

# EdgeConnect and Akamai IPsec Tunnel Integration Using Service Orchestration

INTEGRATION GUIDE

## TABLE OF CONTENTS

<b>OVERVIEW .....</b>	<b>3</b>
<b>TOPOLOGY .....</b>	<b>3</b>
<b>AKAMAI CONTROL CENTER CONFIGURATION.....</b>	<b>3</b>
Configure Branches as Locations in SLA .....	4
Configure IPsec Credentials in SLA .....	5
Akamai POP FQDNs .....	5
<b>ARUBA ORCHESTRATOR TUNNEL CONFIGURATION.....</b>	<b>6</b>
Remote Endpoint Configuration .....	6
Interface Labels .....	8
Tunnel Settings.....	9
IP SLA .....	10
BIO Breakout .....	11
Remote Endpoint Association .....	11
<b>REDIRECT TRAFFIC TO THE AKAMAI SERVICE USING BUSINESS INTENT OVERLAY .....</b>	<b>12</b>
<b>VERIFY SERVICE ORCHESTRATION CONFIG PUSH TO DEVICES.....</b>	<b>15</b>
<b>VERIFY TUNNEL STATUS AND IP SLA STATUS .....</b>	<b>16</b>
Passthrough Tunnel Status.....	17
IP SLA Status .....	17
<b>VERIFY ACTIVE FLOWS ON THE EDGECONNECT SD-WAN.....</b>	<b>18</b>

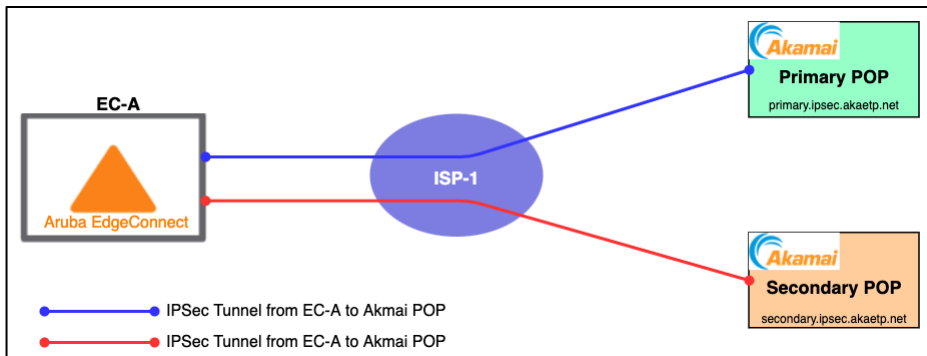
## OVERVIEW

This document details the configurations required on the Aruba Orchestrator and Akamai Control Center portal to provision IPsec tunnels between an EdgeConnect SD-WAN appliance and Akamai VPN endpoints. The Service Orchestration feature on Aruba Orchestrator can be used to orchestrate IPsec tunnel configuration for the SD-WAN fabric, which comprises multiple EdgeConnect appliances.

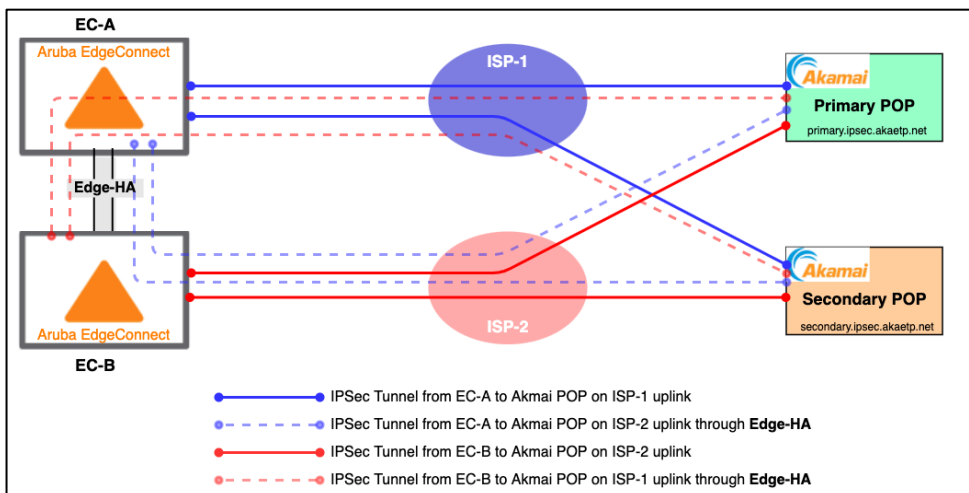
## TOPOLOGY

IPsec tunnels to Akamai endpoints can be deployed in a single appliance site or sites with Aruba Edge-HA deployment, which involves two appliances and multiple uplinks. If configured, Service Orchestration pushes the IPsec tunnel configuration to the appliances to build tunnels using all available uplinks.

The image below shows a simple topology: a single EdgeConnect SD-WAN appliance with one ISP connection.



The image below shows Edge-HA topology: two EdgeConnect SD-WAN appliances sharing their uplink connection. In this case, Service Orchestration builds tunnels using the uplink from each appliance.



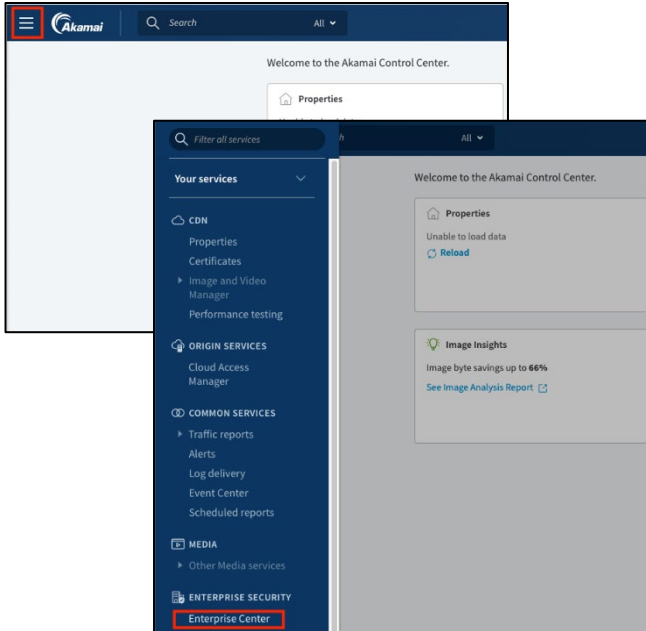
## AKAMAI CONTROL CENTER CONFIGURATION

Prior to configuring Aruba Orchestrator, complete following steps on Akamai Control Center.

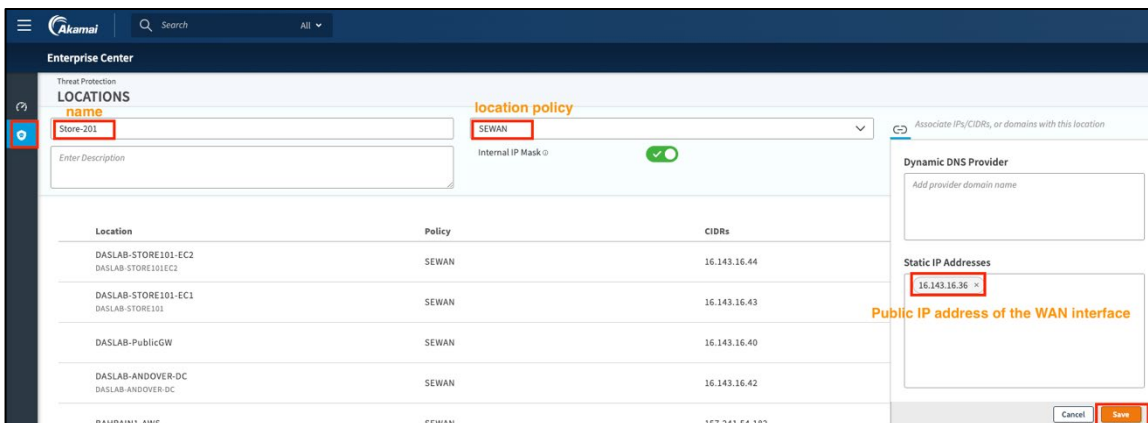
## Configure Branches as Locations in SLA

**NOTE:** For reference, see <https://techdocs.akamai.com/etp/docs/create-location>.

1. Log in to the Akamai Control Center.
2. Using the top-left menu, navigate to **Your services > Enterprise Security > Enterprise Center**.



