ARISTA

# Configuration Guide

# Arista VeloCloud SD-WAN SSE for Symantec

## Services

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

# Contents

Chapter 1

# Configure SSE for Symantec

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

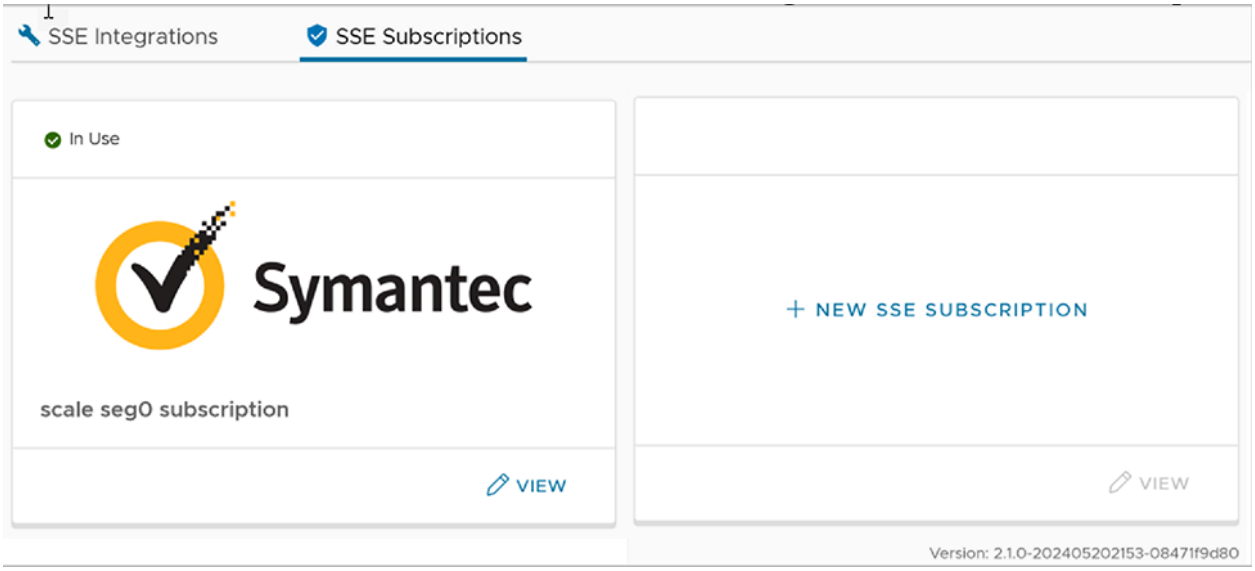
**Prerequisites**

- 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.

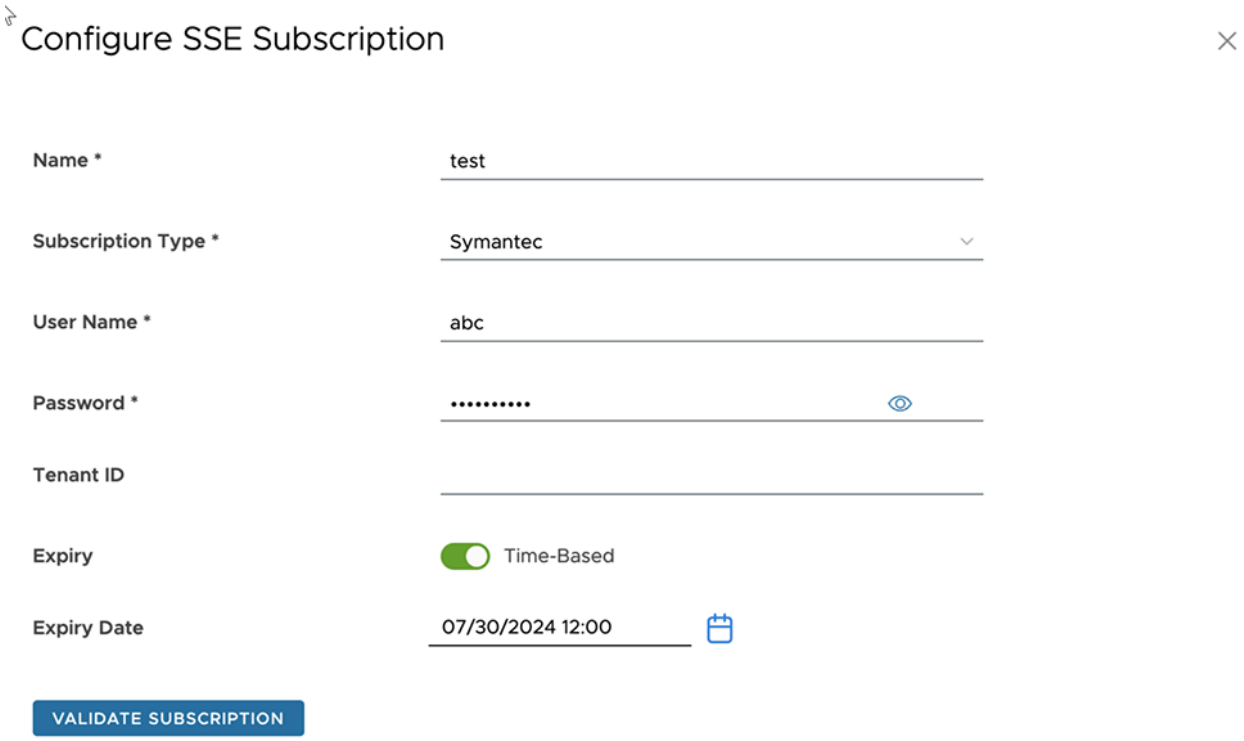
   **Figure 1-1: SSE Subscriptions for Symantec**




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.

