Authentication and Authorization

To provide authentication and authorization services, EdgeConnect appliances:

- Support a built-in, **local database**.
- Can be linked to a **RADIUS** (Remote Authentication Dial-In User Service) server.
- Can be linked to a **TACACS+** (Terminal Access Controller Access Control System) server.

Both RADIUS and TACACS+ are client-server protocols.

## Appliance-based User Database

- The local, built-in user database supports user names, groups, and passwords.
- The two user groups are **admin** and **monitor**. You must associate each user name with one or the other. Neither group can be modified or deleted.
- The **monitor** group supports reading and monitoring of all data, in addition to performing all actions. This is equivalent to the Command Line Interface's (CLI) **enable** mode privileges.
- The **admin** group supports full privileges, along with permission to add, modify, and delete. This is equivalent to the Command Line Interface's (CLI) **configuration** mode privileges.

## RADIUS

- RADIUS uses UDP as its transport.
- With RADIUS, the authentication and authorization functions are coupled together.
- RADIUS authentication requests must be accompanied by a shared secret. The shared secret must be the same as defined in the RADIUS setup. Refer to your RADIUS documentation for details.
- **IMPORTANT:** Configure your RADIUS server's **priv levels** within the following ranges:
  - **admin** = 7 - 15
  - **monitor** = 1 - 6

## TACACS+

- TACACS+ uses TCP as its transport.
- TACACS+ provides separated authentication, authorization, and accounting services.
- Transactions between the TACACS+ client and TACACS+ servers are also authenticated through the use of a shared secret. Refer to your TACACS+ documentation for details.
- **IMPORTANT:** Configure your TACACS+ server's roles to be **admin** and **monitor**.

## What Is Recommended

- Use either RADIUS or TACACS+, but not both.
- For **Authentication Order**, configure the following:
  - **First** - Remote first.
  - **Second** - Local. If not using either, then None.
  - **Third** - None.
- When using RADIUS or TACACS+ to authenticate users, configure **Authorization Information** as follows:
  - **Map Order** - Remote First
  - **Default Role** - admin

## Flow Export Template

You can configure your appliance to export statistical data to NetFlow and IPFIX collectors.

- The appliance exports flows against two virtual interfaces—**sp\_lan** and **sp\_wan**—that accumulate the total of LAN-side and WAN-side traffic, regardless of physical interface.
- These interfaces appear in SNMP and are, therefore, "discoverable" by NetFlow and IPFIX collectors.
- **Enable Flow Exporting** allows the appliance to export the data to collectors (and makes the configuration fields accessible).
- The **Collector's IP Address** is the IP address of the device to which you are exporting the NetFlow/IPFIX statistics. The default Collector Port is **2055**.
- In **Traffic Type**, you can select as many of the traffic types as you want. The default is **WAN TX**.

## Logging Template

Use this template to configure local and remote logging parameters.

Each requires that you specify the minimum severity level of event to log.

- Set up local logging in the **Log Configuration** and **Log Facilities Configuration** sections.
- Set up remote logging in the **Remote Log Receivers** section.

## Minimum Severity Levels

In decreasing order of severity, the levels are as follows.

Severity Level	Description
<b>EMERGENCY</b>	System is unusable.
<b>ALERT</b>	Includes all alarms the appliance generates: <b>CRITICAL</b> , <b>MAJOR</b> , <b>MINOR</b> , and <b>WARNING</b> .
<b>CRITICAL</b>	Critical event.
<b>ERROR</b>	An error. This is a non-urgent failure.
<b>WARNING</b>	A warning condition. Indicates an error will occur if action is not taken.
<b>NOTICE</b>	A normal, but significant, condition. No immediate action required.
<b>INFORMATIONAL</b>	Informational. Used by Silver Peak for debugging.
<b>DEBUG</b>	Used by Support for debugging.
<b>NONE</b>	If you select <b>NONE</b> , no events are logged.

- The bolded part of the name is what displays in the log files.
- If you select **NOTICE** (the default), the log records any event with a severity of NOTICE, WARNING, ERROR, CRITICAL, ALERT, and EMERGENCY.
- These are purely related to event logging levels, **not** alarm severities, even though some naming conventions overlap. Events and alarms have different sources. Alarms, after they clear, list as the ALERT level in the **Event Log**.
- In the **Log Facilities Configuration** section, assign each message/event type (System / Audit / Firewall / IDS/IPS Events) to a syslog facility level (**local0** to **local7**).

## Configure Remote Logging

You can configure the appliance to forward all events, at and above a specified severity, to a remote syslog server.

A syslog server is independently configured for the minimum severity level that it will accept. Without reconfiguring, it might not accept as low a severity level as you are forwarding to it.

To configure remote logging:

1. Under Remote Log Receivers, click **Add**.
2. For each remote syslog server that you add to receive the events, complete the following fields with the appropriate information.

Field	Description
Remote Receiver	The remote receiver's IP address.
Port	The port number of the remote syslog server. Valid values range from 2 through 65535.
Protocol	Select the protocol you want to apply: <b>UDP</b> , <b>TCP</b> , or <b>TCP SSL</b> .
Minimum Severity	Select the minimum severity level of messages you want to log: <b>None</b> , <b>Emergency</b> , <b>Alert</b> , <b>Critical</b> , <b>Error</b> , <b>Warning</b> , <b>Notice</b> , <b>Info</b> , or <b>Debug</b> .
Facility	Select <b>all</b> , <b>local1</b> , <b>local2</b> , <b>local3</b> , <b>local4</b> , <b>local5</b> , <b>local6</b> , or <b>local7</b> .
Client Certificate	If you selected TCP SSL protocol, do one of the following: <ul style="list-style-type: none"> <li>• Click <b>Add</b> to upload the certificate and key files. Then, complete the fields as explained below in <a href="#">Add a Client Certificate below</a>.</li> <li>• Click <b>View</b> to view the client certificate.</li> <li>• Click <b>Don't Apply</b> if you do not want to apply the client certificate.</li> </ul>
Verify	Click this cell to display a checkbox, and then select the checkbox to verify the server certificate.

## Add a Client Certificate

To add a client certificate:

1. In the Client Certificate column, click **Add**.

The Add Remote Receiver SSL Certificate dialog box opens.

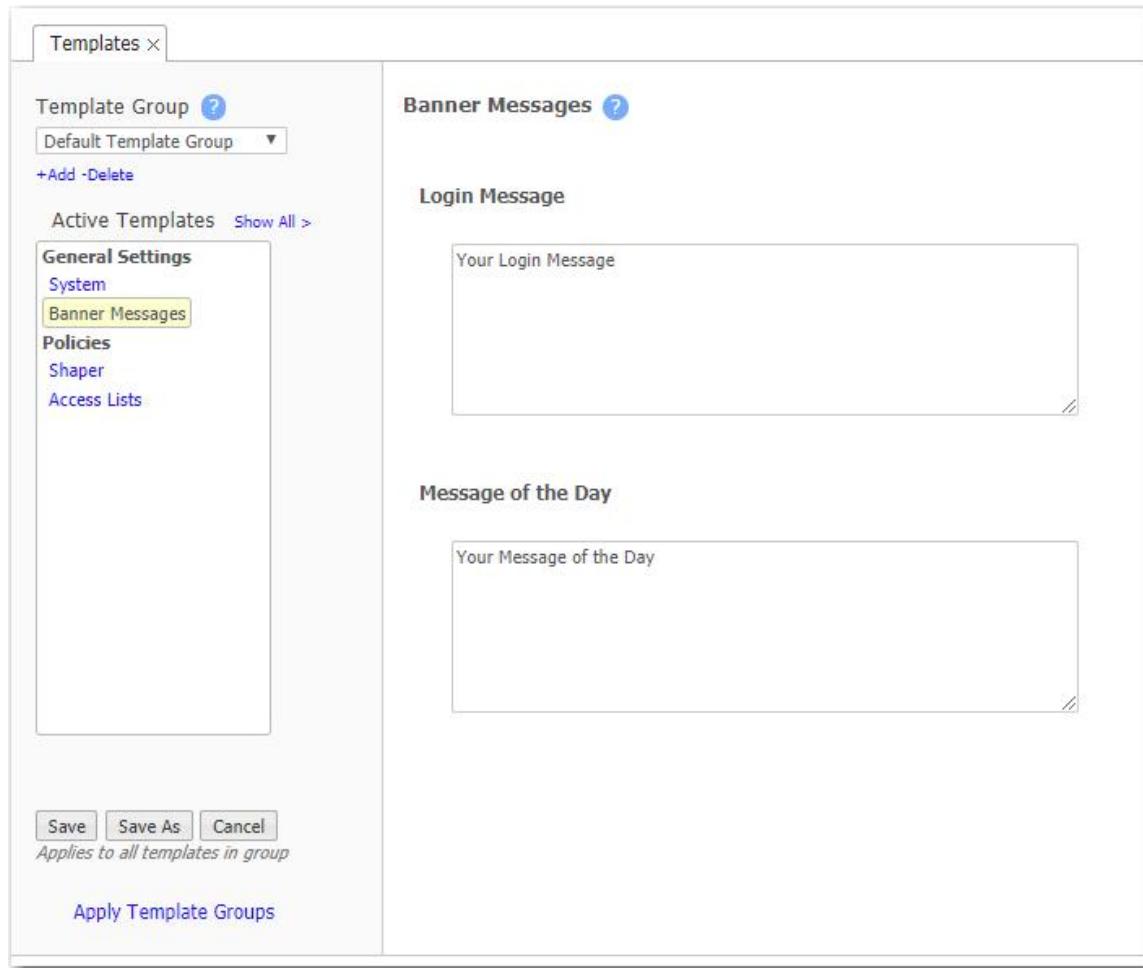
2. Complete the following fields:

Field	Description
<b>PFX</b>	To use a PFX certificate file, select this check box.
<b>Certificate File</b>	
<b>Certificate File</b>	Click <b>Choose File</b> . Locate and select the certificate file, and then click <b>Open</b> .
<b>Private Key File</b>	Click <b>Choose File</b> . Locate and select the private key file, and then click <b>Open</b> . If you selected PFX Certificate File, this field is disabled.
<b>Import Password</b>	Enter the import password for the certificate.
<b>Passphrase</b>	Enter the passphrase for the certificate.

3. Click **Add**.

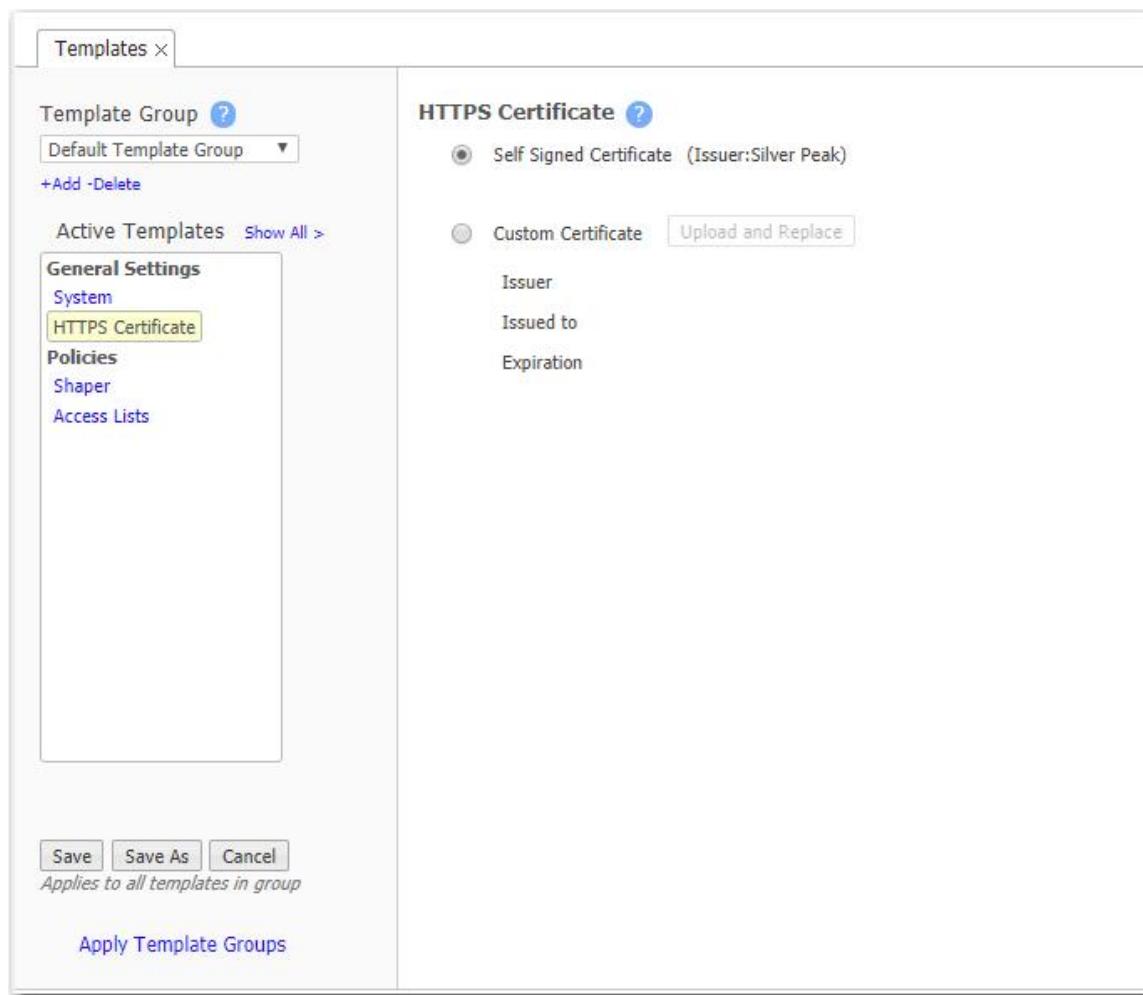
## Banner Messages Template

- The **Login Message** appears before the login prompt.
- The **Message of the Day** appears after a successful login.



## HTTPS Certificate Template

The VXOA software includes a self-signed certificate that secures the communication between the user's browser and the appliance. You also have the option to install your own custom certificate, acquired from a CA certificate authority.



### To use a custom certificate with a specific appliance:

1. Consult with your IT security team to generate a certificate signing request (CSR), and submit it to your organization's chosen SSL Certificate Authority (CA).

Examples of Certificate Authorities include GoDaddy, Verisign, Comodo, Symantec, Microsoft Entrust, GeoTrust, and so forth.

- For a list of what is supported, refer to [EdgeConnect and Orchestrator Security Algorithms](#).
- All certificate and key files must be in **PEM** format.

2. After the Certificate Authority provides a CA-verified certificate:

- If your IT security team advises the use of an Intermediate CA, use an **Intermediate Certificate File**. Otherwise, skip this file.
- Load the **Certificate File** from the CA.
- Upload the **Private Key File** that was generated as part of the CSR.

3. To associate the CA verified certificate for use with Orchestrator, click **Add**.

## User Management Template

Use this tab to manage the default users and, if desired, require a password with the highest user privilege level when using the Command Line Interface.

The screenshot shows the 'User Management' tab within the 'Templates' interface. On the left, there's a sidebar with 'General Settings' and 'System' selected. Under 'User Management', there are 'Policies', 'Shaper', and 'Access Lists'. The main area shows a table of user accounts:

User Name	Capability	Password	Confirm Password	Enabled
admin	admin	*****	*****	Yes
monitor	monitor	*****	*****	<input checked="" type="checkbox"/>

Below the table, there's a section for 'Password for CLI "Enable" privilege' with fields for 'Require Password' (checkbox), 'Password' (text input), and 'Confirm Password' (text input). At the bottom, there are 'Save', 'Save As', and 'Cancel' buttons, and a note 'Applies to all templates in group'. There's also a link 'Apply Template Groups'.

### Default User Accounts

- Each appliance has two default user accounts, **admin** and **monitor**, that cannot be deleted.
- You can, however, assign a new password to either one and apply it to any appliances you want.

### Command Line Interface Privileges

- The Command Line Interface (CLI) for physical EdgeConnect appliances has three command modes. In order of increasing permissions, they are User EXEC Mode, Privileged EXEC Mode, and Global Configuration Mode.

- When you first log in to an EdgeConnect appliance via a console port, you are in User EXEC Mode. This provides access to commands for many non-configuration tasks, such as checking the appliance status.
- To access the next level, Privileged EXEC Mode, you would enter the **enable** command. With this template, you can choose to associate and enforce a password with the **enable** command.

## DNS Template

A **Domain Name Server** (DNS) stores the IP addresses with their associated domain names. It enables you to reference locations by domain name, such as *mycompany.com*, instead of using the routable IP address.

- You can configure up to three name servers.
- Under **Domain Names**, add the network domains to which your appliances belong.

## Date/Time Setting

Configure an appliance's **date and time** manually, or complete the following steps to configure it to use an NTP (Network Time Protocol) server.

1. From the Time Zone list, select the appliance's geographical location.
2. If you select Manual, the appliance is matched to your web client system when the template is applied. This eliminates the delay between configuring time manually and applying the template.
3. To use an NTP server, select **NTP Time Synchronization** and complete the following steps.
  - a. Click **Add**.
  - b. Enter the IP address or host name of the server.
  - c. Select the version of NTP protocol to use.

**NOTE** The server is selected in the order listed when you list more than one NTP server.

## Data Collection

- Orchestrator collects and puts all statistics in its own database in Coordinated Universal Time (UTC).
- When a user views statistics, the appliance (or Orchestrator server) returning the statistics always presents the information relative to the browser time zone.

## SNMP Template

EdgeConnect appliances support Management Information Base (MIB-II) as described in RFC 1213 for cold start traps, warm start traps, and EdgeConnect private MIBs. Appliances issue an SNMP trap during reset when loading a new image, recovering from a crash, or rebooting.

An appliance sends a trap every time an alarm is raised or cleared. Traps contain additional information about alarms, including severity, sequence number, a text-based description of the alarm, and the time the alarm was created. For more information, you can download a .zip archive containing supported MIBs at <https://www.arubanetworks.com/techdocs/sdwan/mibs/>.

Use this dialog box to configure the appliance's **SNMP** agent and trap receivers.

1. Select the **Enable SNMP** check box to activate configuration options for SNMP v1/v2, SNMP v3, and **Trap Receivers** details.
2. If you select the **Enable SNMP Traps** check box, the SNMP agent on the appliance sends traps to configured receivers.
3. Use the **Default Trap Community** field to specify the string the trap receiver uses to accept traps being sent to it. The default value is **public**. You can modify this value.

### SNMP v1/v2

Configure the following fields for SNMP v1 and v2c.

Field	Description
<b>Enable SNMP</b>	Allows the SNMP agent on the appliance to send traps to configured receivers.
<b>Read-Only Community</b>	The SNMP application needs to present this text string (secret) to poll the appliance's SNMP agent. The default value is <b>public</b> . You can modify this value.

## SNMP v3

For additional security, configure SNMP v3 if you want to authenticate without using clear text. To add an SNMP v3 user, click **Add** above the SNMP v3 table and configure the following properties:

Field	Description
<b>Enabled</b>	Select this check box to enable the selected user. Clear this check box to disable the user and maintain the configuration.
<b>Username</b>	Enter the username to identify the SNMP v3 user.
<b>Authentication Type</b>	Select the authentication type to use for SNMP requests from the user. <b>NOTE</b> Authentication type is required and SHA-1 is the only supported algorithm.
<b>Authentication Password</b>	Enter a password that the SNMP agent can use to authenticate requests sent by the user. <b>NOTE</b> The password must be at least 20 characters long.
<b>Privacy Type</b>	Select the encryption type to use for encrypting requests from the SNMP user. <b>NOTE</b> Encryption is required, and AES-128 is the only supported algorithm.
<b>Privacy Password</b>	Enter a password (key) to use for encrypting requests sent by the user. <b>NOTE</b> The password must be at least 20 characters long.

To delete an SNMP v3 user, click the X to the right of the entry in the table.

## Trap Receivers

To configure a trap receiver, click **Add** above the Trap Receivers table and configure the following properties:

**NOTE** You can configure up to three trap receivers per appliance.

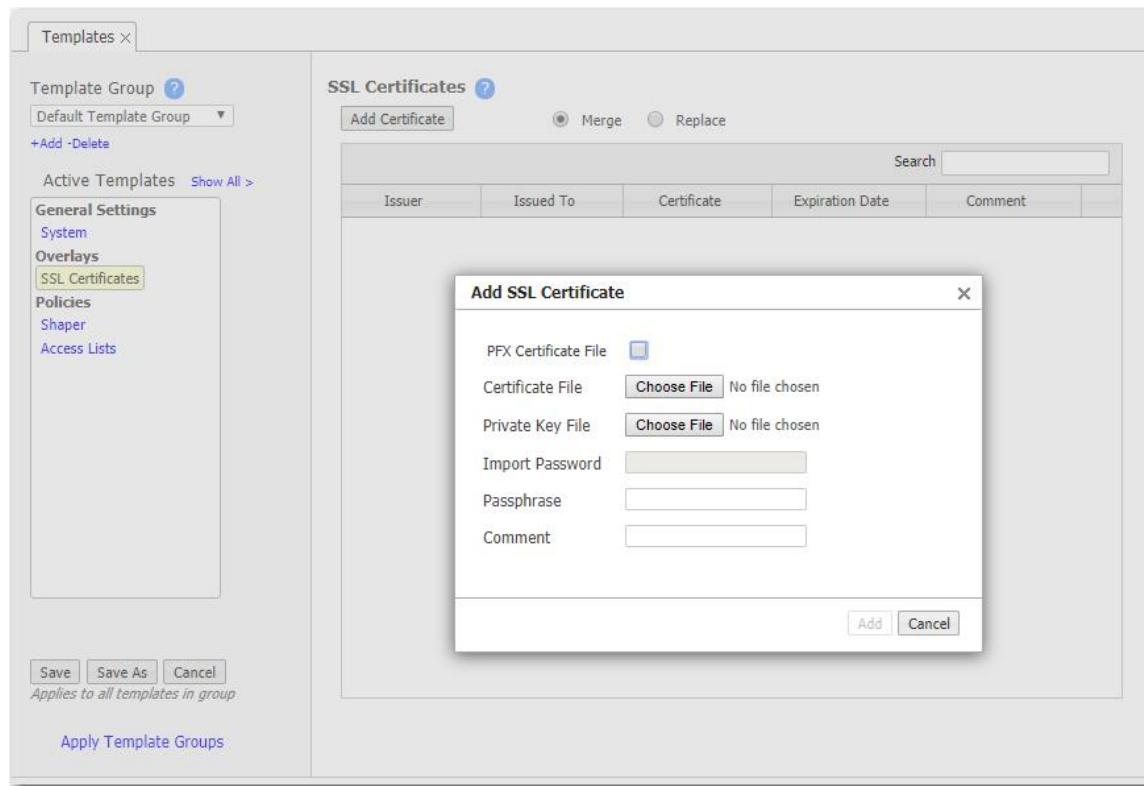
Field	Description
<b>Host</b>	IP address of the host where traps should be sent.
<b>Version</b>	Select the SNMP version of the trap receiver.
<b>Community/Username</b>	For v1 and v2c, enter the community string the receiver should use to accept traps. If left blank, the default community string (public) is used. If a different community string is configured on the trap receiver, enter it here. For v3, specify the SNMP v3 user that is sending traps to the receiver.
<b>Enabled</b>	Select this check box to enable the receiver. Clear this check box to disable the receiver and maintain the configuration.

To delete a receiver, click the X to the right of the entry in the table.

## SSL Certificates Template

Use this page for **SSL Certificates** when the server is *part of your enterprise network* and has its own enterprise SSL certificates and key pairs.

**NOTE** To decrypt SSL for SaaS (cloud-based) services, use the **SSL for SaaS** template.



EdgeConnect provides deduplication for Secure Socket Layer (SSL) encrypted WAN traffic by supporting the use of SSL certificates and other keys:

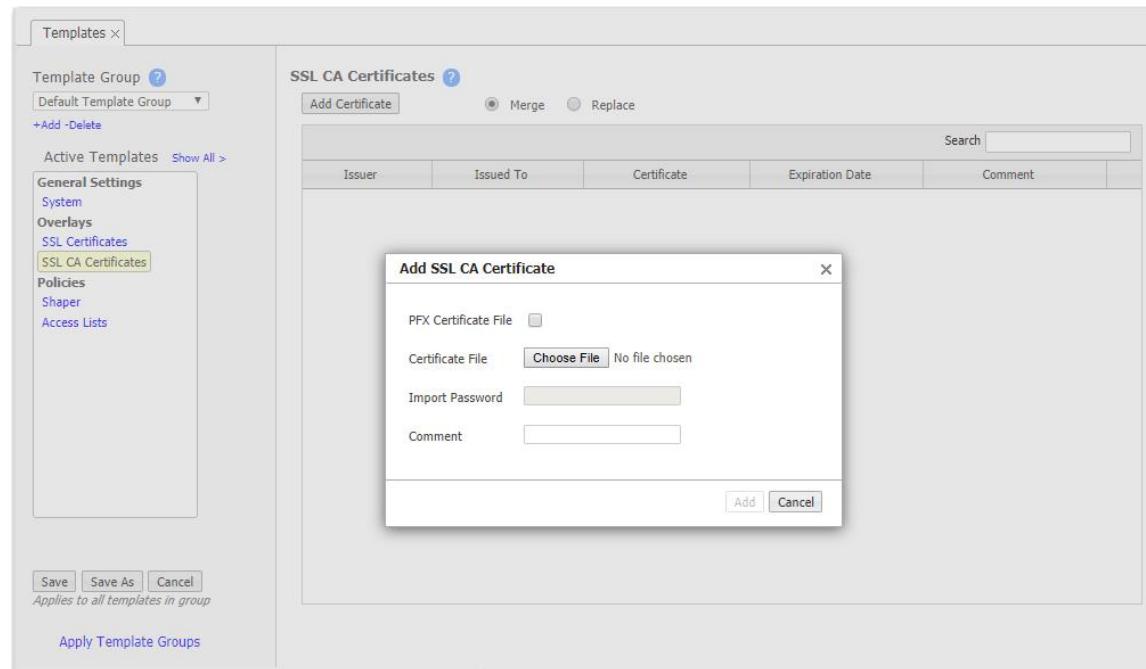
- EdgeConnect decrypts SSL data using the configured certificates and keys, optimizes the data, and transmits data over an IPSec tunnel. The peer EdgeConnect appliance uses configured SSL certificates to re-encrypt data before transmitting.
- Peers that exchange and optimize SSL traffic must use the same certificate and key.
- Use this template to provision a certificate and its associated key across multiple appliances.
  - You can add either a PFX certificate (generally, for Microsoft servers) or a PEM certificate.
  - The default is PEM when PFX Certificate File is deselected.
  - If the key file has an encrypted key, enter the passphrase needed to decrypt it.

- Before installing the certificates, you must do the following:
  - Configure the tunnels bilaterally for **IPSec** (or **IPSec\_UDP**) mode.  
To do so, access the **Configuration > Networking > Tunnels > Tunnels** page, select the tunnel, and for **Mode**, select **IPSec**.
  - Verify that **TCP acceleration** and **SSL acceleration** are enabled.  
To do so, access the **Configuration > Templates & Policies > Optimization Policies** page, and then review the **Set Actions**.
- If you choose to be able to decrypt the flow, optimize it, and send it in the clear between appliances, access the **System** template and select **SSL optimization for non-IPSec tunnels**.

**TIP** For a historical matrix of EdgeConnect and Orchestrator security algorithms, click [here](#).

## SSL CA Certificates Template

If the enterprise certificate you used for signing substitute certificates is subordinate to higher level **Certificate Authorities (CA)**, you must add those CA certificates here. If the browser cannot validate up the chain to the root CA, it will warn you that it cannot trust the certificate.

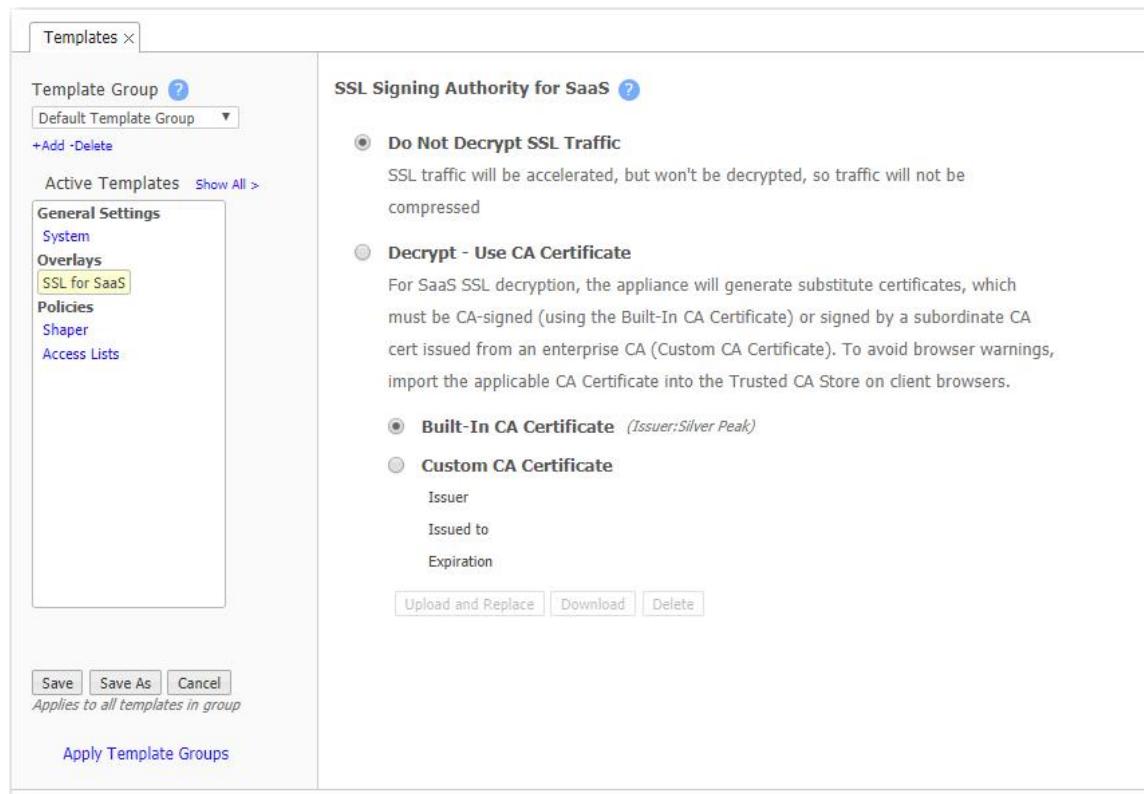


**TIP** For a historical matrix of EdgeConnect and Orchestrator security algorithms, click [here](#).

## SSL for SaaS Template

To fully compress SSL traffic for a SaaS service, the appliance must decrypt it and then re-encrypt it.

To do so, the appliance generates a substitute certificate that then must be signed by a Certificate Authority (CA).



There are two possible signers:

- For a **Built-In CA Certificate**, the signing authority is Silver Peak.
  - The appliance generates it locally, and each certificate is unique. This is an ideal option for Proof of Concept (POC) and when compliance is not a big concern.
  - To avoid browser warnings, follow up by importing the certificate into the browser from the client-side appliance.
- For a **Custom CA Certificate**, the signing authority is the Enterprise CA.
  - If you already have a subordinate CA certificate (for example, an SSL proxy), you can upload it to Orchestrator and push it out to the appliances. If you need a copy of it later, just download it from here.

- If this substitute certificate is subordinate to a root CA certificate, also install the higher-level **SSL CA certificates** (into the **SSL CA Certificates** template) so that the browser can validate up the chain to the root CA.
- If you **do not** already have a subordinate CA certificate, you can access any appliance's **Configuration > Templates & Policies > Applications & SaaS > SaaS Optimization** page and generate a Certificate Signing Request (CSR).

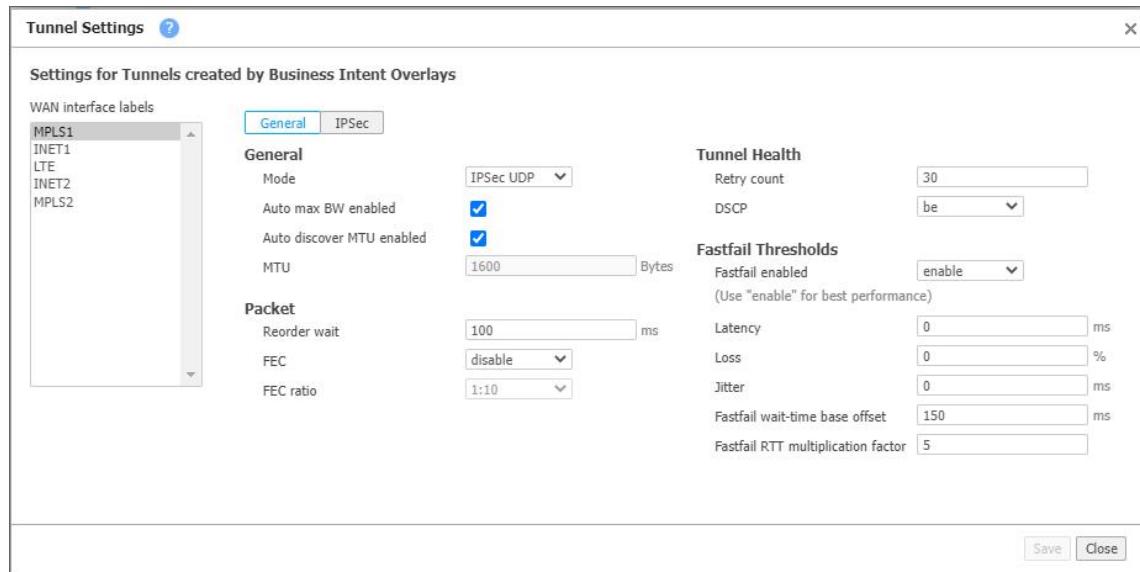
**TIP** For a historical matrix of EdgeConnect and Orchestrator security algorithms, click [here](#).

## Tunnels Template

**NOTE** If you are deploying an SD-WAN network, the Business Intent Overlays (BIOs) govern tunnel properties. In this case, you do not need this template.

*If you are not creating overlays*, use this template to assign and manage tunnel properties.

- Tunnel templates can be applied to any appliances (with or without tunnels). However, only existing tunnels can accept the template settings. To enable an appliance to apply these same settings to future tunnels, select **Make these the Defaults for New Tunnels**.
- To view, edit, and delete tunnels, use the Tunnels tab. The **Mode** selected determines the tabs that display.



*Tunnels Template Settings*

Field	Description
<b>Mode</b>	Indicates whether the tunnel protocol is <b>udp</b> , <b>gre</b> , or <b>ipsec</b> .
<b>Admin state</b>	Indicates whether the tunnel has been set to admin Up or Down.
<b>Auto discover MTU enabled</b>	Allows an appliance to determine the best MTU to use.
<b>Auto max BW enabled</b>	When enabled, allows the appliances to auto-negotiate the maximum tunnel bandwidth.
<b>DSCP</b>	Determines the DSCP marking that the keep-alive messages should use.

### Tunnels Template Settings

Field	Description
<b>Fastfail Thresholds</b>	When multiple tunnels are carrying data between two appliances, this feature determines how quickly to disqualify a tunnel from carrying data.

The Fastfail connectivity detection algorithm for the wait time from receipt of last packet before declaring a **brownout** is:

$$T_{wait} = Base + N * RTTavg$$

where **Base** is a value in milliseconds, and **N** is the multiplier of the average Round Trip Time over the past minute.

For example, if:

$$Base = 200ms$$

$$N = 2$$

Then,

$$RTTavg = 50ms$$

The appliance declares a tunnel to be in **brownout** if it does not see a reply packet from the remote end within 300ms of receiving the most recent packet.

In the Tunnel Advanced Options, **Base** is expressed as **Fastfail wait-time base offset (ms)**, and **N** is expressed as **Fastfail RTT multiplication factor**.

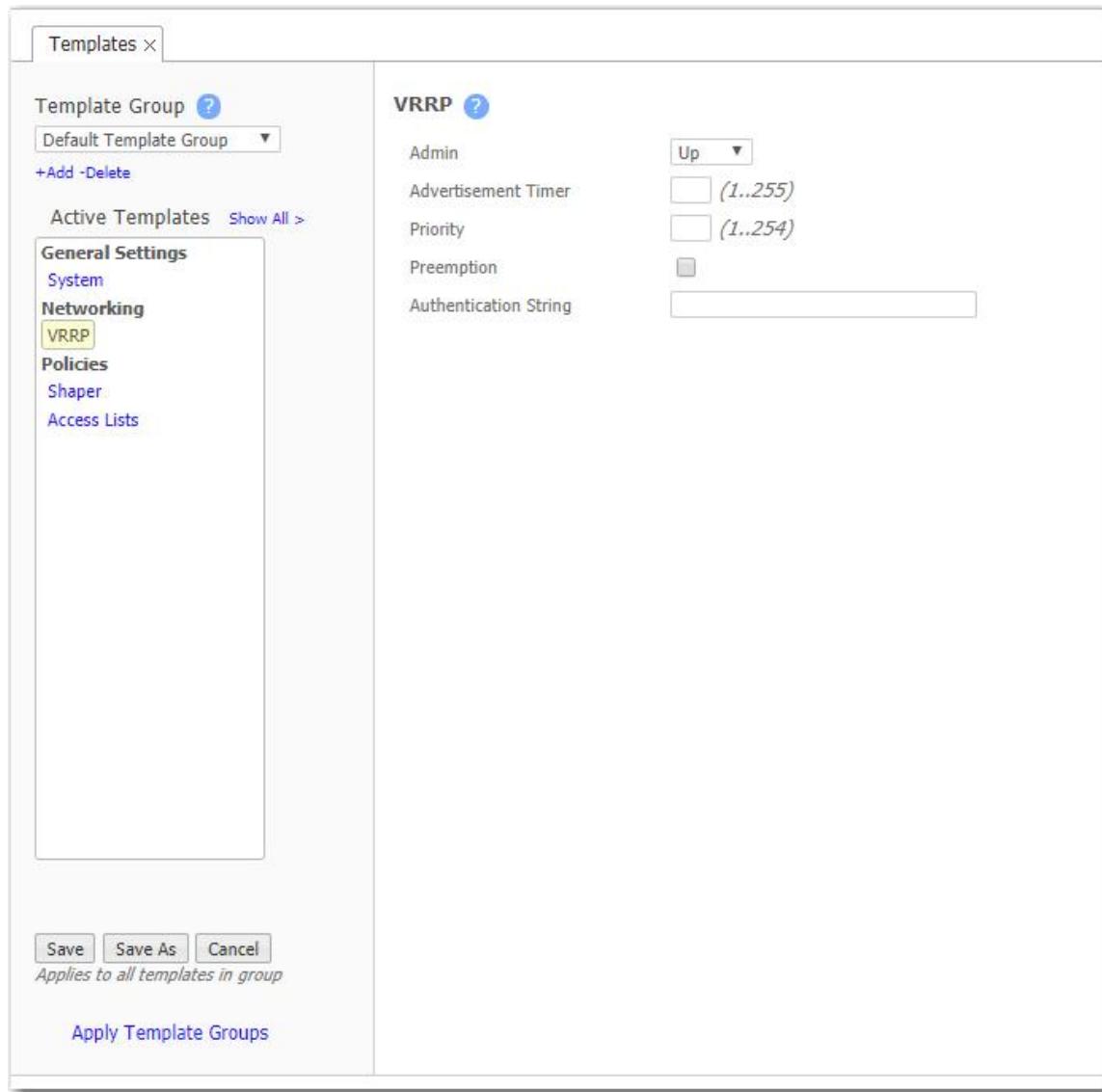
- **Fastfail enabled** - This option is triggered when a tunnel's keepalive signal does not receive a reply. The options are **disable**, **enable**, and **continuous**. If the disqualified tunnel subsequently receives a keepalive reply, its recovery is instantaneous.
  - If set to **disable**, keepalives are sent every second, and 30 seconds elapse before failover. In that time, all transmitted data is lost.
  - If set to **enable**, keepalives are sent every second, and a missed reply increases the rate at which keepalives are sent from one per second to ten per second. Failover occurs after one second.
  - When set to **continuous**, keepalives are continuously sent at ten per second. Therefore, failover occurs after one tenth of a second.
- Thresholds for **Latency**, **Loss**, or **Jitter** are checked once every second.
  - Receiving three successive measurements in a row that exceed the threshold puts the tunnel into a brownout situation and flows will attempt to fail over to another tunnel within the next 100ms.
  - Receiving three successive measurements in a row that drop below the threshold will drop the tunnel out of brownout.

### Tunnels Template Settings

Field	Description
<b>FEC</b>	(Forward Error Correction) can be set to <b>enable</b> , <b>disable</b> , or <b>auto</b> .
<b>FEC ratio</b>	Is an option when FEC is set to <b>auto</b> that specifies the maximum ratio. The options are <b>1:2</b> , <b>1:5</b> , <b>1:10</b> , or <b>1:20</b> .
<b>IPSec anti-replay window</b>	Provides protection against an attacker duplicating encrypted packets by assigning a unique sequence number to each encrypted packet. The decryptor keeps track of which packets it has seen on the basis of these numbers. The default window size is 64 packets.
<b>IPSec pre-shared key</b>	A shared, secret string of Unicode characters that is used for authentication of an IPSec connection between two parties.
<b>MTU</b>	Maximum Transmission Unit (MTU) is the largest possible unit of data that can be sent on a given physical medium. For example, the MTU of Ethernet is 1500 bytes. MTUs up to 9000 bytes are supported. Auto allows the tunnel MTU to be discovered automatically, and it overrides the MTU setting.
<b>Reorder wait</b>	Maximum time (in ms) the appliance holds an out-of-order packet when attempting to reorder. The <b>100ms</b> default value should be adequate for most situations. FEC can introduce out-of-order packets if the reorder wait time is not set high enough.
<b>Retry count</b>	Number of failed keep-alive messages that are allowed before the appliance brings the tunnel down.
<b>UDP destination port</b>	Used in UDP mode. Accept the default value unless the port is blocked by a firewall.
<b>UDP flows</b>	Used in UDP mode. Number of flows over which to distribute tunnel data. Accept the default.

## VRRP Template

Use this template to distribute common parameters for appliances deployed with **Virtual Router Redundancy Protocol (VRRP)**.



In an out-of-path deployment, one method for redirecting traffic to the EdgeConnect appliance is to configure VRRP on a common virtual interface. Possible scenarios are:

- When no spare router port is available, a single appliance uses VRRP to peer with a router (or Layer 3 switch). This is appropriate for an out-of-path deployment in which no redundancy is needed.
- A pair of active, redundant appliances use VRRP to share a common, virtual IP address at their site. This deployment assigns one appliance a higher priority than the other, thereby making it the Master appliance, and the other the Backup.

### VRRP Template Settings

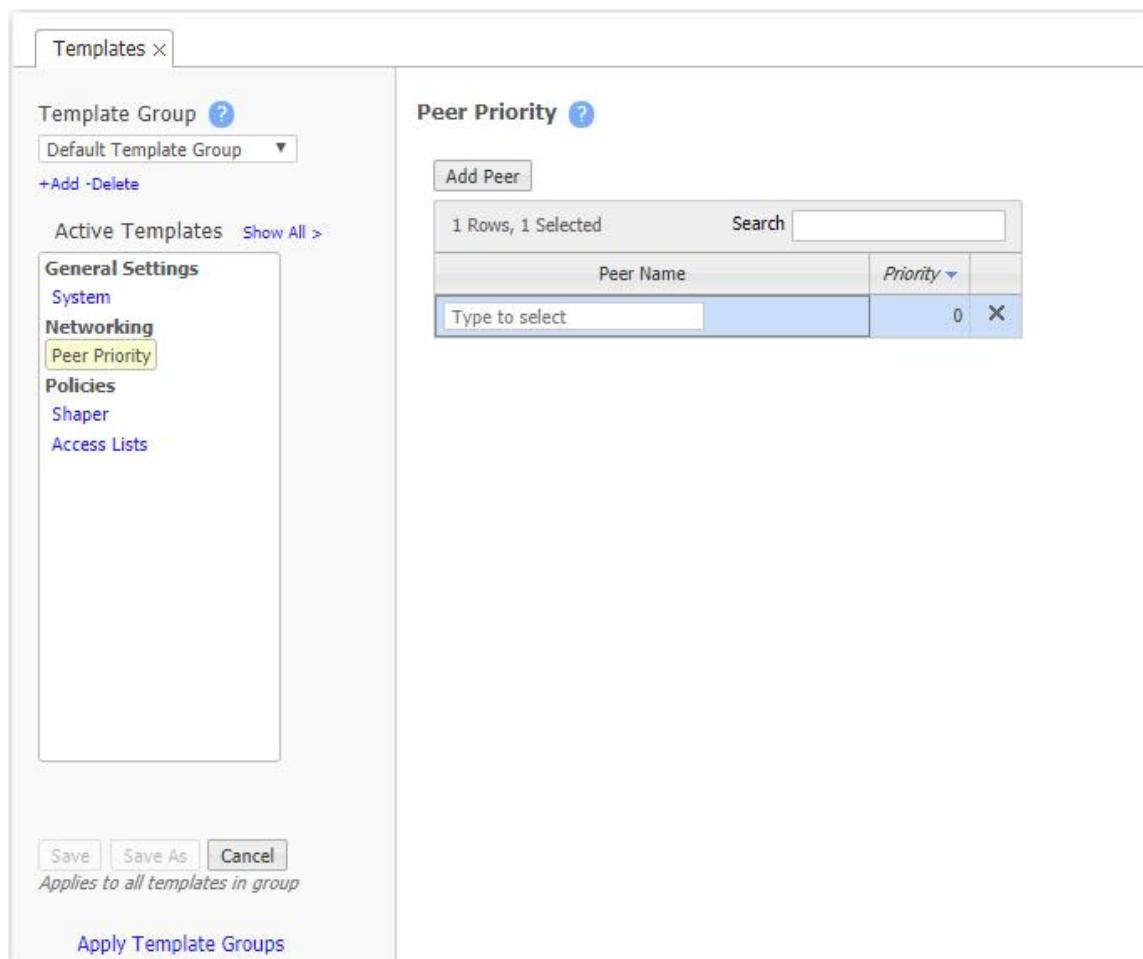
Field	Description
<b>Admin</b>	Options are <b>up</b> (enable) and <b>down</b> (disable).
<b>Advertisement Timer</b>	Default is <b>1 second</b> .
<b>Authentication String</b>	Clear text password for authenticating group members.
<b>Preemption</b>	Leave this selected/enabled so that after a failure, the appliance with the highest priority comes back online and again assumes primary responsibility.
<b>Priority</b>	The greater the number, the higher the priority. The appliance with the higher priority is the VRRP Master.

## Peer Priority Template

When an appliance receives a **Subnet** with the same **Metric** from multiple remote/peer appliances, it uses the Peer Priority list as a tie-breaker.

- If a **Peer Priority** is not configured, the appliance randomly distributes flows among multiple peers.
- The lower the number, the higher the peer's priority.

**NOTE** This feature requires appliance software 8.3.3.0 or higher for version 8 releases, and requires 9.0.2.0 or higher for version 9 releases.



## Route Redistribution Maps Template

To use this template, you must have your route maps configured for either SD-WAN, BGP, and OSPF. See the **Routes** tab for more details about the configuration and defining rules for your route maps.

### Merge and Replace

If you select **Merge**, new maps are added to the existing maps. If the map already exists, the new map will match appliance rules in the orchestrator range. If the configured rules do not match, the new map's rules are appended to the existing rules. **Replace** will take the new maps and replace all existing maps and not include the rules that match outside of the configured range.

To redistribute a route map:

1. Select the direction of traffic you want to redistribute your routes to: **SD-WAN Fabric, BGP Inbound and Outbound, and OSPF**.
2. When selected, click **Add Map**.
3. Enter a **Map Name**, and then click **Add**.
4. Select **Add Rule**. The **Add Rule** window opens.

In this window, you define the rules applied to your route map, which includes the **Match Criteria** and the **Set Actions**. Each route map has a **match** command and **set** command. The match command verifies the attributes of the original route the protocol supports. The set command modifies information that is redistributed into the target protocol.

**NOTE** You can apply 128 rules per map.

5. Click **Add**.

## Routes Template

Use the following settings to apply subnet sharing configuration to appliances associated with this template group. *Subnet sharing* is the protocol used to exchange routes between EdgeConnect appliances across the SD-WAN fabric.

- **Automatically advertise local LAN subnets:** The appliance will advertise LAN and virtual interface subnets to SD-WAN fabric peers.
- **Automatically advertised local WAN subnets:** The appliance will advertise WAN interface subnets to SD-WAN fabric peers.
- **Redistribute learned BGP routes to Silver Peak Peers:** Advertise BGP routes that your appliance has learned to EdgeConnect peers.

Enter specific values for the following:

Field	Description
<b>Metric for automatically added routes</b>	50 (default value).
<b>Route map name to redistribute routes to SD-WAN fabric</b>	Name of the route map being redistributed to the SD-WAN.
<b>Include BGP local ASN to routes sent to SD-WAN fabric</b>	Select <b>Don't apply</b> , <b>Yes</b> , or <b>No</b> .
<b>Filter routes from SD-WAN fabric with matching local ASN</b>	Select <b>Don't apply</b> , <b>Yes</b> , or <b>No</b> .

Field	Description
<b>Tag BGP communities to routes</b>	<p>Send the specified communities with routes that are advertised to both SD-WAN fabric peers and BGP peers, if the routes are learned from any of the following source protocols:</p> <ul style="list-style-type: none"><li>• Local/Static</li><li>• SD-WAN (Local/Static)</li><li>• SD-WAN (BGP)</li><li>• SD-WAN (OSPF)</li></ul> <p>Select <b>Don't apply</b>, <b>Yes</b>, or <b>No</b>. If you select <b>Yes</b>, enter the BGP communities you want to be tagged in the field.</p> <p><b>NOTE</b> A community must be a combination of two numbers (0 to 65535) separated by a colon. For multiple communities, use a comma to separate them.</p>

**NOTE** If you select **Don't apply**, Orchestrator ignores the field when applying this template to appliances.

## BGP Template

Use the BGP template to apply BGP configurations per segment to all appliances in the SD-WAN fabric.

1. Click the edit icon next to the segment for which you want to modify the configuration.
2. Configure the following elements as needed:

Field	Description
<b>AS Path Propagate</b>	Select <b>Yes</b> to enable this appliance to send the full AS path associated with a prefix to other routers and appliances, avoiding routing loops. This will provide the learned path from an external prepend between a remote BGP site to local BGP peers.
<b>Graceful Restart</b>	Select <b>Yes</b> to enable receiver-side graceful restart capability. EdgeConnect retains routes learned from the peer and continues to use it for forwarding (if possible) in the event that a BGP peer goes down. Retained routes are considered stale routes. They will be deleted and replaced when new routes are received.
<b>Max Restart Time</b>	If Graceful Restart is enabled, specifies the maximum time in seconds to wait for a capable peer to come back after a restart or peer session failure.
<b>Stale Path Time</b>	If Graceful Restart is enabled, specifies the maximum time in seconds following a peer restart before removing stale routes associated with a peer.
<b>Next-Hop-Self</b>	Advertised route connected to a CE router that an EdgeConnect appliance learns from a PE router.
<b>Keep Alive Timer</b>	This is the interval, in seconds, between keep alive signals to a peer.
<b>Hold Timer</b>	When availability to a peer is lost, this value specifies how long to wait before dropping the session.
<b>Soft Reconfiguration</b>	Select <b>Yes</b> to prevent the appliance from sending a route-refresh message to the BGP peer when a policy is changed. If you select <b>Don't apply</b> , Orchestrator ignores this field when applying this template to appliances.  When enabled, the appliance applies policy changes against BGP peer learned routes stored in memory. To request a route update from the peer, click the <b>Soft Reset</b> button for the peer on the BGP tab.
<b>Enable MD5 Password</b>	If applied, adds a password to authenticate TCP sessions with peers.
<b>Password / Confirm Password</b>	If the MD5 password is enabled, use these fields to specify the password.

3. Click **Update**.

## BFD Template

Use the BFD template to apply BFD configurations per segment to all appliances in the SD-WAN fabric, as follows:

1. Click the edit icon next to the segment for which you want to modify the configuration.
2. Complete the following fields:

Field	Description
<b>Min Tx Interval</b>	Minimum transmit interval in milliseconds (ms). Specify a value from 300 to 5000. The default setting is 300.
<b>Min Rx Interval</b>	Minimum receive interval in milliseconds (ms). Specify a value from 300 to 5000. The default setting is 300.
<b>Detection Multiplier</b>	Detection time multiplier. In BFD, the detection time is the transmit interval multiplied by the detection multiplier. If BFD data is not received within the detection time, a failure occurs. Specify a value from 3 to 10. The default setting is 3.

3. Click **Update**.

## OSPF Template

Use the OSPF template to apply OSPF configurations per segment to all appliances in the SD-WAN fabric.

1. Click the edit icon next to the segment for which you want to modify the configuration.

2. Configure the following elements as needed:

Field	Description
<b>Enable OSPF</b>	indicates whether the segment can access OSPF protocol. If you select <b>Don't apply</b> , Orchestrator ignores this field when applying this template to appliances.
<b>Route Map name to Redistribute routes to OSPF</b>	Name of the route map being redistributed to the SD-WAN. The OSPF template is used in conjunction with the Route Redistribution Maps template. OSPF route maps are configured in the Route Redistribution Maps template, and then applied in the OSPF template. The default OSPF route map name is "default_rtmap_to_ospf". <b>NOTE</b> Leave this field blank to preserve the current setting on the appliance.
<b>Admin Status</b>	Indicates whether the interface admin status is up or down. If you select <b>Don't apply</b> , Orchestrator ignores this field when applying this template to appliances.
<b>Hello Interval</b>	Length of time (in seconds) that must transpire between hello packets that a router sends on an OSPF interface.
<b>Dead Interval</b>	Length of time (in seconds) that must transpire before neighbors that have not detected a router's hello packets can declare the OSPF router down.
<b>Transmit Delay</b>	Length of time (in seconds) that must transpire before transmitting a link state update packet. Specify a value from 1 to 65535.
<b>Retransmit Interval</b>	Length of time (in seconds) that a router that has received no acknowledgment must wait before resending transmissions.
<b>Authentication Type</b>	Type of authentication to use for requests. Select one of the following drop-down list options: <ul style="list-style-type: none"> <li>• <b>Don't apply</b> – Orchestrator ignores this field when applying this template to appliances.</li> <li>• <b>None</b> – Authentication not performed.</li> <li>• <b>Text</b> – Simple password authentication, which allows a key (password) to be configured per area.</li> <li>• <b>MD5</b> – Message Digest cryptographic authentication. A key ID and key (password) are configured on each router. The router uses an algorithm based on the OSPF packet, the key ID, and the key to generate a message digest that gets appended to the packet.</li> </ul>
<b>Authentication Key</b>	Key (password) to use for authentication of requests. This field is available only if Authentication Type is set to Text.
<b>MD5 Key</b>	Key ID to use for MD5 authentication of requests. This field is available only if Authentication Type is set to MD5.
<b>MD5 Password / MD5 Confirm Password</b>	Password for the MD5 key. These fields are available only if Authentication Type is set to MD5. Specify and confirm the password.

3. Click **Update**.

## Admin Distance Template

This table shows values associated with various types of **Admin Distance**. Admin Distance (AD) is the route preference value assigned to dynamic routes, static routes, and directly connected routes. When the appliance's Routes table has multiple routes to the same destination, the appliance uses the route with the lowest administrative distance.

Field	Description
<b>Local</b>	Manually configured route, or one learned from locally-connected subnets.
<b>Subnet Shared - Static Routes</b>	Route learned from an EdgeConnect peer.
<b>Subnet Shared - BGP Remote</b>	Route shared from an EdgeConnect peer in an external network.
<b>Subnet Shared - OSPF Remote</b>	Route shared from an EdgeConnect peer within the same network.
<b>BGP Branch (pre-8.1.9.4)</b>	Type of dynamic route learned from a local BGP branch peer before version 8.1.9.4.
<b>BGP Transit (pre-8.1.9.4)</b>	Type of dynamic route learned from a local BGP branch-transit peer before version 8.1.9.4.
<b>EBGP (post-8.1.9.4)</b>	External BGP: exchanging routing information with a router outside the company-wide network after version 8.1.9.4.
<b>BGP PE (pre-8.1.9.4)</b>	Type of dynamic route learned from a local BGP PE (Provider Edge) router before version 8.1.9.4.
<b>OSPF</b>	Route learned from an OSPF (Open Shortest Path First) neighbor.
<b>IBGP (post-8.1.9.4)</b>	Internal BGP: exchanging routing information with a router inside the company-wide network after version 8.1.9.4.

## Route Policies Template

If you have deployed an SD-WAN network by using Business Intent Overlays (BIO), Orchestrator uses BIOs to automatically create the necessary Route Policies.

If you are creating a conventional WAN optimization network, there might be occasions when you need to directly configure Route Policies. Then, the following applies.

**Only use the Route Policy template to create (and apply) rules for flows that are to be:**

- Sent pass-through (shaped or unshaped)
- Dropped
- Configured for a specific high-availability deployment
- Routed based on application, ports, VLAN, DSCP, or ACL (Access Control List)

You might also want to create a Route Policy entry when multiple tunnels exist to the remote **peer**, and you want the appliance to dynamically select the best path based on one of these criteria:

- Load balancing
- Lowest loss
- Lowest latency
- A preferred interface
- A specific tunnel

Priority	Match Criteria	Destination	Path	Fallback	Comment
1000	Protocol ip, DSCP ef	auto optimized	low-latency	pass-through	<span style="color: red;">X</span>
1010	Protocol ip, Application datadomain	auto optimized	load balance	pass-through	<span style="color: red;">X</span>
1020	Protocol ip, Dest IP/Subnet 10.10.11.56/32	auto optimized	low-loss	pass-through	<span style="color: red;">X</span>
1030	Protocol ip	auto optimized	load balance	pass-through	<span style="color: red;">X</span>

## Why?

Each appliance's default routing behavior is to auto-optimize all IP traffic, automatically directing flows to the appropriate tunnel. **Auto-optimization** strategies reduce the need to create explicit route map entries for optimization. The three strategies provided are **TCP-based** auto-opt, **IP-based** auto-opt, and **subnet sharing**. By default, all three are enabled on the **System** template.

## Priority

- With this template, you can create rules with a priority from **1000 - 9999**. When the template is applied to an appliance, Orchestrator will delete all rules having a priority in that range before applying its policies.
- If you access an appliance directly, you can create rules with higher priority than Orchestrator rules (**1 - 999**) and rules with lower priority (**10000 - 19999** and **25000 - 65534**).

**NOTE** The priority range from **20000** to **24999** is reserved for Orchestrator.

- When adding a rule, the priority is incremented by ten from the previous rule. The priority can be changed, but this default behavior helps to ensure you can insert new rules without having to change subsequent priorities.

## Match Criteria

- These are universal across all policy maps—**Route**, **QoS**, **Optimization**, **NAT** (Network Address Translation), and **Security**.
- If you expect to use the same match criteria in different maps, you can create an **ACL** (Access Control List), which is a named, reusable set of rules. For efficiency, create them in **Configuration > Templates & Policies > ACLs > Access Lists**, and apply them across appliances.
- The available parameters are **Application**, **Address Map** (for sorting by country, IP address owner, or SaaS application), **Domain**, **Geo Location**, **Interface**, **Protocol**, **DSCP**, **IP/Subnet**, **Port**, **Traffic Behavior Overlay**, **Fabric or Internet**, and **User Role** (the User Role as specified in the authentication exchange with the ClearPass RADIUS server).

**NOTE** User Role options include the RADIUS User Role, User Name, User Group, User Device, or User MAC. Configuring User Role match criteria enables an EdgeConnect to automatically assign traffic steering and firewall zone policies.

**NOTE** Additional attributes under the Address Map parameter can be used as match criteria. These attributes are secondary parameters to the address map, so the attributes are evaluated for a policy match only when the configured address map parameter matches the flow. To configure these attributes, click **+Attributes**.

- To specify different criteria for inbound versus outbound traffic, select the **Source:Dest** check box.

**NOTE** Source and destination role-based policies can be configured when both source and destination users are in the same network.

## Source or Destination

- An IP address can specify a subnet; for example, 10.10.10.0/24 (IPv4) or fe80::204:23ff:fed8:4ba2/64 (IPv6).
- To allow **any IP address**, use 0.0.0.0/0 (IPv4) or ::/0 (IPv6).
- Ports are available only for the protocols **tcp**, **udp**, and **tcp/udp**.
- To allow **any port**, use 0.

## Wildcard-based Prefix Matching Rules

- Even when using a range or a wildcard, the IPv4 address must be specified in the 4-octet format, separated by the dot notation. For example, A.B.C.D.
- Range is specified using a single dash. For example, 128-129.
- Wildcard is specified as an asterisk (\*).
- Range and Wildcard can both be used in the same address, but an octet can only contain one or the other. For example, 10.136-137.\*.64-95.
- A wildcard can only be used to define an entire octet. For example, 10.13\*.\*.64-95 is not supported. Use 10.130-139.\*.64-95 to specify this range.

- The same rules apply to IPv6 addressing.
- CIDR notation and (Range or Wildcard) are mutually exclusive in the same address. For example, **192.168.0.1-127/24** is not supported. Use either **192.168.0.0/24** or **192.168.0.1-127**.
- These prefix-matching rules apply to the following policies only: Route, QoS, Optimization, NAT, Security, and ACLs.

## Set Actions Fields

The Route Policy template's SET actions determine where to direct traffic and what the fallback is when a tunnel is down.

### Where the Appliance Directs Traffic

- In the **Destination** field, you specify how to characterize the flow. The options are a specific overlay, **auto-optimized**, **pass-through [shaped]**, **pass-through-unshaped**, or **dropped**.
- When **auto-optimized**, a flow is directed to the appropriate tunnel. If you choose, you can specify that the appliance use metrics to dynamically select the best path based on one of these criteria:
  - Load balancing
  - Lowest loss
  - Lowest latency
- When configuring the Route Policy for an **individual** appliance when multiple tunnels exist to the remote **peer**, you can also select the path based on a preferred interface or a specific tunnel. For further information, see the [Appliance Manager Operator's Guide](#).

### How Traffic Is Managed If a Tunnel Is Down

- The **Fallback** can be **pass-through [shaped]**, **pass-through-unshaped**, or **dropped**.
- When configuring the Route Policy for an **individual** appliance, the **continue** option is available if a specific tunnel is named in the **Destination** column. That option enables the appliance to read subsequent entries in the individual Route Policy in the event that the tunnel used in a previous entry goes down. For further information, see the [Appliance Manager Operator's Guide](#).

## QoS Policies Template

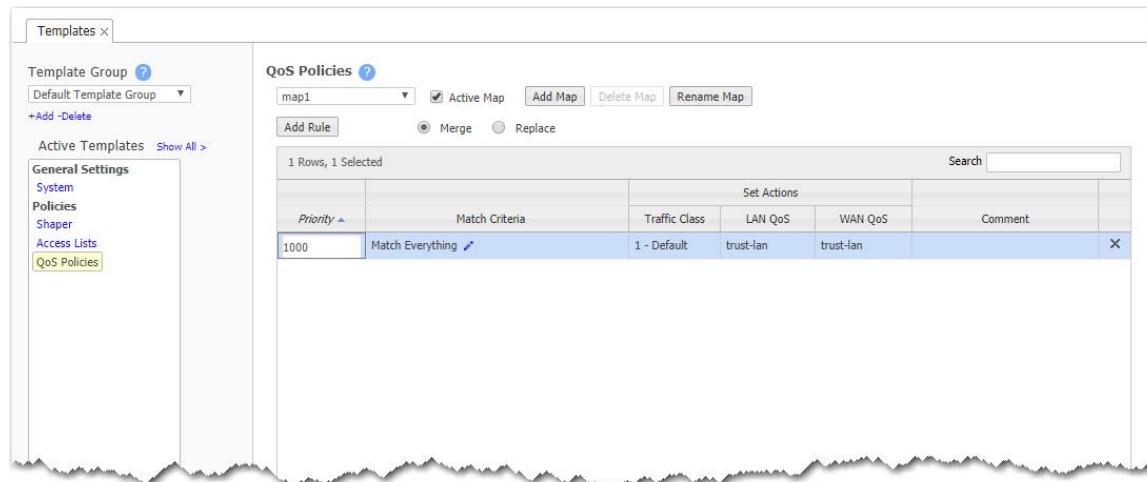
**QoS Policy** determines how flows are queued and marked.

