# EdgeConnect Operational and Troubleshooting Overview

June 2021
PN: 201843-001
Revision A

# Copyright and Trademark



Silver Peak Systems, Inc.
2860 De La Cruz Boulevard
Santa Clara, CA 95050

1.877.210.7325 (toll-free in USA)
+1.408.935.1850

http://www.silver-peak.com/support

# Contents

# Overview

This document provides high-level troubleshooting and operational procedures to consider if you are having issues with you Silver Peak SD-WAN deployment. This information provides a general overview and is supplementary to formal training and experience with the solution.

As much as possible, the document is structured for an operational audience, following a progressive triage workflow driving toward root cause identification. The audience is assumed to have a basic understanding of the EdgeConnect solution.

## Before you Begin

- Appropriate members of a team managing the EdgeConnect installation should have access to the support portal at https://www.silver-peak.com/support.
- If not done already, set up support accounts before you begin.

## Need More Help?

If you are still having issues after performing any of the procedures described in this document, refer to Contact Support to get help from Silver Peak Support.

# Contact Support

This section contains information about creating and managing support cases. For information about case priorities and SLAs, escalations, software maintenance, warranty and equipment returns, training and certification, and much more, see https://www.silver-peak.com/support.

## Open a New Case

There are four ways to open a new support case:

- Email
- Phone
- Orchestrator UI
- Support Portal

Cases are assigned as quickly as possible. For non-urgent issues, customers may specify their time zone or preferred meeting times for the best experience.

**NOTE** When opening a case from the Orchestrator UI or via the Support Portal, it is best practice to always add or attach a sysdump to the case. A detailed procedure about creating and uploading sysdumps is available in the Appendix.

### Email

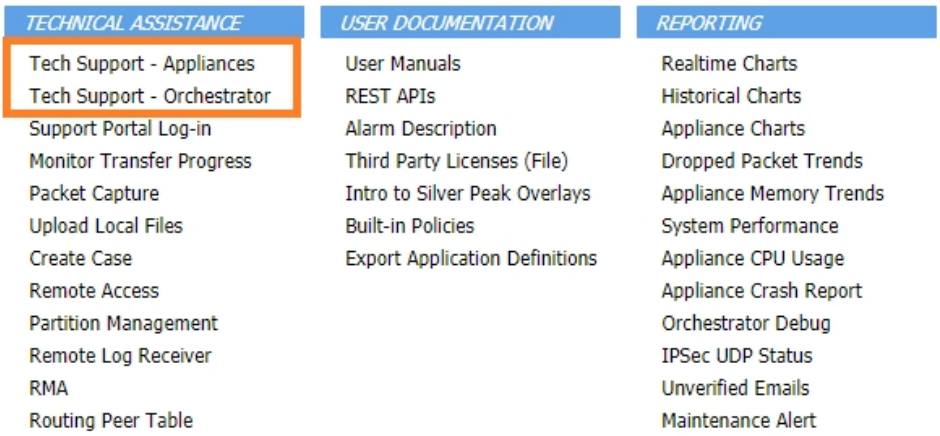
Send an email to support@silver-peak.com. All cases opened via email are opened as Priority 3 cases.

### Phone

The toll-free number for the U.S. and Canada is +1 (877) 210 7325. Other numbers are listed at https://www.silver-peak.com/support.

## Orchestrator UI

1. In Orchestrator, click the **Support** tab, then click **Tech Support - Appliances** or **Tech Support - Orchestrator**, depending on the issue you are experiencing.




2. On the Tech Support tab, click **Generate Sys Dump**.
3. While that process runs, click **Create Case**.
4. Enter the required information, and then click **Create**.
5. When the sysdump is available, select it in the table, and then click **Upload Selected Files**.
6. Attach the sysdump to the case that was just created, and then click **Upload**.

> **NOTE** You can find additional details about creating and uploading sysdumps in the Appendix.

## Support Portal

Log in to the Support Portal at https://www.silver-peak.com/support, click **Open/Manage a Case**, and then click **Open Case**.

# Manage an Existing Case

## Requeue a Case

Cases maintain ownership unless a customer requests a change. If the case needs to change owners, please call Support and ask to requeue the case to the next available engineer.

## Update a Case

To add additional information to a case, reply to the existing support email thread or use the Support Portal. To attach additional files, upload them in Orchestrator.

## Escalate a Case

If a case priority has changed and needs to be escalated, call Support and ask to work with a Duty Manager.

# Cloud Portal Maintenance

Silver Peak performs monthly system maintenance of our Cloud Portal (licensing application) on the second Saturday of each month. During this 3-hour maintenance window, the Cloud Portal application is inaccessible to Orchestrator and Unity EdgeConnect appliances for any new license activations and upgrades.

**TIP** This activity will not impact your SD-WAN network.

- **When:** Second Saturday of each month
- **Start:** Saturday, 9:00 PM Pacific Time
- **End:** Sunday, Midnight Pacific Time

# Basic Diagnostics

One basic function in Silver Peak Orchestrator is checking the health of a network. If you have problems performing this check, consider the diagnostic steps below before calling Support.

**NOTE** In addition to the methods described below, you can run Ping, Traceroute, and Packet Capture (tcpdump) from the command line interface (CLI). You can access the CLI via SSH or the **CLI session** option when right-clicking an appliance in Orchestrator's appliance tree.

## Ping

By default, all pings are sourced from the mgmt0 interface. To troubleshoot from the actual source interface, initiate pings using the "`-I`" flag to test connectivity along the data path between different locations.

To run a ping:

1. Right-click an appliance in tree view, and then click **Appliance Manager**.
2. Click **Maintenance**, and then click **Ping / Traceroute**.
3. Select the **Ping** option, enter the required information, and then click **Start**.

## Traceroute

Traceroute is another important tool to identify latency along the path, as well as identify the broken path where traffic stops.

To run a traceroute:

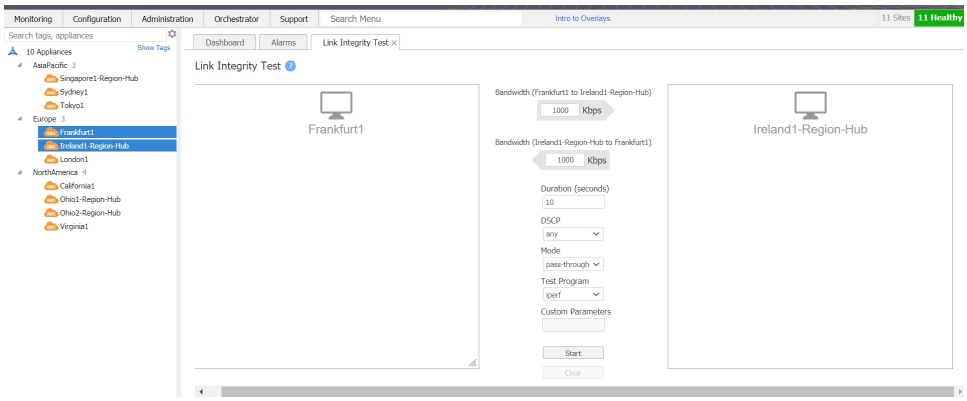
1. Right-click an appliance in tree view, and then click **Appliance Manager**.
2. Click **Maintenance**, and then click **Ping / Traceroute**.
3. Select the **Traceroute** option, enter the required information, and then click **Start**.

**NOTE** Not all intermediate routers respond all the time. In some cases, firewall rules or other device configuration can block responses.

