ARISTA

Configuration Guide

VeloCloud SD-WAN SSE for PAN Prisma

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

Contents

Chapter 1

Configure SSE for PAN Prisma

Prerequisites

For the **PAN Prisma** SSE integration:

- An Enterprise user must first create a service account in the **Palo Alto Networks Strata Cloud Manager** portal. For more information, see Create a Prisma Service Account.
- An Enterprise user must create **IKE** and **IPsec** profiles on the **Palo Alto Networks Strata Cloud Manager** portal. These profiles can then be used for the SSE integration. For more information, see Palo Alto Networks Strata Cloud Manager Configuration.

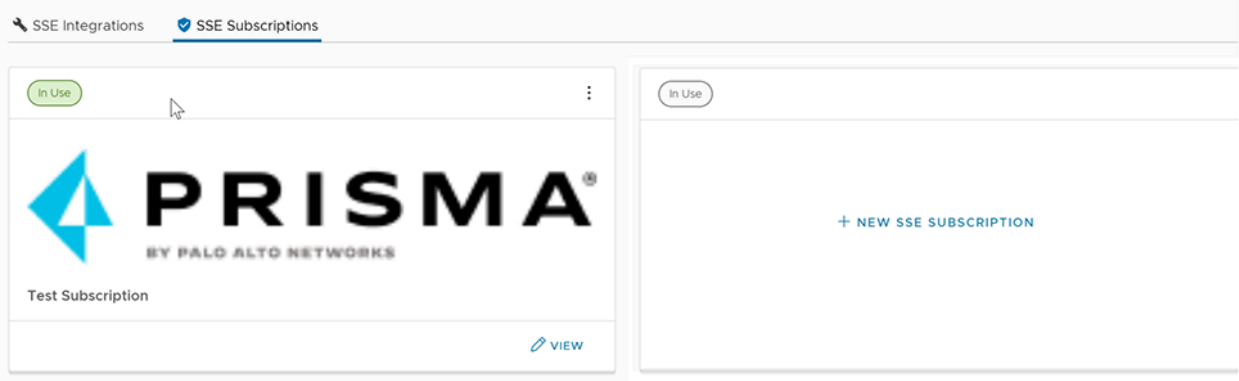
> **Note:** As tunnel establishment is an asynchronous operation, the Security Service Edge (SSE) automated configuration for **PAN Prisma** might take 5 - 30 minutes per WAN link tunnel, to complete.

Prisma Access is the Enterprise Security Solution offered by Palo Alto Networks (PAN). It is a cloud-based solution.

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

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.

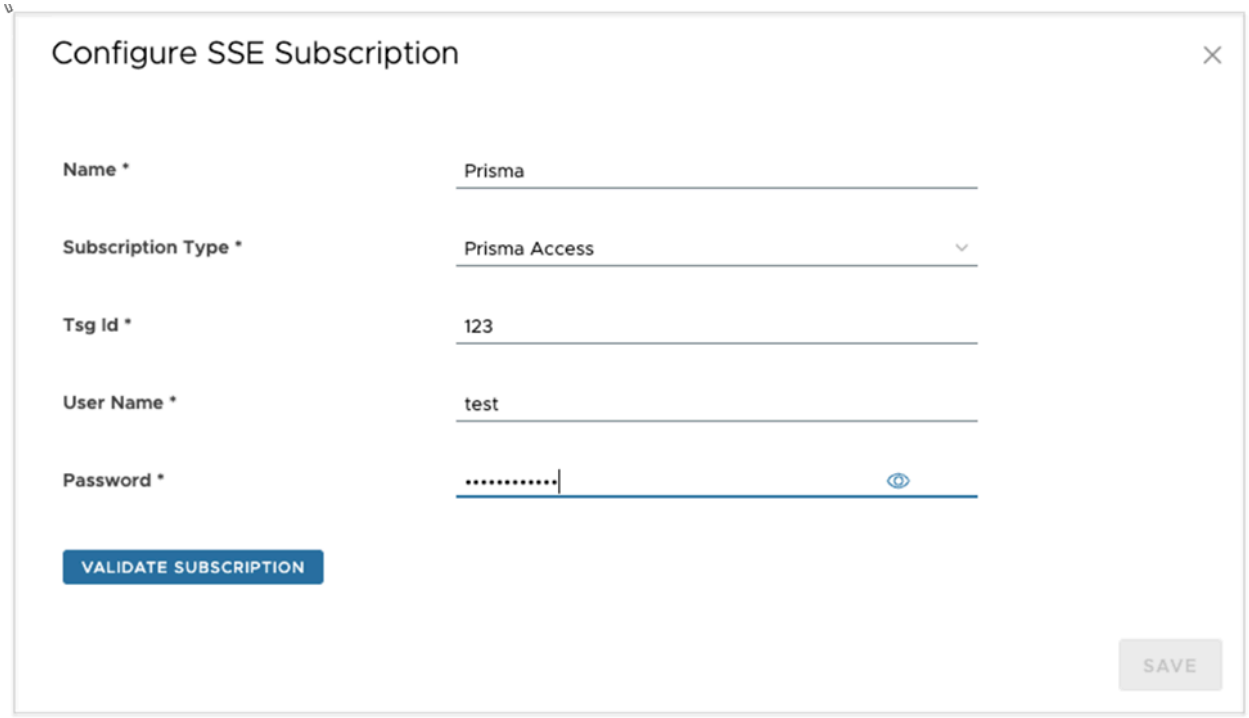
   Figure 1-1: SSE Subscriptions for Prisma



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 **Configure SSE Subscription** window appears.

