

ARISTA

Configuration Guide

Arista VeloCloud SD-WAN SSE for Symantec

Services



Headquarters	Support	Sales
5453 Great America Parkway Santa Clara, CA 95054 USA +1-408-547-5500	+1-408-547-5502 +1-866-476-0000	+1-408-547-5501 +1-866-497-0000
www.arista.com/en/	support@arista.com	sales@arista.com

© Copyright 2026 Arista Networks, Inc. All rights reserved. The information contained herein is subject to change without notice. The trademarks, logos, and service marks ("Marks") displayed in this documentation are the property of Arista Networks in the United States and other countries. Use of the Marks is subject to the Arista Networks Terms of Use Policy, available at www.arista.com/en/terms-of-use. Use of marks belonging to other parties is for informational purposes only.

Contents

Chapter 1: Configure SSE for Symantec.....	1
Chapter 2: Configure Symantec API Credentials.....	7
Chapter 3: Symantec WSS PoP to PoP Integration.....	10
Chapter 4: Security Service Edge (SSE).....	15
Appendix A: References.....	18
A.1 Related Documents.....	18

Configure SSE for Symantec

The VeloCloud SD-WAN offers an automated workflow to integrate SD-WAN enabled branch locations to Symantec SSE.

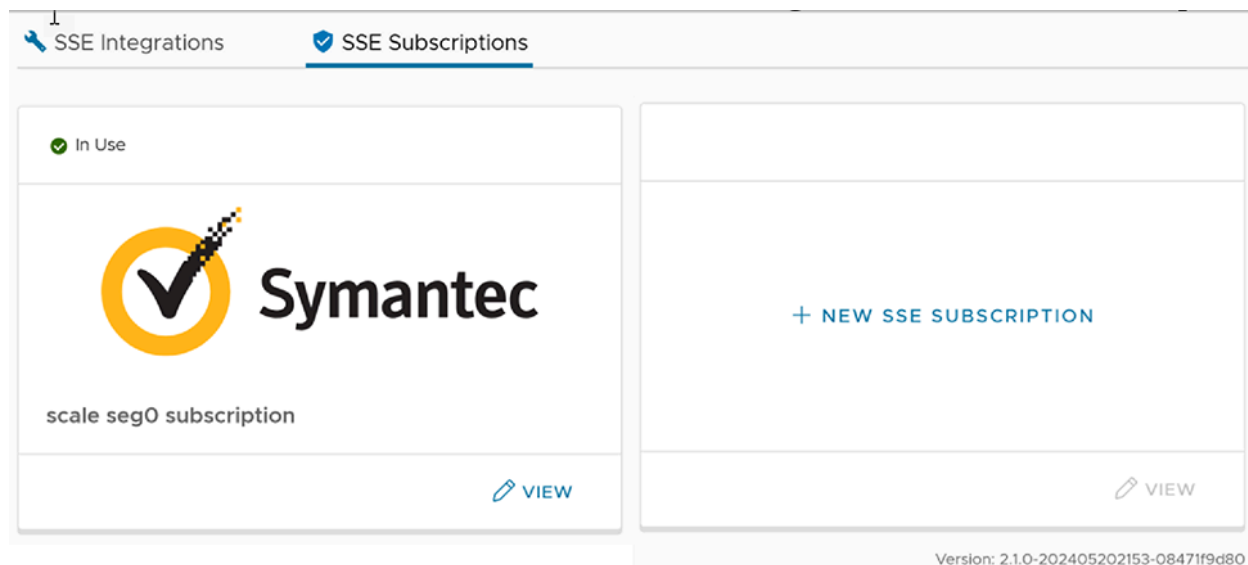
Prerequisites

- For the **Symantec** integration, the Enterprise user must first create username and password for an API credential configured in the **Symantec Cloud** portal. For more information, see [Configure Symantec API Credentials](#).
- To trigger the Symantec Web Security Service (WSS) automation, see [Symantec WSS PoP to PoP Integration](#).

Follow the below procedure to configure **SSE Subscription** and **SSE Integration** for **Symantec**:

1. In the **SD-WAN** service of the Enterprise portal, navigate to **Configure > Security Service Edge (SSE)**.
2. Click the **SSE Subscriptions** tab on the **Security Service Edge (SSE)** screen.


Figure 1-1: SSE Subscriptions for Symantec




3. On each tile, click **View** to view the existing subscription details.
4. Click the vertical ellipsis, and then click **Delete** to delete a subscription.