# Performance Testing

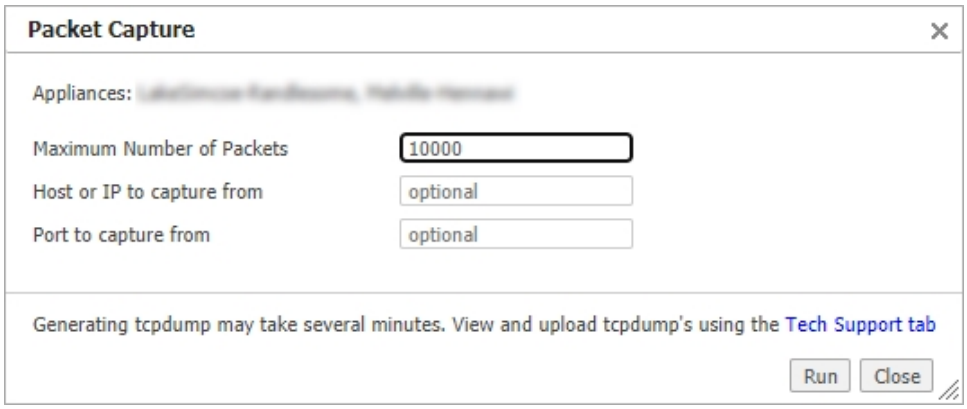
Performance testing can be done from the appliance itself by selecting two appliances from the tree view, clicking **Administration**, and then clicking **Link Integrity Test**.

**CAUTION** This test impacts performance. Use this method only when necessary.




# Packet Capture

Orchestrator provides the option to run packet capture from the appliance. Capture files are in standard .pcap format, which can be read easily with Wireshark. To begin packet capture, select one to five appliances, click **Support**, and then click **Packet Capture**.



# Troubleshooting Workflow: Gather the Details

This section provides a high-level guide for how to approach troubleshooting.

## Diagnose the Problem

Understand the problem through effective questioning and formulate a problem statement. To do so, ask questions to determine both what the problem IS and IS NOT. For example:

- How do you describe the problem?
- What sites have the problem?
- When did the problem begin?
- When does the problem happen?
- Was there a problem before the SD-WAN install?
- Do particular users experience these issues?

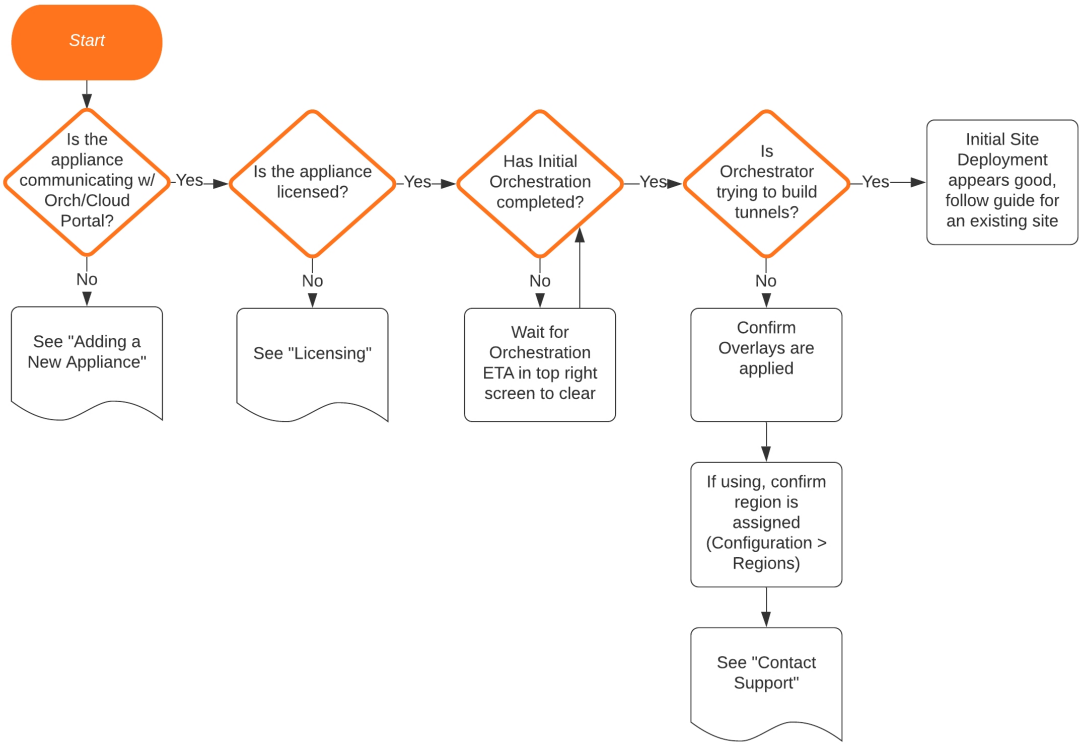
## Establish Next Steps

When you have clear, correct, and relevant answers to these questions, you can establish next steps that ensure a systematic approach to problem solving. For example, you may want to "divide and conquer" by breaking a problem into small, easily resolved issues that build toward a bigger resolution.

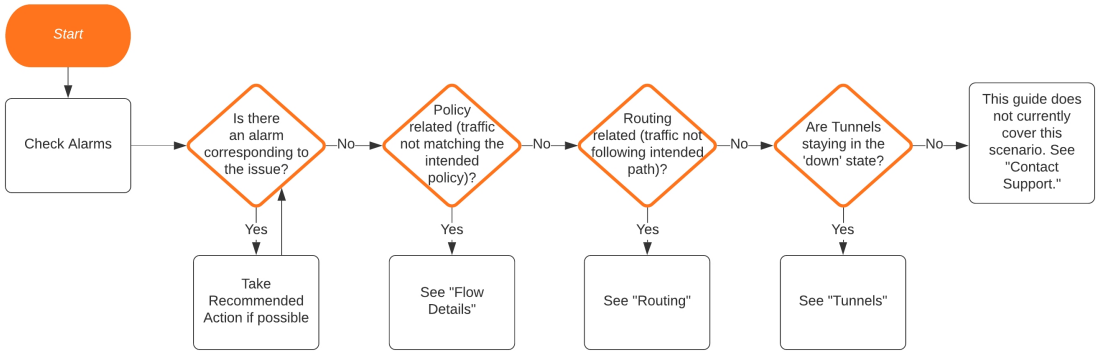
# Initial EdgeConnect Troubleshooting

The following diagrams can help guide initial troubleshooting actions before contacting Silver Peak Support for additional assistance.