5. 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**.

6. Configure the following options:

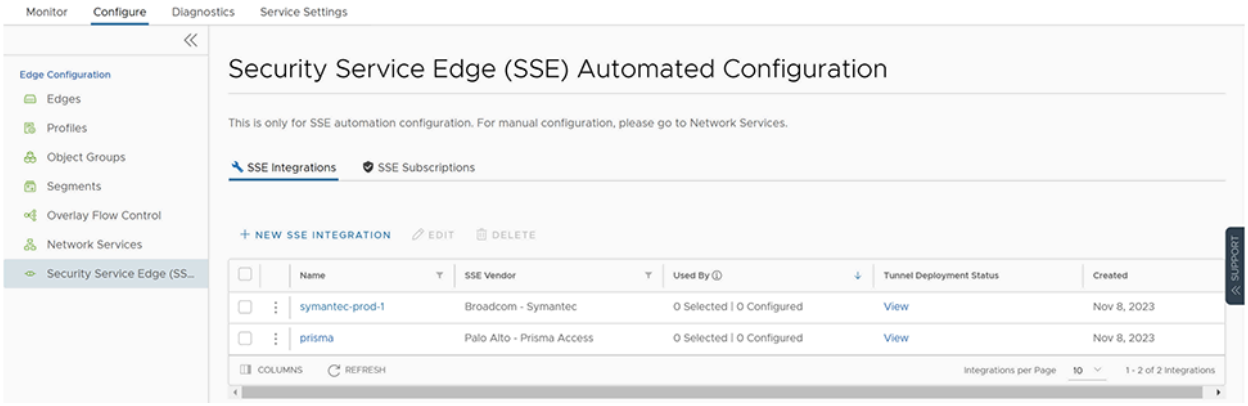
| Option | Description |
|---|---|
| User Name | Enter the API username as configured in the **Symantec Cloud** portal. |
| Password | Enter the API password as configured in the **Symantec Cloud** portal.<br>**Note:** Starting from the 4.5 release, the use of the special character "<" in the password 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. |
| 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.<br>This field is optional and is blank, by default. |

7. 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.

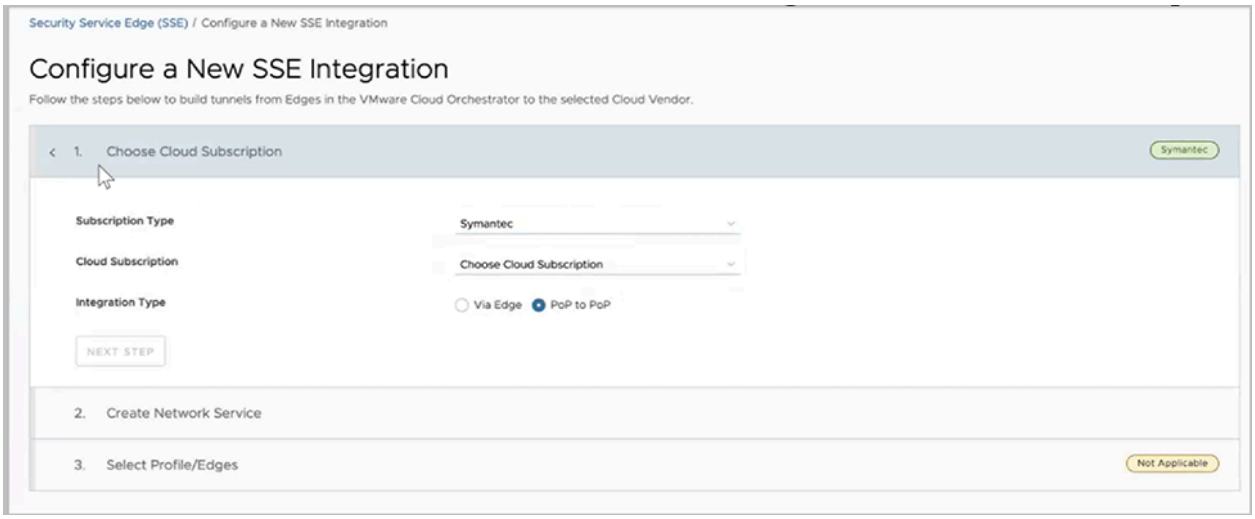
8. Click **Save** to save the configured subscription.
9. After creating an SSE Subscription, you can proceed to create an SSE Integration.
10. Navigate to **Configure** > **Security Service Edge (SSE)**. By default, the **SSE Integrations** tab is displayed.