- To create a new subscription, click **+ New SSE Subscription**. The following **Configure SSE Subscription** window appears on selecting the **Subscription Type** as **Symantec**:

Figure 1-2: Configure a new SSE Subscription for Symantec

 **Note:** The fields displayed on the screen vary depending on the selected **Subscription Type**.

- Configure the following options:

Option	Description
User Name	Enter the API username as configured in the Symantec Cloud portal.
Password	Enter the API password as configured in the Symantec Cloud portal. <div data-bbox="906 1417 1510 1564" style="border: 1px solid #ccc; padding: 5px;"> <p> Note: Starting from the 4.5 release, the use of the special character "<" in the password is no longer supported. In cases where users have already used "<" in their passwords in previous releases, they must remove it to save any changes on the page.</p> </div>
Tenant ID	Enter the Tenant ID associated with the Enterprise. This field is optional and is blank, by default.
Expiry	To set an expiry for the credentials, click the toggle button. The Expiry Date field appears. Click the calendar to set the expiry date and time. This field is optional and is blank, by default.

- Click **Validate Subscription** to make sure that the entered credentials are correct. A message is displayed.

- If the entered credentials are correct, click **Save** to save the configured subscription.
 - If the entered credentials are incorrect, you must re-enter correct values and click **Validate Subscription** again.
8. Click **Save** to save the configured subscription.
 9. After creating an SSE Subscription, you can proceed to create an SSE Integration.
 10. Navigate to **Configure > Security Service Edge (SSE)**. By default, the **SSE Integrations** tab is displayed.

Figure 1-3: SSE Integrations for Symantec

The screenshot shows the 'Security Service Edge (SSE) Automated Configuration' page. The left sidebar lists navigation options: Monitor, Configure (selected), Diagnostics, and Service Settings. Under 'Configure', there is a sub-menu for 'Edge Configuration' with options: Edges, Profiles, Object Groups, Segments, Overlay Flow Control, Network Services, and Security Service Edge (SS...). The main content area has a title 'Security Service Edge (SSE) Automated Configuration' and a note: 'This is only for SSE automation configuration. For manual configuration, please go to Network Services.' Below this, there are tabs for 'SSE Integrations' (selected) and 'SSE Subscriptions'. A '+ NEW SSE INTEGRATION' button is visible. A table lists existing integrations:

	Name	SSE Vendor	Used By	Tunnel Deployment Status	Created
<input type="checkbox"/>	symantec-prod-1	Broadcom - Symantec	0 Selected 0 Configured	View	Nov 8, 2023
<input type="checkbox"/>	prisma	Palo Alto - Prisma Access	0 Selected 0 Configured	View	Nov 8, 2023

At the bottom of the table, there are 'COLUMNS' and 'REFRESH' buttons, and a footer indicating 'Integrations per Page 10' and '1 - 2 of 2 Integrations'.

11. To create a new SSE integration, click **+ New SSE Integration**.

Figure 1-4: Configure a new SSE Integration for Symantec

The screenshot shows the 'Configure a New SSE Integration' wizard. The title is 'Configure a New SSE Integration' and the subtitle is 'Follow the steps below to build tunnels from Edges in the VMware Cloud Orchestrator to the selected Cloud Vendor.' The wizard is currently on step 1: 'Choose Cloud Subscription'. The 'Symantec' vendor is selected. The form fields are:



- Subscription Type:** Symantec
- Cloud Subscription:** Choose Cloud Subscription
- Integration Type:** Via Edge (radio button), PoP to PoP (radio button, selected)

A 'NEXT STEP' button is visible. Below the form, the next steps are listed: '2. Create Network Service' and '3. Select Profile/Edges' (with a 'Not Applicable' label).




Note: The fields displayed on the screen vary depending on the selected **Subscription Type**.