## Troubleshooting a New Site

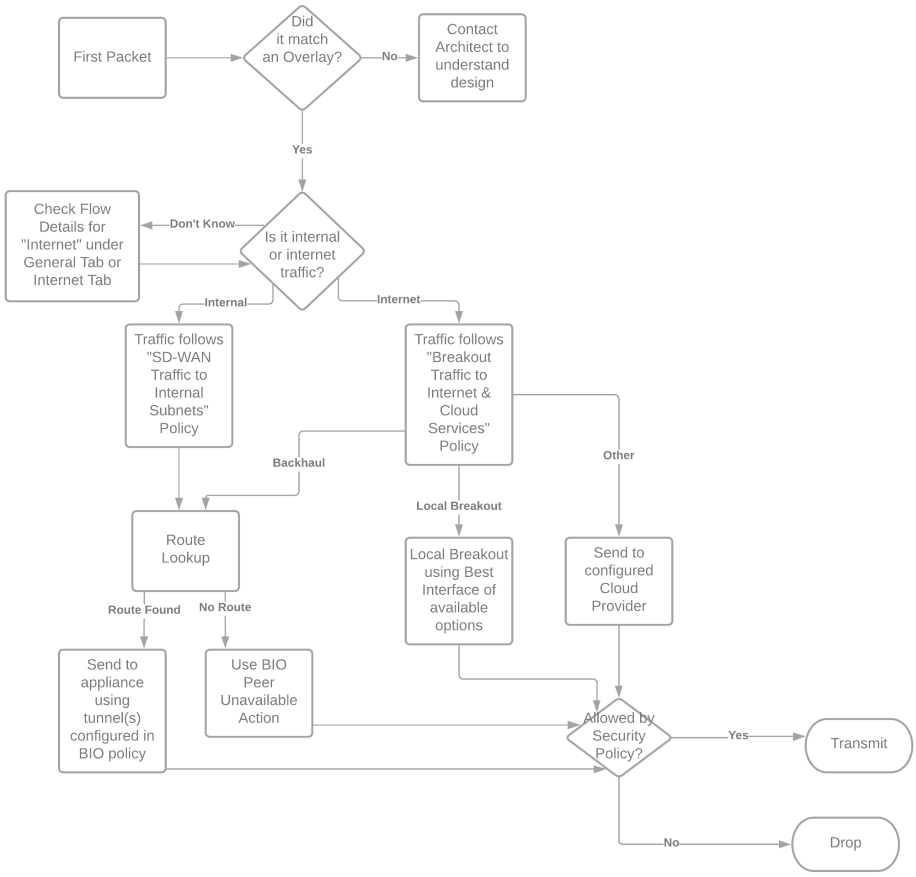



## Troubleshooting an Existing Site



# EdgeConnect Traffic Flow

When traffic enters the EdgeConnect, the first packet is examined. It is important to send traffic to the correct BIO and destination. The following chart details the data traffic flow in EdgeConnect.



# Adding a New Appliance

This section discusses solutions to problems that could occur when trying to bring a Silver Peak EdgeConnect device into Orchestrator.

## Physical EdgeConnect

When a physical EdgeConnect is connected to the internet, its serial number is registered with the Silver Peak Cloud Portal. After bootup, it should appear in the Appliances Discovered tab within Orchestrator.

The following interfaces are found on every physical EdgeConnect:

- WAN interfaces
- LAN interfaces
- Management interfaces

**NOTE** Virtual EdgeConnect appliances must include vNICs, which are discussed later in this guide.

By default, the WAN interfaces and mgmt0 are DHCP-enabled.

Before booting up the appliance, make sure that all connections are properly made. If the appliance does not appear in Orchestrator, take the following steps:

1. Make sure internet access is available either directly on the appliance or elsewhere on the network that the appliance can access.
2. Check that the lights on WAN interfaces (WAN0 and/or WAN1) are lit. If not, stop and troubleshoot the physical connectivity to eliminate a potential cabling issue.
3. Make sure that WAN0 or WAN1 is connected to the internet.
4. If a device appears as a discovered device with a green Approve Appliances button, it is healthy. If a device comes up as unreachable, examine other elements such as firewalls, next hop, or configuration.

5. Pay close attention to the messages received, as an appliance can be in the following modes:
    - *Normal*. Appliance is discovered and working as expected.
    - *Unknown*. Appliance is in transition state and trying to come up.
    - *Unsupported*.Appliance is running a code version not supported by Orchestrator.
    - *Unreachable*. A possible network issue.

## Common Issues

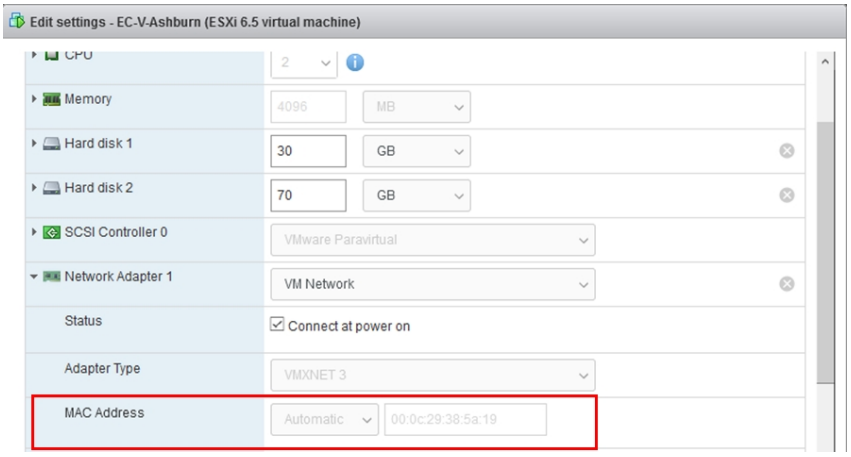
| Issue | Resolution |
|---|---|
| By policy, an appliance cannot access the internet. | Access the local appliance GUI or CLI and configure the Orchestrator name or IP. |
| Management traffic to the Cloud Portal and/or Orchestrator goes through a proxy. | Newer code revisions add a certificate check, which must be disabled. Contact Support. |
| No DHCP available. | Access the local appliance GUI or CLI and configure a WAN interface or mgmt0 with a static IP address. |

# Virtual EdgeConnect (EC-V)

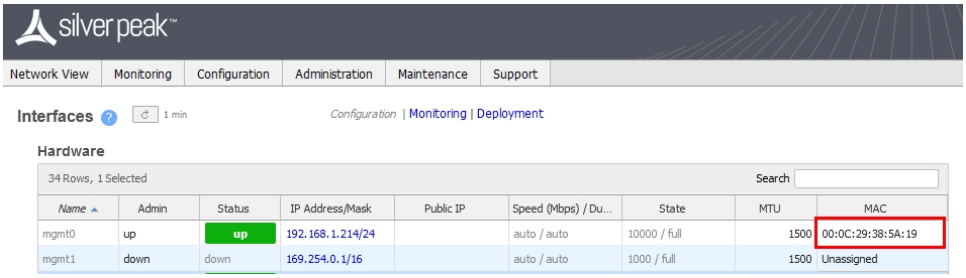
Most of the steps for physical appliances apply to an EC-V. The important difference is that the account name and account key are not configured in the default installation image and must be specified during installation. This can be done at the appliance GUI by clicking **Administration**, and then clicking **License & Registration**.

- An EC-V vNIC only comes with a mgmt interface. If the EC-V is not in the correct port group, it will not be able to communicate with Orchestrator. The mgmt0 vNIC usually sits outside the traffic data path.
- You must add proper vNIC interfaces as part of EC-V networking.
- Be sure the EC-V has connectivity to the internet and to Orchestrator by doing a ping test from the CLI or the EC-V web UI.

The following screenshot illustrates the port mappings in VMware for vNICs. The first vNIC is always the mgmt vNIC in VMware, as shown below. If the mgmt vNIC is not mapped to mgmt0 on the EC-V, the appliance will be unreachable from Orchestrator.




Note the MAC address highlighted above. You will need to assign the same MAC address to the mgmt0 interface on the EC-V, as shown below. You can reach this screen in the Appliance UI from **Configuration > Interfaces** or **Configuration > Initial Config Wizard**.




For current account information, click **Orchestrator**, and then click **Cloud Portal**.

# Licensing

A physical EdgeConnect appliance can be connected to the internet, licensed, and brought online easily if certain conditions are met. This section helps troubleshoot potential problems in this process.