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



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

6. Configure the following options:

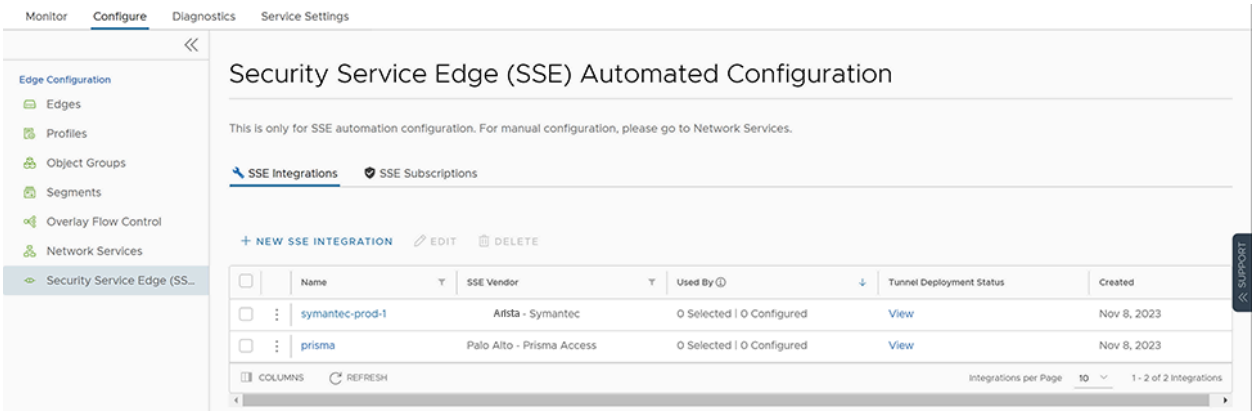
Option	Description
Name	Enter a name for the subscription.
Subscription Type	Select **PAN Prisma** from the drop-down menu.
Tsg Id	Enter the ID. This value is a positive integer and can be found in the **Palo Alto Networks Strata Cloud Manager** portal, under **Settings** > **Products**.
User Name	Enter the service account username.
Password	Enter the service account password. **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.

Note: The fields **Tsg Id**, **User Name**, and **Password** must match the values configured in the **Palo Alto Networks Strata Cloud Manager** portal.

7. Click **Validate Subscription** to make sure that the entered credentials are correct, and then click **Save** to save the configured subscription.
8. After creating an **SSE Subscription**, you can proceed to create an **SSE Integration**.

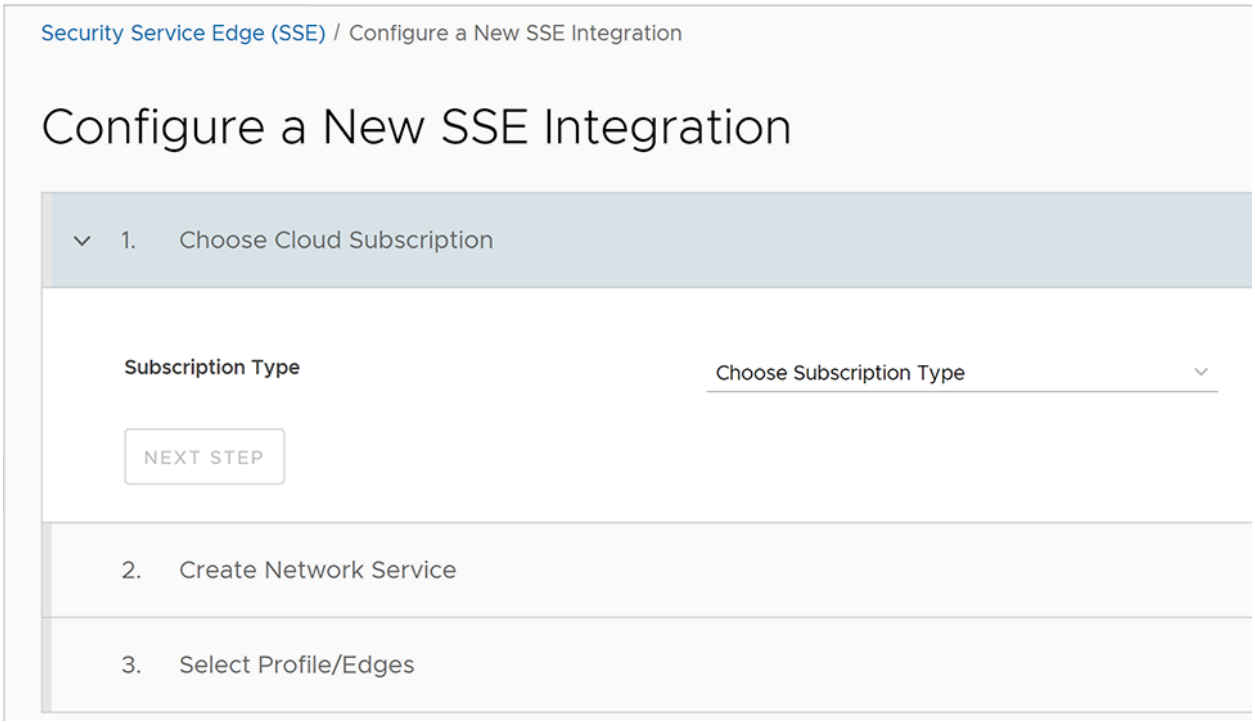
9. Navigate to **Configure→ Security Service Edge (SSE)**. By default, the **SSE Integrations** tab is displayed.