The QoS Policy's SET actions determine two things:

- What traffic class a shaped flow—whether optimized or pass-through—is assigned
- Whether to trust incoming DSCP markings for LAN QoS and WAN QoS, or to remark them as they leave for the WAN

Use the **Shaper** to define, prioritize, and name traffic classes.

Think of it as the Shaper **defines** and the QoS Policy **assigns**.



## Priority

- With this template, you can create rules with a priority from **1000 - 9999**. When the template is applied to an appliance, Orchestrator will delete all rules having a priority in that range before applying its policies.
- If you access an appliance directly, you can create rules with higher priority than Orchestrator rules (**1 - 999**) and rules with lower priority (**10000 - 19999** and **25000 - 65534**).

**NOTE** The priority range from **20000** to **24999** is reserved for Orchestrator.

- When adding a rule, the priority is incremented by ten from the previous rule. The priority can be changed, but this default behavior helps to ensure you can insert new rules without having to change subsequent priorities.

## Match Criteria

- These are universal across all policy maps—**Route**, **QoS**, **Optimization**, **NAT** (Network Address Translation), and **Security**.
- If you expect to use the same match criteria in different maps, you can create an **ACL** (Access Control List), which is a named, reusable set of rules. For efficiency, create them in **Configuration > Templates & Policies > ACLs > Access Lists**, and apply them across appliances.
- The available parameters are **Application**, **Address Map** (for sorting by country, IP address owner, or SaaS application), **Domain**, **Geo Location**, **Interface**, **Protocol**, **DSCP**, **IP/Subnet**, **Port**, **Traffic Behavior Overlay**, **Fabric or Internet**, and **User Role** (the User Role as specified in the authentication exchange with the ClearPass RADIUS server).

**NOTE** User Role options include the RADIUS User Role, User Name, User Group, User Device, or User MAC. Configuring User Role match criteria enables an EdgeConnect to automatically assign traffic steering and firewall zone policies.

**NOTE** Additional attributes under the Address Map parameter can be used as match criteria. These attributes are secondary parameters to the address map, so the attributes are evaluated for a policy match only when the configured address map parameter matches the flow. To configure these attributes, click **+Attributes**.

- To specify different criteria for inbound versus outbound traffic, select the **Source:Dest** check box.

**NOTE** Source and destination role-based policies can be configured when both source and destination users are in the same network.

## Source or Destination

- An IP address can specify a subnet; for example, 10.10.10.0/24 (IPv4) or fe80::204:23ff:fed8:4ba2/64 (IPv6).
- To allow **any IP address**, use 0.0.0.0/0 (IPv4) or ::/0 (IPv6).
- Ports are available only for the protocols **tcp**, **udp**, and **tcp/udp**.
- To allow **any port**, use 0.

## Wildcard-based Prefix Matching Rules

- Even when using a range or a wildcard, the IPv4 address must be specified in the 4-octet format, separated by the dot notation. For example, A.B.C.D.
- Range is specified using a single dash. For example, 128-129.
- Wildcard is specified as an asterisk (\*).
- Range and Wildcard can both be used in the same address, but an octet can only contain one or the other. For example, 10.136-137.\*.64-95.
- A wildcard can only be used to define an entire octet. For example, 10.13\*.\*.64-95 is not supported. Use 10.130-139.\*.64-95 to specify this range.
- The same rules apply to IPv6 addressing.
- CIDR notation and (Range or Wildcard) are mutually exclusive in the same address. For example, 192.168.0.1-127/24 is not supported. Use either 192.168.0.0/24 or 192.168.0.1-127.
- These prefix-matching rules apply to the following policies only: Route, QoS, Optimization, NAT, Security, and ACLs.

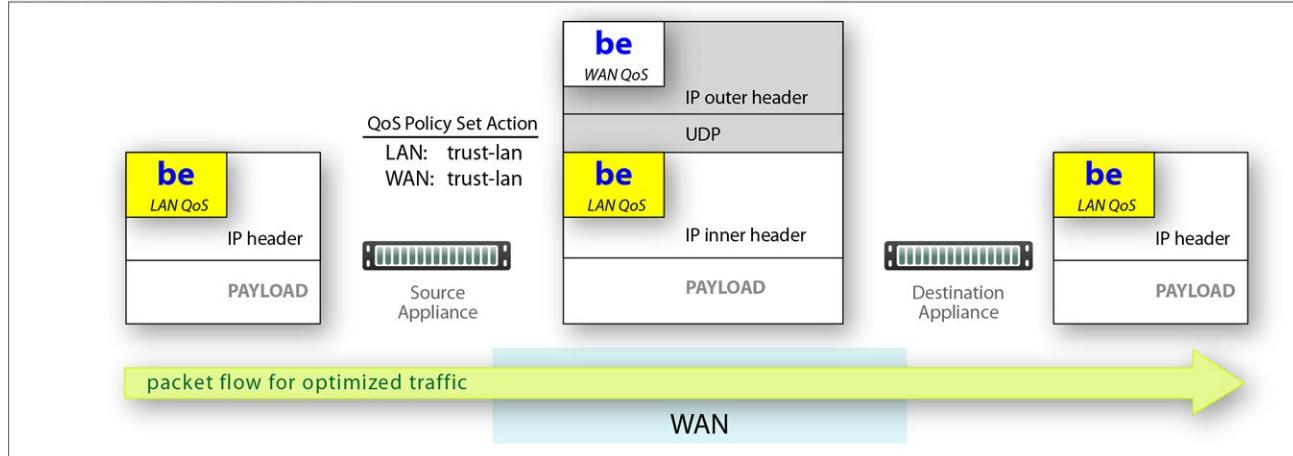
## Handle and Mark DSCP Packets

- DSCP markings specify end-to-end QoS policies throughout a network.
- The default values for **LAN QoS** and **WAN QoS** are **trust-lan**.

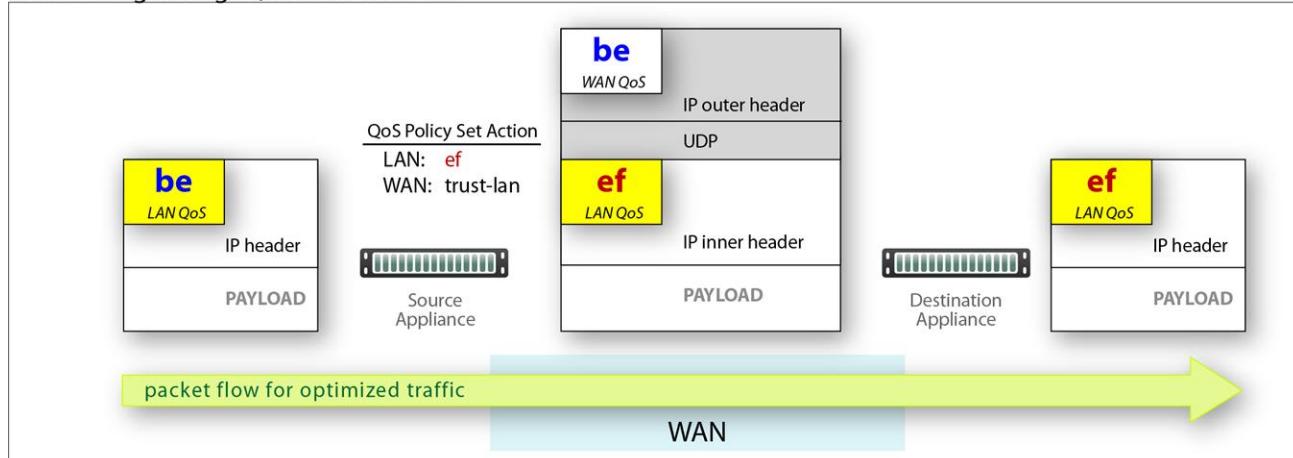
## Apply DSCP Markings to Optimized (Tunnelized) Traffic

- The appliance encapsulates optimized traffic. This adds an IP outer header to packets for travel across the WAN. This outer header contains the **WAN QoS** DSCP marking.
- LAN QoS** - The DSCP marking applied to the IP header before encapsulation.
- WAN QoS** - The DSCP marking in the encapsulating outer IP header. The remote appliance removes the outer IP header.

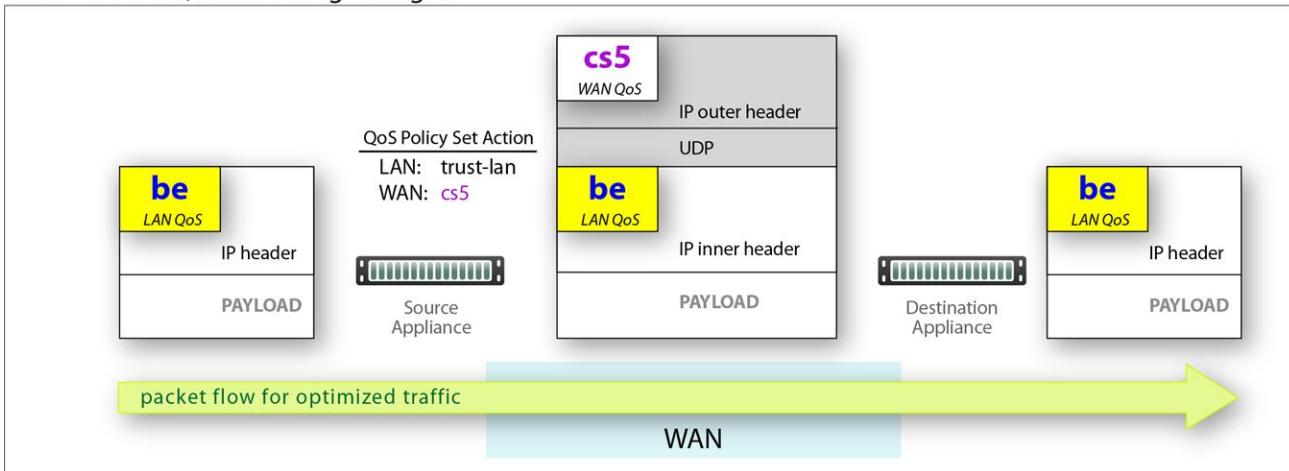
LAN and WAN set to trust-lan



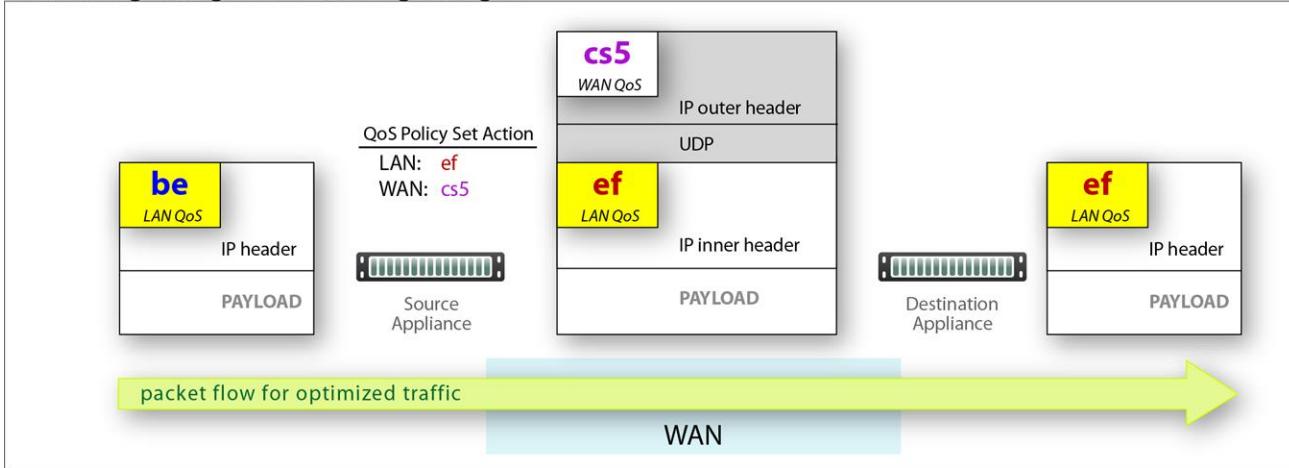
LAN setting changed, WAN is trust-lan



### LAN is trust-lan, WAN setting changed



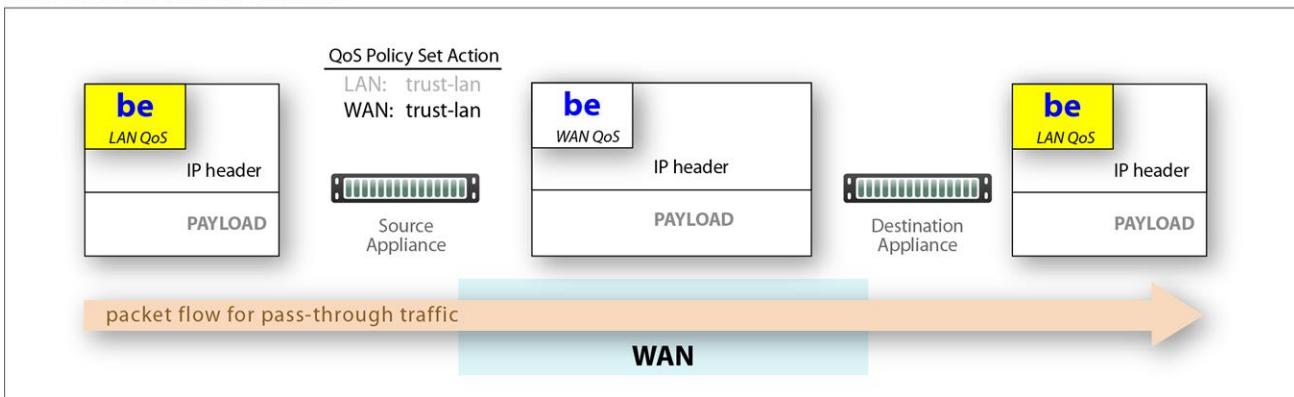
### LAN setting changed, WAN setting changed



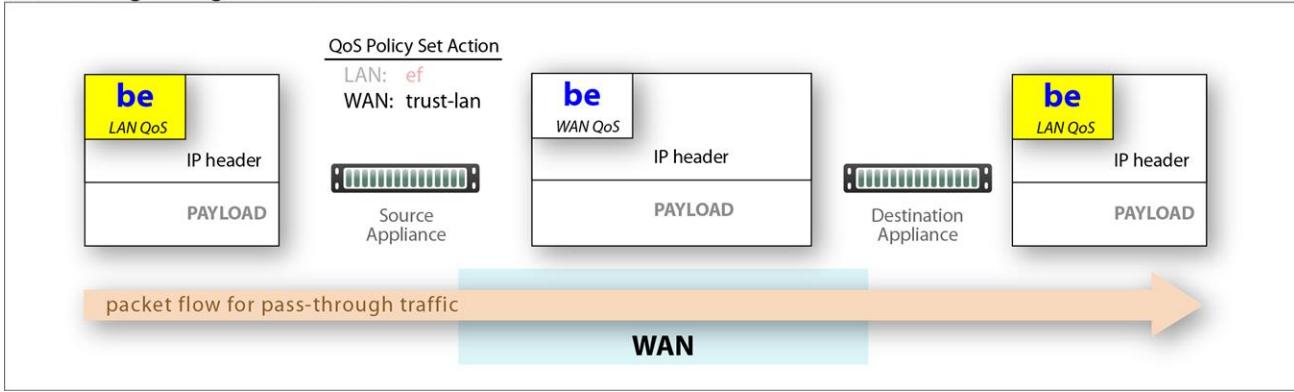
### Apply DSCP Markings to Pass-through Traffic

- The appliance applies the QoS Policy's DSCP markings to all pass-through flows—shaped and unshaped.
- Pass-through traffic does not receive an additional header, so it is handled differently:
  - The Optimization Policy's **LAN QoS** Set Action is ignored.
  - The specified **WAN QoS** marking replaces the packet's existing **LAN QoS** DSCP marking.
  - When the packet reaches the remote appliance, it retains the modified QoS setting as it travels to its destination.

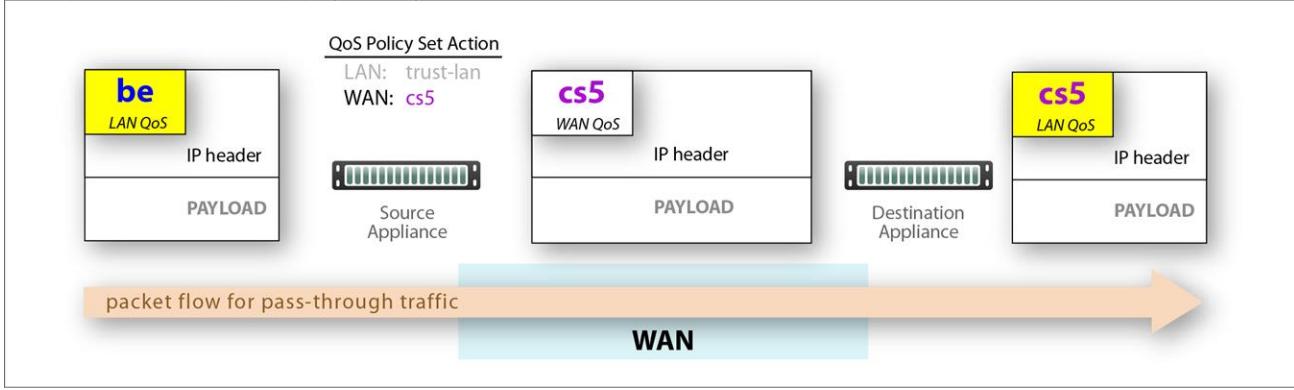
### LAN and WAN set to trust-lan



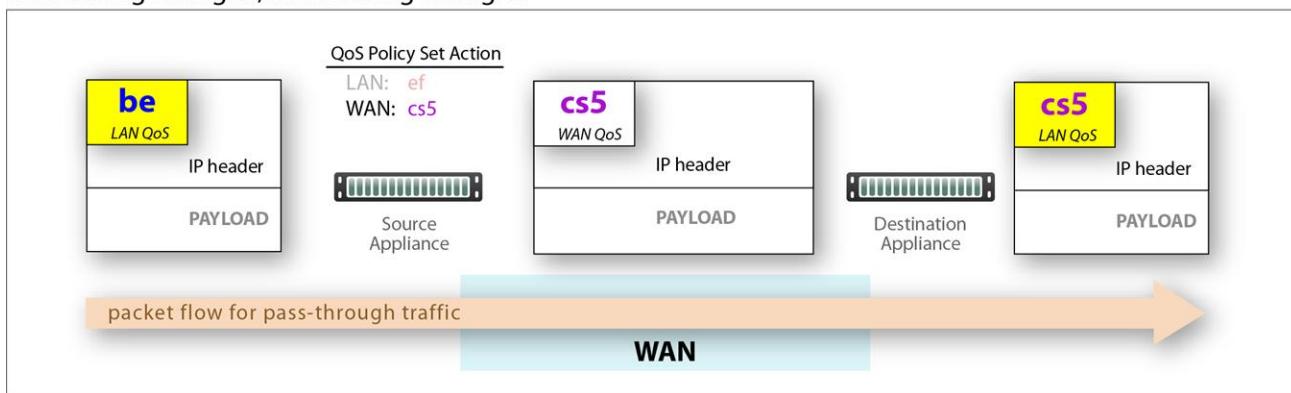
### LAN setting changed, WAN is trust-lan



### LAN is trust-lan, WAN setting changed

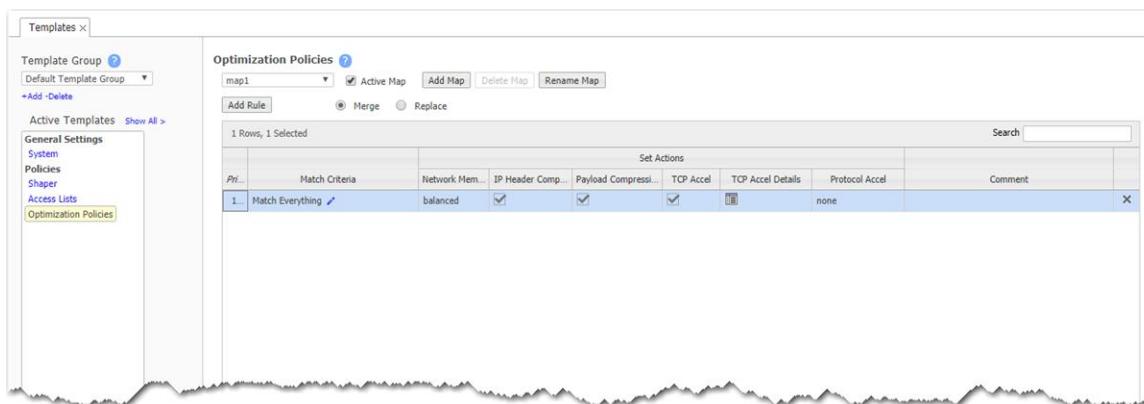


## LAN setting changed, WAN setting changed



## Optimization Policies Template

Optimization templates apply Optimization policies to appliances.



### Priority

- With this template, you can create rules with a priority from **1000 - 9999**. When the template is applied to an appliance, Orchestrator will delete all rules having a priority in that range before applying its policies.
- If you access an appliance directly, you can create rules with higher priority than Orchestrator rules (**1 - 999**) and rules with lower priority (**10000 - 19999** and **25000 - 65534**).

**NOTE** The priority range from **20000** to **24999** is reserved for Orchestrator.

- When adding a rule, the priority is incremented by ten from the previous rule. The priority can be changed, but this default behavior helps to ensure you can insert new rules without having to change subsequent priorities.

## Match Criteria

- These are universal across all policy maps—**Route**, **QoS**, **Optimization**, **NAT** (Network Address Translation), and **Security**.
- If you expect to use the same match criteria in different maps, you can create an **ACL** (Access Control List), which is a named, reusable set of rules. For efficiency, create them in **Configuration > Templates & Policies > ACLs > Access Lists**, and apply them across appliances.
- The available parameters are **Application**, **Address Map** (for sorting by country, IP address owner, or SaaS application), **Domain**, **Geo Location**, **Interface**, **Protocol**, **DSCP**, **IP/Subnet**, **Port**, **Traffic Behavior Overlay**, **Fabric or Internet**, and **User Role** (the User Role as specified in the authentication exchange with the ClearPass RADIUS server).

**NOTE** User Role options include the RADIUS User Role, User Name, User Group, User Device, or User MAC. Configuring User Role match criteria enables an EdgeConnect to automatically assign traffic steering and firewall zone policies.

**NOTE** Additional attributes under the Address Map parameter can be used as match criteria. These attributes are secondary parameters to the address map, so the attributes are evaluated for a policy match only when the configured address map parameter matches the flow. To configure these attributes, click **+Attributes**.

- To specify different criteria for inbound versus outbound traffic, select the **Source:Dest** check box.

**NOTE** Source and destination role-based policies can be configured when both source and destination users are in the same network.

## Source or Destination

- An IP address can specify a subnet; for example, 10.10.10.0/24 (IPv4) or fe80::204:23ff:fed8:4ba2/64 (IPv6).
- To allow **any IP address**, use 0.0.0.0/0 (IPv4) or ::/0 (IPv6).
- Ports are available only for the protocols **tcp**, **udp**, and **tcp/udp**.
- To allow **any port**, use 0.

## Wildcard-based Prefix Matching Rules

- Even when using a range or a wildcard, the IPv4 address must be specified in the 4-octet format, separated by the dot notation. For example, A.B.C.D.
- Range is specified using a single dash. For example, 128-129.
- Wildcard is specified as an asterisk (\*).
- Range and Wildcard can both be used in the same address, but an octet can only contain one or the other. For example, 10.136-137.\*.64-95.
- A wildcard can only be used to define an entire octet. For example, 10.13\*.\*.64-95 is not supported. Use 10.130-139.\*.64-95 to specify this range.

- The same rules apply to IPv6 addressing.
- CIDR notation and (Range or Wildcard) are mutually exclusive in the same address. For example, **192.168.0.1-127/24** is not supported. Use either **192.168.0.0/24** or **192.168.0.1-127**.
- These prefix-matching rules apply to the following policies only: Route, QoS, Optimization, NAT, Security, and ACLs.

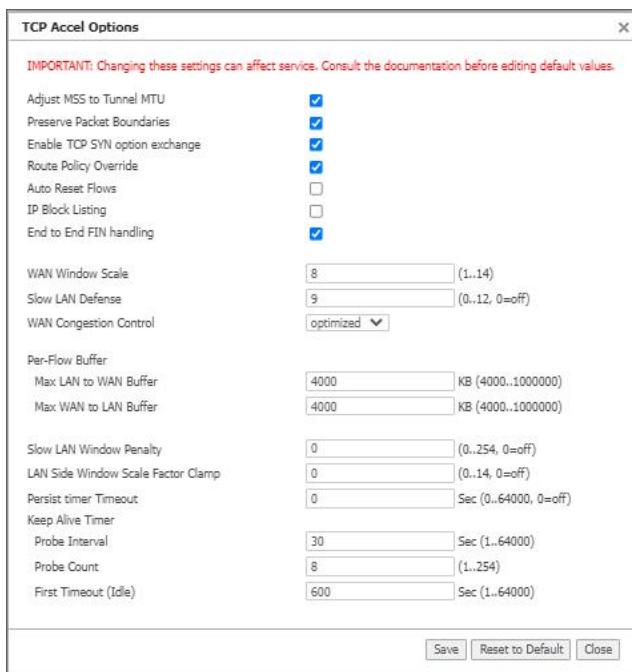
## Set Actions Fields

Set Action	Description
<b>Network Memory</b>	<p>Addresses limited bandwidth. This technology uses advanced fingerprinting algorithms to examine all incoming and outgoing WAN traffic. Network Memory localizes information and transmits only modifications between locations.</p> <ul style="list-style-type: none"> <li>• <b>Maximize Reduction</b> – Optimizes for maximum data reduction at the potential cost of slightly lower throughput and/or some increase in latency. It is appropriate for bulk data transfers such as file transfers and FTP, where bandwidth savings are the primary concern.</li> <li>• <b>Minimize Latency</b> – Ensures that Network Memory processing adds no latency. This might come at the cost of lower data reduction. It is appropriate for extremely latency-sensitive interactive or transactional traffic. It is also appropriate when the primary objective is to fully utilize the WAN pipe to increase the LAN-side throughput, as opposed to conserving WAN bandwidth.</li> <li>• <b>Balanced</b> – Is the default setting. It dynamically balances latency and data reduction objectives and is the best choice for most traffic types.</li> <li>• <b>Disabled</b> – Turns off Network Memory.</li> </ul>
<b>IP Header Compression</b>	<p>Process of compressing excess protocol headers before transmitting them on a link and uncompressing them to their original state at the other end. It is possible to compress the protocol headers due to the redundancy in header fields of the same packet, as well as in consecutive packets of a packet stream.</p>
<b>Payload Compression</b>	<p>Uses algorithms to identify relatively short byte sequences that are repeated frequently. These are then replaced with shorter segments of code to reduce the size of transmitted data. Simple algorithms can find repeated bytes within a single packet; more sophisticated algorithms can find duplication across packets and even across flows.</p>
<b>TCP Acceleration</b>	<p>Uses techniques such as selective acknowledgments, window scaling, and maximum segment size adjustment to mitigate poor performance on high-latency links.</p> <p>Slow LAN alert goes off when the loss has fallen below 80% of the specified value configured in the <b>TCP Accel Options</b> window.</p> <p>For more information, see <a href="#">TCP Acceleration Options</a>.</p>
<b>Protocol Acceleration</b>	<p>Provides explicit configuration for optimizing CIFS, SSL, SRDF, Citrix, and iSCSI protocols. In a network environment, it is possible that not every appliance has the same optimization configurations enabled. Therefore, the site that initiates the flow (the <b>client</b>) determines the state of the protocol-specific optimization.</p>

## TCP Acceleration Options

TCP acceleration uses techniques such as selective acknowledgment, window scaling, and message segment size adjustment to compensate for poor performance on high latency links.

This feature has a set of advanced options with default values.



**CAUTION** Because changing these settings can affect service, it is recommended that you **do not modify** these without direction from Support.

Option	Description
<b>Adjust MSS to Tunnel MTU</b>	Limits the TCP MSS (Maximum Segment Size) advertised by the end hosts in the SYN segment to a value derived from the Tunnel MTU (Maximum Transmission Unit). This is <i>TCP MSS = Tunnel MTU - Tunnel Packet Overhead</i> . This feature is enabled by default so that the <b>maximum value</b> of the end host MSS is always coupled to the Tunnel MSS. If the end host MSS is smaller than the tunnel MSS, the end host MSS is used instead. A use case for disabling this feature is when the end host uses Jumbo frames.

Option	Description
<b>Auto Reset Flows</b>	<p><b>NOTE</b> Whether this feature is enabled or not, the default behavior when a tunnel goes Down is to automatically reset the flows.</p> <p>If enabled, it resets all TCP flows that are not accelerated, but should be (based on policy and on internal criteria like a Tunnel Up event).</p> <p>The internal criteria can also include:</p> <ul style="list-style-type: none"> <li>• Resetting all TCP accelerated flows on a Tunnel Down event.</li> <li>• Resetting <ul style="list-style-type: none"> <li>• TCP acceleration is enabled.</li> <li>• SYN packet was not seen (so this flow was either part of WCCP redirection or it already existed when the appliance was inserted in the data path).</li> </ul> </li> </ul>
<b>Enable TCP SYN option exchange</b>	<p>Controls whether or not the proprietary TCP SYN option is forwarded on the LAN side. Enabled by default, this feature detects if there are more than two EdgeConnect appliances in the flow's data path and optimizes accordingly.</p> <p>Disable this feature if there is a LAN-side firewall or a third-party appliance that would drop a SYN packet when it encounters an unfamiliar TCP option.</p>
<b>End to End FIN Handling</b>	<p>This feature helps to fine tune TCP behavior during a connection's graceful shutdown event. When this feature is <b>ON</b> (Default), TCP on the local appliance synchronizes this graceful shutdown of the local LAN side with the LAN side of the remote appliance. When this feature is <b>OFF</b> (Default TCP), no such synchronization happens and the two LAN segments at the ends gracefully shut down, independently.</p>
<b>IP Block Listing</b>	<p>If selected, and if the appliance does not receive a TCP SYN-ACK from the remote end within five seconds, the flow proceeds without acceleration and the destination IP address is blocked for one minute.</p>
<b>Keep Alive Timer</b>	<p>Allows changing the Keep Alive timer for the TCP connections.</p> <ul style="list-style-type: none"> <li>• <b>Probe Interval</b> - Time interval in seconds between two consecutive Keep Alive probes.</li> <li>• <b>Probe Count</b> - Maximum number of Keep Alive probes to send.</li> <li>• <b>First Timeout (Idle)</b> - Time interval until the first Keep Alive timeout.</li> </ul>
<b>LAN Side Window Scale Factor Clamp</b>	<p>This setting allows the appliance to present an artificially lowered Window Scale Factor (WSF) to the end host. This reduces the need for memory in scenarios in which there are many out-of-order packets being received from the LAN side. These out-of-order packets cause much buffer utilization and maintenance.</p>
<b>Per-Flow Buffer</b>	<p><b>(Max LAN to WAN Buffer and Max WAN to LAN Buffer)</b></p> <p>This setting clamps the maximum buffer space that can be allocated to a flow, in each direction.</p>
<b>Persist timer Timeout</b>	<p>Allows the TCP to terminate connections that are in Persist timeout stage after the configured number of seconds.</p>

Option	Description
<b>Preserve Packet Boundaries</b>	<p>Preserves the packet boundaries end-to-end. If this feature is disabled, the appliances in the path can coalesce consecutive packets of a flow to use bandwidth more efficiently.</p> <p>It is enabled by default so that applications requiring packet boundaries to match do not fail.</p>
<b>Route Policy Override</b>	<p>Tries to override asymmetric route policy settings. It emulates auto-opt behavior by using the same tunnel for the returning SYN+ACK as it did for the original SYN packet.</p> <p>Disable this feature if the asymmetric route policy setting is necessary to correctly route packets. In this case, you might need to configure flow redirection to ensure optimization of TCP flows.</p>
<b>Slow LAN Defense</b>	<p>Resets all flows that consume a disproportionate amount of buffer and have a very slow throughput on the LAN side. Owing to a few slower end hosts or a lossy LAN, these flows affect the performance of all other flows so that no flows see the customary throughput improvement gained through TCP acceleration.</p> <p>This feature is enabled by default. The number relates indirectly to the amount of time the system waits before resetting such slow flows.</p>
<b>Slow LAN Window Penalty</b>	<p>This setting (<b>OFF</b> by default) penalizes flows that are slow to send data on the LAN side by artificially reducing their TCP receive window. This causes less data to be received and helps to reach a balance with the data sending rate on the LAN side.</p>
<b>WAN Congestion Control</b>	<p>Selects the internal Congestion Control parameter:</p> <ul style="list-style-type: none"> <li>• <b>Optimized</b> - This is the default setting. This mode offers optimized performance in almost all scenarios.</li> <li>• <b>Standard</b> - In some unique cases, it might be necessary to downgrade to Standard performance to better interoperate with other flows on the WAN link.</li> <li>• <b>Aggressive</b> - Provides aggressive performance and should be used with caution. Recommended mostly for Data Replication scenarios.</li> </ul>
<b>WAN Window Scale</b>	<p>This is the WAN-side TCP Window scale factor that is used internally for WAN-side traffic. This is independent of the WAN-side factor advertised by the end hosts.</p>

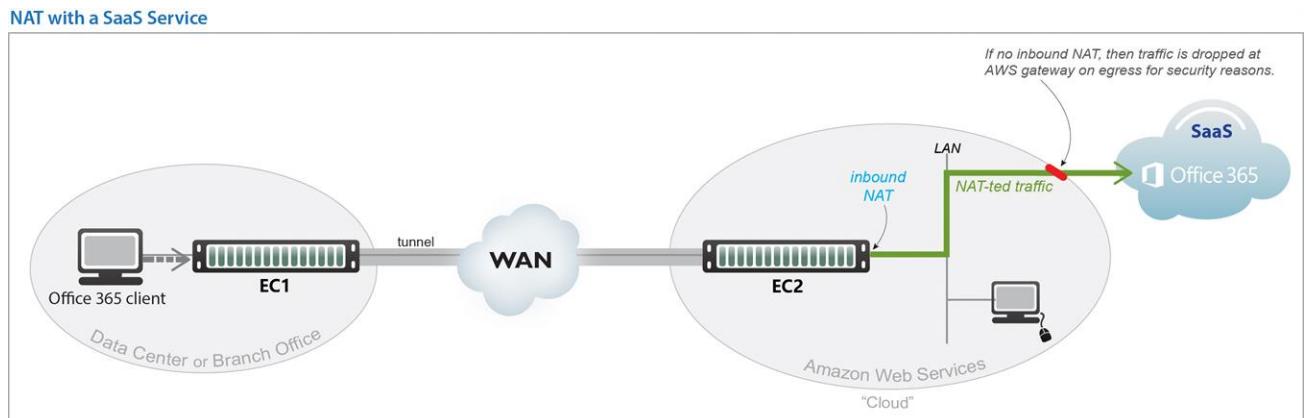
## SaaS NAT Policies Template

Use this template to add NAT map rules to all the appliances that support **Network Address Translation**.

## When to NAT

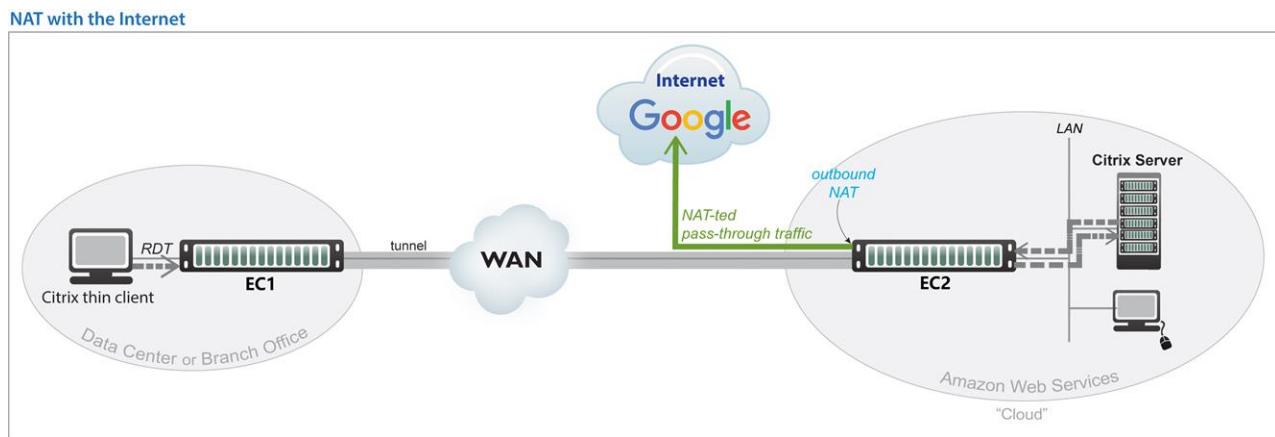
Two use cases illustrate the need for NAT:

1. **Inbound NAT.** The appliance automatically creates a source NAT (Network Address Translation) map when retrieving subnet information from the Cloud Portal. This ensures that traffic destined to SaaS servers has a return path to the appliance from which that traffic originated.



2. **Outbound NAT.** The appliance and server are in the cloud, and the server accesses the internet. As in the example below, a Citrix thin client accesses its cloud-based server, and the server accesses

the internet.



For deployments in the cloud, **best practice is to NAT all traffic**—either inbound (WAN-to-LAN) or outbound (LAN-to-WAN), depending on the direction of initiating request. This avoids black-holing that can result from cloud-specific IP addressing requirements.

- Enabling **NAT all** applies NAT policies to pass-through traffic as well as optimized traffic, ensuring that black-holing does not occur. **NAT all** on outbound only applies pass-through traffic.
- If **Fallback** is enabled, the appliance moves to the next IP (if available) when ports are exhausted on the current NAT IP.

In general, when applying NAT policies, configure separate WAN and LAN interfaces to ensure that NAT works properly. You can do this by deploying the appliance in Router mode in-path with two (or four) interfaces.

## Advanced Settings

The appliance can perform **source network address translation** (Source NAT or SNAT) on inbound or outbound traffic.

There are two types of NAT policies:

- **Dynamic** - Created automatically by the system for inbound NAT when the **SaaS Optimization** feature is enabled and SaaS service(s) are selected for optimization. The appliance polls the Cloud Intelligence Service for a directory of SaaS services, and NAT policies are created for each of the subnets associated with selected SaaS service(s), ensuring that traffic destined for servers in use by those SaaS services has a return path to the appliance.
- **Manual** - Created by the administrator for specific IP addresses / ranges or subnets. When assigning priority numbers to individual policies within a NAT map, first view **dynamic policies** to ensure that the manual numbering scheme does not interfere with dynamic policy numbering (that is, the manually assigned priority numbers cannot be in the range: 4000-5000). The default (**no-NAT**) policy is numbered 65535.

The NAT policy map has the following criteria and **Set Actions**:

## Match Criteria

- These are universal across all policy maps—**Route**, **QoS**, **Optimization**, **NAT** (Network Address Translation), and **Security**.
- If you expect to use the same match criteria in different maps, you can create an **ACL** (Access Control List), which is a named, reusable set of rules. For efficiency, create them in **Configuration > Templates & Policies > ACLs > Access Lists**, and apply them across appliances.
- The available parameters are **Application**, **Address Map** (for sorting by country, IP address owner, or SaaS application), **Domain**, **Geo Location**, **Interface**, **Protocol**, **DSCP**, **IP/Subnet**, **Port**, **Traffic Behavior Overlay**, **Fabric or Internet**, and **User Role** (the User Role as specified in the authentication exchange with the ClearPass RADIUS server).

**NOTE** User Role options include the RADIUS User Role, User Name, User Group, User Device, or User MAC. Configuring User Role match criteria enables an EdgeConnect to automatically assign traffic steering and firewall zone policies.

**NOTE** Additional attributes under the Address Map parameter can be used as match criteria. These attributes are secondary parameters to the address map, so the attributes are evaluated for a policy match only when the configured address map parameter matches the flow. To configure these attributes, click **+Attributes**.

- To specify different criteria for inbound versus outbound traffic, select the **Source:Dest** check box.

**NOTE** Source and destination role-based policies can be configured when both source and destination users are in the same network.

## Source or Destination

- An IP address can specify a subnet; for example, 10.10.10.0/24 (IPv4) or fe80::204:23ff:fed8:4ba2/64 (IPv6).
- To allow **any IP address**, use 0.0.0.0/0 (IPv4) or ::/0 (IPv6).
- Ports are available only for the protocols **tcp**, **udp**, and **tcp/udp**.
- To allow **any port**, use 0.

## Wildcard-based Prefix Matching Rules

- Even when using a range or a wildcard, the IPv4 address must be specified in the 4-octet format, separated by the dot notation. For example, A.B.C.D.
- Range is specified using a single dash. For example, 128-129.
- Wildcard is specified as an asterisk (\*).
- Range and Wildcard can both be used in the same address, but an octet can only contain one or the other. For example, 10.136-137.\*.64-95.
- A wildcard can only be used to define an entire octet. For example, 10.13\*.\*.64-95 is not supported. Use 10.130-139.\*.64-95 to specify this range.
- The same rules apply to IPv6 addressing.

- CIDR notation and (Range or Wildcard) are mutually exclusive in the same address. For example, **192.168.0.1-127/24** is not supported. Use either **192.168.0.0/24** or **192.168.0.1-127**.
- These prefix-matching rules apply to the following policies only: Route, QoS, Optimization, NAT, Security, and ACLs.

## Set Actions

### NAT Type

Option	Description
<b>no-nat</b>	Is the <i>default</i> . No IP addresses are changed.
<b>source-nat</b>	Is the <i>default</i> . No IP addresses are changed.

### NAT Direction

Option	Description
<b>inbound</b>	NAT is on the LAN interface.
<b>outbound</b>	NAT is on the WAN interface.
<b>none</b>	Only option if the NAT type is <b>no-nat</b> .

### NAT IP

Option	Description
<b>auto</b>	Select if you want to NAT <b>all</b> traffic. The appliance then picks the first available NAT IP/Port.
<b>tunnel</b>	Select if you want to NAT <b>tunnel</b> traffic only. Applicable only for inbound NAT, as outbound does not support NAT on tunnel traffic.
<b>[IP address]</b>	Select if you want to make NAT use this IP address during address translation.

For **Fallback**, if the IP address is full, the appliance uses the next available IP address.

When you select a specific IP, ensure that the routing is in place for NAT-ed return traffic.

## Merge / Replace

At the top of the page, choose

**Merge** to use the values in the template, but keep any values set on the appliance as is (producing a mix of template and appliance rules),

-OR-

**Replace** (recommended) to replace all values with those in the template.

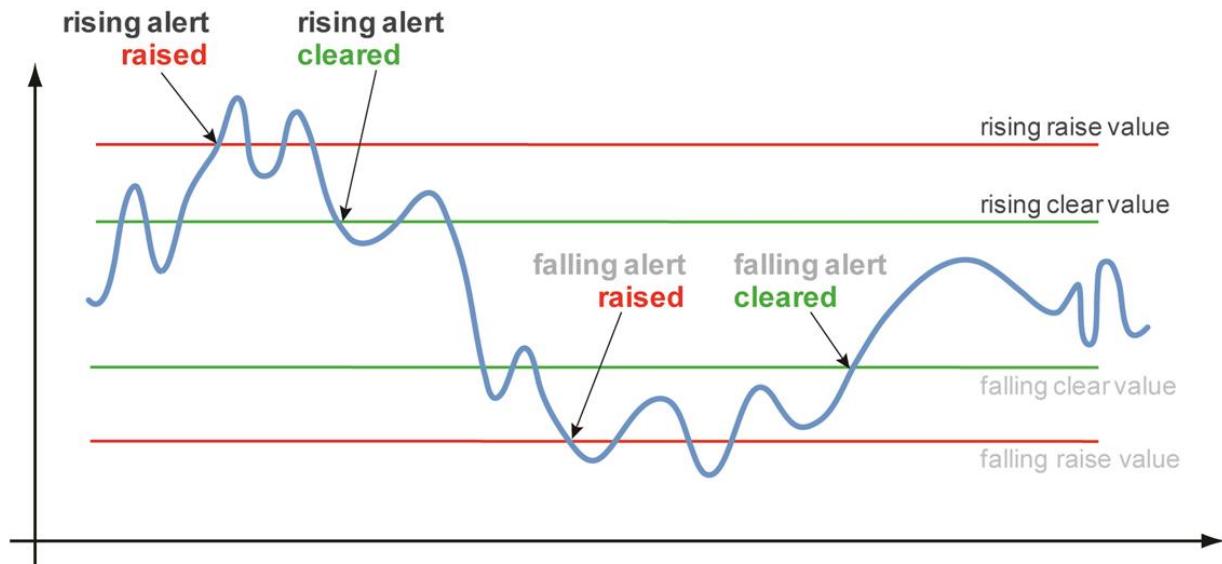
## Threshold Crossing Alerts Template

**Threshold Crossing Alerts (TCAs)** are preemptive, user-configurable alarms that are triggered when the specific thresholds are crossed.

The screenshot shows the 'Threshold Crossing Alerts' configuration page. On the left, there's a sidebar with 'Template Group' dropdown, '+Add -Delete' button, and a list of Active Templates: General Settings (System, Policies, Shaper), Access Lists (Access Lists, Threshold Crossing Alerts, highlighted in yellow), and Threshold Crossing Alerts. Below this is a 'Save' button, 'Save As' button, 'Cancel' button, and a note 'Applies to all templates in group'. At the bottom is an 'Apply Template Groups' button. The main area has a 'Search' input and a table titled 'Threshold Crossing Alerts' with 12 rows. The table has two sections: 'Rising' and 'Falling'. Each section has columns for Name, Raise, Clear, Times to Trigger, and Enabled. The table lists various network metrics with their respective threshold values and alert configurations.

Name	Rising				Falling			
	Raise	Clear	Times to Trigger	Enabled	Raise	Clear	Times to Trigger	Enabled
File-system utilization	90%	85%	5	<input checked="" type="checkbox"/>	75%	75%	5	<input type="checkbox"/>
LAN-side receive throughput	1000000 kbps	1000000 kbps	5	<input type="checkbox"/>	0 kbps	0 kbps	5	<input type="checkbox"/>
Total number of flows	90%	85%	5	<input checked="" type="checkbox"/>	0%	0%	5	<input type="checkbox"/>
Total number of optimized flows	90%	85%	5	<input type="checkbox"/>	0%	0%	5	<input type="checkbox"/>
Tunnel OOP post-POC	100%	100%	5	<input type="checkbox"/>	0%	0%	5	<input type="checkbox"/>
Tunnel OOP pre-POC	100%	100%	5	<input checked="" type="checkbox"/>	0%	0%	5	<input type="checkbox"/>
Tunnel latency	1000 ms	850 ms	5	<input checked="" type="checkbox"/>	0 ms	0 ms	5	<input type="checkbox"/>
Tunnel loss post-FEC	100%	100%	5	<input type="checkbox"/>	0%	0%	5	<input type="checkbox"/>
Tunnel loss pre-FEC	100%	100%	5	<input type="checkbox"/>	0%	0%	5	<input type="checkbox"/>
Tunnel reduction	100%	100%	5	<input type="checkbox"/>	0%	0%	5	<input type="checkbox"/>
Tunnel utilization	100%	100%	5	<input type="checkbox"/>	0%	0%	5	<input type="checkbox"/>
WAN-side transmit throughput	1000000 kbps	1000000 kbps	5	<input type="checkbox"/>	0 kbps	0 kbps	5	<input type="checkbox"/>

They alarm on both rising and falling threshold crossing events (that is, floor and ceiling levels). For both levels, one value raises the alarm while another value clears it.

**Rules:**

- High raise threshold is greater than high clear threshold
- Low raise threshold is less than low clear threshold

**ON by Default**

- **Appliance Capacity** - Triggers when an appliance reaches 95% of its total flow capacity. It is not configurable and can be cleared only by an operator.
- **File-system utilization** - Percent of non-Network Memory disk space filled by the appliance. This TCA cannot be disabled.
- **Tunnel latency** - Measured in milliseconds, the maximum latency of a one-second sample within a 60-second span.

**OFF by Default**

- **LAN-side receive throughput** - Based on a one-minute average, the LAN-side receive **TOTAL** for all interfaces.
- **WAN-side transmit throughput** - Based on a one-minute average, the WAN-side transmit **TOTAL** for all interfaces.
- **TCAs based on an end-of-minute count:**
  - Total number of flows
  - Total number of optimized flows

- **TCA based on a one-minute average:**

- Tunnel loss post-FEC
- Tunnel loss post-FEC
- Tunnel OOP post-POC
- Tunnel OOP post-POC
- Tunnel reduction
- Tunnel utilization (based on percent of configured maximum [system] bandwidth)

## TCA Metrics

**Times to Trigger** - A value of **1** triggers an alarm on the first threshold crossing instance. The default sampling granularity (or *rate* or *interval*) is one minute.

This table lists the **metrics** of each type of threshold crossing alert:

*Metrics for Threshold Crossing Alerts*

TCA Name	Unit	Metric
<b>Appliance Level</b>		
<b>WAN-side transmit throughput</b>	kbps	Minute average WAN-side transmit TOTAL for all interfaces
<b>LAN-side receive throughput</b>	kbps	Minute average LAN-side receive TOTAL for all interfaces
<b>Total number of optimized flows</b>	flows	End of minute count
<b>Total number of flows</b>	flows	End of minute count
<b>File-system-utilization</b>	% (non-Network Memory)	End of minute count
<b>Tunnel Level</b>		
<b>Tunnel latency</b>	msec	Second-sampled maximum latency during the minute
<b>Tunnel loss pre-FEC</b>	1/10 <sup>th</sup> %	Minute average
<b>Tunnel loss post-FEC</b>	1/10 <sup>th</sup> %	Minute average
<b>Tunnel OOP pre-POC</b>	1/10 <sup>th</sup> %	Minute average
<b>Tunnel OOP post-POC</b>	1/10 <sup>th</sup> %	Minute average
<b>Tunnel utilization</b>	% of configured bandwidth	Minute average

TCA Name	Unit	Metric
Tunnel reduction	%	Minute average

## SaaS Optimization Template

Use this template to select the SaaS applications/services you want to optimize.

To use this template, your EdgeConnect appliance must be registered with an **Account Name** and **Account Key** for the SaaS optimization feature.

The screenshot shows the 'SaaS Optimization' configuration page. On the left, there's a sidebar with 'Template Group' set to 'trial', 'Active Templates' (Show All), and a list of policy types: Policies, Access Lists, Security Policies, and SaaS Optimization (which is selected). At the bottom of the sidebar are 'Save', 'Save As', and 'Cancel' buttons, with a note 'Applies to all templates in group'. Below that is an 'Apply Template Groups' button. The main area is titled 'SaaS Optimization' and contains settings for 'Enable SaaS Optimization' (checked), 'RTT Calculation Interval' (set to 1440 minutes), and 'RTT Ping Interface' (set to default). A large table lists 52 SaaS applications with their RTT thresholds and domains. The columns are Application Name, Opti..., Adver..., RTT Threshold, Domains, and SaaS ... (with a small downward arrow). Applications listed include Adobe, AirWatch, AthenaHealth, BlueJeans, Box, CCcone, ConstantContact, CornerstoneOnDemand, Dropbox, Dynamics, Eloqua, GoToAssist, GoToMeeting, GoToTraining, GoToWebinar, Intuit, Jobvite, and Lithium. Each row shows the application name, its RTT threshold (e.g., 10 ms), the domains it affects (e.g., adobe.com, \*.air-watch.com), and a numerical value in the SaaS ... column.

Application Name	Opti...	Adver...	RTT Threshold	Domains	SaaS ...
Adobe	<input type="checkbox"/>	<input type="checkbox"/>	10 ms	adobe.com	1
AirWatch	<input type="checkbox"/>	<input type="checkbox"/>	10 ms	*.air-watch.com	31
AthenaHealth	<input type="checkbox"/>	<input type="checkbox"/>	10 ms	*.athenahealth.com, athenahealth.com	34
BlueJeans	<input type="checkbox"/>	<input type="checkbox"/>	10 ms	*.bluejeans.com, *.bjn.vc	69
Box	<input type="checkbox"/>	<input type="checkbox"/>	10 ms	*.box.com, *.app.box.com, *.boxcloud.com, *.box.net, *.boxcdn.net	2
CCcone	<input type="checkbox"/>	<input type="checkbox"/>	10 ms	*.myccportal.com, myccportal.com	30
ConstantContact	<input type="checkbox"/>	<input type="checkbox"/>	10 ms	constantcontact.com	3
CornerstoneOnDemand	<input type="checkbox"/>	<input type="checkbox"/>	10 ms	cornerstoneondemand.com	4
Dropbox	<input type="checkbox"/>	<input type="checkbox"/>	10 ms	dropbox.com, *.dropbox.com, *.dl.dropboxusercontent.com	5
Dynamics	<input type="checkbox"/>	<input type="checkbox"/>	10 ms	*.dynamics.com, *.microsoft.com, dynamics.com, microsoft.com	75
Eloqua	<input type="checkbox"/>	<input type="checkbox"/>	10 ms	eloquatrainingcenter.com, eloqua.com	6
GoToAssist	<input type="checkbox"/>	<input type="checkbox"/>	10 ms	gototraining.com	7
GoToMeeting	<input type="checkbox"/>	<input type="checkbox"/>	10 ms	gotomeeting.com	8
GoToTraining	<input type="checkbox"/>	<input type="checkbox"/>	10 ms	gototraining.com	9
GoToWebinar	<input type="checkbox"/>	<input type="checkbox"/>	10 ms	gotoassist.com, gotowebinar.com	10
Intuit	<input type="checkbox"/>	<input type="checkbox"/>	10 ms	intuit.com	11
Jobvite	<input type="checkbox"/>	<input type="checkbox"/>	10 ms	www.jobvite.com, hire.jobvite.com, careers.jobvite.com	12
Lithium	<input type="checkbox"/>	<input type="checkbox"/>	10 ms	lithium.com	13

**SaaS optimization** requires three things to work in tandem: **SSL** (Secure Socket Layer), **subnet sharing**, and **Source NAT** (Network Address Translation).

**Enable SaaS optimization** enables the appliance to contact the Cloud Intelligence Service and download information about SaaS services.

- If **Advertise** is **selected** for a service (for example, SFDC), the appliance will:
  - Ping active SaaS subnets to determine RTT/metric
    - Add subnet sharing entries locally for subnets within RTT threshold
    - Advertise subnets and their metric (within threshold) via subnet sharing to client-side appliances
  - Upon seeing an SFDC flow, generate a substitute certificate for an SFDC SSL domain (one substitute certificate per domain)
  - Auto-generate dynamic NAT rules for SFDC (but not for unchecked services)
- When **Optimize** is **selected** for a service (for example, SFDC), the appliance will:
  - Ping active SFDC subnets to determine the RTT (metric)
  - Does not advertise metric via subnet sharing (unless **Advertise** is also selected)
  - Receives subnet sharing metric (RTT) from associated appliances
  - Compares its own RTT (local metric) with advertised metric
    - If its own RTT is lower, then the packet is sent pass-through (direct to the SaaS server).
    - If an advertised RTT is lower, then the packet is tunnelized.
  - Generate a substitute certificate for an SFDC SSL domain (one sub cert per domain)
  - No NAT rules created
- When **Optimize** is **not selected** for a service (for example, SFDC), the appliance:
  - Receives subnet sharing advertisements for SFDC but does not use them
  - Does no RTT calc pinging
  - Does not participate in SSL
  - Creates no NAT rules
  - Sends all SFDC traffic as pass-through

The **RTT Calculation Interval** specifies how frequently Orchestrator recalculates the Round Trip Time for the enabled Cloud applications.

The **RTT Ping Interface** specifies which interface to use to ping the enabled SaaS subnets for Round Trip Times. The **default** interface is **wan0**.

## TIPS

- Initially, you might want to set a higher **RTT Threshold** value so that you can see a broader scope of reachable data centers/servers for any given SaaS application/service.

- If the **Monitoring** page shows no results at **50 ms**, you might want to reposition your SaaS gateway (advertising appliance) closer to the service.

## Security Policies Template

Use this page to set up security policies, also known as **zone-based firewalls**.

**CAUTION** If segmentation is enabled, do not use the Security Policies Template. Instead, configure Security Policies from the Routing Segmentation (VRF) tab.

- Zones are created on the Orchestrator and applied to an **Interface**.
- By default, traffic is allowed between interfaces labeled with the same zone. Any traffic between interfaces with different zones is dropped. Users can create exception rules (Security Policies) to allow traffic between interfaces with different zones.
- When you create an interface, it is assigned **Default** zone.
- If you create a new zone and assign that to an interface, all traffic between that interface and rest of the interfaces (which are still in the **Default** zone) are dropped. This implies that zone creation and assignment to interfaces should be performed during a planned network maintenance.
- You can also assign a zone label to an **Overlay**. On a new system, all overlays are assigned the **Default** zone.
- Traffic between an **Interface** and an **Overlay** follows the same rules as traffic between **Interfaces** or two **Overlays**; traffic is allowed between zones with the same label and any traffic between different zones is dropped. Users can create Security Policies to allow traffic between different zones.

### Implicit Drop Logging

Implicit Drop Logging enables you to configure implicit zone-based firewall drop logging levels. Implicit zone-based firewall drop is for inter-zone traffic by default. For example, if all the zone\_x to zone\_y traffic is the default **Deny All** (all the red cells from matrix), the traffic will be dropped by the zone-based firewall engine.

Select one of the following levels for the Implicit Drop Logging from the list: **None**, **Emergency**, **Alert**, **Critical**, **Error**, **Warning**, **Notice**, **Info**, or **Debug**.

**NOTE** The default logging level is **Alert**.

### Template

Complete the following steps to create a Security Policies Template:

1. Create zone names in **Configuration > Overlays & Security > Security > Firewall Zones**.
2. Create security policies to define exceptions.

To edit or add a rule, select the desired square in the matrix, and when the Edit Rules pop-up appears, make the desired changes.

3. Select the edit icon in the Match Criteria column and the Match Criteria pop-up appears. Make the desired changes.
4. You can select **More Options** to customize your rules. Select the check box next to the specific match criteria and select your desired changes from the list.
5. Click **Save**.

## Wildcard-based Prefix Matching Rules

- Even when using a range or a wildcard, the IPv4 address must be specified in the 4-octet format, separated by the dot notation. For example, A.B.C.D.
- Range is specified using a single dash. For example, 128-129.
- Wildcard is specified as an asterisk (\*).
- Range and Wildcard can both be used in the same address, but an octet can only contain one or the other. For example, 10.136-137.\*.64-95.
- A wildcard can only be used to define an entire octet. For example, 10.13\*.\*.64-95 is not supported. Use 10.130-139.\*.64-95 to specify this range.
- The same rules apply to IPv6 addressing.
- CIDR notation and (Range or Wildcard) are mutually exclusive in the same address. For example, 192.168.0.1-127/24 is not supported. Use either 192.168.0.0/24 or 192.168.0.1-127.
- These prefix-matching rules apply to the following policies only: Route, QoS, Optimization, NAT, Security, and ACLs.

## DNS Proxy Template

*Configuration > Templates & Policies > Templates*

If you select ON, complete the following steps to configure and define your DNS Proxy policies.

**NOTE** This feature is configurable only if you have loopback interfaces configured.

1. Choose whether you want the DNS Proxy enabled by selecting **ON** or **OFF**.
2. Select the name of the loopback interface or LAN-side label associated with your DNS proxy.
3. Enter the IP addresses for Server A in the **Server A Addresses** field.
4. Choose whether you want Caching to be **ON** or **OFF**. If selected, the domain name to the IP address mapping is cached. By default, caching is **ON**.
5. Enter the domain names of the Server A for the above IP addresses.

- Enter Server B IP addresses in the **Server B Addresses** field. Server B will be used if there are no matches to the Server A domains.

**NOTE** You can **Clear DNS Cache**. This will erase the domain name to the IP address mapping you had cached for both Server A and B.

## Shaper Template

The **Shaper** template is a simplified way of globally configuring QoS (Quality of Service) on the appliances:

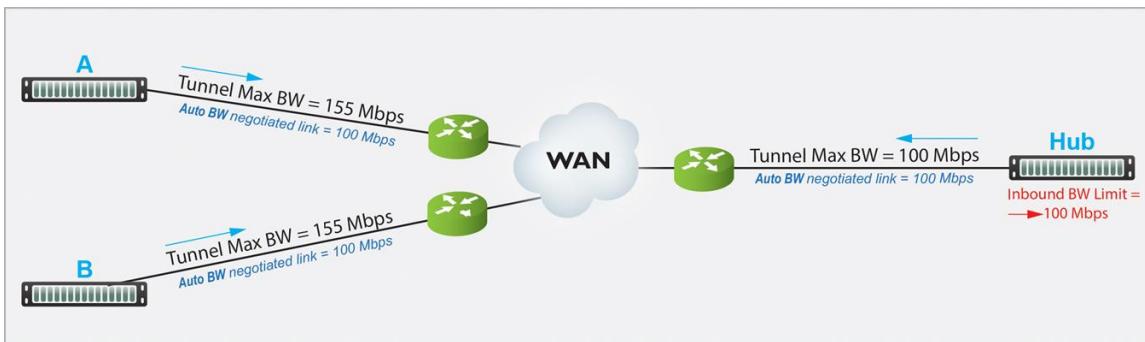
- The Shaper shapes traffic by allocating bandwidth as a percentage of the **system bandwidth**.
- The Shaper's parameters are organized into ten traffic classes. Four traffic classes are preconfigured and named **real-time**, **interactive**, **default**, and **best effort**.
- The system applies these QoS settings globally after compressing (deduplicating) all the outbound tunneled and pass-through-shaped traffic, shaping it as it exits to the WAN.
- Applying the template to an appliance updates its system-level **wan** Shaper. If the appliance has any added, interface-specific Shapers, they are preserved.
- For minimum and maximum bandwidth, you can configure traffic class values as a percentage of total available system bandwidth and as an absolute value. The appliance always provides the larger of the minimum values and limits bandwidth to the lower of the maximum values.
- You can rename or edit any traffic class.
- To view any applied configurations, access the **Configuration Templates & Policies > Shaping > Shaper** page.