3. From the left sidebar, navigate to **Threat Protection > Locations**.
4. Click the **+** icon at the top-left of the screen to add new location.
5. Add the branch details, such as name and public IP address, and then associate an existing location policy.



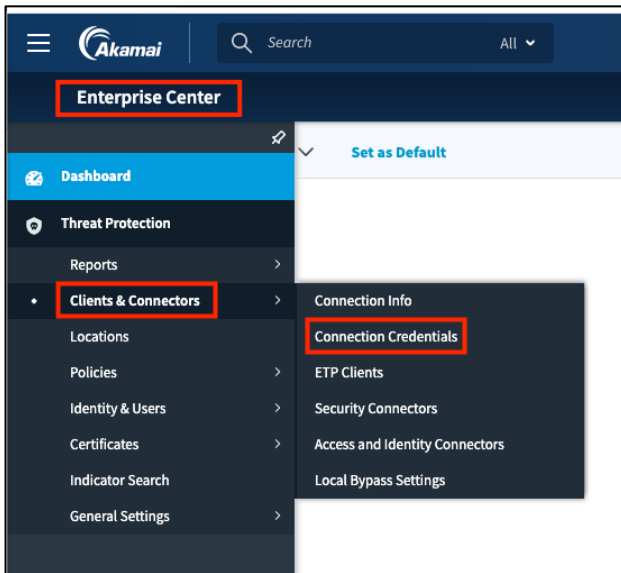
6. Click **Save**.
7. To commit the changes, click **Save and Deploy**.

8. Repeat the steps in this procedure for each branch location.

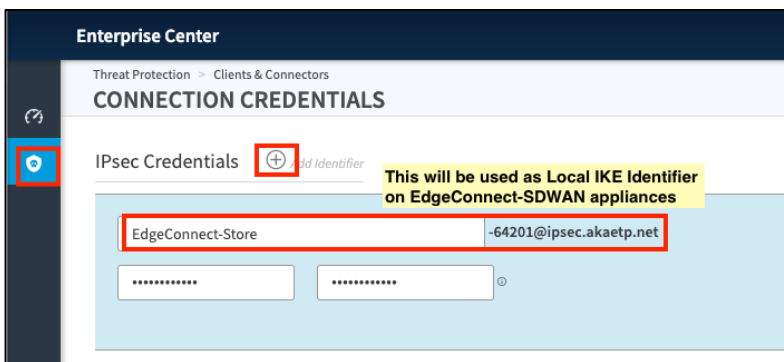
### Configure IPsec Credentials in SLA

**NOTE:** For reference, see <https://techdocs.akamai.com/etp/docs/prepare-sdwan-setup>.

1. From the left sidebar in the Akamai Control Center, navigate to **Threat Protection > Clients & Connectors > Connection Credentials**.



2. To add new IPsec credentials associated with an IKE identifier, click the + icon.
3. Enter the IKE identifier name for your SD-WAN fabric and pre-shared key used for IPsec negotiation.



### Akamai POP FQDNs

To build tunnels from SD-WAN appliances to Akamai, use the primary and secondary DNS names below. When an individual appliance resolves these FQDNs, the nearest Akamai POP IPv4 address resolves as well, with resulting SD-WAN appliances automatically picking up the nearest POP location to build tunnels.

- primary.ipsec.akaetp.net
- secondary.ipsec.akaetp.net

These will be used for the configuration steps in the next section.

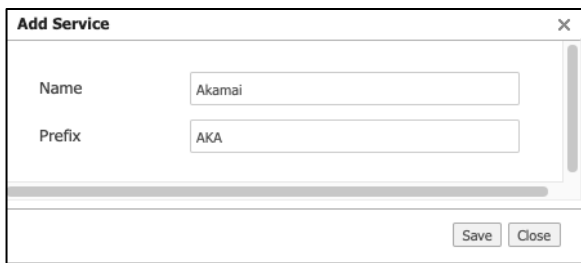
## ARUBA ORCHESTRATOR TUNNEL CONFIGURATION

The Service Orchestration feature orchestrates tunnel configuration for all appliances managed by Aruba Orchestrator.

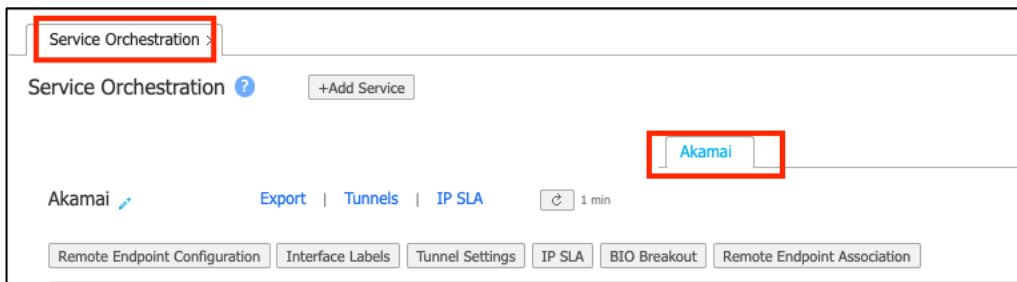
1. Log in to your Aruba Orchestrator.
2. Navigate to **Configuration > Cloud Services > Service Orchestration**, and then click **Add Service**.

The Add Service window opens.

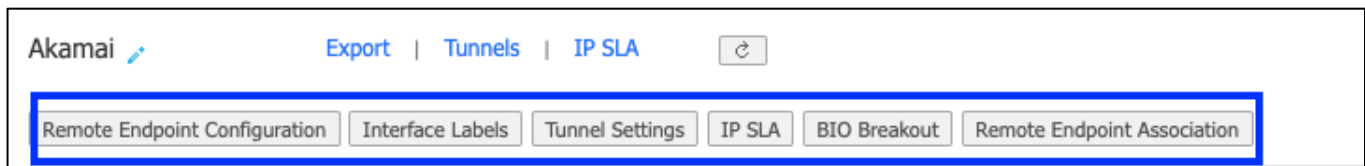
3. Enter a name and prefix—in this example, *Akamai* and *AKA*, respectively—and then click **Save**.



This should create a new service on the Service Orchestration tab called *Akamai*.

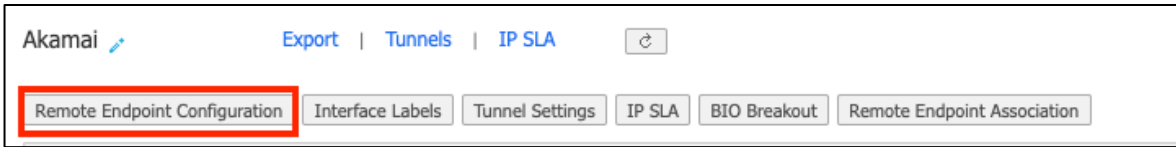


The sections that follow explain how to configure each of the tabs under the Akamai service.



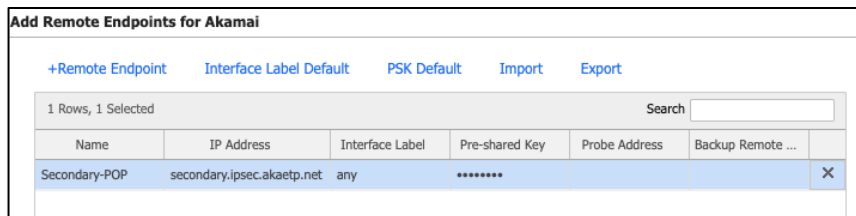
### Remote Endpoint Configuration

This section explains how to configure the primary and secondary Akamai POP endpoints using the FQDN identified previously, along with the pre-shared key configured in the Akamai Enterprise Center.



1. Click **Remote Endpoint Configuration**.
2. To add a row, click **+Remote Endpoint**.
3. Enter the following:

Field	Value
<b>Name</b>	Secondary-POP
<b>IP Address</b>	secondary.ipsec.akaetp.net
<b>Interface Label</b>	any
<b>Pre-shared Key</b>	Enter the key configured in the Akamai Enterprise Center.