Figure 1-3: SSE Integrations for Prisma



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

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



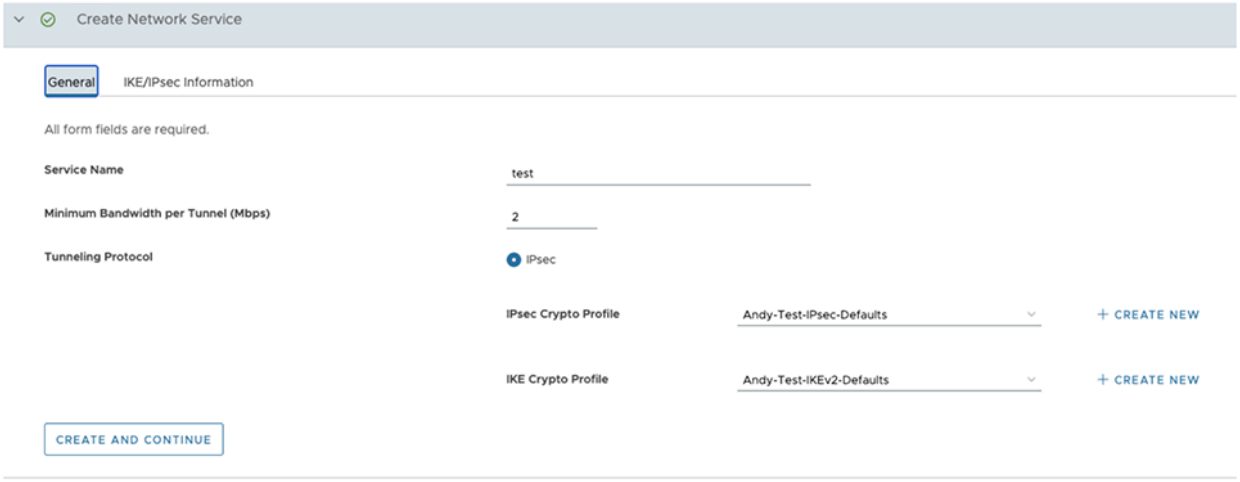
Note: The fields displayed on the screen vary depending on the selected **Subscription Type**.

11. 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: • Prisma Access • 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. These cloud subscriptions are populated based on the configurations under **Configure** > **Security Service Edge (SSE)** > **SSE Subscriptions**. **Note:** This field appears only when you select a subscription type.

12. Click **Next Step** to activate the next section. Under the **Network Service** section, there are two tabs. Configure the following options under the **General** tab:

Figure 1-5: Create Network Service - General

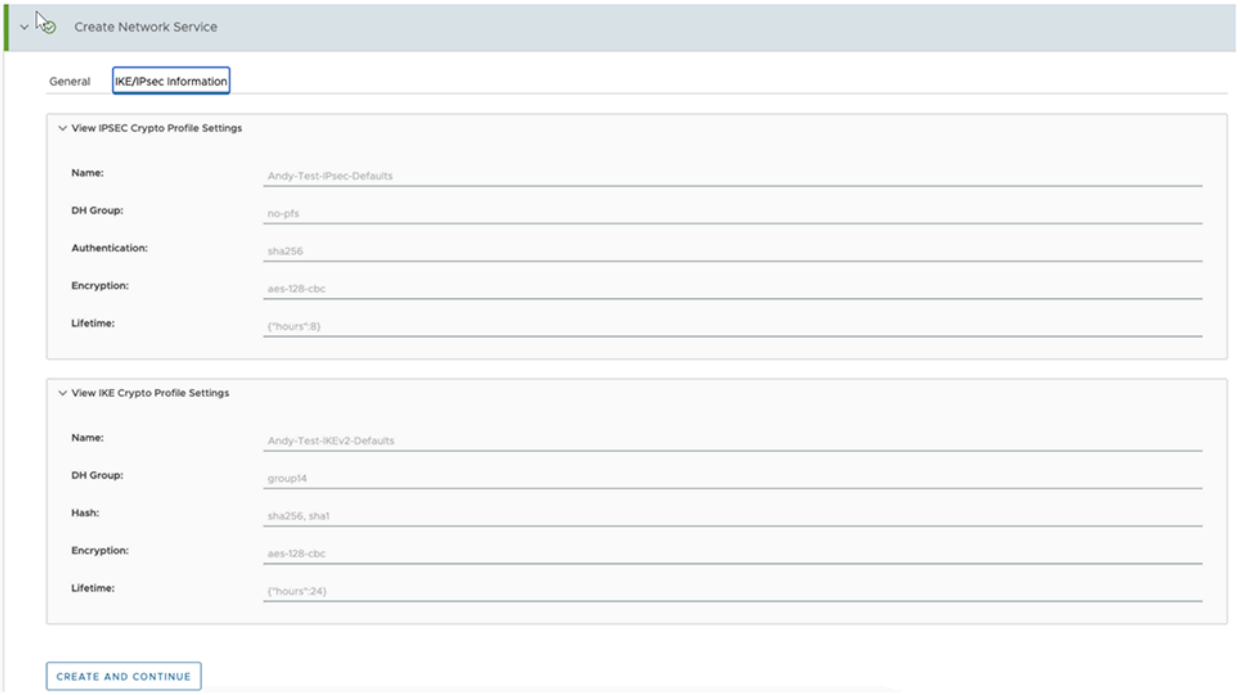


Option	Description
Service Name	Enter a unique service name.
Minimum Bandwidth per Tunnel (Mbps)	Enter the required bandwidth. The default value is **2**.
Tunneling Protocol	By default, IPsec tunneling protocol is selected. You must select the **IPsec Crypto Profile** and **IKE Crypto Profile** from the respective drop-down menus. These drop-down menus are populated based on the Profiles created in the **Palo Alto Networks Strata Cloud Manager** portal.

13. The following options are displayed under the **IKE/IPsec Information** tab. These values must be configured in the **Palo Alto Networks Strata Cloud Manager** portal. For more details about these fields,

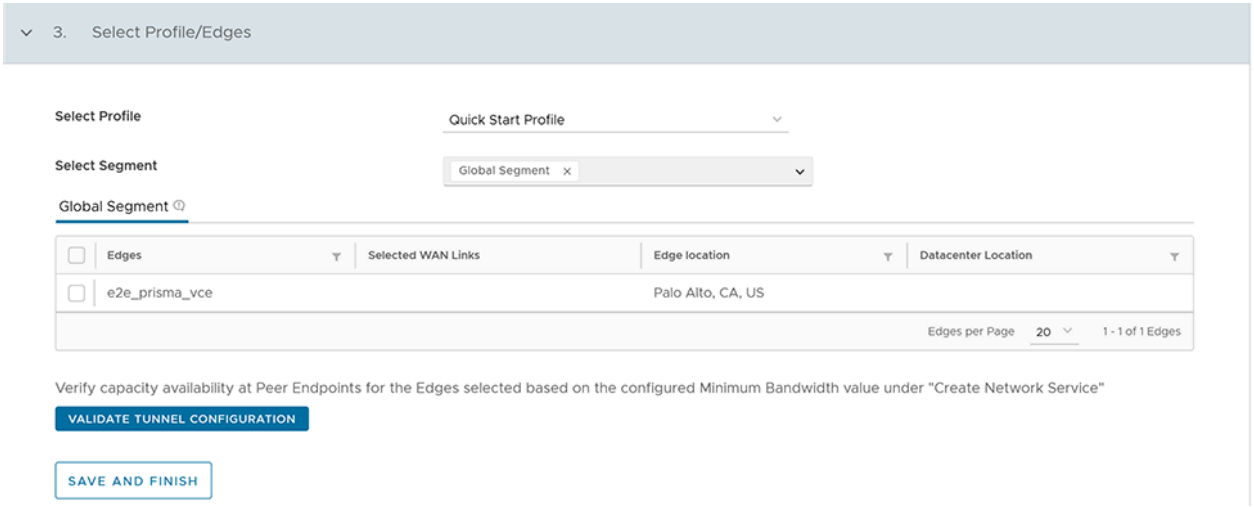
refer to the *Arista VeloCloud SD-WAN Administration Guide - Configure Non SD-WAN Destinations Via Edge* section.

Figure 1-6: Create Network Service - IKE/IPsec Information



14. Click **Create and Continue** to activate the next section.
15. Under **Select Profile/Edges** section, configure the following options:

Figure 1-7: Select Profile/Edges



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. **Note:** You can select only one Segment for **Prisma** subscription.

16. 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.
17. 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.
18. Click **Validate Tunnel Configuration**. A warning is displayed if any of the datacenters is over subscribed.

    Note: The **Validate Tunnel Configuration** button is available only for the **Prisma Access** subscription type. In Prisma deployment, you must buy a license to add bandwidth capacity at a datacenter. This license restricts the maximum throughput, thus displaying a warning.