ID	Traffic Name	Priority	Min Bandwidth %	Min Bandwidth Absolute (kbps)	Excess Weighting	Max Bandwidth %	Max Bandwidth Absolute (kbps)	Max Wait Time (ms)	Rate Limit (kbps)
1	Default	1	0	0	250	100	10,000,000	500	0
2	Interactive	1	0	0	1000	100	10,000,000	500	0
3	RealTime	1	0	0	500	100	10,000,000	100	0
4	Replication	1	0	0	100	100	10,000,000	1000	0
5	GuestWireless	1	0	0	100	100	10,000,000	1000	0
6	UNUSED6	6	0	0	1	100	10,000,000	500	0
7	UNUSED7	7	0	0	1	100	10,000,000	500	0
8	UNUSED8	8	0	0	1	100	10,000,000	500	0
9	UNUSED9	9	0	0	1	100	10,000,000	500	0
10	UNUSED10	10	0	0	1	100	10,000,000	500	0

## Dynamic Rate Control

**Tunnel Max Bandwidth** is the maximum rate at which an appliance can transmit.

**Auto BW** negotiates the link between a pair of appliances. In this example, the appliances negotiate each link down to the lower value, 100 Mbps.



However, if **A** and **B** transmit at the same time, **Hub** could easily be overrun.

If **Hub** experiences congestion:

- Select **Enable Dynamic Rate Control**. Allows **Hub** to regulate the tunnel traffic by lowering each remote appliance's Tunnel Max Bandwidth. The smallest possible value is that appliance's **Tunnel Minimum Bandwidth**.
- **Inbound BW Limit** caps how much bandwidth the appliance can receive.

### Shaper Settings

Field	Description
<b>Add Interface Shaper</b>	Adds an interface-specific shaper for outbound or inbound traffic.
<b>Enable Interface Shaper</b>	Enables a separate shaper for a specific WAN interface. <ul style="list-style-type: none"> <li>• For WAN optimization, the interface shaper can be used, but it is not recommended.</li> <li>• For SD-WAN, it should never be used because overlay traffic is not directed to an interface shaper; traffic is always shaped by the default WAN shaper.</li> </ul>
<b>Excess Weighting</b>	If there is bandwidth left over after satisfying the minimum bandwidth percentages, the excess is distributed among the traffic classes in proportion to the weightings specified in the <b>Excess Weighting</b> column. Values range from 1 to 10,000.
<b>Interface Shaper</b>	Interface that is being shaped.
<b>Max Bandwidth %</b>	This limits the maximum bandwidth that a traffic class can use to a percentage of total available system bandwidth.

Field	Description
<b>Max Bandwidth Absolute (kbps)</b>	This limits the maximum bandwidth that a traffic class can use to an absolute value (kbps). You can specify a maximum absolute value to cap the bandwidth for downloads and streaming.
<b>Max Wait Time</b>	Any packets waiting longer than the specified <b>Max Wait Time</b> are dropped.
<b>Min Bandwidth %</b>	Refers to the percentage of bandwidth guaranteed to each traffic class, allocated by priority. However, if the sum of the percentages is greater than 100%, lower-priority traffic classes might not receive their guaranteed bandwidth if it is all consumed by higher-priority traffic.  <b>Max</b> overrides <b>Min</b> if you set <b>Min Bandwidth</b> to a value greater than <b>Max Bandwidth</b> .
<b>Min Bandwidth Absolute (kbps)</b>	This guarantees a specific level of service when total system bandwidth declines. This is useful for maintaining the quality of VoIP, for example.
<b>Priority</b>	Determines the order in which to allocate each class' minimum bandwidth - <b>1</b> is first, <b>10</b> is last.
<b>Rate Limit (kbps)</b>	You can set per-flow rate limit that a traffic class uses by specifying a number in the Rate Limit column. For no limit, use <b>0</b> (zero).
<b>Recalc on IF State Changes</b>	When an interface state changes to UP or DOWN, selecting this recalculates the total bandwidth based on the configured bandwidth of all UP interfaces. For example, when <b>wan0</b> goes down, <b>wan0</b> bandwidth is removed from the total bandwidth when recalculating.
<b>Traffic Name</b>	Name assigned to a traffic class, either prescriptively or by the user.

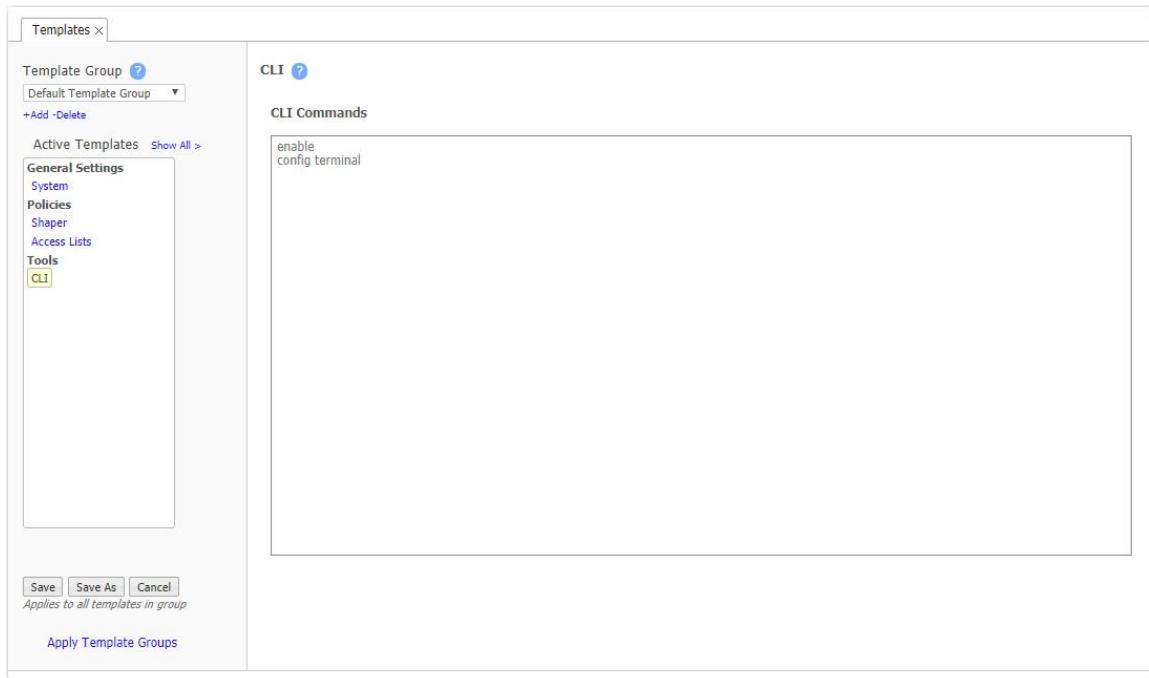
## Management Services Template

Use this template to globally apply the modifications made to your Management Services if segmentation is enabled or disabled. **Any** is used as the default Interface for the Source IP address; however, you can change the interface with any interfaces you have previously configured on the **Management Services** tab. To modify the interface, click **Any** in the table. For more information, refer to the **Management Services** tab.

## CLI Template

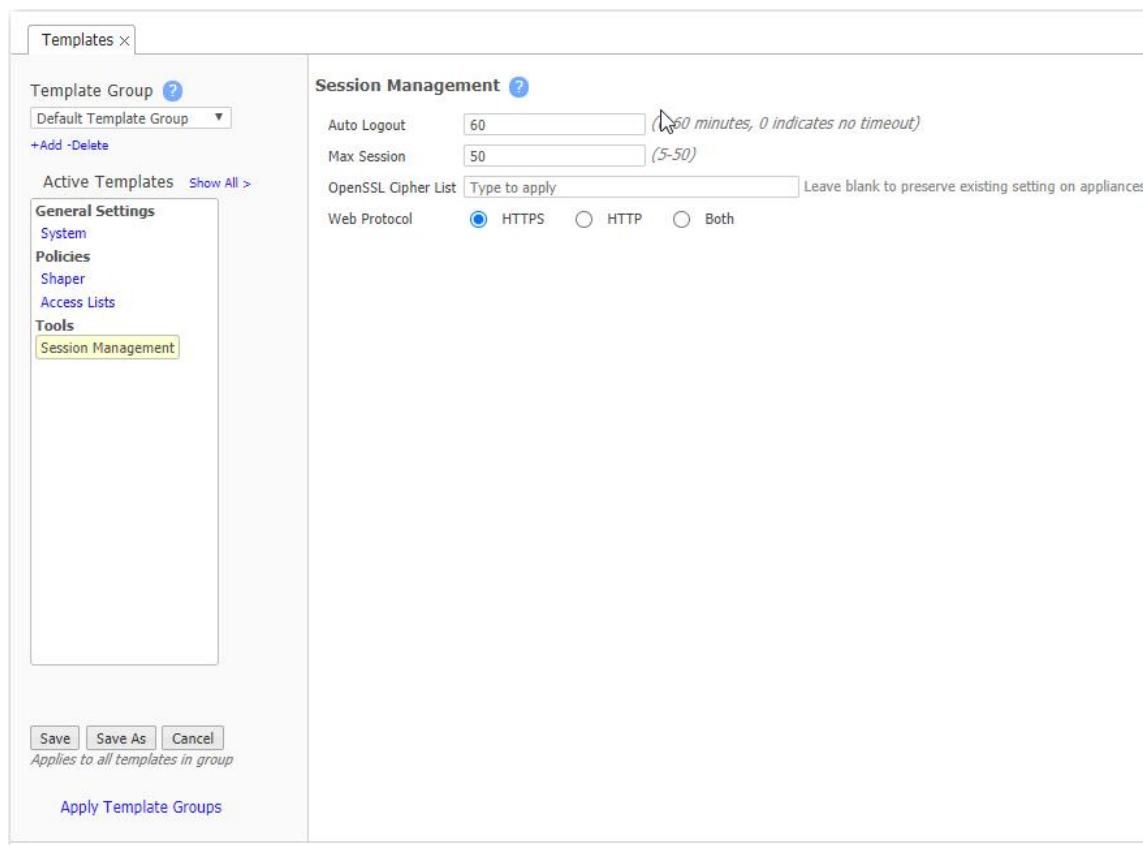
Use this template to enter any sequence of **Command Line Interface (CLI)** commands.

Enter each CLI command on a new line.



## Session Management Template

Use this page to configure settings that control access to the appliance web UI.



Field	Description
<b>Auto Logout</b>	Specifies the amount of time in minutes after which an inactive session will be automatically logged out. The valid range is 0-60. Use 0 to disable automatic logout.
<b>Max Sessions</b>	Maximum number of active sessions on the appliance. If the maximum number of sessions is reached, users who try to log in to the appliance web UI will receive a message that the browser cannot access the appliance. On non-EdgeConnect appliance models, Orchestrator might not be able to access the appliance.
<b>OpenSSL Cipher List</b>	<p>List of cipher suites to enable or disable on the appliance. For details about formatting this string, see <a href="#">this page</a>.</p> <p>The string can only contain the following characters: a-z, A-Z, 0-9, and +:-.!@</p> <p><b>WARNING:</b> Cipher format and availability are not validated. Ciphers should be thoroughly tested in a lab environment before being applied. When ciphers are applied from a template, an improperly formatted string or unavailable ciphers can cause an appliance crash.</p>
<b>Web Protocol</b>	Select the web protocol to use for appliance UI sessions. HTTPS is recommended for maximum security.

## Apply Template Groups

*Configuration > Templates & Policies > Apply Template Groups*

Use this tab to add or remove templates from appliances.

The screenshot shows the 'Apply Template Groups' interface. On the left, there's a sidebar titled 'Template Apply Order' with a list of categories: Default Template Group, Default Hub Settings, Default Branch Settings, Branch Protection Profiles, Enable Google DNS, Enable Cloudflare DNS, US-EAST, US-SOUTHEAST, US-CENTRAL, US-WEST, US-POWERS, API, AUS, EMEA, MIDWEST, and INDIA. Each category has a 'Present' checkbox. In the main area, there's a table titled '2 Rows' with columns for 'Appliance' (Edinburgh-Main), 'Present' (checkboxes), and 'Changes' (checkboxes). The table shows two rows for 'Edinburgh-Main'. At the bottom, there are 'Apply' and 'Cancel' buttons.

- If multiple template groups are applied to an appliance, the order in which they are applied determines which template is used. Templates applied later (lower on the apply order list) overwrite any conflicting templates applied earlier.
- Drag templates up or down to reorder the list.
- Orchestrator automatically applies any changed templates to the associated appliances.

## Cloud Services

This section includes the various cloud services that are offered.

### AWS Transit Gateway Network Manager

*Configuration > Cloud Services > AWS Network Manager*

Orchestrator supports association with Amazon Web Services and their Transit Gateway Network Manager. Orchestrator builds AWS Site-to-Site VPN tunnels, enabling you to securely connect your on-premises network to one or more Transit Gateways (TGWs).

Before you begin configuring AWS Transit Gateway Network Manager in Orchestrator, create an AWS account to authenticate and authorize Orchestrator with your AWS account. Then complete the prerequisite tasks in the following section.

## Prerequisites for AWS Transit Gateway Network Manager

Make sure you complete the following tasks in AWS console before configuring Orchestrator:

- Navigate to the **Identity and Access Management (IAM)** under **Services** to create a user profile with permissions for Orchestrator.
- Navigate to the **Virtual Private Cloud (VPC) Dashboard** and configure your Transit Gateways for the regions you want.
- Navigate to **Network Manager** from the **VPC Dashboard** under **Transit Gateways** to create a Global Network.
- Associate your Transit Gateways to the Global Network.

## Create a User Profile in AWS

To create a user profile in AWS, complete the following steps:

1. Sign in to AWS and navigate to the **Identity and Access Management (IAM)** service from the main AWS Management Console (**Services > Security, Identity, & Compliance > IAM**).

The screenshot shows the AWS Management Console with a dark-themed interface. At the top, there is a search bar with placeholder text "Search for services, features, marketplace products, and docs" and a keyboard shortcut "[Alt+S]". Below the search bar, the title "All services" is displayed. The services are organized into several categories:

- Migration & Transfer**: AWS Migration Hub, AWS Application Migration Service, Application Discovery Service, Database Migration Service, Server Migration Service, AWS Transfer Family, AWS Snow Family, DataSync.
- Networking & Content Delivery**: VPC (CloudFront, Route 53, API Gateway, Direct Connect, AWS App Mesh, AWS Cloud Map, Global Accelerator).
- Config**: OpsWorks, Service Catalog, Systems Manager.
- AWS Data Exchange**, AWS Glue, AWS Lake Formation, MSK, AWS Glue DataBrew, Amazon FinSpace.
- Security, Identity, & Compliance**: IAM (Resource Access Manager, Cognito, Secrets Manager, GuardDuty, Inspector, Amazon Macie, AWS Single Sign-On, Certificate Manager, Key Management Service, CloudHSM, Directory Service, WAF & Shield, AWS Firewall Manager, Artifact, Security Hub, Detective, AWS Audit Manager, AWS Signer, AWS Network Firewall).
- Media Services**: Kinesis Video Streams, MediaConnect, MediaConvert, MediaLive, MediaPackage, MediaStore, MediaTailor, Elemental Appliances & Software, Amazon Interactive Video Service, Elastic Transcoder, Nimble Studio.

2. Click **User** in the left menu under **Access Management**.
3. Click **Add User**.
4. Enter a username in the **User name** field.
5. Choose the **Access Type: Programmatic Access** and **AWS Management Console Access**.
6. Click **Next: Permissions**.
7. Set the Permissions for your user on this page. You can do this in one of three ways:

- **Adding a user to your group** - The user will inherit the permissions assigned to the group.
  - **Copying permissions from an existing user** - Copy permissions from an existing user in AWS and assign them to the user you want.
  - **Attaching existing policies directly** - Attach a file containing the permissions and assign it to the user.
8. Assign optional tags for your user. If you choose to add a tag, complete these steps:
- a. Enter a **key** - This represents the name of your tag.
  - b. Enter a **value** - Enter text that you want the key/tag to represent.
- Tags enable you to provide additional information about your user or group for tracking and organizational purposes. Up to 50 tags are allowed.
9. Select **Next: Review**. This page displays the review of the profile you just created for your user. The **User Details, Permissions Summary**, and additional information such as tag, are shown.
10. Select **Create User**. The page should now show the following success message, along with **Access Key ID** and the **Secret Access Key** associated with your configured user. Copy and paste the Access Key ID and the Secret Access Key to a secure place for later use. You will need these when adding the AWS account on Orchestrator.

## Create Transit Gateways

Next, you must create Transit Gateways (or select existing Transit Gateways you have already created) to associate with your AWS Network Manager, which you create in the steps below. Transit Gateways will terminate the Site-to-Site IPSec tunnels established from the EdgeConnect appliances in your network.

To create a new Transit Gateway, complete the following steps:

1. Navigate to the **Virtual Private Cloud (VPC) Dashboard (Services > Networking & Content Delivery)**.
2. Click **Transit Gateways**, under **Transit Gateways** in the left menu.
3. Click **Create Transit Gateways**.

[Transit Gateways](#) > Create Transit Gateway

## Create Transit Gateway

A Transit Gateway (TGW) is a network transit hub that interconnects attachments (VPCs and VPNs) within the same account or across accounts.

Name tag  ⓘ

Description  ⓘ

### Configure the Transit Gateway

Amazon side ASN  ⓘ

DNS support  enable ⓘ

VPN ECMP support  enable ⓘ

Default route table association  enable ⓘ

Default route table propagation  enable ⓘ

### Configure sharing options for cross account

Auto accept shared attachments  enable ⓘ

\* Required

4. Complete the following fields to create the Transit Gateway.

Field	Description
<b>Name Tag</b>	Enter a name that represents your Transit Gateway.
<b>Description</b>	Enter a description to help identify your Transit Gateway. This is the description for the Name Tag.
<b>Amazon side ASN</b>	Autonomous System Number that represents your Transit Gateways in AWS. You can use an existing ASN assigned to your global network or a private ASN. See the range limitations in AWS.
<b>DNS Support</b>	Select this check box if you want to enable Domain Name System support for your VPC within your Transit Gateways.
<b>VPN ECMP support</b>	Select this check box if you want to enable Equal Cost Multi-Path routing support in your Transit Gateways. This allows traffic with the same source and destination to be sent across the same multiple paths.
<b>Default Route Table Association</b>	Select this check box if you want to automatically associate other Transit Gateways to the route table that this one is using.
<b>Default Route Propagation</b>	Select this check box if you want to automatically create other Transit Gateways with this same route table.
<b>Auto-accept shared attachments</b>	Select this check box if you want your transit gateways to automatically accept attachments associated with different accounts.

- Click **Create Transit Gateway**. A success message should display along with your Transit Gateway ID.

## Create a Network Manager

After you create your Transit Gateway, you must create a Global Network in AWS. A Global Network hosts your specified Transit Gateways. It is managed by the AWS Network Manager.

- Navigate to the **VPC Dashboard**.
- Click **Network Manager** under **Transit Gateways**.
- Click **Create Global Network**.
- Enter a **Name** and **Description** for your **Global Network**.
- Click **Create**.

## Orchestrator Configuration

After completing the AWS prerequisites, navigate to the **AWS Network Manager** tab in Orchestrator. There are six buttons above the table on this tab that you use to complete the AWS and Orchestrator integration: **Subscription**, **Interface Labels**, **Network Manager Association**, **Tunnel Settings**, **VTI Subnet Pool**, and **Zone**.

### Subscription

1. To begin, click the **Subscription** button.
2. Enter the **Access Key ID** and the **Secret Access Key** that reflect your user account in AWS. This is the Access Key ID and the Secret Access Key you copied earlier in the [Create a User Profile in AWS](#) section.
3. Click **Save** after you finish entering the information in the table below. The **AWS Reachability** field should reflect **Connected**.

Field	Description
<b>AWS Reachability</b>	Connection status of the AWS Network Manager to Orchestrator: <b>Connected</b> or <b>Not Connected</b> .
<b>Access Key ID</b>	Access Key given to you in AWS to log in to the AWS console.
<b>Secret Access Key</b>	Secret Access Key given to you in AWS to log in to the AWS console.
<b>Polling Interval</b>	Indicates how often Orchestrator should check for configuration changes in the AWS transit gateways or Network Manager. The default polling interval is ten minutes.

4. Click **Save**.

You now should have an established connection with Orchestrator to your AWS account.

### Interface Labels

The Build Tunnels Using These Interfaces dialog box enables you to select the interfaces to build your tunnels to AWS.

1. Click the **Interface Labels** button. The Build Tunnels Using These Interfaces dialog box opens.
2. Drag the interface labels you want to apply from the column on the right into the **Primary** columns.
3. Click **Save**.

### Network Manager Association

In this dialog box, you can choose which Transit Gateways you want to associate with your EdgeConnect appliances.

**NOTE** You must first select the EdgeConnect appliances on the Orchestrator appliance tree, and then open the Network Manager Association tab to associate the appliances to your Transit Gateways.

1. Select or clear the check box next to the appliance you want to connect to or disconnect from the Network Manager.
2. See the following table for field descriptions.

Field	Description
<b>Hostname</b>	Host name of the appliance you want to connect to or disconnect from the Network Manager.
<b>Transit Gateways Present</b>	Lists the Transit Gateways that are already associated with the EdgeConnect appliances.
<b>Transit Gateways Changes</b>	Displays the EdgeConnect appliances that will be added or removed from the Transit Gateways.

3. Click **Save**.

Orchestrator starts to establish the Site-to-Site IPSec tunnels from the EdgeConnect appliances to the selected Transit Gateways.

### Tunnel Settings

The **Tunnel Settings** dialog box shows IKE and IPSec parameters used by Orchestrator when building Site-to-Site IPSec tunnels from the EdgeConnect appliances to the Transit Gateways. No changes are necessary for these parameters.

### VTI Subnet Pool

In this dialog box, set the Subnet IP address and the mask for the AWS subnet pool. Enter the subnet IP address and the mask ID in the designated fields.

- Any updates to the subnet pool configuration results in service disruption.
- You can have duplicated ASNs if you have a site with the same name.

**NOTE** This is an AWS-specific subnet pool. Therefore, every subnet IP address must start with **169.254** to be included in this pool.

### Zone

You can apply configured segments to your VTI interfaces associated for AWS. Click the **Zone** icon and select the zone you want to apply from the drop-down list.

### Verification

You can verify the stability and connectivity of your tunnels to the AWS Network Manager using the Connection Status column on the AWS Network Manager tab. This column shows the BGP Peer status. You can find additional details on the **Tunnels**, **VTI**, and **BGP** tabs.

Also, you can verify the AWS resources that Orchestrator created on the VPC Dashboard. To view the resources on the VPC dashboard, navigate back to the **Virtual Private Network** section in AWS and select **Customer Gateways** and **Site-to-Site VPN Connections**. On these tabs, you can confirm that the IPSec tunnels you created in Orchestrator are functioning correctly.

The tunnels should be in the 'available' state.

<input type="checkbox"/>	Name	ID	State	Type	IP Address	BGP ASN
<input type="checkbox"/>	California-AZ1_INET1	cgw-080ae8d050e7f65de	available	ipsec.1	13.52.48.80	65529
<input type="checkbox"/>	California-AZ2_INET1	cgw-0f7e7240ae2422368	available	ipsec.1	54.153.97.217	65529

The IPSec tunnel statuses should be 'UP'.

Tunnel Number	Outside IP Address	Inside IPv4 CIDR	Status	Status Last Changed	Details	Certificate ARN
Tunnel 1	52.8.56.35	169.254.10.132/30	UP	August 11, 2020 at 6:23:31 PM UTC-7	1 BGP ROUTES	
Tunnel 2	54.153.81.110	169.254.10.136/30	UP	August 11, 2020 at 7:14:05 PM UTC-7	1 BGP ROUTES	

## Route Tables and Static Routes

After the tunnels and the BGP sessions are established, the TGW route table shows the routes learned from the EdgeConnect devices. To create a route table for your transit gateways, navigate to the **VPC Dashboard** in AWS and click **Transit Gateway Route Tables** under **Transit Gateways**. To create a static route, select the transit gateway from the Route Table and navigate to the **Routes** tab.

<input type="checkbox"/>	CIDR	Attachment	Resource type	Route type	Route state
<input type="checkbox"/>	10.192.0.0/16	tgw-attach-07781aa5f63142731   vpc-04ba33464fdaa4a82	VPC	propagated	active
<input type="checkbox"/>	10.30.12.0/24	2 Attachments	VPN	propagated	active
<input type="checkbox"/>	10.30.2.0/24	2 Attachments	VPN	propagated	active

Complete the following fields, and then click **Create Static Route**.

Field	Description
<b>CIDR</b>	Specified range of IPv4 addresses for your VPC.
<b>Blackhole</b>	Enable if you want your matched traffic to be dropped.
<b>Choose attachment</b>	Choose the attachment for your static route.

## Peering

To begin sending traffic from the spoke VPCs where your AWS workloads are running, you must peer the VPCs with the Transit Gateways. To peer your configured Transit Gateways, navigate back to your VPC dashboard in AWS and click **Transit Gateway Attachments** under **Transit Gateways**. Complete the following steps.

[Transit Gateway Attachments](#) > Create Transit Gateway Attachment

### Create Transit Gateway Attachment

Select a Transit Gateway and the type of attachment you would like to create.

Transit Gateway ID\*  C

Attachment type  VPC  
 VPN  
 Peering Connection

#### VPC Attachment

Select and configure your VPC attachment.

Attachment name tag  i

DNS support  enable i

IPv6 support  enable i

VPC ID\*  C i

\* Required

1. Select the check box next to the available transit gateways you want to peer.
2. Click **Create Transit Gateway Attachment**.
3. Choose the **Transit Gateway ID** from the drop-down menu.
4. For **Attachment Type**, select **Peering Connection**.
5. For **Attachment Name Tag**, enter text for identification purposes.
6. For **Account**, select the check box for **My Account**.
7. For **Region**, choose the destination region you want the BGP peering to connect with.

## Microsoft Azure Virtual WAN

*Configuration > Cloud Services > Microsoft Azure Virtual WAN*

Microsoft Azure optimizes routing, automates large scale connectivity from various branches to Azure workloads, and provides unified network and policy management within Orchestrator. Use Azure to deploy to a single WAN circuit or for branch to branch connectivity by configuring virtual WANs to associated hubs.

Before you begin Microsoft Azure Virtual WAN configuration in Orchestrator, you need to use the Azure Virtual WAN portal to authenticate and authorize Orchestrator in Azure. You need to create the service principal, which focuses on single-tenant application to run within only one organization. Click [here](#) to get started.

### Microsoft Azure Prerequisites

1. Create an application in Azure and note the following Subscription details from the Azure Active Directory:
  - Subscription ID
  - Tenant (Directory) ID
  - Application (Client) ID
  - Client Secret Key
2. Create a storage account in Azure and get the following:
  - Storage Account Name
  - Storage Access Key
3. Create a resource group.
4. Create Azure Virtual WANs with hubs from your resource groups.

### Orchestrator Prerequisites

Complete the following tasks in Orchestrator:

1. Configure a VTI IP Pool.
  - Enter a valid IPv4 Subnet.

**NOTE** This is a unique address across the network. VTI interfaces created for Azure integration will be selected from this pool.

Azure VTI interface zone is set to WAN interface zone. Any change in deployment for the WAN interface zone is applied to Azure VTI as well.

**WARNING** Any change in the VTI pool after it is configured is networking affecting. This operation should be performed during a maintenance window as it can take several hours for some Cloud services to complete.

## 2. Configure BGP ASN Global Pool.

- Enter the start and end ranges for ASNs.
- Add any reserved ASNs to exclude from being applied to appliances.

**NOTE** If not previously enabled, Orchestrator enables BGP.

## Orchestrator Configuration

When you are finished with the Azure and Orchestrator prerequisites, navigate to the **Microsoft Azure Virtual WAN** tab in Orchestrator. There are five buttons at the top of the table that are used to complete the Azure and Orchestrator integration: **Subscription**, **Interface Labels**, **Virtual Wan Association**, **Tunnel Settings**, and **Zone**.

To begin, click the **Subscription** icon.

### Subscription

1. Enter the information in the Subscription fields that reflect your Azure portal account.
2. Click **Save** after you have finished entering the information in the table below. The Azure field should reflect **Connected**.

The following table represents the values in the **Subscription** window from the Azure portal.

Field	Description
<b>Azure Reachability</b>	Connection status of your account with Azure.
<b>Subscription ID</b>	ID of your subscription.
<b>Tenant ID</b>	Name of your Azure AD tenant.
<b>Client ID</b>	Client ID of your Azure portal.
<b>Client Secret Key</b>	Secret key of your Azure application.
<b>Storage Account Name</b>	Name of your storage account.
<b>Storage Account Key</b>	Storage account key.
<b>Storage URL</b>	Storage account URL.*
<b>Configuration Polling Interval</b>	Indicates how often Orchestrator should check for configuration changes in Azure. The default polling interval is ten minutes.

\*Storage URL

The Storage URL is present on the **Storage Accounts** tab in your Azure portal. Complete the following steps to obtain your storage account URL.

1. After your storage account is created in Azure, create a blob container.
2. Get the blob container URL.
3. Suffix the URL with a slash and add a file name in the **Storage URL** field.

**NOTE** Append the URL with a slash for the file name. Do not end the URL with a slash.

## Interface Labels

Select the order in which you want your interface labels to be used.

1. Click the **Interface Labels** button. The **Build Tunnels Using These Interfaces** displays.
2. Drag the Interface labels you want to use into the **Preferred Interface Label Order** column.
3. Click **Save**.

## Virtual WAN Association

Each appliance is associated with **one** virtual WAN. Use the Virtual Wan Association button to add or remove specific sites to your virtual WANs.

1. Click the **Virtual Wan Association** button.
2. Select an appliance from the tree in the left menu.
3. Select the check box to **Add** or **Remove** the appliance to your virtual WAN in Azure.

## Tunnel Settings

The **Tunnel Settings** button opens the Tunnel Settings dialog box, which enables you to define the tunnels associated with Azure and Orchestrator. It is recommended that you use the default tunnel settings for General, IKE, and IPSec; however, you can modify any field. The tunnel settings are set using the default VPN configuration parameters received from virtual WAN APIs located in your Azure portal account.

In your Azure Portal Account, navigate to the Azure Configuration table. This table displays the VPN site created for Orchestrator appliances associated to Azure virtual WANs. Additionally, manually associate sites to your hubs in Azure.

1. Navigate to **Azure Virtual WAN**.
2. Select **Azure VPN site**.
3. Select **New Hub Association**.

## Zone

You can apply configured segments to your VTI interfaces associated for Azure. Click the **Zone** button and select the zone from the drop-down you want to apply.

## Verification

The **Tunnel** page displays that Azure and Orchestrator have an established connection with Azure by displaying a tunnel status of **up - active**.

For more information about Azure configuration, visit the following link: <https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-site-to-site-portal>.

## Check Point CloudGuard Connect

Check Point CloudGuard Connect provides network and cloud security with policies defined within Orchestrator overlays. The **Check Point CloudGuard Connect** tab has the following fields.

Field	Description
<b>Subscription</b>	Name of the appliance you want to connect with Check Point.
<b>Interface Labels</b>	Name of the interfaces you want to connect with Check Point.
<b>Tunnel Settings</b>	Defines the tunnels associated with Orchestrator and Check Point.
<b>LAN Subnets</b>	Subnets configured on the LAN side associated with Check Point.

Before you begin to configure Check Point CloudGuard Connect, you need to create a Check Point account. Visit the following link to make an account: <https://portal.checkpoint.com>.

After you create an account, you will need to create an API Key.

### Subscription

1. After you complete the steps in the above URL to create your Check Point account, navigate to the **Check Point CloudGuard Connect** tab in Orchestrator.
2. Select the **Subscription** tab to get started with Check Point.
3. Enter your **Client ID** and the **Secret Key** you received when you created your Check Point account.
4. Select **Save** after you finish entering the information in the table below. The **Connection Status** should appear at the top of the **Subscription** window.

### Interface Labels

1. Select the **Interface Labels** tab. The **Build Tunnels Using These Interfaces** opens.
2. Drag the interface labels you want to use into the **Preferred Interface Label Order** column.
3. Select **Save**.

## Tunnel Settings

The **Tunnel Settings** tab helps you define the tunnels associated with Check Point and EdgeConnect. Use the Check Point default values for the **General**, **IKE**, and **IPSec** tunnel settings.

**NOTE** You can also configure specific General, IKE, and IPSec tunnel settings. The settings are automatically generated; however, you can make modifications if you choose to do so. To go back to the default settings, select **Use Default** on any of the tunnel windows.

## LAN Subnets

You can select the LAN subnets for a given appliance to associate with your Check Point integration. By default, LAN subnets are configured on the **Deployment** tab. You can also add, import a CSV file, or export a CSV file of the configured subnets.

## Enabling Check Point CloudGuard Connect

When you have completed configuration, you need to enable the Check Point service.

1. Navigate to the **Business Intent Overlay** tab in Orchestrator.
2. Go to the **Breakout Traffic to Internet & Cloud Services**.
3. Select the overlay that breaks out traffic to Check Point.
4. Drag **Check Point CloudGuard Connect** from the **Available Policies** column to the **Preferred Policy Order** column.

## Verification

Navigate to the **Check Point CloudGuard Connect** tab in Orchestrator to verify successful deployment under **Site Status**. You can also verify successful deployment on the **Tunnels** tab.

## Import and Export Subnets

**Import** enables you to import a Comma Separated Values (CSV) file into a pair of appliances used in Orchestrator. Before you import, you must remove the header row and save the files on your computer. Complete the following steps to begin your import.

1. Select **Choose File**.
2. Locate the file you want to import on your desktop.
3. Select **Open**.
4. Select Import. Orchestrator generates the CSV file. The following table represents the fields in the exported CSV file.

Appliance	Configured Subnets
<Appliance Hostname>	<Configured subnets IP addresses>

**NOTE** The titles and double quotes should be removed from your file before importing.

**CAUTION** This import overwrites previously configured imports.

## Microsoft Office 365

*Configuration > Cloud Services > Microsoft Office 365*

Ensure that your overlays have the following options configured to preserve the Works with Office 365 default applications. The table below indicates the default overlays, applications, and preferred policy order configured on the **Business Intent Overlays** tab within Orchestrator. The overlay name indicated in the table below is the default that ships with Orchestrator. This can be modified with user configuration.

**NOTE** Skype for Business, SharePoint Online, and Office 365 Exchange **must** break out locally.

Overlay	Application	Preferred Policy Order (Breakout Traffic to Internet & Cloud Services)	What It Matches
Real-Time	Skype for Business	 Break Out Locally	<ul style="list-style-type: none"> <li>• Microsoft Office 365 <b>Optimize</b> and <b>Allow</b> categories for the respective applications</li> </ul>
CriticalApps	SharePoint Online, Office 365 Exchange	 Break Out Locally	<ul style="list-style-type: none"> <li>• Microsoft Office 365 <b>Optimize</b> and <b>Allow</b> categories for the respective applications</li> </ul>
Default	For everything	Any policy order except "Drop"	<ul style="list-style-type: none"> <li>• Matches Microsoft Office 365 <b>Default</b> categories</li> <li>• Office365 Common applications</li> </ul> <p><b>NOTE</b> Do not specify other individual Office applications in this group or overlay.</p>

For more information about applications that work with Office 365, go to [Microsoft 365 & Security for Partners](#).

## Zscaler Internet Access

*Configuration > Cloud Services > Zscaler Internet Access*

Zscaler Internet Access (ZIA) is a cloud security service. EdgeConnect traffic can be service chained to Zscaler for additional security inspection. Orchestrator supports IPSec and GRE tunnel modes for Zscaler.

**NOTE** GRE tunnels are not formed across an EdgeHA link.

**NOTE** Zscaler's term for *ZEN* is now *Service Edge*.

The following table describes the fields on the Zscaler Internet Access tab.

Field	Description
<b>Appliance</b>	Name of the appliance to connect to Zscaler.
<b>Interface Label</b>	Interface label for the interfaces you want to connect to Zscaler.
<b>Mode</b>	Tunnel mode ( <b>IPSec</b> or <b>GRE</b> ) for Zscaler. The default mode is IPSec.
<b>Gateway Options</b>	A feature that enables you to configure sub-locations and various rules for your sub-locations. Gateway Options is an optional add-on.
<b>Bandwidth</b>	Upload and download bandwidth speeds (in Mbps) to and from Zscaler.
<b>Zscaler Deployment Status</b>	Status of the Zscaler deployment ( <b>Creating</b> , <b>Pending</b> , or <b>Deployed</b> ). <i>Deployed</i> indicates successful deployment.
<b>Zscaler Service Edges</b>	These are the Zscaler endpoints to which the tunnels connect. This field is populated with discovered Public Service Edges based on the appliance's geographical location.
<b>Connection Status</b>	Status of the Zscaler connection based on tunnel and IP SLA statuses.

### Configure Zscaler

Before you configure Zscaler, you must create a Zscaler account and ensure that you have an established connection with Zscaler.

**NOTE** This section represents the **automated** configuration of IPSec, IKE, and GRE tunnels from EdgeConnect to the Zscaler cloud. To manually configure the tunnels with the Zscaler cloud, refer to the *EdgeConnect and Zscaler IPSec Integration Guide* and the *EdgeConnect and Zscaler GRE Integration Guide*.

### Subscription

1. Go to <https://help.zscaler.com/zia/sd-wan-api-integration> and follow the steps to configure your Zscaler account.
2. After configuring your Zscaler account, navigate to the Zscaler Internet Access tab in Orchestrator (**Configuration > Cloud Services > Zscaler Internet Access**).

3. Click the **Subscription** button.

The Subscription dialog box opens.

4. Enter the appropriate information to reflect your Zscaler account.

The following table describes the fields.

Field	Description
<b>Zscaler</b>	Indicates whether you are connected to your Zscaler account.
<b>Zscaler Cloud</b>	Zscaler cloud URL. For example, admin.zscalerthree.net.
<b>Partner Username</b>	Partner administrator username you created when configuring Zscaler.
<b>Partner Password</b>	Partner administrator password you created when configuring Zscaler.
<b>Partner Key</b>	Partner key you created when configuring your Zscaler account. Select Silver Peak from the list of partners.
<b>Domain</b>	Domain provisioned in Zscaler for your enterprise.
<b>Subscription Cloud ID</b>	(Optional) A subcloud can be a subset of ZIA Public Service Edges, a subset of Private Service Edges, a subset of PZENs, or a subset of both ZIA Public Service Edges and Private Service Edges or PZENs. If you subscribe to any of these services, you must specify in this field the name of your subcloud (for example, Americas) to obtain a full list of Service Edges for your organization. <b>WARNING</b> Because this is service affecting, configure this ID during a maintenance window only. This will cause previously built tunnels to be deleted and rebuilt.
<b>Configuration Polling Interval</b>	Indicates how often Orchestrator should check for configuration changes in Zscaler. The default polling interval is ten minutes.

5. Click **Save**. The Zscaler field should indicate *Connected*.

## Interface Labels

Select Primary labels you want your traffic to go to. Backup labels will be used as the second option if the primary is unreachable.

1. Click the **Interface Labels** button on the Zscaler Internet Access tab.

The Build Tunnels Using These Interfaces dialog box opens.

2. Drag the Interface labels you want to use into the Primary and Backup areas of the dialog box.
3. Click **Save**.

**WARNING** This is service affecting. Any changes to the interface selection can cause previously built tunnels to be deleted and rebuilt.

## Tunnel Settings

The **Tunnel Settings** button opens the Zscaler Tunnel Setting dialog box, enabling you to define the tunnels associated with Zscaler and EdgeConnect. The Mode field on the General tab allows you to select **IPSec** or **GRE** as the tunnel protocol for the specified WAN interface label. Use Zscaler defaults for tunnel settings defined by the system.

**NOTE** For IPSec mode, you can configure General, IKE, and IPSec tunnel settings. For GRE mode, you can configure General tunnel settings. Settings are automatically generated, but you can change them if you want to.

## Service Edge Override

You can override the automatically selected Service Edge pair for specific sites. You have the option to add this exception to one or more sites within your network.

**NOTE** Orchestrator does not support Service Edge Override for GRE tunnels.

1. Click the **Service Edge Override** button on the Zscaler Internet Access tab.

The Service Edge Override dialog box opens.

2. Enter the appliance name, the interface label, and the primary and secondary IP addresses. Orchestrator will build tunnels to those Service Edges.

Field	Description
<b>Appliance</b>	Appliance for which to override Zscaler Service Edges.
<b>Interface Label</b>	Interface label from which tunnels are built.
<b>Primary IP</b>	IP address of the primary Zscaler Service Edge.
<b>Secondary IP</b>	IP address of the secondary Zscaler Service Edge.

## IP SLA

Configure IP SLA for Zscaler tunnels. This configuration ensures tunnel connectivity and internet availability between Zscaler and Orchestrator. If the tunnel cannot reach Zscaler, the tunnel is considered DOWN.

1. Click the **IP SLA** button on the Zscaler Internet Access tab.

The Zscaler IP SLA Configuration dialog box opens.

2. If all fields are dimmed, click **Enable IP SLA rule orchestration**.
3. Complete the following fields.

Field	Description
<b>Monitor</b>	Ping or HTTP/HTTPS.

Field	Description
<b>Address</b>	URL to the Zscaler endpoint that the IP SLA subsystem will ping. You can configure up to three addresses.
<b>Source Interface</b>	Select an orchestrated loopback label.

- Accept the default values for the remaining fields and click **Save**.

Orchestrator builds the tunnels.

## Country / Timezone

You can use the Zscaler Country / Timezone dialog box to configure standard ISO Country Codes to Zscaler Country Enums and standard Time Zones to Zscaler Time Zone Enums. Click the **Country / Timezone** button on the Zscaler Internet Access tab to open the dialog box. Make changes, and then click **Save**.

## Gateway Options

You can configure gateway options and rules for Zscaler sub-locations. Orchestrator uses location and sub-locations to better define a branch site in the Zscaler cloud. Sub-locations are LAN-side segments within each branch. They can be identified by LAN interfaces, zones, or a collection of LAN subnets.

### Enable Gateway Options

To enable gateway options:

- Click the **Gateway Options** button on the Zscaler Internet Access tab.

The Zscaler Gateway Options dialog box opens.

- Click **Add**.

The Location / Sub-Location Match Criteria dialog box opens.

- Enter a name for the new rule in the **Rule Name** field.

**WARNING** If two rules have the same sub-location name or IP address, Orchestrator picks the first match and considers the order of the rules.

- Specify a location by entering an appliance name, region, or group in the **Appliances** field.

- Enter the WAN label in the **Location Label** field.

- If you select the **Sub-Location** check box:

- Enter the sub-location name in the **Name** field.
- Enter the subnet address (LAN label, Firewall Zone, or subnet) in the **Internal IPs** field.

- Click **Save**.

**NOTE** Sub-locations can be applied to all WAN links selected in the Build Tunnels Using These Interfaces dialog box (accessed by clicking the Interface Label button on the Zscaler Internet Access tab).

If you select the **Show sub-locations** check box on the Zscaler Internet Access tab, the sub-locations configured in Gateway Options appear in the Zscaler table.

## Configure Bandwidth Control

You can set up bandwidth controls for your Zscaler sub-locations configured in Gateway Options. Select from bandwidth control options that use fixed amounts of bandwidth, inherit bandwidth values from parent locations, or use percentages of deployment bandwidth.

1. Click the **Gateway Options** button on the Zscaler Internet Access tab.

The Zscaler Gateway Options dialog box opens.

2. In the table, locate the rule name row for which you want to configure bandwidth control, and then click the linked text in the **Gateway Options** column.

The Zscaler Gateway Options & Bandwidth Control dialog box opens.

3. Select one of the following options from the **Bandwidth Control** drop-down list:

Bandwidth Control Option	Description
<b>OFF</b>	Do not use bandwidth control. This is the default setting.
<b>Fixed bandwidth</b>	Use fixed amounts of bandwidth for the sub-location. Specify amounts for download and upload in Mbps.
<b>Inherit (parent) location bandwidth</b>	Inherit the parent location's bandwidth values.
<b>Use deployment WAN label bandwidth</b>	Use percentages of the deployment WAN label's bandwidth. Specify amounts for download and upload as percentages. Each specified percentage cannot exceed 100%. Orchestrator will automatically translate percentages into Mbps and send them to Zscaler. Sub-locations will use these values as percentages of deployment bandwidth.

4. Click **Save**.

The Change Gateway Options dialog box opens.

**WARNING** Changing Gateway Options is service affecting. Make changes during a maintenance window.

5. Click **Change Gateway Options**.

Your changes are applied to Orchestrator and Zscaler. This process takes time to complete.

## Zscaler Association

The final step to configure the integration in Orchestrator is to associate EdgeConnect appliances to Zscaler.

1. In the Orchestrator appliance tree, select one or more appliances to associate with Zscaler.
2. Click the **Zscaler Association** button on the Zscaler Internet Access tab.  
The Zscaler Appliance Association dialog box opens.
3. In the table, select one or more appliances you want to associate with Zscaler, and then select the **Add** check box.  
Select the **Remove** check box to remove Zscaler association from selected appliances in the table.
4. Verify the changes, and then click **Save**.

## Pause Orchestration

When troubleshooting, you can click **Pause Orchestration** and save to pause orchestration. To restart, click **Resume Orchestration**.

## Using Zscaler for Breakout Traffic

Finally, you need to select the Zscaler service in at least one Business Intent Overlay Breakout Traffic Policy to steer traffic to it.

1. Navigate to the Business Intent Overlays tab in Orchestrator (**Configuration > Overlays & Security > Business Intent Overlays**).
2. Click the overlay that breaks out traffic to Zscaler.  
The Overlay Configuration dialog box opens.
3. Click the **Breakout Traffic to Internet & Cloud Services** tab.
4. Drag **Zscaler Cloud** from the **Available Policies** column to the **Preferred Policy Order** column.

## Verify Zscaler Deployment

After Zscaler Internet Access is configured, deployment will begin automatically. Navigate to the Zscaler Internet Access tab to verify successful deployment. The Zscaler Deployment Status column should have a green status of *Deployed*, and the Connection Status column should have a green status of *Up*. The Connection Status column indicates the status of the Zscaler connection based on tunnel and IP SLA statuses.

**NOTE** Zscaler is deployed and orchestrated for an appliance based on the Zscaler Appliance Association dialog box. Business Intent Overlays (BIOS) are used to configure breakout internet policies to Zscaler. This is used for automatic load distribution and failover.

You can also verify that your Zscaler tunnels have been successfully deployed on the Tunnels tab. The Passthrough Tunnel column should list your Zscaler tunnels, and the Status column should have a green status of *up - active*.

## Service Orchestration

*Configuration > Cloud Services > Service Orchestration*

To watch a video of this feature, see [How to Integrate with Third-Party Service Providers](#).

Use the Service Orchestration tab to automate 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.

Service Orchestration creates a local tunnel identifier (IKE ID) for each tunnel to the third-party service. After the tunnels are created, complete the integration on the third-party service's site by replacing the source identity values with the local tunnel identifiers (IKE IDs) that Orchestrator created for each endpoint.

**NOTE** By default, Service Orchestration provides the framework for Netskope integration. The instructions on this page are specific to Netskope, but you can apply the same general procedure to other third-party services.

### Prerequisites

- You must have loopback interfaces configured to use the Service Orchestration feature.
- Service Orchestration supports third-party services that use IPSec IKEv2 endpoints.
- You will need the following information from the third-party service for each endpoint you want to add:
  - Endpoint name
  - IP address
  - Probe address

### Remote Endpoint Configuration

Add the remote endpoints for Netskope. You can add one endpoint at a time or add endpoints in bulk by importing the information from a CSV file.

#### Add Endpoints One at a Time

1. Click **Remote Endpoint Configuration**.

The Add Remote Endpoints for Netskope dialog box opens.

2. Click **+Remote Endpoint**.
3. Complete the following fields. Press the **Tab** key to navigate to the next field.

Field	Description
<b>Name</b>	Name of the Netskope endpoint. <b>IMPORTANT:</b> If an endpoint name is decommissioned or modified, you must update the value in this table.
<b>IP Address</b>	IP address of the Netskope endpoint. <b>IMPORTANT:</b> If an IP address is decommissioned or modified, you must update the value in this table.
<b>Interface Label</b>	The interface labels that can be provisioned for this endpoint. Only labels in this list will be provisioned. <b>HINT:</b> Click <b>Interface Label Default</b> to reset the Interface Label for every endpoint in the table to the default value of <b>Any</b> .
<b>Pre-shared Key</b>	The pre-shared key for the endpoint. To display the pre-shared key, click anywhere in the field. Do one of the following: <input type="checkbox"/> Edit this field for each endpoint. This value can be an ASCII string, a hex-encoded string (if it has a 0x prefix), or a base64-encoded string (if it has a 0s prefix). <input type="checkbox"/> Click <b>PSK Default</b> to create and save a pre-shared key. Every endpoint will use the pre-shared key you create. Because traffic going to these endpoints is encrypted, it will not compromise security to use the same pre-shared key for each endpoint.
<b>Probe Address</b>	The Netskope endpoint that the IP SLA subsystem will ping. You can obtain the probe address from the third-party security provider. <b>IMPORTANT:</b> Orchestrator will prefill the Address field in the IP SLA Settings dialog box with this value. If you delete the value in the Probe Address field in this table, Service Orchestration will ping the value specified in the Address field in the IP SLA Settings for Netskope dialog box.
<b>Backup Remote Endpoint</b>	Enter the Netskope endpoint that you want to use as a backup tunnel. For example, ATL1-Atlanta could use DFW1-Dallas as a backup remote endpoint. If you leave this field empty, the endpoint will not have a backup tunnel. The BIO determines how traffic will be handled if a single or single and backup tunnel go down.

4. Repeat these steps for each endpoint.

**TIP** To delete an endpoint, click the X in the last column in the table.

5. Click **Save**.

Updates are orchestrated immediately.

## Add Endpoints in Bulk

1. Click **Remote Endpoint Configuration**.

The Add Remote Endpoints for Netskope dialog box opens.

2. Click **Import** to import a list of remote endpoints from a CSV file. The CSV file must contain columns for name, IP address, interface label, pre-shared key, probe address, and backup remote endpoint, in that order.

**NOTE** Remove any header rows before you import the file.

3. Click **Choose File**.

4. Navigate to the file, select the file, and then click **Open**.
5. Click **Save**.

Updates are orchestrated immediately.

## Bulk Edits

To make bulk edits to the table:

1. Click **Export**.
  2. Open the CSV file and delete the three header rows.
  3. Modify, save, and close the file.
  4. Click **Import**, and then click **Choose File**.
  5. Locate and select the file, and then click **Open**.
- Orchestrator updates the table.
6. Click **Save**.

## Interface Labels

Select the Primary and Backup interface labels for your traffic. Backup interface labels will be used if the primary interface labels are unreachable.

**NOTE** Netskope does not support Active - Active backup.

1. Click **Interface Labels**.  
The Build Tunnels using these Interfaces for Netskope dialog box opens.
2. Drag the interface labels you want to use into the Primary area. (The Peer/Service names in the Tunnels table will be NSK\_Primary\_1 and NSK\_Primary\_2.)
3. Drag the interface labels you want to use into the Backup area. (The Peer/Service names in the Tunnels table will be NSK\_Backup\_1 and NSK\_Backup\_2.)
4. Drag the interface labels up or down to reorder the list as necessary.
5. Click **Save**.

## Tunnel Settings

1. Click **Tunnel Settings** to configure the tunnel settings.

The Tunnel Settings dialog box opens. The General tab is displayed with the Mode field set to IPSec.

2. Complete the following fields as required for security service. (To configure Netskope, accept the default values for all fields.)

Field	Description
<b>Mode</b>	Indicates that the tunnel protocol is IPSec. You cannot edit this field.
<b>IPSec Suite B Preset</b>	Select an IPSec Suite B preset if required by the security service ( <b>GCM-128</b> , <b>GCM-256</b> , <b>GMAC-128</b> , or <b>GMAC-256</b> ). The default setting is None. <ul style="list-style-type: none"> <li>If IPSec Suite B Preset is set to None, no preset is selected, but GCM and GMAC algorithms are available to set independently.</li> <li>If an IPSec Suite B preset is selected, various settings on the IKE and IPSec tabs are configured automatically based on the selected preset.</li> </ul>
<b>Auto max BW enabled</b>	When enabled, allows the appliances to auto-negotiate the maximum tunnel bandwidth. Enabled by default.

3. Click the **IKE** tab, and then complete the following fields. (To configure Netskope, accept the default values for all fields.)

Field	Description
<b>IKE Version</b>	IKE v2. You cannot edit this field.
<b>Preshared Key</b>	Pre-shared key used for IKE authentication. This key is generated dynamically.
<b>Authentication algorithm</b>	Authentication algorithm used for IKE security association (SA). Authentication algorithm can be set to <b>SHA1</b> , <b>SHA2-256</b> , <b>SHA2-384</b> , <b>SHA2-512</b> , or <b>NULL</b> .
<b>Encryption algorithm</b>	Encryption algorithm used for IKE security association (SA). Encryption algorithm can be set to <b>AES-128</b> , <b>AES-256</b> , <b>AES-GCM-128</b> , <b>AES-GCM-256</b> , or <b>NULL</b> .

<b>Diffie-Hellman group</b>	Diffie-Hellman Group used for IKE security association (SA) negotiation.												
	<ul style="list-style-type: none"> <li>If the IPSec Suite B Preset field on the General tab is set to None, you can select the appropriate group. Available groups are 14 through 21, 26, and 31.</li> <li>If the IPSec Suite B Preset field is set to any other setting, this field is automatically set to the appropriate group.</li> </ul>												
<b>Rekey interval/lifetime</b>	Rekey interval/lifetime of IKE security association (SA) in minutes. The default is 480 minutes.												
<b>Dead peer detection</b>	<p><b>Delay time:</b> The interval (in seconds) to check the lifetime of the IKE peer.</p> <p><b>Retry count:</b> The number of times to retry the connection before determining that the connection is dead. This field is not editable.</p>												
<b>Phase 1 mode</b>	Exchange mode for the IKE security association (SA) negotiation. This field is automatically set to Aggressive. This field is not editable.												
<b>IKE identifier</b>	<p>By default, the Service Orchestration feature creates IKE IDs using the following fixed format: <code>hostname_label@endpoint</code></p> <p>You can create custom IKE IDs by specifying one or more of the following macros:</p> <table border="1"> <thead> <tr> <th>Macro</th> <th>Definition</th> </tr> </thead> <tbody> <tr> <td><code>%hostname%</code></td> <td>Appliance host name</td> </tr> <tr> <td><code>%label%</code></td> <td>Interface label name</td> </tr> <tr> <td><code>%tunnel_source_ip%</code></td> <td>Tunnel source IP</td> </tr> <tr> <td><code>%tunnel_dst_ip%</code></td> <td>Tunnel destination IP/FQDN</td> </tr> <tr> <td><code>%appliance_key%</code></td> <td>Appliance key</td> </tr> </tbody> </table> <p>For example, to create an IKE ID that contains an email domain, enter  <code>%hostname%_%label%@customerdomain.com</code></p>	Macro	Definition	<code>%hostname%</code>	Appliance host name	<code>%label%</code>	Interface label name	<code>%tunnel_source_ip%</code>	Tunnel source IP	<code>%tunnel_dst_ip%</code>	Tunnel destination IP/FQDN	<code>%appliance_key%</code>	Appliance key
Macro	Definition												
<code>%hostname%</code>	Appliance host name												
<code>%label%</code>	Interface label name												
<code>%tunnel_source_ip%</code>	Tunnel source IP												
<code>%tunnel_dst_ip%</code>	Tunnel destination IP/FQDN												
<code>%appliance_key%</code>	Appliance key												

- Click the **IPSec** tab, and then complete the following fields:

Field	Description
-------	-------------

<b>Authentication algorithm</b>	Authentication algorithm used for the IPSec security association (SA). Authentication algorithm can be set to <b>SHA1</b> , <b>SHA2-256</b> , <b>SHA2-384</b> , <b>SHA2-512</b> , <b>AES-GCM-128</b> , <b>AES-GCM-256</b> , or <b>NULL</b> .
<b>Encryption algorithm</b>	Encryption algorithm used for the IPSec security association (SA). Encryption algorithm can be set to <b>AES-CBC-128</b> , <b>AES-CBC-256</b> , <b>AES-GCM-128</b> , <b>AES-GCM-256</b> , or <b>NULL</b> .
<b>IPSec anti-replay window</b>	Select a size from the drop-down list or <b>Disable</b> to disable the IPSec anti-replay window. If a size is selected, protection is provided against an attacker duplicating encrypted packets by assigning a unique sequence number to each encrypted packet.
<b>Rekey interval/lifetime</b>	Rekey interval/lifetime of the IPSec security association (SA) in minutes. The default is 120 minutes.
<b>Perfect forward secrecy group</b>	Diffie-Hellman group used for IPSec security association (SA) negotiation. Based on the setting of the <b>IPSec Suite B Preset</b> field on the General tab, this field is set to the following Diffie-Hellman group: <ul style="list-style-type: none"> <li>• For None: 14 (by default)</li> <li>• For GCM-128 or GMAC-128: 19</li> <li>• For GCM-256 or GMAC-256: 20</li> </ul>

5. Click **Save**.

**TIP** Click **Use Netskope Default** to reset all Tunnel settings to the global defaults for Service Orchestration.

## IP SLA Settings

1. Click **IP SLA Settings**.

The IP SLA Settings for Netskope dialog box opens.

2. If all fields are dimmed, click **Enable IP SLA rule orchestration**.
3. Complete the following fields.

Field	Description
<b>Monitor</b>	Ping or HTTP/HTTPS.
<b>Address</b>	Netskope endpoint that the IP SLA subsystem will ping. Orchestrator prefills the <b>Address</b> field with the value from the Remote Endpoint Configuration table. You can configure up to three addresses.

Field	Description
<b>Source interface</b>	Select an orchestrated loopback label.

- Accept the default values for the remaining fields, and then click **Save**.

Orchestrator builds the tunnels.

## Pause Orchestration (Optional)

When troubleshooting, you can click **Pause Orchestration** and then click **Save** to pause the service orchestration. To restart the service orchestration, click **Resume Orchestration**.

## +BIO Breakout

By default, the tunnels associated with a third-party service will be available for BIOs. You can upload an icon to display on the Business Intent Overlays tab.

**NOTE** Supported file types include PNG, JPEG, SVG, and WEBP. The recommended dimensions are 60 x 20 pixels.

- Click **+BIO Breakout**.

The Configure BIO Breakout for Netskope dialog box opens.

- Click **Upload Service Icon**.
- Locate and select the file, then click **Open**.
- Click **Save**.

This icon will display next to the service name on the Business Intent Overlays tab.

If you do not want this third-party provider to be available for BIOs, do the following:

- Click **+BIO Breakout**.

The Configure BIO Breakout for Netskope dialog box opens.

- Clear the **BIO Breakout** check box.
- Click **Save**.

## Remote Endpoint Association

The final step to configure the integration in Orchestrator is to associate EdgeConnect appliances with remote endpoints. Use this page to add or remove endpoints from an appliance. It is recommended that you associate one remote endpoint per EdgeConnect appliance.

1. In the Orchestrator appliance tree, select one or more appliances to associate with Netskope remote endpoints.
  2. Click **Remote Endpoint Association**.
- The Associate an Appliance to Netskope Remote Endpoints dialog box opens.
3. Select the **Add** or **Remove** check box next to the endpoints you want to associate with the selected appliances. Be sure to add the endpoints that are geographically closest to the appliances.
  4. Verify the proposed changes to remote endpoints in the table to the right, and then click **Save**.

## Add Tunnel Local Identifiers to Netskope

After the Service Orchestration integration is complete in Orchestrator, you must add the local tunnel identifiers (IKE IDs) to Netskope. You can simplify this process by exporting the Netskope configuration to a CSV file. The exported file contains all of the configuration details in the table on the Netskope page for all selected appliances, including IKE IDs.

**NOTE** The default tunnel local identifier value is a fixed format: *hostname\_labelname@IPaddress*. For example, EAST3-AWS\_INETA@192.x.x.xxx.

If you created a custom IKE ID, the local tunnel identifier value will follow the format you defined in the IKE identifier field on the Tunnel Settings dialog box.

1. In the Orchestrator appliance tree, select all appliances associated with Netskope remote endpoints.
2. On the **Netskope** page on the Service Orchestration tab, click **Export** to save the contents of the table to a CSV file.
3. Log in to Netskope.
4. In the IPSec configuration panel, replace the Source Identity values with the corresponding Tunnel Local Identifiers (IKE IDs) created by Orchestrator.

## Verification

After Netskope is configured and the Netskope policy is applied successfully in the BIO, deployment will begin automatically. Go to the **Netskope** tab and view the Connection Status column to verify that the deployment was successful.

## Set Up a New Service

To set up a new third-party service:

1. Click **+Add Service** and complete the following fields.

Field	Description
<b>Name</b>	Name of the new service.
<b>Prefix</b>	A prefix to assign to all tunnels for this service. Orchestrator will use this prefix to filter tunnels and IP SLAs.

2. Click **Save**.

A new tab is created on the Service Orchestration page.

**TIP** To edit or delete a service, click the edit icon next to the service name.

3. Select the tab for the new service and follow the steps explained in Set Up Netskope Integration to integrate this new service.

## Deploy Cloud Hubs

You can deploy one or more EdgeConnect Virtual (EC-V) appliances in supported platforms. At this time, AWS and Azure are supported.

Before you begin, complete the following tasks:

1. On the AWS dashboard or the Azure portal, create an Identity and Access Management (IAM) user account with required permissions for Orchestrator to create resources. A dedicated IAM user account for Orchestrator is recommended.
  - a. Create a policy that contains all permissions the Orchestrator requires to create an EC-V.
  - b. Attach the policy to the Orchestrator's IAM user account.
  - c. Download the Security credentials of the Orchestrator's IAM user account.
2. If you are deploying EV-Cs in AWS, on the EC2 dashboard, create a key pair to assign to the EC-V. You will need this key pair if you want to SSH into the EC-V after the deployment.

After creating the IAM account, click **New Deployment** on the [Cloud Hubs in AWS](#) on the next page or [Cloud Hubs in Azure](#) on page 412 tab to configure and deploy one or more EC-V cloud instances.

After deploying an EC-V in the cloud, navigate to the Discovered Appliances page in Orchestrator to view the deployment status. If the EC-V is still being deployed, the status in the Approve column will indicate Configuring. It takes approximately ten minutes to deploy and configure a cloud EC-V. Click **Refresh Discovery Information** to determine whether the appliance is ready to be approved into the SD-WAN fabric.

When configuration is complete and the green Approve button appears, the EC-V is fully configured in Inline Router mode with mgmt0, wan0, and lan0 MAC addresses assigned. While adding the EC-V, the Deployment Profile page will show LAN IP address, WAN IP address, WAN interface firewall mode, and WAN bandwidth value assigned by Orchestrator.

You can upgrade the appliance software version on a cloud EC-V after approving and adding it to the SD-WAN fabric.

After a cloud EC-V has been deployed, you can add another EC-V into the same deployment. The new EC-V will use the same settings from the existing deployment configuration such as account, region, VPC, key pair, and instance type. You can deploy the new instance into an Availability Zone that is already used by an existing appliance or a new Availability Zone.

## Cloud Hubs in AWS

*Configuration > Cloud Services > IaaS > Deploy Cloud Hubs in AWS*

The Cloud Hubs in AWS tab provides the AWS account details and EC-V deployment configuration details for all cloud EC-Vs that have been deployed.

Use this tab to:

- Create and modify AWS accounts
- Deploy EC-Vs in the AWS cloud
- Remove an AWS deployment

The following table describes each field on this tab.