4. To add an additional row, click **+Remote Endpoint** again.
5. Enter the following:

Field	Value
<b>Name</b>	Primary-POP
<b>IP Address</b>	primary.ipsec.akaetp.net
<b>Interface Label</b>	any
<b>Pre-shared Key</b>	Enter the key configured in the Akamai Enterprise Center.
<b>Backup Remote Endpoint</b>	Secondary-POP

**Add Remote Endpoints for Akamai**

+Remote Endpoint   Interface Label Default   PSK Default   Import   Export

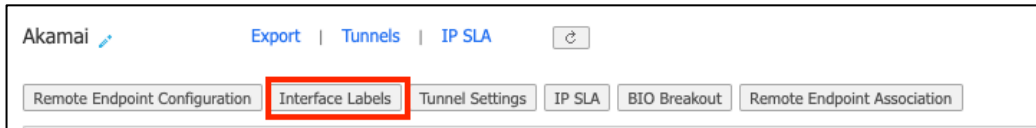
2 Rows, 1 Selected   Search

Name	IP Address	Interface Label	Pre-shared Key	Probe Address	Backup Remote Endpoint	
Primary-POP	secondary.ipsec....	any	*****		Secondary-POP	X
Secondary-POP	secondary.ipsec....	any	*****			X

**NOTE:** In steps 3 and 5, the interface label is configured as “any.” This means the Orchestrator will use all available WAN interfaces configured under Interface Labels to build tunnel configuration.

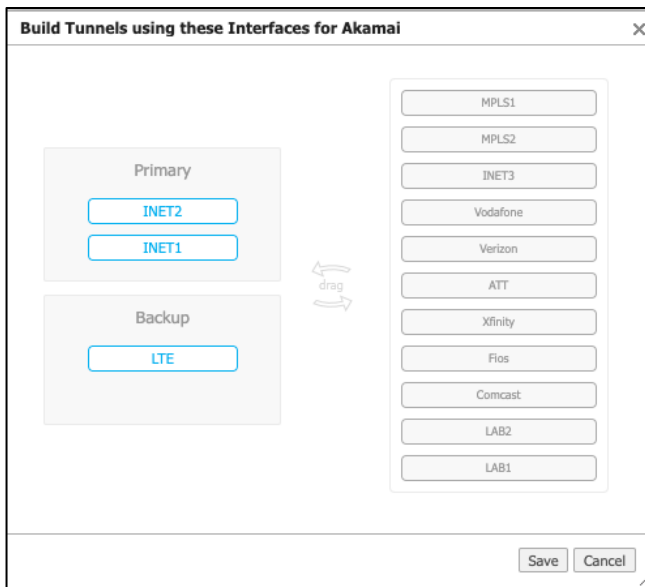
### Interface Labels

This section explains how to select the uplink interfaces (labels) used to build tunnels to Akamai primary and secondary POP endpoints.



1. Click **Interface Labels**.
2. Select all WAN Interface labels that your SD-WAN fabric is using. Service Orchestration will prepare IPsec tunnel configuration for each WAN interface selected here.

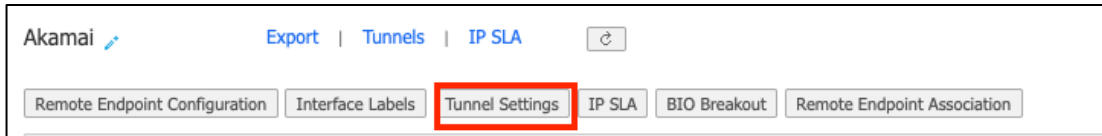
**NOTE:** You must have added each of the WAN IPs (public IP address) on Akamai Enterprise Center (under Locations). For example, if one branch has two WAN uplinks, then both WAN public IP addresses must be added in Akamai Enterprise Center.



3. Click **Save**.

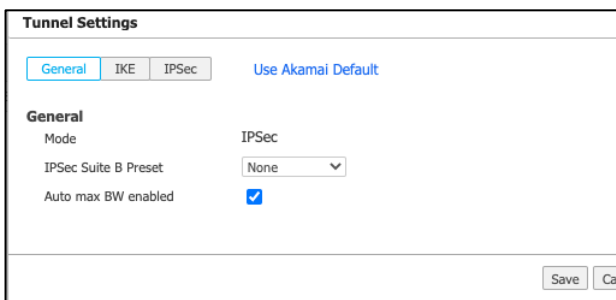
## Tunnel Settings

This section explains how to configure the IKE-Phase1 and Phase-2 settings the SD-WAN appliance uses to build tunnels to Akamai POP endpoints.



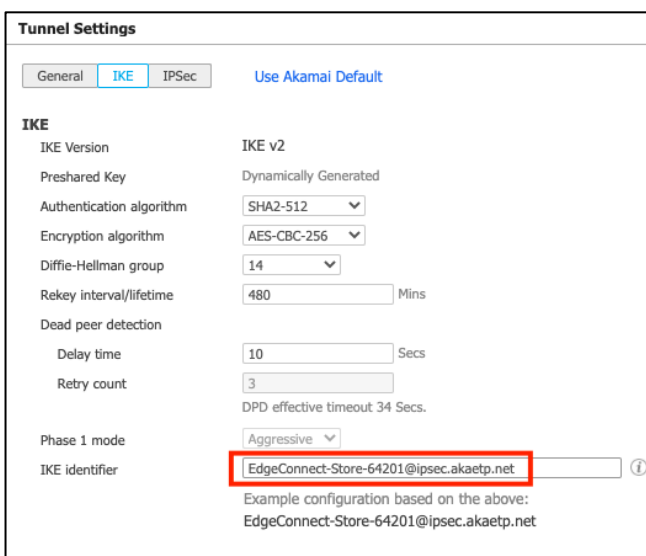
Akamai-supported cipher suites for IKE and ESP are listed here: <https://techdocs.akamai.com/etp/docs/ipsec-cipher-suites>. This serves as a reference when configuring the tunnel settings.

1. Click **Tunnel Settings**.
2. Configure the General tab as follows:



3. Configure the IKE and IPsec tabs as follows.

**NOTE:** The IKE identifier is configured based on the IPsec credential settings in the Akamai Control Center. It is important to enter the same string copied from Akamai Control Center > Enterprise Center > Threat Protection > IPsec Credentials.



4. Click **Save**.

## IP SLA

This section illustrates how to enable IP SLA settings so the appliance can monitor tunnel health using HTTPS probe to sp-ipsla.silverpeak.cloud. The probe destination URL in this setting can be customized.

1. Click **IP SLA**.
2. Configure the IP SLA Settings for Akami window as follows:

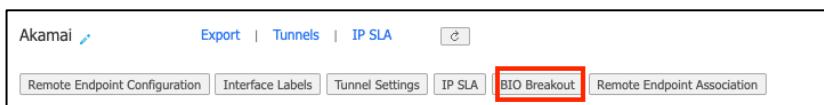
**NOTE:** Take special care to ensure that the following settings are configured correctly:

- **Enable IP SLA rule orchestration:** Enabled
- **Monitor:** HTTP/HTTPS
- **Source interface:** Select the interface label from the drop-down list. In this example, **Loopback** is selected. IP SLA uses this value to source probe traffic to the probe destination address. Note that for the IP SLA profile to be pushed to the SD-WAN appliances, there must be at least one interface on the appliance with the matching label.
- **HTTP request timeout:** 2

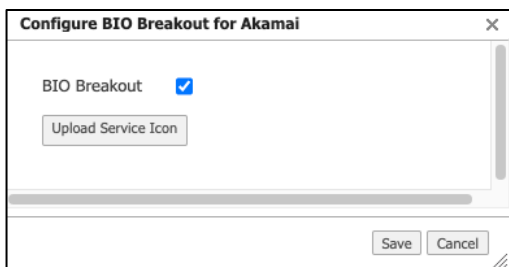
3. Click **Save**.

### BIO Breakout

This section explains how to ensure that the tunnels created for the Akamai endpoints are added to the Business Intent Overlay (BIO) as a service.

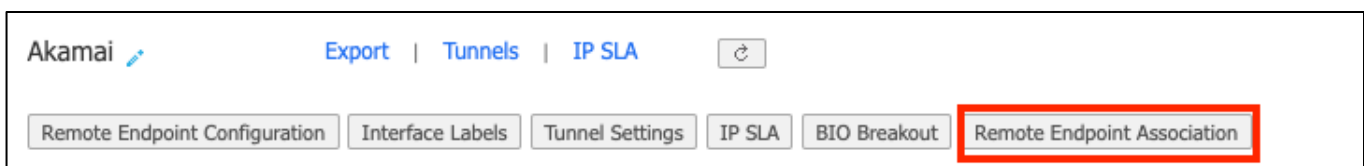


1. Click **BIO Breakout**.
2. Ensure that the **BIO Breakout** check box is selected.



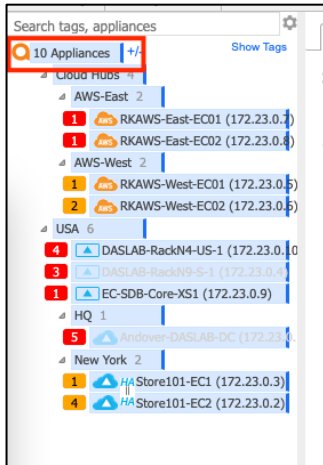
3. (Optional) If an icon must be visible on BIO, upload a Service Icon.
4. Click **Save**.