**Figure 1-3: SSE Integrations for Symantec**




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

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




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

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

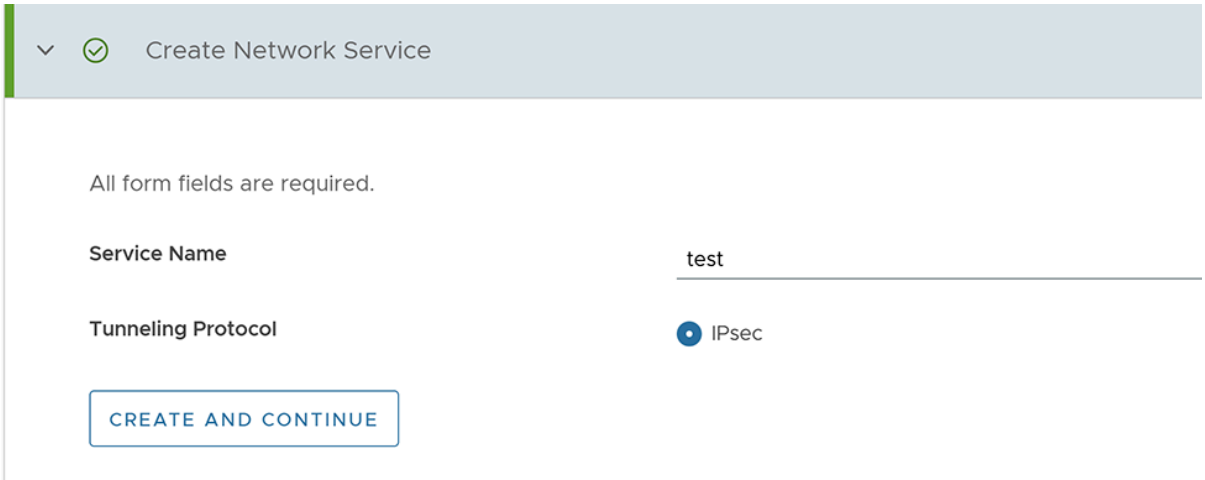
| Option | Description |
|---|---|
| Subscription Type | Select a subscription type for which you want to set up an SSE integration. The available options are:<br>• **Prisma Access**<br>• **Symantec** |
| Cloud Subscription | Select a cloud subscription from the drop-down menu. Only those cloud subscriptions that are configured under the SSE vendor selected in **Subscription Type**, appear in the drop-down menu.<br>These cloud subscriptions are populated based on the configurations under **Configure** > **Security Service Edge (SSE)** > **SSE Subscriptions**.<br>**Note:** This field appears only when you select a subscription type. |
| Integration Type | Select either one of the following options:<br>• **Via Edge**: Tunnel is established from Edge to Symantec.<br>• **PoP to PoP**: Geneve tunnel is established from a VeloCloud Gateway to Symantec WSS.<br>**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 . |