Field	Description
<b>Name</b>	Name given on the deployment configuration page.
<b>VPC</b>	CIDR block used for deployment.
<b>Account</b>	Name of the AWS account that was used to deploy the EC-Vs.
<b>Instances</b>	Number of EC-V instances in the deployment. To add one or more EC-Vs to the deployment, click <b>+Add</b> . In the New Instance on AWS dialog box, select the availability zone to use and any optional tags to apply to the new instance. <b>Max</b> indicates that the maximum number of instances have been created for the VPC CIDR block.
<b>Status</b>	Status of the deployment. If more information is available, an info icon is displayed. <b>NOTE</b> If the deployment was incomplete, the info dialog contains a link to download the log file and steps to resolve the issue.
<b>Terminate</b>	To permanently delete a deployment, click <b>Terminate</b> . This action deletes all resources associated with the EC-Vs, including all EC2 resources.
<b>Deployment Info</b>	Click the info icon in this column to view deployment and instance details, including the IP addresses associated with the mgmt0, wan0, and lan0 interfaces.
<b>Resources</b>	Click the info icon in this column to view details about each AWS resource that Orchestrator created during the deployment. This information is helpful when, for example, you need to identify the IP address of a security group to add a user to.
<b>Comment</b>	Comments that were added to the deployment when the EC-V was created. To edit the comment, click the edit icon.

## Create or Modify an AWS Account

To create or modify an AWS account to Orchestrator:

1. Click **AWS Accounts**.

The AWS Accounts dialog box opens.

2. Click **New AWS Account** or click the edit icon next to the account you want to edit.

The AWS Account Configuration dialog box opens.

3. Complete or modify the elements as necessary.

## Deploy a New EC-V

Click **New Deployment** to deploy one or more EC-V instances in AWS.

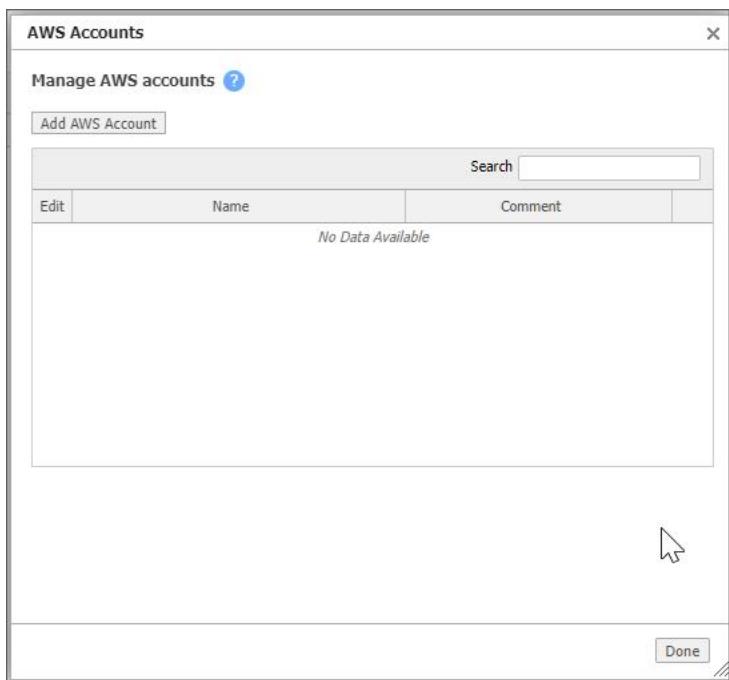
## Remove an EC-V

If a deployment does not complete or you no longer want the EC-V in the AWS cloud, you can remove the deployment and all associated artifacts.

To remove a deployment, locate the deployment you want to remove, and then click **Terminate** in the desired row.

## AWS Accounts

The AWS Accounts dialog box lists all of the AWS accounts that have been added.



- Click **Add AWS Account** to create a new account for EC-V deployments.
- Click the edit icon next to an existing account to modify that account's details.

**NOTE** You cannot modify accounts that have active deployments.

## AWS Account Configuration

Complete the following steps to create an AWS IAM user account with the required permissions for creating EC-V instances in AWS.

### Create a Policy with Required Permissions

1. Log in to the AWS Dashboard.
2. On the Find Services search menu, enter **IAM** to open the Identity and Access Management (IAM) page.
3. Under Access Management, click **Policies**. The Policies page opens.
4. Click **Create policy** and click the **JSON** tab.
5. Delete the existing text.
6. Go to this **web page**, click the link for your version of Orchestrator, and then copy and paste the JSON policy text into the editor.
7. Click **Next: Tags**.
8. (Optional) Add metadata to the policy by attaching tags as key-value pairs.

9. On the Review policy page, enter a name and optional description for the new policy.
10. Review the policy summary to see the permissions granted by your policy, and then click **Create policy** to save your work.

### Attach Policy to the Orchestrator IAM User Account

1. Click **Users > Add user**. The Add user page opens.
2. Enter a user name in the User name field (for example, ArubaOrchestrator).
3. Under Access type, select **Programmatic access**, and clear the AWS Management Console access check box.
4. Click **Next: Permissions**.
5. Under Set Permissions, click **Attach existing policies**.
6. Select the Policy document you created from the list, and then click **Next: Review**.
7. Under Permissions summary, click **Add permissions**.

### Download Orchestrator IAM User Account Credentials

1. On the Users page, click the **Security credentials** tab.
2. Download or copy and paste the Access key ID and Secret key ID to a secure place for later use.

### Create a Key Pair to Assign to EC-Vs

Review the instructions on [this page](#) to create a key pair on the AWS region where you plan to deploy the EC-V.

### Add the AWS Account to Orchestrator

Complete the following fields for Orchestrator, and then click **Save** when finished.

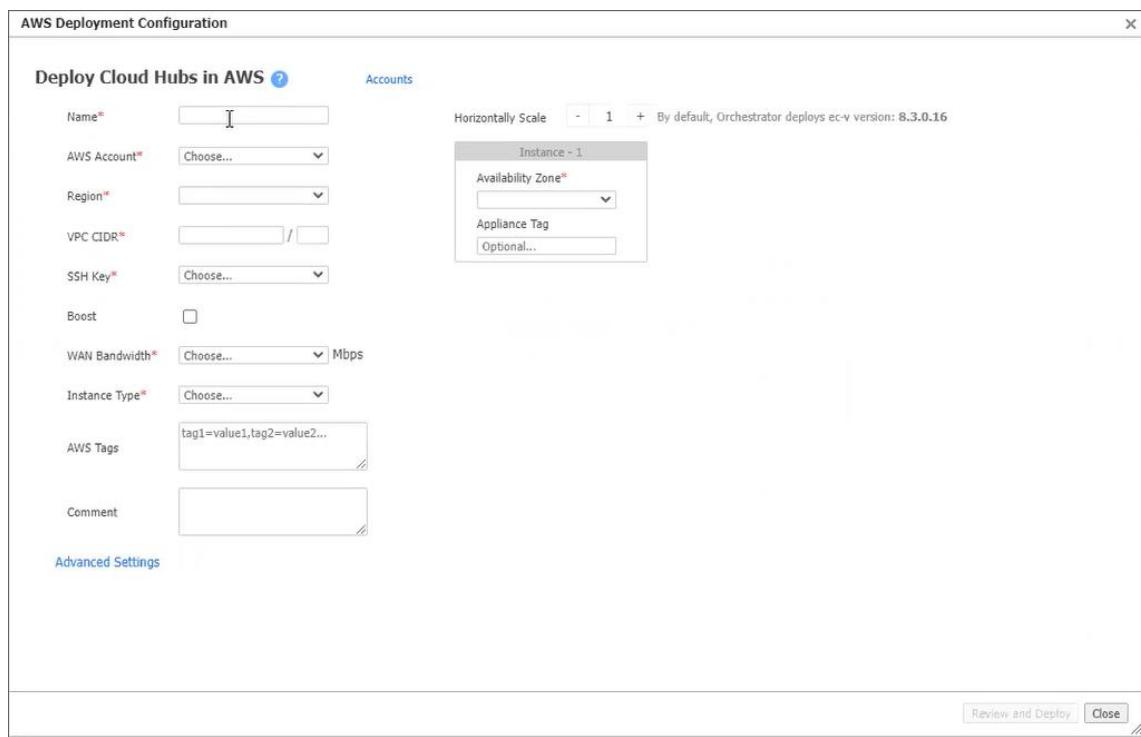
Field	Description
<b>Name</b>	Enter a unique name. If you have multiple AWS accounts, you must enter a unique name for each account.
<b>Access Key</b>	Enter the Orchestrator IAM user's Access Key ID that you saved earlier.
<b>Secret Key</b>	Enter the Orchestrator IAM user's Secret Key ID that you saved earlier.
<b>Comment</b>	Enter a comment that provides any additional information about the AWS account.

Orchestrator validates the account information. This takes approximately 45 seconds.

### AWS Deployment Configuration

Use the AWS Deployment Configuration page to create one or more EC-V instances in an AWS region.

**NOTE** If you do not have an AWS account configured in Orchestrator, the AWS Deployment Configuration dialog box is blank. Click the **Accounts** link to create an AWS account.



Field	Description
<b>Name</b>	Enter a name for the deployment. This name is used only for identifying the deployment. A deployment consists of one or more EC-Vs that an Orchestrator creates in an AWS Virtual Private Cloud (VPC). Only alphanumerical letters and hyphens are allowed in the deployment name. The maximum allowed length is 20 characters.
<b>AWS Account</b>	Select an AWS account to use for deploying the EC-V.
<b>Region</b>	Select an AWS region where you want to deploy the EC-V.
<b>VPC CIDR</b>	Enter a VPC Classless Inter-Domain Routing (CIDR) block. The smallest supported CIDR block is /24 and the largest supported CIDR block is /16. Orchestrator creates all AWS resources required for the EC-V deployment within this VPC. For each EC-V you deploy, Orchestrator creates three subnets that are /28 in size. In other words, if you deploy two EC-Vs, Orchestrator creates six subnets in total. This is true even if both EC-Vs are created in a single Availability Zone.
<b>SSH Key</b>	Select an existing AWS key pair to assign to the EC-V. A key pair must be created prior to the deployment.

Field	Description
<b>Boost (Optional)</b>	Boost requires additional resources on an AWS EC2 instance. After Boost and an appropriate WAN Bandwidth value are selected, Orchestrator displays the appropriate AWS instance types for the deployment on the Instance Type drop-down menu. <b>NOTE</b> Selecting the Boost check box does not enable Boost on the EC-V. It only allows Orchestrator to display appropriate AWS instance types that can support Boost for the selected WAN bandwidth. To enable Boost on the EC-V, go to the Deployment page and the Business Intent Overlay (BIO) page after the deployment is complete.
<b>WAN Bandwidth</b>	The Bandwidth drop-down list displays the current EdgeConnect license tiers. After you select a WAN Bandwidth value, Orchestrator displays the appropriate AWS instance types for the deployment on the Instance Type drop-down menu.
<b>Instance Type</b>	Based on your selection of Boost and WAN Bandwidth values, Orchestrator displays the appropriate AWS instance types on this drop-down menu.
<b>AWS Tags (Optional)</b>	Any comma-separated tags entered here are applied to all AWS resources that Orchestrator creates while deploying the EC-V. If you do not enter any tags, Orchestrator automatically creates a unique tag for each AWS resource that it creates while deploying the EC-V. This AWS tag is created to identify each resource created by Orchestrator. The tag is formatted as follows: <i>sp-automated-deployment name-instance-index-resource name</i> .
<b>Comment (Optional)</b>	Enter an optional comment if you want to attach any additional details for the deployment.
<b>Advanced Settings</b>	<b>Custom AMI ID:</b> If you want to deploy the EC-V with a specific public or private image, provide the AMI ID. You can obtain the AMI ID from the AWS console. Leave this field blank to allow Orchestrator to deploy the EC-V with the base AMI obtained from the AWS Marketplace.
<b>Horizontally Scale</b>	You can deploy multiple EC-Vs by clicking + and selecting the Availability Zone for each EC-V. If the selected region supports multiple Availability Zones, each Availability Zone is shown on the drop-down menu. When deploying multiple EC-Vs, it is best practice to deploy each EC-V in a unique Availability Zone.
<b>Appliance Tag (Optional)</b>	Enter an Appliance Tag on this field if you want to assign a pre-configuration file to the deployment. If this field is left blank, Orchestrator will automatically assign an Appliance Tag for its own configuration purposes.

When you have completed all of the required fields, click **Review and Deploy**. Review the configuration summary, and click **Deploy** to create the EC-V instances.

## Cloud Hubs in Azure

*Configuration > Cloud Services > IaaS > Cloud Hubs in Azure*

The Cloud Hubs in Azure tab provides the Azure account details and EC-V deployment configuration details for all Azure cloud EC-Vs that have been deployed.

**NOTE** EC-Vs that are deployed manually in Azure will not be displayed in Orchestrator.

Use this tab to:

- Create and modify Azure subscriptions
- Deploy EC-Vs in the Azure cloud
- Remove an Azure cloud deployment

**NOTE** When you remove a deployment, all EC-Vs in the deployment will be deleted.

The following table describes each field on this tab.

Field	Description
<b>Name</b>	Name given on the deployment configuration page.
<b>Virtual Network</b>	CIDR block used for deployment.
<b>Account</b>	Name of the Azure account that was used to deploy the EC-Vs.
<b>Instances</b>	<p>Number of EC-V instances in the deployment. To add one or more EC-Vs to the deployment, click <b>+Add</b>. In the New Instance on Azure dialog box, select the Availability Zone to use and any optional tags to apply to the new instance.</p> <p><b>Max</b> indicates that the maximum number of instances have been created for this deployment.</p> <p>If the region you selected does not support Availability Zones, the New Instance on Azure dialog box will not display an Availability Zone menu.</p>
<b>Region</b>	Region of the EC-V deployment.
<b>Resource Group</b>	Name of the Azure Resource Group that was used for the EC-V deployment.
<b>Status</b>	<p>Status of the deployment. If more information is available, an information icon is displayed.</p> <p><b>NOTE</b> If the deployment was incomplete, the info dialog contains a link to download the log file and steps to resolve the issue.</p>
<b>Terminate</b>	<p>To permanently delete a deployment, click <b>Terminate</b>. This action deletes all resources associated with the EC-Vs, including all Azure resources.</p> <p>If you created more than one EC-V in the deployment, all EC-Vs will be deleted when you click <b>Terminate</b>. The Resource Group that was used for the deployment will <i>not</i> be deleted.</p>
<b>Deployment Info</b>	Click the info icon in this column to view deployment and virtual machine details.
<b>Resources</b>	Click the info icon in this column to view details about each Azure resource that Orchestrator created during the deployment.
<b>Comment</b>	Comments that were added to the deployment when the EC-V was created. To edit the comment, click the edit icon.

## Create or Modify an Azure Subscription

Click **Azure Subscriptions** to create or modify an Azure subscription to Orchestrator.

## Deploy a New EC-V

Click **New Deployment** to deploy one or more EC-V instances in Azure.

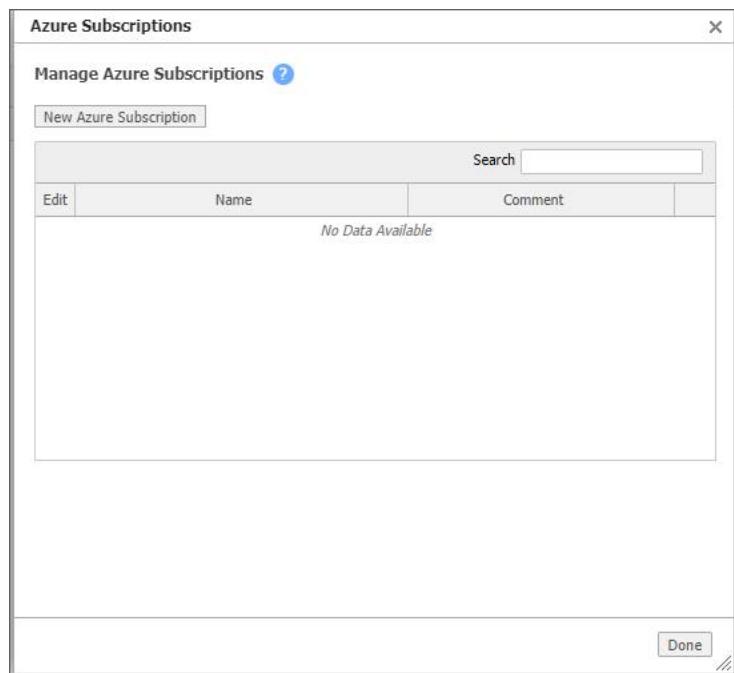
## Remove an EC-V

If a deployment does not complete or you no longer want the EC-V in the Azure cloud, you can remove the deployment and all associated artifacts.

To remove a deployment, locate the deployment you want to remove, and then click **Terminate** in the desired row.

The Azure Subscriptions dialog box opens.

## Azure Subscriptions



The Azure Subscriptions dialog box lists all Azure subscriptions that have been added to Orchestrator.

- Click **New Azure Subscription** to add a new Azure subscription.
- Click the edit icon next an existing subscription to modify its details.

**NOTE** You cannot modify subscriptions that have active deployments.

### Add New Azure Subscription

To add a new Azure subscription, click **New Azure Subscription**.

### Edit an Existing Azure Subscription

To edit an existing Azure subscription:

1. Click the edit icon next to an existing subscription to modify that subscription's details.

The Azure Subscription Configuration dialog box displays.

**NOTE** You cannot modify subscriptions that have active deployments.

2. Modify the elements as necessary.

3. Click **Save**.

Orchestrator validates the subscription information.

4. Click **Close**.

The Azure Subscription Configuration dialog box displays.

## Azure Subscription Configuration

Before you begin an EC-V deployment from the Orchestrator, you must perform the following tasks on the Azure portal.

1. [Accept Azure Marketplace Terms below](#) for EdgeConnect to enable programmatic deployment.
2. [Create a New App Registration on page 417](#) (also known as a Service Principle)
3. [Create a New Resource Group on page 418](#)
4. [Create a Custom Role on page 418](#)
5. [Assign the Custom Role to the Resource Group on page 421](#)

You will need the following information as noted in the steps below to add the Azure subscription to Orchestrator:

- Subscription ID
- Tenant ID
- Client ID
- Client Secret

## Accept Azure Marketplace Terms

Accepting Azure Marketplace image terms for EdgeConnect is required for the Orchestrator to automatically deploy an EdgeConnect image from the Azure Marketplace. You will only need to do this once per Azure subscription.

1. Log in to the Azure Portal.
2. Under Azure services, click **+ Create a resource**.

3. On the Create a resource page, enter edgeconnect and select the **Silver Peak Unity EdgeConnect** option.

The screenshot shows the Microsoft Azure 'Create a resource' interface. At the top, there's a search bar with the text 'edgeconnect'. Below the search bar, a dropdown menu is open, showing 'Silver Peak Unity EdgeConnect' as the selected option. Other options visible in the dropdown include 'Oceanblue Cloud SD-WAN EdgeCo...' and 'Silver Peak Unity E...'. To the left of the search bar, there are links for 'Get started' and 'Recently created'. Below these, there's a 'Categories' section.

4. On the Plan drop-down menu, select **Silver Peak Unity EdgeConnect 8.3.0.19**, and then click **Get started**.

The screenshot shows the Microsoft Azure 'Silver Peak Unity EdgeConnect' creation page. At the top, there's a navigation bar with 'Home > Create a resource > Silver Peak Unity EdgeConnect'. Below the navigation, there's a logo for 'Silver Peak Systems' and the title 'Silver Peak Unity EdgeConnect'. A 'Plan' dropdown menu is open, showing 'Silver Peak Unity EdgeConnect 8.3.0.19' as the selected option. To the right of the dropdown are 'Create' and 'Start with a pre-set configuration' buttons. Below the dropdown, there's a link 'Want to deploy programmatically? Get started'.

5. On the Configure Programmatic Deployment page, select **Enable** next to the subscription ID that you want to use to deploy the EdgeConnect VMs.

Microsoft Azure

Search resources, services, and docs (G+/)

Home > Create a resource > Silver Peak Unity EdgeConnect >

## Configure Programmatic Deployment

Use API calls, ARM templates, or the PowerShell console to automatically deploy without using the Azure portal. You'll only need to do this once—the settings you choose will be used each time you deploy.

**Product + plan details**

Silver Peak Unity EdgeConnect 8.3.0.19  
by Silver Peak Systems  
[Terms of use](#) | [privacy policy](#)

Pricing does not include [Azure infrastructure costs](#) (e.g., virtual machine compute time or storage) and is based on the pricing tier you select at the time of deployment. The pricing above applies only to Azure subscriptions purchased from Microsoft. For Azure subscriptions purchased from a reseller, contact your reseller for pricing. Neither subscription credits nor monetary commitment funds may be used to purchase non-Microsoft offerings. These purchases are billed separately. If any Microsoft products are included in the above offering(s) (e.g., Windows Server or SQL Server), such products are licensed by Microsoft and not by any third party.

**Terms of use**

By enabling programmatic purchases for the subscriptions selected below, I (a) agree to the legal terms and privacy statement(s) associated with each offering above, (b) for Azure subscriptions purchased from Microsoft, authorize Microsoft to charge or bill my current payment method for the fees associated with my use of the offering(s), including applicable taxes, with the same billing frequency as my Azure subscription, until I discontinue use of the offering(s), and (c) agree that Microsoft may share my contact information, and transaction details associated with my purchase of the above offering(s), with any third-party vendors, if listed above. Microsoft does not provide rights for third-party products or services. See the [Azure Marketplace Terms](#) for additional terms.

**Choose the subscriptions**

Select the Azure subscriptions for which you would like to enable programmatic deployments of the above offering(s)

Subscription Name	Subscription ID	Status
Pay-As-You-Go	951	96... <span style="border: 1px solid #ccc; padding: 2px;">Enable</span> <span style="border: 1px solid #ccc; padding: 2px;">Disable</span>

**Save** **Discard**

6. Click **Save**.

A message at the top of the screen notifies you when configuration updates are complete.

### Create a New App Registration

To create a new App registration:

1. Log in to the Azure Portal.
2. In the main search menu, enter `app registrations` and click **App registrations**.
3. Click the **+ New registration** button.
4. On the Register an application page, in the **Name** field, enter a user-facing display name for the application.
5. Under Supported account types, select **Accounts in this organizational directory only (Default Directory only - single tenant)**.
6. **Optional:** Enter a redirect URI.

7. Click **Register**.

**NOTE** Note the Application (client) ID and Directory (tenant) ID. You will need these IDs when you add the subscription details on the Orchestrator.

8. Under Manage, click **Certificates & secrets**.

9. Click **New client secret**.

10. Enter a **Description** and **Expiration Date**.

11. Click **Add**.

A new client secret is created.

12. Copy the text in the **Value** column.

**NOTE** This text can only be viewed immediately after creation. Be sure to save the secret before leaving the page.

13. On the main search menu bar, enter `subscription` and press Enter.

14. Copy the subscription ID.

You have successfully registered your application and gathered the details that are required for adding the Azure subscription details on the Orchestrator. Continue to [Create a New Resource Group below](#).

## Create a New Resource Group

Creating a new Resource Group on the Azure portal is a best practice. This ensures that the Aruba Orchestrator only has access to that Resource Group to deploy EC-Vs. However, it is possible to deploy one or more EC-Vs into an existing Resource Group that contains other Azure resources.

To create a new resource group:

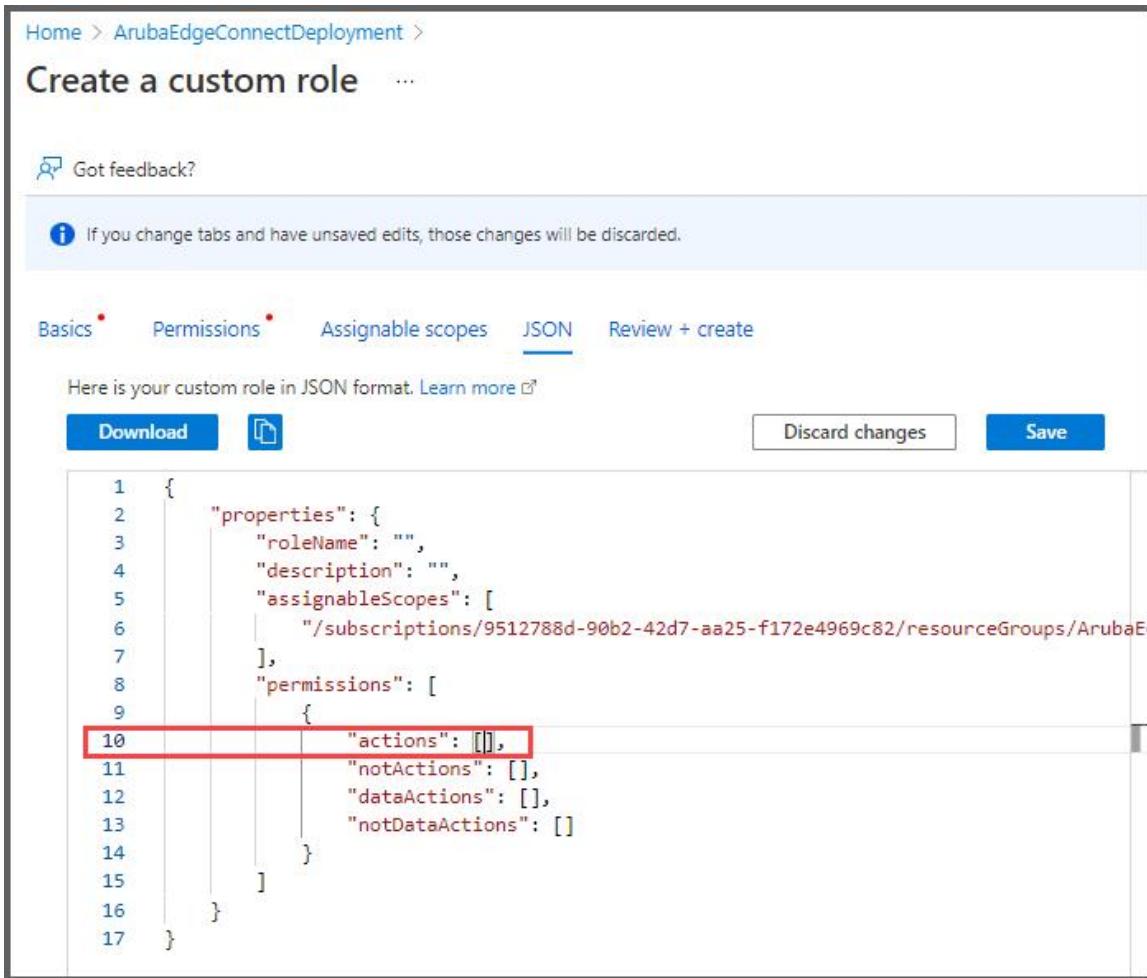
1. On the main search menu, enter `resource group`, and then select the **Resource groups** menu.
2. Click **+ Create**.
3. On the Create a resource group page, select the subscription that you want to use to create the resource group.
4. Enter a name for the resource group, and then select a region.
5. Click **Review + create**.
6. Click **Create**.

Continue to [Create a Custom Role below](#).

## Create a Custom Role

You must have [Owner](#) or [User Access Administrator](#) permissions to create custom roles. There are multiple ways to create a custom role. The following steps create a custom role from within the Resource Group that you created.

1. Select the resource group you created in [Create a New Resource Group on the previous page](#), and then click **Access control (IAM)**.
2. Click **Add**, and then click **Add custom role**.  
The Custom Roles editor opens (the Basic tab is displayed).
3. In the **Custom role name** field, enter a name for the custom role. The name must be unique for the Azure AD directory. The name can include letters, numbers, spaces, and special characters.
4. In the **Description** field, enter an optional description for the custom role. The description will display in the tool tip for the custom role.
5. Accept the default value for the Baseline permissions, and then click the **JSON** tab.
6. Click **Edit**.
7. Go to this [web page](#), and then click the link for your version of Orchestrator.
8. Copy the list of Azure permissions, and then paste the list within the square brackets under **Actions** (line 10), as shown in the following figures.



The screenshot shows the 'Create a custom role' interface in the Azure portal. The JSON tab is selected. The JSON code is displayed in a code editor with line numbers. Line 10, which contains the 'actions' key, is highlighted with a red rectangle.

```

1  {
2      "properties": {
3          "roleName": "",
4          "description": "",
5          "assignableScopes": [
6              "/subscriptions/9512788d-90b2-42d7-aa25-f172e4969c82/resourceGroups/ArubaEdgeConnectDeployment/providers/Microsoft.ManagedIdentity/userAssignedIdentities/ArubaEdgeConnectDeploymentUserAssignedIdentity"
7          ],
8          "permissions": [
9              {
10                 "actions": [],
11                 "notActions": [],
12                 "dataActions": [],
13                 "notDataActions": []
14             }
15         ]
16     }
17 }

```

Home > ArubaEdgeConnectDeployment >

## Create a custom role

Got feedback?

If you change tabs and have unsaved edits, those changes will be discarded.

Basics \* Permissions \* Assignable scopes JSON Review + create

Here is your custom role in JSON format. Learn more ↗

Download  Discard changes Save

```
1  {
2   "properties": {
3     "roleName": "",
4     "description": "",
5     "assignableScopes": [
6       "/subscriptions/9512788d-90b2-42d7-aa25-f172e4969c82/resourceGroups/ArubaE
7     ],
8     "permissions": [
9       {
10        "actions": [
11          "Microsoft.Compute/virtualMachines/read",
12          "Microsoft.Compute/virtualMachines/write",
13          "Microsoft.Compute/virtualMachines/delete",
14          "Microsoft.Compute/virtualMachines/start/action",
15          "Microsoft.Compute/virtualMachines/powerOff/action",
16          "Microsoft.Compute/virtualMachines/redeploy/action",
17          "Microsoft.Compute/virtualMachines/restart/action",
18          "Microsoft.Compute/virtualMachines/retrieveBootDiagnosticsData/action",
19          "Microsoft.Compute/virtualMachines/deallocate/action",
20          "Microsoft.Compute/virtualMachines/generalize/action",
21          "Microsoft.Compute/virtualMachines/capture/action",
22        ]
23      }
24    ]
25  }
26}
```

```

67 "Microsoft.Compute/images/read",
68 "Microsoft.Compute/images/write",
69 "Microsoft.Compute/images/delete",
70 "Microsoft.Resources/subscriptions/resourceGroups/read",
71 "Microsoft.Resources/subscriptions/resourceGroups/write",
72 "Microsoft.Resources/deployments/validate/action",
73 "Microsoft.Resources/deployments/write",
74 "Microsoft.Resources/subscriptions/providers/read",
75 "Microsoft.StoragePool/register/action",
76 "Microsoft.StoragePool/unregister/action"
77 ],
78     "notActions": [],
79     "dataActions": [],
80     "notDataActions": []
81   }
82 ]
83 }
84 }
```

9. Click **Save**.
10. Click the **Assignable scopes** tab. Verify that the resource group you created is added as an assignable scope and **Type** is set to the resource group.
11. Click the **Permissions** tab. Verify that the permissions, descriptions, and permission types you added are listed.
12. Click **Review + create**.
13. Click **Create**.  
A message displays to confirm that you have successfully created your custom role. Continue to [Assign the Custom Role to the Resource Group below](#).

### Assign the Custom Role to the Resource Group

1. Navigate to the Resource Group you created, and then click **Access control (IAM)**.
 

**TIP** If you just completed the previous task of creating a custom role, the Access control (IAM) page is already open.
2. Click **Add**, and then click **Add role assignment**.  
The Role assignment page opens.
3. On the **Role** tab, enter the name of your custom role.  
**TIP** If the role you created is not displayed, refresh the page.
4. Select the custom role, and then click **Next**.  
The Members tab opens.
5. Ensure that **User, group, or service principle** is selected, and then click **+ Select members**.  
The Select members page opens.

6. Enter the name of your **App registration (Service Principle)**, and then select your app and click **Select**.  
Your app is added under Members.
7. Click **Review + assign**.
8. Click **Review + assign** again.  
You have successfully assigned your custom role to the resource group. Continue to [Add the Azure Subscription to Orchestrator below](#).

## Add the Azure Subscription to Orchestrator

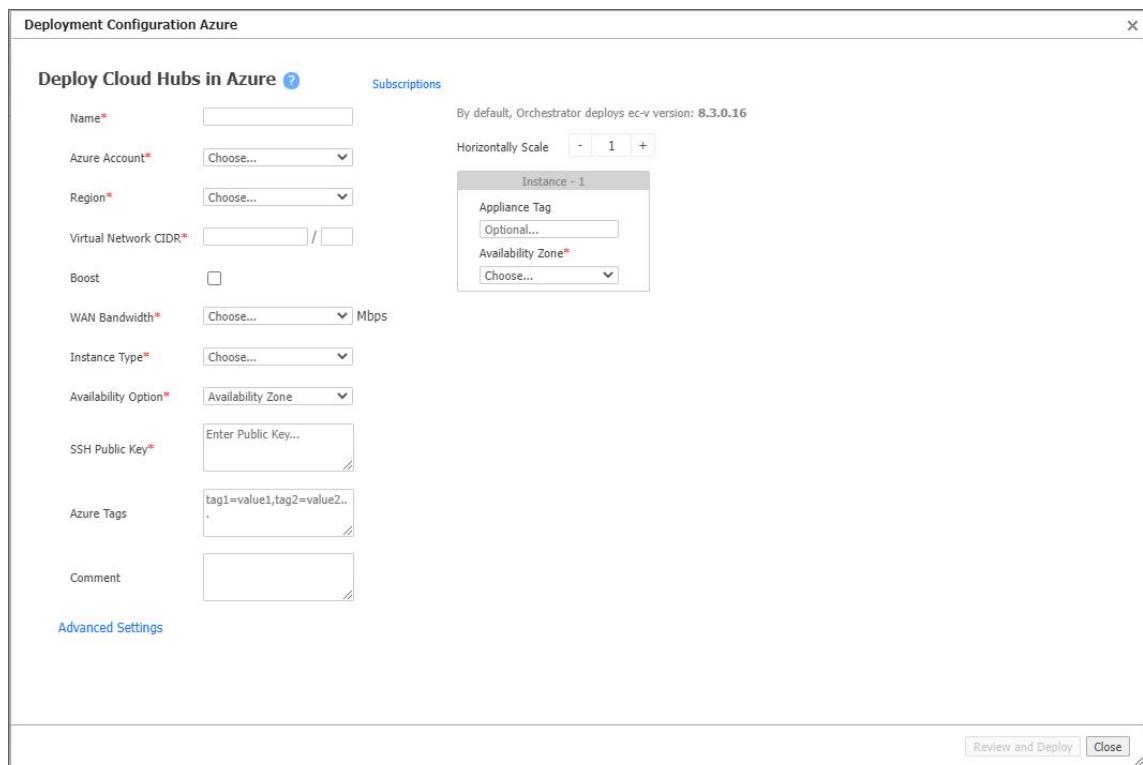
To add the Azure subscription to Orchestrator:

1. Log in to Orchestrator.
2. Click **Configuration > IaaS > Cloud Hubs in Azure**.
3. Click **Azure Subscriptions**.
4. Click **Add Azure Subscriptions**.
5. Enter the Subscription ID, Tenant ID, Client ID, and Client Secret for the Azure subscription.  
**NOTE** If you copy and paste the subscription ID, Azure might add a blank space to the beginning of the subscription ID. Be sure to remove all spaces from your subscription ID.
6. Click **Save**.  
Orchestrator validates the subscription information.

## Deployment Configuration Azure

Use the Deployment Configuration Azure dialog box to create one or more EC-V instances in Azure.

**NOTE** If you do not have an Azure subscription configured in Orchestrator, the Azure Deployment Configuration dialog box is blank. Click the **Subscriptions** link to create an Azure subscription.



Field	Description
<b>Name</b>	Enter a name for the deployment. This name is used only for identifying the deployment. A deployment consists of one or more EC-Vs that an Orchestrator creates in an Azure Virtual Network. Only alphabetical letters and hyphens are allowed in the deployment name. The maximum allowed length is 20 characters.
<b>Azure Account</b>	Select an Azure account to use for deploying the EC-V.
<b>Region</b>	Select an Azure region where you want to deploy the EC-V.
<b>Virtual Network CIDR</b>	Enter a Virtual Network Classless Inter-Domain Routing (CIDR) block. The smallest supported CIDR block is /24 and the largest supported CIDR block is /16. Orchestrator creates all Azure resources required for the EC-V deployment within this virtual network. For each EC-V you deploy, Orchestrator creates three subnets that are /28 in size. In other words, if you deploy two EC-Vs, Orchestrator creates six subnets in total. This is true even if both EC-Vs are created in a single Availability Set or Availability Zone.
<b>Boost</b>	After Boost and an appropriate WAN Bandwidth value are selected, Orchestrator displays the appropriate Azure instance types for the deployment on the Instance Type menu. <b>NOTE</b> Selecting Boost does not enable Boost on the EC-V. It only allows Orchestrator to display appropriate Azure instance types that can support Boost for the selected WAN bandwidth. To enable Boost on the EC-V, go to the Deployment page and the Business Intent Overlay (BIO) page after the deployment is complete.
<b>WAN Bandwidth</b>	The WAN bandwidth list displays the current EdgeConnect license tiers. After you select a WAN Bandwidth value, Orchestrator displays the appropriate Azure instance types for the deployment in the Instance Type list.

Field	Description
<b>Instance Type</b>	Based on your selected Boost and WAN Bandwidth values, Orchestrator displays the appropriate instance types.
<b>Availability Option</b>	Select <b>Availability Set</b> or <b>Availability Zone</b> . Some regions only support Availability Set. Aruba recommends selecting Availability Zone, if it is available.
<b>SSH Public Key</b>	Generate a public key with an application, such as PutTYgen, and then input the value here. <b>IMPORTANT:</b> EdgeConnect only supports single-line SSH public keys. <i>Do not use multi-line SSH public keys.</i>

**Use this:**

```

12 ssh-rsa
AAAAAB3NzaC1yc2EAAAABJQAAQEAqIb+GIxoVXoh5B++gi0VaPgtOnqjtYDcjztBoOP3caB9DS
cm0o5qG6Um+UzhaAp8B+K92rHMfbjThHu+PfH9TxFcfoU8NPQCcGoqqUpwp8qmNW5h1LILMr9
2If+9SEum2H8IuMJAWj6NoDpLGHyHGOV519Yn8uS3VuFru7vbCoN9vjfsZKPqEzB6mJoKXNYQq
/68ITX/QBgmpsDxkwMVsZTgD/gsp/+XC/GHLNAHOTkxwCfJ9fi1733/dtT GhhGhh7i2xpWBulc
KDcy4vjo90JOB8PcAkk9SrtwBsmrQJp2SnwwaDPzoNKli0zr5zRz4SQZulnobHoM8AZOZsJgnQ
== rsa-key-20220119

```

**Not this:**

```

1 ----- BEGIN SSH2 PUBLIC KEY -----
2 Comment: "rsa-key-20220119"
3 AAAAB3NzaC1yc2EAAAABJQAAQEAqIb+GIxoVXoh5B++gi0VaPgtOnqjtYDcjztBoOP3caB9DS
4 cm0o5qG6Um+UzhaAp8B+K92rHMfbjThHu+PfH9TxFcfoU8NPQCcGoq
5 quUpwp8qmNW5h1LILMr92If+9SEum2H8IuMJAWj6NoDpLGHyHGOV519Yn8uS3VuF
6 ru7vbCoN9vjfsZKPqEzB6mJoKXNYQq/68ITX/QBgmpsDxkwMVsZTgD/gsp/+XC/
7 GHLNAHOTkxwCfJ9fi1733/dtT GhhGhh7i2xpWBulcKDcy4vjo90JOB8PcAkk9Srtw
8 BsmrQJp2SnwwaDPzoNKli0zr5zRz4SQZulnobHoM8AZOZsJgnQ==
9 ----- END SSH2 PUBLIC KEY -----

```

**NOTE** Save the private key file. If you need to log in via SSH to the appliance after it is deployed, you will need this key.

<b>Azure Tags (Optional)</b>	Any comma-separated tags entered here are applied to all Azure resources that Orchestrator creates while deploying the EC-V. If you do not enter any tags, Orchestrator automatically creates a unique tag for each Azure resource that it creates while deploying the EC-V. This Azure tag is created to identify each resource created by Orchestrator. The tag is formatted as follows: <i>sp-automated-deployment name-instance-index-resource name</i> .
<b>Comment (Optional)</b>	Enter an optional comment if you want to attach any additional details for the deployment.
<b>Advanced Settings</b>	<b>Custom VHD:</b> Leave this field blank unless you have an EdgeConnect VHD that you want to use for the deployment. When this field is blank, the Azure Marketplace image is deployed.
<b>Horizontal Scale</b>	You can deploy multiple EC-Vs by clicking + and selecting the Availability Set or Availability Zone for each EC-V. If the selected region supports multiple Availability Zones, each Availability Zone displays on the menu. You can deploy up to 5 EC-Vs with a CIDR block of /24. If you need to deploy more than five EC-Vs within a single virtual network, select a virtual network CIDR block that is bigger than /24, such as /23 or /22. The maximum number of EC-Vs you can deploy within a single network is 20.

Field	Description
<b>Appliance Tag (Optional)</b>	Enter an Appliance Tag. If this field is left blank, Orchestrator automatically assigns an Appliance Tag for its own configuration purposes.
<b>Availability Zone</b>	Enter the Azure Availability Zone for the EC-V. <b>NOTE</b> This field only displays if the region supports Availability Zones.

When you have completed all the required fields, click **Review and Deploy**. Review the configuration summary, and then click **Deploy** to create the EC-V instances.

## Cloud Hubs in GCP

*Configuration > Cloud Services > IaaS > Deploy Cloud Hubs in GCP*

The Cloud Hubs in GCP tab provides the Google Cloud Platform account details and EC-V deployment configuration details for all cloud EC-Vs that have been deployed.

Use this tab to:

- Add and modify GCP accounts
- Deploy EC-Vs in GCP
- Manage EC-V instances deployed in GCP

**NOTE** Before you deploy EC-Vs to the GCP cloud, you must perform several tasks in GCP. For more information, see [GCP Account Configuration on page 427](#).

The following table describes each field on this tab.

Field	Description
<b>Project</b>	Project ID for the EC-V deployment.
<b>Region</b>	GCP Region in which the EC-V instance was deployed.
<b>Zone</b>	GCP zone in which the EC-V was deployed.
<b>Tag</b>	Appliance tag for an EC-V instance. If not configured, this value is automatically assigned.
<b>Status</b>	Status of an EC-V instance deployed in GCP. If more information is available, an info icon is displayed. <b>NOTE</b> If the deployment failed for the selected instance, the info dialog contains a link to download the log file and steps to resolve the issue.
<b>Terminate</b>	To terminate an EC-V instance in GCP, click <b>Terminate</b> . This action deletes all resources associated with the selected EC-V instance.
<b>Deployment Info</b>	Click the info icon in this column to view details of the selected EC-V instance, including the IP addresses associated with the mgmt0, wan0, and lan0 interfaces.

Field	Description
<b>Resources</b>	Click the info icon in this column to view details about all GCP resources that Orchestrator created during the deployment for the selected EC-V instance.
<b>Info</b>	The appliance hostname after it has been approved and added to Orchestrator. If an appliance has not been approved, this column will be blank.
<b>Comment</b>	Comments that were added to the deployment when the EC-V was created. To edit the comment, click the edit icon.

## Add or Modify a GCP Account

To add or modify a GCP account to Orchestrator:

1. Click **GCP Service Accounts**.

The GCP Service Accounts dialog box opens.

2. Click **New GCP Account** or click the edit icon next to the account you want to edit.

The GCP Account Configuration dialog box opens.

3. Complete or modify the elements as necessary.

## Deploy a New EC-V

To deploy one or more EC-V instances in GCP, click **New Deployment**.

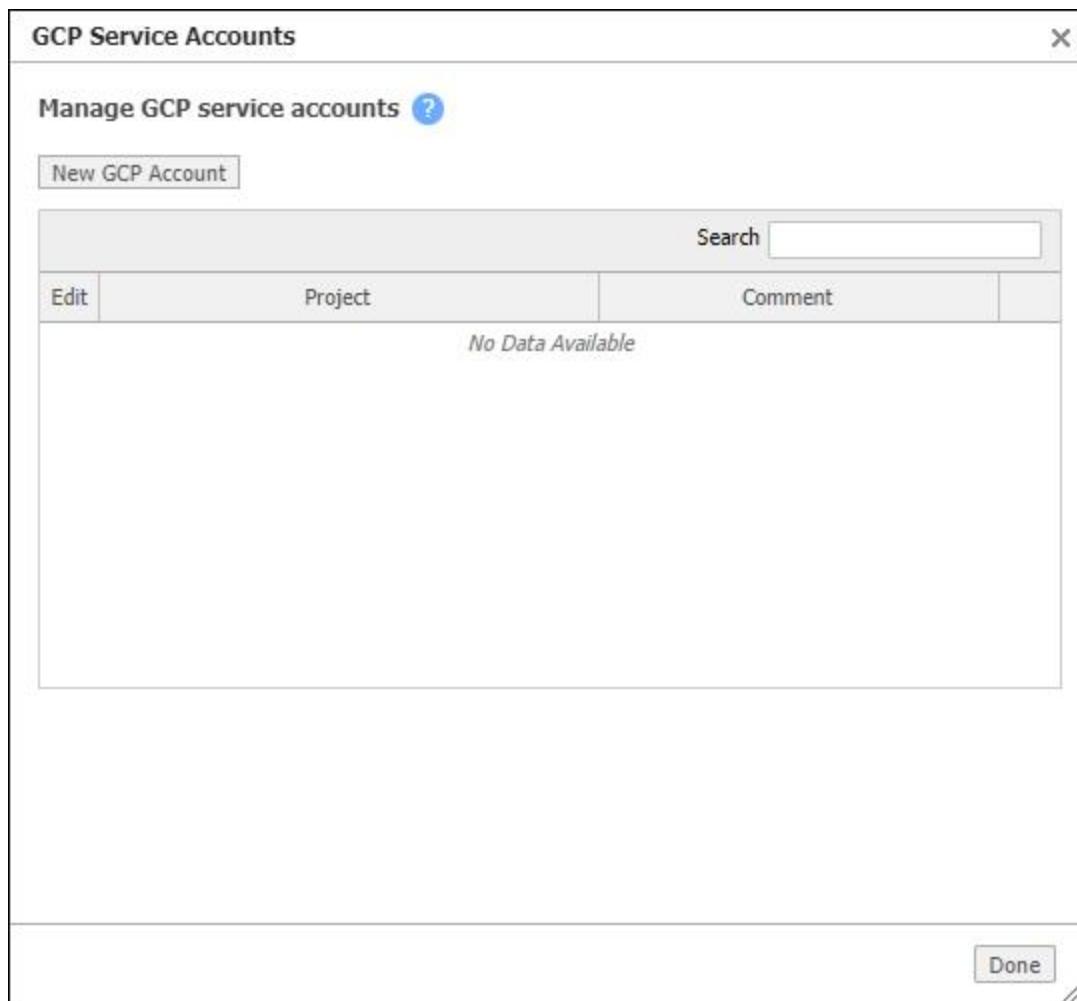
## Manage an EC-V

If a deployment does not complete or you no longer want the EC-V in the GCP cloud, you can remove the deployment and all associated artifacts.

To remove a deployment, locate the deployment you want to remove, and then click **Terminate** in that row.

## GCP Accounts

The GCP Service Accounts dialog box lists all of the GCP accounts that have been added.



- To create a new account for EC-V deployments, click **New GCP Account**.
- To modify an existing account's details, click the edit icon next to the account.

## GCP Account Configuration

Complete the following steps to create an GCP user account with the required permissions for creating EC-V instances in GCP.

### Create a GCP Project

1. Log in to GCP (<https://cloud.google.com>).
2. On the right-side menu, hover over **IAM & Admin**, and then click **Create a Project**.
3. Enter a project name and location, and then click **Create**.

### Enable GCP APIs

This section explains how to enable two different APIs required for creating EC-V instances in GCP.

## Enable Compute Engine API

1. On the right-side menu, hover over **APIs & Services**, and then click **Library**.
2. In the search bar, search for **Compute Engine API**.
3. Click **Compute Engine API**.
4. Click **Enable**.

## Enable Google Cloud Resource Manager API

1. On the right-side menu, hover over **APIs & Services**, and then click **Library**.
2. In the search bar, search for **Cloud Resource Manager API**.
3. Click **Cloud Resource Manager API**.
4. Click **Enable**.

## Create a Custom Role

This section explains how to create a custom role and attach permissions in GCP. There are two ways to do this. Select one of the following options (you do not need to do them both):

- [Create a Custom Role Using Google Cloud Shell](#) (Recommended)
- [Create a Custom Role Using Google Cloud Console](#)

### Create a Custom Role Using Google Cloud Shell (Recommended)

1. In Google Cloud, click the **Activate Cloud Shell** icon on the top menu bar.
2. Paste the following into the command line, making sure to replace the **<PROJECT NAME>** variable with the project name you created above:

```
gcloud iam roles create CustomRoleForArubaOrchestrator --  
project=<PROJECT NAME> --title="Custom Role for Aruba Orchestrator"  
--description="Custom Role for Aruba Orchestrator." --  
permissions="compute.disks.create,compute.firewalls.create,compute.  
firewalls.delete,compute.firewalls.get,compute.images.get,compute.i  
nstances.create,compute.instances.delete,compute.instances.get,comp  
ute.instances.setMetadata,compute.networks.create,compute.networks.  
delete,compute.networks.get,compute.networks.updatePolicy,compute.r  
egions.list,compute.subnetworks.create,compute.subnetworks.delete,c  
ompute.subnetworks.get,compute.subnetworks.use,compute.subnetworks.  
useExternalIp,compute.zones.get" --stage=GA
```

3. Exit Cloud Shell and verify that **Custom Role for Aruba Orchestrator** is enabled in the list of roles for your project.

## Create a Custom Role Using Google Cloud Console

1. On the right-side menu, hover over **IAM & Admin**, and then click **Roles**.
2. Click **Create Role**.
3. Fill in the Title and ID fields.
4. In the Role launch stage field, select **General Availability**.
5. Click **Add Permissions**.
6. Add the following permissions to the role:
  - compute.disks.create
  - compute.firewalls.create
  - compute.firewalls.delete
  - compute.firewalls.get
  - compute.images.get
  - compute.instances.create
  - compute.instances.delete
  - compute.instances.get
  - compute.instances.setMetadata
  - compute.networks.create
  - compute.networks.delete
  - compute.networks.get
  - compute.networks.updatePolicy
  - compute.regions.list
  - compute.subnetworks.create
  - compute.subnetworks.delete
  - compute.subnetworks.get
  - compute.subnetworks.use
  - compute.subnetworks.useExternallIp
  - compute.zones.get
7. On the Create Role page, verify the assigned permissions, and then click **Create**.

**NOTE** These permissions cannot be batch-added in GCP. For each entry, you must search for the permission, select the check box next to it, and then click **Add**.

## Create a GCP Service Account

1. On the right-side menu, hover over **IAM & Admin**, and then click **Service Accounts**.
2. Click the project created in the previous steps.
3. Click **Create Service Account**.
4. Enter the required information, and then click **Create and Continue**.
5. In the Select a role field, select **Custom Role for Aruba Orchestrator**, and then click **Continue**.
6. Click **Done**.

## Create a Service Account Key Pair

1. On the right-side menu, click **Service Accounts**.
2. From your project home page, click your service account from the list.
3. Click the **Keys** tab.
4. From the drop-down menu, click **Create new key**.
5. Leave the key type as **JSON**, and then click **Create**.

The .json file saves to your system.

## Add the GCP Account to Orchestrator

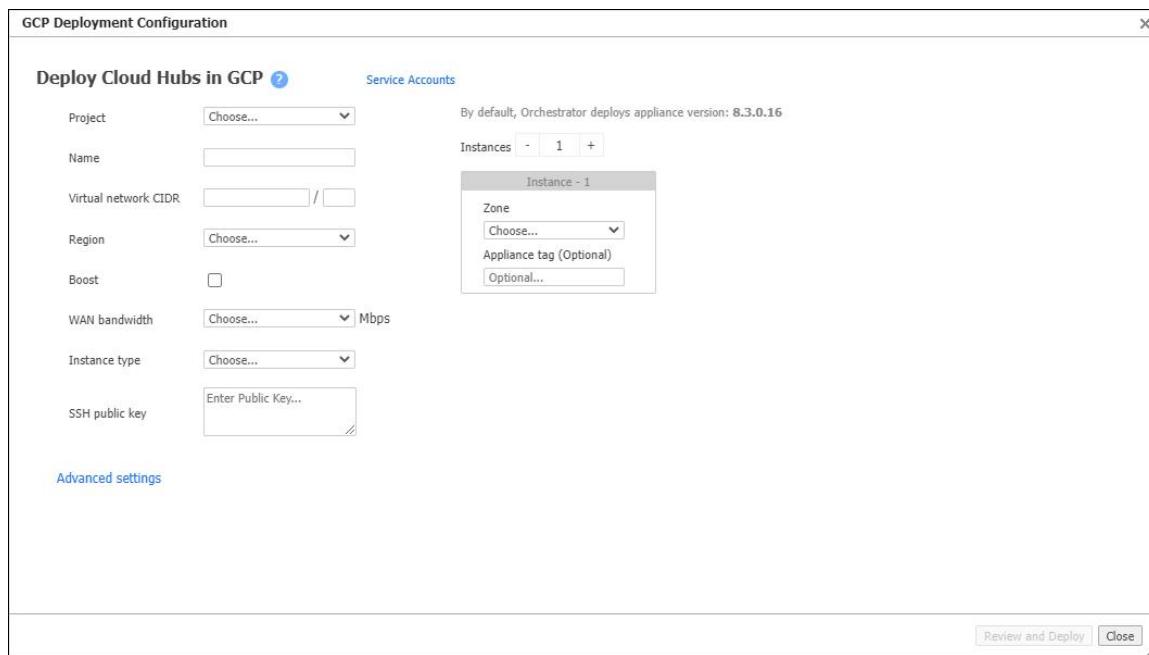
1. In Orchestrator, navigate to **Configuration > IaaS > Cloud Hubs in GCP**.
2. Click **GCP Service Accounts**.
3. Click **New GCP Account**.
4. Paste all content from the .json file saved in the previous section into the Key field, and then click **Save**.

Orchestrator validates the account information. This takes approximately 45 seconds.

## GCP Deployment Configuration

Use the GCP Deployment Configuration page to create one or more EC-V instances in a GCP region.

**NOTE** If you do not have a GCP account configured in Orchestrator, the GCP Deployment Configuration dialog box is blank. To create a GCP account, click the **Service Accounts** link.



Field	Description
<b>Project</b>	Select the GCP project created earlier in this procedure.
<b>Name</b>	Enter a name for the deployment. This name is used only for identifying the deployment. A deployment consists of one or more EC-Vs that an Orchestrator creates in GCP. Only alphanumerical letters and hyphens are allowed in the deployment name. The maximum allowed length is 20 characters.
<b>Virtual network CIDR</b>	Enter a Virtual Classless Inter-Domain Routing (CIDR) block. The CIDR block must be at least /16. Orchestrator carves out three x /26 global subnets (mgmt, wan, lan) from Virtual Network CIDR for each region. A /16 CIDR supports deploying in 300 regions. <b>NOTE</b> You only need to enter this value once per GCP project.
<b>Region</b>	Select the GCP region where you want to deploy the EC-V.
<b>Boost (Optional)</b>	Boost requires additional resources on a GCP instance. After Boost and an appropriate WAN Bandwidth value are selected, Orchestrator displays the appropriate GCP instance types for the deployment on the Instance Type drop-down menu. <b>NOTE</b> Selecting the Boost check box does not enable Boost on the EC-V. It only allows Orchestrator to display appropriate GCP instance types that can support Boost for the selected WAN bandwidth. To enable Boost on the EC-V, go to the Deployment page and the Business Intent Overlay (BIO) page after the deployment is complete.
<b>WAN Bandwidth</b>	The Bandwidth drop-down list displays the current EdgeConnect license tiers. After you select a WAN Bandwidth value, Orchestrator displays the appropriate GCP instance types for the deployment on the Instance Type drop-down menu.
<b>Instance Type</b>	Based on your selection of Boost and WAN Bandwidth values, Orchestrator displays the appropriate GCP instance types on this drop-down menu.
<b>SSH public key</b>	Enter the SSH public key for the deployment.

Field	Description
<b>Instances</b>	<b>Zone:</b> You can deploy multiple EC-Vs by clicking + and selecting the Zone for each EC-V. If the selected region supports multiple zones, each zone is shown on the drop-down menu. When deploying multiple EC-Vs, it is best practice to deploy each EC-V in a unique zone.  <b>Appliance tag (<i>Optional</i>):</b> Enter an Appliance Tag in this field if you want to assign a pre-configuration file to the deployment. If this field is left blank, Orchestrator will automatically assign an Appliance Tag for its own configuration purposes.
<b>Advanced Settings</b>	<b>Custom image:</b> If you want to deploy the EC-V with a specific public or private image, specify the image ID here. You can obtain the image ID from the GCP console.  Leave this field blank to allow Orchestrator to deploy the EC-V with the base image obtained from GCP.

When you have completed all of the required fields, click **Review and Deploy**. Review the configuration summary, and then click **Deploy** to create the EC-V instances.

# Administration

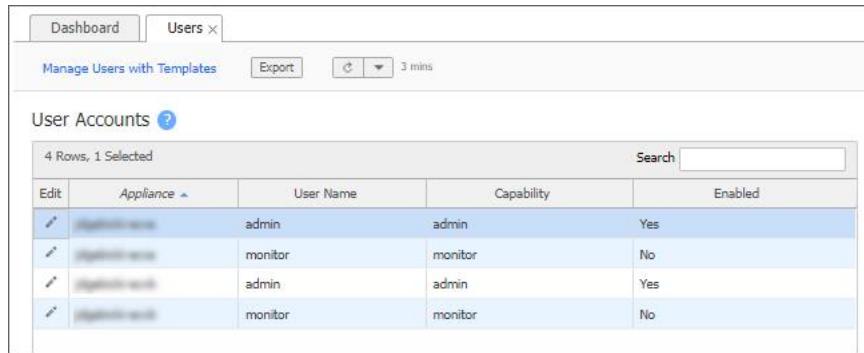
These menus are related to appliance administration. They include general settings, software management, and tools for troubleshooting and maintenance.

## General Settings

### Appliance User Accounts Tab

*Administration > General Settings > Users & Authentication > Users*

This tab provides data about the user accounts on each appliance.



The screenshot shows a user interface for managing user accounts. At the top, there are tabs for 'Dashboard' and 'Users'. Below the tabs, there are buttons for 'Manage Users with Templates', 'Export', and a refresh icon with a '3 mins' timer. The main area is titled 'User Accounts' with a help icon. It displays a table with 4 rows and 1 selected row. The table has columns: 'Edit', 'Appliance', 'User Name', 'Capability', and 'Enabled'. The data in the table is as follows:

Edit	Appliance	User Name	Capability	Enabled
<input type="checkbox"/>	edgeconnect-test	admin	admin	Yes
<input type="checkbox"/>	edgeconnect-test	monitor	monitor	No
<input type="checkbox"/>	edgeconnect-test	admin	admin	Yes
<input type="checkbox"/>	edgeconnect-test	monitor	monitor	No

The EdgeConnect appliance's built-in user database supports user names, groups, and passwords.

- Each appliance has two default user accounts, *admin* and *monitor*, that cannot be deleted.
- Each User Name belongs to one of two user groups: *admin* or *monitor*.
  - The *monitor* group supports reading and monitoring of all data, in addition to performing all actions. This is equivalent to the Command Line Interface's (CLI) *enable* mode privileges.
  - The *admin* group supports full privileges, along with permission to add, modify, and delete. This is equivalent to the CLI's *configuration* mode privileges.
- Named user accounts can be added by using the Appliance Manager or the Command Line Interface (CLI).
- User Names are case-sensitive.
- The table lists all users known to the appliances, whether or not their accounts are enabled.

### Appliance User Accounts Edit Row

This dialog box provides data about the user accounts on an appliance.

The EdgeConnect appliance's built-in user database supports user names, groups, and passwords.

- Each appliance has two default user accounts, *admin* and *monitor*, that cannot be deleted.
- Each User Name belongs to one of two user groups: *admin* or *monitor*.
  - The *monitor* group supports reading and monitoring of all data, in addition to performing all actions. This is equivalent to the Command Line Interface's (CLI) *enable* mode privileges.
  - The *admin* group supports full privileges, along with permission to add, modify, and delete. This is equivalent to the CLI's *configuration* mode privileges.
- Named user accounts can be added by using the Appliance Manager or the Command Line Interface (CLI).
- User Names are case-sensitive.
- The table lists all users known to the appliances, whether or not their accounts are enabled.

## Auth/RADIUS/TACACS+ Tab

*Administration > General Settings > Users & Authentication > Auth/RADIUS/TACACS+*

This tab displays the configured settings for **authentication** and **authorization**.

If the appliance relies on either a RADIUS or TACACS+ server for those services, those settings are also reported.

All settings are initially applied via the **Auth/RADIUS/TACACS+** configuration **template**.

### Authentication and Authorization

#### *Authentication and Authorization Fields*

Field	Description
<b>Appliance</b>	Name of the appliance selected.
<b>Authentication Order</b>	When it is possible to validate against more than one database (local, RADIUS server, TACACS+ server), <b>Authentication Order</b> specifies which method to try in what sequence: <b>Authentication Order First</b> , <b>Order Second</b> , and <b>Order Third</b> .
<b>Authorization Map Order</b>	Map ordering determines which server is used first. Select the map ordering from the drop-down list: <b>Local-Only</b> , <b>Remote-First</b> , and <b>Remote-Only</b> . The default (and recommended) value is <b>remote-first</b> .
<b>Authorization Default Role</b>	Default role assigned for authorization. The default (and recommended) value is <b>admin</b> .

Field	Description
<b>Authentication</b>	Process of validating that the end user, or a device, is who they claim to be.
<b>Authorization</b>	Action of determining what a user is allowed to do. Generally, authentication precedes authorization.
<b>Map Order</b>	Default (and recommended) value is <b>Remote First</b> .

## RADIUS and TACACS+

### *RADIUS and TACACS+ Server Fields*

Field	Description
<b>Server Type</b>	RADIUS or TACACS+.
<b>Auth Port</b>	For RADIUS, the default value is <b>1812</b> . For TACACS+, the default value is <b>49</b> .
<b>Auth Type</b>	[TACACS+] The options are <b>pap</b> or <b>ascii</b> .
<b>Timeout</b>	If a logged-in user is inactive for an interval that exceeds the inactivity time-out, the appliance logs them out and returns them to the login page. You can change that value, as well as the maximum number of sessions, in the Session Management template.
<b>Retries</b>	Number of attempts allowed before lockout.
<b>Enabled</b>	Whether or not the server is enabled.

## Auth/RADIUS/TACACS+ Edit Row

Select the Authentication Order and Authorization information in this dialog box. You can also add a RADIUS and TACACS+ Server by clicking **Add** under each section.

### Authentication Order

Choose which authentication database you want to be **First**, **Second**, and **Third** from the designated drop-down lists.

### Authorization Information

Select the Map Order and the Default Role from the designated drop-down lists.

This tab displays the configured settings for **authentication** and **authorization**.

If the appliance relies on either a RADIUS or TACACS+ server for those services, those settings are also reported.

All settings are initially applied via the **Auth/RADIUS/TACACS+** configuration **template**.

## Authentication and Authorization

### *Authentication and Authorization Fields*

Field	Description
<b>Authentication</b>	Process of validating that the end user, or a device, is who they claim to be.
<b>Authorization</b>	Action of determining what a user is allowed to do. Generally, authentication precedes authorization.
<b>Authentication Order</b>	When it is possible to validate against more than one database (local, RADIUS server, TACACS+ server), <b>Authentication Order</b> specifies which method to try in what sequence. Default is Local-first.
<b>Map Order</b>	Default (and recommended) value is <b>Remote First</b> .
<b>Default Role</b>	Default (and recommended) value is <b>admin</b> .