## EdgeConnect Licensing

There are a few important factors to consider when the appliance is online, but is unable to register with the Orchestrator:

- Does the new EdgeConnect appliance have the correct account name and key listed? Account name is case sensitive. White spaces, typos, or missing letters prevent the appliance from registering with the Orchestrator.
- If the EdgeConnect appliance connects to the Orchestrator via another Silver Peak appliance, make sure the intermediate appliance is licensed as well.
- Appliances manually added to the Orchestrator will not be licensed. An appliance can only be added when Orchestrator discovers it.

For additional troubleshooting tips, see Adding a New Appliance.

# Orchestrator Licensing

For customer-hosted Orchestrator configurations, the Orchestrator requires account name and key configuration during setup. Orchestrator must be able to contact Silver Peak Cloud Portal and establish a web socket for ongoing communication. For configurations hosted by Silver Peak, these settings are confirmed during deployment.

Use the Cloud Portal tab (**Orchestrator** > **Cloud Portal**) to confirm the following:

- Is the Orchestrator reachable?
  - Does the Orchestrator have HTTPS reachability to the Cloud Portal? If not, troubleshoot security policy and DNS configuration.
  - Does the Orchestrator have web socket reachability to the Cloud Portal? If not, a security configuration issue most likely exists in the network.
- Is the Orchestrator registered?
  - If this is not the first Orchestrator deployed for the network, the new Orchestrator must be approved by a previously deployed Orchestrator.
  - If the Orchestrator has been approved but is still not registered, open a case with Silver Peak Support.

When reaching out to the Orchestrator hosted in the cloud, make sure that:

- Proper APIs and ports are allowed through the firewall, if traffic is going through the firewall.
- The Orchestrator name can be resolved via DNS.

# Alarms

For clues to resolve any issues you encounter, review alerts and alarms. For instance, EdgeConnect appliances issue alarms on half duplex that can help you find and correct service issues quickly. Many alarms include recommended actions for issue resolution.

For an overview of alarms, search for the *Alarms Tab* topic in the *Silver Peak Unity Orchestrator User Guide*.

## Alarm Levels

The Orchestrator has four main 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 IPSLA being down.

## View Alarms in Orchestrator

In the Orchestrator, the appliance tree view in the left pane displays the color of the highest severity alarm and the number of alarms at that level. For example, a red "2" next to an appliance name indicates two critical alarms for that appliance. Hover over the appliance name for brief alarm descriptions, or for more details, click **Monitoring**, and then click **Alarms**.

The top-right corner of the Orchestrator displays the number of sites at each alarm level. To view the Alarms page, click this area, and then click **View All Alarms**.

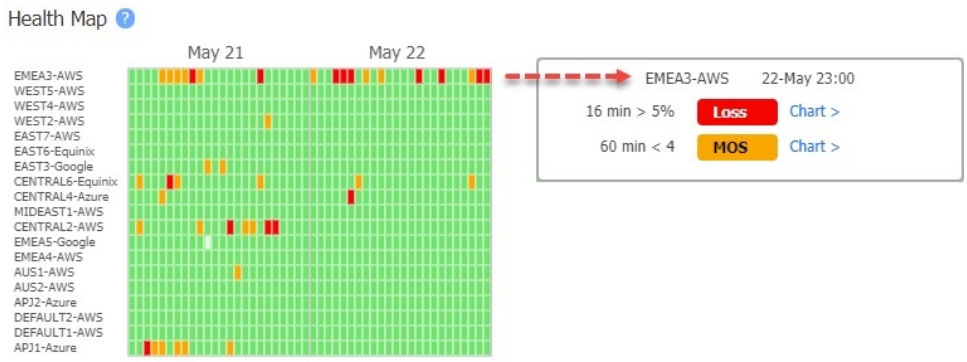
Some alarms clear themselves automatically after the issue resolves. Some alarms require user intervention.

# Orchestrator Health Map

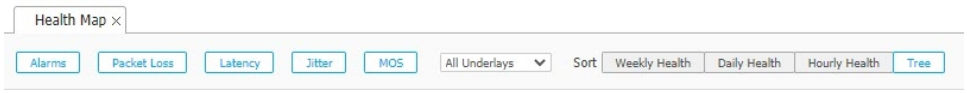
The Orchestrator Health Map provides a high-level view of a network's health in hourly increments. It is the ideal place to begin any troubleshooting.

Health Map is available as a widget on the Orchestrator Dashboard. It can also be accessed by clicking **Monitoring**, and then clicking **Health Map**.

The Health Map is color-coded, showing health status for hourly blocks based on the filters selected. Click one of the hourly blocks to show the status for the appliance at that hour, as well as any corresponding alerts.

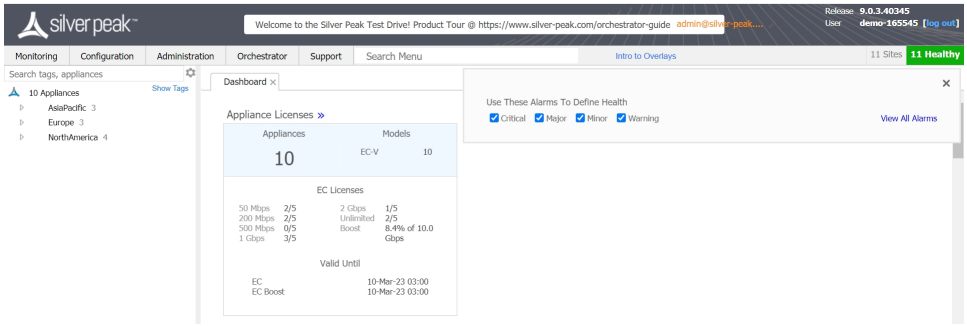



An administrator can adjust the display to reduce noise and focus on attributes critical to the organization. For example, the following settings display alerts across underlay tunnels only.

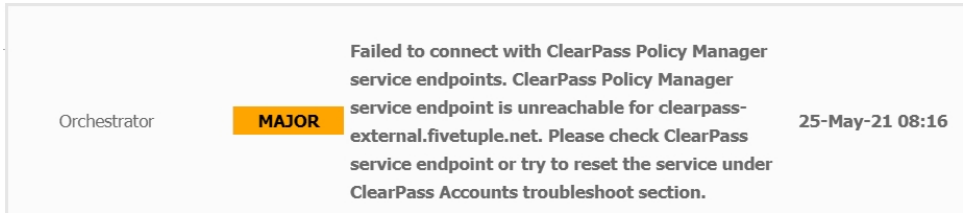


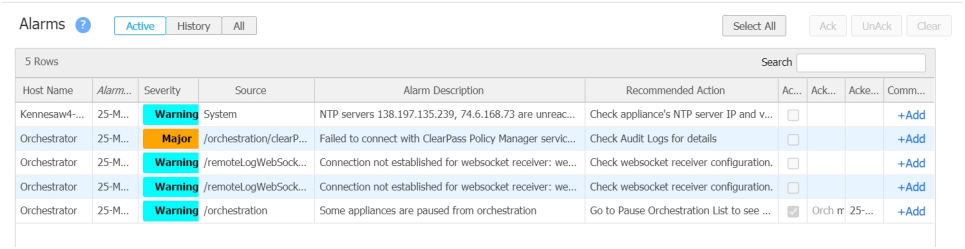
Use threshold settings to adjust the criticality of an issue and associated color coding.


In the following screenshot, the alarm bar in the top-right corner of Orchestrator indicates that the network is healthy:



When something goes wrong, an alarm appears, indicating the severity level assigned by Orchestrator. Click the alarm type indicator (MAJOR in the example below) to view more details about the alarm.




For more information about alarms, search for the *Viewing Alarms* topic in the *Silver Peak Unity Orchestrator User Guide*.