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**

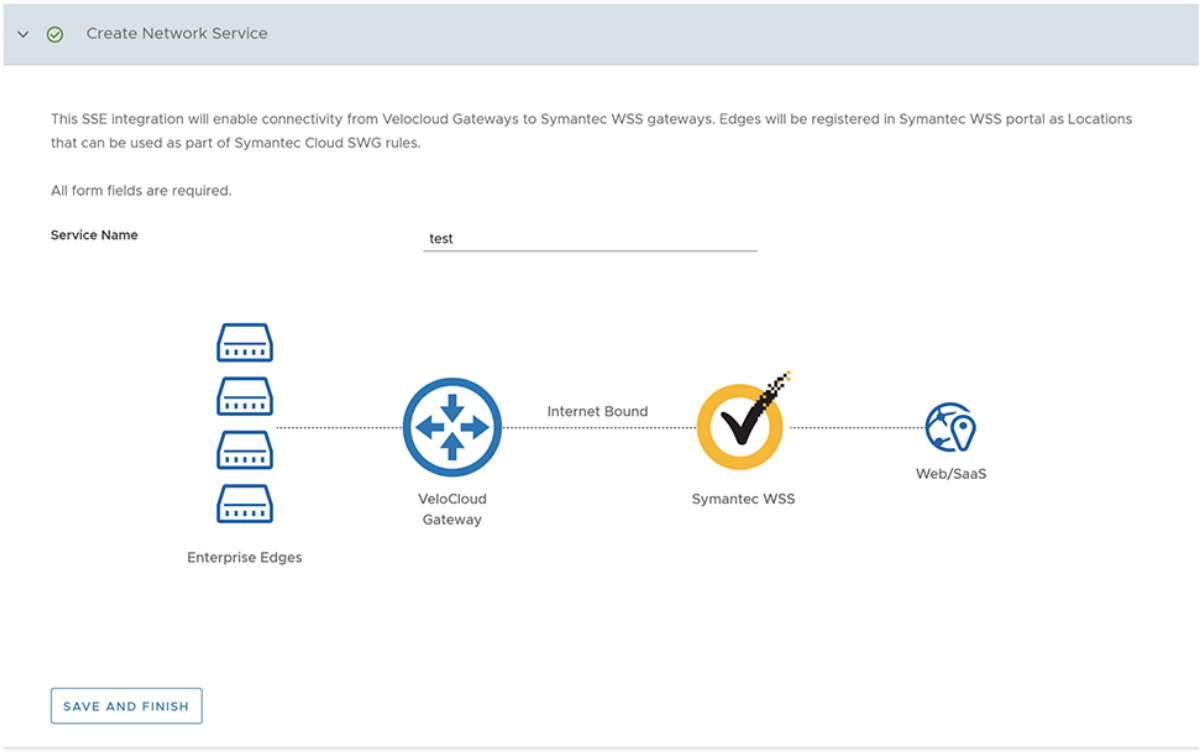


| Option | Description |
|---|---|
| Service Name | Enter a unique service name. |
| Tunneling Protocol | This field is set to **IPsec**, which is the only supported protocol. |

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.<br>**Note:** You can select multiple Segments for **Symantec** subscription. |
| 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.

Chapter 2

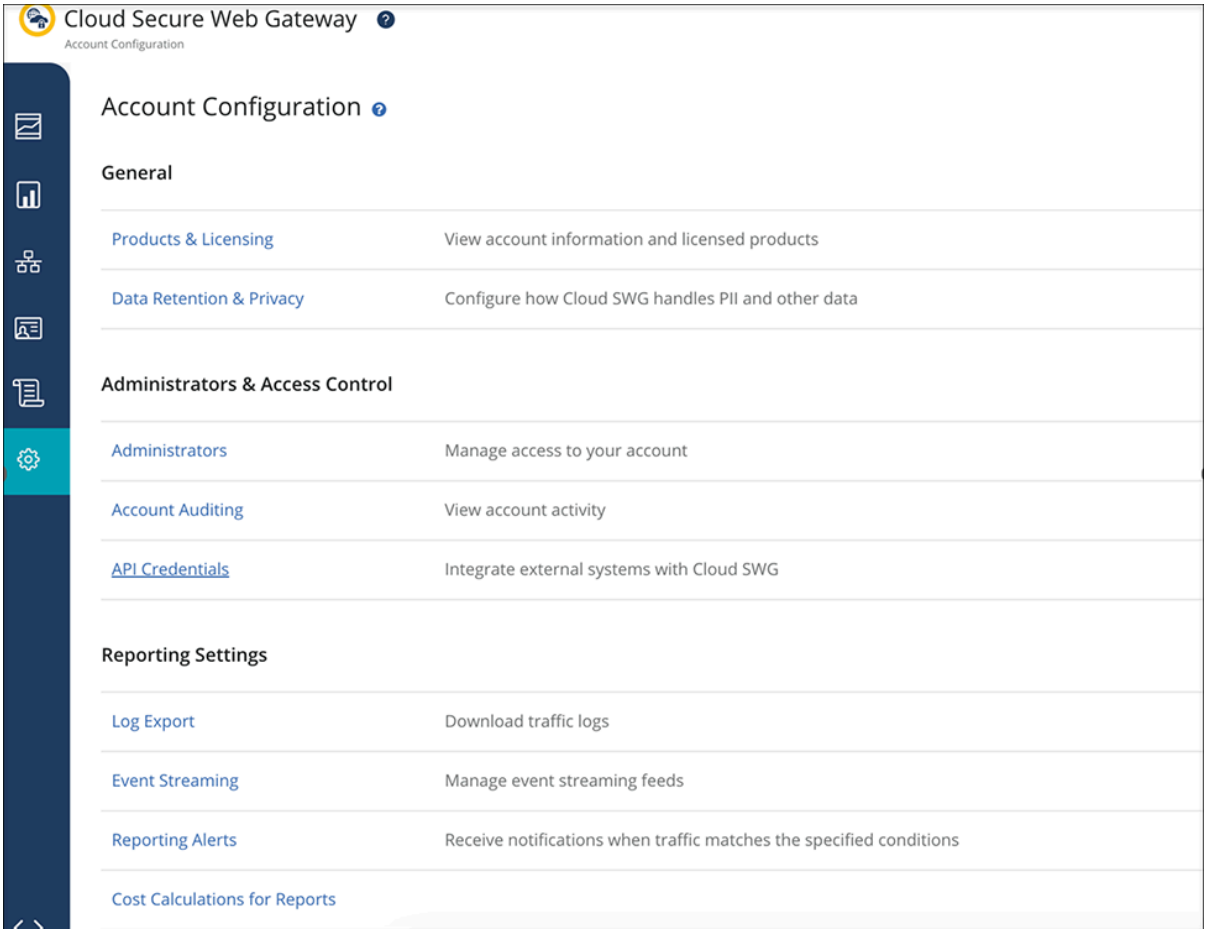
# Configure Symantec API Credentials

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:

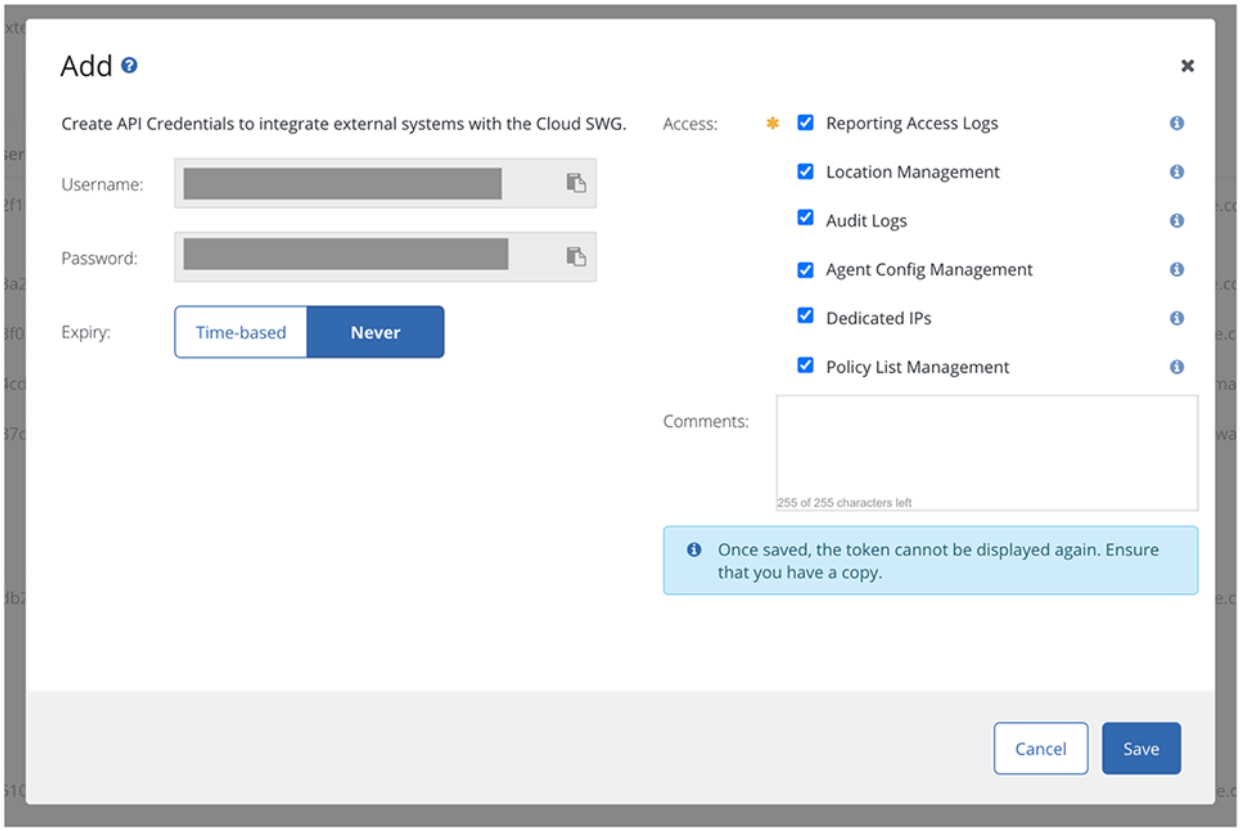
1. Log into the **Symantec Cloud** portal, and then click **Account Configuration**.
   The **Account Configuration** screen appears:

   **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**




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 | 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.<br>**Note:** Selecting this check box is mandatory. |
| Location Management | 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.<br>**Note:** Selecting this check box is mandatory. |
| 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 topicSecurity Service Edge (SSE).

# Chapter 3

# 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*.

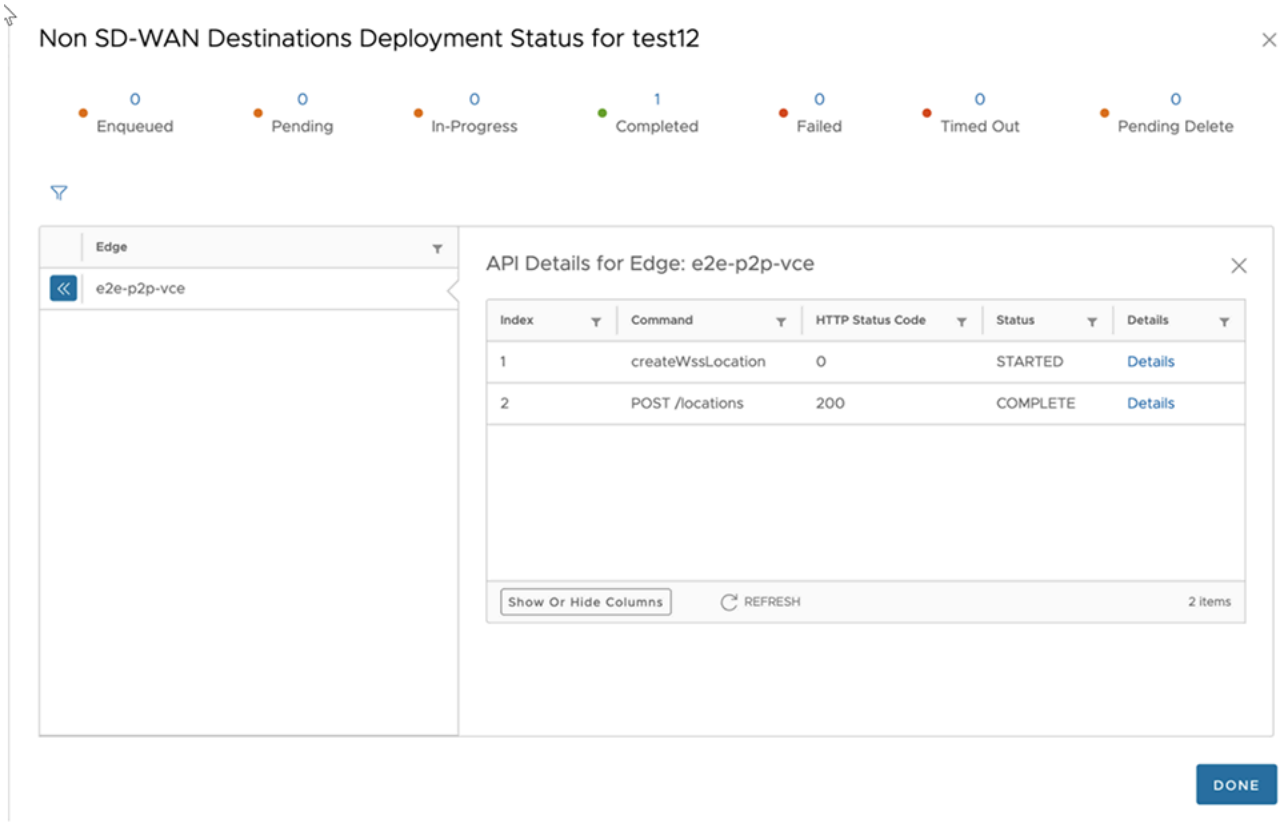
To perform **Symantec WSS PoP to PoP Integration**, follow the below workflow:

- 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.

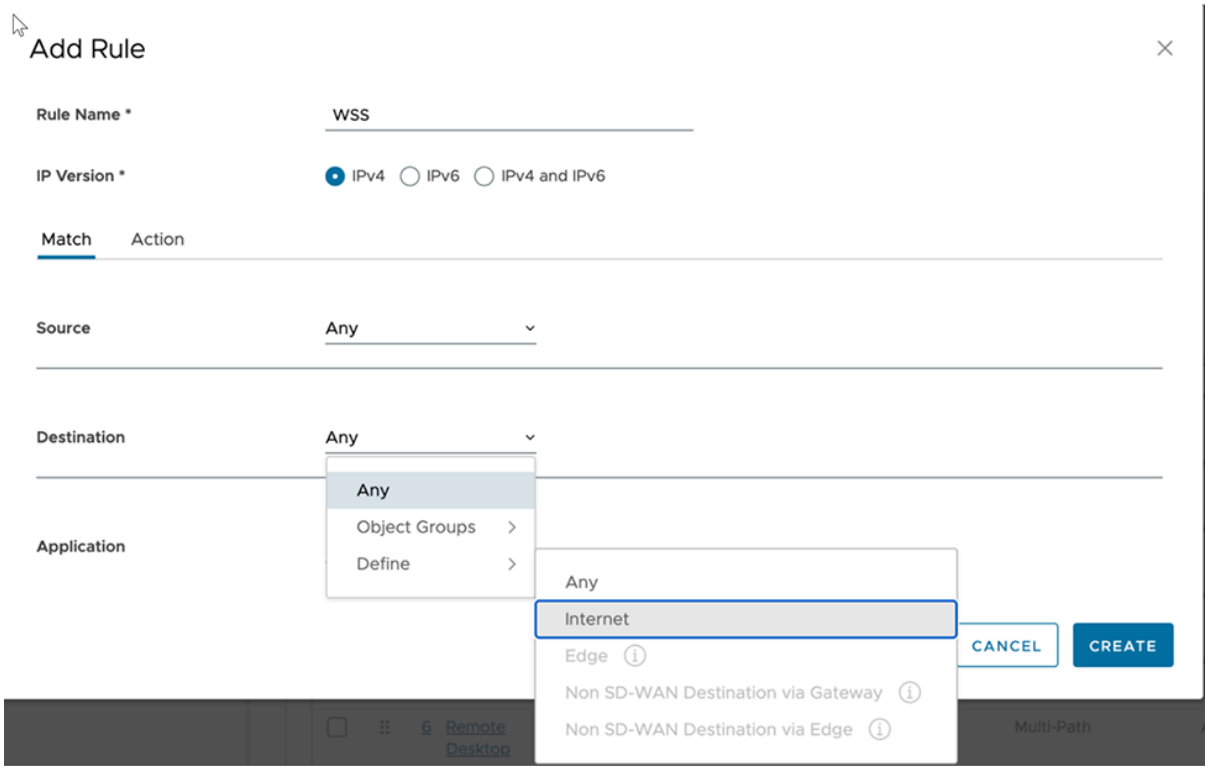
**Figure 3-1: Tunnel Deployment Status**