## RADIUS and TACACS+

### *RADIUS and TACACS+ Server Fields*

Field	Description
<b>Order</b>	Method RADIUS and TACAC+ specifies first-- <b>local first</b> .
<b>Auth Port</b>	For RADIUS, the default value is <b>1812</b> . For TACACS+, the default value is <b>49</b> .
<b>Auth Type</b>	[TACACS+] The options are <b>pap</b> or <b>ascii</b> .
<b>Enabled</b>	Whether or not the server is enabled.
<b>Retries</b>	Number of attempts allowed before lockout.
<b>Server Type</b>	RADIUS or TACACS+.
<b>Timeout</b>	If a logged-in user is inactive for an interval that exceeds the inactivity time-out, the appliance logs them out and returns them to the login page. You can change that value, as well as the maximum number of sessions, in the Session Management template.

## Date/Time Tab

*Administration > General Settings > Setup > Date/Time*

This tab highlights significant time discrepancies among the devices recording statistics.

Appliance	Time Zone	NTP Enabled	NTP servers	Appliance Date/Time	Orchestrator Delta	Browser Delta
appliance-name	UTC	Yes	time.nist.gov (Version 4)	2022/08/09 15:48:28	-51 hrs : 24 mins : 11 secs	-51 hrs : 24 mins : 11 secs
appliance-name	UTC	Yes	time.nist.gov (Version 4)	2022/08/09 15:48:28	-51 hrs : 24 mins : 11 secs	-51 hrs : 24 mins : 11 secs

If the date and time of an appliance, the Orchestrator server, and your browser are not all synchronized, charts (and statistics) inevitably have different timestamps for the same data, depending on which device you use to view the reports.

**TIP** For consistent results, configure the appliance, the Orchestrator server, and your PC to use an NTP (Network Time Protocol) server.

To specify date and time settings for your appliances, click the **Edit** icon.

### Date/Time Settings Dialog Box

Use this dialog box to configure a synchronized date and time across your Orchestrator server, appliances, and NTP server. Complete the following steps to begin.

1. From the **Time Zone** drop-down list, select the current time zone that is applicable to your network.
2. Select either Manual or NTP Time Synchronization.
  - Manual: Select either Manual or NTP Time Synchronization.
  - NTP: Click **Add**, and then enter the IP address of the NTP Server along with the version.
3. Click **Save**.

## DNS (Domain Name Servers) Tab

*Administration > General Settings > Setup > DNS*

This tab lists the Domain Name Servers that the appliances reference.

The screenshot shows the 'DNS' tab in the Aruba Orchestrator interface. At the top, there are buttons for 'Dashboard', 'DNS', 'Manage DNS with Templates', 'Export', and a refresh icon. A search bar is also present. Below the header, a table titled 'DNS' lists two rows of configuration data. The columns are: Edit, Appliance, Primary DNS IP addr, Primary Source I..., Primary Segment..., Secondary DNS IP ad..., Secondary Sourc..., Secondary Segm..., Tertiary DNS IP addr, Tertiary Source I..., Tertiary Segment..., and Domain Names. The first row has 'Appliance' as 'appliance-000001', 'Primary DNS IP addr' as 'any', 'Primary Source I...' as 'Default', 'Secondary DNS IP ad...' as 'any', 'Secondary Sourc...' as 'Default', and 'Domain Names' as ' '. The second row has similar values. An 'Edit' icon is visible next to the first row.

A **Domain Name Server** (DNS) uses a table to map domain names to IP addresses. So, you can reference locations by a domain name, such as *mycompany.com*, instead of using the IP address.

Each appliance can support up to three name servers.

Field	Description
<b>Appliance</b>	Name of the appliance.
<b>Primary DNS IP addr</b>	IP address of the DNS the system uses first.
<b>Secondary DNS IP addr</b>	IP address of the DNS the system uses second.
<b>Tertiary DNS IP addr</b>	IP address of the DNS the system uses last.

Click the edit icon to add the three domain name servers.

### DNS (Domain Name Servers) Edit Row

On this dialog box, you can configure up to three name servers. Enter the three server DNS IP addresses, and then click **Add** to apply the name to the domain.

## SNMP Tab

### Administration > General Settings > Setup > SNMP

This tab summarizes the **SNMP** configuration for each of the selected appliances.

The screenshot shows the 'SNMP' tab in the Aruba Orchestrator interface. At the top, there are buttons for 'Dashboard', 'SNMP', 'Manage SNMP with Templates', 'Export', and a refresh icon. A search bar is also present. Below the header, a table titled 'SNMP' lists two rows of configuration data. The columns are: Edit, Appliance, Enable SNMP Agent, Enable SNMP Traps, Enable SNMP V1/V2, Enabled V3 Users, Trap Receiver 1, Trap Receiver 2, and Trap Receiver 3. The first row has 'Appliance' as 'appliance-000001', 'Enable SNMP Agent' as 'No', 'Enable SNMP Traps' as 'No', 'Enable SNMP V1/V2' as 'No', 'Enabled V3 Users' as ' ', 'Trap Receiver 1' as ' ', 'Trap Receiver 2' as ' ', and 'Trap Receiver 3' as ' '. The second row has similar values. An 'Edit' icon is visible next to the first row.

## SNMP Overview

EdgeConnect appliances support Management Information Base (MIB-II) as described in RFC 1213 for cold start traps, warm start traps, and EdgeConnect private MIBs. Appliances issue an SNMP trap during reset when loading a new image, recovering from a crash, or rebooting.

An appliance sends a trap every time an alarm is raised or cleared. Traps contain additional information about alarms, including severity, sequence number, a text-based description of the alarm, and the time the alarm was created. For more information, you can download a .zip archive containing supported MIBs at <https://www.arubanetworks.com/techdocs/sdwan/mibs/>.

## Modify SNMP Configuration

Click the edit icon to the left of an appliance row to modify the SNMP configuration.

Use this dialog box to configure the appliance's **SNMP** agent and trap receivers.

1. Select the **Enable SNMP** check box to activate configuration options for SNMP v1/v2, SNMP v3, and **Trap Receivers** details.
2. If you select the **Enable SNMP Traps** check box, the SNMP agent on the appliance sends traps to configured receivers.
3. Use the **Default Trap Community** field to specify the string the trap receiver uses to accept traps being sent to it. The default value is **public**. You can modify this value.

### SNMP v1/v2

Configure the following fields for SNMP v1 and v2c.

Field	Description
<b>Enable SNMP</b>	Allows the SNMP agent on the appliance to send traps to configured receivers.
<b>Read-Only Community</b>	The SNMP application needs to present this text string (secret) to poll the appliance's SNMP agent. The default value is <b>public</b> . You can modify this value.

## SNMP v3

For additional security, configure SNMP v3 if you want to authenticate without using clear text. To add an SNMP v3 user, click **Add** above the SNMP v3 table and configure the following properties:

Field	Description
<b>Enabled</b>	Select this check box to enable the selected user. Clear this check box to disable the user and maintain the configuration.
<b>Username</b>	Enter the username to identify the SNMP v3 user.
<b>Authentication Type</b>	Select the authentication type to use for SNMP requests from the user. <b>NOTE</b> Authentication type is required and SHA-1 is the only supported algorithm.
<b>Authentication Password</b>	Enter a password that the SNMP agent can use to authenticate requests sent by the user. <b>NOTE</b> The password must be at least 20 characters long.
<b>Privacy Type</b>	Select the encryption type to use for encrypting requests from the SNMP user. <b>NOTE</b> Encryption is required, and AES-128 is the only supported algorithm.
<b>Privacy Password</b>	Enter a password (key) to use for encrypting requests sent by the user. <b>NOTE</b> The password must be at least 20 characters long.

To delete an SNMP v3 user, click the X to the right of the entry in the table.

## Trap Receivers

To configure a trap receiver, click **Add** above the Trap Receivers table and configure the following properties:

**NOTE** You can configure up to three trap receivers per appliance.

Field	Description
<b>Host</b>	IP address of the host where traps should be sent.
<b>Version</b>	Select the SNMP version of the trap receiver.
<b>Community/Username</b>	For v1 and v2c, enter the community string the receiver should use to accept traps. If left blank, the default community string (public) is used. If a different community string is configured on the trap receiver, enter it here. For v3, specify the SNMP v3 user that is sending traps to the receiver.
<b>Enabled</b>	Select this check box to enable the receiver. Clear this check box to disable the receiver and maintain the configuration.

To delete a receiver, click the X to the right of the entry in the table.

## Flow Export Tab

*Administration > General Settings > Setup > Flow Export*

This tab summarizes how the appliances are configured to export statistical data to NetFlow and IPFIX collectors. The Flow Exporting Enabled setting allows the appliance to export the data to collectors. The appliance exports flows against two virtual interfaces—sp\_lan and sp\_wan—that accumulate the total of LAN-side and WAN-side traffic, regardless of physical interface.

To open the Flow Export Configuration dialog box, click the **Edit** icon.

## Custom Information Elements

The following tables describe the Custom Information Elements.

*Data Type: ipv4Address*

Custom IE Name and Implementation Description	Semantics	Units	Field Length (bytes)	Enterprise ID
<b>clientIPv4Address:</b> <ul style="list-style-type: none"><li>• TCP: Source ipv4 address of SYN initiator is the client.</li><li>• UDP: Source ipv4 address of the first packet is the client.</li></ul>	default		4	1
<b>serverIPv4Address</b> <ul style="list-style-type: none"><li>• TCP: Destination ipv4 address of SYN initiator is the client.</li><li>• UDP: Destination ipv4 address of the first packet is the client.</li></ul>	default		4	2
<b>connectionInitiator</b> <ul style="list-style-type: none"><li>• TCP: Source ipv4 address of SYN initiator is the connection initiator.</li><li>• UDP: Source ipv4 address of the first packet is the connection initiator.</li></ul>	default		4	7

*Data Type: unsigned8*

Custom IE Name and Implementation Description	Semantics	Units	Field Length (bytes)	Enterprise ID
<b>connectionNumberOfConnections</b> <ul style="list-style-type: none"><li>• Number of TCP connections (3-way handshake) or UDP sessions established.</li></ul>	totalCounter		1	9

Custom IE Name and Implementation Description	Semantics	Units	Field Length (bytes)	Enterprise ID
<b>connectionServerResponsesCount</b> • Currently 1.	totalCounter		1	10
<b>connectionTransactionCompleteCount</b> • Currently 1.	totalCounter		1	21

*Data Type:* `unsigned32`

Custom IE Name and Implementation Description	Semantics	Units	Field Length (bytes)	Enterprise ID
<b>connectionServerResponseDelay</b> • TCP: Round-trip time between SYN and SYN-ACK. • UDP: Round-trip time between first onward and return packet.		MS	4	11
<b>connectionNetworkToServerDelay</b> • TCP, Round-trip time between SYN and SYN-ACK. • UDP, Round-trip time between first onward and return packet. It is also called Server Network Delay (SND).		MS	4	12
<b>connectionNetworkToClientDelay</b> • TCP: Round trip between SYN-ACK and ACK. • UDP: Round-trip time between first response and second request packet. It is also called Client Network Delay (CND).		MS	4	13
<b>connectionClientPacketRetransmissionCount</b> • Currently 1.	totalCounter		4	14
<b>connectionClientToServerNetworkDelay</b> • Network Time/Network Delay is known as the round-trip time that is the summation of CND and SND. It is also called Network Delay (ND).		MS	4	15
<b>connectionApplicationDelay</b> • TCP: Round-trip time between SYN and SYN-ACK. • UDP: Round-trip time between first onward and return packet.		MS	4	16

Custom IE Name and Implementation Description	Semantics	Units	Field Length (bytes)	Enterprise ID
<b>connectionClientToServerResponseDelay</b> • Round-trip time that is the summation of CND and SND.		MS	4	17
<b>connectionTransactionDuration</b> • Flow displays the time difference between the first and last packet.		MS	4	18
<b>connectionTransactionDurationMin</b> • Flow displays the time difference between the first and last packet.		MS	4	19
<b>connectionTransactionDurationMax</b> • Flow displays the time difference between the first and last packet.		MS	4	20

*Data Type: unsigned64*

Custom IE Name and Implementation Description	Semantics	Units	Field Length (bytes)	Enterprise ID
<b>connectionServerOctetDeltaCount</b> • Server initiated byte count. If flow is lan to wan, Lan-Tx byte counter. If flow is wan to lan Lan-Rx byte counter.	deltaCounter	octets	8	3
<b>connectionServerPacketDeltaCount</b> • Server initiated byte count. If flow is lan to wan, Lan-Tx byte counter. If flow is wan to lan Lan-Rx byte counter.	deltaCounter	packets	8	4
<b>connectionClientOctetDeltaCount</b> • Server initiated byte count. If flow is lan to wan, Lan-Tx byte counter. If flow is wan to lan Lan-Rx byte counter.	deltaCounter	octets	8	5
<b>connectionClientPacketDeltaCount</b> • Server initiated byte count. If flow is lan to wan, Lan-Tx byte counter. If flow is wan to lan Lan-Rx byte counter.	deltaCounter	packets	8	6

**Data Type: String**

Custom IE Name and Implementation Description	Semantics	Units	Field Length (bytes)	Enterprise ID
<b>applicationHttpHost</b> • HTTP destination domain name.	default		variable length	8
<b>applicationCategory</b> • Application group.	default		variable length	27
<b>from-zone</b> • (Source zone) name for the flow when ZBF is configured.	default		variable length	22
<b>to-zone</b> • (Destination zone) name for the flow when ZBF is configured.			variable length	23
<b>tag</b> • User-specified readable string/tag that can be specified when the ZBF rule is configured. If "tag" is not specified, an automatic tag will be created and exported. The automatic/default tag is constructed by concatenating <from-zone>_<to-zone>_<rule priority>. For example, "lan-zone_corp-zone_10000".	default		variable length	24
<b>overlay</b> • Overlay name the zone belongs to.	default		variable length	25
<b>direction</b> • Direction of the flow: outbound or inbound.	default		variable length	26

**Flow Export Edit Row**

The following table describes the Flow Export configuration options.

Field	Description
<b>Enable Flow Exporting</b>	Move the toggle to enable or disable flow exporting.
<b>Active Flow Timeout</b>	Amount of time an active flow has been timed out (in minutes).
<b>IPFIX Template Timeout</b>	Resending of templates based on a timeout.
<b>Traffic Type</b>	Check as many of the traffic types as you want. The default is <b>WAN TX</b> .
<b>Information Elements</b>	Check <b>Firewall Zones</b> , <b>Application Performance</b> , or both.

- If you check **Firewall Zones**:
  - Orchestrator generates data based specifically on the zone-based firewalls associated with the specified flow.
  - For example: Host Name, From Zone, To Zone, Tag, Action, Direction, and so forth.
- If you check **Application Performance**:
  - Orchestrator generates data based specifically on the application performance associated with each flow.
  - For example: clientIPv4Address, serverIPv4Address, connectionInitiator, applicationHttpHost, and so forth.
  - These interfaces appear in SNMP and are, therefore, "discoverable" by NetFlow and IPFIX collectors.
  - The **Collector's IP Address** is the IP address of the device to which you are exporting the NetFlow/IPFIX statistics. The default Collector Port is **2055**.
- For more information about IPFIX and the associated Custom Information Elements (IEs), see the Custom Information Elements section in the Flow Export Tab topic in the Orchestrator User Guide.

## Logging Tab

*Administration > General Settings > Setup > Logging*

This tab summarizes the following configured logging parameters:

- *Log Settings* refers to local logging.
- *Log Facilities Configuration* refers to remote logging.

The logs keep track of alarms, events, and any other issues involving your appliances.

The following table provides more details.

Field	Description
<b>Appliance</b>	Name of the appliance associated with the recorded logs.
<b>Minimum Severity</b>	Minimum severity the issue is recorded as. For details about severity levels, see the "Severity Levels" section below this table.
<b>Log File Size Threshold</b>	Set threshold configured for the log size limit.
<b>Number of Logs to Keep</b>	Maximum number of logs to keep for the appliance.
<b>Log Stateful WAN Drops</b>	Enable to log information for discarded inbound packets, even at high-traffic rates.
<b>System</b>	Assigned log facility for System.

Field	Description
<b>Audit</b>	Assigned log facility for Audit.
<b>Firewall</b>	Assigned log facility for Firewall.
<b>Ids</b>	Assigned log facility for IDS.
<b>Remote Receiver</b>	IP address of the remote receiver applicable to the log file.
<b>Remote Receiver Minimum Severity</b>	Lowest level of severity logged for the remote log receiver. For details about severity levels, see the "Severity Levels" section below this table.
<b>Facility</b>	Log facility used for the remote log receiver.

To edit the logging configuration for one of the listed appliances, click the edit icon in the left column of the table.

## Severity Levels

In order of decreasing severity, the levels are as follows:

Severity Level	Description
<b>Emergency</b>	System is unusable.
<b>Alert</b>	Includes all alarms that the appliance generates: <b>CRITICAL</b> , <b>MAJOR</b> , <b>MINOR</b> , and <b>WARNING</b> .
<b>Critical</b>	Critical event.
<b>Error</b>	An error. This is a non-urgent failure.
<b>Warning</b>	A warning condition. Indicates an error will occur if action is not taken.
<b>Notice</b>	A normal, but significant, condition. No immediate action required.
<b>Info</b>	Informational. Used by Support for debugging.
<b>Debug</b>	Used by Support for debugging.
<b>None</b>	If you select <b>None</b> , no events are logged.

These are purely related to event logging levels, not alarm severities, even though some naming conventions overlap. Events and alarms have different sources. Alarms, when they clear, list as the ALERT level in the Event Log.

## Remote Logging

- You can configure the appliance to forward all events, at and above a specified severity, to a remote syslog server.
- A syslog server is independently configured for the minimum severity level that it will accept. Without reconfiguring, it might not accept as low a severity level as you are forwarding to it.
- Each message/event type (System / Audit / Firewall / Ids) is assigned to a syslog facility level (local0 to local7).

## Logging Edit Row

Use this dialog box to set log settings, configure log facilities, and add remote log receivers.

### Log Settings

Setting	Description
<b>Minimum severity level</b>	Minimum severity level that the system will log.
<b>Start new file when log reaches</b>	Enter the maximum size (in MB) for a log file. Orchestrator generates a new file when this maximum size is reached. Specify a size from 1 to 50.
<b>Keep at most log files</b>	Maximum number of log files to allow to be stored. Specify a value from 1 to 100.
<b>Log stateful wan-interface drops</b>	Select to log information for discarded inbound packets, even at high-traffic rates. <b>NOTE</b> Enabling this option may impact system performance.

### Log Facilities Configuration

Select the log facilities you want the System, Audit, Firewall, and IDS/IPS Events logs to use. You can choose between Local0 and Local7 for each.

### Remote Log Receivers

Click **Add** and enter the IP address of the remote log receiver you want to add. Set the other fields as appropriate.

## Banners Tab

*Administration > General Settings > Setup > Banners*

This tab lists the **banner messages** on each appliance.

The screenshot shows the 'Banners' tab interface. At the top, there are buttons for 'Dashboard' and 'Banners', and links for 'Manage Banners with Templates' and 'Export'. A search bar is also present. Below this, a table displays two rows of banner messages. The columns are labeled 'Edit', 'Appliance', 'Login Message', and 'Message of the Day'. Each row contains two entries, one for each appliance, with identical message content: 'Your Login Message' and 'Test message 5' respectively.

Banners			
2 Rows			
Edit	Appliance	Login Message	Message of the Day
	Appliance 1	Your Login Message	Test message 5
	Appliance 2	Your Login Message	Test message 5

Each appliance can have two **banner messages**:

- The **Login Message** appears before the login prompt.
- The **Message of the Day** appears after a successful login.

Click the edit icon to enter your banner message.

## Banners Edit Row

Enter your message in the boxes, and then click **Save**.

## HTTPS Certificate Tab

*Administration > General Settings > Setup > HTTPS Certificate*

The VXOA software includes a self-signed certificate that secures the communication between the user's browser and the appliance.

You also have the option to install your own custom certificate, acquired from a CA certificate authority.

Edit	Appliance	Type	Issuer	Issued To	Certificate	Expiration Date
#	Appliance Name	Self Signed	Silver Peak			
#	Appliance Name	Self Signed	Silver Peak			

### To use a custom certificate with a specific appliance:

1. Consult with your IT security team to generate a certificate signing request (CSR), and submit it to your organization's chosen SSL Certificate Authority (CA).

Examples of Certificate Authorities include GoDaddy, Verisign, Comodo, Symantec, Microsoft Entrust, GeoTrust, and so forth.

- For a list of what is supported, refer to [EdgeConnect and Orchestrator Security Algorithms](#).
- All certificate and key files must be in **PEM** format.

2. After the Certificate Authority provides a CA-verified certificate:

- If your IT security team advises the use of an Intermediate CA, use an **Intermediate Certificate File**. Otherwise, skip this file.
- Click the Edit icon next to the target appliance, and Upload the **Certificate File** from the CA.
- Upload the **Private Key File** that was generated as part of the CSR.

3. To associate the CA verified certificate for use with Orchestrator, click **Add**.

## HTTPS Certificate Edit Row

Select one of the following two options:

- **Self Signed Certificate** - The VXOA software includes a self-signed certificate that secures the communication between the user's browser and the appliance.
- **Custom Certificate** - You also have the option to install your own custom certificate, acquired from a CA certificate authority.

### To use a custom certificate with a specific appliance:

1. Consult with your IT security team to generate a certificate signing request (CSR), and then submit it to your organization's chosen SSL Certificate Authority (CA).

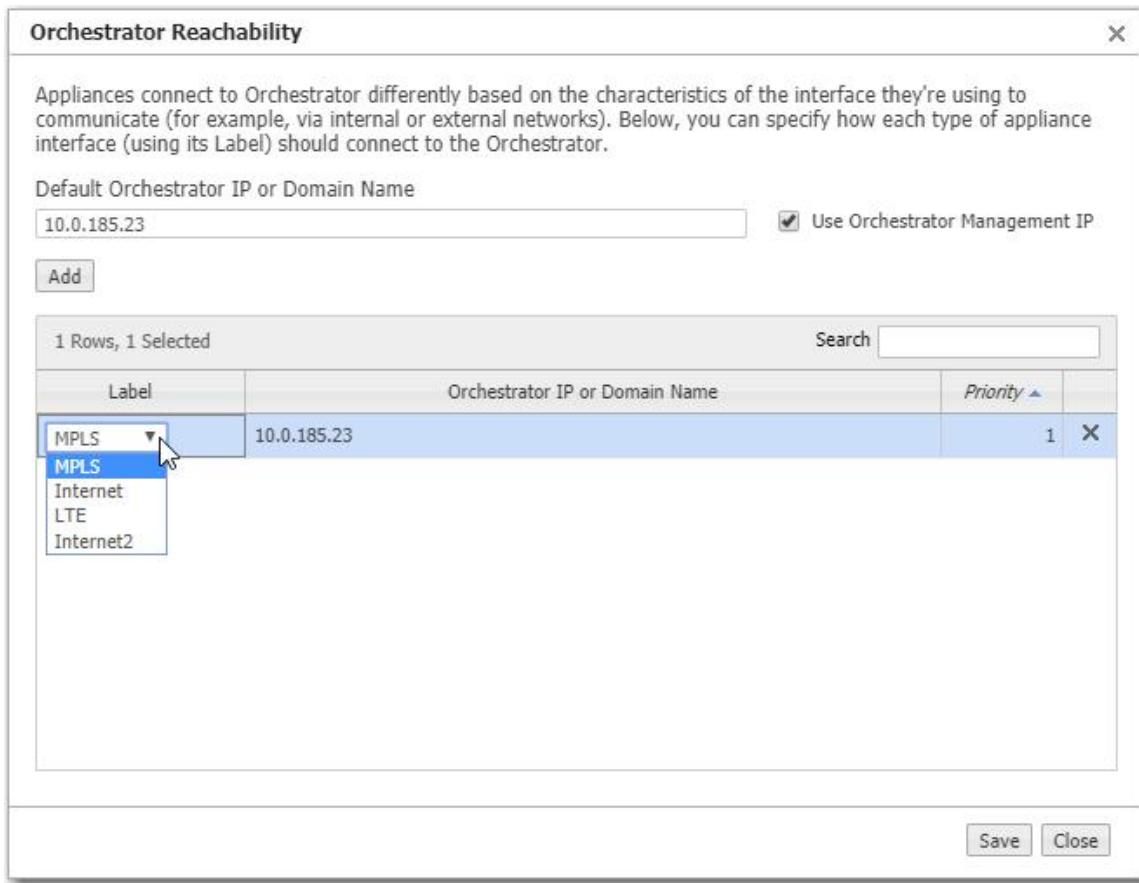
Examples of Certificate Authorities include GoDaddy, Verisign, Comodo, Symantec, Microsoft Entrust, GeoTrust, and so forth.

- For a list of what is supported, refer to [EdgeConnect and Orchestrator Security Algorithms](#).
  - All certificate and key files must be in **PEM** format.
2. After the Certificate Authority provides a CA-verified certificate:
    - If your IT security team advises the use of an Intermediate CA, use an **Intermediate Certificate File**. Otherwise, skip this file.
    - Click the Edit icon next to the target appliance, and Upload the **Certificate File** from the CA.
    - Upload the **Private Key File** that was generated as part of the CSR.
  3. To associate the CA verified certificate for use with Orchestrator, click **Add**.

## Orchestrator Reachability Tab

*Administration > General Settings > Setup > Orchestrator Reachability*

You can specify how each appliance connects to Orchestrator by designating one of its interface Labels.



## Custom Appliance Tags

*Administration > General Settings > Setup > Custom Appliance Tags*

Use this tab to create and assign tags to an appliance or a group of appliances. A tag acts as a filter or identity when searching for appliances. Complete the following steps to create a custom tag.

1. Click the edit icon.
2. Click the selected row in **Key**, and then enter the name of the tag you want to use.
3. Click the selected row in **Value**, and then enter a brief description of what the tag represents.
4. Click **Save**.

**NOTE** You can create up to eight tags.

# Software

## System Information

*Administration > Software > Upgrade > System Information*

You can manage system information with templates, except for Deployment Mode, which is an appliance-specific configuration. To change a Deployment Mode, navigate to **Configuration > Networking > Deployment**.

When you click the **Edit** icon next to a specific appliance on the System Information tab, the following two screens are available.

### System Summary

General		Configuration	
Appliance Key	1.NE	System Bandwidth	4000 Kbps
Platform	VMware	Mode	router
Uptime	2d 5h 49m 18s		
Active Release	9.0.3.0_89659		
Appliance ID	634918		
Discovery Method	PORTAL		
Connection Type	WEBSOCKET		
<b>Hardware</b>			
Appliance Model	EC-V 208001009006 Rev 76564		
BIOS Version	6.00		
Serial Number	00-1B-BC-09-B0-26		

**Apply** | **Cancel**

Property Key	Description
<b>Appliance Key</b>	Orchestrator assigns and uses this key to identify the appliance.
<b>Platform</b>	Underlying cloud platform on which the EdgeConnect appliance runs, such as Amazon EC2, Azure, Google Cloud, or VMware.
<b>Uptime</b>	Time elapsed since the appliance became operational and available.
<b>Active Release</b>	Specifies the software release the appliance is running.

Property Key	Description
<b>Appliance ID</b>	Unique identifier for the appliance.
<b>Discovery Method</b>	<p>Specifies how Orchestrator discovered the appliance:</p> <ul style="list-style-type: none"> <li>• <b>PORTAL</b> – Orchestrator discovered the appliance through the portal account.</li> <li>• <b>MANUAL</b> – The appliance was added manually.</li> <li>• <b>APPLIANCE</b> – The Orchestrator IP address was added to the appliance. Portal was not involved.</li> </ul>
<b>Connection Type</b>	Method that Orchestrator uses to communicate with the appliance. Options are WEBSOCKET, PORTAL, and HTTP.
<b>Appliance Model</b>	Specific EC, EC-V, NX, VX, or VRX model.
<b>BIOS Version</b>	Version of BIOS firmware that the appliance is using.
<b>Serial Number</b>	Serial number of the appliance.
<b>System Bandwidth</b>	Appliance's total outbound bandwidth, determined by appliance model or license.
<b>Mode</b>	Specifies the appliance's deployment mode: Server, Router, or Bridge.

## *System Settings*

**System Information - ecv**

System Summary    **System Settings** ?

**General**

Model	EC-V 208001009006 Rev 76564
Serial	001BBC09B026
Site Name	<input type="text"/>
Hub Site?	No
Contact Name	<input type="text"/>
Contact Email	<input type="text"/>
Location	Santa Clara, California, 95050, US
Region	Default

**Optimization**

IP Id auto optimization	<input type="checkbox"/>
TCP auto optimization	<input type="checkbox"/>
Flows and tunnel failure	<input type="checkbox"/> fail-stick

**Network Memory**

Encrypt data on disk	<input checked="" type="checkbox"/>
Configured Media Type	<input type="checkbox"/> ram and disk
Media Type	ram and disk

**Shell Access**

Shell Access Status	Open Shell Access
---------------------	-------------------

**Excess Flow Handling**

Excess flow policy	<input type="button" value="bypass"/>
--------------------	---------------------------------------

**NextHop Health Check**

Enable Health check	<input checked="" type="checkbox"/>
Retry count	<input type="text" value="4"/> (1..255)
Interval	<input type="text" value="10"/> (1..255) seconds
Hold down count	<input type="text" value="1"/> (1..255)

**Miscellaneous**

SSL optimization for non-IPSec tunnels	<input type="checkbox"/>
Bridge Loop Test	<input checked="" type="checkbox"/>
Enable IGMP snooping <i>(Not Available in 9.2.1.0)</i>	<input type="checkbox"/>
Auto Flow Re-Classify	<input type="checkbox"/>
Always send pass-through traffic to original sender	<input type="checkbox"/>
IPSec UDP Port	<input type="text" value="12000"/>
Enable default DNS lookup	<input checked="" type="checkbox"/>
Enable HTTP/HTTPS snooping	<input checked="" type="checkbox"/>
Quiescent tunnel keep alive time	<input type="text" value="60"/> (0..65535) seconds
UDP flow timeout	<input type="text" value="120"/> (0..65535) seconds
Non-accelerated TCP Flow Timeout	<input type="text" value="1800"/> (1..65535) secs
Maximum TCP MSS	<input type="text" value="9000"/> (500..9000) bytes
NAT-T keep alive time	<input type="text" value="300"/> (0..65535) seconds
Tunnel Alarm Aggregation Threshold Raise only 1 alarm above this threshold	<input type="text" value="5"/> Tunnel Alarms
Maintain end-to-end overlay mapping	<input checked="" type="checkbox"/>
IP Directed Broadcast	<input type="checkbox"/>
Allow WAN to WAN routing	<input checked="" type="checkbox"/>

Apply Cancel

Property Key	Description
<b>Model</b>	Specific EC, EC-V, NX, VX, or VRX model.
<b>Serial</b>	Serial number of the appliance.
<b>Site Name</b>	Orchestrator will not build tunnels between appliances with the same user-assigned site name.
<b>Hub Site?</b>	Specifies whether the appliance has been assigned the role, Hub, in Orchestrator.
<b>Contact Name</b>	Name of the person to contact within your organization (optional).
<b>Contact Email</b>	Email address of the person to contact within your organization (optional).
<b>Location</b>	Appliance location, optionally specified during appliance setup.
<b>Region</b>	User-assigned name created for segmenting topologies and streamlining the number of tunnels created. When regions contain at least one hub, you can choose to connect regions through hubs only.

Property Key	Description
<b>IP Id auto optimization</b>	Enables any IP flow to automatically identify the outbound tunnel and gain optimization benefits. Enabling this option reduces the number of required static routing rules (route map policies).
<b>TCP auto optimization</b>	Enables any TCP flow to automatically identify the outbound tunnel and gain optimization benefits. Enabling this option reduces the number of required static routing rules (route map policies).
<b>Flows and tunnel failure</b>	<p>If there are parallel tunnels and one fails, <b>Dynamic Path Control</b> determines where to send the flows. There are three options:</p> <ul style="list-style-type: none"> <li>• <b>fail-stick</b> - When the failed tunnel comes back up, the flows do not return to the original tunnel. They stay where they are.</li> <li>• <b>fail-back</b> - When the failed tunnel comes back up, the flows return to the original tunnel.</li> <li>• <b>disable</b> - When the original tunnel fails, the flows are not routed to another tunnel.</li> </ul>
<b>Encrypt data on disk</b>	Enables encryption of all the cached data on the disks. Disabling this option is not recommended.
<b>Configured Media Type</b>	Is either <b>ram and disk</b> (VX) or <b>ram only</b> (VRX). Can be changed for special circumstances if recommended by Support.
<b>Media Type</b>	Displays the actual media being used.
<b>Shell Access Status</b>	<p>Specifies the current shell access policy for EdgeConnect appliances.</p> <ul style="list-style-type: none"> <li>• <b>Open Shell Access</b> – Full access granted to the underlying Linux operating system shell.</li> <li>• <b>Secure Shell Access</b> – Access denied to the shell, but Support can grant access. Contact Support for assistance. You cannot change this setting to Open Shell Access.</li> <li>• <b>Disabled Shell Access</b> – Access permanently denied to the shell. You cannot change this setting to Open Shell Access or Secure Shell Access.</li> </ul> <p>This setting is managed on the Advanced Security Settings page (<b>Configuration &gt; Overlays &amp; Security &gt; Security &gt; Advanced Security Settings</b>). Changes to this setting affect all appliances in your network.</p>
<b>Excess flow policy</b>	Specifies what happens to flows when the appliance reaches its maximum capacity for optimizing flows. The default is to <b>bypass</b> flows. Or, you can choose to <b>drop</b> the packets.
<b>Enable Health check</b>	Activates pinging of the next hop router.
<b>Retry count</b>	Specifies the number of ICMP echoes to send without receiving a reply before declaring that the link to the WAN next hop router is down.
<b>Interval</b>	Specifies the number of seconds between each ICMP echo sent.
<b>Hold down count</b>	If the link has been declared down, this specifies how many successful ICMP echoes are required before declaring that the link to the next hop router is up.

Property Key	Description
<b>SSL optimization for non-IPSec tunnels</b>	Specifies whether the appliance should perform SSL optimization when the outbound tunnel for SSL packets is not encrypted (for example, a GRE or UDP tunnel). To enable Network Memory for encrypted SSL-based applications, you must provision server certificates in Orchestrator. This activity can apply to the entire distributed network of EdgeConnect appliances or just to a specified group of appliances.
<b>Bridge Loop Test</b>	Only valid for virtual appliances. When enabled, the appliance can detect bridge loops. If it detects a loop, the appliance stops forwarding traffic and raises an alarm. Appliance alarms include recommended actions.
<b>Enable IGMP snooping</b>	IGMP snooping is a common Layer 2 LAN optimization that filters the transmit of multicast frames only to ports where multicast streams have been detected. Disabling this feature floods multicast packets to all ports. IGMP snooping is recommended and enabled by default.
<b>Auto Flow Re-Classify</b>	Specifies how often to do a policy lookup.
<b>Always send pass-through traffic to original sender</b>	If the tunnel goes down when using WCCP and PBR, traffic that was intended for the tunnel is sent back the way it came.
<b>IPSec UDP Port</b>	Specifies the port that Orchestrator uses to build IPSec UDP tunnels. If the field is blank, Orchestrator uses the default.
<b>Enable default DNS lookup</b>	Allows the appliance to snoop the DNS requests to map domains to IP addresses. This mapping then can be used in ACLs for traffic matching.
<b>Enable HTTP/HTTPS snooping</b>	Enables a more granular application classification of HTTP/HTTPS traffic by inspection of the HTTP/HTTPS header, Host. This is enabled by default.
<b>Quiescent tunnel keep alive time</b>	Specifies the rate at which to send keep alive packets after a tunnel has become idle (quiescent mode). The default is 60 seconds.
<b>UDP flow timeout</b>	Specifies how long to keep the UDP session open after traffic stops flowing. The default is 120 seconds (2 minutes).
<b>Non-accelerated TCP Flow Timeout</b>	Specifies how long to keep the TCP session open after traffic stops flowing. The default is 1800 seconds (30 minutes).
<b>Maximum TCP MSS</b>	Maximum Segment Size. The default value is 9000 bytes. This ensures that packets are not dropped for being too large. You can adjust the value (500 to 9000) to lower a packet's MSS.
<b>NAT-T keep alive time</b>	If a device is behind a NAT, this specifies the rate at which to send keep alive packets between hosts to keep the mappings in the NAT device intact.
<b>Tunnel Alarm Aggregation Threshold</b>	Specifies the number of alarms to allow before alerting the tunnel alarm.
<b>Maintain end-to-end overlay mapping</b>	Enforces the same overlay to be used end-to-end when traffic is forwarded on multiple nodes.
<b>IP Directed Broadcast</b>	Allows an entire network to receive data that only the target subnet initially receives.
<b>Allow WAN to WAN routing</b>	Redirects inbound LAN traffic back to the WAN.

## Software Versions

*Administration > Software > Upgrade > Software Versions*

This tab lists the **software versions** on each appliance.

The screenshot shows the 'Software Versions' tab in the Orchestrator interface. At the top, there are buttons for 'Dashboard' and 'Software Versions', and links for 'Upgrade appliances software' and 'Export'. A search bar and a timer indicating '3 mins' are also present. Below this, a table displays software versions for two appliances. The columns are 'Appliance' (sorted by Active Version), 'Active Version', and 'Inactive Version'. The data is as follows:

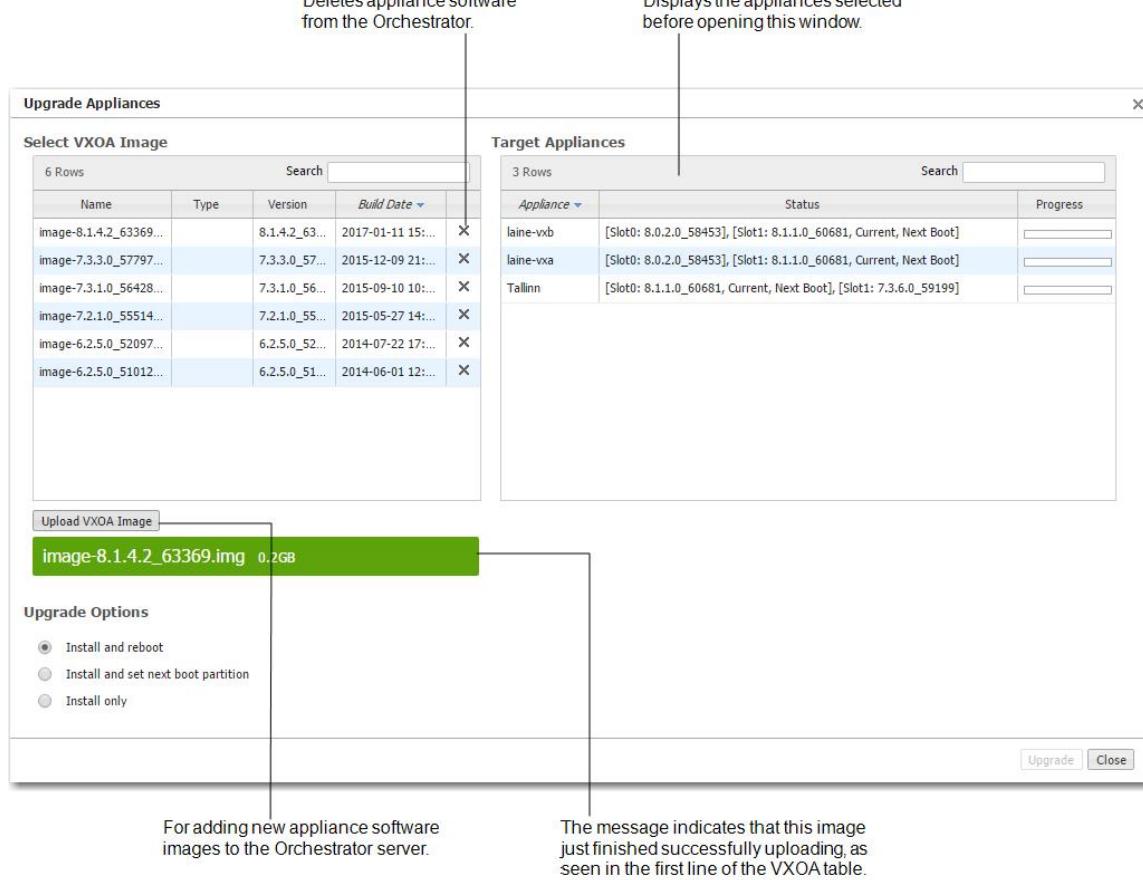
Appliance	Active Version	Inactive Version
Appliance 00000000000000000000000000000000	9.2.1.0_93911   Next Boot	9.2.0.0_93551
Appliance 00000000000000000000000000000001	9.2.1.0_93911   Next Boot	9.2.0.0_93551

## Upgrade Appliance Software

*Administration > Software > Upgrade > Upgrade Appliances*

You can download and store new appliance software from your network or computer to the Orchestrator server, staging it for installation to the appliance(s).

Use the **Upgrade Appliances** dialog box to upload appliance software to Orchestrator and to install appliance software from the Orchestrator server into the appliance's inactive partition.



- **Install and reboot** installs the image into the appliance's inactive partition and then reboots the appliance to begin using the new software.
- **Install and set next boot partition** installs the image into the appliance's inactive partition and then points to that partition for the next reboot.
- **Install only** downloads the image into the inactive partition.

## Appliance Configuration Backup

*Administration > Software > Backup & Restore > Backup Now*

Orchestrator automatically creates a weekly backup of each appliance's configuration to the Orchestrator server. Additionally, you can create an immediate backup on demand.

After selecting the appliance(s) in the appliance tree, navigate to **Administration > Software > Backup & Restore > Backup Now**, and then click **Backup**.

The screenshot shows two instances of the 'Appliance Backup' dialog box. Both dialogs have a header bar with a close button ('X') and a 'Comment' input field. Below the comment field is a search bar with a placeholder 'Search' and an empty text input.

The first dialog (top) contains a table with the following data:

Mgmt IP ▲	Appliance	Status	Duration (Sec)	Details
10.0.233.196	dall	Not started		
10.0.233.197	falcon	Not started		
10.0.238.135	Seattle-EC	Not started		
10.0.238.136	SanFran-EC	Not started		
10.0.238.181	Denver-EC	Not started		

The second dialog (bottom) contains a table with the following data:

Mgmt IP ▲	Appliance	Status	Duration (Sec)	Details
10.0.233.197	falcon	Completed	7.3	Backup for Appliance 10.0.233.197 Complet...
10.0.233.196	dall	Completed	7.4	Backup for Appliance 10.0.233.196 Complet...
10.0.238.135	Seattle-EC	Completed	6.1	Backup for Appliance 10.0.238.135 Complet...
10.0.238.136	SanFran-EC	Completed	5.7	Backup for Appliance 10.0.238.136 Complet...
10.0.238.181	Denver-EC	Completed	5.6	Backup for Appliance 10.0.238.181 Complet...

Both dialogs have a footer with 'Backup' and 'Close' buttons. A large black arrow points vertically from the top dialog to the bottom one.

You cannot delete an appliance backup from Orchestrator.

## View Configuration History

*Administration > Software > Backup & Restore > Configuration History*

- You can view an appliance's current or previous configuration.
- You can compare any two appliance configuration files.

The screenshot shows the 'Configuration History' window with the following details:

- Header:** Configuration History, Select any two records to compare.
- Table:** Shows 10 rows selected, with columns: Appliance, File Name, Backup Time, Software Versi..., File Conte..., and Comment. Each row has a 'View' button.
- Comparison Result:** A 'Compare' button is visible. Below it, two configuration snippets are shown side-by-side:
  - Left Snippet (13:00:05):**

```

1 ##
2 ## Network interface MAC assignment
3 ##
4 interface lan0 mac address
5 interface mgmt0 mac address
6 interface wan0 mac address
7
8 ##
9 ## Network interface co
10 ##
11 interface "" create
12 interface "" create
13 interface "" create
14 interface "" create
15 interface "" create
16 interface "" create
17 interface "" create
      
```
  - Right Snippet (13:00:05):**

```

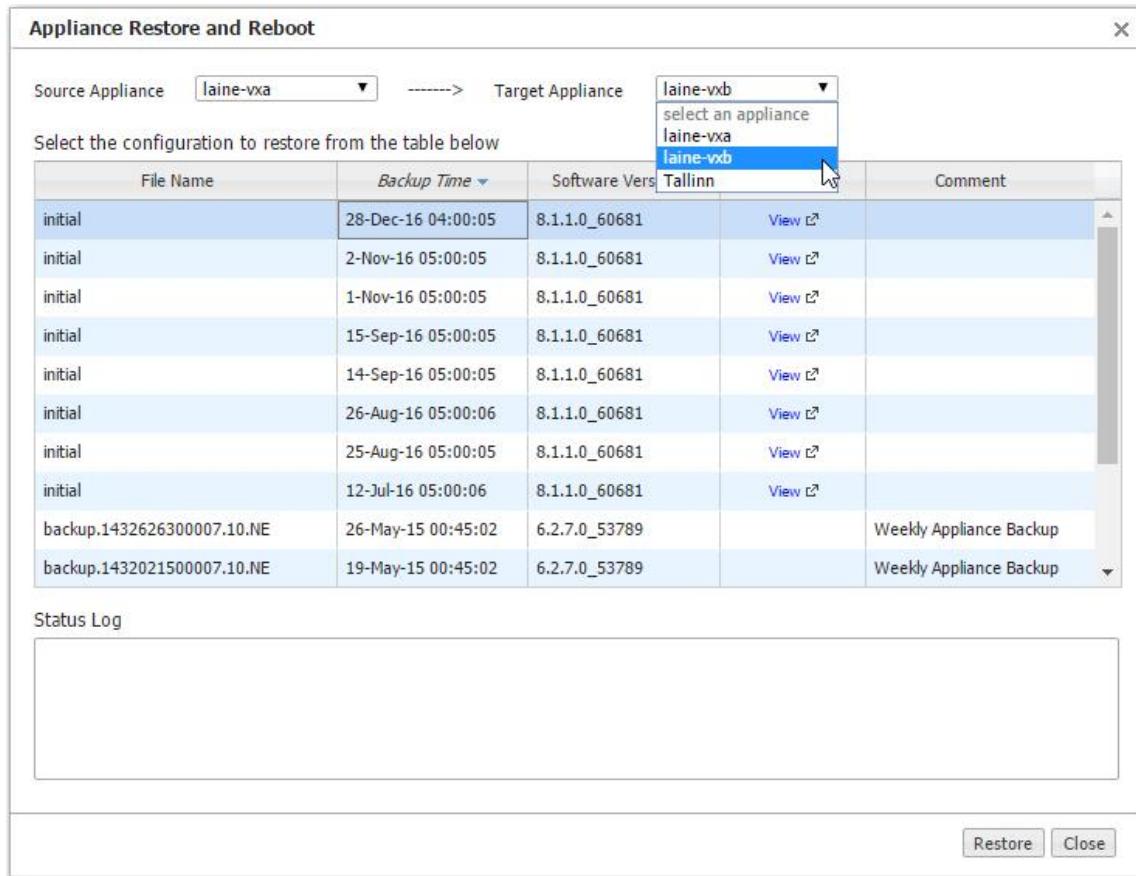
1 ##
2 ## Network interface MAC assignment
3 ##
4 interface lan0 mac address
5 interface mgmt0 mac address
6 interface wan0 mac address
7
      
```
- Backup file content:** A modal window showing the full configuration content of the selected file, including many 'interface "" create' entries.

## Restore a Backup to an Appliance

*Administration > Software > Backup & Restore > Restore*

You can restore an appliance configuration backup from Orchestrator to any other EdgeConnect appliances in your network.

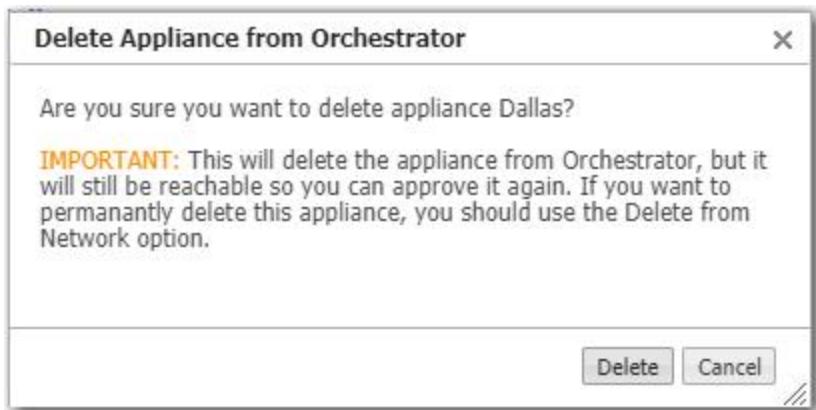
However, be careful to consider any potential conflicts when the backup specifies a static **mgmt0** IP address, as opposed to specifying DHCP.



## Remove Appliance from Orchestrator

*Administration > Software > Remove Appliances > Remove from Orchestrator*

Removing an appliance with this action returns the appliance to the **Discovered Appliances** list.



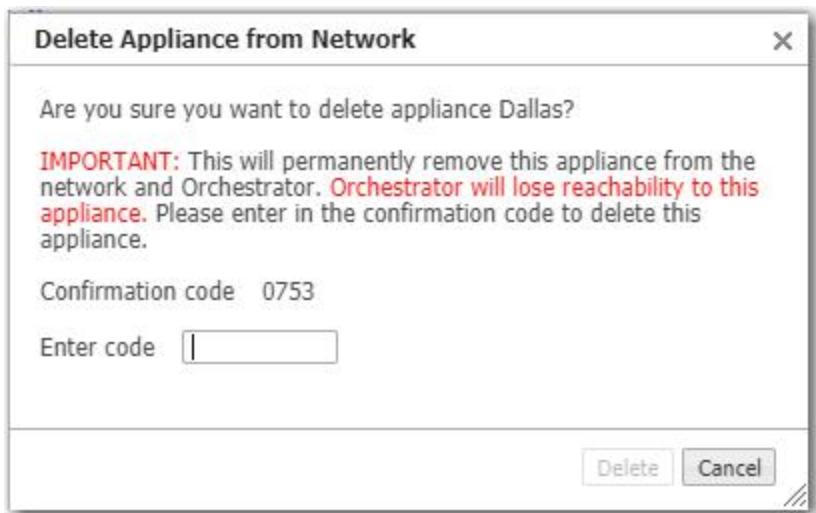
Additionally,

- It deletes the appliance from the navigation tree.
- Orchestrator will break all tunnels, overlays, and so forth to this device.

## Remove Appliance from Orchestrator and Account

*Administration > Software > Remove Appliances > Remove from Orchestrator and Account*

Removing an appliance with this action places the appliance in the **Denied Devices** list, which is located as a link in the **Configuration - Discovered Appliances** menu.



Additionally,

- It deletes the appliance from the navigation tree.
- Orchestrator will break all tunnels, overlays, and so forth to this device.
- It tells the Portal to "unlicense" the appliance.

## Tools

### Synchronize Appliance Configuration

*Administration > Tools > Synchronize*

Orchestrator keeps its database synchronized with the running configurations for the appliances.

- When you use Orchestrator to make a configuration change to an appliance's running configuration, the appliance responds by sending an **event** back to the Orchestrator server to log. This keeps Orchestrator and the appliance in sync.
- Whenever an appliance starts or reboots, Orchestrator automatically inventories the appliances to resync.
- Whenever Orchestrator restarts, it automatically resyncs with the appliances.
- When an appliance is in an **OutOfSync** management state, the Orchestrator server resyncs with it as it comes back online.

If your overall network experiences problems, you can use this dialog box to manually resync to ensure that Orchestrator has an appliance's current running configuration.

Synchronize Appliance Configuration	
Appliance ▲	Mgmt IP
laine2-vxa	10.0.238.20
laine2-vxb	10.0.238.21
laine-vxa	10.0.238.71
laine-vxb	10.0.238.69
Tallinn	10.0.236.198

[Synchronize](#) [Close](#)

## Put the Appliance in System Bypass Mode

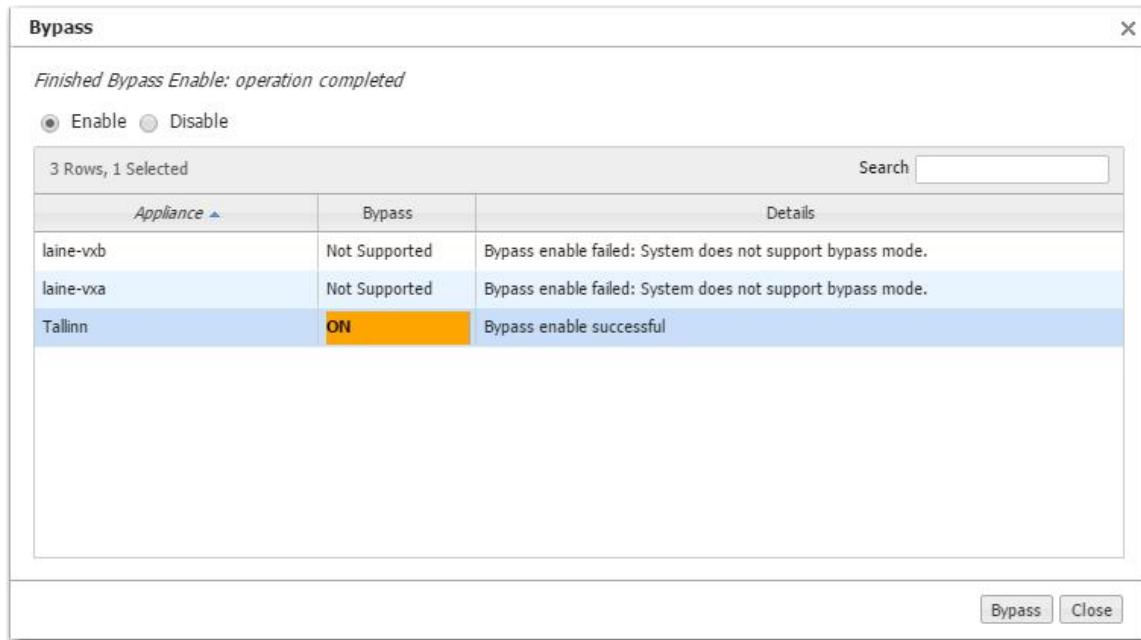
*Administration > Tools > Bypass*

System Bypass mode is only available for certain models of EdgeConnect physical appliances. Virtual appliances do not support bypass mode.

In **system bypass mode**, the fail-to-wire (or fail-to-glass) card **DOES NOT** receive or process packets.

Fail-to-wire network interfaces mechanically isolate the appliances from the network in the event of a hardware, software, or power failure. This ensures that all traffic bypasses the failed appliance and maximizes uptime.

- In an in-line deployment (Bridge mode), the **LAN** interface is physically connected to the **WAN** interface.
- In Server mode and any Router mode, the appliance is in an open-port state.



When the appliance is in Bypass mode, a message displays in red text in the upper-right corner of the user interface.



## Broadcast CLI Commands

*Administration > Tools > Broadcast CLI*

You can simultaneously apply Command Line Interface (CLI) commands to multiple, selected appliances.

The dialog box automatically provides you with the highest user privilege level.

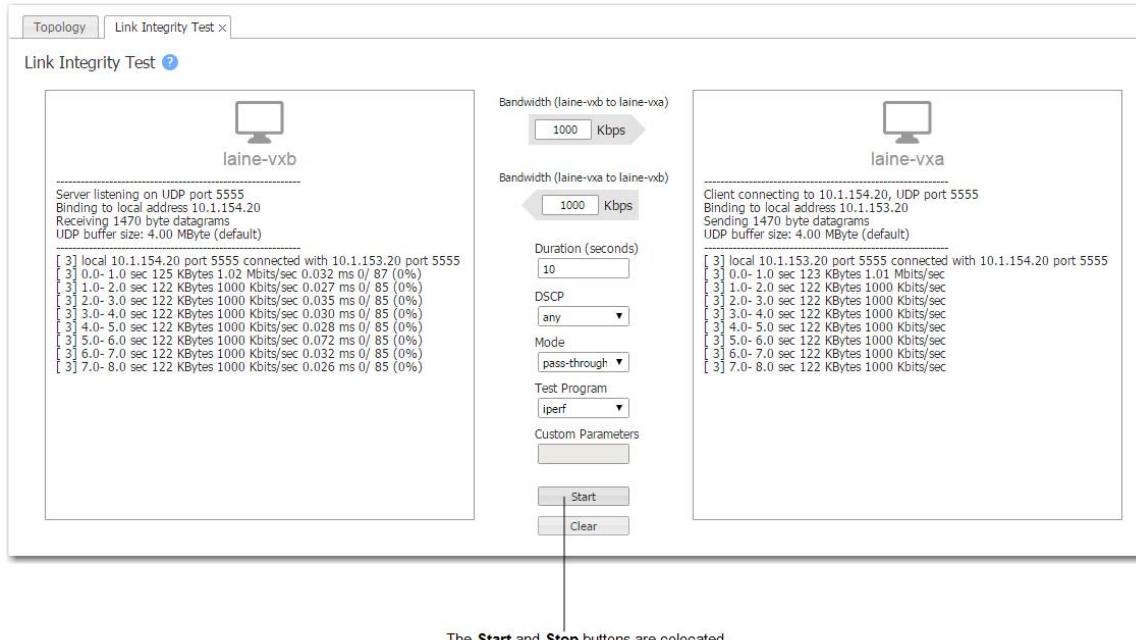


For more information, refer to the [EdgeConnect Command Line Interface \(CLI\) Reference](#).

## Link Integrity Test

*Administration > Tools > Link Integrity Test*

Used for debugging, the **link integrity** test enables you to measure the throughput and integrity (amount of loss) of your WAN link. You can run either **iperf** or **tcpperf** (Version 1.4.8).



- These tests run on the two selected appliances using user-specified parameters for bandwidth, duration, DSCP marking, and type of traffic (tunnelized / pass-through-shaped / pass-through-unshaped).
- Orchestrator runs the selected test twice—once passing traffic from Appliance A to Appliance B, and the second run passing traffic from Appliance B to Appliance A.
- **Custom Parameters** are available for **tcpiperf** and should be used cautiously by advanced users.

## TCPPERF Version 1.4.8

### Basic Mode

Option	Description
<b>-h</b>	<i>help</i>
<b>-s</b>	<i>server</i> : Run tcpperf in server mode (not applicable for file generation). Listens on TCP port 2153 by default. [server_port [server_port [server_port..]]]
<b>-sr</b>	<i>server range</i> : <server_port_start:server_port_end>
<b>-c</b>	<i>client server_IP</i> : TCPperf Server's IP address (not applicable for file generation). [server_port [server_port [server_port..]]]
<b>-cr</b>	<server_port_start:server_port_end> <server_port_start:server_port_end>
<b>-g</b>	<i>generate basfilename</i> . Dump generated data to a file.
<b>-sw</b>	<i>sgwrite conffilename</i>

### Notes:

1. The default server ports are 2153 and 2154.
2. You can specify multiple odd-numbered server ports.
3. The next even-numbered server ports will also be assigned automatically.
4. These even numbers are reserved for double connection testing (see **-I**, *interface IP*).
5. Generate mode generates a local file per flow with the same content that the client would have generated with the specified parameters.
6. SG write mode is like generate mode except that it writes to an SG device.

#### General Parameters

Option	Description
<b>-6</b>	<i>ip6</i> . Forces tcpperf to use IPv6 addresses only. Default is IPv4 addresses.
<b>-I</b>	<i>interface IP</i> : Specify source interface IP address. Default is <b>any</b> .
<b>-o</b>	<i>outname</i> : Output filename. Default is <b>stdout</b> .
<b>-u</b>	<i>update &lt;secs&gt;</i> : Frequency of printed updates in seconds. Default is <b>1</b> .
<b>-d</b>	<i>duration &lt;secs&gt;</i> : Set maximum test duration in seconds. Default is <b>infinite</b> .
<b>-w</b>	<i>wait &lt;secs&gt;</i> : Wait until <secs> since 1970 before transmitting data.
<b>-z</b>	<i>realtime</i> : Elevate to realtime priority. Requires root privilege.
<b>-cm</b>	<i>cpu mask</i> : Specify CPU affinity. Requires root privilege.
<b>-q</b>	<i>quiet &lt;level&gt;</i> : Suppresses detail based on level: <ul style="list-style-type: none"> <li>• <b>0</b>: None. Print results when test is complete.</li> <li>• <b>1</b>: Default. Periodic packet/byte statistics.</li> <li>• <b>2</b>: Verbose. Adds connection state changes.</li> <li>• <b>3</b>: Debug. Prints everything.</li> </ul>

#### TCP Parameters

Option	Description
<b>-tw</b>	<i>tcpwindow</i> . TCP window_size. Default is OS default.
<b>-tm</b>	<i>tcpmss</i> : TCP mss. Default is OS default.
<b>-tn</b>	<i>tcpnodelay</i> : TCP nodelay option. Default is nagle enabled.
<b>-tq</b>	<i>tcpquickack</i> : TCP quick ack option. Default is delayed acks.
<b>-td</b>	<i>tcpdscp &lt;cp&gt;</i> : Sets IP DSCP to <cp> (decimal). Default is <b>0</b> .
<b>-tr</b>	<i>tcpretries &lt;n&gt;</i> : Sets number of times to retry TCP connections.

Option	Description
-tp	<b>tcppace &lt;n&gt; [mode]</b> : Pace TCP connection setup rate. Limits number of half-open connections to <n>. Valid <mode> types are: <ul style="list-style-type: none"> <li>• <b>preestablish</b>: All connections are established before data transmission. Default.</li> <li>• <b>simultaneous</b>: Begin data transmission as soon as connection made.</li> </ul>
-ta	<b>tcpabort</b> : Sends RSTs instead of FINs on close.
-tf	<b>tcpfindelay &lt;secs&gt;</b> : Time to wait after all data is sent before sending FIN/RST.