### Remote Endpoint Association

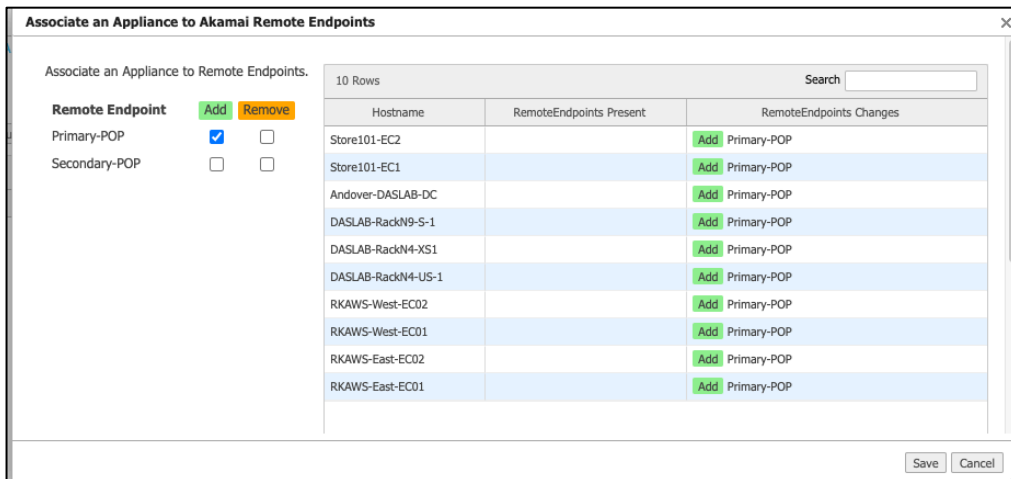


This section explains how to associate the Akamai endpoints to the EdgeConnect SD-WAN appliances. When association is completed, Aruba Orchestrator pushes the required IPsec tunnel configuration and IP SLA configurations to the EdgeConnect appliances.

1. In Orchestrator, select the appliances from the left-side Appliance Tree. This example will associate all appliances with the Akamai endpoints.



2. Click **Remote Endpoint Association**.
3. Select the **Add** check box next to Primary-POP. This associates both the primary and secondary Akamai endpoints with the EdgeConnect SD-WAN appliance.



4. Click **Save**.

## REDIRECT TRAFFIC TO THE AKAMAI SERVICE USING BUSINESS INTENT OVERLAY

This section explains how to configure the Business Intent Overlay for which internet traffic is directed to the Akamai service.

1. In Orchestrator, navigate to **Configuration > Overlays & Security > Business Intent Overlay**.
2. Either select any existing Overlay that is currently matching the internet traffic or create a new overlay for redirecting internet traffic. This example will reconfigure an existing overlay called *CASB*.

Priority	Overlay	Region	Topology	Primary Interfaces	Backup Interfaces	QoS & Security	Policy Order	Primary Interfaces	Backup Interface
1	RealTime Match Traffic Overlay ACL	Global Regions ▶	Regional Hub & Spoke	INET1 INET2 INET3 MPLS1 MPLS2 High Availability Waterfall: Overall Quality			1 Break out 2 Backhaul	INET1 INET2 Waterfall: Auto	LTE
2	<b>CASB</b> Match Traffic Overlay ACL	Global Regions ▶	Regional Hub & Spoke	INET1 INET2 INET3 MPLS1 MPLS2 High Throughput Balanced: Link Capacity ...			1 Break out	INET1 INET2 Waterfall: Auto <b>Click anywhere on this section</b>	LTE
3	CriticalApps Match Traffic Overlay ACL	Global Regions ▶	Regional Hub & Spoke	INET1 INET2 INET3 MPLS1 MPLS2 High Quality Waterfall: Overall Quality			1 Break out	INET2 INET1 Waterfall: Auto	LTE
4	BulkApps Match Traffic Overlay ACL	Global Regions ▶	Regional Hub & Spoke	INET2 INET1 INET3 MPLS2 MPLS1 High Quality Waterfall: Overall Quality			1 Break out	INET2 INET1 Waterfall: Auto	LTE
5	DefaultOverlay Match Traffic Overlay ACL	Global Regions ▶	Regional Hub & Spoke	INET1 INET3 INET2 MPLS1 MPLS2 High Quality Waterfall: Overall Quality			1 Break out	INET2 INET1 Waterfall: Auto	LTE

- In the Match field, click the **Edit** icon.
- Modify the Overlay ACL to match **TCP** port **80** (HTTP) and **443** (HTTPS).

**Overlay Configuration**

Name: CASB **1** Match: Overlay ACL Protocol: tcp, Port 80|443 **2**

**Associate ACL**

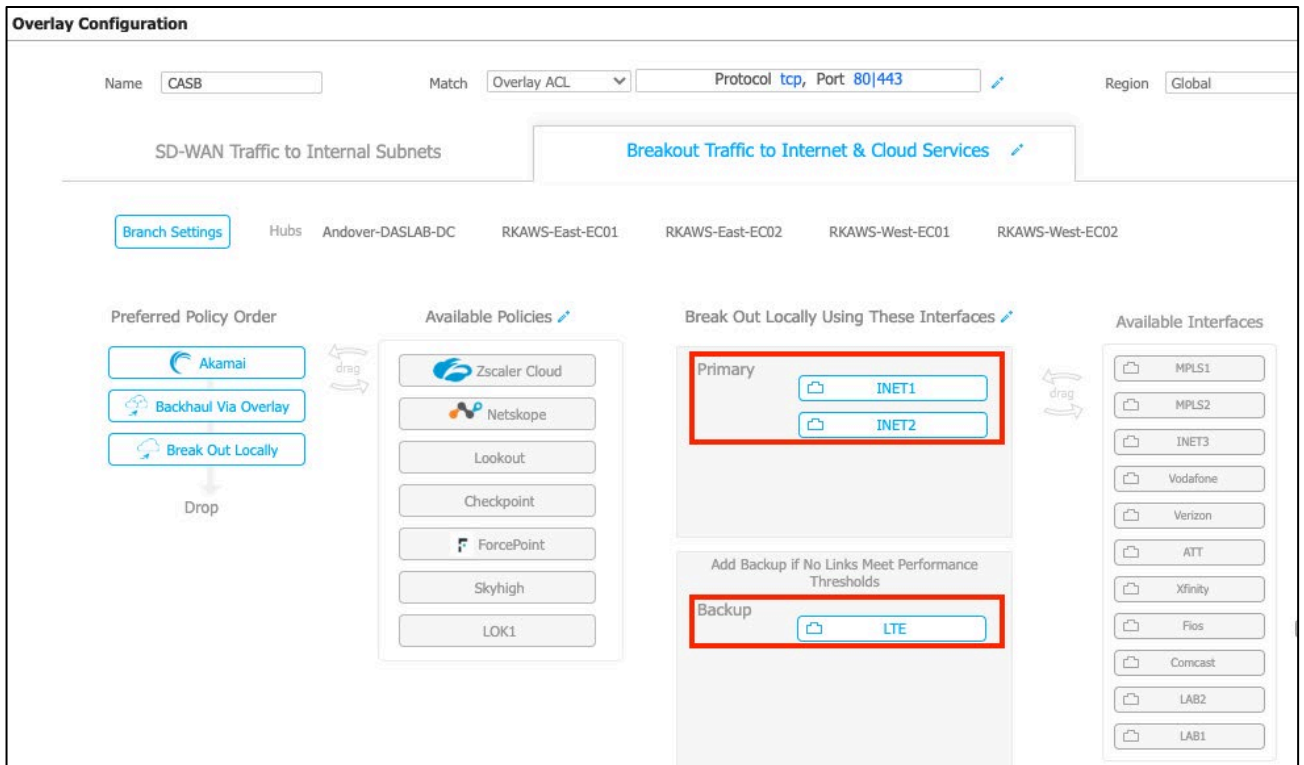
Priority	Match Criteria	Permit
1010	Protocol tcp, Port 80 443 <b>3</b>	permit

- Click the **Breakout Traffic to Internet & Cloud Services** tab.
- Drag the **Akamai** policy from the Available Policies column to the Preferred Policy Order column.