19. Once the tunnel configuration is validated, click **Save and Finish**.

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

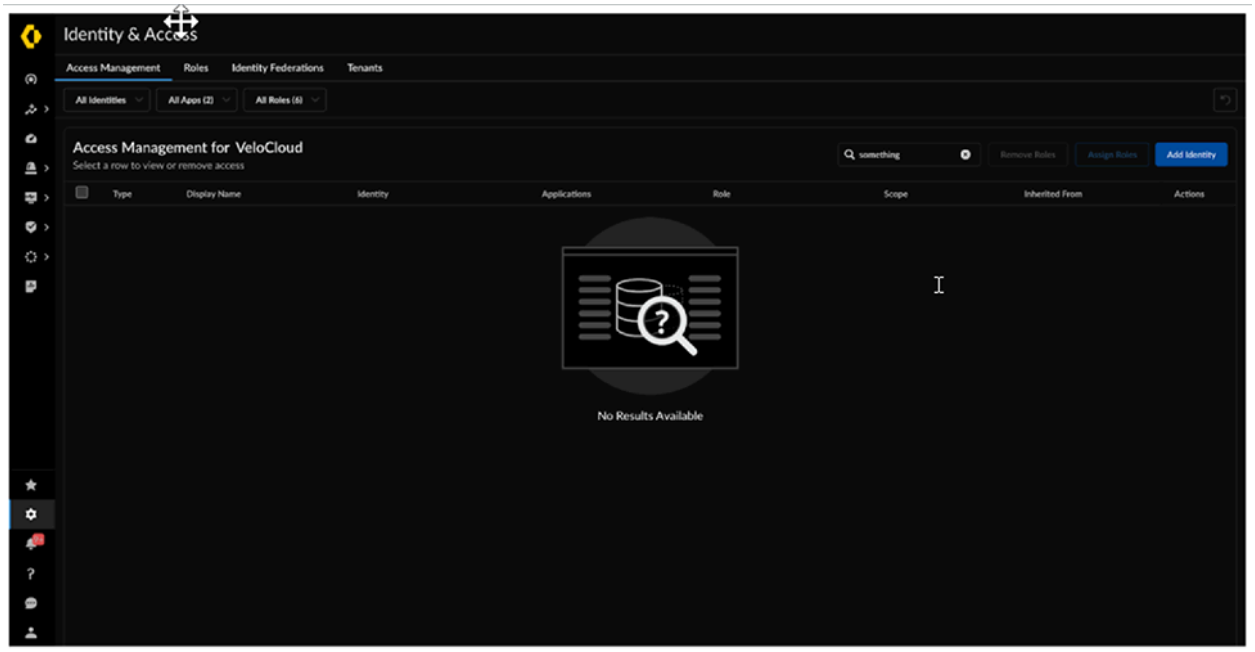
Chapter 2

Create a Prisma Service Account

The VeloCloud Orchestrator requires API access for creating and configuring the integration service from SD-WAN enabled branch locations. For the API integration to work, a service account must be created. This service account authenticates the Orchestrator when it reaches out to the Prisma Access solution to request OAuth 2.0 access tokens from the platform for API authorization. This access type can be configured by following the steps below:

1. In the **Palo Alto Networks Strata Cloud Manager** portal, navigate to **Settings** > **Identity & Access**. The following screen appears:

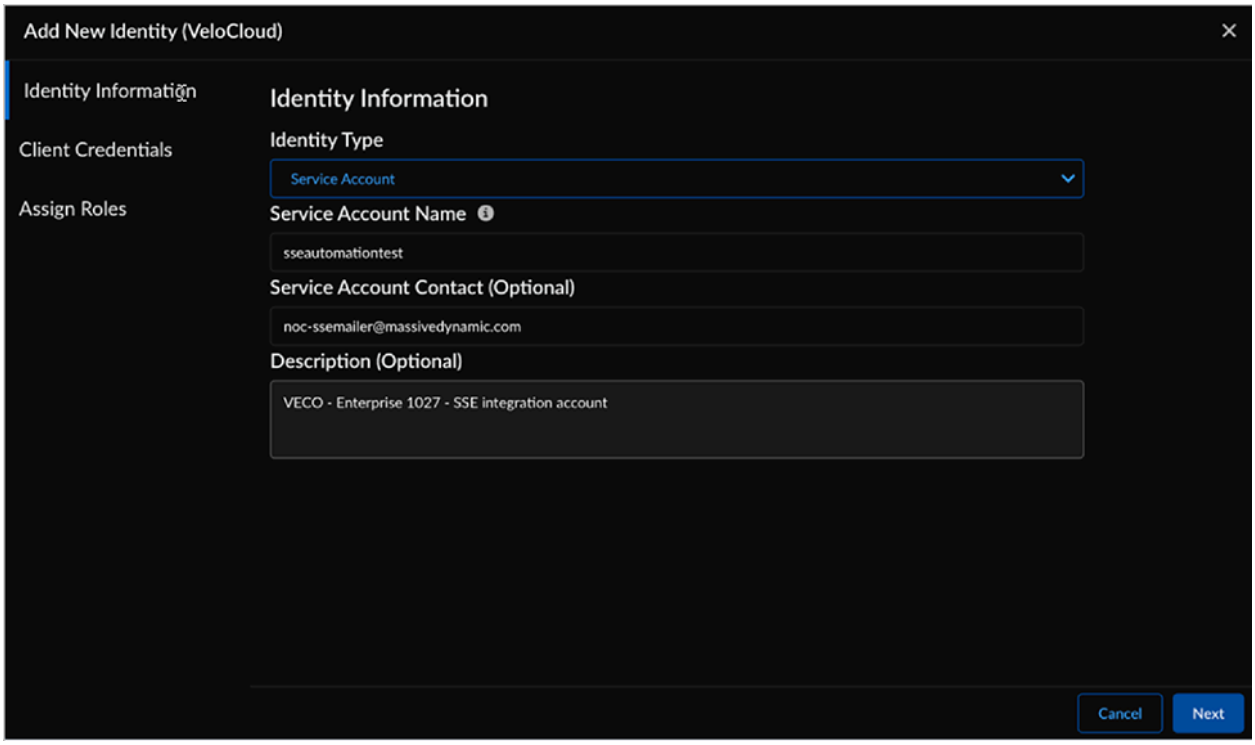
   Figure 2-1: Identity & Access



2. Click the **Add Identity** button.

The **Add New Identity (VeloCloud)** screen appears:

Figure 2-2: Add New Identity (VeloCloud)



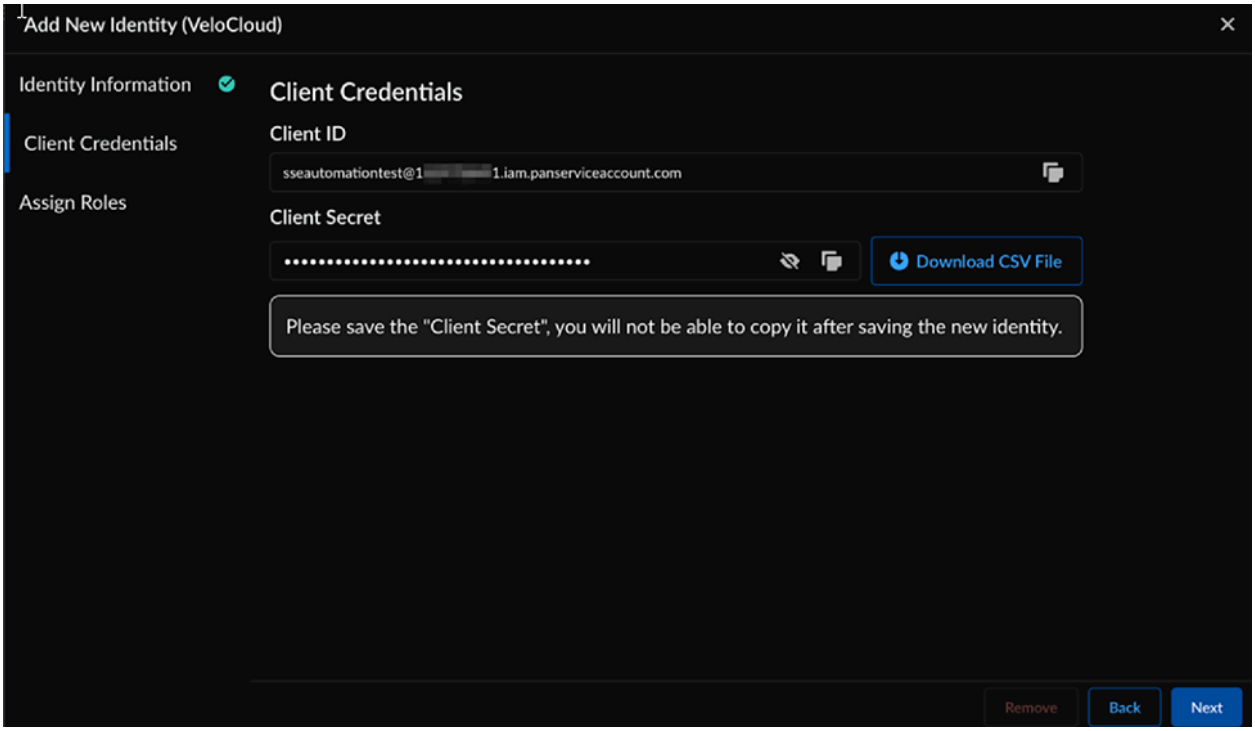
3. Enter the following details:

Option	Description
Identity Type	Click the drop-down menu. The available options are: • **User**: Portal user that is bound to a single person or human identity. • **Service Account**: These accounts are not bound to a particular person and can be used for API integration. You must select **Service Account** for the SSE integration.
Service Account Name	Enter a unique name, that can be used to identify the account on any platform.
Service Account Contact	Enter the contact email address, that can be used to identify and contact the account owner in case of emergencies. This field is optional.
Description	Enter description of the scope and use of the account. This field is optional.

4. Click **Next**.

The **Client Credentials** screen appears:

Figure 2-3: Client Credentials



5. Enter the following details:

Option	Description
Client ID	This value is system generated and is in the format: <service account name>@<tsg ID>.iam.panserviceaccount.com **Note:** Make a note of <service account name> and <tsg ID>. These values are required during the SSE workflow in the Orchestrator.
Client Secret	This value is system generated. It is a pre-shared key that can be used to request the OAuth2.0 tokens.