### Traffic Generation Parameters

Option	Description
-f	<i>file</i> . Source filename to load. Default is <b>10MB</b> of random data.
-i	<i>test id &lt;i&gt;</i> : Set test ID. The same test ID produces the same data set. Use different test IDs to generate unique data for each test run. Default is <b>zero</b> .
-n	<i>number &lt;n&gt;</i> : Generate <n> flows. Default is <b>one</b> .
-b	<i>begin &lt;byte&gt;</i> : First byte in transmission. Default is <b>zero</b> .
-e	<i>end &lt;byte&gt;</i> : End byte in transmission (number of bytes to transmit). Default is <b>file size</b> . Begin and end bytes can be greater than file size. The content is repeated to create extra bytes.
-a	<i>antipat &lt;mode&gt;</i> : Antipattern mode: default is <b>mutate</b> . <ul style="list-style-type: none"> <li>• <b>none</b>: Repeats same content verbatim on all flows. Repeats content if end byte exceeds content size.</li> <li>• <b>mutate</b>: Ensures all flows and data repeats are unique. Preserves short range patterns within flow. Destroys cross flow similarity. Destroys original byte code distribution.</li> <li>• <b>shuffle</b>: Ensures all flows and data repeats are unique. Preserves short range patterns within flow. Preserves cross flow similarity. Preserves original byte code distribution.</li> <li>• <b>fast</b>: Ensures all flows and data repeats are unique. Does not preserve short range patterns. Destroys cross flow similarity. Destroys original byte code distribution. Uses less CPU than mutate or shuffle.</li> </ul>

Option	Description
<b>-l</b>	<p><i>loopback [mode]</i>: Loopback. Default is <b>unidirectional</b>.</p> <ul style="list-style-type: none"> <li>• <b>uni</b>: Unidirectional client to server.</li> <li>• <b>rev</b>: Unidirectional server to client.</li> <li>• <b>bidir</b>: Bidirectional, client and server independently send data on the same TCP connection.</li> <li>• <b>bidir2</b>: Bidirectional, client and server independently send data on secondary TCP connections.</li> <li>• <b>loop</b>: Bidirectional, server loops data back to client on the same TCP connection.</li> <li>• <b>loop2</b>: Bidirectional, server loops data back to client on a secondary TCP connection.</li> <li>• <b>bidir2</b>: Bidirectional, transmits one transaction at a time. Client waits for previous transaction to be echoed. Emulates transactional data.</li> </ul>
	<p>NOTES:</p> <ul style="list-style-type: none"> <li>• Content source for traffic originating at the server is determined by the server (not client) command line.</li> <li>• <b>loop2</b> and <b>bidir2</b> modes 2 x &lt;n&gt; TCP connections and requires that the server has even-numbered ports available.</li> </ul>
<b>-r</b>	<p><i>rate &lt;bps&gt;</i>: Limits aggregate transmission rate to &lt;bps&gt;. Default is <b>no rate limit</b>.</p>
<b>-t</b>	<p><i>trans &lt;min&gt; [max]</i>: Sets size of each socket transaction. Default is <b>64000</b>. If &lt;min&gt; and &lt;max&gt; are specified, client generates transactions with random sizes between &lt;min&gt; and &lt;max&gt;. This feature is often used with <b>-l</b> and <b>-r</b>. Set the minimum transaction size to 100000 to improve single-flow performance.</p>
<b>-v</b>	<p><i>verify &lt;mode&gt;</i>: Verify integrity of received data. Default is <b>global</b>.</p> <ul style="list-style-type: none"> <li>• <b>none</b>: No verification. Fastest/least CPU load.</li> <li>• <b>global</b>: Single global hash per flow. Fast, but cannot isolate an errored block.</li> <li>• <b>literal</b>: Literal comparison of data upon reception. Fast, can isolate errors to the byte level. Requires that server has same content as client. Use random data gen or same -f file at server.</li> <li>• <b>embedded</b>: Embedded hashes every 4096 bytes. Slower, can isolate errors to 4096 byte block.</li> </ul>
<b>-p</b>	<p><i>repeat &lt;n&gt;</i>: Repeat each content byte n times. Default is <b>1</b> (no repeats). Works for both random data and file content.</p>
<b>-k</b>	<p><i>corrupt &lt;n&gt; &lt;m&gt; &lt;s&gt; [&lt;%change&gt; [&lt;%insert&gt; [&lt;%delete&gt;]]]</i>: Corrupt 0 to n bytes of data every m bytes using seed s. Delta bytes will require 0.5*n/m percent overhead. Each corrupt can be a change, insert or delete with the probability of each being specifiable. The default is 33.3% changes, 33.3% inserts, and 33/3% deletes.</p>
<b>-x</b>	<p><i>excerpts &lt;b&gt; &lt;e&gt; &lt;/&gt; [&lt;s&gt;]</i>: Send random excerpts of average &lt;l&gt; length bytes from content between &lt;b&gt;egin and &lt;e&gt;nd bytes. The <b>-b</b> and <b>-e</b> options still specify total bytes to send. Uses random seed <b>s</b>.</p>

Option	Description
<b>-y</b>	<p><i>defred &lt;s%&gt; &lt;m%&gt; &lt;l%&gt; &lt;sb&gt; &lt;smin&gt; &lt;smax&gt; &lt;mb&gt; &lt;mmin&gt; &lt;mmax&gt; &lt;lb&gt; &lt;lmin lmax&gt; :</i></p> <p>Generate content based on defined reduction model.</p> <p>Content is drawn from three data sets: <b>s</b>, <b>m</b>, and <b>l</b>:</p> <ul style="list-style-type: none"> <li>• <b>s%</b>: Specifies fraction [50%] of s-type content (short term reducible).</li> <li>• <b>m%</b>: Specifies fraction [30%] of m-type content (medium term reducible).</li> <li>• <b>l%</b>: Specifies fraction [20%] of l-type content (long term reducible).</li> </ul> <p>Short term content comes from data set of sb Mbytes [100MB] with excerpts uniformly distributed between smin and smax bytes [10K-1M].</p> <p>Medium term content comes from data set of mb Mbytes [100GB] with excerpts uniformly distributed between lmin and lmax bytes [10K-1M].</p> <p>Long term content comes from data set of lb Mbytes [100TB] with excerpts uniformly distributed between smin and smax bytes [10K-1M].</p> <p>The <b>-b</b> and <b>-e</b> options still specify total bytes to send.</p> <p>Performance is best if <b>-b</b> is <b>0</b>.</p> <p>Uses random seed <b>s</b>.</p>
<b>-ssl</b> [param=value ...]	<p>Enable SSL on connection with optional parameters.</p> <ul style="list-style-type: none"> <li>• <b>version=2 3 t10 t11 t12</b>: Set the protocol version.</li> <li>• <b>cipher=OPENSSL-CIPHER-DESC</b>: Set the choice of ciphers.</li> <li>• <b>ticket=yes no</b>: Enable/disable session ticket extension.</li> <li>• <b>cert=FILENAME</b>: Use this certificate file.</li> <li>• <b>key=FILENAME</b>: Use this private keyfile.</li> <li>• <b>compression=none any deflate zlib rle</b>: Set the compression method.</li> <li>• <b>sslcert</b>: Print the SSL certificate in PEM format.</li> <li>• <b>sslkey</b>: Print the SSL key in PEM format.</li> </ul>

## Disk Management

*Administration > Tools > Disk Management*

The **Disk Management** tab lists information about physical and virtual appliance disks.

- The progress bar shows what percentage of the polling is complete.
- Physical appliances use RAID (Redundant Array of Independent Disks) arrays with encrypted disks.
- Disk failure results in a **critical alarm**.
- If a row indicates that a disk has failed, click the edit icon to access the appliance, and then follow the directions in the local help to replace the failed disk.
- You can view the SMART (Self-Monitoring Analysis and Reporting Technology) data from physical appliance disks only.

The screenshot shows the Aruba Orchestrator Disk Management interface. At the top, there are tabs for 'Dashboard' and 'Disk Management'. Below the tabs, there are buttons for 'Export' and a refresh icon with the text '1 min'. A search bar is also present. The main area is titled 'Disk Management' with a question mark icon. It displays a table with 6 rows and 1 selected row. The columns are: Edit, Appliance ▲, Appliance Model, Slot ID, Pairing Slot ID, Status, Size(GB), Serial Number, Removable, and SMART Data. The selected row is for 'Kennesaw3-' with Appliance Model 'EC-S', Slot ID '0', Pairing Slot ID '1', Status 'OK', Size '447', Serial Number '109-0119242-011...', Removable 'No', and SMART Data 'N/A'. An edit icon is shown next to the appliance name. A large black arrow points from the bottom of the main table down to a detailed SMART data view for the selected disk.

Appliance ▲	Appliance Model	Slot ID	Pairing Slot ID	Status	Size(GB)	Serial Number	Removable	SMART Data
Kennesaw3-	EC-S	0	1	OK	447	109-0119242-011...	No	(i)
Kennesaw3-	EC-S	1	0	OK	447	109-0119242-009...	No	(i)
Kennesaw6-	EC-V	0		OK	30		No	N/A
Tevatron	EC-V	0		OK	30		No	N/A
Valheim-	EC-V	0		OK	30		No	N/A
Woodstock-	EC-US	0		OK	111	W2EM120GDTAS7...	No	(i)

**Smart data for Kennesaw3- ID 0**

Attribute	Normalized Value	Worst Value	Raw Value
Read Error Rate	100	100	0
Power on hours	100	100	22,143
Device power cycle count	100	100	27
	100	100	0
Grown Failing Block Count	100	100	766
Wear Leveling Count	100	100	14,156,059
Power-off Retract Count	100	100	18
Temperature	94	77	720,929
	100	100	0
Temperature	100	100	93
Total LBAs Written	100	100	62,405

To replace a failed disk:

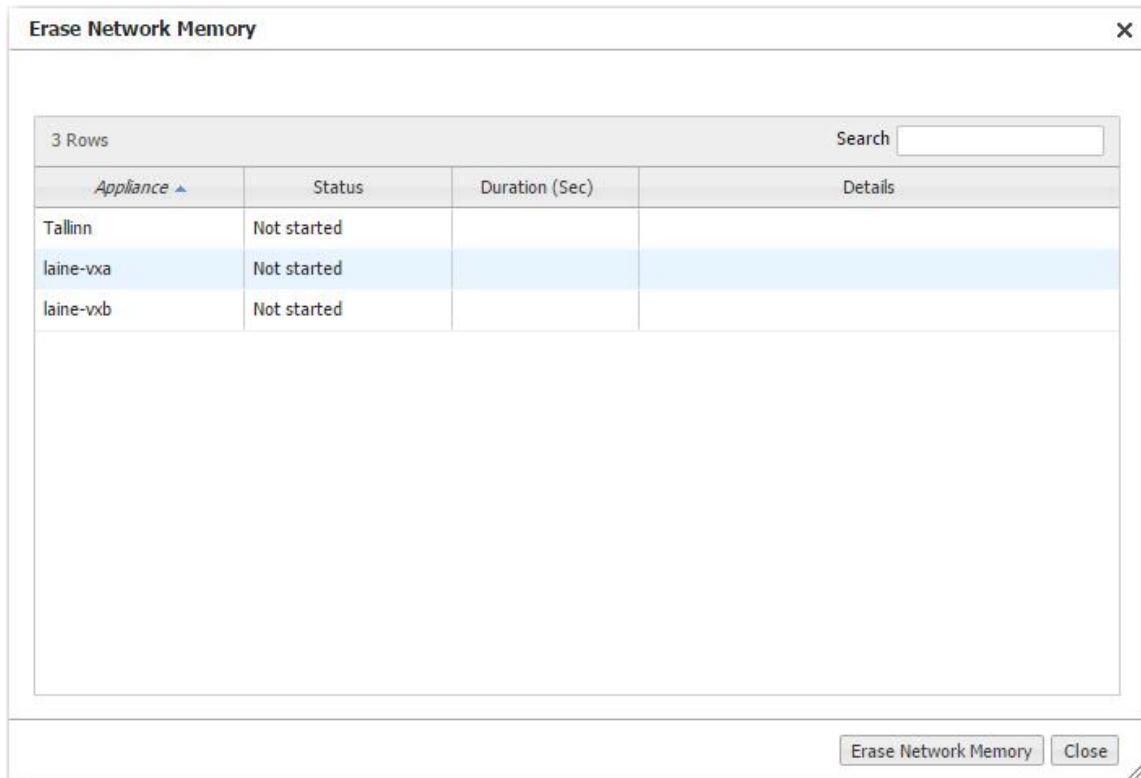
1. Log in to your Support portal account, and then click **Open a Self Service RMA** for disk replacement.
2. Complete the wizard. Use the serial number of the appliance (not the disk).
3. After you receive the new disk, access Appliance Manager by clicking any edit icon that belongs to the appliance in question.
4. Follow the instructions on that page's online help.

## Erase Network Memory

*Administration > Tools > Erase Network Memory*

Erasing Network Memory removes all stored local instances of data.

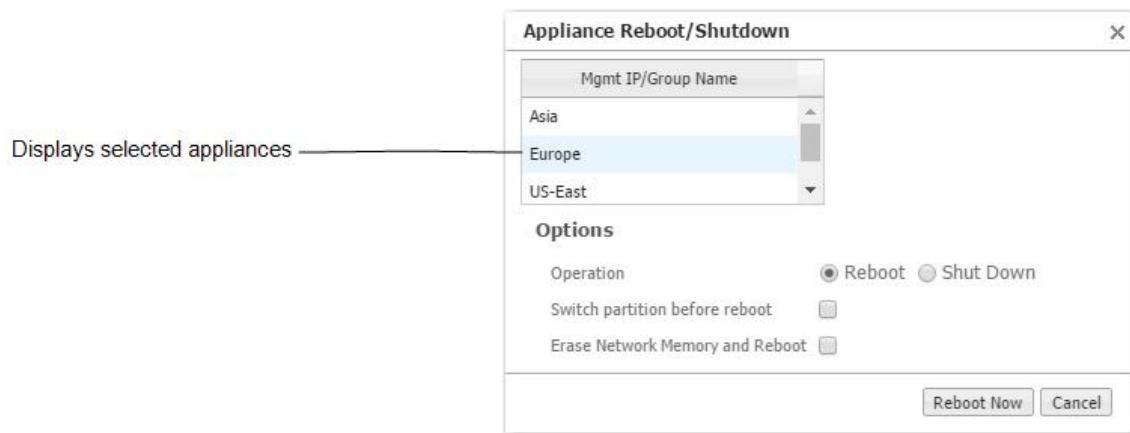
No reboot required.



## Reboot or Shut Down an Appliance

*Administration > Tools > Reboot > Appliance Reboot / Shutdown*

The appliance supports three types of reboot:



- **Reboot.** Reboots the appliance gracefully. This is your typical "vanilla" restart.

Use case: You are changing the deployment mode or other configuration parameters that require a reboot.

- **Erase Network Memory and Reboot.** Erases the Network Memory cache and reboots the appliance.

Use case: You need to restart the appliance with an empty Network Memory cache.

- **Shutdown.** Shuts down the appliance and turns the power off. To restart, go to the appliance and physically turn the power on with the Power switch.

Use case:

- You are decommissioning the appliance.
- You need to physically move the appliance to another location.
- You need to recable the appliance for another type of deployment.

## Behavior During Reboot

A *physical appliance* enters into one of the following states:

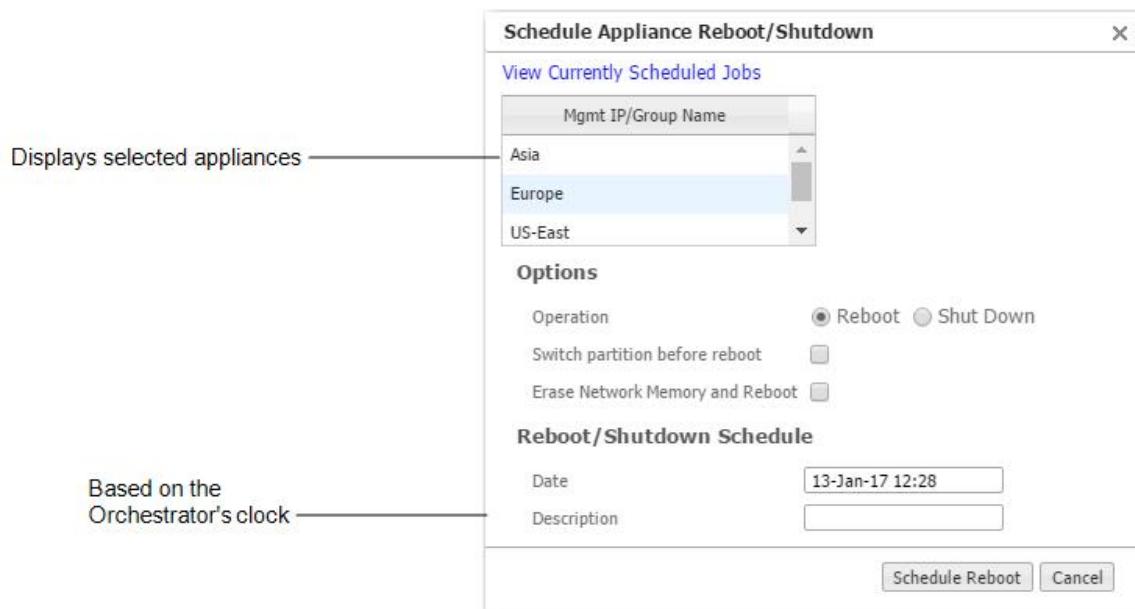
- *hardware bypass*, if deployed in-line (Bridge mode), or
- *an open-port state*, if deployed out-of-path (Router mode or Server mode).

Unless a *virtual appliance* is configured for a high availability deployment, all flows are discontinued during reboot.

## Schedule an Appliance Reboot

*Administration > Tools > Reboot > Schedule Appliance Reboot*

You can schedule an appliance for any of three types of reboot:



- **Reboot.** Reboots the appliance gracefully. This is your typical "vanilla" restart.

Use case: You are changing the deployment mode or other configuration parameters that require a reboot.

- **Erase Network Memory and Reboot.** Erases the Network Memory cache and reboots the appliance.

Use case: You need to restart the appliance with an empty Network Memory cache.

- **Shutdown.** Shuts down the appliance and turns the power off. To restart, go to the appliance and physically turn the power on with the Power switch.

- Use case:

- You are decommissioning the appliance.
- You need to physically move the appliance to another location.
- You need to re-cable the appliance for another type of deployment.

## Behavior During Reboot

- A **physical appliance** enters into one of the following states:
  - **hardware bypass**, if deployed in-line (Bridge mode), or
  - **an open-port state**, if deployed out-of-path (Router/Server mode).
- Unless a **virtual appliance** is configured for a high availability deployment, all flows are discontinued during reboot.

To specify the timezone for scheduled jobs and reports, navigate to **Orchestrator > Software & Setup > Setup > Timezone for Scheduled Jobs**.

# Reachability Status Tab

*Administration > Tools > Monitoring > Reachability Status*

This tab summarizes the status of communications in two directions—Orchestrator to Appliances and Appliances to Orchestrator.

Appliance	Admin Username	Protocol	State
Kennesaw3-[REDACTED]	admin	BOTH	Normal
Kennesaw6-[REDACTED]	admin	BOTH	Normal
Tevtron-[REDACTED]	admin	BOTH	Normal
Valheim-[REDACTED]			
Woodstock-[REDACTED]			

Appliance	Orchestrator IP	Web Socket
Kennesaw3-[REDACTED]	[REDACTED]	Reachable
Kennesaw6-[REDACTED]	[REDACTED]	Reachable
Tevtron-[REDACTED]	[REDACTED]	Reachable
Valheim-[REDACTED]	[REDACTED]	Reachable
Woodstock-[REDACTED]	[REDACTED]	Reachable

- **Admin Username** is the username that an Orchestrator server uses to log in to an appliance.
- An Orchestrator can use the web protocols, **HTTP**, **HTTPS**, or **Both** to communicate with an appliance. Although **Both** exists for legacy reasons, using **HTTPS** is recommended for maximum security.
- An appliance's **State** can be Normal, Unknown, Unsupported, or Unreachable.
  - **Normal** indicates that all is well.
  - **Unknown** is a transitional state that appears when first adding an appliance to the network.
  - **Unsupported** indicates an unsupported version of appliance software.
  - **Unreachable** indicates a problem in your network. Check your ports, firewalls, and deployment configuration.

## Active Sessions Tab

*Administration > Tools > Monitoring > Active Sessions*

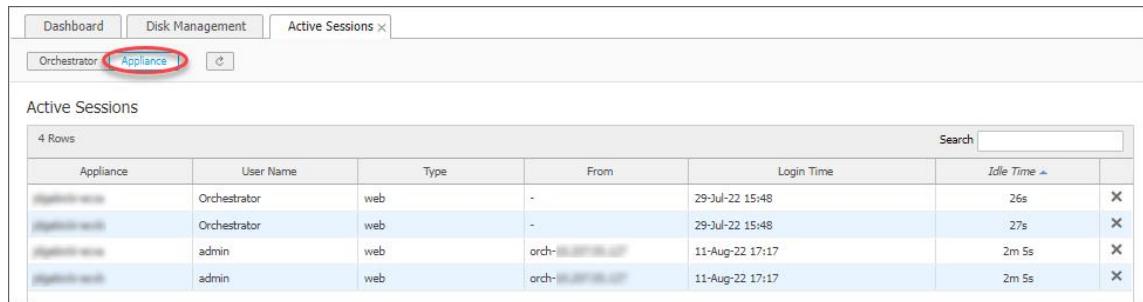
This tab lists users who are logged in to Orchestrator and the appliances that Orchestrator is currently managing.

To list active user sessions, click **Orchestrator**.



The screenshot shows the 'Active Sessions' tab in the Orchestrator interface. The top navigation bar includes 'Dashboard', 'Disk Management', 'Active Sessions', and tabs for 'Orchestrator' (which is highlighted with a red circle) and 'Appliance'. Below the tabs is a search bar and a table titled 'Active Sessions' with 1 row. The table columns are 'User Name', 'Type', 'From', 'Login Time', 'Idle Time', and 'Roles'. A single entry shows 'admin' as the User Name, 'web' as the Type, and the login time as '11-Aug-22 09:37'. There is also an 'Idle Time' column showing '0s'.

To list active appliance sessions, click **Appliance**.



The screenshot shows the 'Active Sessions' tab in the Orchestrator interface. The top navigation bar includes 'Dashboard', 'Disk Management', 'Active Sessions', and tabs for 'Orchestrator' and 'Appliance' (which is highlighted with a red circle). Below the tabs is a search bar and a table titled 'Active Sessions' with 4 rows. The table columns are 'Appliance', 'User Name', 'Type', 'From', 'Login Time', 'Idle Time', and an 'X' column for closing entries. Four entries are listed: two for 'Orchestrator' (User Name 'Orchestrator', Type 'web') and two for 'admin' (User Name 'admin', Type 'web'). The 'From' column shows '-' for the first two and 'orch-' followed by a redacted IP address for the last two. The 'Login Time' column shows '29-Jul-22 15:48' for the first two and '11-Aug-22 17:17' for the last two. The 'Idle Time' column shows '26s', '27s', '2m 5s', and '2m 5s' respectively. Each row has an 'X' button in the last column.

# Orchestrator

This section describes items related to managing Orchestrator itself. These activities do not relate to managing appliances.

## Orchestrator Server

### Role Based Access Control

*Orchestrator > Orchestrator Server > Users & Authentication > Role Based Access Control*

Role Based Access Control (RBAC) provides a more customized Orchestrator experience. On a per-user basis, you can assign roles that specify access levels for a user, control the menu options available in the Orchestrator UI, and grant or deny access to appliance groups.

#### Roles

Orchestrator provides a set of default roles. You can create new roles or modify an existing role.

Field	Description
<b>Role</b>	Name of the role.
<b>Permission</b>	Overall access level assigned to the selected role, <b>Read-Write</b> or <b>Read-Only</b> .
<b>Features</b>	Orchestrator features available to the selected role.

To add a role:

1. Click **Manage Roles**. The Roles dialog box opens.



The screenshot shows the 'Roles' dialog box with the following details:

Edit	Role	Permission	Features	X
	SiteAdmin	Read-Write	Dashboard, Topology, Health Map, Alarms, Schedule & Run Repo...	
	SiteUpgrade...	Read-Write	System Information, Software Versions, Upgrade Appliances, Re...	
	Monitor	Read-Only	Hubs, Orchestration Progress, Popup Messages, NAT, Loopback I...	
	SiteMonitor	Read-Only	Dashboard, Topology, Health Map, Alarms, Schedule & Run Repo...	
	Support	Read-Write	Audit Logs, Tech Support - Appliances, Tech Support - Orchestrat...	
	OverlayAdmin	Read-Write	Deployment Profiles, Business Intent Overlays, Interface Labels, ...	
	SiteOperator	Read-Write	Dashboard, Topology, Health Map, Alarms, Schedule & Run Repo...	
	Orchestrator...	Read-Write	Server Information, User Management, Role Based Access Contro...	
	ConfigAdmin	Read-Write	Backup Now, Configuration History, Restore, Audit Logs, Popup ...	
	SuperAdmin	Read-Write	Dashboard, Topology, Health Map, Alarms, Schedule & Run Repo...	

At the bottom right of the dialog box is a 'Close' button.

2. Click **Add** to create a new role, or click the **Edit** icon to the left of any existing role.
3. Enter or modify the role name.
4. Select a category you want to assign to your user from the following tabs: **Monitoring, Configuration, Administration, Orchestrator, Support, or Miscellaneous**.
5. Select **Read Only** or **Read & Write** to assign the overall access level for the role.
6. Select the check box corresponding to the Orchestrator menu options you want to make available to the role.

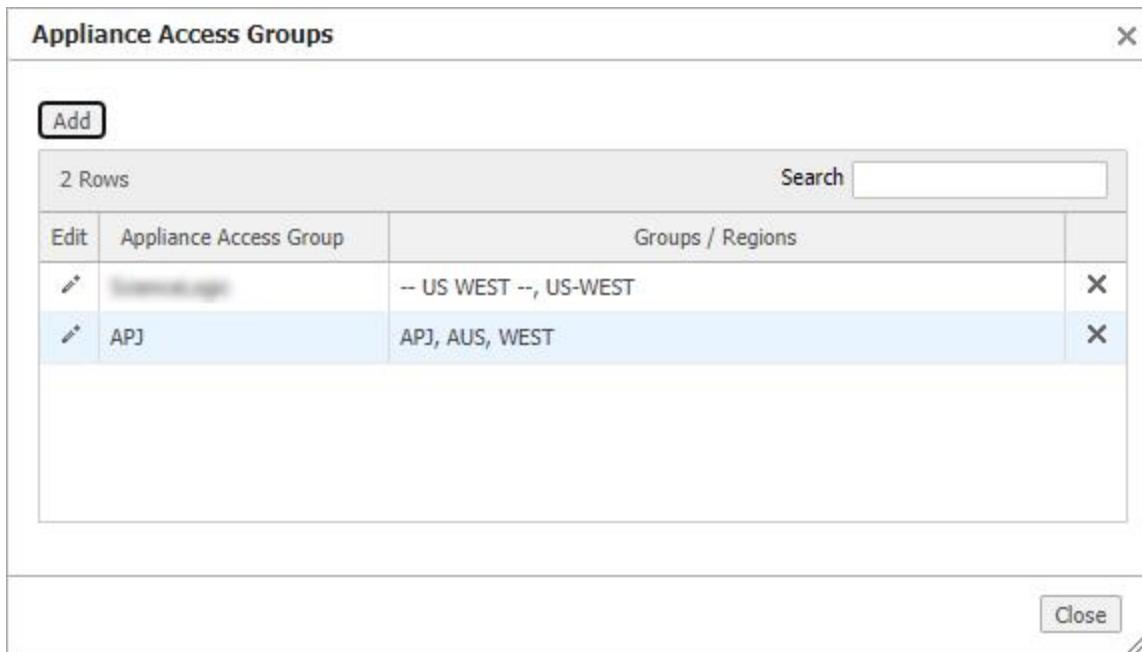
**NOTE** You can **Select All** or **UnSelect All**.

7. Click **Save**.

## Appliance Access

With appliance access groups, you can restrict appliance access to one or more groups or regions. Complete the following steps to customize appliance access.

1. Click **Manage Appliance Access Groups** on the **Role Based Access Control** tab. The Appliance Access Groups dialog box opens.



2. Click **Add** to create a new group, or click the **Edit** icon to the left of any existing group.
3. Add or modify the name of the appliance access group.
4. Choose how you want to add appliances: **Select By Groups** or **Select By Region**. You can manually select groups or regions to include, or use the buttons to select or clear all options.
5. Click **Save**.

**WARNING** A non-RBAC user or an RBAC user with appliance access and no assigned role will have access to the Appliance Manager, CLI Session, and Broadcast CLI. An RBAC user with any role assigned will be denied access to the Appliance Manager, CLI Session, and Broadcast CLI.

User	Appliance Access	Roles?	Menu Options
Non-RBAC User	N/A	N/A	Appliance Manager, CLI Session, Broadcast CLI
RBAC User	Yes	None assigned	Appliance Manager, CLI Session, Broadcast CLI
RBAC User	No	Any	Appliance Manager, CLI Session, and Broadcast CLI will be denied

## Assign Roles and Appliance Access

Complete the following steps to assign roles and appliance access.

1. On the **Role Based Access Control** tab, select **Assign Roles & Appliance Access Groups**.
2. Click in the **User** field and enter a name of an existing Orchestrator user.
3. Click the arrow in the **Appliance** field and select the name of an existing Appliance Access Group.
4. Select the check boxes for one or more roles you want to assign to the user.
5. Click **Save**.

The following table defines the roles that are provided by default in Orchestrator (roles are listed alphabetically).

Role	Description
<b>ConfigAdmin</b>	Back up and restore appliance configuration and view the configuration history.
<b>OrchestratorAdmin</b>	Enables you to perform Orchestrator operations <b>only</b> , such as settings, tools, user management, and Orchestrator upgrades. Appliance operations are <b>not</b> allowed.
<b>OverlayAdmin</b>	A global role for managing SD-WAN overlays. <b>NOTE</b> Overlay management cannot be specific to a site or region.
<b>SiteMonitor</b>	Read-only permissions equivalent to SiteAdmin.
<b>SiteOperator</b>	Enables appliance or site specific operations, such as configuring appliance specific policies, ACLs, TCAs, and SSL certificates. You <b>cannot</b> upgrade an appliance or remove it from the network, or perform global SD-WAN functions such as overlay management or Zscaler orchestration.
<b>SiteUpgradeAdmin</b>	Upgrade appliances and remove them from the network.
<b>SuperAdmin</b>	Enables full read-write access to all menu items.
<b>SiteAdmin</b>	Enables appliance or site-specific operations, such as configuring appliance specific policies, ACLs, TCAs, SSL certificates, and upgrades. You <b>cannot</b> remove an appliance from the network or perform global SD-WAN functions such as overlay management or Zscaler orchestration.
<b>Support</b>	Enables access to all support operations.
<b>Monitor</b>	Provides read-only access to all menu items.

## View Orchestrator Server Information

*Orchestrator > Orchestrator Server > Server Management > Server Information*

This dialog box provides data specific to this Orchestrator server.

Orchestrator Server Information			
Orchestrator Hostname	DMerwin-GXV	IP Address	10.0.2.14
Serial Number	0000000000000000	Active users	2
Uptime	1d 5h 10m 31s	Load Average	0.00, 0.01, 0.05
Time	Thu Jun 25 19:47:11 PDT 2015	OS Version	2.6.35.14-106.fc14.x86_64
Used disk space	26G	Free disk space	57G
Number of CPUs	4	Memory (MB)	3964
Model	GX-V	Revision	6.0.0.0

[Close](#)

## Restart, Reboot, or Shutdown

*Orchestrator > Orchestrator Server > Server Management > Reboot Orchestrator  
 Orchestrator > Orchestrator Server > Server Management > Shutdown Orchestrator*

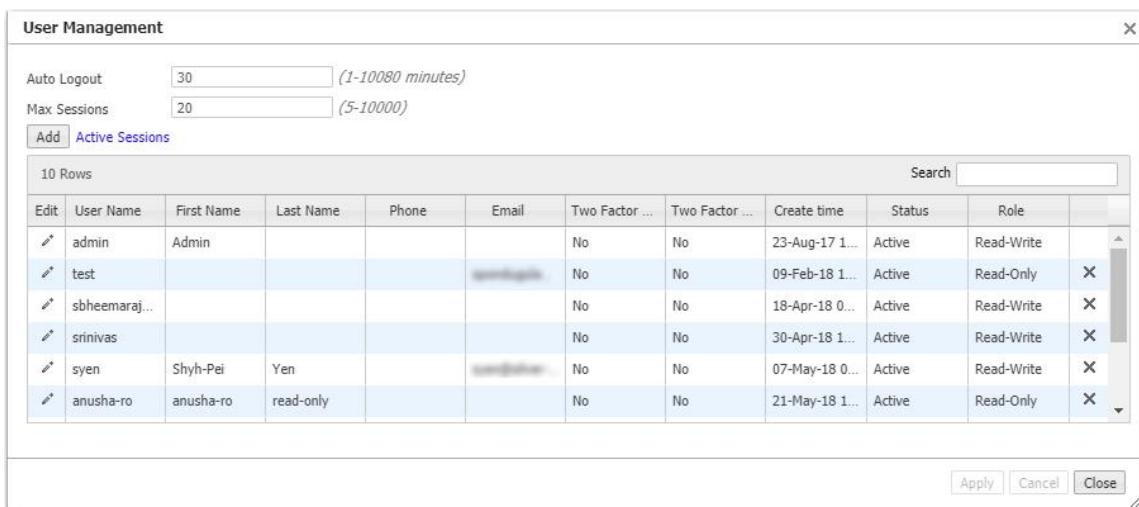
Orchestrator provides these two convenient actions in the **Orchestrator** menu:

- **Reboot Orchestrator** reboots the Orchestrator server.
- **Shutdown Orchestrator** results in the server being unreachable. You will have to manually power on the server to restart.

## Manage Orchestrator Users

*Orchestrator > Orchestrator Server > Users & Authentication > User Management*

Use the **User Management** dialog box to manage who has Read-Write or Read-Only access to Orchestrator.



## Add a User

- Users can have either **Read-Write** or **Read-Only** privileges. These provide prescribed access to Orchestrator menus.

To further limit the what users can see, you can assign them to customized menu groups in **Orchestrator > User Menu Access**.

- Multi-Factor Authentication (MFA) is a recommended option for each Orchestrator user.
- A username cannot be more than 40 characters long.
- You cannot modify a Username.** You must delete it and create a new user.

## Multi-Factor Authentication

Orchestrators support Multi-Factor Authentication (MFA). This is available on all platforms of the Orchestrator, including on-premise and cloud versions.

The first step in authentication is always username/password. For added security, users can choose between **Application-** or **Email-based** authentication, as described below.

**NOTE** Currently, only **admin** users can configure Multi-Factor Authentication, and only for themselves.

### Configuring Multi-Factor Authentication Through an Application

Orchestrator supports applications that provide time-based keys for two-factor authentication and are compliant with RFC 4226 / RFC 6238. Google Authenticator is one such app. The example below uses Google Authenticator on a mobile phone. You can also use a desktop version.

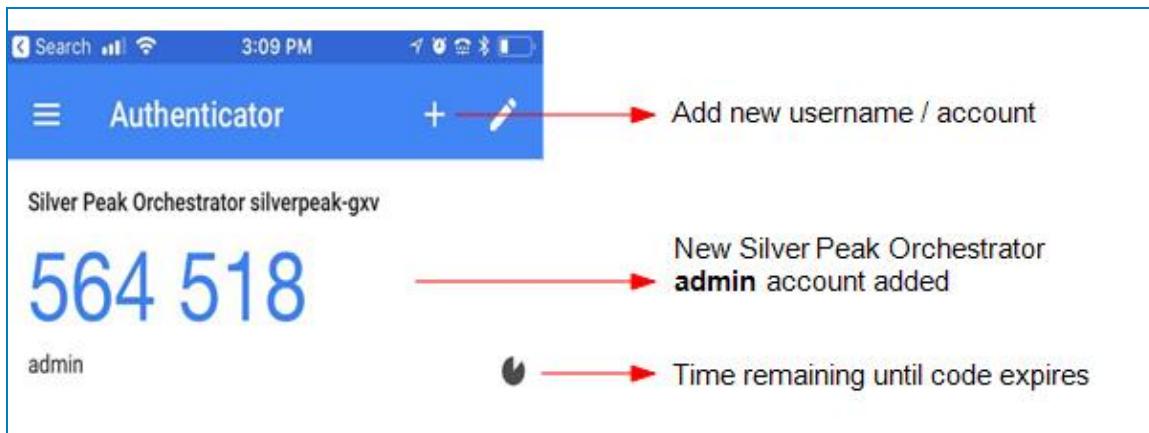
- To enable Multi-Factor Authentication, navigate to **Orchestrator > Orchestrator Server > Users & Authentication > User Management**, and then click on your username.

- For Two Factor, click **Application**. Orchestrator generates a time-limited QR code.



- With the Google Authenticator app, use the **Scan barcode** function to read the QR code. You will also be prompted to enter your Orchestrator username and password.

Here you can see Google Authenticator with the new **admin** account added for the Orchestrator, **silverpeak-gxv**.



## Configuring Multi-Factor Authentication Through Email

- To enable Multi-Factor Authentication, navigate to **Orchestrator > Orchestrator Server > Users & Authentication > User Management**, and then click on your username.

2. For **Two Factor**, click **Email** and enter your email address.

If an invalid email address is entered, the account could be locked out and would require password reset procedures.

3. After you click **Add** at the bottom of the dialog box, Orchestrator sends a time-limited authentication code to your email address. To verify your email address, click that link.

Orchestrator then opens a browser window telling you that your email address has been verified.

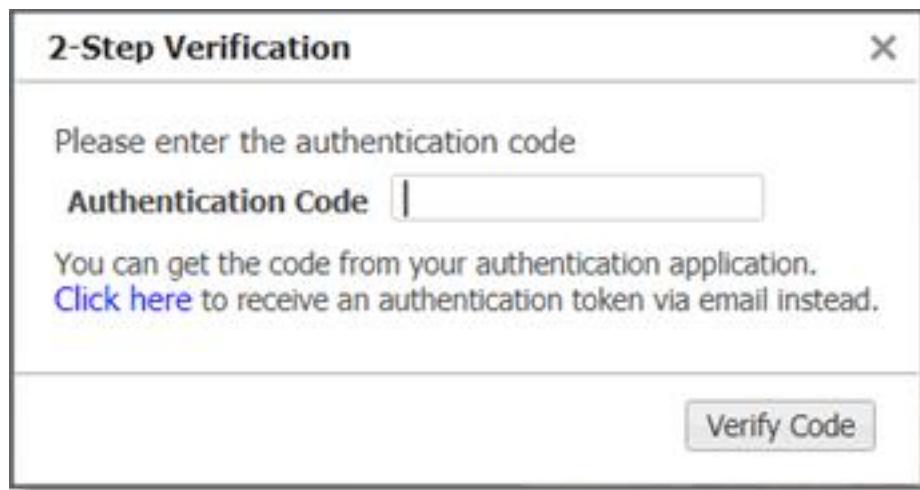
## Using Multi-Factor Authentication

After Multi-Factor Authentication is configured, every login requires two steps—entering the username/password and entering the current token.

Based on the authentication method you chose, do one of the following:

- Use the current token from the Google Authenticator (or other) app.
- Use the code you receive in email.

In both cases, the codes have a specific expiry time.



## Modify User

*Orchestrator > Orchestrator Server > Users & Authentication > User Management > Edit > Modify User*

The screenshot shows the 'Modify User' dialog box. It contains the following fields:

Field	Value
User Name	test
First Name	(empty)
Last Name	(empty)
Phone	(empty)
Email	[REDACTED]
Two Factor	<input checked="" type="radio"/> Application <input type="radio"/> Email
Password	****
Repeat Password	****
Status	Active ▾
Role	Read-Only ▾

At the bottom right are 'Apply' and 'Cancel' buttons.

- **User Name** is the identifier the user uses to log in, and it cannot be more than 40 characters long.
- **First Name, Last Name, and Phone Number** are optional information.
- **Email** is required if two-factor authentication is enabled.
- **Two-factor Authentication**

This is a second step in the login process that requires an authentication code.

The code can be obtained in two ways:

- Using an **Authentication Application** that generates time based authentication codes. If this is activated, a Barcode will be generated that can be scanned to set up an authentication app like Google Authenticator for your mobile device.
- Using your **Email** to receive authentication codes every time you log in. This requires access to your email every time you log in.
- **Password** is used at login.
- **Status** determines whether the user can log in.
- **Role** determines the user's permissions.

## API Key

*Orchestrator > Orchestrator Server > Users & Authentication > API Keys*

Use this page to allow your applications to utilize REST APIs without session authentication and management. You can specify permissions, status, name, and IP allow list for your API keys.

An API key can be passed either in the HTTP request header field "X-Auth-Token" or as a query parameter "apiKey".

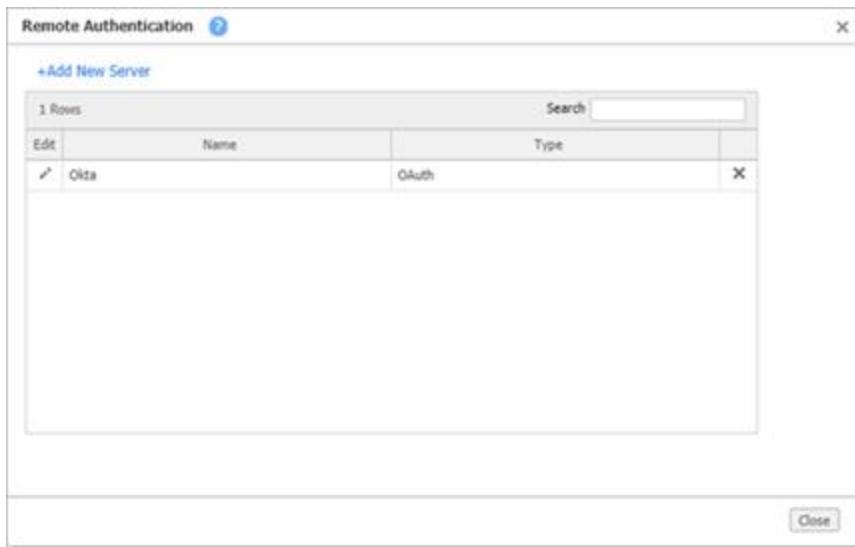
**NOTE** It is recommended to use different keys for different applications and users.

Click the edit icon to add and define a new API key by entering the fields below.

Field	Description
<b>Key Name</b>	Name of the key you are creating.
<b>Key</b>	Text you cut and paste and insert into your client code.
<b>Permission</b>	Read-Only or Read-Write.
<b>Description</b>	Enter details in this field that describe the purpose of the key you are configuring.
<b>Expiration</b>	Set the expiration date if you want a certain application or script to access the key for a fixed amount of time.
<b>Active</b>	Select <b>Yes</b> or <b>No</b> to display if the key is active or inactive.
<b>IP Allow List</b>	Filters traffic to your private resources through this specified IP range. Traffic is able to pass through with the IP addresses defined in this field.

## Remote Authentication

*Orchestrator > Orchestrator Server > Users & Authentication > Authentication*



Use the **Remote Authentication** dialog box to manage different remote authentication methods for Orchestrator users.

- To add a new remote authentication method, click **+Add New Server**.
- To view or modify the settings for an existing remote authentication method, click the edit icon in the row of the existing method.

Orchestrator supports the following for remote authentication:

- RADIUS
- TACACS+
- OAuth
- JWT
- SAML

## Configure a RADIUS or TACACS+ Server

You will need to configure the following when adding or modifying a RADIUS or TACACS+ server:

Field	Description
<b>Read-Write Privilege</b>	<b>RADIUS only:</b> Lowest value at which a user has Read-Write privileges. This value must be the same as the value configured on the RADIUS server.
<b>Read-Only Privilege</b>	<b>RADIUS only:</b> Lowest value at which a user has Read-Only privileges. This value must be the same as the value configured on the RADIUS server.
<b>Authentication Type</b>	Select the authentication type that matches what is configured on the RADIUS or TACACS+ server.
<b>Default Role</b>	If RBAC is enabled, you must specify a default role.
<b>Primary/Secondary Server</b>	For each server in use, enter the IP address or hostname, port, and secret key of the RADIUS or TACACS+ server.

## Authenticate using RADIUS or TACACS+

1. Select the access control protocol you want to use.
2. Under **Servers**, enter the information for a Primary server of that type. Entering a Secondary server is optional.

Field	Description
<b>Authentication Order</b>	Whether to use the remote map or the local map first. The default is <b>Remote First</b> . <b>NOTE</b> If the Authentication Order field is set to Remote First, and if a password is configured for the CLI <b>enable</b> command, add a user named "enableuser" on the remote server and set the password to be identical to the one configured locally.
<b>Primary/Secondary Server</b>	IP address or hostname of the RADIUS or TACACS+ server.
<b>Secret Key</b>	String defined as the shared secret on the server.
<b>Read-Write Privilege</b>	Lowest value at which a user has Read-Write privileges. This value must be the same as the value configured on the RADIUS server.
<b>Read-Only Privilege</b>	Lowest value at which a user has Read-Only privileges. This value must be the same as the value configured on the RADIUS server.
<b>Authentication Type</b>	When configuring to use the TACACS+ server, select the type from the drop-down list that matches what is configured on the TACACS+ server.

## Configure an OAuth Server

Orchestrator supports remote authentication via the OAuth 2.0 framework. Before configuring an OAuth server in Orchestrator, you will need to register Orchestrator as an application with your OAuth provider.

### Prerequisites

- The OAuth server must support OAuth 2.0 authorization codes, ID tokens, and optionally refresh tokens.
- The ID token is used to get username, RBAC roles, and RBAC appliance access groups.
- The refresh token can be checked periodically to ensure the user is still authorized/valid.
- Depending on the OAuth server configuration, refresh tokens can be permanent or they can expire. If a token is revoked or expires, the user will be forced to authenticate again.

## Register Orchestrator as an App

Before adding an OAuth server in Orchestrator, register a new app on your OAuth server for Orchestrator. You will need to provide the following details when registering the app:

Needed Information	Description
<b>Application Type</b>	Register Orchestrator as a web app.
<b>Allowed Grant Types</b>	Authorization code (required). Refresh token (optional).
<b>Redirect URL</b>	Orchestrator endpoint to which the user will be redirected after successful authentication, which should be <code>https://&lt;Orchestrator_domain_or_IP_address&gt;/gms/rest/authentication/oauth/redirect</code> .

## Configure OAuth Server Properties in Orchestrator

When adding a new OAuth server or modifying an existing server, you will need to configure the following fields in the Remote Authentication Server dialog box:

Field	Description
<b>Name</b>	Name to identify the server. This name will be displayed on a button on the Orchestrator login page as an alternative method of authentication.
<b>Client ID</b>	Client ID for the Orchestrator application that you created in your OAuth provider.
<b>Client Secret</b>	Client secret for the Orchestrator application that you created in your OAuth provider.
<b>Scopes</b>	OAuth 2.0 uses scope values, as defined in RFC6749, to specify which access privileges are being requested for in Access Tokens. The default scopes for Orchestrator are <b>openid</b> , <b>offline_access</b> , and <b>email</b> .
<b>Authentication URL</b>	This is the Issuer Identifier URL with the authentication request path appended. For example: <code>https://&lt;your-oauth-domain&gt;/oauth2/v1/authorize</code> .
<b>Token URL</b>	This is the Issuer Identifier URL with the token path appended. For example: <code>https://&lt;your-oauth-domain&gt;/oauth2/v1/token</code> .
<b>Username key</b>	This is the OAuth attribute to be sent as the username. Use <b>email</b> if username is an email address. If any other key is used, ensure that it is mapped to the correct scope on the OAuth server.

Field	Description
<b>Roles key (optional)<sup>1</sup></b>	This field can be left with the default value, <i>ec-roles</i> , or you can enter a new key name, but the key name must match what is configured in your OAuth provider. This is a user claim sent in the ID token that maps to Orchestrator roles defined in Role Based Access Control (RBAC). For example, the OAuth server attribute <i>userType</i> maps to <i>ec-roles</i> , and the OAuth user in Orchestrator has <i>userType</i> = <i>OverlayAdmin</i> .
<b>Appliance Access Group key (optional)<sup>1</sup></b>	This field can be left with the default value, <i>ec-aag</i> , or you can enter a new key name, but the key name must match what is configured in your OAuth provider. This is a user claim sent in the ID token that maps to Orchestrator Appliance Access Groups defined in Role Based Access Control (RBAC). For example, the OAuth server attribute <i>department</i> maps to <i>ec-aag</i> , and the OAuth user in Orchestrator has <i>department</i> = <i>Asia-Admin</i> .
<b>Default role</b>	If RBAC is enabled, you must specify a default role.

**Remote Authentication Server**

Type	OAuth
Name	<input type="text"/>
Client ID	<input type="text"/>
Client Secret	<input type="text"/>
Scopes	<input type="text"/> openid,offline_access
Authentication Url	<input type="text"/> https://authserver.com/oauth2/serve123/v1/authorize
Token Url	<input type="text"/> https://authserver.com/oauth2/serve123/v1/token
Username key	<input type="text"/> ec-name
Roles key	<input type="text"/> ec-roles (optional)
Appliance Access Group key	<input type="text"/> ec-aag (optional)
Default role	Select role <input type="button" value="▼"/> (optional)
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

## Configure a JWT Server

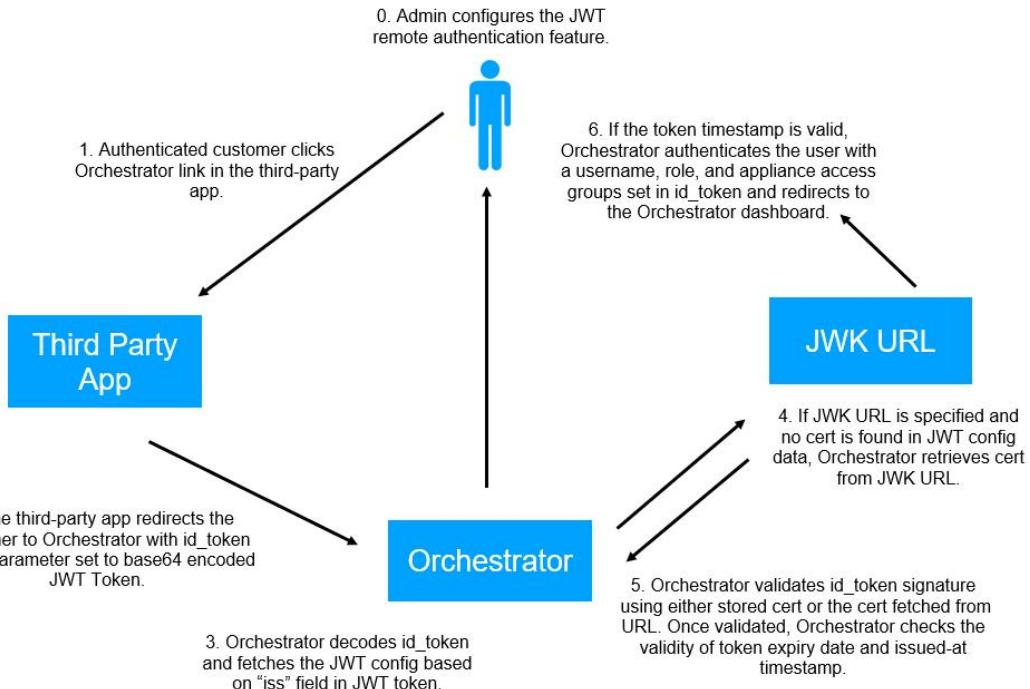
To begin JWT server configuration, the assigned admin needs to specify the following JWT configuration parameters. This includes the following:

- Issuer 'iss'
- Auditor 'aud'
- expiration 'exp'
- signature
- user, role, and AAG

**NOTE** See the following descriptions in the table below.

- Redirect URL based on successful authentication: [https://<orchestrator\\_domainName>?access\\_token=<token>&id\\_token=<token>&state=<state>&token\\_type=Bearer&expires\\_in=3596](https://<orchestrator_domainName>?access_token=<token>&id_token=<token>&state=<state>&token_type=Bearer&expires_in=3596)

Review the following diagram for more details about the workflow of JWT authentication.



Then, complete the following steps in Orchestrator:

1. Navigate to the **Authentication** tab in Orchestrator.
2. Click **+Add New Server**. The **Remote Authentication Server** window opens.
3. Select **JWT** from the **Type** drop-down menu and complete the following fields.

Field	Description
<b>Name</b>	Name of your JWT provider.
<b>Cert/Signing Key</b>	HMAC or RSA public key used to verify the id_token.
<b>JWK URL</b>	URL that hosts the public certification.
<b>Validation Window</b>	Maximum amount of time in minutes that the expiration is found for the id_token, before a new id_token is created.
<b>Issuer</b>	Issuer claim found in the id_token.
<b>Auditor</b>	Auditor claim found in the id_token.
<b>Username key</b>	This attribute is sent as the username. Use <b>email</b> if username is an email address. If any other key is used, ensure that it is mapped to the correct scope on the OAuth server.
<b>Roles key<sup>1</sup></b>	<p>This field can be left with the default value, <i>ec-roles</i>, or you can enter a new key name, but the key name must match what is configured in your JWT provider.</p> <p>This is a user claim sent in the ID token that maps to Orchestrator roles defined in Role Based Access Control (RBAC). For example, the OAuth server attribute <i>userType</i> maps to <i>ec-roles</i>, and the OAuth user in Orchestrator has <i>userType</i> = <i>OverlayAdmin</i>.</p>
<b>Appliance Access Group key<sup>1</sup></b>	<p>This field can be left with the default value, <i>ec-aag</i>, or you can enter a new key name, but the key name must match what is configured in your JWT provider.</p> <p>This is a user claim sent in the ID token that maps to Orchestrator Appliance Access Groups defined in Role Based Access Control (RBAC). For example, the JWT server attribute <i>department</i> maps to <i>ec-aag</i>, and the JWT user in Orchestrator has <i>department</i> = <i>Asia-Admin</i>.</p>
<b>Default role</b>	If RBAC is enabled, you must specify a default role.
<b>JWT token consuming URL</b>	URL of Orchestrator that remains the same.

## Configure a SAML Server

Orchestrator supports SAML 2.0 integration, providing authentication and authorization of your credentials through an IdP (Identity Provider), SP (Service Provider), and a Principal. Refer to the list below for the represented meanings:

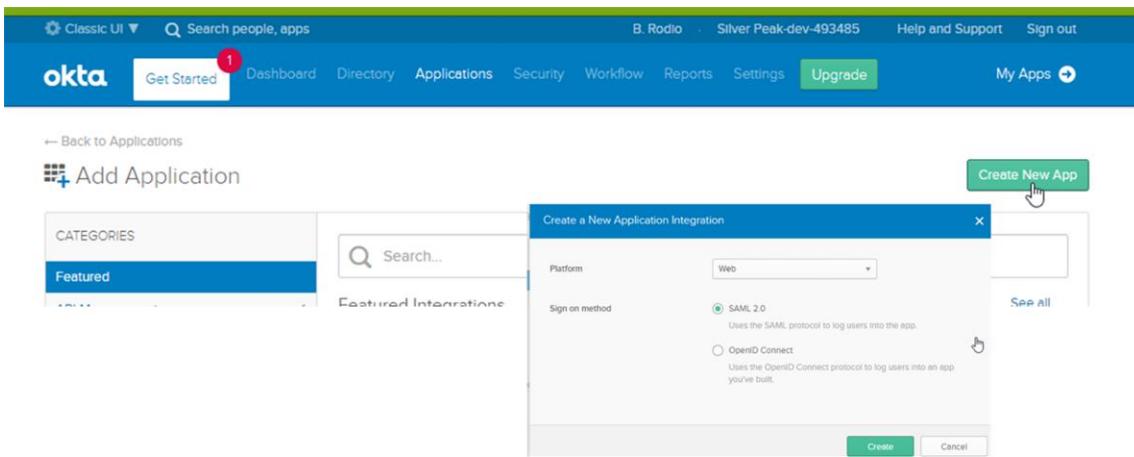
- IdP: Okta
- SP: Orchestrator
- Principal: Principal end user

## SAML and Orchestrator Configuration

Complete the following instructions to complete SAML and Orchestrator integration.

**TIP** It is recommended to have Orchestrator open next to your Okta window while completing these instructions.

1. Sign in to your Okta account.
2. Select **Add Application**, and then select **SAML 2.0**.
3. Click **Create New App**.



4. Sign in to Orchestrator and navigate to the **Authentication** tab (**Orchestrator > Users & Authentication > Authentication**).
5. Click **+Add New Server**.
6. Select **SAML** from the **Type** field.
7. In Orchestrator, copy the **ACS URL** and the **EdgeConnect SLO Endpoint** by clicking the icon next to the fields.
8. Navigate back to your SAML application configuration window.
9. Enter the copied URLs in the following fields in the **Step 2: Configure SAML** section:
  - a. Paste the **ACS URL** in the **Single Sign On URL** and **Audience URL (SP Entity ID)** fields.
10. Specify the attributes and their corresponding values on the SAML Settings page. These are configured and assigned on the **RBAC** tab in Orchestrator.
  - a. ec-name: user.email
  - b. ec-role: user.usertype
  - c. ec-aag: user.department
11. Click **Next**.
12. Click **Finish**.
13. Click the **View Setup Instructions** box on the completed **SAML Application Settings** page and enter the following URLs in the corresponding Orchestrator fields:

SAML Field	Orchestrator Field
Identity Provider Single Sign-On URL	SSO Endpoint
Identity Provider Issuer	Issuer URL
X.509 Certificate	IdP X.509 Cert

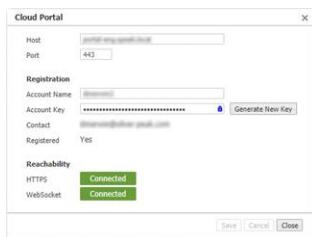
The following table provides more details about the fields in Orchestrator.

Field	Description
<b>Name</b>	Any text value for your SAML account for identification purposes.
<b>Username Attribute</b>	This attribute is used to retrieve the username from the SAML XML response.
<b>Issuer URL</b>	Unique identifier of the issuer (for example: Okta, OneLogin).
<b>SSO Endpoint</b>	Unique endpoint for the SAML application created on the IdP server.
<b>IdP X.509 cert</b>	Certificate issued by IdP to verify and validate the response received from the IdP (Okta) server.
<b>ACS URL</b>	Orchestrator endpoint needed for configuration on the IdP server. This is provided as a redirect URL after you are authenticated on the IdP server.
<b>EdgeConnect SLO Endpoint (Optional)</b>	This endpoint is used by IdP to initiate the logout request from Orchestrator to the IdP server.
<b>IdP SLO Endpoint (Optional)</b>	This endpoint is used by IdP to initiate the logout request from Orchestrator to the IdP server. The endpoint used by Orchestrator to initiate the logout request to IdP.
<b>EdgeConnect X.509 Cert SLO (Optional)</b>	Certificate used by IdP to verify the Single Logout request initiated by Orchestrator to logout the IdP.
<b>Roles Attribute (optional)<sup>1</sup></b>	This field can be left with the default value, <i>ec-roles</i> , or you can enter a new key name, but the key name must match what is configured in your SAML provider. This is a claim sent to Orchestrator that maps to roles defined in Role Based Access Control (RBAC).
<b>Appliance Access Group Attribute (optional)<sup>1</sup></b>	This field can be left with the default value, <i>ec-aag</i> , or you can enter a new key name, but the key name must match what is configured in your OAuth provider. This is a claim sent to Orchestrator that maps to Orchestrator Appliance Access Groups defined in Role Based Access Control (RBAC).
<b>Default role</b>	If RBAC is enabled, you must specify a default role.

## Cloud Portal

*Configuration > Overlays & Security > Licensing > Cloud Portal*  
*Orchestrator > Orchestrator Server > Licensing > Cloud Portal*

The **Cloud Portal** is used to register cloud-based features and services, such as **SaaS optimization** and **EdgeConnect**.



- When you purchase one of these services, an **Account Name** and instructions to obtain your **Account Key** are sent to you. You will use these to register your appliances.
- The cloud portal populates the **Contact** field from information included in your purchase order.
- Use of these services requires that your appliances can access the cloud portal via the Internet.

## Audit Logs

*Orchestrator > Orchestrator Server > Tools > Audit Logs*

The **Audit Logs** tab lists actions from a user or the system itself, initiated by Orchestrator.

You can apply the following filters to your audit logs.

- You can select **Completed**, **In Progress**, or **Queued** filters to determine which actions you want to display in the table.
- You can select the following different log levels: **Debug**, **Info**, **Error** to apply to your filter.
- You can choose either **Auto Refresh** or **Pause** to refresh or pause the table. By default, the table refreshes automatically.
- You can enter in the **Record Count**. This limits the filtering criteria. The default value is 500 and 10,000 is the maximum amount you can filter.
- You can choose the name of the **Appliance** from the lists to apply as a filter.
- You can also search a wild card character (\*) as a username and all user logs will display. If you enter any value in the user field, there will be no filter applied to the search. The following are true for audit log wild cards:
  - x\*= anything that starts with the entered value
  - \*x= anything that ends with the entered value

Dashboard		Audit Logs >																																																																																																																											
<input checked="" type="checkbox"/> Completed		<input type="checkbox"/> In Progress		<input type="checkbox"/> Queued		Log Level: Info		<input type="checkbox"/> Auto Refresh		<input type="checkbox"/> Pause		Record Count: 000 (Max 10000) Appliance Type to select																																																																																																																	
												From: 11-Aug-22 13:04 To: 12-Aug-22 13:04 User: Type to select Export																																																																																																																	
<b>Audit Logs</b> <span>(12 Rows)</span>																																																																																																																													
<table border="1"> <thead> <tr> <th>User Name</th> <th>IP Address</th> <th>Appliance</th> <th>Action</th> <th>Task Status</th> <th>Results</th> <th>Start Time</th> <th>End Time</th> <th>Queued Time</th> <th>% Completed</th> <th>Completion Status</th> <th>Search:</th> <th colspan="2"></th> </tr> </thead> <tbody> <tr> <td>InternalJob</td> <td>[REDACTED]</td> <td>[REDACTED]</td> <td>Check application definition data (Address M)</td> <td>COMPLETED</td> <td>Timestamp from portal is 1650426833131, timestamp from Orchestrator is 0. File h...</td> <td>12-Aug-22 09:55</td> <td>12-Aug-22 09:55</td> <td>12-Aug-22 09:55</td> <td>100</td> <td>Success</td> <td></td><td colspan="2"></td> </tr> <tr> <td>OverlayManager</td> <td>[REDACTED]</td> <td>[REDACTED]</td> <td>PushSaaSClassificationAction</td> <td>COMPLETED</td> <td>SaaS Classification file applied to appliance</td> <td>12-Aug-22 09:47</td> <td>12-Aug-22 09:47</td> <td>12-Aug-22 09:47</td> <td>100</td> <td>Success</td> <td></td><td colspan="2"></td> </tr> <tr> <td>OverlayManager</td> <td>[REDACTED]</td> <td>[REDACTED]</td> <td>PushSaaSClassificationAction</td> <td>COMPLETED</td> <td>SaaS Classification file applied to appliance</td> <td>12-Aug-22 09:47</td> <td>12-Aug-22 09:47</td> <td>12-Aug-22 09:47</td> <td>100</td> <td>Success</td> <td></td><td colspan="2"></td> </tr> <tr> <td>SaaSClassificationJob</td> <td>[REDACTED]</td> <td>[REDACTED]</td> <td>Check application definition data (SAAS) from [REDACTED]</td> <td>COMPLETED</td> <td>Hash code from portal is [REDACTED]</td> <td>12-Aug-22 09:47</td> <td>12-Aug-22 09:47</td> <td>12-Aug-22 09:47</td> <td>100</td> <td>Success</td> <td></td><td colspan="2"></td> </tr> <tr> <td>MalwareSignatureDownload</td> <td>[REDACTED]</td> <td>[REDACTED]</td> <td>Downloading Signature</td> <td>COMPLETED</td> <td>Signature version up to date</td> <td>12-Aug-22 09:47</td> <td>12-Aug-22 09:47</td> <td>12-Aug-22 09:47</td> <td>100</td> <td>Success</td> <td></td><td colspan="2"></td> </tr> <tr> <td>SYSTEM</td> <td>[REDACTED]</td> <td>[REDACTED]</td> <td>Check DateTime</td> <td>COMPLETED</td> <td>Check appliance datetime successfully</td> <td>12-Aug-22 09:47</td> <td>12-Aug-22 09:47</td> <td>12-Aug-22 09:47</td> <td>100</td> <td>Success</td> <td></td><td colspan="2"></td> </tr> <tr> <td>InternalJob</td> <td>[REDACTED]</td> <td>[REDACTED]</td> <td>CheckDateTime</td> <td>COMPLETED</td> <td>Check appliance datetime successfully</td> <td>12-Aug-22 09:47</td> <td>12-Aug-22 09:47</td> <td>12-Aug-22 09:47</td> <td>100</td> <td>Success</td> <td></td><td colspan="2"></td> </tr> </tbody> </table>														User Name	IP Address	Appliance	Action	Task Status	Results	Start Time	End Time	Queued Time	% Completed	Completion Status	Search:			InternalJob	[REDACTED]	[REDACTED]	Check application definition data (Address M)	COMPLETED	Timestamp from portal is 1650426833131, timestamp from Orchestrator is 0. File h...	12-Aug-22 09:55	12-Aug-22 09:55	12-Aug-22 09:55	100	Success				OverlayManager	[REDACTED]	[REDACTED]	PushSaaSClassificationAction	COMPLETED	SaaS Classification file applied to appliance	12-Aug-22 09:47	12-Aug-22 09:47	12-Aug-22 09:47	100	Success				OverlayManager	[REDACTED]	[REDACTED]	PushSaaSClassificationAction	COMPLETED	SaaS Classification file applied to appliance	12-Aug-22 09:47	12-Aug-22 09:47	12-Aug-22 09:47	100	Success				SaaSClassificationJob	[REDACTED]	[REDACTED]	Check application definition data (SAAS) from [REDACTED]	COMPLETED	Hash code from portal is [REDACTED]	12-Aug-22 09:47	12-Aug-22 09:47	12-Aug-22 09:47	100	Success				MalwareSignatureDownload	[REDACTED]	[REDACTED]	Downloading Signature	COMPLETED	Signature version up to date	12-Aug-22 09:47	12-Aug-22 09:47	12-Aug-22 09:47	100	Success				SYSTEM	[REDACTED]	[REDACTED]	Check DateTime	COMPLETED	Check appliance datetime successfully	12-Aug-22 09:47	12-Aug-22 09:47	12-Aug-22 09:47	100	Success				InternalJob	[REDACTED]	[REDACTED]	CheckDateTime	COMPLETED	Check appliance datetime successfully	12-Aug-22 09:47	12-Aug-22 09:47	12-Aug-22 09:47	100	Success			
User Name	IP Address	Appliance	Action	Task Status	Results	Start Time	End Time	Queued Time	% Completed	Completion Status	Search:																																																																																																																		
InternalJob	[REDACTED]	[REDACTED]	Check application definition data (Address M)	COMPLETED	Timestamp from portal is 1650426833131, timestamp from Orchestrator is 0. File h...	12-Aug-22 09:55	12-Aug-22 09:55	12-Aug-22 09:55	100	Success																																																																																																																			
OverlayManager	[REDACTED]	[REDACTED]	PushSaaSClassificationAction	COMPLETED	SaaS Classification file applied to appliance	12-Aug-22 09:47	12-Aug-22 09:47	12-Aug-22 09:47	100	Success																																																																																																																			
OverlayManager	[REDACTED]	[REDACTED]	PushSaaSClassificationAction	COMPLETED	SaaS Classification file applied to appliance	12-Aug-22 09:47	12-Aug-22 09:47	12-Aug-22 09:47	100	Success																																																																																																																			
SaaSClassificationJob	[REDACTED]	[REDACTED]	Check application definition data (SAAS) from [REDACTED]	COMPLETED	Hash code from portal is [REDACTED]	12-Aug-22 09:47	12-Aug-22 09:47	12-Aug-22 09:47	100	Success																																																																																																																			
MalwareSignatureDownload	[REDACTED]	[REDACTED]	Downloading Signature	COMPLETED	Signature version up to date	12-Aug-22 09:47	12-Aug-22 09:47	12-Aug-22 09:47	100	Success																																																																																																																			
SYSTEM	[REDACTED]	[REDACTED]	Check DateTime	COMPLETED	Check appliance datetime successfully	12-Aug-22 09:47	12-Aug-22 09:47	12-Aug-22 09:47	100	Success																																																																																																																			
InternalJob	[REDACTED]	[REDACTED]	CheckDateTime	COMPLETED	Check appliance datetime successfully	12-Aug-22 09:47	12-Aug-22 09:47	12-Aug-22 09:47	100	Success																																																																																																																			

Field	Description
<b>User Name</b>	You can filter/search for an audit log by the user name of the appliance.
<b>IP Address</b>	IP address of the selected appliance.
<b>Appliance</b>	Name of the appliance the audit log comes from.
<b>Action</b>	The action that was taken by the user or the system, initiated by Orchestrator.
<b>Task Status</b>	Status of the audit log task.
<b>Results</b>	Contains a brief description of the audit log including any actions taken. If the audit log refers to template changes or segment (VRF) firewall zone policy changes, any comments entered in the <b>Audit Log Comment</b> field will be included in the description. Click the cell to view the full description.
<b>Start Time</b>	Time when the search of the audit log started.
<b>End Time</b>	Time when the search of the audit log ended.
<b>Queued Time</b>	Time when the process/task was requested or scheduled in the queue.
<b>% Completed</b>	Percent completed of the audit log task.
<b>Completion Status</b>	Whether the task has been completed.