# Flow Monitoring

Flow monitoring is critical to diagnosing network problems. From the Orchestrator, you can simultaneously view flows for one or more appliances using real-time data.

## Flow Details

The Flow Details page for a given flow provides information about the rules matched on a given session or connection. Clicking the Flow Chart icon for a flow immediately produces a flow bandwidth chart for that flow, providing a view of how it is operating from moment to moment.

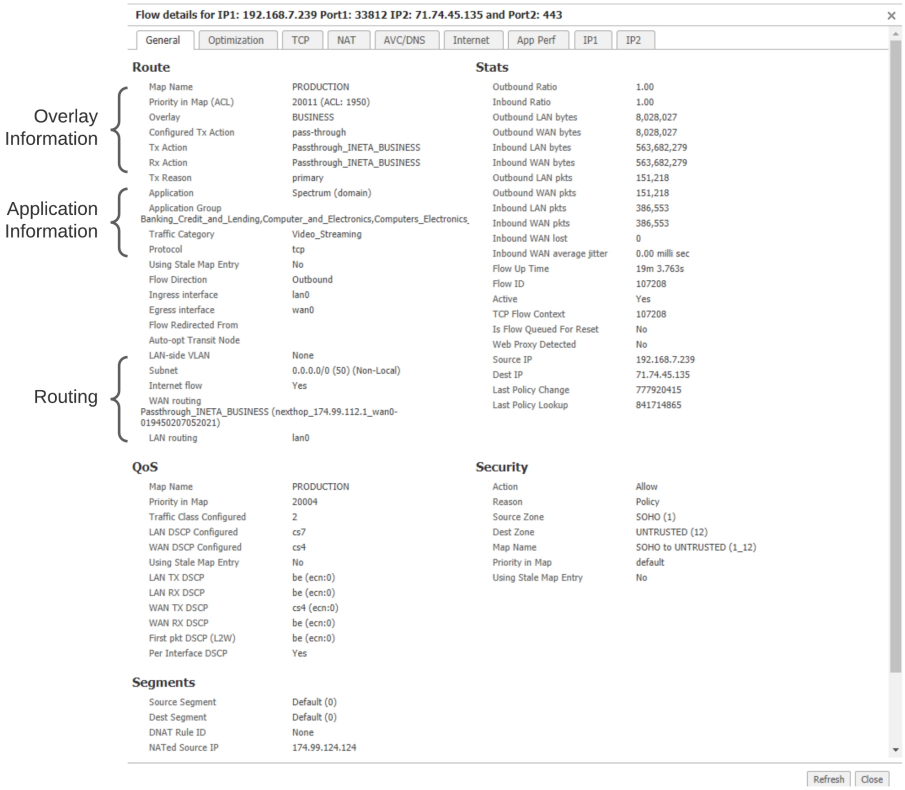
Flow details are extremely useful for diagnosing problems, as they include flow statistics and specific information associated with the flow. To access this information in Orchestrator, click **Monitoring**, and then click **Active & Recent Flows**.

**NOTE** The Orchestrator provides the best view of this information, but the information can also be accessed from the appliance's user interface.

Select the affected appliances from the tree view and use the filters at the top to find an affected flow. When the table shows that flow, click the **Information** icon in the Detail column. If the Detail column is not displayed in the table, right-click anywhere on the table header row to display a complete list of column options. Make sure the Detail column is selected.

# Analyze Flow Details

To troubleshoot a flow, pay close attention to three specific areas of a flow detail, explained below.




## Overlay Information

This section shows which overlay the flow matched into (in this example, BUSINESS) and the exact ACL entry in the overlay match (1950). If this information does not represent the desired configuration, click **Configuration**, click **Business Intent Overlays**, and then make the appropriate changes.

## Application Information

This section shows a high-level overview of the identified application. If this classification is not unexpected, click the **AVC/DNS** tab to gather more information and take corrective action.

## Routing

This section includes the following information:

- *Subnet*. This indicates the route prefix the flow matched (0.0.0.0/0), the metric of that route (50), and where it was learned (non-local). If any of these metrics are unexpected, see Routing for troubleshooting steps.
- *Internet Flow*. Generally, if the destination IP address is non-RFC 1918 address space, the flow is marked as an internet flow and follows the Breakout Traffic to Internet & Cloud Services policy on the Business Intent Overlays page. Confirm that the flow exhibits the expected behavior.

# Routing

A complete guide to EdgeConnect routing is beyond the scope of this document. Before troubleshooting, you should have an understanding of subnet sharing, peer priority, and route redistribution.

## Routing Decisions

Routing decisions are made based on a well-known evaluation process:

1. Longest Prefix Match
2. Lowest Administrative Distance
3. Lowest Metric
4. Lowest Peer Priority

**NOTE** Peer Priority is a concept specific to Silver Peak. If the first three values are equal, Peer Priority breaks the tie. If all values are equal and Peer Priority is not configured, traffic is load balanced over all peers involved in the tie.

## Routes

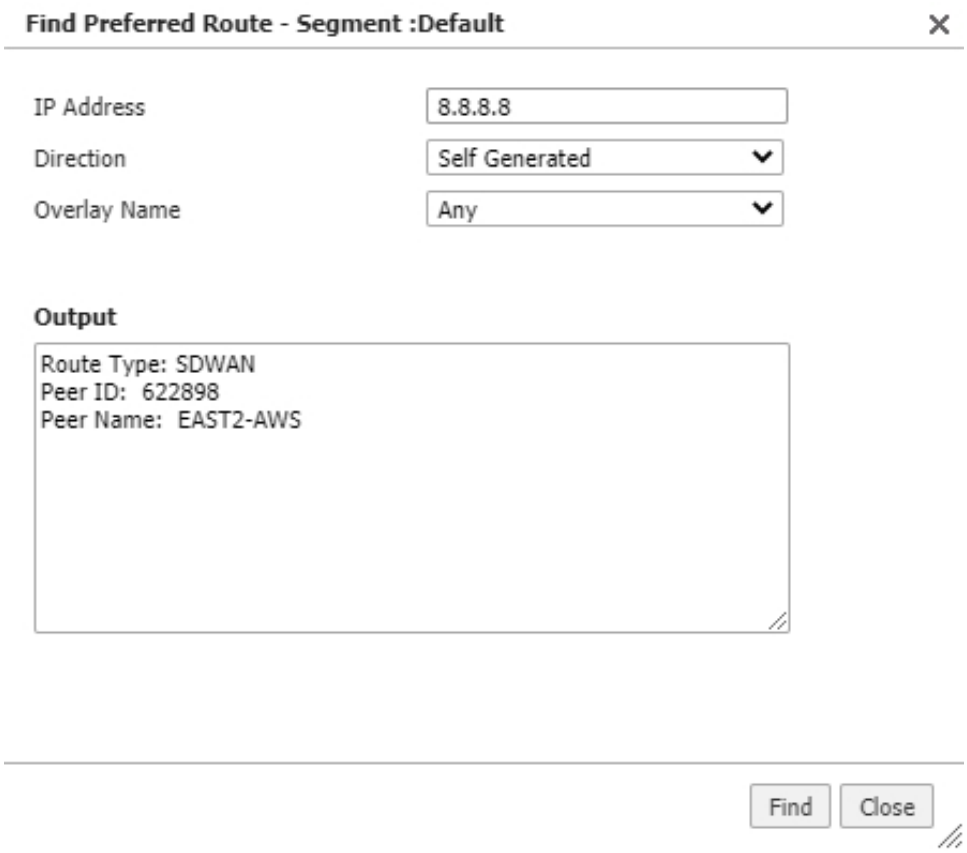
To show routes learned by appliances in the fabric, click **Configuration**, and then click **Routes**. Use this information to confirm configuration for route presence, AD, metric, and more.