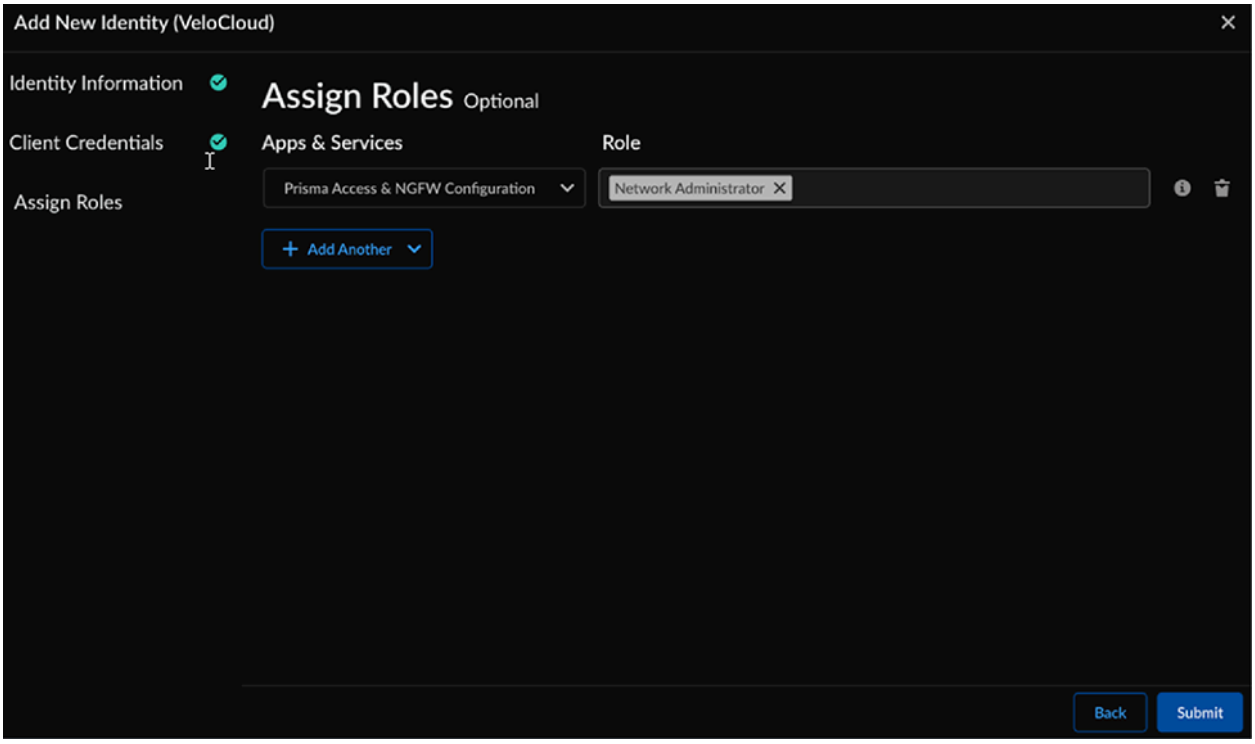
Note:

- These credentials must be used to access the OAuth token request API. As this is sensitive information, make sure to store these credentials taking into consideration your organization's data protection policies.
- After the account is created, the credentials can no longer be pulled from the Prisma UI. If you lose the credentials, you must create new credentials. The old credentials become invalid.

6. After you have entered all the details, click **Next**.

The **Assign Roles** screen appears:

Figure 2-4: Assign Roles



7. To limit the scope of access for the service account, it must be associated with the **Apps & Services**, and within each associated App, a **Role** must be designated. For the SSE workflow, ensure that the following access is defined:

Option	Description
Apps & Services	Select **Prisma Access & NGFW Configuration** from the drop-down menu.
Role	Select **Network Administrator**.

8. After the account scope is defined, click **Submit**.

Configure the IKE and IPsec profiles. For more information, see Palo Alto Networks Strata Cloud Manager Configuration.

Chapter 3

Palo Alto Networks Strata Cloud Manager Configuration

Before configuring the Security Service Edge (SSE) automation, you must first configure IKE and IPsec profiles to be used by the SSE automation. This is required for initiating the tunnel from the Edge to Prisma Cloud. This is a one-time manual configuration that must be performed in the Palo Alto Networks Strata Cloud Manager portal.

There is no dedicated location in the **Palo Alto Networks Strata Cloud Manager** portal to configure the **IKE** and **IPsec** profiles. Hence, this configuration must be done in the **Remote Networks** configuration section.