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**



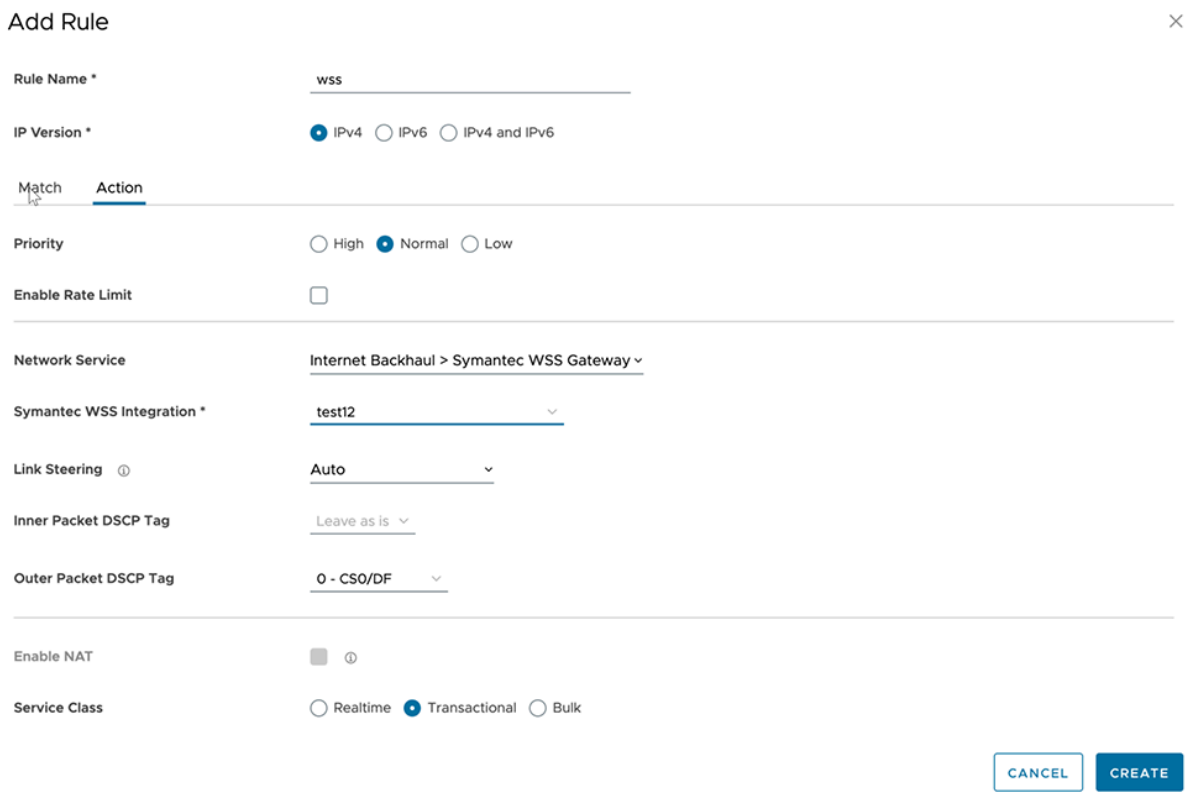

**c.** Enter the **Rule Name** and select the **IP Version** as **IPv4**.

> **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**




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.

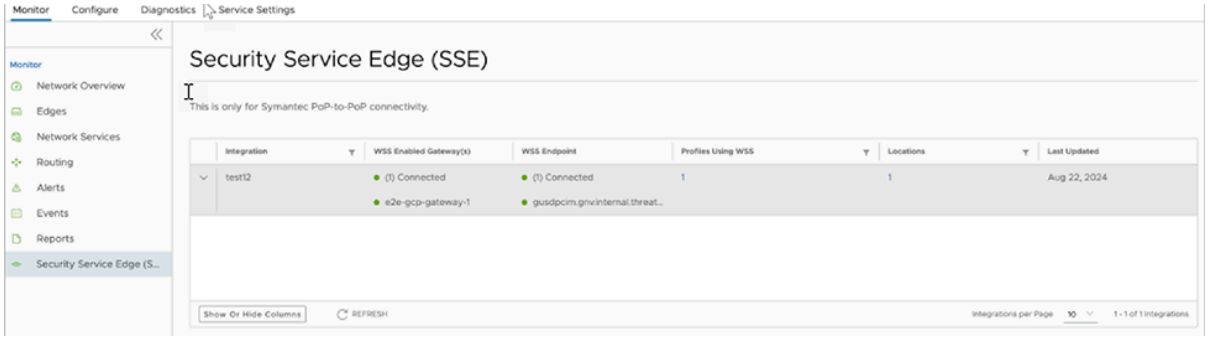
g. Configure all the other fields, and then click **Create**. For more information on these fields, see the topic *Create Business Policy Rule* in the *Arista VeloCloud SD-WAN Administration Guide*.