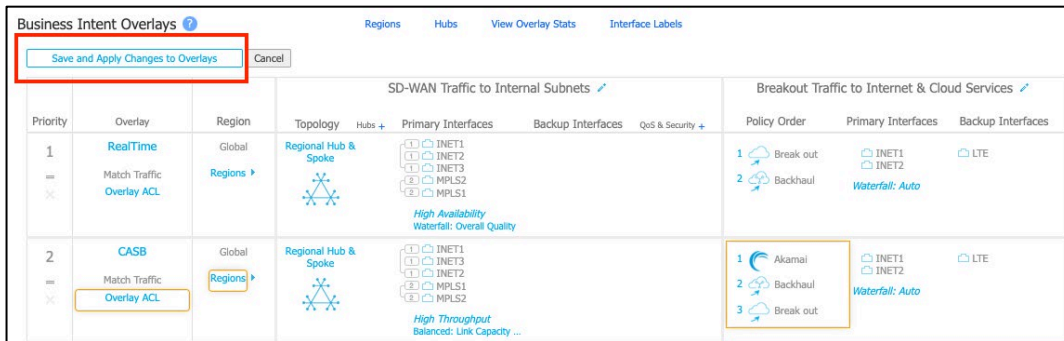
The screenshot displays the 'Overlay Configuration' page for a policy named 'CASB'. The match criteria are set to 'Overlay ACL' with 'Protocol tcp, Port 80|443'. The region is 'Global'. The traffic is categorized as 'Breakout Traffic to Internet & Cloud Services'. Under 'Preferred Policy Order', 'Akamai' is at the top, followed by 'Backhaul Via Overlay' and 'Break Out Locally'. The 'Available Policies' list includes Zscaler Cloud, Netskope, Lookout, Checkpoint, ForcePoint, Skyhigh, and LOK1. The 'Break Out Locally Using These Interfaces' section has a 'Primary' section with 'INET1' and 'INET2', and a 'Backup' section with 'LTE'. The 'Available Interfaces' list includes MPLS1, MPLS2, INET3, Vodafone, Verizon, ATT, Xfinity, Fios, Comcast, LAB2, and LAB1.

**NOTE:** It is important to put the Akamai policy at the top of the Preferred Policy Order. This enables all internet-bound traffic to be redirected to Akamai tunnels.

7. If you select **Backhaul Via Overlay**, **Break Out Locally**, or both to use as backup options, then if the Akamai tunnel service goes down, traffic is redirected using these policies. If you do not want a backup option, remove them from Preferred Policy Order. In that case, internet-bound traffic drops if the Akamai tunnel service is down.
8. Under Break Out Locally Using These Interfaces, drag and drop all primary WAN interfaces to the **Primary** section, and all backup interfaces to the **Backup** section. If more than one interface is added to the Primary section, then the traffic is load-balanced on the Akamai IPsec tunnel built on those WAN interfaces.



9. To complete the setting changes, click **OK**.
10. To complete Business Intent Overlay configurations, click **Save and Apply Changes to Overlays**.



## VERIFY SERVICE ORCHESTRATION CONFIG PUSH TO DEVICES

This section explains how to run a passthrough tunnel config push to verify Service Orchestration on EdgeConnect SD-WAN appliances.

1. Navigate to **Orchestrator > Tools > Audit Logs**.
2. Search for **AKA** (or the prefix entered [when configuring the Akamai service](#)).
  - a. The image below shows that the passthrough tunnel configuration has been pushed to the device successfully.

OverlayManager	EC-S0B-Core-N11	Add pass through tunnels	COMPLETED	Pass through tunnels added. Tunnels added: 2 Data = ("Added":"ThirdParty_AKA_Primary_POP_INET1_...	19-Dec-22 18:29	19-Dec-22 18:29	19-Dec-22 18:29	100	Success
OverlayManager	DASLAB-RackM-US-1	Add pass through tunnels	COMPLETED	Pass through tunnels added. Tunnels added: 2 Data = ("Added":"ThirdParty_AKA_Primary_POP_INET1_...	19-Dec-22 18:29	19-Dec-22 18:29	19-Dec-22 18:29	100	Success
OverlayManager	RKAW5-East-EC02	Add pass through tunnels	COMPLETED	Pass through tunnels added. Tunnels added: 2 Data = ("Added":"ThirdParty_AKA_Primary_POP_INET1_...	19-Dec-22 18:28	19-Dec-22 18:28	19-Dec-22 18:28	100	Success
OverlayManager	RKAW5-East-EC01	Add pass through tunnels	COMPLETED	Pass through tunnels added. Tunnels added: 2 Data = ("Added":"ThirdParty_AKA_Primary_POP_INET1_...	19-Dec-22 18:30	19-Dec-22 18:30	19-Dec-22 18:30	100	Success
OverlayManager	RKAW5-West-EC02	Add pass through tunnels	COMPLETED	Pass through tunnels added. Tunnels added: 2 Data = ("Added":"ThirdParty_AKA_Primary_POP_INET1_...	19-Dec-22 18:30	19-Dec-22 18:30	19-Dec-22 18:30	100	Success
OverlayManager	RKAW5-West-EC01	Add pass through tunnels	COMPLETED	Pass through tunnels added. Tunnels added: 2 Data = ("Added":"ThirdParty_AKA_Primary_POP_INET1_...	19-Dec-22 18:29	19-Dec-22 18:29	19-Dec-22 18:29	100	Success
OverlayManager	Andover-DASLAB-DC	Add pass through tunnels	COMPLETED	Pass through tunnels added. Tunnels added: 2 Data = ("Added":"ThirdParty_AKA_Primary_POP_INET1_...	19-Dec-22 18:30	19-Dec-22 18:30	19-Dec-22 18:30	100	Success
OverlayManager	DASLAB-RackM-US-1	Add pass through tunnels	COMPLETED	Pass through tunnels added. Tunnels added: 2 Data = ("Added":"ThirdParty_AKA_Primary_POP_INET1_...	19-Dec-22 18:29	19-Dec-22 18:29	19-Dec-22 18:29	100	Success
OverlayManager	Store101-EC2	Add pass through tunnels	COMPLETED	Pass through tunnels added. Tunnels added: 4 Data = ("Added":"ThirdParty_AKA_Primary_POP_INET1_...	19-Dec-22 18:29	19-Dec-22 18:29	19-Dec-22 18:29	100	Success
OverlayManager	Store101-EC1	Add pass through tunnels	COMPLETED	Pass through tunnels added. Tunnels added: 4 Data = ("Added":"ThirdParty_AKA_Primary_POP_INET1_...	19-Dec-22 18:29	19-Dec-22 18:29	19-Dec-22 18:29	100	Success

**NOTE:** Passthrough tunnel configuration will only be pushed if at least one matching WAN label (as configured under Interface Labels) exists on the EdgeConnect SD-WAN appliance.

- b. The image below shows that the FQDNs for NSLOOKUP have been applied successfully. Because FQDNs are used for the primary and secondary POP, the EdgeConnect SD-WAN appliance must be able to resolve those FQDNs before tunnel can be built.