## Find Preferred Route

Use this tool to determine traffic-forwarding decisions for traffic coming from the WAN or LAN, or for traffic self-generated by the appliance. To access the tool, click **Configuration**, and then click **Routes**. To edit one of the table entries, click the **Pencil** icon. The appliance-specific route page appears with a button displayed to load the tool.

**NOTE** If segmentation is enabled, make sure the entry selected is part of the segment under investigation.

The following example shows that self-generated traffic from this appliance, destined for 8.8.8.8, will be sent to the EAST2-AWS appliance, and that the route was learned over the SD-WAN fabric.




# Common Issues

| Issue | Resolution |
|---|---|
| Route not present on appliance from another appliance. | Confirm there is a tunnel up between the two appliances, or between the appliance and its hubs if using regional routing. |
| Routes not being advertised to other appliances. | Confirm there is a tunnel up between the two appliances, or between the appliance and its hubs if using regional routing. |
| Not enough or too many routes being seen from non-EdgeConnect devices. | Check inbound/outbound route maps for the routing protocol being used. |
| Routes not being advertised to other network equipment. | Confirm the routing protocol is in the appropriate state. Confirm the route maps are configured properly. |

# Tunnels

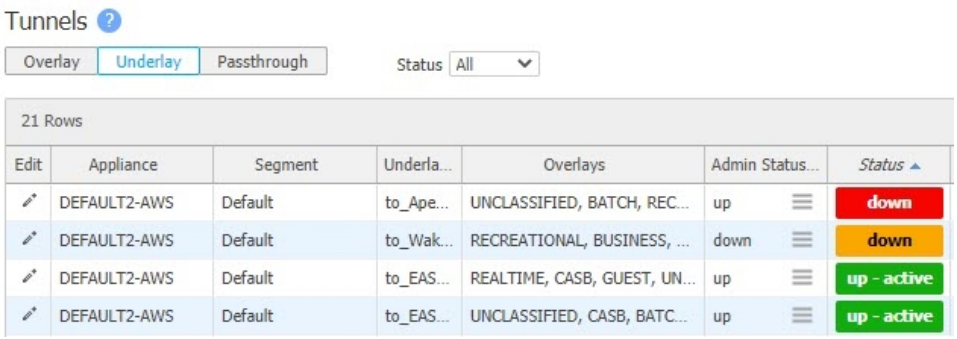
EdgeConnect tunnels are the foundation of SD-WAN and take three primary forms:

- *Overlay tunnels.* SD-WAN bonded tunnels.
- *Underlay tunnels*. IPsec tunnels mapping to discrete transports.
- *Passthrough tunnels*. Third-party tunnels (IPsec) and local breakout.

Underlay tunnels are the focus of this section. Overlay tunnels only go down if all associated underlay tunnels are also down. For third-party tunnel troubleshooting, see the appropriate configuration guide for that integration.

## Current Tunnel State

First, determine the current tunnel state. In Orchestrator, click **Configuration**, and then click **Tunnels**.




If there is no entry for the tunnel, Orchestrator is either pending synchronization or is configured to not build the tunnel (via Tunnel Exception, Regionalization, etc.).

Tunnels that are down in yellow have been configured this way administratively. Tunnels that are down in red are down due to an issue, and are the focus of troubleshooting here.

Possible reasons for issues with underlay tunnels include:

- Router configurations
- Firewall settings
- Carrier problems on MPLS, internet, LTE, etc.
- Appliance configurations (networking, labels, NAT)

# Troubleshooting Steps

## Research Tunnel History

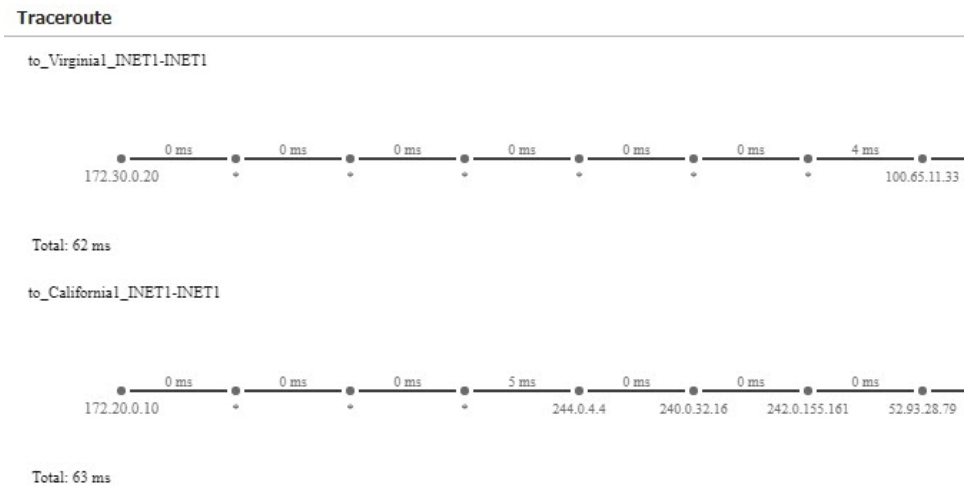
Begin by analyzing the history of the problematic tunnel. History can be viewed from the Tunnels tab (**Configuration** > **Tunnels**) or the Alarms page for the appliance.

An administrator should assess if the tunnel has ever come up active, and if so, when it went down. Tunnels that never established point to initial deployment problems, whereas tunnels that failed after deployment point to environment or network changes.

## Validate Routing and Connectivity

With history established, an administrator can validate routing and connectivity. From the same Tunnels tab, the tunnel traceroute provides quick feedback on whether there is reachability, and if not, where the tunnel is failing.

**NOTE** For internet-based transport, a failed traceroute or ping reachability does not mean there is no connectivity.




Ping and traceroute commands are available from the appliance UI and CLI, and can be used to further validate transport behavior.

## Validate IP and Port

With routing and connectivity validated, an administrator can validate IPs and ports.

- The *Remote IP:Port* field is the IP address learned by Cloud Portal and the associated port specified by the Overlay Setting page.
- The *Discovered IP:Port* field is the IP address and port contained in the NAT Discovery (NAT-D) packet sent at the beginning of tunnel setup.

If there is a difference of only ports, then there is a PAT (Port Address Translation) occurring. If the tunnel does not establish, validate that both ends are not dynamic PATs, as you cannot connect dynamic PATs to PATs.

If there is a difference in both IPs and ports, then a CGNAT (Carrier-Grade NAT) is occurring. If the tunnel does not establish, validate that both ends are not CGNATs or PATs, as CGNATs cannot connect to other CGNATs or PATs.

| Local IP:Port | Remote IP:Port | *Discovered IP:Port* ▾ | Max BW (Kb... | Mode | Uptime |
|---|---|---|---|---|---|
| 10.37.6.28:11121 | 49.199.20.16:11121 | *49.184.12.131:20911* | 50000(Auto) | IPSec UDP | 5d 8h 2m 6s |
| 10.37.6.28:11121 | 203.123.105.234:11... | *203.123.105.121:11...* | 100000(Auto) | IPSec UDP | 14d 15h 50m 30s |
| 10.37.6.28:11121 | 1.129.110.21:11121 | *1.129.110.32:34276* | 10000(Auto) | IPSec UDP | 14d 11h 32m 47s |

If you see *NONE:NONE* in the Discovered field, the local EdgeConnect never received a NAT-D packet from the remote appliance. In this case, validate transport and firewall configurations between the two EdgeConnects.

| Local IP:Port | Remote IP:Port | Discovered IP:Port | Max BW (Kbp... | Mode | Uptime |
|---|---|---|---|---|---|
| 64.191.210.143:11121 | 181.50.247.166:11121 | NONE:NONE | 10000(Auto) | IPSec UDP | 0 |
| 64.191.210.143:11121 | 98.109.122.122:11121 | NONE:NONE | 50000(Auto) | IPSec UDP | 0 |
| 10.0.0.6:11121 | 52.86.45.214:11131 | 52.86.45.214:11131 | 100000(Auto) | IPSec UDP | 10d 16h 30m 43s |
| 10.0.0.6:11121 | 34.89.22.72:11121 | 34.89.22.72:11121 | 100000(Auto) | IPSec UDP | 17d 13h 21m 43s |

# Overlay Troubleshooting

The Business Intent Overlay (BIO) is the one of the most important components for application matching and forwarding.