12. Under **Choose Cloud Subscription** section, configure the following options:

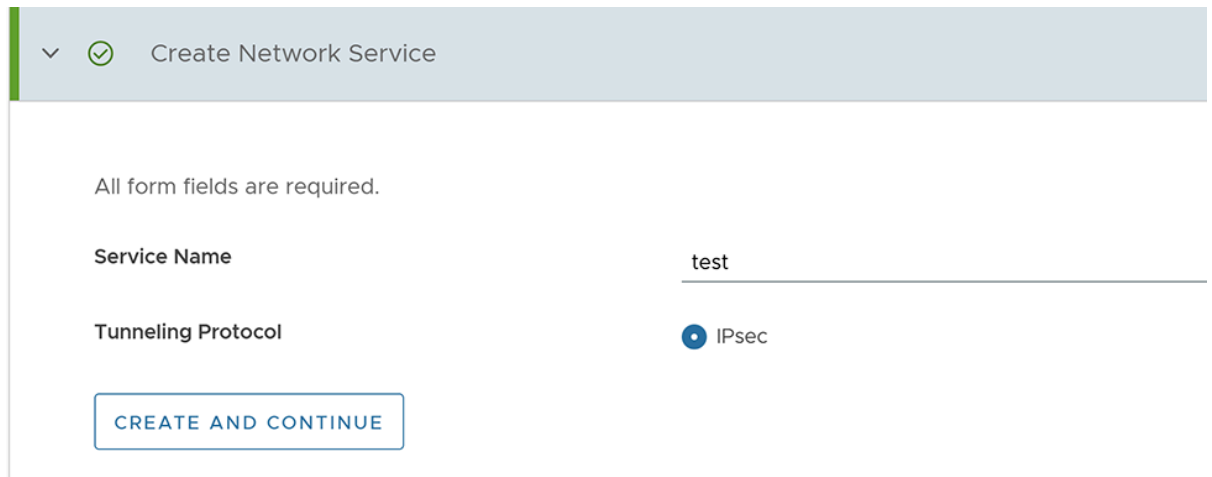
Option	Description
Subscription Type	<p>Select a subscription type for which you want to set up an SSE integration. The available options are:</p> <ul style="list-style-type: none"> • Prisma Access • Symantec
Cloud Subscription	<p>Select a cloud subscription from the drop-down menu. Only those cloud subscriptions that are configured under the SSE vendor selected in Subscription Type, appear in the drop-down menu.</p> <p>These cloud subscriptions are populated based on the configurations under Configure > Security Service Edge (SSE) > SSE Subscriptions.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> Note: This field appears only when you select a subscription type.</p> </div>
Integration Type	<p>Select either one of the following options:</p> <ul style="list-style-type: none"> • Via Edge: Tunnel is established from Edge to Symantec. • PoP to PoP: Geneve tunnel is established from a VeloCloud Gateway to Symantec WSS. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> Note: This field is available only for the Symantec subscription type, and it is introduced in the release 6.1.1. For more information, see Symantec WSS PoP to PoP Integration .</p> </div>

13. Click **Next Step** to activate the **Create Network Service** section.

 **Note:** The fields displayed on the screen vary depending on the selected **Integration Type**.

a. When you select the **Integration Type** as **Via Edge**, the following screen appears:

Figure 1-5: Create Network Service - Via Edge



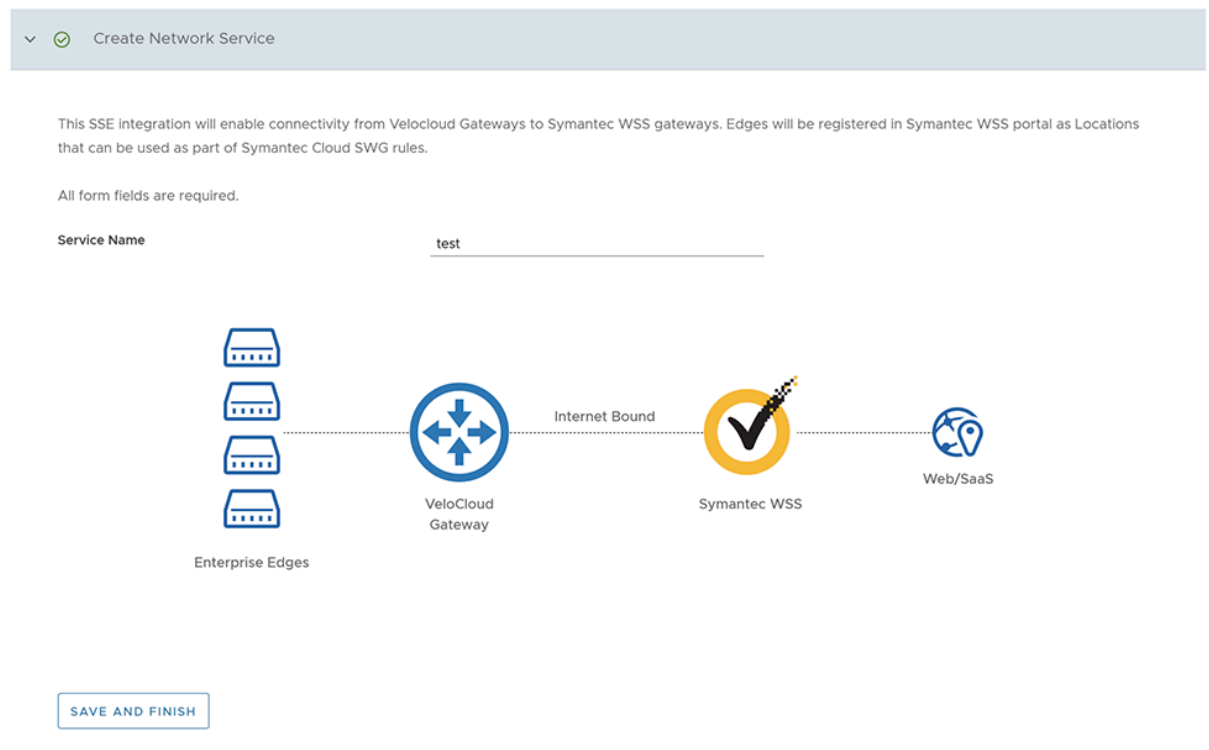
The screenshot shows a web interface for creating a network service. At the top, there is a header with a dropdown arrow, a checkmark icon, and the text "Create Network Service". Below the header, a message states "All form fields are required." There are two input fields: "Service Name" with the value "test" and "Tunneling Protocol" with a radio button selected for "IPsec". At the bottom, there is a button labeled "CREATE AND CONTINUE".