OverlayManager	RKAW5-East-EC02	Apply FQDNs for Nslookup	COMPLETED	Applied FQDNs. Data = ("secondary.ipsec.akatp.net","primary.ipsec.akatp.net")	19-Dec-22 18:29	19-Dec-22 18:29	19-Dec-22 18:29	100	Success
OverlayManager	RKAW5-East-EC01	Apply FQDNs for Nslookup	COMPLETED	Applied FQDNs. Data = ("secondary.ipsec.akatp.net","primary.ipsec.akatp.net")	19-Dec-22 18:29	19-Dec-22 18:29	19-Dec-22 18:29	100	Success
OverlayManager	Andover-DASLAB-DC	Apply FQDNs for Nslookup	COMPLETED	Applied FQDNs. Data = ("secondary.ipsec.akatp.net","primary.ipsec.akatp.net")	19-Dec-22 18:29	19-Dec-22 18:29	19-Dec-22 18:29	100	Success
OverlayManager	DASLAB-RackM-US-1	Apply FQDNs for Nslookup	COMPLETED	Applied FQDNs. Data = ("secondary.ipsec.akatp.net","primary.ipsec.akatp.net")	19-Dec-22 18:28	19-Dec-22 18:28	19-Dec-22 18:28	100	Success
OverlayManager	RKAW5-West-EC01	Apply FQDNs for Nslookup	COMPLETED	Applied FQDNs. Data = ("secondary.ipsec.akatp.net","primary.ipsec.akatp.net")	19-Dec-22 18:28	19-Dec-22 18:28	19-Dec-22 18:28	100	Success
OverlayManager	Store101-EC2	Apply FQDNs for Nslookup	COMPLETED	Applied FQDNs. Data = ("secondary.ipsec.akatp.net","primary.ipsec.akatp.net")	19-Dec-22 18:28	19-Dec-22 18:28	19-Dec-22 18:28	100	Success
OverlayManager	Store101-EC1	Apply FQDNs for Nslookup	COMPLETED	Applied FQDNs. Data = ("secondary.ipsec.akatp.net","primary.ipsec.akatp.net")	19-Dec-22 18:28	19-Dec-22 18:28	19-Dec-22 18:28	100	Success
OverlayManager	EC-S0B-Core-N11	Apply FQDNs for Nslookup	COMPLETED	Applied FQDNs. Data = ("secondary.ipsec.akatp.net","primary.ipsec.akatp.net")	19-Dec-22 18:28	19-Dec-22 18:28	19-Dec-22 18:28	100	Success
OverlayManager	DASLAB-RackM-US-1	Apply FQDNs for Nslookup	COMPLETED	Applied FQDNs. Data = ("secondary.ipsec.akatp.net","primary.ipsec.akatp.net")	19-Dec-22 18:28	19-Dec-22 18:28	19-Dec-22 18:28	100	Success

- c. The image below shows that IP SLA rules have been pushed to the device successfully. IP SLA rules are pushed to the device only if the following two conditions are met:

- The interface must exist on the EdgeConnect SD-WAN appliance with a matching label that is configured as a Source Interface for IP SLA probes (see [IP SLA](#)).
- There is at least one overlay (under Business Intent Overlay) using the Akamai service tunnel in the Preferred Policy Order section. (see [Redirecting Traffic to Akamai](#)).

OverlayManager	RKAW5-East-EC02	Add Ipsla Rules	COMPLETED	Ipsla rules added ("MGR_https-monitor_om_passThrough_233","operation":"OPERATION_om_passThrough_2...	19-Dec-22 19:09	19-Dec-22 19:09	19-Dec-22 19:09	100	Success
OverlayManager	RKAW5-East-EC01	Add Ipsla Rules	COMPLETED	Ipsla rules added ("MGR_https-monitor_om_passThrough_242","operation":"OPERATION_om_passThrough_2...	19-Dec-22 19:09	19-Dec-22 19:09	19-Dec-22 19:09	100	Success
OverlayManager	RKAW5-West-EC02	Add Ipsla Rules	COMPLETED	Ipsla rules added ("MGR_https-monitor_om_passThrough_253","operation":"OPERATION_om_passThrough_2...	19-Dec-22 19:09	19-Dec-22 19:09	19-Dec-22 19:09	100	Success
OverlayManager	DASLAB-RackM-US-1	Add Ipsla Rules	COMPLETED	Ipsla rules added ("MGR_https-monitor_om_passThrough_67","operation":"OPERATION_om_passThrough_60...	19-Dec-22 19:09	19-Dec-22 19:09	19-Dec-22 19:09	100	Success
OverlayManager	RKAW5-West-EC01	Add Ipsla Rules	COMPLETED	Ipsla rules added ("MGR_https-monitor_om_passThrough_649","operation":"OPERATION_om_passThrough_6...	19-Dec-22 19:09	19-Dec-22 19:09	19-Dec-22 19:09	100	Success
OverlayManager	Store101-EC1	Add Ipsla Rules	COMPLETED	Ipsla rules added ("MGR_https-monitor_om_passThrough_80","operation":"OPERATION_om_passThrough_8...	19-Dec-22 19:09	19-Dec-22 19:09	19-Dec-22 19:09	100	Success
OverlayManager	Andover-DASLAB-DC	Add Ipsla Rules	COMPLETED	Ipsla rules added ("MGR_https-monitor_om_passThrough_84","operation":"OPERATION_om_passThrough_84...	19-Dec-22 19:09	19-Dec-22 19:09	19-Dec-22 19:09	100	Success
OverlayManager	Store101-EC2	Add Ipsla Rules	COMPLETED	Ipsla rules added ("MGR_https-monitor_om_passThrough_869","operation":"OPERATION_om_passThrough_8...	19-Dec-22 19:09	19-Dec-22 19:09	19-Dec-22 19:09	100	Success
OverlayManager	DASLAB-RackM-US-1	Add Ipsla Rules	COMPLETED	Ipsla rules added ("MGR_https-monitor_om_passThrough_148","operation":"OPERATION_om_passThrough_148...	19-Dec-22 19:25	19-Dec-22 19:25	19-Dec-22 19:25	100	Success

## VERIFY TUNNEL STATUS AND IP SLA STATUS

On the Service Orchestration tab (Configuration > Cloud Services > Service Orchestration), the Connection Status should be Up. This indicates that the IPsec tunnel is functional and IP SLA probes are working through the tunnel.

Appliance	Interface Label	Primary Remote Endpoint	Backup Remote Endpoint	Tunnel Local Identifier	Primary Tunnel Remote Identifier	Backup Tunnel Remote Identifier	Connection Status
RKAW5-East-EC02	INET1	Primary-POP	Secondary-POP	EdgeConnect:Store-64201@ipsec.akatp.net	primary.ipsec.akatp.net	secondary.ipsec.akatp.net	Up
RKAW5-East-EC01	INET1	Primary-POP	Secondary-POP	EdgeConnect:Store-64201@ipsec.akatp.net	primary.ipsec.akatp.net	secondary.ipsec.akatp.net	Up
RKAW5-West-EC01	INET1	Primary-POP	Secondary-POP	EdgeConnect:Store-64201@ipsec.akatp.net	primary.ipsec.akatp.net	secondary.ipsec.akatp.net	Up
RKAW5-West-EC02	INET1	Primary-POP	Secondary-POP	EdgeConnect:Store-64201@ipsec.akatp.net	primary.ipsec.akatp.net	secondary.ipsec.akatp.net	Up
DASLAB-RackM-US-1	INET1	Primary-POP	Secondary-POP	EdgeConnect:Store-64201@ipsec.akatp.net	primary.ipsec.akatp.net	secondary.ipsec.akatp.net	Up
Store101-EC2	INET1	Primary-POP	Secondary-POP	EdgeConnect:Store-64201@ipsec.akatp.net	primary.ipsec.akatp.net	secondary.ipsec.akatp.net	Up
Store101-EC1	INET2	Primary-POP	Secondary-POP	EdgeConnect:Store-64201@ipsec.akatp.net	primary.ipsec.akatp.net	secondary.ipsec.akatp.net	Up
DASLAB-RackM-US-1	INET2	Primary-POP	Secondary-POP	EdgeConnect:Store-64201@ipsec.akatp.net	primary.ipsec.akatp.net	secondary.ipsec.akatp.net	Up
Andover-DASLAB-DC	INET1	Primary-POP	Secondary-POP	EdgeConnect:Store-64201@ipsec.akatp.net	primary.ipsec.akatp.net	secondary.ipsec.akatp.net	Up
Store101-EC1	INET1	Primary-POP	Secondary-POP	EdgeConnect:Store-64201@ipsec.akatp.net	primary.ipsec.akatp.net	secondary.ipsec.akatp.net	Up
Store101-EC1	INET2	Primary-POP	Secondary-POP	EdgeConnect:Store-64201@ipsec.akatp.net	primary.ipsec.akatp.net	secondary.ipsec.akatp.net	Up

## Passthrough Tunnel Status

On the Akamai Service Orchestration tab, click **Tunnels**. The Tunnels tab of the Orchestrator opens, allowing you to view the IPsec tunnel status of the appliances:



Service Orchestration Business Intent Overlays **Tunnels** X

Tunnel Exception Export Sites C

Tunnels 0 Search filter is auto populated with this string to show only Akamai Passthrough tunnels Search ThirdParty\_AKA