Each BIO can be configured differently depending on application flow requirements. However, if prerequisites for traffic going through the overlay are not met—including proper interface labels, application identification, and templates assigned—then creating an overlay is not enough.

If prerequisites are met and an application is not behaving as expected or not going through the overlay at all, there are typically three ways to match traffic coming into an overlay and troubleshoot:

- *Overlay ACLs (recommended).* Overlay ACLs are the most often used option for BIO configuration, so if application traffic is not matched to the correct overlay, this should be the first troubleshooting consideration. Validate the overlay configuration by addressing the following potential issues:
  - Is the application assigned to the correct overlay?
  - Does it have the correct permissions?
  - Because ACLs are per overlay, has the correct ACL been created for the correct overlay?
- *Appliance ACLs.* These are configured on each appliance, and can be applied to either a single appliance or a group of appliances. If an appliance ACL was created, make sure traffic coming from the LAN is properly matched into the Appliance ACL.
- *LAN Port Labels.* If LAN port labels are used, traffic is routed based on the matching label.

## Common Issues

| Issue | Resolution |
|---|---|
| Traffic matching into wrong BIO. | Make sure the traffic is being identified as the intended application. If it is, review BIO match criteria to verify that the application is in the list.<br>Appliances match traffic from the top BIO to the bottom one. Drag and drop the overlays to reorder if needed.<br>Make sure the overlay is applied on the **Configuration** > **Apply Overlays** tab. |
| Traffic not taking desired path. | Make sure desired interfaces are primary for the overlay. Review circuit performance for provider issues.<br>Review the Bonding Policy configuration and make any required changes. |

# Appendix

This appendix provides procedures for creating and uploading appliance system dumps to Silver Peak Support and replacing EdgeConnect appliances.

## Create and Upload Appliance System Dumps

To create and upload appliance system dumps to Support, complete the following steps.

1. Log in to the Orchestrator web interface.
2. Click **Support**, and then click **Tech Support - Appliances**.
3. From the tree view, select the appliances you want to work with.
4. Click **Generate Sys Dump**. This process can take a few minutes to complete. When it completes, the page refreshes.
5. Select the newly generated files in the table. Select multiple files by clicking each file while holding the **Ctrl** key. If you cannot find the files, click the **Last Modified** column to sort by most recent. Ignore any files starting with "tunbug." File names for system dumps use the format *sysdump-hostname-yyyymmdd-hhmmss.tgz*.
6. Click **Upload to Support**.
7. On the Upload Selected Files to Support dialog box, enter the case number in the **Case** field, and then click **Upload**.

## Replace an EdgeConnect Appliance

There are two ways to replace a Silver Peak EdgeConnect appliance, both of which impact service. Apply all organizational standard change control and related procedures accordingly.

If appliances are the same make and model, use RMA Wizard.

- The RMA Wizard swaps EdgeConnect configurations, as well as any Orchestrator configuration, such as tunnel exceptions.
- Both EdgeConnect appliances must be the same make and model (for example, EC-XS and EC-XS, not EC-XS and EC-M).

If appliances are not the same make and model, use the backup/restore process.

- This process copies the EdgeConnect configuration, but does not account for Orchestrator configurations such as tunnel exceptions, Business Intent Overlays (BIOs), templates, and site names.
- When using this process for appliances that are not the same make and model, check configurations carefully. Using different WAN port types, such as WAN0 on the old appliance and TWAN0 on the new appliance, could produce a configuration error.

These two methods of replacing an EdgeConnect appliance are explained below.

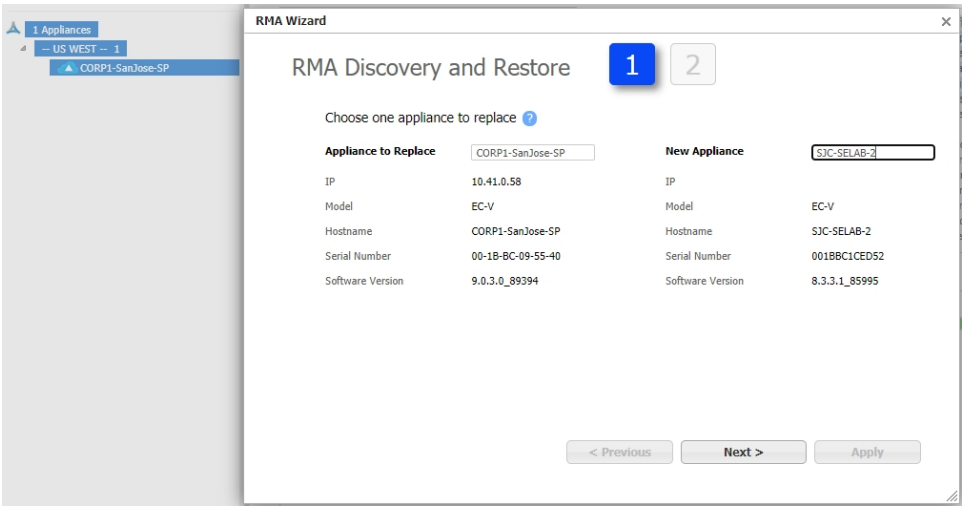
## RMA Wizard

Use this appliance replacement procedure if the appliances are the same make and model.

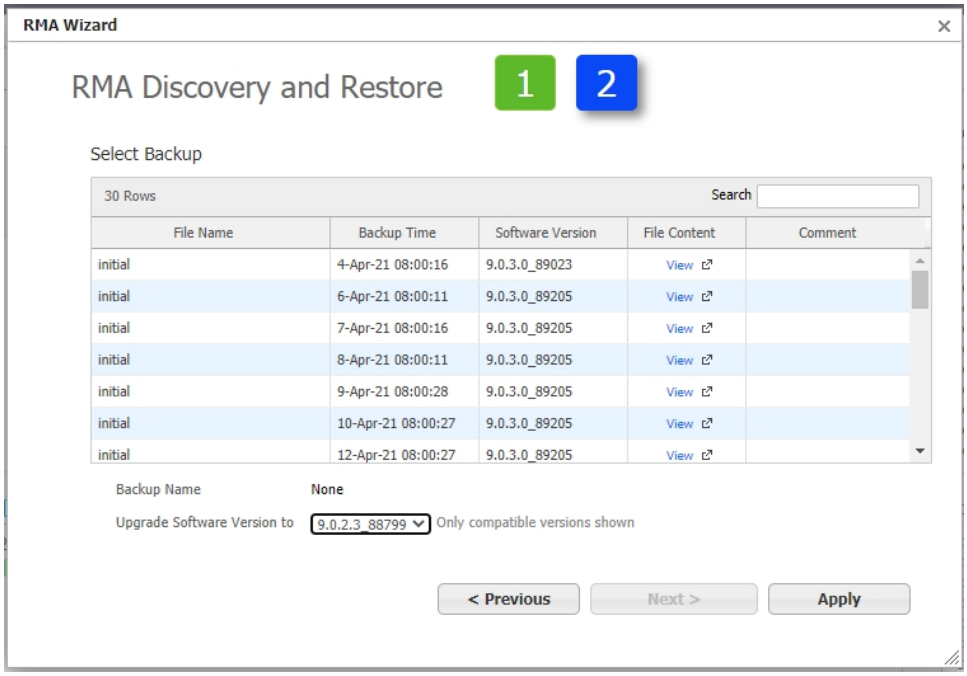
**NOTE** To perform this procedure, the new appliance must be a discovered appliance in the Orchestrator, reachable and ready to approve.