Option	Description
Service Name	Enter a unique service name.
Tunneling Protocol	This field is set to IPsec , which is the only supported protocol.

Click **Create and Continue**. The **Select Profile/Edges** section appears. See step 14.

b. When you select the **Integration Type** as **PoP to PoP**, the following screen appears:

Figure 1-6: Create Network Service - PoP to PoP



Enter a unique **Service Name**, and then click **Save and Finish**.

14. Configure the following in the **Select Profile/Edges** section.

Option	Description
Select Profile	Select an SD-WAN Edge Profile from the drop-down menu.
Select Segment	Select a Segment from the drop-down menu. By default, Global Segment is selected. <div style="border: 1px solid #ccc; padding: 5px; background-color: #e6f2ff;"> <p>Note: You can select multiple Segments for Symantec subscription.</p> </div>
Edges	Once you select Profile and Segment, a list of Edges associated with the selected Profile gets auto-populated. Select one or more Edges for which you wish to apply the SSE integration.
Selected WAN Links	If an Edge has more than two WAN links, the first two WAN links are auto-populated in the table. You can select the WAN links that you wish to use for the automation.
Edge Location	Displays the location of the Edge.
Datacenter Location	Displays the location of the Datacenter.



Note: The **Select Profile/Edges** section is not applicable for the **PoP to PoP** integration type. You must configure the Profile by navigating to **Configure > Profiles**.

15. Click **Save and Finish.**

The newly created SSE integration appears on the list on the **Security Service Edge (SSE)** screen.

Configure Symantec API Credentials

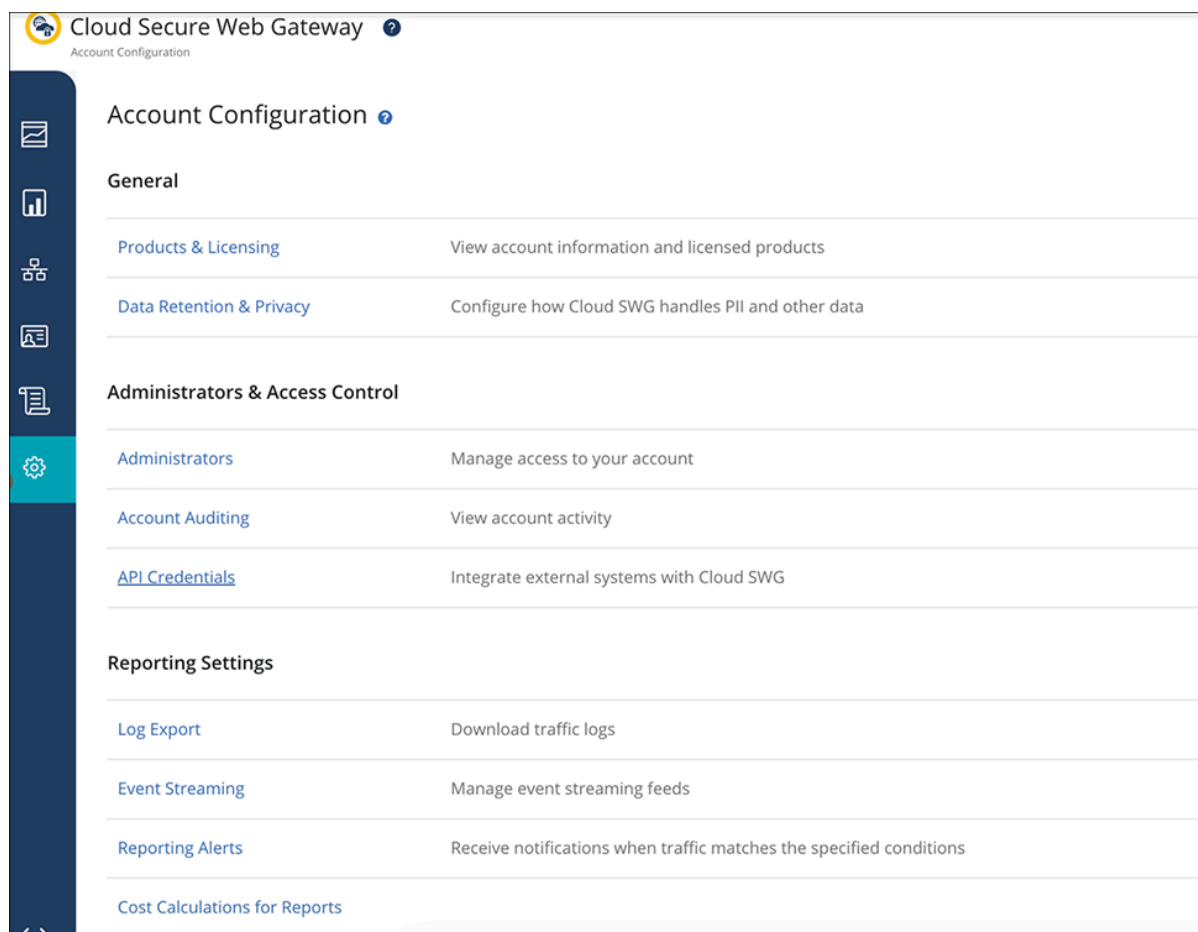
Before configuring the Security Service Edge (SSE) automation, you must first configure API credentials on the Symantec Cloud portal, which must be then used on the Orchestrator subscription screen.