22/62 Rows

Edt	Appliance	Segment	Passthrough Tunnel	A...	Charts	Status	Local IP	Remote IP	Mode	NAT	Peer/Service	Max BW Kbps	Advanced Options
✓	Andover-DASLAB-DC	Default	ThirdParty_AKA_Primary-POP_INET1_Primary_2	up	📊	up - active	16.143.16.42	23.215.105.130	IPSec	none	AKA_Primary_2	50000(Auto)	ⓘ
✓	Andover-DASLAB-DC	Default	ThirdParty_AKA_Primary-POP_INET1_Primary_1	up	📊	up - active	16.143.16.42	23.49.56.172	IPSec	none	AKA_Primary_1	50000(Auto)	ⓘ
✓	DASLAB-Rack94-US-1	Default	ThirdParty_AKA_Primary-POP_INET1_Primary_1	up	📊	up - active	172.16.50.115	23.215.105.130	IPSec	none	AKA_Primary_1	20000(Auto)	ⓘ
✓	DASLAB-Rack94-US-1	Default	ThirdParty_AKA_Primary-POP_INET1_Primary_2	up	📊	up - active	172.16.50.115	23.215.105.130	IPSec	none	AKA_Primary_2	20000(Auto)	ⓘ
✓	DASLAB-Rack99-S-1	Default	ThirdParty_AKA_Primary-POP_INET1_Primary_1	up	📊	up - active	172.16.50.106	23.215.105.130	IPSec	none	AKA_Primary_1	10000(Auto)	ⓘ
✓	DASLAB-Rack99-S-1	Default	ThirdParty_AKA_Primary-POP_INET1_Primary_2	up	📊	up - active	172.16.50.106	23.49.56.172	IPSec	none	AKA_Primary_2	10000(Auto)	ⓘ
✓	RKAW5-East-EC01	Default	ThirdParty_AKA_Primary-POP_INET1_Primary_1	up	📊	up - active	172.20.36.30	104.114.78.183	IPSec	none	AKA_Primary_1	5000(Auto)	ⓘ
✓	RKAW5-East-EC01	Default	ThirdParty_AKA_Primary-POP_INET1_Primary_2	up	📊	up - active	172.20.36.30	23.215.105.130	IPSec	none	AKA_Primary_2	5000(Auto)	ⓘ
✓	RKAW5-East-EC02	Default	ThirdParty_AKA_Primary-POP_INET1_Primary_1	up	📊	up - active	172.20.36.70	104.114.78.183	IPSec	none	AKA_Primary_1	5000(Auto)	ⓘ
✓	RKAW5-East-EC02	Default	ThirdParty_AKA_Primary-POP_INET1_Primary_2	up	📊	up - active	172.20.36.70	23.215.105.130	IPSec	none	AKA_Primary_2	5000(Auto)	ⓘ
✓	RKAW5-West-EC01	Default	ThirdParty_AKA_Primary-POP_INET1_Primary_1	up	📊	up - active	172.20.32.25	104.114.78.183	IPSec	none	AKA_Primary_1	2000(Auto)	ⓘ
✓	RKAW5-West-EC01	Default	ThirdParty_AKA_Primary-POP_INET1_Primary_2	up	📊	up - active	172.20.32.25	23.215.105.130	IPSec	none	AKA_Primary_2	2000(Auto)	ⓘ
✓	RKAW5-West-EC02	Default	ThirdParty_AKA_Primary-POP_INET1_Primary_1	up	📊	up - active	172.20.32.105	104.114.78.183	IPSec	none	AKA_Primary_1	2000(Auto)	ⓘ
✓	RKAW5-West-EC02	Default	ThirdParty_AKA_Primary-POP_INET1_Primary_2	up	📊	up - active	172.20.32.105	23.215.105.130	IPSec	none	AKA_Primary_2	2000(Auto)	ⓘ
✓	Store101-EC1	Default	ThirdParty_AKA_Primary-POP_INET1_Primary_1	up	📊	up - active	169.254.1.17	23.49.56.172	IPSec	none	AKA_Primary_1	20000(Auto)	ⓘ
✓	Store101-EC1	Default	ThirdParty_AKA_Primary-POP_INET1_Primary_2	up	📊	up - active	16.143.16.43	23.49.56.172	IPSec	none	AKA_Primary_2	40000(Auto)	ⓘ
✓	Store101-EC1	Default	ThirdParty_AKA_Primary-POP_INET1_Primary_1	up	📊	up - active	16.143.16.43	23.215.105.130	IPSec	none	AKA_Primary_1	20000(Auto)	ⓘ
✓	Store101-EC1	Default	ThirdParty_AKA_Primary-POP_INET1_Primary_2	up	📊	up - active	169.254.1.17	23.215.105.130	IPSec	none	AKA_Primary_2	20000(Auto)	ⓘ
✓	Store101-EC2	Default	ThirdParty_AKA_Primary-POP_INET1_Primary_1	up	📊	up - active	169.254.1.13	23.49.56.172	IPSec	none	AKA_Primary_1	40000(Auto)	ⓘ
✓	Store101-EC2	Default	ThirdParty_AKA_Primary-POP_INET1_Primary_2	up	📊	up - active	16.143.16.44	23.215.105.130	IPSec	none	AKA_Primary_2	20000(Auto)	ⓘ
✓	Store101-EC2	Default	ThirdParty_AKA_Primary-POP_INET1_Primary_1	up	📊	up - active	16.143.16.44	23.49.56.172	IPSec	none	AKA_Primary_1	20000(Auto)	ⓘ

## IP SLA Status

On the Akamai Service Orchestration tab, click **IP SLA**. The IP SLA tab of the Orchestrator opens, allowing you to verify tunnel health using IP SLA probes:



Service Orchestration Business Intent Overlays Tunnels **IP SLA** X

Export C

IP SLA 0 Search filter auto populated to display IP SLA for Akamai Tunnels Search ThirdParty\_AKA