1. If reachable, create a backup of the current appliance. Click **Orchestrator**, and then click **Backup Now**. *WARNING:* Do not approve the new appliance or delete the old appliance.
2. If the appliance to be replaced is at a site with BGP/OSPF, shut down BGP/OSPF from the core to prevent routes from being propagated until the last step.
3. If replacing a VRRP site, change the working EdgeConnect's priority to a higher number so it remains the active VRRP for the duration of the swap process.
4. From the tree view in Orchestrator, select only the appliance you want to replace.
5. To run the RMA Wizard, click **Support**, and then click **RMA**.
6. On the first screen of the RMA Wizard, enter the name of the new appliance in the **New Appliance** field.

**NOTE** The new appliance must be discovered by the Orchestrator, but not approved.




7. Click **Next**.
8. Select the backup file you want to use for the new appliance.
9. In the **Upgrade Software Version to** dropdown list, select the software version for the new appliance.



10. Click **Apply**. The Orchestrator fully swaps out the two appliances.
11. Verify that all configurations for the new appliance have been restored.
12. To verify routes, click **Configuration**, and then click **Routes**. On the Routes page, click **SD-WAN Fabric** and verify the routes.
13. *(Optional)* Turn up BGP or appropriately set VRRP priorities.
14. Verify all routes and routing.

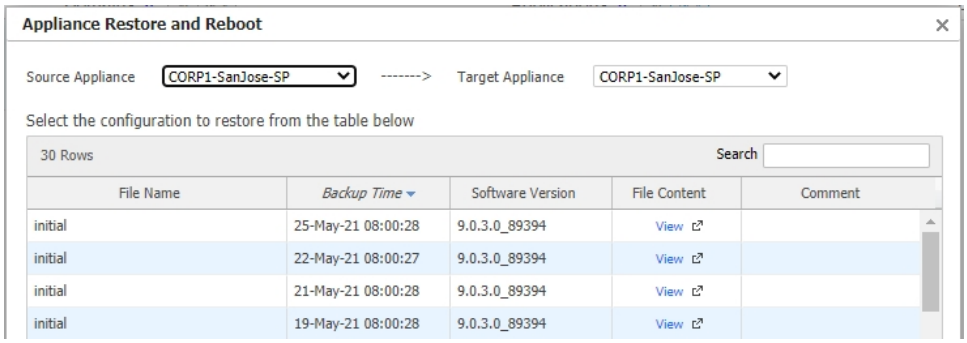
## Backup/Restore Process

Use this appliance replacement procedure if the appliances are not the same make and model.

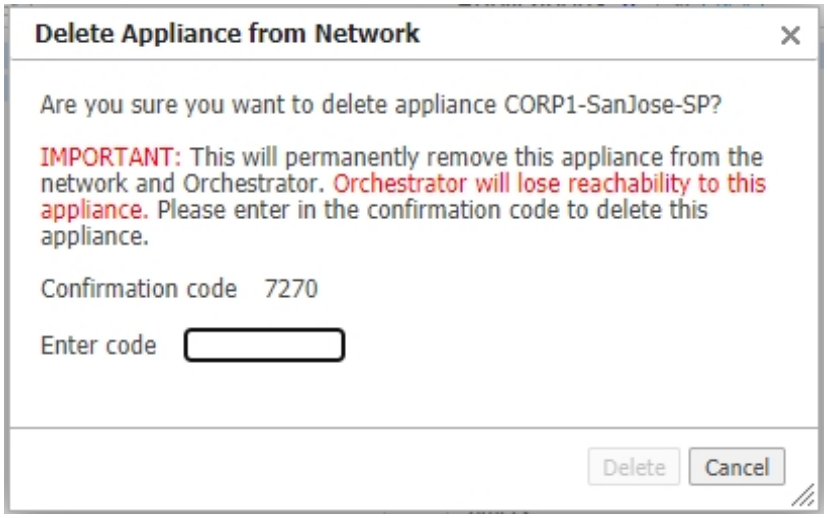
**WARNING** Do not delete the old appliance.

1. From the tree view in Orchestrator, select only the appliance to replace.
2. Click **Configuration**, and then click **Interfaces**.
3. Create a capture of the **Interfaces** page for reference.
4. If reachable, create a backup of the current appliance. Click **Orchestrator**, and then click **Backup Now**.
5. Swap the appliances (physical or virtual). Be sure to match each old appliance interface with the new.
    a. If upgrading an appliance to a larger appliance, this might mean going from WAN0 to TWAN0.
    b. You must manually enter the new interface information on the Deployment tab.
6. Click **Configuration**, and then click **Templates**.
7. Verify and note the templates that are currently applied to the appliance, because you will apply the same templates to the new appliance.
8. Approve the new appliance.
    a. Click **Configuration**, and then click **Configuration Wizard**.
    b. Upgrade to the proper version to match existing appliances.
    c. At this time, you only need a temporary hostname, password, and site name. If the site being replaced has two EdgeConnect appliances, make sure the site name matches the other appliance.
    d. Skip the Deployment, Loopback, and Local Routes pages.
    e. Apply only the default template to the appliance.
9. If the appliance you are replacing is at a site with BGP/OSPF, shut down BGP/OSPF from the core so that routes do not propagate until the last step.

10. If replacing a VRRP site, change the working EdgeConnect's priority to a higher number so it remains the active VRRP for the duration of the swap process.
11. From the tree view in Orchestrator, select only the appliance you want to replace.
12. Click **Administration**, and then click **Restore**.
13. Verify and select the appropriate Source Appliance and the Target Appliance you just approved.




14. Select the appropriate backup file from the table, and then click **Restore**. The new appliance gets the configuration from the backup file and reboots.
15. After rebooting completes, verify the configuration of the new appliance.
    a. Check the Deployment page, site name, and hostname. You might need to reconfigure the Deployment page based on whether the appliance is being upgraded and you are using a different port (for example, WAN0 to TWAN0 on the new appliance).
    b. If site name does not match the other appliance at the site, tunnels could be built between the appliances.
16. After verifying the configuration, delete the old appliance from Orchestrator. Click **Administration**, and then click **Remove from Orchestrator and Account**.
17. Enter the confirmation code, and then click **Delete**.




18. Now that the new appliance has its configuration, perform any configurations related to the Orchestrator.
19. Verify that all tunnels are built.
20. Verify that the new appliance is receiving the correct routes.
21. Turn up BGP facing the new EdgeConnect appliance.
    a. If this is a hub appliance, check downstream-connected routers to make sure they are receiving routes from the sites on SD-WAN only.
    b. If this is a spoke site, it should be receiving all routes.
22. If using VRRP, restore the priorities to the normal settings.
23. Verify that all traffic is working.