Follow the below steps to configure Symantec API credentials:

1. Log into the **Symantec Cloud** portal, and then click **Account Configuration**.

The **Account Configuration** screen appears:

Figure 2-1: Account Configuration



2. Under the **Administrators & Access Control** section, click **API Credentials**, and then click the **Add** button. The following window appears:

Figure 2-2: Add API Credentials

Add ⓘ

Create API Credentials to integrate external systems with the Cloud SWG.

Access: * Reporting Access Logs ⓘ
 Location Management ⓘ
 Audit Logs ⓘ
 Agent Config Management ⓘ
 Dedicated IPs ⓘ
 Policy List Management ⓘ

Username: ⓘ



Password: ⓘ

Expiry:

Comments:
255 of 255 characters left

ⓘ Once saved, the token cannot be displayed again. Ensure that you have a copy.

3. Configure the following options:

Option	Description
Username	This field is auto-generated and cannot be edited.
Password	This field is auto-generated and cannot be edited.
Expiry	To set an expiry for the entered credentials, select Time-based , and then select the date and time as required.
Reporting Access Logs	<p>Select this check box to allow the user to download or sync the Access Logs from Cloud SWG to Reporter or a third party SIEM.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  Note: Selecting this check box is mandatory. </div>
Location Management	<p>Select this check box to allow the user to create or update locations. This is useful when the external IP address of a location changes.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  Note: Selecting this check box is mandatory. </div>
Audit Logs	Select this check box to allow the user to download the audit logs and retain the data post expiry.
Agent Config Management	Select this check box to allow the user to create or update agent configuration.
Dedicated IPs	Select this check box to allow dedicated IP management.
Policy List Management	Select this check box to allow access to the REST API for Policy List Management.
Comments	Enter your comments if any. This field is not mandatory.



Note: Make sure to copy the entered **Username** and **Password**. You must use these credentials for the Symantec SSE automation.

4. Click **Save**.

You may now log into the Orchestrator to configure the Security Service Edge (SSE) and initiate the automation. For more information, see the topic [Security Service Edge \(SSE\)](#).

Symantec WSS PoP to PoP Integration

Starting with the 6.1.0 release, VeloCloud SD-WAN introduces the Symantec Web Security Service (WSS) PoP to PoP integration, which supports pre-provisioned Geneve tunnels from VeloCloud Gateways (VCG) to Symantec WSS Gateways in GCP. With pre-provisioned Geneve tunnels, SD-WAN customers who have a Symantec SSE subscription need not configure and setup IPsec tunnels from the Edge or Gateway for their tenant. They can use the pre-provisioned connectivity between VeloCloud Gateway to WSS to carry their network traffic. This is inspected by Symantec SSE via a Business Policy.

Only an Operator user can activate this feature by navigating to **Gateway Management > Gateways**. For more information, see the topic *Configure Gateways* in the *Arista VeloCloud SD-WAN Operator Guide*.