20/78 Rows

Edt	Appliance	Active	State	Monitor	Down Action	Up Action	Comment	Up State	Down State
✓	Andover-DASLAB-DC	Yes	Up	HTTP/HTTPS: Keep Alive Time = 5, URL = sp-ipsla.silverpeak.cloud:8.8.8.8.8.4.4, HTTP Request Timeout = 2, Up Thresh: Tunnel Down: Tunnel = ThirdParty_AKA_Primary-POP_INET1	Tunnel Up: Tunnel = ThirdParty_AKA_Primary-POP_INET1	generated by overlay manager	Last:10m 31s	Total 0, Last:0	
✓	Andover-DASLAB-DC	Yes	Up	HTTP/HTTPS: Keep Alive Time = 5, URL = sp-ipsla.silverpeak.cloud:8.8.8.8.8.4.4, HTTP Request Timeout = 2, Up Thresh: Tunnel Down: Tunnel = ThirdParty_AKA_Primary-POP_INET1	Tunnel Up: Tunnel = ThirdParty_AKA_Primary-POP_INET1	generated by overlay manager	Last:10m 31s	Total 0, Last:0	
✓	DASLAB-Rack94-US-1	Yes	Up	HTTP/HTTPS: Keep Alive Time = 5, URL = sp-ipsla.silverpeak.cloud:8.8.8.8.8.4.4, HTTP Request Timeout = 2, Up Thresh: Tunnel Down: Tunnel = ThirdParty_AKA_Primary-POP_INET1	Tunnel Up: Tunnel = ThirdParty_AKA_Primary-POP_INET1	generated by overlay manager	Last:11m 07s	Total 0, Last:0	
✓	DASLAB-Rack94-US-1	Yes	Up	HTTP/HTTPS: Keep Alive Time = 5, URL = sp-ipsla.silverpeak.cloud:8.8.8.8.8.4.4, HTTP Request Timeout = 2, Up Thresh: Tunnel Down: Tunnel = ThirdParty_AKA_Primary-POP_INET1	Tunnel Up: Tunnel = ThirdParty_AKA_Primary-POP_INET1	generated by overlay manager	Last:11m 0s	Total 0, Last:0	
✓	RKAW5-East-EC01	Yes	Up	HTTP/HTTPS: Keep Alive Time = 5, URL = sp-ipsla.silverpeak.cloud:8.8.8.8.8.4.4, HTTP Request Timeout = 2, Up Thresh: Tunnel Down: Tunnel = ThirdParty_AKA_Primary-POP_INET1	Tunnel Up: Tunnel = ThirdParty_AKA_Primary-POP_INET1	generated by overlay manager	Last:10m 42s	Total 0, Last:0	
✓	RKAW5-East-EC01	Yes	Up	HTTP/HTTPS: Keep Alive Time = 5, URL = sp-ipsla.silverpeak.cloud:8.8.8.8.8.4.4, HTTP Request Timeout = 2, Up Thresh: Tunnel Down: Tunnel = ThirdParty_AKA_Primary-POP_INET1	Tunnel Up: Tunnel = ThirdParty_AKA_Primary-POP_INET1	generated by overlay manager	Last:10m 32s	Total 0, Last:0	
✓	RKAW5-East-EC02	Yes	Up	HTTP/HTTPS: Keep Alive Time = 5, URL = sp-ipsla.silverpeak.cloud:8.8.8.8.8.4.4, HTTP Request Timeout = 2, Up Thresh: Tunnel Down: Tunnel = ThirdParty_AKA_Primary-POP_INET1	Tunnel Up: Tunnel = ThirdParty_AKA_Primary-POP_INET1	generated by overlay manager	Last:10m 32s	Total 0, Last:0	
✓	RKAW5-East-EC02	Yes	Up	HTTP/HTTPS: Keep Alive Time = 5, URL = sp-ipsla.silverpeak.cloud:8.8.8.8.8.4.4, HTTP Request Timeout = 2, Up Thresh: Tunnel Down: Tunnel = ThirdParty_AKA_Primary-POP_INET1	Tunnel Up: Tunnel = ThirdParty_AKA_Primary-POP_INET1	generated by overlay manager	Last:10m 33s	Total 0, Last:0	
✓	RKAW5-West-EC01	Yes	Up	HTTP/HTTPS: Keep Alive Time = 5, URL = sp-ipsla.silverpeak.cloud:8.8.8.8.8.4.4, HTTP Request Timeout = 2, Up Thresh: Tunnel Down: Tunnel = ThirdParty_AKA_Primary-POP_INET1	Tunnel Up: Tunnel = ThirdParty_AKA_Primary-POP_INET1	generated by overlay manager	Last:10m 53s	Total 0, Last:0	
✓	RKAW5-West-EC01	Yes	Up	HTTP/HTTPS: Keep Alive Time = 5, URL = sp-ipsla.silverpeak.cloud:8.8.8.8.8.4.4, HTTP Request Timeout = 2, Up Thresh: Tunnel Down: Tunnel = ThirdParty_AKA_Primary-POP_INET1	Tunnel Up: Tunnel = ThirdParty_AKA_Primary-POP_INET1	generated by overlay manager	Last:10m 53s	Total 0, Last:0	
✓	RKAW5-West-EC02	Yes	Up	HTTP/HTTPS: Keep Alive Time = 5, URL = sp-ipsla.silverpeak.cloud:8.8.8.8.8.4.4, HTTP Request Timeout = 2, Up Thresh: Tunnel Down: Tunnel = ThirdParty_AKA_Primary-POP_INET1	Tunnel Up: Tunnel = ThirdParty_AKA_Primary-POP_INET1	generated by overlay manager	Last:10m 53s	Total 0, Last:0	
✓	RKAW5-West-EC02	Yes	Up	HTTP/HTTPS: Keep Alive Time = 5, URL = sp-ipsla.silverpeak.cloud:8.8.8.8.8.4.4, HTTP Request Timeout = 2, Up Thresh: Tunnel Down: Tunnel = ThirdParty_AKA_Primary-POP_INET1	Tunnel Up: Tunnel = ThirdParty_AKA_Primary-POP_INET1	generated by overlay manager	Last:10m 53s	Total 0, Last:0	
✓	Store101-EC1	Yes	Up	HTTP/HTTPS: Keep Alive Time = 5, URL = sp-ipsla.silverpeak.cloud:8.8.8.8.8.4.4, HTTP Request Timeout = 2, Up Thresh: Tunnel Down: Tunnel = ThirdParty_AKA_Primary-POP_INET1	Tunnel Up: Tunnel = ThirdParty_AKA_Primary-POP_INET1	generated by overlay manager	Last:10m 50s	Total 0, Last:0	
✓	Store101-EC1	Yes	Up	HTTP/HTTPS: Keep Alive Time = 5, URL = sp-ipsla.silverpeak.cloud:8.8.8.8.8.4.4, HTTP Request Timeout = 2, Up Thresh: Tunnel Down: Tunnel = ThirdParty_AKA_Primary-POP_INET1	Tunnel Up: Tunnel = ThirdParty_AKA_Primary-POP_INET1	generated by overlay manager	Last:10m 50s	Total 0, Last:0	
✓	Store101-EC1	Yes	Up	HTTP/HTTPS: Keep Alive Time = 5, URL = sp-ipsla.silverpeak.cloud:8.8.8.8.8.4.4, HTTP Request Timeout = 2, Up Thresh: Tunnel Down: Tunnel = ThirdParty_AKA_Primary-POP_INET1	Tunnel Up: Tunnel = ThirdParty_AKA_Primary-POP_INET1	generated by overlay manager	Last:10m 52s	Total 0, Last:0	
✓	Store101-EC2	Yes	Up	HTTP/HTTPS: Keep Alive Time = 5, URL = sp-ipsla.silverpeak.cloud:8.8.8.8.8.4.4, HTTP Request Timeout = 2, Up Thresh: Tunnel Down: Tunnel = ThirdParty_AKA_Primary-POP_INET1	Tunnel Up: Tunnel = ThirdParty_AKA_Primary-POP_INET1	generated by overlay manager	Last:10m 52s	Total 0, Last:0	
✓	Store101-EC2	Yes	Up	HTTP/HTTPS: Keep Alive Time = 5, URL = sp-ipsla.silverpeak.cloud:8.8.8.8.8.4.4, HTTP Request Timeout = 2, Up Thresh: Tunnel Down: Tunnel = ThirdParty_AKA_Primary-POP_INET1	Tunnel Up: Tunnel = ThirdParty_AKA_Primary-POP_INET1	generated by overlay manager	Last:10m 51s	Total 0, Last:0	
✓	Store101-EC2	Yes	Up	HTTP/HTTPS: Keep Alive Time = 5, URL = sp-ipsla.silverpeak.cloud:8.8.8.8.8.4.4, HTTP Request Timeout = 2, Up Thresh: Tunnel Down: Tunnel = ThirdParty_AKA_Primary-POP_INET1	Tunnel Up: Tunnel = ThirdParty_AKA_Primary-POP_INET1	generated by overlay manager	Last:10m 51s	Total 0, Last:0	

## VERIFY ACTIVE FLOWS ON THE EDGECONNECT SD-WAN

This section explains how to validate whether internet traffic is being redirected on the Akami service tunnels by checking the flows on the EdgeConnect SD-WAN appliances.

1. Navigate to **Monitoring > Flows > Active & Recent Flows**.
2. Filter based on IP or port number.

The example below has filtered traffic for a PC with an IP address 172.23.21.30. The traffic matches the CASB overlay, and inbound and outbound tunnels show as “AKA\_Primary-POP\_INET1.” This confirms that the traffic is being redirected to the Akamai service tunnel properly and the user has successful inbound and outbound connections through the Akamai service tunnels.

Appliance	Detail	Start Time	Uptime	Overlay	Protocol	Application	Source Role	IP1	Port1	IP2	Port2	Inb.	Out.	Inbound Tunnel	Outbound Tunnel
DAQLAB-RackM-UG-1		19:43:43	1m 7s	CASB	tcp	Office365CommonDefault	unknown	172.23.21.30	54585	array603.prod.do.dsp.mp.mico.	443			ThirdParty_AKA_Primary-POP_INET1_Primary_1	ThirdParty_AKA_Primary-POP_INET1_Primary_1
DAQLAB-RackM-UG-1		19:44:00	50s	CASB	tcp	Https	unknown	172.23.21.30	54590	mozilla.cloudflare-dns.com [104.	443			ThirdParty_AKA_Primary-POP_INET1_Primary_1	ThirdParty_AKA_Primary-POP_INET1_Primary_1
DAQLAB-RackM-UG-1		19:44:24	26s	CASB	tcp	Office365Common	unknown	172.23.21.30	54596	login.live.com (40.126.26.135)	443			ThirdParty_AKA_Primary-POP_INET1_Primary_1	ThirdParty_AKA_Primary-POP_INET1_Primary_1