## Orchestration Settings

*Orchestrator > Orchestrator Server > Tools > Orchestration Settings*

The Orchestration Settings dialog box manages Business Intent Overlays (BIOS) and the properties that control them. It builds new tunnels and fixes existing ones.

Field	Description
<b>Orchestrate appliances by applying and updating overlays</b>	When selected, updates all associated appliances when overlay changes are saved.  <b>NOTE</b> Tunnels are rebuilt only if this field is enabled.
<b>Reset all flows</b>	When selected, Orchestrator automatically resets all flows whenever you edit overlays or change policies or priorities. When deselected, the flows can only be reset manually.

Field	Description
<b>Autosave appliance changes</b>	Selected by default, this automatically saves any changes made to an appliance. If you need a time delay for troubleshooting or testing, deselect this option to suspend automatic saving of configuration changes.
<b>Apply templates</b>	When selected, updates all associated appliances when template changes are saved.
<b>Idle time</b>	Amount of time Orchestrator sleeps or is idle between checking for any configuration changes. For normal-sized networks, the recommended idle time is <b>60</b> seconds. For smaller networks, the recommended idle time is <b>30</b> seconds.
<b>Auto flow re-classify</b>	Specifies how the Overlay Manager waits before surveying the network when configuration changes are not being made.

#### IPSec UDP Settings

Field	Description
<b>Default port</b>	By default, BIOS create IPSec UDP tunnels. The default port is <b>10002</b> . If necessary, you can configure this for an individual appliance on its System Information page, under System Settings. This is accessible from the appliance's context-sensitive menu in the Orchestrator navigation pane.
<b>Increment port by</b>	Referenced when configuring an Edge HA (High Availability) pair. When the value is 1000, the second appliance's default port becomes 11002.

## Maintenance Mode

*Orchestrator > Orchestrator Server > Tools > Maintenance Mode*

You can set maintenance mode on an appliance in two ways. You can:

- Use the menu available from the appliance tree. This method automatically suppresses alarms and pauses orchestration.
- Use the Orchestrator menu to select appliances and specify settings. This method allows you to specify whether to pause orchestration or suppress alarms.

### Set Maintenance Mode Using the Menu Available from the Appliance Tree

1. Right-click on one or more appliances in the appliance tree, and then select **Maintenance Mode**.
2. In the Maintenance Mode dialog box, click **OK**.

Alarms are automatically suppressed, and orchestration is automatically paused for the selected appliances.

## Set Maintenance Mode Using the Orchestrator Menu

1. Navigate to **Orchestrator > Orchestrator Server > Tools > Maintenance Mode**.
2. In the Maintenance Mode dialog box, click **Add**.  
The Configure Maintenance Mode dialog box opens.
3. In the **Appliance** field, enter the name of the appliance you want to put into maintenance mode.
4. To pause orchestration, select **Pause Orchestration**.
5. To suppress alarms associated with this appliance while in maintenance mode, select **Suppress Alarms**.
6. Click **OK**.
7. Click **Save**.

The following table describes the fields on the Maintenance Mode dialog box.

Field	Description
<b>Appliance</b>	Name of the appliance you put into maintenance mode.
<b>Alarms</b>	Indicates whether to suppress alarms while the appliance is in maintenance mode.
<b>Orchestration</b>	If paused, all orchestration is paused on the selected appliance, except IPSec UDP Tunnel Key material.
<b>IP</b>	IP address of the appliance in maintenance mode.
<b>Version</b>	Current version of the appliance.

## Tunnel Settings Tab

### *Orchestrator > Orchestrator Server > Tools > Tunnels Settings*

This tab enables you to manage properties for tunnels created by Orchestrator. Tunnel settings are controlled on a per-label basis, such as MPLS, Internet, or LTE.

### IPSec Suite B Presets

As of version 9.2, Orchestrator provides you with four IPSec Suite B presets, as follows:

- GCM-128
- GCM-256
- GMAC-128
- GMAC-256

Each preset includes a predetermined set of IKE and ESP (IPSec) cryptographic algorithms. By selecting an IPSec Suite B preset, you can streamline the algorithm aspect of your tunnel setup rather than selecting individual algorithms. However, you can select individual algorithms if you want to. To select a preset, use the **IPSec Suite B Preset** drop-down field on the General tab.

The following tables show the IPSec Suite B presets in the header row and provide the associated algorithm setups for the IKEv2 and ESP (IPSec) stages.

#### IKEv2 Stage

	GCM-128	GCM-256	GMAC-128	GMAC-256
<b>Encryption (Note)</b>	AES-128-CBC	AES-256-CBC	AES-128-CBC	AES-256-CBC
<b>Pseudo Random Function</b>	HMAC-SHA-256	HMAC-SHA-384	HMAC-SHA-256	HMAC-SHA-384
<b>Integrity (IKE Data Authentication)</b>	HMAC-SHA-256-128	HMAC-SHA-384-192	HMAC-SHA-256-128	HMAC-SHA-384-192
<b>Key Exchange (NIST Elliptic Curve Groups)</b>	DH-19 256-bit Prime Size	DH-20 384-bit Prime Size	DH-19 256-bit Prime Size	DH-20 384-bit Prime Size

#### ESP (IPSec) Stage

	GCM-128	GCM-256	GMAC-128	GMAC-256
<b>Encryption</b>	AES-128-GCM with 16 octet ICV	AES-256-GCM with 16 octet ICV	NULL	NULL
<b>Integrity (Data Authentication)</b>	NULL	NULL	AES-128-GMAC	AES-256-GMAC

Notice in the second table that the encryption and data authentication is done in one step for GCM. For GMAC, there is no encryption.

#### General Tab

Access the following fields by clicking the General Tab.

## General

Field	Description
<b>Mode</b>	<p>Indicates whether the tunnel protocol is <b>UDP</b>, <b>GRE</b>, <b>IPSec</b>, or <b>IPSec UDP</b>. The default setting is IPSec UDP.</p> <p>If you select IPSec, you can specify the IKE version on the IKE tab.</p> <p><b>NOTE</b> If this field is set to IPSec UDP, it is recommended that you use the <b>AES_256_GCM_16</b> algorithm, which performs both encryption and authentication, resulting in better performance.</p>
<b>IPSec Suite B Preset</b>	<p>This field is available only if the Mode field is set to IPSec. Select an IPSec Suite B preset if required by the security service (<b>GCM-128</b>, <b>GCM-256</b>, <b>GMAC-128</b>, or <b>GMAC-256</b>). The default setting is None.</p> <ul style="list-style-type: none"> <li>• If IPSec Suite B Preset is set to None, no preset is selected, but GCM and GMAC algorithms are available to set independently.</li> <li>• If an IPSec Suite B preset is selected, various settings on the IKE and IPSec tabs are configured automatically based on the selected preset.</li> </ul>
<b>Auto max BW enabled</b>	When enabled, allows the appliances to auto-negotiate the maximum tunnel bandwidth. Enabled by default.
<b>Auto discover MTU enabled</b>	When enabled, allows the appliances to auto-negotiate the maximum tunnel bandwidth. Enabled by default.
<b>MTU</b>	Maximum Transmission Unit (MTU) is the largest possible unit of data that can be sent on a given physical medium. For example, the MTU of Ethernet is 1500 bytes. MTUs up to 9000 bytes are supported. Auto allows the tunnel MTU to be discovered automatically, and it overrides the MTU setting. This field is not available if the Auto discover MTU enabled check box is selected.
<b>UDP destination port</b>	Used in UDP mode. Accept the default value unless the port is blocked by a firewall.
<b>UDP flows</b>	Used in UDP mode. Number of flows over which to distribute tunnel data.

## Packet

**NOTE** FEC settings do not apply when overlays are used. FEC settings only apply when routing directly to an underlay via Route Policy.

Field	Description
<b>Reorder wait</b>	Maximum time (in milliseconds) the appliance holds an out-of-order packet when attempting to reorder. <b>100</b> ms is the default value and should be adequate for most situations. FEC can introduce out-of-order packets if the reorder wait time is not set high enough.
<b>FEC</b>	Forward Error Correction (FEC) can be set to <b>enable</b> , <b>disable</b> , or <b>auto</b> .
<b>FEC ratio</b>	When FEC is set to <b>auto</b> , FEC will range dynamically from off to 1:10 based on detected loss. The options are <b>1:1</b> , <b>1:2</b> , <b>1:5</b> , <b>1:10</b> , or <b>1:20</b> . This field is available only if FEC is set to enable.

### Tunnel Health

Field	Description
<b>Retry count</b>	Number of failed keep-alive messages allowed before the appliance brings the tunnel down.
<b>DSCP</b>	Determines the DSCP marking that the keep-alive messages should use.

### FastFail Thresholds

**NOTE** FastFail thresholds do not apply when overlays are used. FastFail only applies when routing directly to an underlay via Route Policy.

Field	Description
<b>Fastfail enabled</b>	<p>When multiple tunnels are carrying data between two appliances, this feature determines how quickly to disqualify a tunnel from carrying data.</p> <p>The Fastfail connectivity detection algorithm for the wait time from receipt of last packet before declaring a <b>brownout</b> is:</p> $T_{wait} = Base + N * RTT_{avg}$ <p>where <b>Base</b> is a value in milliseconds, and <b>N</b> is the multiplier of the average Round Trip Time over the past minute.</p> <p>For example, if:</p> $\begin{aligned} \text{Base} &= 200\text{mS} \\ N &= 2 \end{aligned}$ <p>Then,</p> $RTT_{avg} = 50\text{mS}$

The appliance declares a tunnel to be in brownout if it does not see a reply packet from the remote end within 300 mS of receiving the most recent packet.

In the Tunnel Advanced Options, **Base** is expressed as **Fastfail wait-time base offset (ms)**, and **N** is expressed as **Fastfail RTT multiplication factor**.

**Fastfail enabled** – This option is triggered when a tunnel's keep-alive signal does not receive a reply. The options are **disable**, **enable**, and **continuous**. If the disqualified tunnel subsequently receives a keep-alive reply, its recovery is instantaneous.

- For disable, keep-alives are sent every second, and 30 seconds elapse before failover. In that time, all transmitted data is lost.
- For enable, keep-alives are sent every second, and a missed reply increases the rate at which keep-alives are sent from one per second to ten per second. Failover occurs after one second.
- For continuous, keep-alives are continuously sent at ten per second. Therefore, failover occurs after one tenth of a second.

Field	Description
<b>Latency</b>	Amount of latency in milliseconds. Thresholds for Latency, Loss, or Jitter are checked once every second. <ul style="list-style-type: none"> <li>Receiving three successive measurements in a row that exceed the threshold puts the tunnel into a brownout situation and flows will attempt to fail over to another tunnel within the next 100 ms.</li> <li>Receiving three successive measurements in a row that drop below the threshold will drop the tunnel out of brownout.</li> </ul>
<b>Loss</b>	Amount of data lost as a percentage.
<b>Jitter</b>	Amount of jitter in milliseconds.
<b>Fastfail wait-time base offset</b>	Fastfail basic timeout time in milliseconds.
<b>Fastfail RTT multiplication factor</b>	Amount of RTT (Round Trip Time) added to the basic timeout.

## IKE Tab

Access the following fields by clicking the IKE tab. This tab is displayed only if the Mode field on the General tab is set to IPSec.

### IKE

Field	Description
<b>Authentication algorithm</b>	Authentication algorithm used for IKE security association (SA). <ul style="list-style-type: none"> <li>If the IPSec Suite B Preset field on the General tab is set to None, you can select <b>SHA1</b>, <b>SHA2-256</b>, <b>SHA2-384</b>, or <b>SHA2-512</b>. The default setting is SHA1.</li> <li>If the IPSec Suite B Preset field is set to any other setting, this field is automatically set to the appropriate algorithm.</li> </ul> <p><b>NOTE</b> With IKEv2 and the Encryption algorithm field set to auto, AES-GCM will probably be negotiated, which includes encryption and authentication. In this case, this field might show a SHA setting that is not actually used.</p> <ul style="list-style-type: none"> <li>If the Encryption algorithm field is set to AES-GCM-128 or AES-GCM-256, this field is not applicable.</li> </ul>
<b>Encryption algorithm</b>	Encryption algorithm used for IKE security association (SA). <ul style="list-style-type: none"> <li>If the IPSec Suite B Preset field on the General tab is set to None, and the IKE Version field is set to IKE v1, you can select <b>AES-CBC-128</b>, <b>AES-CBC-256</b>, or <b>auto</b>. The default setting is auto.</li> <li>If the IPSec Suite B Preset field is set to None, and the IKE Version field is set to IKE v2, you can select <b>AES-CBC-128</b>, <b>AES-CBC-256</b>, <b>AES-GCM-128</b>, <b>AES-GCM-256</b>, or <b>auto</b>. The default setting is auto.</li> <li>If the IPSec Suite B Preset field is set to any other setting, this field is automatically set to the appropriate algorithm.</li> </ul>

Field	Description
<b>Pseudo Random Function</b>	This field is displayed only if the IKE Encryption Algorithm field is set to AES-GCM-128 or AES-GCM-256. <ul style="list-style-type: none"> <li>For AES-GCM-128, you can select <b>SHA2-256</b>, <b>SHA2-384</b>, or <b>SHA2-512</b>.</li> <li>For AES-GCM-256, you can select <b>SHA-384</b> or <b>SHA-512</b>.</li> </ul>
<b>Diffie-Hellman group</b>	Diffie-Hellman Group used for IKE security association (SA) negotiation. <ul style="list-style-type: none"> <li>If the IPSec Suite B Preset field on the General tab is set to None, you can select the appropriate group. Available groups are 14 through 21, 26, and 31.</li> <li>If the IPSec Suite B Preset field is set to any other setting, this field is automatically set to the appropriate group.</li> </ul>
<b>Rekey interval/lifetime</b>	Rekey interval/lifetime of IKE security association (SA) in minutes. The default is 360 minutes.
<b>Dead peer detection</b>	<p><b>Delay time:</b> Interval (in seconds) to check the lifetime of the IKE peer.</p> <p><b>Retry count:</b> Number of times to retry the connection before determining that the connection is dead. This field is not editable.</p>
<b>Phase 1 mode</b>	Exchange mode for the IKE security association (SA) negotiation. <ul style="list-style-type: none"> <li>If the IKE Version field is set to IKE v1, you can select <b>Main</b> or <b>Aggressive</b>.</li> <li>If the IKE Version field is set to IKE v2, this field is automatically set to Aggressive.</li> </ul>
<b>IKE version</b>	<ul style="list-style-type: none"> <li>If the IPSec Suite B Preset field on the General tab is set to None, you can select <b>IKE v1</b> or <b>IKE v2</b>.</li> <li>If the IPSec Suite B Preset field is set to any other setting, this field is automatically set to IKE v2.</li> </ul>

## IPSec Tab

Access the following fields by clicking the IPSec tab. This tab is displayed only if the Mode field on the General tab is set to **IPSec** or **IPSec UDP**.

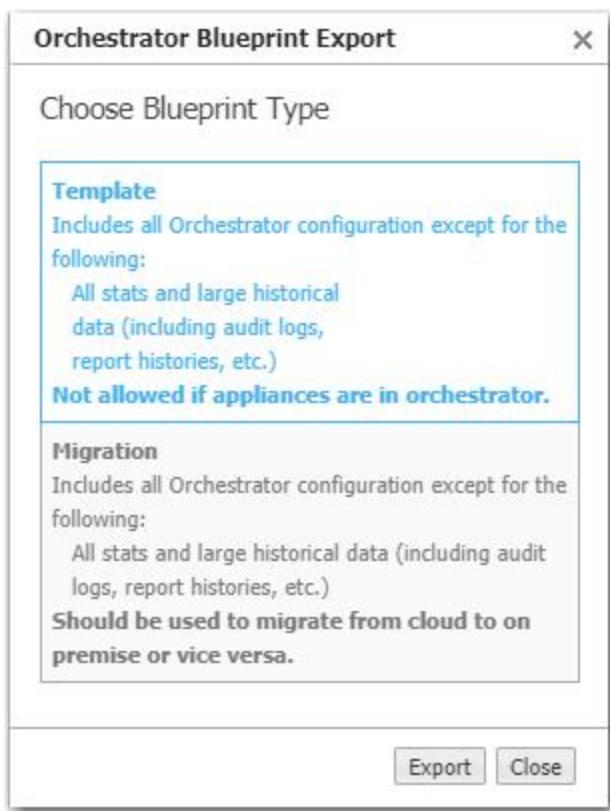
## IPSec

Field	Description
<b>Authentication algorithm</b>	<p>Authentication algorithm used for the IPSec security association (SA).</p> <ul style="list-style-type: none"> <li>If the IPSec Suite B Preset field on the General tab is set to None, you can select <b>SHA1</b>, <b>SHA2-256</b>, <b>SHA2-384</b>, <b>SHA2-512</b>, <b>AES-GMAC-128</b>, or <b>AES-GMAC-256</b>. The default setting is SHA1.</li> <li>If the IPSec Suite B Preset field is set to GMAC-128 or GMAC-256, this field is automatically set to the appropriate algorithm.</li> <li>If the IPSec Suite B Preset field is set to GCM-128 or GCM-256, this field is not applicable.</li> </ul>
<b>Encryption algorithm</b>	<p>Encryption algorithm used for the IPSec security association (SA).</p> <ul style="list-style-type: none"> <li>If the IPSec Suite B Preset field on the General tab is set to None, and the IPSec Authentication algorithm field is set to SHA1, SHA2-256, SHA2-384, or SHA2-512, you can select <b>AES-CBC-128</b>, <b>AEC-CBC-256</b>, <b>AES-GCM-128</b>, <b>AES-GCM-256</b>, <b>NULL</b>, or <b>Auto</b>. The default setting is Auto.</li> <li>If the IPSec Suite B Preset field is set to None, and the IPSec Authentication algorithm field is set to AES-GMAC-128 or AES-GMAC-256, this field is automatically set to NULL.</li> </ul>
<b>IPSec anti-replay window</b>	<p>Select a size from the drop-down list or <b>Disable</b> to disable the IPSec anti-replay window.</p> <p>If a size is selected, protection is provided against an attacker duplicating encrypted packets by assigning a unique sequence number to each encrypted packet.</p>
<b>Relay interval/lifetime</b>	Rekey interval/lifetime of the IPSec security association (SA) in minutes. The default is 360 minutes.
<b>Perfect forward secrecy group</b>	<p>Diffie-Hellman group used for IPSec security association (SA) negotiation. Based on the setting of the IPSec Suite B Preset field on the the General tab, this field is set to the following Diffie-Hellman group:</p> <ul style="list-style-type: none"> <li>For None: 14 (by default)</li> <li>For GCM-128 or GMAC-128: 19</li> <li>For GCM-256 or GMAC-256: 20</li> </ul>

## Orchestrator Blueprint Export

*Orchestrator > Orchestrator Server > Tools > Orchestrator Blueprint Export*

Use this dialog box to export the current Orchestrator configuration to a blueprint that you can apply to another Orchestrator instance.



You can use a blueprint when creating a new Orchestrator or when migrating an existing Orchestrator to on-prem or cloud.

- Blueprints can **only** be created from Orchestrators that have **no appliances** associated with them. If the source Orchestrator manages any appliances, blueprint creation will fail.
- You can create and store multiple blueprints with the same Orchestrator.
- After creating as many blueprints as you need, you then can add appliances to the source Orchestrator.
- Blueprints **automatically exclude** all statistics, large historical data files (including audit logs, report histories, and so forth), and account information.

To export an Orchestrator blueprint:

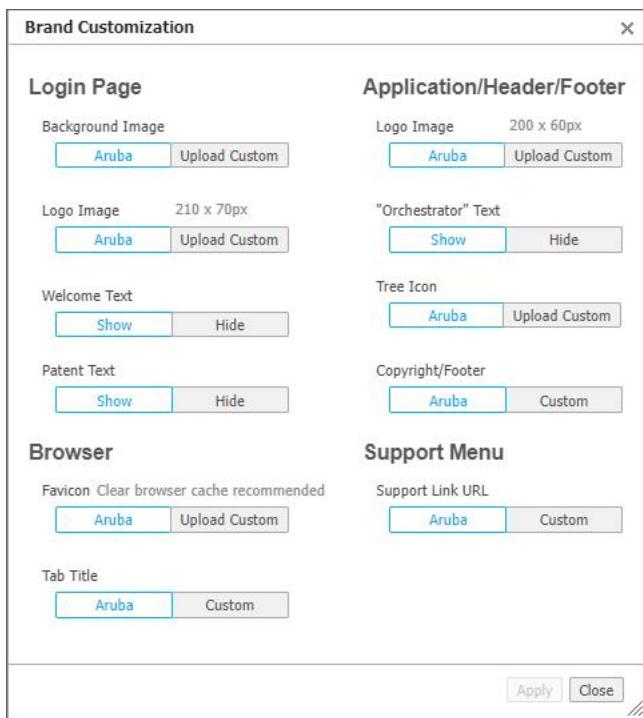
1. In the Orchestrator Blueprint Export dialog box, select the blueprint type: **Template** or **Migration**.
2. Click **Export**. Export will download an SQL file to your local desktop.

**WARNING** This will completely replace the configuration of the existing Orchestrator.

## Brand Customization

*Orchestrator > Orchestrator Server > Tools > Brand Customization*

Use this dialog box to customize the branding aspects of the Orchestrator user interface.



## Software & Setup

### Upgrade Orchestrator Software

*Orchestrator > Software & Setup > Upgrade > Upgrade Orchestrator*

If you are already using Orchestrator 8.6.0 or later and want to upgrade to a newer version, complete the following procedure.

**WARNING** An upgrade that fails can put Orchestrator into a corrupt state. Be sure to back up Orchestrator before you start the upgrade process.

1. Open an SSH session to the Orchestrator.
2. Log in as **admin** or a user with administrative privileges.

3. Switch to root:

```
su - root
```

4. Enter the root password when prompted. Contact Support if you do not know your root password.
5. Change to the /home directory:

```
cd /home
```

Depending on your environment, you can upgrade Orchestrator in either of the following ways:

- Upgrade via HTTP
- Upgrade via SCP

### Upgrade via HTTP

If you have an HTTP URL to the Orchestrator installation file, enter the following in the existing SSH console to run the install script and point it to the hosted installation file:

```
/home/gms/gms/setup/install_orchestrator.sh <HTTP URL of the Orchestrator Installation File>
```

**NOTE** The upgrade process can take several hours to complete.

### Upgrade via SCP

If you do not have an HTTP server, copy the installation file to Orchestrator by using SCP, run the install script, and point it to the local installation file:

**NOTE** This procedure assumes that the scp programs on both ends are patched for [CVE-2020-15778](#) and/or you trust the remote server from which you will scp the installation file.

1. From the Orchestrator SSH console, enter the following as root:

```
mv /bin/scp-local /bin/scp #
```

2. From your local PC console, enter the following:

```
scp <Orchestrator Installation file> admin@<orchestrator_ip_address>:/home/gms
```

3. From the Orchestrator SSH console, enter the following:

```
/home/gms/gms/setup/install_orchestrator.sh /home/gms/<Orchestrator Installation file>
```

**NOTE** The upgrade process can take several hours to complete.

## Check for Orchestrator and Appliance Software Updates

*Orchestrator > Software & Setup > Upgrade > Check for Updates*

These pages show what appliance and Orchestrator server software is available for download.

**Check for Updates**

**Orchestrator Releases**

Release	Type	Release Date	Description	Release Notes
8.3.0.00000	BETA	03-Nov-17 00:00		
8.4.0.35900	BETA	13-May-18 00:00	Test for orchestrator feature GMS-11402	<a href="#">Download</a>
99.99.99.35870	BETA	13-May-18 00:00	Test for orchestrator feature GMS-11402	<a href="#">Download</a>
99.99.99.36894	BETA	13-May-18 00:00	Test for orchestrator feature GMS-11402	<a href="#">Download</a>

**VXOA Releases**

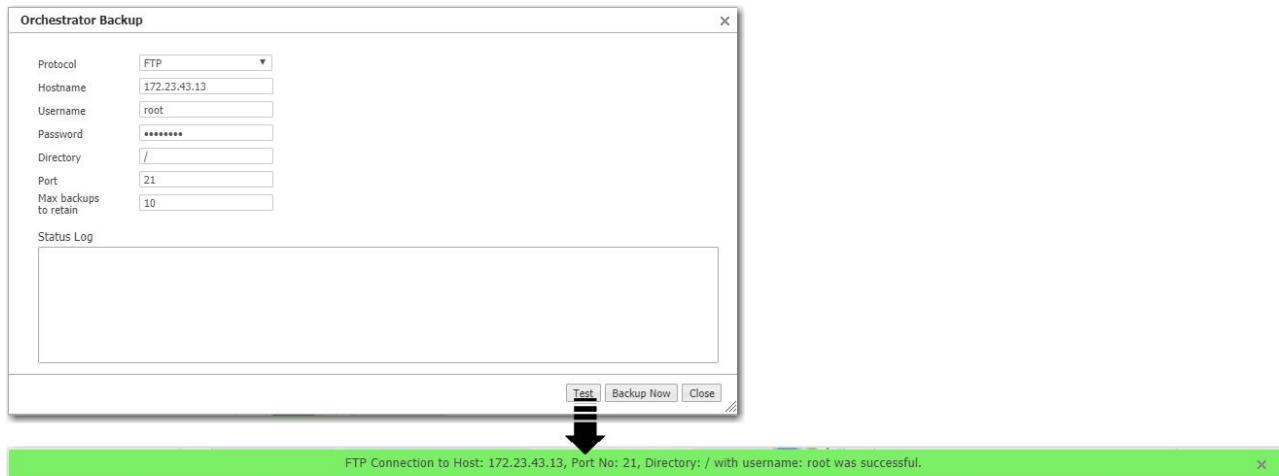
Release	Type	Release Date	Description	Release Notes
0.0.0.0_67610	BETA	09-Nov-17 00:00	KR test vxoa image	
0.0.0.0_67847	BETA	27-Nov-17 00:00	KR test	
8.1.7.1_68811	GA	07-Feb-18 00:00		
8.1.7.3_69551	BETA	09-Apr-18 00:00	rma testing	
8.1.7.7_70949	GA	15-May-18 00:00	test for upgrade from portal image	
8.1.7.7_72000	BETA	15-May-18 00:00	For testing purpose only	

[Go to Support Portal to Download](#) [Close](#)

## Back Up on Demand

*Orchestrator > Software & Setup > Backup > Backup Now*

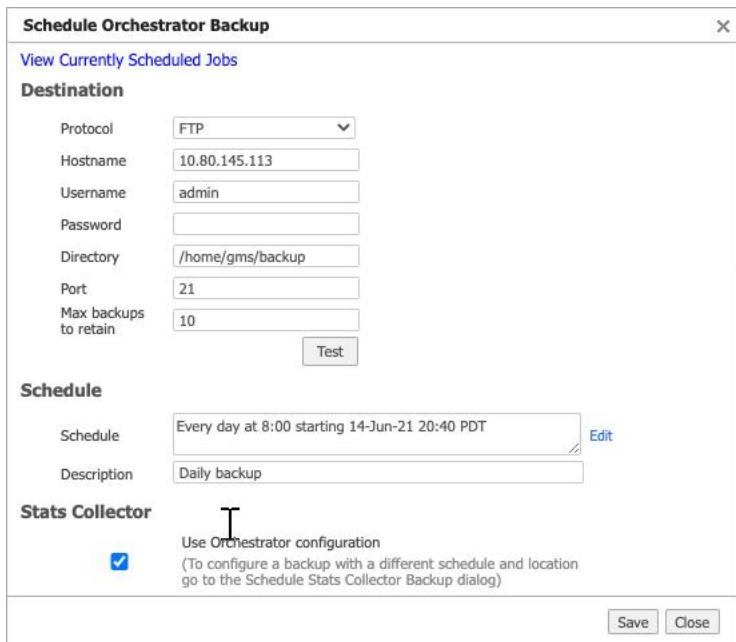
Use this dialog box to backup the Orchestrator database on demand.



## Schedule Orchestrator Backup

*Orchestrator > Software & Setup > Backup > Schedule Backup*

Use this dialog box to schedule backups of the Orchestrator database and optionally schedule backups of the Orchestrator Stats Collector using the same destination and schedule.



Field	Description
<b>View Currently Scheduled Jobs</b>	Click to open the Scheduled Jobs tab.
<b>Protocol</b>	Protocol to apply: <b>FTP</b> , <b>SCP</b> , <b>HTTP</b> , <b>HTTPS</b> , or <b>SFTP</b> .
<b>Hostname</b>	Host name of the backup server.
<b>Username</b>	Username that the Orchestrator server uses to log in to the backup server.
<b>Password</b>	Password for the username.
<b>Directory</b>	Directory name of the backup server.
<b>Port</b>	Port number of the backup server.
<b>Max backups to retain</b>	Maximum number of backups to retain.
<b>Test</b>	Click <b>Test</b> to verify that Orchestrator can reach the destination.
<b>Schedule</b>	To create a schedule, click <b>Add</b> . To modify a schedule, click <b>Edit</b> . In the Schedule dialog box, select <b>Daily</b> , <b>Weekly</b> , <b>Monthly</b> , or <b>Yearly</b> . Complete the remaining fields, and then click <b>OK</b> . <b>TIP</b> To specify the timezone for scheduled jobs and reports, navigate to <b>Orchestrator &gt; Software &amp; Setup &gt; Setup &gt; Timezone for Scheduled Jobs</b> .
<b>Description</b>	(Optional) Description for the backup schedule.
<b>Stats Collector</b>	Do one of the following: <ul style="list-style-type: none"> <li>Select the <b>Use Orchestrator configuration</b> check box to back up the Orchestrator Stats Collector on the same schedule and to the same destination.</li> <li>Clear the <b>Use Orchestrator configuration</b> check box to specify a different backup destination and set a different schedule for the Orchestrator Stats Collector.</li> </ul> <b>CAUTION</b> If you clear the <b>Use Orchestrator configuration</b> check box, and you do not complete the Schedule Stats Collector Backup dialog box, the Stats Collector will not be backed up. For more information, see <a href="#">Schedule Stats Collector Backup below</a> .

## Schedule Stats Collector Backup

*Orchestrator > Software & Setup > Backup > Schedule Stats Collector Backup*

Use this dialog box to schedule backups of the Orchestrator Stats Collector.

**Schedule Stats Collector Backup**

[View Currently Scheduled Jobs](#)

Use Orchestrator backup configuration

**Destination**

Protocol	SCP
Hostname	10.99.217.23
Username	admin
Password	
Directory	/home/gms
Port	22
Max backups to retain	4

**Schedule**

Schedule	Every day at 20:08 starting 12-Aug-21 23:58 PDT
Description	sss

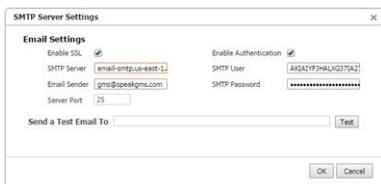
**Buttons:** Save | Close

Field	Description
<b>View Currently Scheduled Jobs</b>	Click to open the Scheduled Jobs tab.
<b>Use Orchestrator backup configuration</b>	Select this check box to back up the Stats Collector using the same destination and schedule set in the Schedule Orchestrator Backup dialog box. For more information, see <a href="#">Schedule Orchestrator Backup on page 510</a> .
<b>Protocol</b>	Protocol to apply: <b>FTP, SCP, HTTP, HTTPS, or SFTP</b> .
<b>Hostname</b>	Host name of the backup server.
<b>Username</b>	Username that the Orchestrator server uses to log in to the backup server.
<b>Password</b>	Password for the username.
<b>Directory</b>	Directory name of the backup server.
<b>Port</b>	Port number of the backup server.
<b>Max backups to retain</b>	Maximum number of backups to retain.
<b>Test</b>	Click <b>Test</b> to verify that Orchestrator can reach the destination.
<b>Schedule</b>	To create a schedule, click <b>Add</b> . To modify a schedule, click <b>Edit</b> . In the Schedule dialog box, select <b>Daily, Weekly, Monthly, or Yearly</b> . Complete the remaining fields, and then click <b>OK</b> . <b>TIP</b> To specify the timezone for scheduled jobs and reports, navigate to <b>Orchestrator &gt; Software &amp; Setup &gt; Setup &gt; Timezone for Scheduled Jobs</b> .
<b>Description</b>	(Optional) Description for the backup schedule.

## SMTP Server Settings

*Orchestrator > Software & Setup > Setup > SMTP Server Settings*

For permanent and private email delivery, change the SMTP (Simple Mail Transfer Protocol) server and settings to your company's SMTP settings.

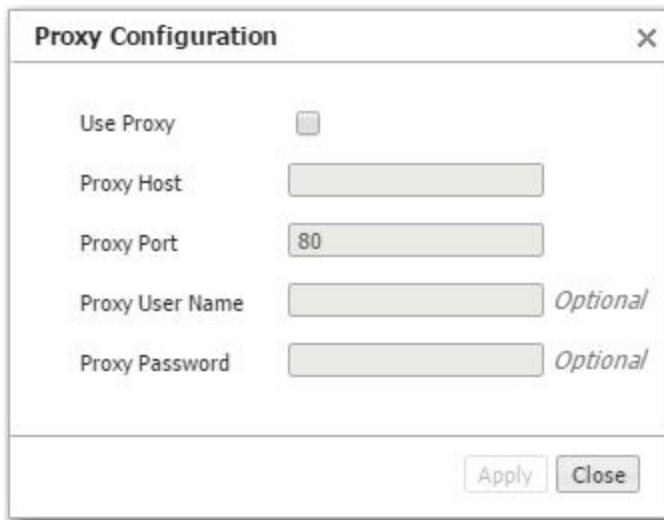


- If a test email does not arrive within minutes, check your firewall.
- After configuring the SMTP settings, you can specify email recipients for:
  - **alarms** (Monitoring > Alarms > Alarm Email Recipients), and
  - **reports** (Monitoring > Reporting > Schedule & Run Reports)

## Proxy Configuration

*Orchestrator > Software & Setup > Setup > Proxy Configuration*

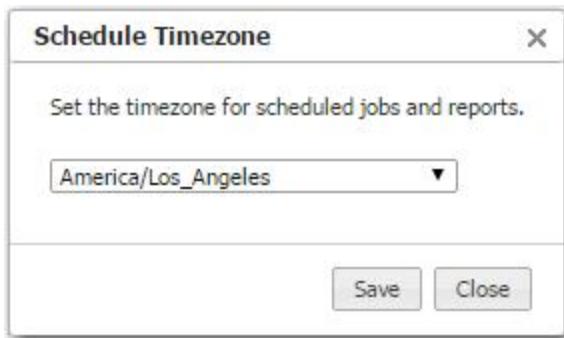
If necessary (for example, because of firewall issues), you can configure a proxy for reaching the Cloud Portal.



## Timezone for Scheduled Jobs

*Orchestrator > Software & Setup > Setup > Timezone for Scheduled Jobs*

Use this dialog box to set the timezone for scheduled jobs and reports.



## Orchestrator Advanced Properties

*Orchestrator > Software & Setup > Setup > Advanced Properties*

**IMPORTANT:** Changing the default settings is not recommended without consulting Support.

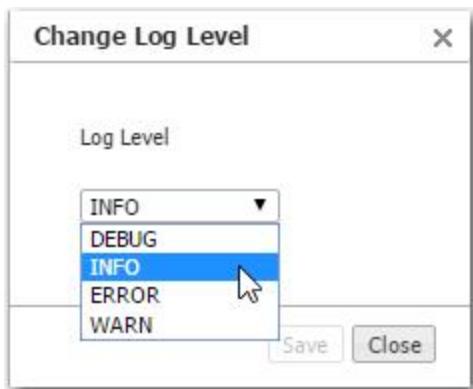
Orchestrator Advanced Properties		
IMPORTANT: Changing the default values of these settings is not recommended without consulting Aruba.		
Property Name	Property Value	Restart Required
fileOpsChunkSize	1048576	No
dbJdbcSocketTimeoutLongRunningQu...	0	Yes
statsNumberOfAppliancesToFetchInEa...	2	No
ParallelOrchestrationTasks	50	Yes
restRequestTimeout	60	Yes
sslExcludeCiphers	*NULL*, *RC4*, *MD5*, *DES*, *...	Yes
interfaceBandwidthCheckPerTunnelOv...	6	No
ContentSecurityPolicyHeaderEnabled	true	Yes
zscalerParallelTasks	1	Yes
excludeTables	false	No
dbMigrationPauseTime	0	No
azureVWANParallelTasks	1	Yes
maxNotificationQueueSize	100000	Yes
jvmArgsMaxHeap(MB)		Yes
endToEndEncryptionKeyLifeSpan(Days)	30	Yes
statsMinutesCatchUpThreshold	43200	No
interfaceBandwidthCheckMinimumNu...	100	No
bridgeCacheExpireTime	120	Yes
dbPoolMaxConnectionLifeTime	300000	Yes
..		

## Change the Orchestrator Log Level

*Orchestrator > Software & Setup > Setup > Change Log Level*

Use this form to change what level of server-side Orchestrator logs are retained.

The default is **INFO**.



## Minimum Severity Levels

In decreasing order of severity, the levels are as follows.

Level	Description
<b>ERROR</b>	An error. This is a non-urgent failure.
<b>WARNING</b>	A warning condition. Indicates an error will occur if action is not taken.
<b>INFORMATIONAL</b>	Informational. Used by Support for debugging.
<b>DEBUG</b>	Used by Support for debugging.

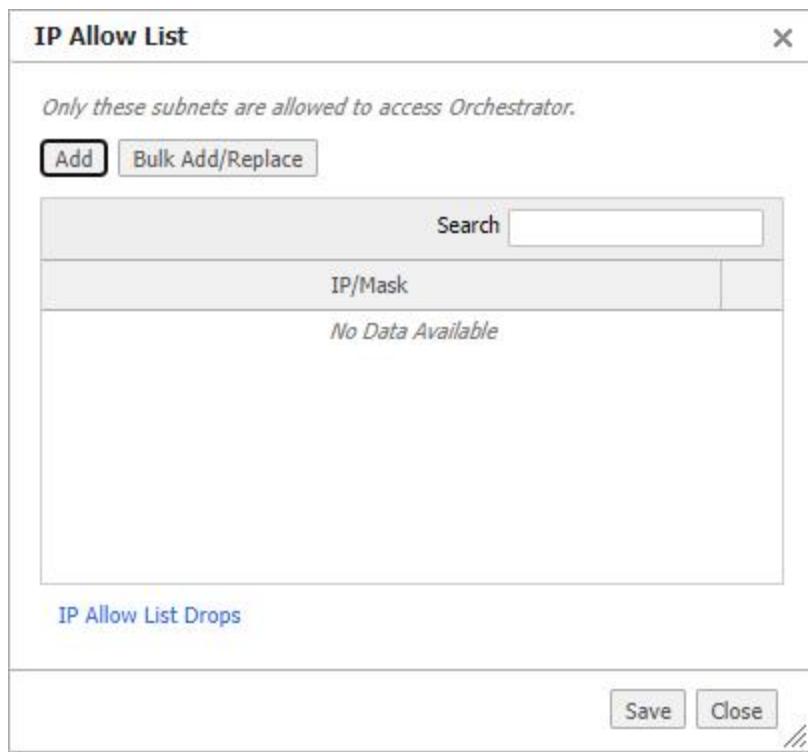
- The bolded part of the name is what displays in Orchestrator logs.
- If you select **INFO** (the default), the log records any event with a severity of INFO, WARNING, and ERROR.
- These are purely related to event logging levels, **not** alarm severities, even though some naming conventions overlap. Events and alarms have different sources. Alarms, when they clear, list as the **ALERT** level in the **Event Log**.

## IP Allow List

*Orchestrator > Software & Setup > Setup > IP Allow List*

**IP Allow List** is a feature that restricts access to Orchestrator to a specified list of source subnets.

If a source IP address changes (for example, with NAT IP), users can get locked out of Orchestrator.

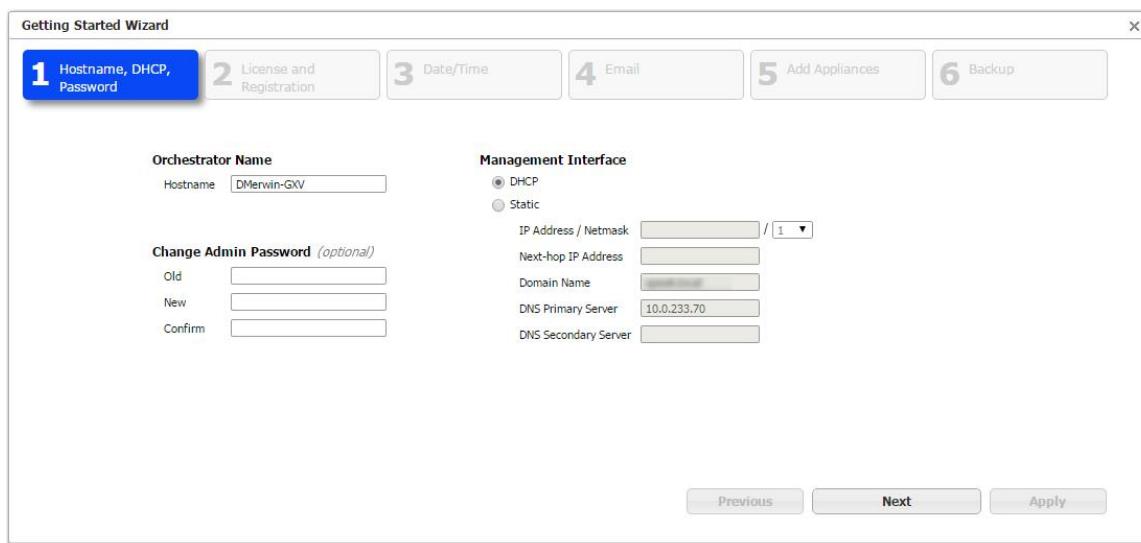


To view a list of traffic that has been dropped because of these restrictions, click **IP Allow List Drops**.

## Orchestrator Getting Started Wizard

*Orchestrator > Software & Setup > Setup > Configuration Wizard*

When you first install Orchestrator and use a web browser to access the IP address you have assigned it, the Orchestrator **Getting Started Wizard** opens.



The wizard guides you through the basics of configuring the following:

Setting	Description
<b>Orchestrator Name, management IP address, and password</b>	The default for username and password is <b>admin</b> .
<b>License and Registration</b>	EdgeConnect registration is required for Cloud-based features and products, including CPX and SaaS. The associated Account Name and Account Key enable Orchestrator to discover EdgeConnect appliances via the Cloud Portal, as they are added to your network.
<b>Date/Time</b>	Using an NTP server is strongly recommended so that data is synchronized across Orchestrator and the appliances.
<b>Email</b>	Change the default settings to your Company's SMTP server, and then test. Separate fields are provided for Global Report recipients and Alarm recipients.
<b>Add Appliances</b>	(Optional) You can use this to add NX, VX, and VRX appliances that are already up and running in your network. You can also add them later.
<b>Backup</b>	Specifies the database backup destination, transfer protocol, and backup schedule.

If you do not **Apply** after you complete the last page, the Orchestrator wizard reappears at your next login.

To access the Orchestrator wizard again after initial configuration, navigate to **Orchestrator > Software & Setup > Setup > Configuration Wizard**.

## Statistics Retention

This tab displays all the statistics Orchestrator collects from appliances. Orchestrator saves the statistics data in a database with the retention policies defined on this tab. Complete the following steps to begin.

1. Click the edit icon in the table next to the statistic you want Orchestrator to collect.
2. Select the **Collect this statistic in Orchestrator** check box to enable or disable statistics collection.
3. Enter how long you want Orchestrator to retain the statics for Minute Granularity, Hourly Granularity, and Daily Granularity before it collects data and stores in the partition.

**TIP** If you click **More Options**, you can enter values for the Database Duration.

4. Click **Apply**.

Refer to the table below for more detail.

Field	Description
<b>Statistic</b>	The selected statistic of which you want Orchestrator to collect data.
<b>Enabled</b>	If you have enabled or disabled statistics retention.
<b>Minute Granularity (hours)</b>	Amount of times in one minute Orchestrator stores data.
<b>Hourly Granularity (days)</b>	Amount of times in one hour Orchestrator stores data.
<b>Daily Granularity (months)</b>	Amount of time in one day Orchestrator stores data.
<b>Estimated Disk Space</b>	Estimated amount of disk space the selected statistic uses. At the bottom of the screen, you can get an estimated disk space required for a number of appliances, overlays, and tunnels.

To display the default settings for appliance properties, click **Advanced Properties**.

**IMPORTANT:** Changing the default values of these settings is not recommended without consulting Support.

## Stats Collector Configuration

*Orchestrator > Software & Setup > Setup > Stats Collector Configuration*

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

To improve Orchestrator performance, Orchestrator 9.1.0 includes a new Stats Collector feature that eliminates the use of Orchestrator resources for monitoring your appliances. This new architecture enables you to scale your network with greater performance.

The new Stats Collector feature collects statistics from appliances and provides the information to Orchestrator. When enabled, the new Stats Collector runs in parallel with the legacy stats collector to collect the necessary historical statistical data. After collecting that data, you can discontinue legacy stats collection. You will not experience performance improvement until you discontinue legacy stats collection.

## Prerequisites

- Upgrade all appliances to version 9.1.0 before enabling the new Stats Collector feature.
- Create at least one remote stats collector for every 150 appliances—if you have less than 150 appliances, you can use the predefined local stats collector. Each remote stats collector must meet the following minimum requirements:
  - CPU: 4 GHz
  - RAM: 16 GB

## Before You Begin

Before you configure the new Stats Collector feature in Orchestrator, you must:

1. [Create a Remote Stats Collector below](#).
2. [Authenticate the Remote Stats Collector on the next page](#).

Create and authenticate as many remote stats collectors as needed.

## Create a Remote Stats Collector

To create a remote stats collector, use the Command Line Interface (CLI) to run an Orchestrator on a virtual machine (VM) in Stats Collector Mode only, as follows.

1. Open an SSH session to the Orchestrator you want to use as a remote stats collector.
2. Log in as **admin** or a user with administrative privileges.
3. Switch to root:  
`su - root`
4. When prompted, enter the root password. If you do not know your root password, contact Support.
5. Change to the gms directory:  
`cd gms`
6. Enter `orch-setup`, and then press Enter.
7. Enter `-m`, and then press Enter.
8. Enter the root password, and then press Enter.
9. At the prompt, enter `s`.
10. To proceed, enter `y`.

This VM is now a remote stats collector. Note the DNS name. You will need the DNS name when you configure the remote stats collector in Orchestrator.

## Authenticate the Remote Stats Collector

After you create a remote stats collector, authenticate it by copying the Orchestrator public key and pasting it into the same folder on the new remote stats collector, as follows.

1. Open an SSH session to the Orchestrator.
2. Log in as **admin** or a user with administrative privileges.
3. Go to:  
`cd /home/gms/sc/publickeys`
4. To list the public key, enter `ls`, and then press Enter.
5. Copy the public key.
6. Open an SSH session to the remote stats collector.
7. Log in as **admin** or a user with administrative privileges.
8. Go to:  
`cd /home/gms/sc/publickeys`
9. Paste the public key, and then press Enter.

## Configure the New Stats Collector Feature

After the remote stats collectors are created and authenticated, configure the new Stats Collector feature in Orchestrator. Complete the following tasks:

1. Back up Orchestrator. For more information about backing up Orchestrator, see [Back Up on Demand on page 509](#).  
Before you enable the new Stats Collector feature and discontinue legacy stats collection, it is recommended that you back up the Orchestrator database. Discontinuing legacy stats collection is permanent. To return to your previous configuration, you must restore the Orchestrator configuration backup.
2. [Add Remote Stats Collectors below](#). You need at least one remote stats collector for every 150 appliances. If your network contains less than 150 appliances, you can use the predefined local stats collector.
3. [Associate Appliances with a Remote Stats Collector on the next page](#) or [Associate Appliances with the Predefined Local Stats Collector on page 523](#)
4. When the necessary historical data has been collected, [Discontinue Legacy Stats Collection on page 524](#).

## Add Remote Stats Collectors

You must add at least one remote stats collector for every 150 appliances in your network.

To add a remote stats collector:

1. Navigate to **Software & Setup > Setup > Stats Collector Configuration**.

The Stats Collector Configuration tab opens.

2. Click **Edit Remote Stats Collectors**.

The Edit Stats Collectors dialog box opens.

3. Click **Add Remote Stats Collector**.

The New Stats Collector dialog box opens.

4. Configure the following elements as needed:

Field	Description
<b>Name</b>	Name of the remote stats collector.
<b>DNS Name</b>	DNS name you noted when you created this remote stats collector.
<b>Port</b>	Port number the remote stats collector is running on.
<b>Protocol</b>	HTTPS.

5. Click **Save**.

## Delete a Remote Stats Collector

To delete an existing remote stats collector, click the delete icon (X) in the last column of the entry in the table.

## Associate Appliances with a Remote Stats Collector

To associate appliances with a remote stats collector:

1. Navigate to **Software & Setup > Setup > Stats Collector Configuration**.

The Stats Collector Configuration tab opens.

2. In the Orchestrator appliance tree, select one or more appliances to associate with a specific remote stats collector. You can associate up to 150 appliances with each remote stats collector.

**IMPORTANT:** The statistics for an appliance are tied to the remote stats collector it is associated with. If you associate an appliance with a different remote stats collector, you lose all statistical data associated with that appliance.

3. Select the **Add** check box next to the remote stats collector you want to associate the selected appliance(s) with.

4. Click **Apply**.

The Apply Changes dialog box opens.

5. Click **Apply Changes**.

## Associate Appliances with the Predefined Local Stats Collector

If you are installing Orchestrator version 9.1.0 or upgrading to version 9.1.0 or later, Orchestrator provides a default stats collector called “local.” You cannot edit or delete the local stats collector. You can associate up to 150 appliances with the local stats collector.

**NOTE** If you are upgrading to Orchestrator 9.1.0, all appliances will be automatically associated with the local stats collector.

**NOTE** If you run Orchestrator in Orchestrator Only mode (`orch-setup -m o`), the local stats collector will be disconnected.

To associate appliances with the local stats collector:

1. Navigate to **Software & Setup > Setup > Stats Collector Configuration**.

The Stats Collector Configuration tab opens. This tab displays the stats collector configuration for all appliances selected in the appliance tree to the left.

2. In the Orchestrator appliance tree, select one or more appliances to associate with the local stats collector.
3. Select the **Add** check box next to the local stats collector.
4. Click **Apply**.

The selected appliances are associated with the local stats collector. The Changes column indicates the stats collectors that were added and removed.

## Enable the New Stats Collector

After you associate appliances with either the local stats collector or new remote stats collectors, you must enable the new Stats Collector feature to begin collecting data.

**NOTE** The legacy stats collector continues to collect statistics in parallel with the new Stats Collector feature until you discontinue legacy stats collection. For more information, see [Discontinue Legacy Stats Collection on the next page](#).

**IMPORTANT:** You cannot disable the new Stats Collector after you enable it. It is recommended that you back up Orchestrator before you enable the new Stats Collector. For more information about backing up Orchestrator, see [Back Up on Demand on page 509](#).

To enable the new Stats Collector:

1. Navigate to **Software & Setup > Setup > Stats Collector Configuration**.

The Stats Collector Configuration tab opens.

2. Click **Enable New Stats Collection**.

The Enable New Stats Collection dialog box opens.

Before you can enable the new Stats Collector feature, you must upgrade all appliances to version 9.1.0. The Enable New Stats Collection dialog box lists appliances that must be upgraded to support the new stats collection.

3. Click **Enable New Stats Collection Now**.

### Discontinue Legacy Stats Collection

**IMPORTANT:** Do not discontinue legacy stats collection until you have collected sufficient historical data with the new Stats Collector feature. For example, if you need 30 days of statistical data, enable the new Stats Collector, wait 30 days, and then disable the legacy stats collection.

To discontinue legacy stats collection:

1. Navigate to **Software & Setup > Setup > Stats Collector Configuration**.

The Stats Collector Configuration tab opens.

2. Click **Discontinue Legacy Stats Collection**.

The Discontinue Legacy Stats Collection dialog box opens.

**IMPORTANT:** This step permanently disables legacy stats collection and deletes all legacy statistics.

3. Click **Discontinue Legacy Stats Collection**.

## Notification Banner

You can add a notification in the header of your Orchestrator UI if you are conducting downtime or for maintenance reasons. Complete the following steps to add a notification.

1. Navigate to **Orchestrator > Software & Setup > Setup > Notification Banner** in Orchestrator.

The Notification dialog box opens.

2. Enter the message you want to display in the Orchestrator header.

3. Click **Save**.

## Aruba Central

### Aruba Central Site Mapping

*Orchestrator > Aruba Central > Aruba Central Site Mapping*

Use this tab to create an Aruba Central account in Orchestrator. After you create an Aruba Central account, Orchestrator maps EdgeConnect appliances to Aruba Central sites. When mapped, EdgeConnect appliances display in the Network Health tab in Aruba Central and provide real-time site health updates.

**NOTE** Single Sign-On (SSO) to Aruba Central from Orchestrator is not supported. If your account is SSO-enabled, or if two-factor user verification is enabled, you will not be able to use the account for Central Site Mapping integration.

## Prerequisites

Before you can integrate Unity EdgeConnect devices with Aruba Central, you must do the following:

1. Create an Aruba Central account. For more information on creating an Aruba Central account, see [Aruba Central Online Help](#) and search for **Unity EdgeConnect Integration**.
2. Generate an API token for Orchestrator in Aruba Central. For more information on generating an API token for Orchestrator, see [Aruba Central Online Help](#) and search for **Unity EdgeConnect Integration**.
3. Have existing Aruba Central sites to map EdgeConnect appliances to. If you do not have any existing Aruba Central sites, you can export the location details for EdgeConnect appliances and create Aruba Central sites in bulk from that exported list. For more information on creating Aruba Central Sites in bulk, see [Create Aruba Central Sites in Bulk](#) on the next page.

You need the following details from your Aruba Central account.

Field	Steps
<b>Customer ID</b>	Navigate to <b>Account Home</b> , and then click the User icon in the upper right corner.
<b>Email</b>	Navigate to <b>Account Home &gt; API Gateway &gt; System Apps &amp; Tokens</b> . The email is listed in the <b>Name</b> column.
<b>Password</b>	Navigate to <b>Account Home &gt; API Gateway &gt; System Apps &amp; Tokens</b> , and then click <b>View Tokens</b> . <b>NOTE</b> If the Aruba Central password changes, you must update this password whether authentication is configured as a system user or as a federated user. <b>NOTE</b> If you do not remember the password, you must reset the Aruba Central password from Aruba Central. For more information on resetting your Aruba Central password, see <a href="#">Aruba Central Online Help</a> .
<b>Client ID</b>	Navigate to <b>Accounts Home &gt; API Gateway &gt; APIs &gt; System Apps &amp; Tokens</b> .
<b>Client Secret</b>	Navigate to <b>Accounts Home &gt; API Gateway &gt; APIs &gt; System Apps &amp; Tokens</b> .
<b>API Gateway URL</b>	Navigate to <b>Account Home &gt; API Gateway</b> . The URL is listed in the <b>Documentation</b> column. <b>NOTE</b> Copy the URL <i>without</i> the protocol (for example, internal-apigw.central.arubanetworks.com).

## Create Aruba Central Sites in Bulk

1. In Orchestrator, navigate to **Administration > Software > Upgrade > System Information**.
  2. In the appliance tree, select the appliances you want to create Aruba Central sites for, and then click **Export**.  
Orchestrator creates and downloads a .csv file.
  3. Open the .csv file, and then delete the three header rows.
- TIP** Refer to the sample import file provided by Aruba Central for proper formatting. To view the sample import file, in Aruba Central, navigate to **Launch > Network Operations > Organization > Sites > Bulk Update**, and then click **Download a sample file** on the Bulk Import dialog.
4. Save and close the file.
  5. In Aruba Central, navigate to **Launch > Network Operations > Organization > Sites**.
  6. Scroll to the bottom of the page, click **Bulk Upload**, and then follow the prompts.

## Create an Aruba Central Account in Orchestrator

To create an Aruba Central account in Orchestrator:

1. On the Aruba Central Site Mapping tab, click **Aruba Central Account**.

The Aruba Central Account dialog box opens.

2. Configure the following elements as needed:

Field	Description
<b>Aruba Central</b>	Status of the connection.
<b>Customer ID</b>	Customer ID generated from Aruba Central.
<b>Email</b>	Email provided by Aruba Central.
<b>Password</b>	Aruba Central password. <b>NOTE</b> If the Aruba Central password changes, you must update this password whether authentication is configured as a system user or as a federated user. <b>NOTE</b> If you do not remember the password you must reset the Aruba Central password from Aruba Central. For more information on resetting your Aruba Central password, see <a href="#">Aruba Central Online Help</a> .
<b>Client ID</b>	Client ID generated from Aruba Central.
<b>Client Secret</b>	Client Secret generated from Aruba Central.
<b>API Gateway URL</b>	API Gateway URL without protocol (for example, internal-apigw.central.arubanetworks.com).

3. To test the connection, click **Test**.
4. If the connection is successful, click **Save**.

Orchestrator maps EdgeConnect appliances to Aruba Central sites based on geolocation. (Addresses assigned to EdgeConnect appliances are converted to geolocations.)

5. If "None" displays in the Aruba Central Site column of an appliance, Orchestrator did not locate an Aruba Central site within range of the appliance (within 0.2 degrees of the `latitudeDelta` and the `longitudeDelta` combined). Do one of the following:
  - Edit the appliance and manually map it to any Aruba Central site. For more information on mapping an EdgeConnect appliance to an Aruba Central site, see [Edit EdgeConnect to Aruba Central Site Mapping below](#).
  - Add an Aruba Central Site within range of the EdgeConnect appliance, and then check for site list updates. For more information on checking for site list updates, see [Check for Site List Updates on the next page](#).

## Edit EdgeConnect to Aruba Central Site Mapping

Orchestrator maps EdgeConnect appliances to Aruba Central sites based on geolocation. Orchestrator maps EdgeConnect appliances to Aruba Central sites that are within 0.2 degrees of the `latitudeDelta` and the `longitudeDelta` combined.

You can edit an EdgeConnect appliance to map it to a different Aruba Central site. You can also edit an EdgeConnect appliance to map it to an Aruba Central site if Orchestrator did not locate an Aruba Central site within range of the EdgeConnect appliance.

To map an EdgeConnect appliance to an Aruba Central site:

1. Click the Edit icon next to an EdgeConnect appliance.

The Edit EdgeConnect to Aruba Central Site Mapping dialog box opens.

2. Configure the following elements as needed:

Field	Description
<b>EdgeConnect Appliance</b>	Selected EdgeConnect appliance.
<b>Aruba Central Site</b>	Available sites to map the EdgeConnect appliance to.
<b>Geolocation Suggested Site</b>	Aruba Central site that Orchestrator mapped by geolocation to the EdgeConnect appliance. <b>NOTE</b> If you map the EdgeConnect appliance to any other site, the site that Orchestrator suggests based on geolocation will display next to that site in parentheses.

3. Click **Save**.

Orchestrator maps the appliance to the Aruba Central site you selected.

## Check for Site List Updates

To refresh the Aruba Central site list in Orchestrator to check for Aruba Central site list updates, click **Check for Site List Updates**.