To perform **Symantec WSS PoP to PoP Integration**, follow the below workflow:

- [Configure Symantec API Credentials](#)
- Configure SSE Subscription
- Configure SSE Integration
- Create a Business Policy
- Monitor SSE Integration

See [Configure SSE for Symantec](#) for information on configuring SSE Subscription and SSE Integration for Symantec.

After you have created the SSE Symantec integration using PoP to PoP, you can view the deployment status on the **Security Service Edge (SSE) Automated Configuration** screen, by clicking the **View** link in the **Tunnel Deployment Status** column.

Figure 3-1: Tunnel Deployment Status

Non SD-WAN Destinations Deployment Status for test12

0 Enqueued
0 Pending
0 In-Progress
1 Completed
0 Failed
0 Timed Out
0 Pending Delete

Edge

e2e-p2p-vce

API Details for Edge: e2e-p2p-vce

Index	Command	HTTP Status Code	Status	Details
1	createWssLocation	0	STARTED	Details
2	POST /locations	200	COMPLETE	Details

Show Or Hide Columns REFRESH 2 items

DONE

1. Create a Business Policy

- a. Navigate to **Configure > Profiles > Business Policy**.
- b. Click **Add**.

The following window appears:

Figure 3-2: Add Rule - Match tab

The screenshot shows the 'Add Rule' window with the 'Match' tab selected. The 'Rule Name' field contains 'WSS'. Under 'IP Version', 'IPv4' is selected. The 'Source' field is set to 'Any'. The 'Destination' field is also set to 'Any', and its dropdown menu is open, showing 'Internet' as the selected option. The 'Application' field is empty. At the bottom right, there are 'CANCEL' and 'CREATE' buttons. The bottom of the window shows a dark navigation bar with 'Remote Desktop' and 'Multi-Path' options.

- c. Enter the **Rule Name** and select the **IP Version** as **IPv4**.



Note: For Symantec WSS integration, only **IPv4** is supported.

- d. Under the **Match** tab, select **Destination** as **Internet**.

- e. Under the **Action** tab, select the **Network Service** as **Internet Backhaul > Symantec WSS Gateway**.

Figure 3-3: Add Rule - Action tab

The screenshot shows the 'Add Rule' configuration page with the following settings:

- Rule Name ***: wss
- IP Version ***: IPv4 IPv6 IPv4 and IPv6
- Match** / **Action** (selected)
- Priority**: High Normal Low
- Enable Rate Limit**:
- Network Service**: Internet Backhaul > Symantec WSS Gateway
- Symantec WSS Integration ***: test12
- Link Steering** ⓘ: Auto
- Inner Packet DSCP Tag**: Leave as is
- Outer Packet DSCP Tag**: 0 - CS0/DF
- Enable NAT**: ⓘ
- Service Class**: Realtime Transactional Bulk

Buttons: CANCEL, CREATE

- f. On selecting **Symantec WSS Gateway**, the field **Symantec WSS Integration** appears. The drop-down menu lists the SSE integrations configured for WSS. Select an SSE integration to use.
- g. Configure all the other fields, and then click **Create**. For more information on these fields, see the topic *Create Business Policy Rule* in the *Arista VeloCloud SD-WAN Administration Guide*.

Note:



- For Symantec WSS integration, the business policy can only be configured at Profile level and not Edge level.
- Ensure that **Cloud VPN** is activated for the selected Profile.

2. Monitor SSE Integration

- a. Navigate to **Monitor > Security Service Edge**, to monitor the Symantec WSS PoP integration status.

Figure 3-4: Monitor SSE Integration

Monitor | Configure | Diagnostics | Service Settings

Security Service Edge (SSE)

This is only for Symantec PoP-to-PoP connectivity.

Integration	WSS Enabled Gateway(s)	WSS Endpoint	Profiles Using WSS	Locations	Last Updated
test12	(1) Connected e2e-gcp-gateway-1	(1) Connected gusdpcim.gm/internal.threat...	1	1	Aug 22, 2024

Show Or Hide Columns | REFRESH | Integrations per Page: 10 | 1-1 of 1 Integrations

- b. Expand the integration name to view the following details:

- Number of connected Gateways
- WSS Endpoint details
- Number of Profiles using this integration
- Number of locations associated
- Last updated date

Security Service Edge (SSE)

Starting from the 5.4.0 release, VeloCloud SD-WAN supports the Security Service Edge (SSE) feature. This feature allows VeloCloud SD-WAN to easily integrate with a third party SSE vendor using seamless automation through the Orchestrator. You can configure multiple SSE integrations with the same vendor.