> **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**




**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

Chapter 4

# 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

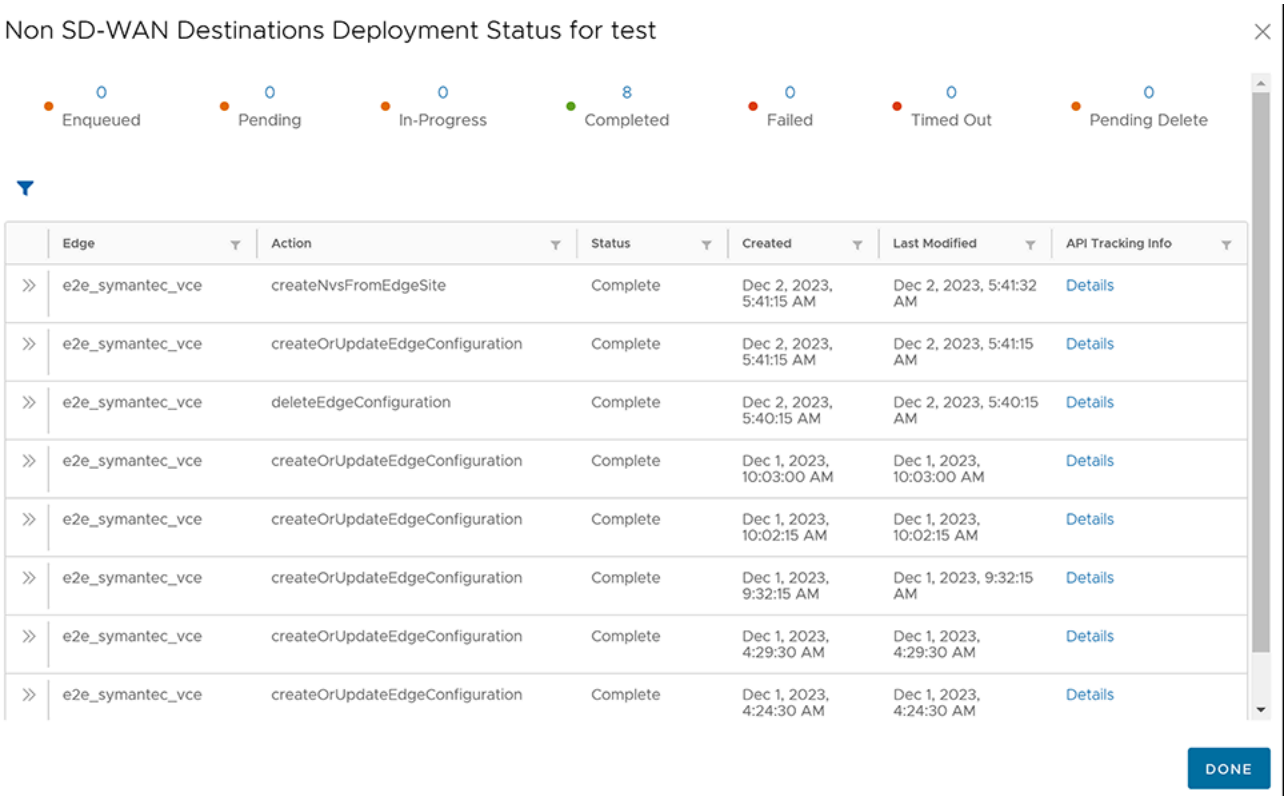
If you wish to edit the existing SSE integration, select the SSE integration from the list on the **Security Service Edge (SSE)** screen, and then click **Edit**. You can also click the SSE integration name link to edit it.

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**

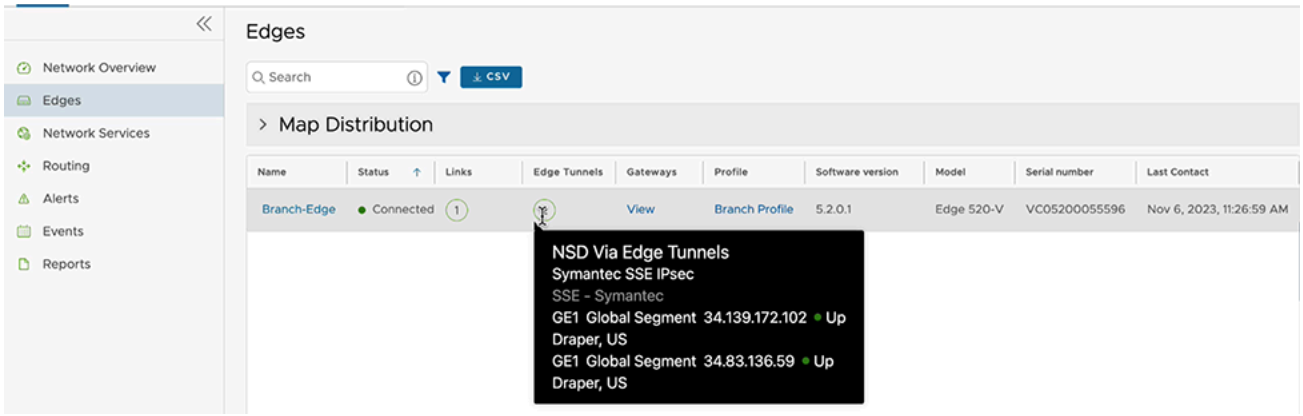



The actions `createOrUpdateEdgeConfiguration` and `deleteEdgeConfiguration` indicate the SSE automation to update the Orchestrator Edge Device settings. The other actions are for third party automations.

**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*.

# Appendix A

# 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*