If new Aruba Central sites are detected within range of unmapped EdgeConnect appliances (within 0.2 degrees of the `latitudeDelta` and the `longitudeDelta` combined), Orchestrator maps the EdgeConnect appliances to the new Aruba Central sites.

## ClearPass Policy Manager

*Orchestrator > Aruba Central > ClearPass Policy Manager*

Orchestrator 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.

The ClearPass Policy Manager tab displays information about users and devices provisioned to access your network via ClearPass. The searchable information on this tab includes details such as username, IP address, and role.

You can apply the following filters to your ClearPass logs:

- Select the **All**, **Active**, or **Historical** filters to determine which actions you want to display in the table.
- Select **Auto Refresh** or **Pause** to refresh or pause the table. By default, the table refreshes automatically.
- To limit the filtering criteria, enter a value in the **Record Count** field. The default value is 500, and the maximum number you can filter is 10,000.
- To filter by date and time, enter values in the **From** and **To** fields.
- To search for a specific username, enter a value in the **User** field. You can search a wild card character (\*) as a username using the following schema:
  - **x\*** = anything that starts with the entered value
  - **\*x** = anything that ends with the entered value
- To search for a specific IP address, enter a value in the **IP** field.

To export a .csv file of your table, click **Export**.

Field	Definition
<b>Start Time</b>	Time when the device began its network session.
<b>End Time</b>	Time when the device ended its network session.

Field	Definition
<b>CPPM</b>	ClearPass Policy Manager server used to authenticate.
<b>IP Address</b>	IP address authenticated to the network.
<b>Username</b>	Username authenticated to the network.
<b>Role</b>	Role assigned to the user that authenticated to the network.
<b>Device Type</b>	Device type used to connect to the network.
<b>MAC Address</b>	MAC address of the system connecting to the network.
<b>Posture</b>	Security health posture of the connected device.
<b>Location ID</b>	Location ID of the user connecting to the network.
<b>Protocol</b>	Type of authentication server used to connect to the network.
<b>Details</b>	All user information sent from CPPM but not required by Orchestrator. Values are in JSON format.

## Manage ClearPass Policy Manager Accounts

Click **Accounts** on the ClearPass Policy Manager tab to view and manage ClearPass accounts that are associated with Orchestrator.

**NOTE** Before you begin the ClearPass Policy Manager (CPPM) configuration in Orchestrator, you must have a ClearPass account to authenticate and authorize Orchestrator. If you do not have these credentials, contact your system administrator.

## View ClearPass Policy Manager Accounts

The ClearPass Policy Manager Accounts dialog box displays the following information about ClearPass accounts that are already associated with Orchestrator:

Field	Definition
<b>Edit</b>	Click the icon to edit your CPPM instance.
<b>Name</b>	Name of your CPPM instance.
<b>Domain/IP</b>	Domain or URL of your CPPM instance.
<b>Connectivity</b>	Status of the connection between Orchestrator and your CPPM instance. The status may appear as Connected, Connecting, Auth Failed, and Unreachable.
<b>Service Status</b>	Status of your CPPM instance. A status other than Connected could indicate a problem with your CPPM configuration. To troubleshoot, click the Info icon, and then reset any service that is not currently connected.
<b>Pause</b>	To pause the connection for your CPPM instance, click this toggle.

## Add a ClearPass Policy Manager Server

Follow the steps below to add a new ClearPass Policy Manager account.

1. If not already opened, click **Accounts** to open the ClearPass Policy Manager Accounts dialog box.
2. Click **+Add New Server**.

The ClearPass Policy Manager Server Configuration dialog box opens.

3. Enter the following information:

Field	Definition
<b>Name</b>	Name of your CPPM instance.
<b>Domain/IP</b>	Domain or URL of your CPPM instance.
<b>Client ID</b>	Client ID generated from your CPPM account.
<b>Secret Key</b>	Secret key generated from your CPPM account.
<b>Verify server certificate</b>	If you are using cloud instances of both CPPM and Orchestrator, or if you are using an on-premise instance of CPPM with a valid certificate, select this check box.  If you are using an on-premise instance of Orchestrator or an on-premise instance of CPPM without a valid certificate, clear this check box.

4. Click **Save**.

Your CPPM instance now appears in the ClearPass Policy Manager Accounts dialog box. The Connectivity and Service Status fields should both appear as Connected.

## Edit a ClearPass Policy Manager Server

1. If not already opened, click **Accounts** to open the ClearPass Policy Manager Accounts dialog box.
2. Click the **Edit** icon next to the instance you want to edit.

The ClearPass Policy Manager Server Configuration dialog box opens.

3. Edit the information in the dialog box, and then click **Save**.

## Pause ClearPass Policy Manager Integration

To pause the integration between CPPM and Orchestrator, click **Pause Orchestration** from the ClearPass Policy Manager tab.

**NOTE** Clicking **Pause Orchestration** pauses the connection between all instances of CPPM configured in Orchestrator. To pause an individual instance, click **Accounts**, and then click the toggle under Pause for the instance you want to pause.

# Support

When working with Support, these tabs facilitate your opening a support case. They also provide Support with data and reports needed to troubleshoot network issues.

## Technical Assistance

### Tech Support - Appliances

*Support > Technical Assistance > Tech Support - Appliances*

Use this tab to create a new case, generate a system dump, upload files to an existing case, or download selected files to Orchestrator.

By default, the table displays all files available on the selected appliances. Click the appropriate button to filter files by type (Logs, Sys Dump, Snapshot, TCP Dump). The table includes the following details for each file:

Field	Description
<b>Appliance</b>	Name of the appliance on which the file is available.
<b>File type</b>	Specific file type (log, sys dump, snapshot, or TCP dump).
<b>File Name</b>	Name of the file.
<b>Last Modified</b>	Date when the file was last modified.
<b>File Size</b>	Size of the file.

#### Download to Orchestrator

Complete the following steps if you want to download one or more files to Orchestrator.

1. Select one or more files in the table (use Ctrl or Shift to select multiple files).
2. Click the **Download to Orchestrator** button above the table.
3. When prompted, click **Download** to confirm or click **Close** to cancel.

The Monitor Transfer Progress window appears, showing the status of current and previous downloads.

4. To stop any downloads that are not yet finished, click **Cancel**.

**NOTE** To access any files that have been downloaded, open the **Tech Support - Orchestrator** tab under the Support menu. After selecting one or more files, you can create a new case, upload files to an existing case, or download files to your local machine.

## Tech Support - Orchestrator

*Support > Technical Assistance > Tech Support - Orchestrator*

This tab displays a list of Orchestrator log files and system dump files, as well as support files that have been downloaded from appliances. You can use these files to create or update support cases, or you can download files to your local machine from Orchestrator.

By default, the table displays all files available on Orchestrator. Click the appropriate button to filter files by type (logs, system dumps, or appliance files). The table includes the following details for each file:

Field	Description
<b>Source</b>	Source of the selected file (Orchestrator or a specific appliance).
<b>File Type</b>	Specific file type (log, sys dump, snapshot, or TCP dump).
<b>File Name</b>	Name of the file.
<b>Last Modified</b>	Date when the file was last modified.
<b>File Size</b>	Size of the file.

### Take Action with Files

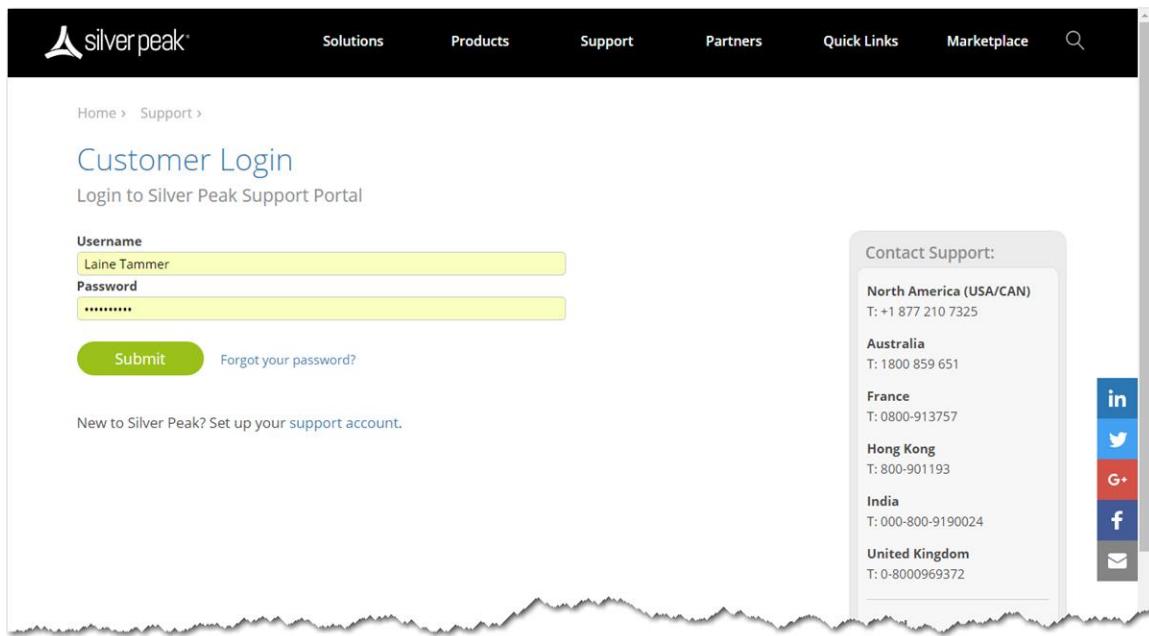
With one or more files selected, you can create a new support case, add files to an existing case, or download files to your local machine.

- Click **Create Case** to open a new support case. Fill in a few additional details and the selected files will be attached to a new support case.
- Click **Upload Selected Files** to attach files to an existing support case. You will need to know the case number when using this option.
- Click **Download selected Files** to download files to your local machine. Confirm the download and select a location where you want to save the files.

## Log In to the Support Portal

*Support > Technical Assistance > Support Portal Log-in*

When you have a Silver Peak account and need technical assistance or customer support, select **Support > Technical Assistance > Support Portal Log-in**. The following page opens in a separate browser tab.



You can also access this page directly by going to Silver Peak's web page and selecting **Support > Customer Login** from the menu bar.

## Monitor Transfer Progress

*Support > Technical Assistance > Monitor Transfer Progress*

This table displays the current status of any files being uploaded to Support.



## Packet Capture

*Support > Technical Assistance > Packet Capture*

When requested by Support, use this tab to capture packets for appliances that are selected in the appliance tree.

The following table describes each field on this tab.

Field	Description
<b>Maximum number of packets</b>	Enter the maximum number of packets to capture.
<b>Filter by IP (optional)</b>	Enter the host or IP address to capture from.
<b>Filter by port number (optional)</b>	Enter the port to capture from. For example, to capture DNS traffic, enter 53.
<b>Bytes to capture from each packet (snap length)</b>	Enter the number of bytes (the amount of data) for each frame to capture. For example, enter 96 to capture headers only or 1500 to capture full frames. <b>NOTE</b> Configuring a large snap length will result in larger packet capture file sizes.
<b>Additional filter options</b>	Enter other options to filter the capture. For example, proto 17 src 1.1.1.1

Field	Description
<b>Enable circular storage</b>	Select this check box to limit the amount of data to store by setting a maximum number of files and maximum file size for the capture. For example, set the <b>Number of files</b> to 5 and <b>Max size per file</b> to 100 (MB). Once the size limit is reached for a file, a new file will be written. Once the maximum number of files is reached, the oldest file will be overwritten.
<b>Number of files</b>	If you enabled circular storage, enter the maximum number of files that can be stored for this packet capture.
<b>Max size per file</b>	If you enabled circular storage, enter the maximum file size that can be stored for this packet capture.
<b>Command preview</b>	Displays the progress of the packet capture.

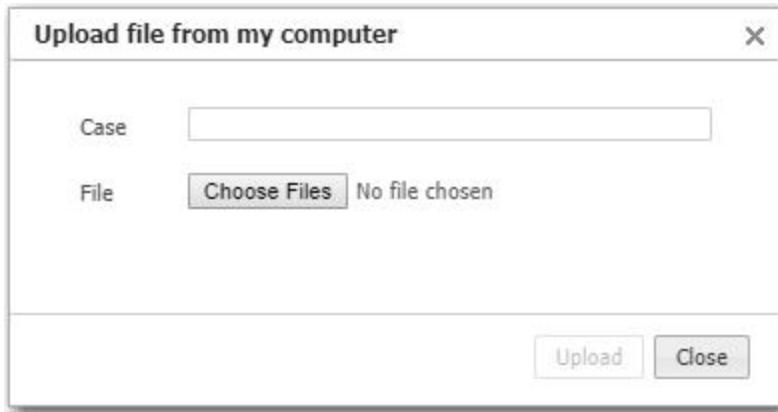
Click **Run** to initiate the packet capture.

Click **Stop** to cancel the packet capture.

## Upload Local Files

*Support > Technical Assistance > Upload Local Files*

Use this dialog box to upload files related to your Support case from your computer.



## Create a Support Case

*Support > Technical Assistance > Create Case*

Use this file to create an Support case.

You will receive a case number and instructions for what to do next.

**Create Case**

---

Name	<input type="text"/>
Email	<input type="text"/>
Phone	<input type="text"/>
Appliance	Chennai <input type="button" value="▼"/>
Case Priority	P3 - Normal <input type="button" value="▼"/>
Subject	<input type="text"/>
Description	<input type="text"/>

---

## Partition Management

*Support > Technical Assistance > Partition Management*

Use this tab to regain Orchestrator disk space by selectively eliminating statistics no longer needed.

Partition Management					
807 Rows					
Table Name	Partition Name	Rows	Size	Start Time	End Time
actionlog	defaultPartition	1400427	2.8 GB		
actionlog	p1524096000	0	180 KB	20-Oct-17 17:00	18-Apr-18 17:00
actionlog	p1508544000	0	180 KB	23-Apr-17 17:00	20-Oct-17 17:00
actionlog	p1492992000	0	180 KB	25-Oct-16 17:00	23-Apr-17 17:00
actionlog	p1477440000	0	180 KB	28-Apr-16 17:00	25-Oct-16 17:00
actionlog	p1461888000	0	180 KB	31-Oct-15 17:00	28-Apr-16 17:00
actionlog	p1446336000	0	180 KB	04-May-15 17:00	31-Oct-15 17:00
actionlog	p1430784000	0	213 KB		04-May-15 17:00
dailyapp	defaultPartition	0	74 KB		
dailyapp	p1524096000	0	74 KB	20-Oct-17 17:00	18-Apr-18 17:00
dailyapp	p1508544000	0	74 KB	23-Apr-17 17:00	20-Oct-17 17:00
dailyapp	p1492992000	0	74 KB	25-Oct-16 17:00	23-Apr-17 17:00
dailyapp	p1477440000	0	74 KB	28-Apr-16 17:00	25-Oct-16 17:00
dailyapp	p1461888000	0	74 KB	31-Oct-15 17:00	28-Apr-16 17:00
dailyapp	p1446336000	0	74 KB	04-May-15 17:00	31-Oct-15 17:00

## Remote Log Receivers

*Support > Technical Assistance > Remote Log Receiver*

This table lists all configured remote log receivers that are sent and managed by Orchestrator. You can choose between sending your data between the following different types of receivers: HTTP, HTTPS, KAFKA, SYSLOG, and WEBSOCKET. Each receiver employs a different mechanism for supporting asynchronous notifications. After you determine which remote receiver you want to use to send your data, you can configure specific settings for that receiver.

Complete the following instructions to add a receiver.

1. Click **Add Receiver**.
2. Select the type of receiver you want to use from the list.
3. Depending on which receiver you choose, a settings pop-up will appear. Enter the appropriate information for each receiver. See the following tables below for each receiver's settings.
4. Click **Save**.

### HTTP Receiver Settings

Field	Description
<b>Enable Receiver</b>	Click this slider to toggle between enabled and disabled state.

Field	Description
<b>Name</b>	Name of the receiver the logs are going to.
<b>Log Type</b>	Select the type of log from the list you want to apply.
<b>URL</b>	URL served by HTTP/HTTPS log server that Orchestrator will send log data with POST REST calls.
<b>User Name</b>	User name used in Basic Authentication when making REST calls (Optional).
<b>Password</b>	Password used in Basic Authentication when making REST calls. (Optional).
<b>Repeat Password</b>	Your password repeated.

## HTTPS Receiver Settings

Field	Description
<b>Enable Receiver</b>	Click this slider to toggle between enabled and disabled state.
<b>Name</b>	Name of the receiver the logs are going to.
<b>Log Type</b>	Select the type of log from the list you want to apply.
<b>URL</b>	URL of the HTTPS Receiver.
<b>User Name</b>	User name used in Basic Authentication when making REST calls (Optional).
<b>Password</b>	Password used in Basic Authentication when making REST calls (Optional).
<b>Repeat Password</b>	Your password repeated.

## KAFKA Receiver Settings

Field	Description
<b>Enable Receiver</b>	Click this slider to toggle between enabled and disabled state.
<b>Name</b>	Name of the receiver the logs are going to.
<b>Log Type</b>	Select the type of log from the list you want to apply.
<b>Topic</b>	Topic name on KAFKA Receiver.
<b>Bootstrap Servers</b>	Domain name served by KAFKA Receiver. For example, "xxx.com:9092", "1.1.1.1:9092".
<b>Acks</b>	Defines the amount of KAFKA servers that acknowledge a message before considering the message delivered. <ul style="list-style-type: none"> <li>• <b>acks=0:</b> Expect no acknowledgement.</li> <li>• <b>acks=1:</b> Only leader server must acknowledge.</li> <li>• <b>ack=all:</b> All servers must acknowledge.</li> </ul>
<b>Retries</b>	Amount of times KAFKA will try before returning an error.
<b>Batch Size</b>	Multiple messages KAFKA will produce until the batch size is exceeded.
<b>Buffer Size</b>	Maximum memory size that can be used for buffering messages. When buffer size is exceeded, a message will be blocked.
<b>Linger Time</b>	Amount of time that KAFKA will wait before sending next message batch.

## SYSLOG Receiver Settings

Field	Description
<b>Enable Receiver</b>	Click this slider to toggle between enabled and disabled state.

### General Settings

Field	Description
<b>Log Type</b>	Type of log being sent to the SYSLOG receiver.
<b>Protocol</b>	Protocol being used between devices.
<b>Hostname</b>	Hostname of the SYSLOG receiver to identify the device.
<b>Port</b>	Port number of the SYSLOG receiver that accepts incoming events.
<b>Custom Data</b>	Custom data embedded inside the SYSLOG message.

### Facility Settings

Field	Description
<b>Audit Log</b>	Type of audit log.

### Audit Log Severity Settings

Field	Description
<b>Error</b>	Severity level of the error; select from the drop-down menu.
<b>Info</b>	Severity level of the information; select from the drop-down menu.
<b>Debug</b>	Severity level of the debug; select from the drop-down menu.

## WEBSOCKET Receiver Settings

Provides a reliable streaming mechanism for alarms and Orchestrator audit logs across all appliances. It is initiated from the client side and sent to Orchestrator for authentication. When authenticated by Orchestrator, asynchronous notifications are sent in JSON objects.

Field	Description
<b>Enable</b>	Click this slider to toggle between enabled and disabled state.
<b>Name</b>	Name of the WebSocket receiver.
<b>Log Type</b>	Type of log being sent to the WebSocket receiver.
<b>IP Allow List</b>	List of source IP addresses that are allowed WebSocket access to Orchestrator.

## WebSocket Receiver Configuration

You need the following items to establish connectivity from Orchestrator to the WebSocket receiver:

- Key generated by Orchestrator after the above configuration is completed
- ID created by Orchestrator when it is configuring the WebSocket server

## Routing Peers Table

*Support > Technical Assistance > Routing Peers Table*

The **Routing Peer Table** tab can be used to track the communication between multiple peers within a network and for troubleshooting purposes. It also reflects the details of the subnet information being shared between each set of peers.

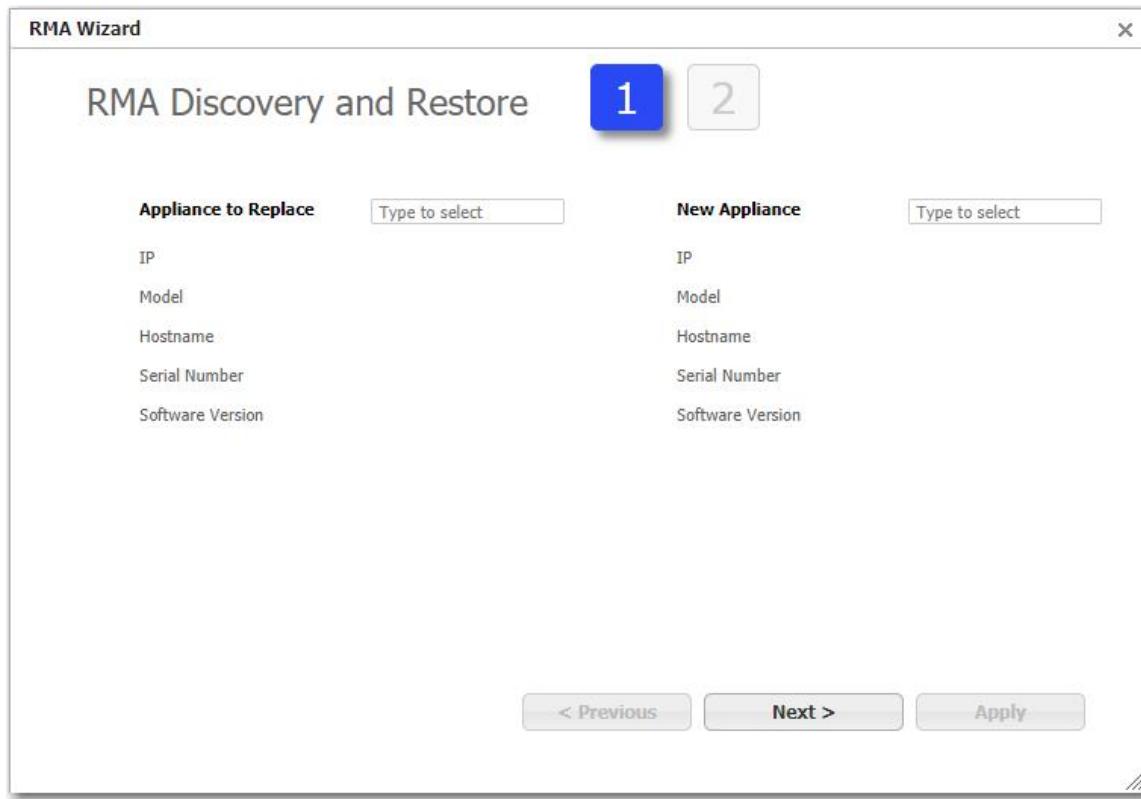
The following table describes the values for the Routing Peers table.

Field	Description
<b>Appliance</b>	Name of the appliance.
<b>Peer Id</b>	ID of the peer.
<b>Peer Name</b>	Name of the peer.
<b>Role</b>	Whether the hub or spoke topology is being used for the specified peer.
<b>Last transmission count</b>	Last transaction count the peer was sent.
<b>Time since last transmission</b>	How many seconds have elapsed since the last subnet update was sent to the peer.
<b>Last received count</b>	Last transaction count from the peer that was received.
<b>Time since last received</b>	Amount of time since the last received update.
<b>MainVer and Region</b>	Main version and the region of the designated peer.
<b>Message</b>	Peer information to assist Support in troubleshooting.

## RMA Wizard

*Support > Technical Assistance > RMA*

The RMA (Return Merchandise Authorization) Wizard automates the RMA process for an exchange or replacement of your appliance, if needed. It includes appliance discovery, the version of the appliance, and a backup selection. Use this screen as instructed by Support to prepare an RMA.



Note the following before you begin the RMA process.

- Upgrade or downgrade the new appliance to the same software version before shipping to the site. This will save time.
- Perform a backup of the Orchestrator and EdgeConnect appliances.
- Install the new EdgeConnect appliance onsite.
- When Orchestrator discovers the new device, do not approve it. Start the RMA process to move the license to the new EdgeConnect appliance.

## Run the RMA Wizard

Complete the following steps to RMA your appliance.

1. Navigate to the **RMA** tab in Orchestrator.
2. Select the appliance you want to replace from the menu.

**NOTE** The IP address, appliance model, hostname, serial number and software version will auto-populate after you select the appliance.

3. Select the newly discovered appliance that will replace the current appliance.

**NOTE** The IP address, appliance model, hostname, serial number and software version will auto-populate after you select the appliance.

4. Click **Next >**.
5. If you are adding a backup appliance, proceed to the next section. Otherwise, click **Apply**.

The Applying Configuration dialog box opens and displays the status of the upgrade and restore.

## Add a Backup Appliance

If you choose to add a backup appliance from the table, complete the following steps.

1. Select the backup appliance from the table.
2. Select the version you want the backup appliance to have from the drop down menu.

**NOTE** If your selection results in a software downgrade, a backup must be provided.

## Upgrade and Downgrade

If the software version you selected for your backup appliance is **higher** than that of the discovered appliance, you will need to do the following:

- Upgrade to the new version using Orchestrator.
- Back up the appliance from a restore, if applicable.

If the software version you selected for your backup appliance is **lower** than that of the discovered appliance, you will need to do the following:

- Install the desired version as a next boot on the appliance.
- Restore from backup.

# User Documentation

## Alarm Descriptions

*Support > User Documentation > Alarm Descriptions*

Orchestrator enables you to export to a CSV file a full list of alarms you could potentially receive. To automatically export the CSV file, navigate to **Support > User Documentation > Alarm Descriptions**.

The CSV file includes the following information:

- Type ID: Unique ID assigned to the alarm.
- Severity: Severity level of the alarm, as follows:
  - Critical: Critical alarms are service-affecting and require immediate attention. They reflect conditions that adversely affect an appliance or indicate the loss of a broad category of service.
  - Major: While service-affecting, major alarms are less severe than critical alarms. They reflect conditions that should be addressed in the next 24 hours. An example would be an alarm caused by an unexpected traffic class error.
  - Minor: Minor alarms are not service-affecting and can be addressed at any time. Examples include alarms caused by a user who has not changed their account's default password, a degraded disk, or a software version mismatch.
  - Warning: Warning alarms are not service-affecting. They warn of conditions that could become problems over time—for example, an alarm caused by IP SLA being down.
- Description: Brief description of the alarm.
- Recommended Action: Recommended actions to take to resolve the alarm.
- Service Affecting: Indicates whether the alarm is service affecting.
- Source: Indicates where the alarm originated.
- System Type: Identifies the type of system the alarm originated from, as follows:
  - 0: EdgeConnect appliance
  - 100: Orchestrator
  - 200: Orchestrator-SP or Orchestrator Global Enterprise
- Source Type: Identifies the alarm category, as follows:
  - 1: Tunnel (applicable to both Orchestrator and appliance alarms)
  - 2: Traffic Class (applicable to appliance alarms only)
  - 3: Equipment
  - 4: Software
  - 5: Threshold Crossing (applicable to appliance alarms only)
- Alarm Type: Indicates an index into the specific alarm category. For example, within the Tunnel alarm category, there is an alarm type associated with index 0 (INTERFACES\_WITH\_DUPLICATE\_IP\_EXIST), another with index 1 (INTERFACES\_WITH\_NO\_PUBLIC\_IP\_EXIST), and so forth. Each alarm type within an alarm category has a unique ID.
- Clearable: Indicates whether you can clear the alarm.

## Built-in Policies

*Support > User Documentation > Build-in Policies*

This table displays read-only built-in policies, which are executed before any other policies.

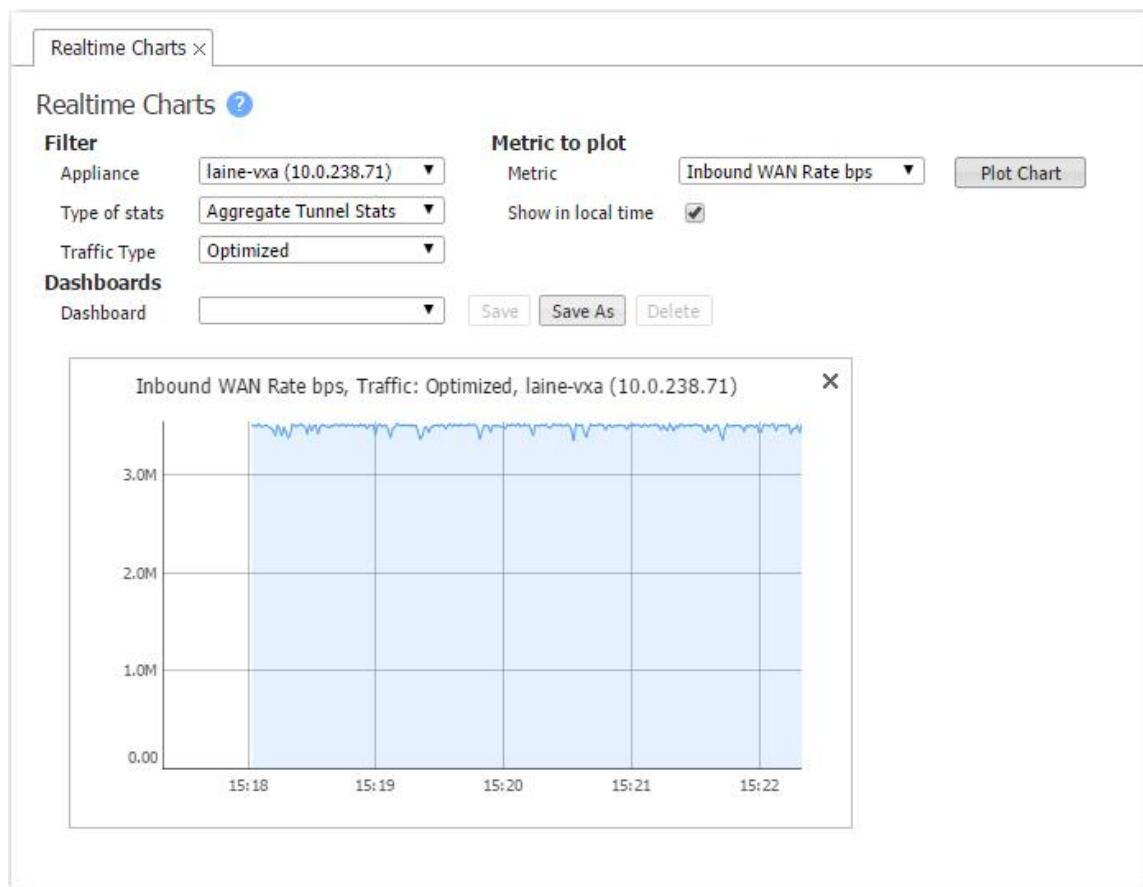
Built-in Policies <span style="color: #0070C0;">?</span> <span style="font-size: small;">2 min</span>						
Match Criteria			Action	Comment		
Appliance	Map	Priority				
Telartron	map1	65400	Source IP any local ip, Destination IP any, Source Port any, Destination Port any, Protocol any, Application any	Force Bypass false, Drop false, Passthrough-unshaped true, Bind To Tunnel false, Source IP Based Routing	Nest hop monitoring pings, IPSLA pings a...	
Telartron	map1	65499	Source IP ha subnet, Destination IP ha subnet, Source Port any, Destination Port any, Protocol any, Application any	Force Bypass false, Drop false, Passthrough-unshaped true, Bind To Tunnel true, Source IP Based Routing	Traffic between HA subnets	
Telartron	map1	65500	Source IP any local ip, Destination IP any, Source Port any, Destination Port 4784, Protocol udp, Application any	Force Bypass false, Drop false, Passthrough-unshaped true, Bind To Tunnel true, Source IP Based Routing	BFD Multi-hop	
Telartron	map1	65501	Source IP any local ip, Destination IP any, Source Port 4784, Destination Port any, Protocol udp, Application any	Force Bypass false, Drop false, Passthrough-unshaped true, Bind To Tunnel true, Source IP Based Routing	BFD Multi-hop	
Telartron	map1	65502	Source IP any local ip, Destination IP any, Source Port any, Destination Port 3784, Protocol udp, Application any	Force Bypass false, Drop false, Passthrough-unshaped true, Bind To Tunnel true, Source IP Based Routing	BFD Single-hop	
Telartron	map1	65503	Source IP any local ip, Destination IP any, Source Port 3784, Destination Port any, Protocol udp, Application any	Force Bypass false, Drop false, Passthrough-unshaped true, Bind To Tunnel true, Source IP Based Routing	BFD Single-hop	
Telartron	map1	65505	Source IP any local ip, Destination IP any, Source Port any, Destination Port 647, Protocol any, Application any	Force Bypass false, Drop false, Passthrough-unshaped true, Bind To Tunnel false, Source IP Based Routing	DHCP Failover dest port 647	
Telartron	map1	65506	Source IP any local ip, Destination IP any, Source Port 647, Destination Port any, Protocol any, Application any	Force Bypass false, Drop false, Passthrough-unshaped true, Bind To Tunnel false, Source IP Based Routing	DHCP Failover source port 647	
Telartron	map1	65507	Source IP any local ip, Destination IP any, Source Port any, Destination Port any, Protocol any, Application any	Force Bypass false, Drop false, Passthrough-unshaped false, Bind To Tunnel true, Source IP Based Routing	TOMIP Error packets, Third-party tunnels	

## Reporting

### Realtime Charts

*Support > Reporting > Realtime Charts*

As an aid to troubleshooting, **Realtime Charts** are useful for monitoring the performance of individual appliances. You can save sets of charts as dashboards.



1. Select the filters you want, and then click **Plot**.

The chart appears at the bottom of the page.

2. To save as a dashboard, click **Save As**, and then enter a name for your dashboard. Do not include spaces in your name. Click **Save**.

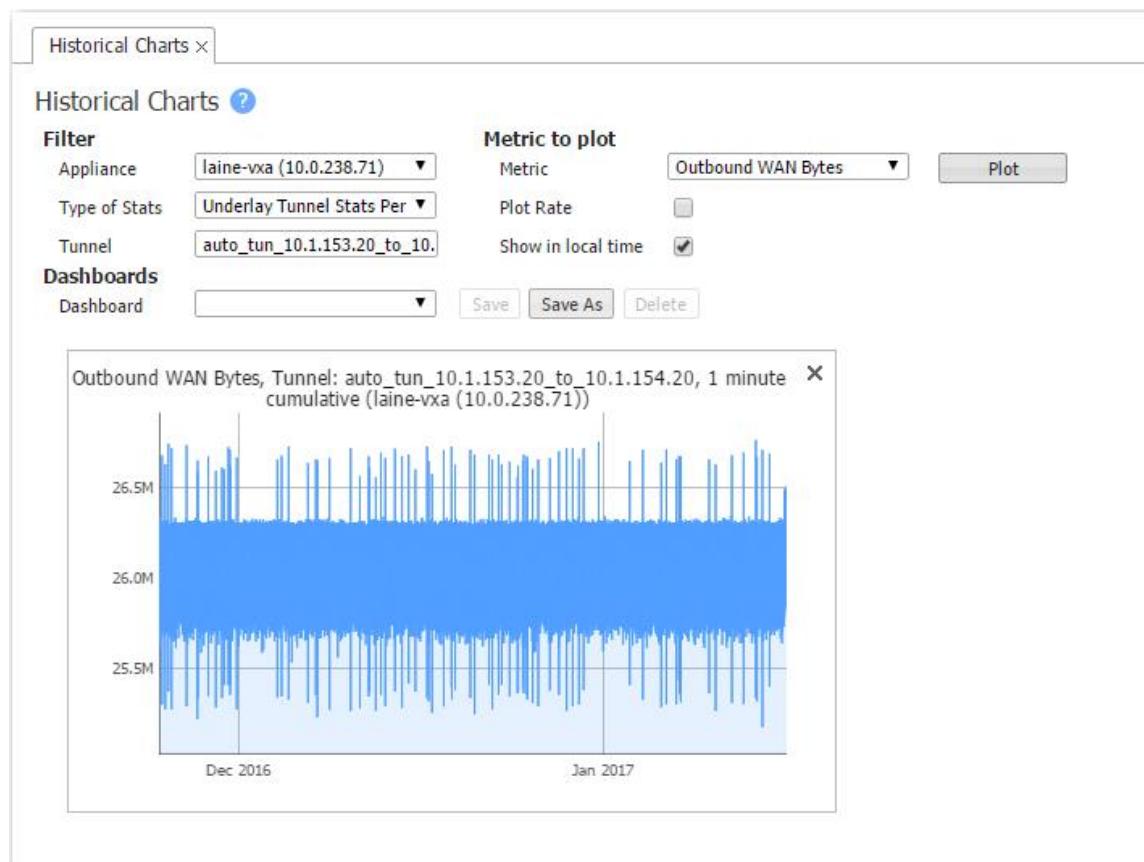
If successful, a green Success bar appears and the dashboard name shows up in the **Dashboard** field.

To retrieve it later, go to this tab and choose the dashboard from the drop-down list.

## Historical Charts

*Support > Reporting > Historical Charts*

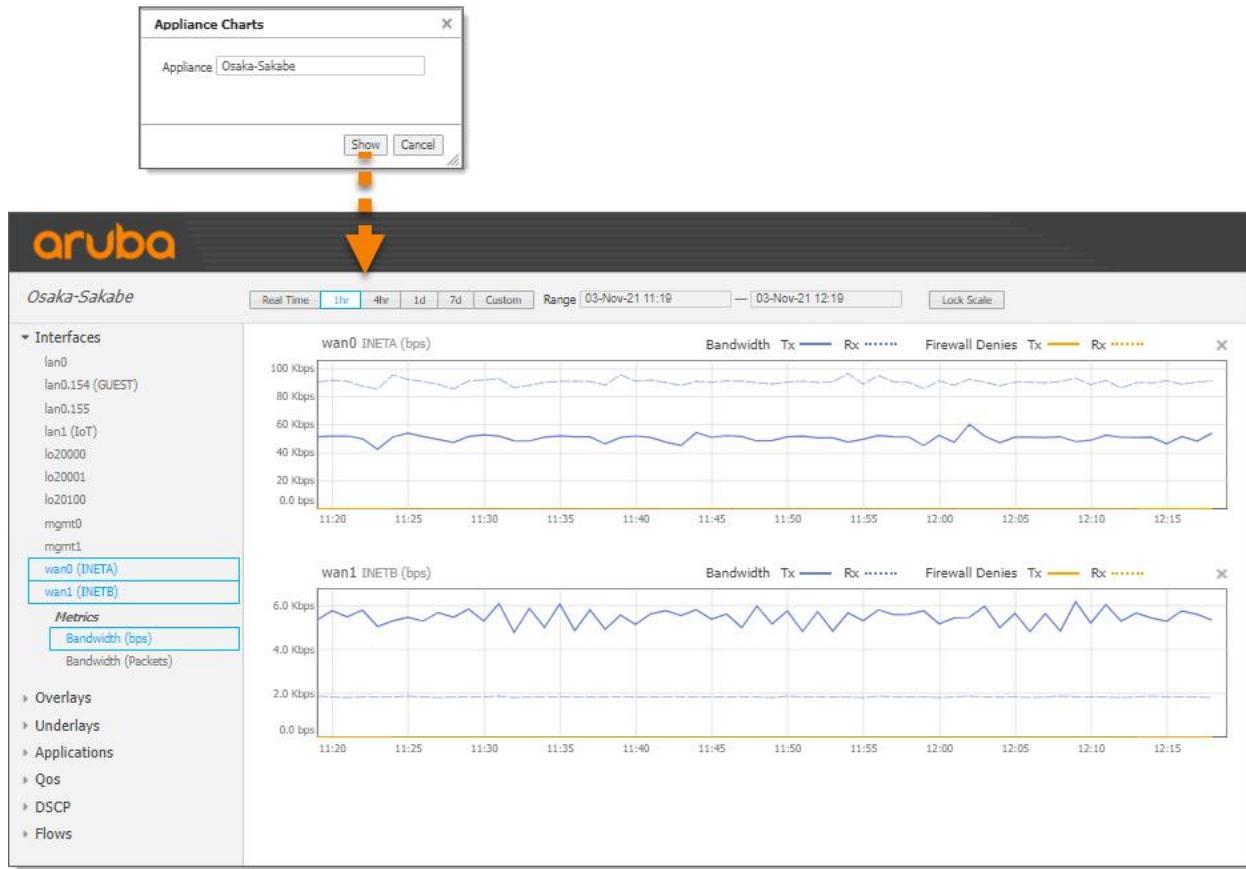
As an aid to troubleshooting, **Historical Charts** are useful for reviewing the performance of individual appliances. You can save sets of charts as dashboards.



## Appliance Charts

*Support > Reporting > Appliance Charts*

Use this dialog box to access an individual appliance's realtime and historical charts.

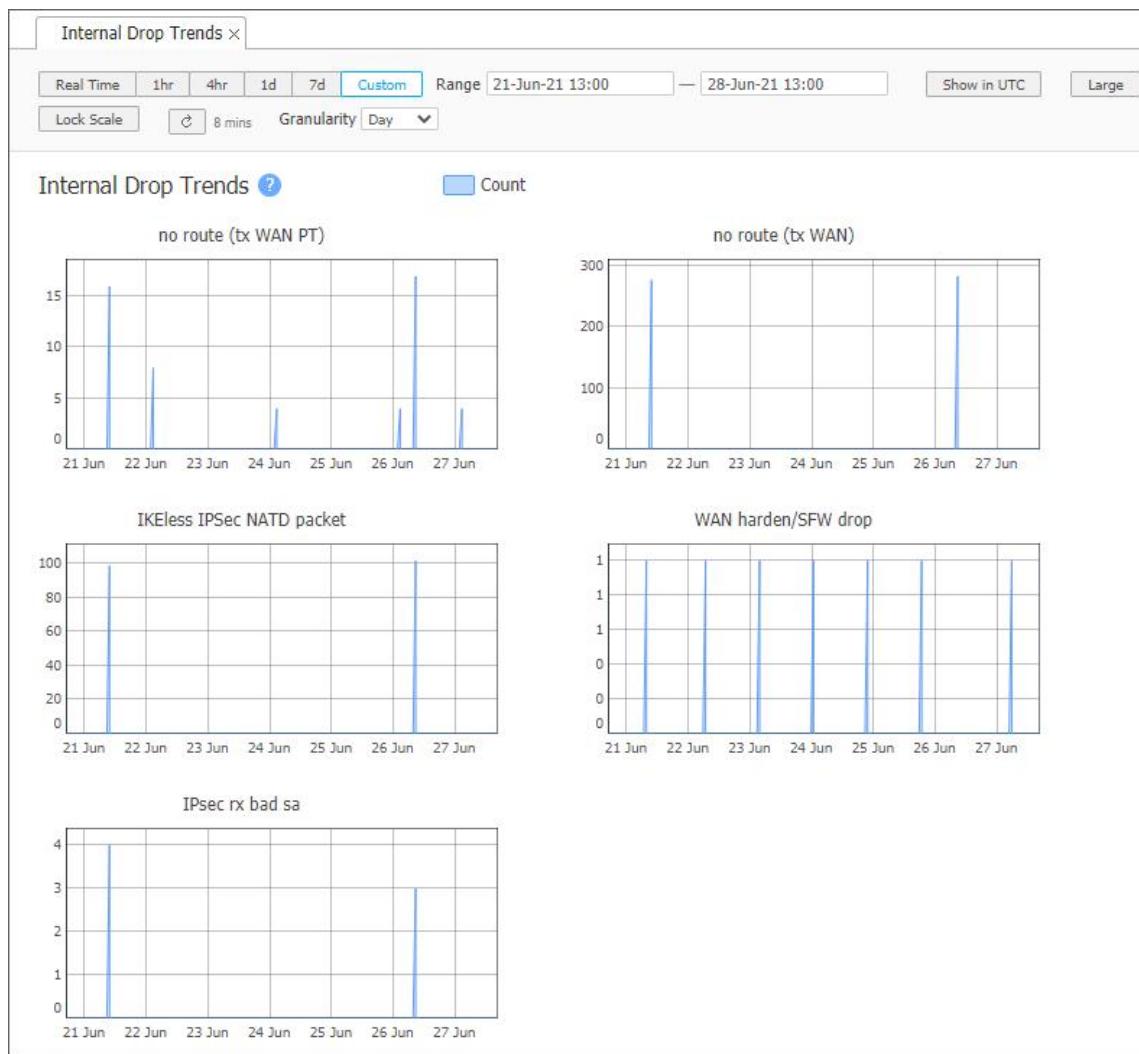


## Internal Drop Trends

*Support > Reporting > Dropped Packet Trends*

The **Internal Drop Trends** report shows internal packet drop trends for a single selected appliance. The charts that are displayed will vary according to the cause of the drop.

Charts are available in real time or for a specific time period. Real time charts show drops over the last five minutes and refresh every five seconds.



You can customize the chart settings using the controls at the top of the tab, as follows:

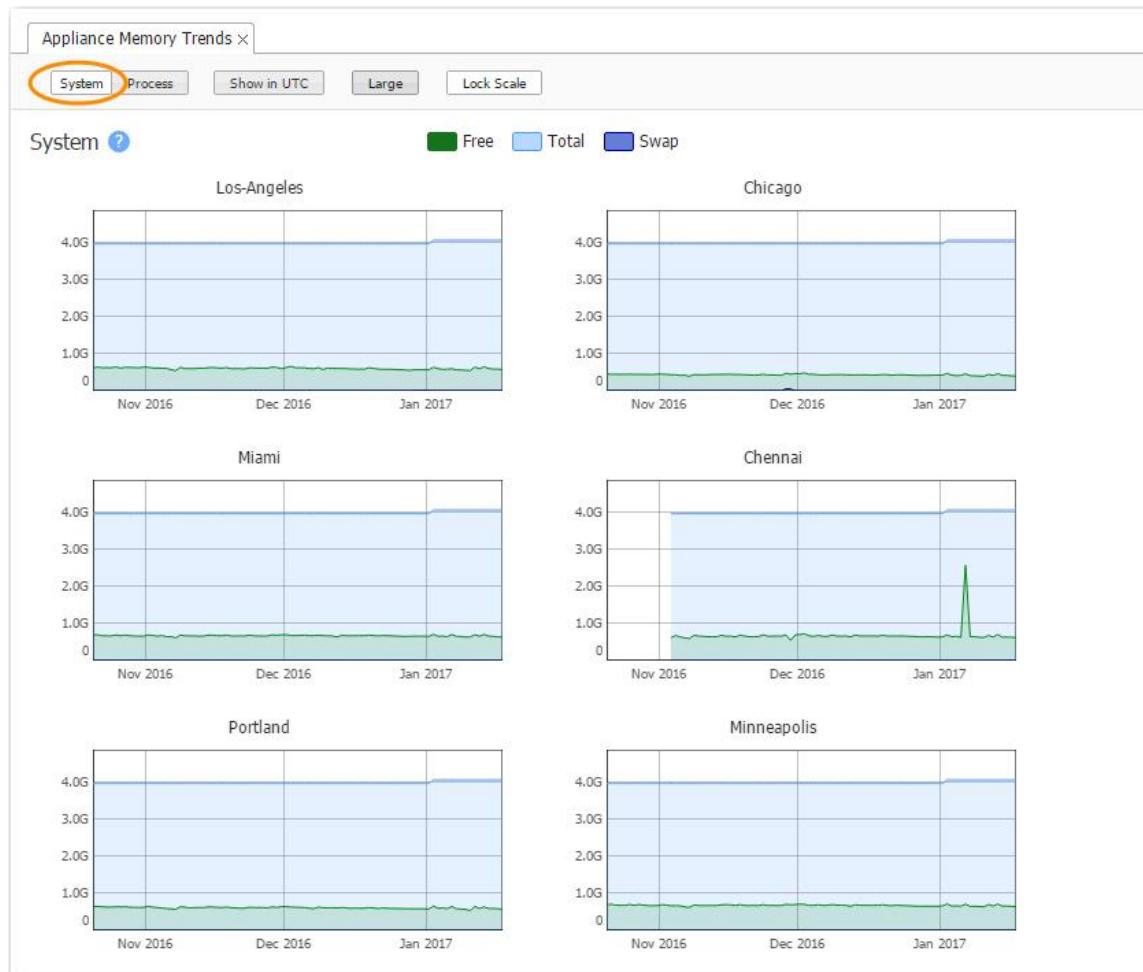
Option	Description
<b>Time period</b>	<ul style="list-style-type: none"> <li>Click <b>Real Time</b> to enable live statistics for all available interfaces.</li> <li>Click a predefined time period (<b>1h</b>, <b>4h</b>, <b>1d</b>, <b>7d</b>) to display statistics over the last hour, four hours, day, or seven days.</li> <li>Click <b>Custom</b> and set your own custom time range to display statistics for that time period.</li> </ul>
<b>Show in UTC</b>	Click this option to toggle chart times between local appliance time or UTC.
<b>Large</b>	Click this option to toggle the size of the charts between smaller (default) and large.
<b>Lock Scale</b>	By default, each chart uses its own scale that is relative to the data displayed. Click this option to apply and lock the same scale to each chart.

Option	Description
<b>Refresh</b> 	Click the <b>Refresh</b> button to fetch data again for the selected time period.
<b>Granularity</b>	When a custom time period is used, select the granularity level to be applied to charts ( <b>Minute</b> , <b>Hour</b> , or <b>Day</b> ).

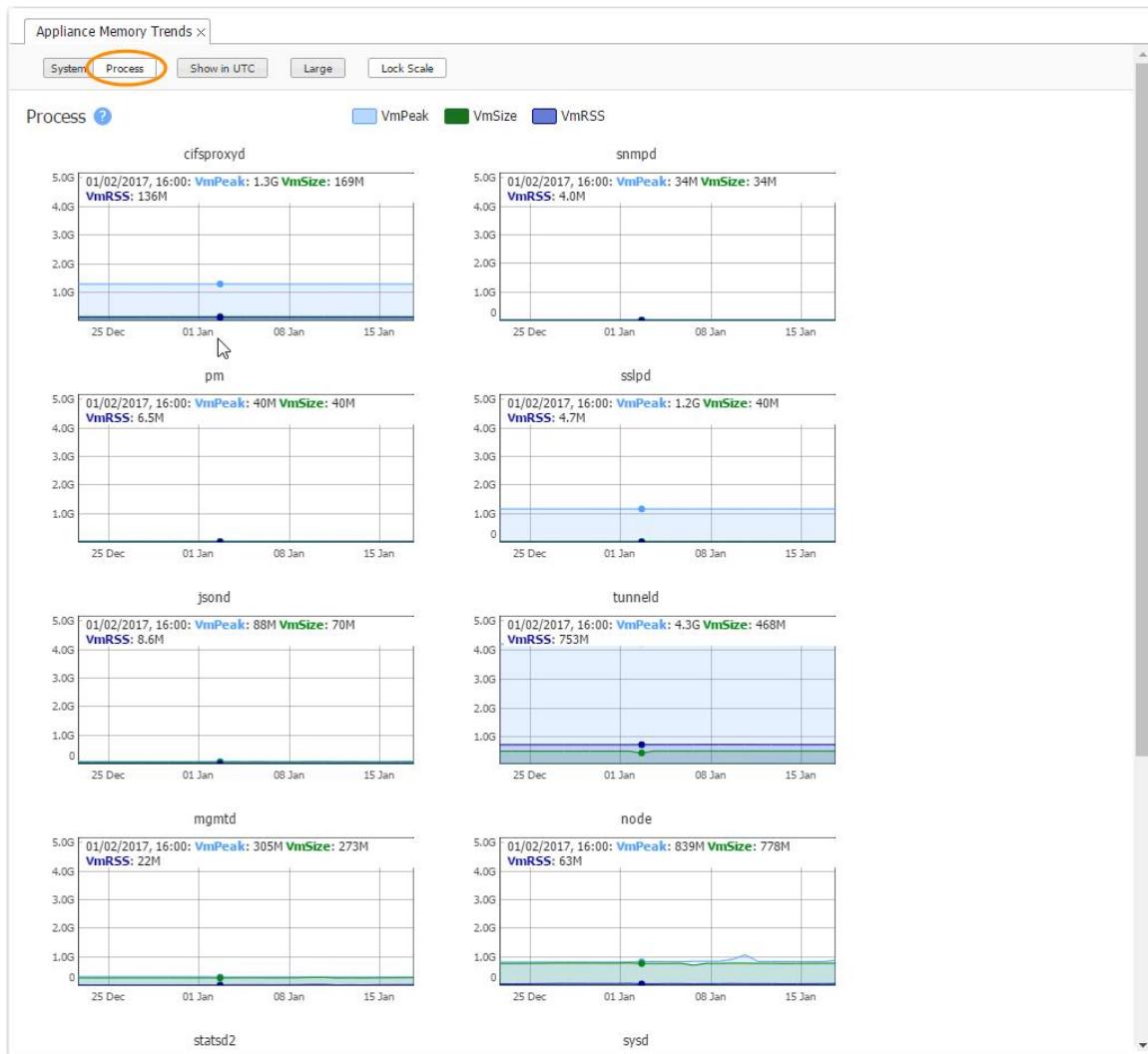
## Appliance Memory Trends

*Support > Reporting > Appliance Memory Trends*

The **System** view shows appliance daily memory usage.



The **Process** view is for individual appliances.

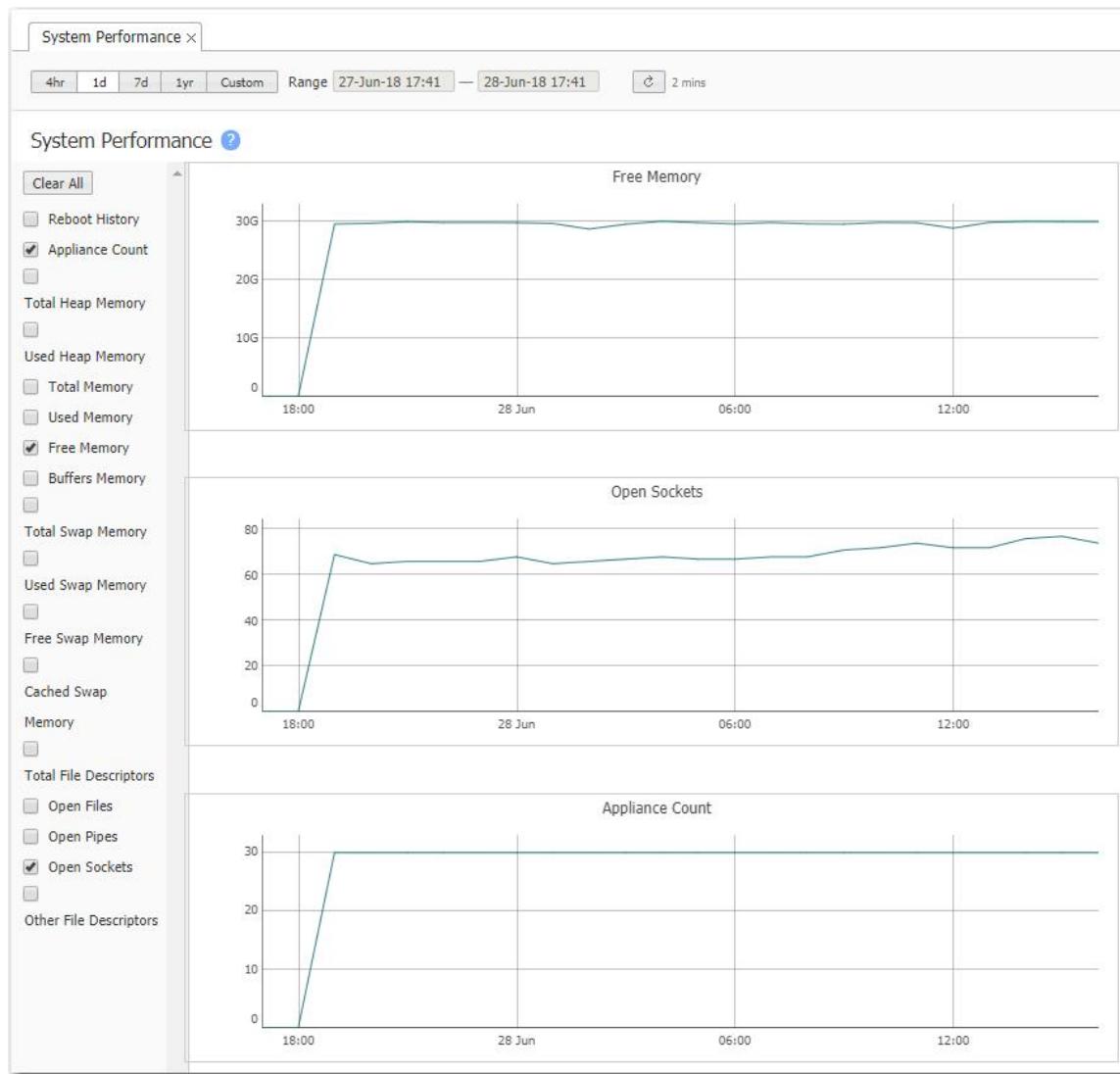


## System Performance

*Support > Reporting > System Performance*

This tab shows Orchestrator metrics.

Orchestrators located in the cloud cannot display useful information about host memory, file descriptors, sockets, or pipes.

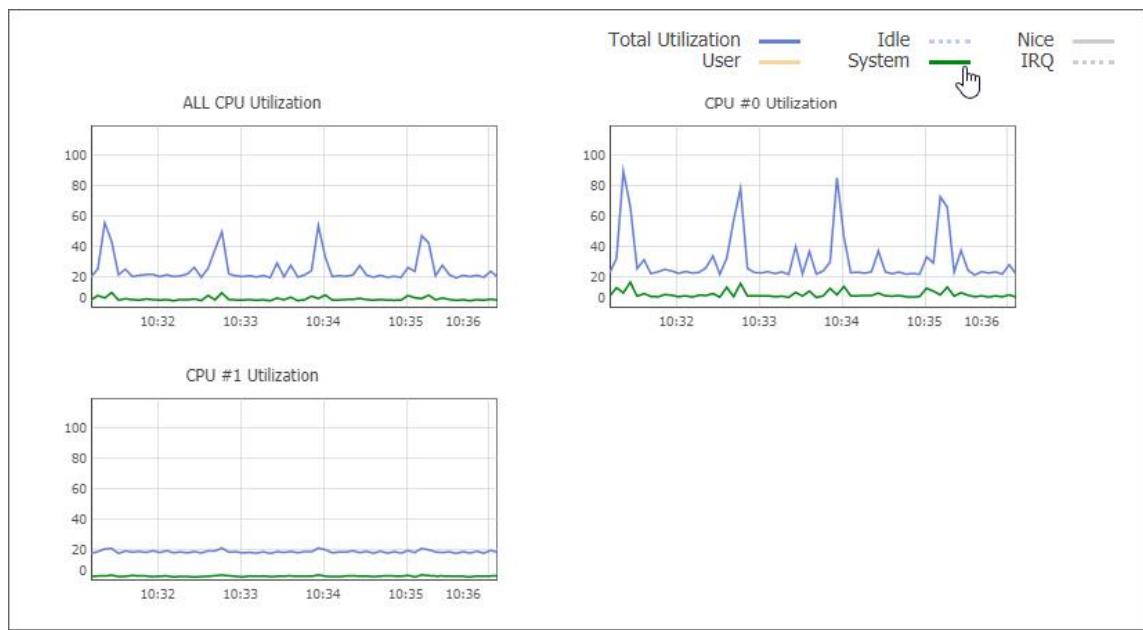


## Appliance CPU Usage

[Support > Reporting > Appliance CPU Usage](#)

The charts on this page provide real-time views of combined and individual CPU usage statistics for a single selected appliance. Charts show the past five minutes of usage and refresh every five seconds. By default, only total utilization is displayed on the charts. You can toggle the available statistics on or off by clicking the sample indicator line next to each statistic name.

**NOTE** On appliances with Boost enabled, it is common for non-CPU0 cores to run at or close to 100%. CPU0 will show occasional spikes of high usage when statistics are rolled up and archived.



## Orchestrator Debug

*Support > Reporting > Orchestrator Debug*

This dialog box provides the various debugging tools available to Support for troubleshooting and debugging issues with Orchestrator.

Orchestrator Debug																																		
Appliance Info		Built-in Stats		Appliance Polling		Reachability Stats		Stack Dump																										
Sync Stats		REST Request Time Stats		Orchestration Task		Orchestration Progress		Tunnel Counts																										
Appliance Stats Collector																																		
Stats Collector V2																																		
Appliance Configuration Limit																																		
2 Rows																																		
<table border="1"> <thead> <tr> <th>ID</th><th>Appliance</th><th>Site</th><th>Mgmt IP</th><th>Discovered Pro...</th><th>Software Versi...</th><th>UUID</th><th>Portal Object ID</th><th>Dynamic UUID</th></tr> </thead> <tbody> <tr> <td>1.NE</td><td>appliance-1.ne</td><td></td><td>10.99.238.140</td><td>PORTAL</td><td>9.2.0.0_93412</td><td>00000000-0000-0000-0000-000000000000</td><td>10100000000000000000000000000000</td><td>00000000-0000-0000-0000-000000000000</td></tr> <tr> <td>0.NE</td><td>appliance-0.ne</td><td></td><td>10.99.238.139</td><td>PORTAL</td><td>9.2.0.0_93412</td><td>00000000-0000-0000-0000-000000000000</td><td>10100000000000000000000000000000</td><td>00000000-0000-0000-0000-000000000000</td></tr> </tbody> </table>								ID	Appliance	Site	Mgmt IP	Discovered Pro...	Software Versi...	UUID	Portal Object ID	Dynamic UUID	1.NE	appliance-1.ne		10.99.238.140	PORTAL	9.2.0.0_93412	00000000-0000-0000-0000-000000000000	10100000000000000000000000000000	00000000-0000-0000-0000-000000000000	0.NE	appliance-0.ne		10.99.238.139	PORTAL	9.2.0.0_93412	00000000-0000-0000-0000-000000000000	10100000000000000000000000000000	00000000-0000-0000-0000-000000000000
ID	Appliance	Site	Mgmt IP	Discovered Pro...	Software Versi...	UUID	Portal Object ID	Dynamic UUID																										
1.NE	appliance-1.ne		10.99.238.140	PORTAL	9.2.0.0_93412	00000000-0000-0000-0000-000000000000	10100000000000000000000000000000	00000000-0000-0000-0000-000000000000																										
0.NE	appliance-0.ne		10.99.238.139	PORTAL	9.2.0.0_93412	00000000-0000-0000-0000-000000000000	10100000000000000000000000000000	00000000-0000-0000-0000-000000000000																										
Close																																		

## IPSec UDP Status

*Support > Reporting > IPSec UDP Status*

Use this tab to review and monitor the IPSec UDP key material status for all appliances in your network.

Field	Description
<b>Appliance</b>	Name of the appliance.
<b>Active Key</b>	Indicates whether the appliance is using the active IPSec UDP key.
<b>Active Key Pushed Time</b>	Time when the active key was pushed to the appliance.
<b>Active Key Activation Time</b>	Time when the key was activated on the appliance.
<b>Reachability</b>	Indicates whether the appliance is reachable.
<b>Detail</b>	Additional details about reachability or key material status.

## Unverified Emails

*Support > Reporting > Unverified Emails*

When you add an email address to either the Alarms or the Reports email distribution list, Orchestrator sends the recipient an email that contains a link, asking them to click to provide verification.

If Orchestrator does not receive a verification, either the recipient has not responded or the email address is invalid.



- An unverified email address remains inactive and does not generate an alarm.
- You can retest an address with **Resend**.
- You can only correct an email address in the Alarm or Reports email distribution list.

---

**1** If roles and appliance access group keys are not provided, Orchestrator inspects its own configuration to determine the role and appliance access group for the user. If it does not find that information, the user is not allowed to log in.