Enterprise users can now configure **Non SD-WAN Destinations via Edge** and **Cloud Subscription** through the **Security Service Edge (SSE)** feature. For manual configuration of network services, see the *VeloCloud SD-WAN Administration Guide - Configure Network Services*.



Note: Currently, only **Non SD-WAN Destination via Edge** network service is supported.

To access the SSE feature, navigate to **Configure > Security Service Edge (SSE)**. By default, the **SSE Integrations** tab is displayed. Before creating an **SSE Integration**, you must first create an **SSE Subscription**.

For an Enterprise user, the **Security Service Edge (SSE)** feature is activated by default. This feature currently supports **PAN Prisma** and **Symantec** configurations.

For more information, please refer to the following topics:

- [SSE for Pan Prisma Configuration Guide](#)
- [Configure SSE for Symantec](#)

If you wish to edit the existing SSE integration, select the SSE integration from the list on the **Security Service Edge (SSE)** screen, and then click **Edit**. You can also click the SSE integration name link to edit it.

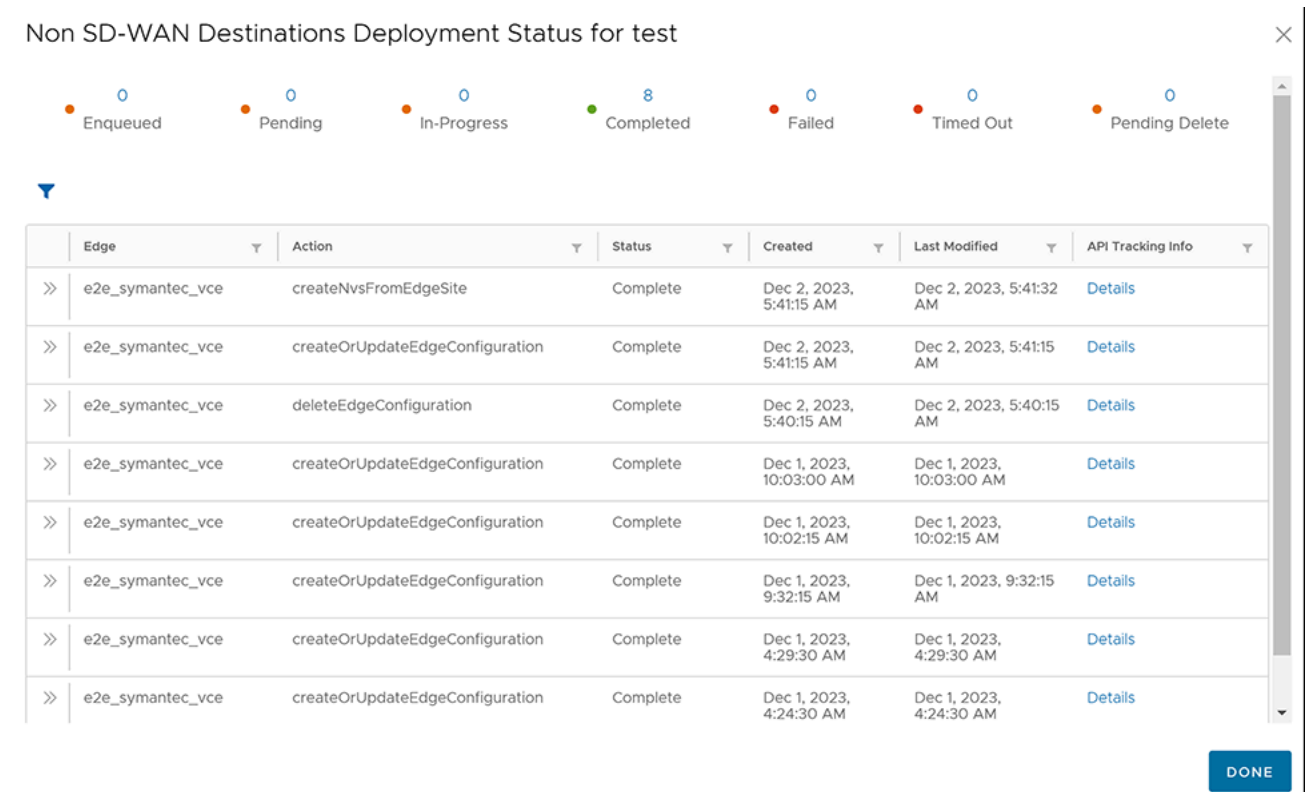
To delete the SSE integration, select the SSE integration from the list, and then click **Delete**.



Note: You cannot delete SSE integrations that are currently used by Edges.

To monitor the automation status, click the **View** link in the **Tunnel Deployment Status** column. The following screen appears:

Figure 4-1: Tunnel Deployment Status

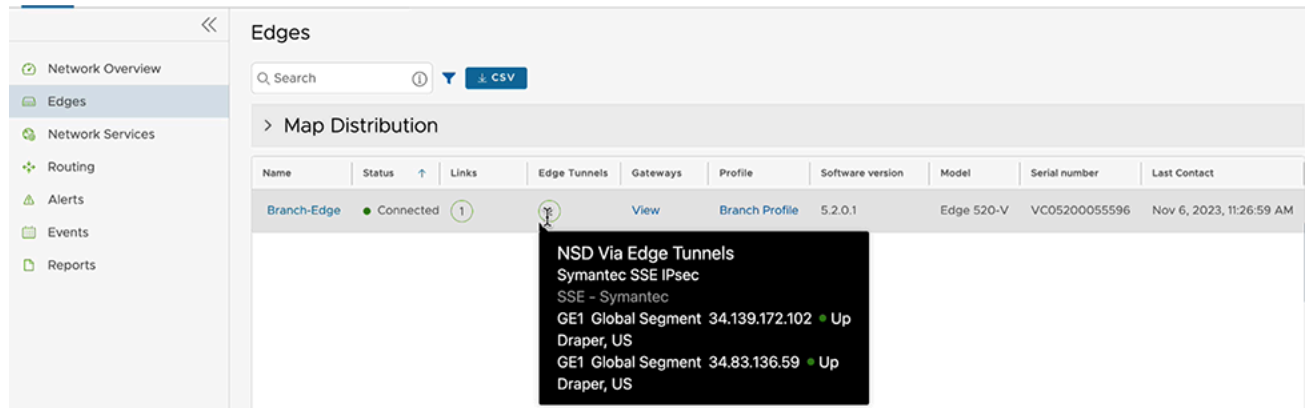


The actions `createOrUpdateEdgeConfiguration` and `deleteEdgeConfiguration` indicate the SSE automation to update the Orchestrator Edge Device settings. The other actions are for third party automations.

Note: You can also monitor the SSE deployment status on **Monitor > Events** and **Monitor > Network Services > Non SD-WAN Destinations via Edge** screens. For more information, see the *VeloCloud SD-WAN Administration Guide - Monitor events and Monitor Network Services*.

To verify whether the tunnels are up, go to **Monitor > Edges**, and hover the mouse under the **Edge Tunnels** column. You can view the details as shown below:

Figure 4-2: Edge Tunnels



After configuring the SSE subscription and integration:

- Associate the Security Service Edge Subscription to an Edge. For more information, see the *VeloCloud SD-WAN Administration Guide*.
- Direct the network traffic to a specific Enterprise Cloud. Navigate to **Configure > Edges > Business Policy**. Click **+ Add** to add a new rule. For more information, see the *VeloCloud SD-WAN Administration Guide - Create Business Policy Rule*.

References

A.1 Related Documents

The following documentation is available for **Arista VeloCloud SD-WAN**:

- *Arista VeloCloud SD-WAN Operator Guide*
- *Arista VeloCloud SD-WAN Administration Guide*
- *Arista VeloCloud SD-WAN Gateway Monitoring Guide*
- *Arista VeloCloud SD-WAN Orchestrator Deployment and Monitoring Guide*
- *Arista VeloCloud SD-WAN Partner Guide*
- *Arista VeloCloud SASE Global Settings Guide*
- *Arista VeloCloud SD-WAN Troubleshooting Guide*
- *Arista VeloCloud SD-WAN Design Guide for Enhanced Firewall Services*
- *Arista VeloCloud SD-WAN 6.4 API*
- *Arista VeloCloud Portal API 6.4*
- *Arista AliCloud Virtual Edge Deployment Guide*
- *Arista AWD Virtual Edge Deployment Guide*
- *Arista Azure Virtual Edge Deployment Guide*
- *Arista Google Cloud Platform Virtual Edge Deployment Guide*
- *Arista VeloCloud SASE and QRadar SIEM Integration Guide*
- *Arista VeloCloud SD-WAN and Cloud on AWS Deployment Guide*
- *Arista VeloCloud SD-WAN and Forcepoint SSE Integration Guide*
- *Arista VeloCloud SD-WAN and Google Network Connectivity Center Integration Guide*
- *Arista VeloCloud SD-WAN and Microsoft Route Server Integration Guide*
- *Arista VeloCloud SD-WAN and Netskope SSE Integration Guide*
- *Arista VeloCloud SD-WAN Azure Private Multi-Access Edge Compute Deployment Guide*
- *Arista VeloCloud SD-WAN License Management Guide*