You can reuse the existing profiles if they have been already configured and supported by the Edges. To create new profiles, refer to the below template:

- AES 128 CBC
- DH Group 14 (IKE Crypto Profile)
- PFS configured (same as the DH Group value)
- SHA 256
- IKE SA Lifetime 1440 min
- IPsec SA Lifetime 480 min

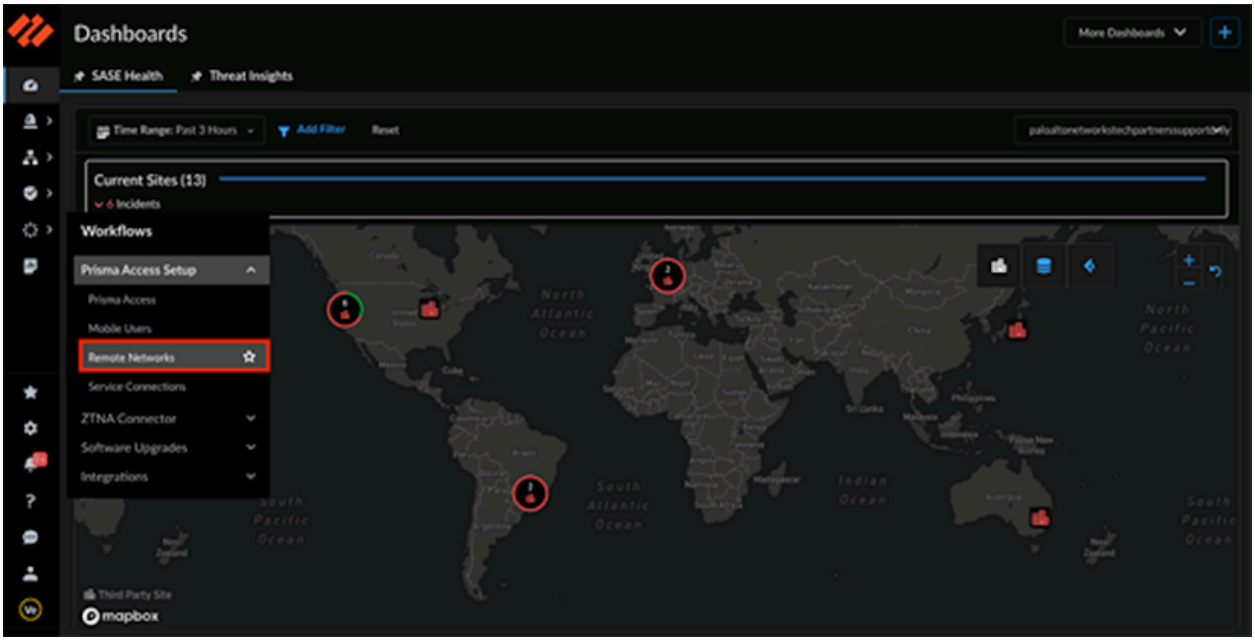
Note: This template is just an example. You can configure a stronger encryption algorithm if needed.

Follow the below steps to configure **IKE** and **IPsec** profiles:

Note: This procedure is for guidance purpose only.

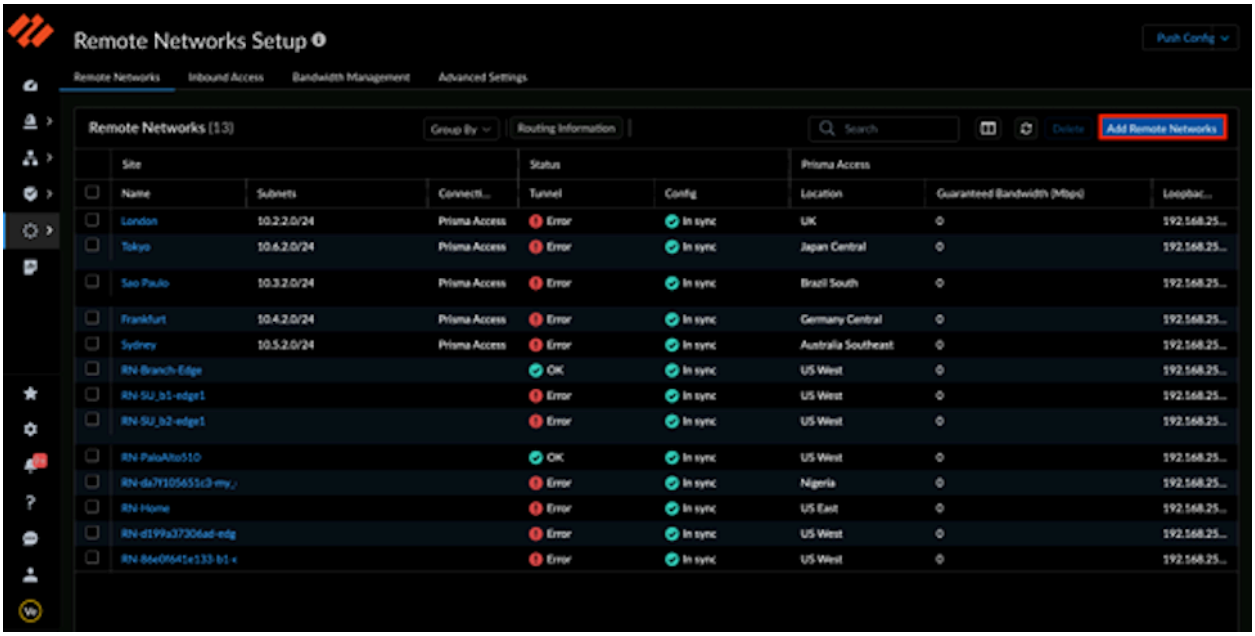
1. Log into the **Palo Alto Networks Strata Cloud Manager** portal. The following screen is displayed:

   Figure 3-1: Dashboards



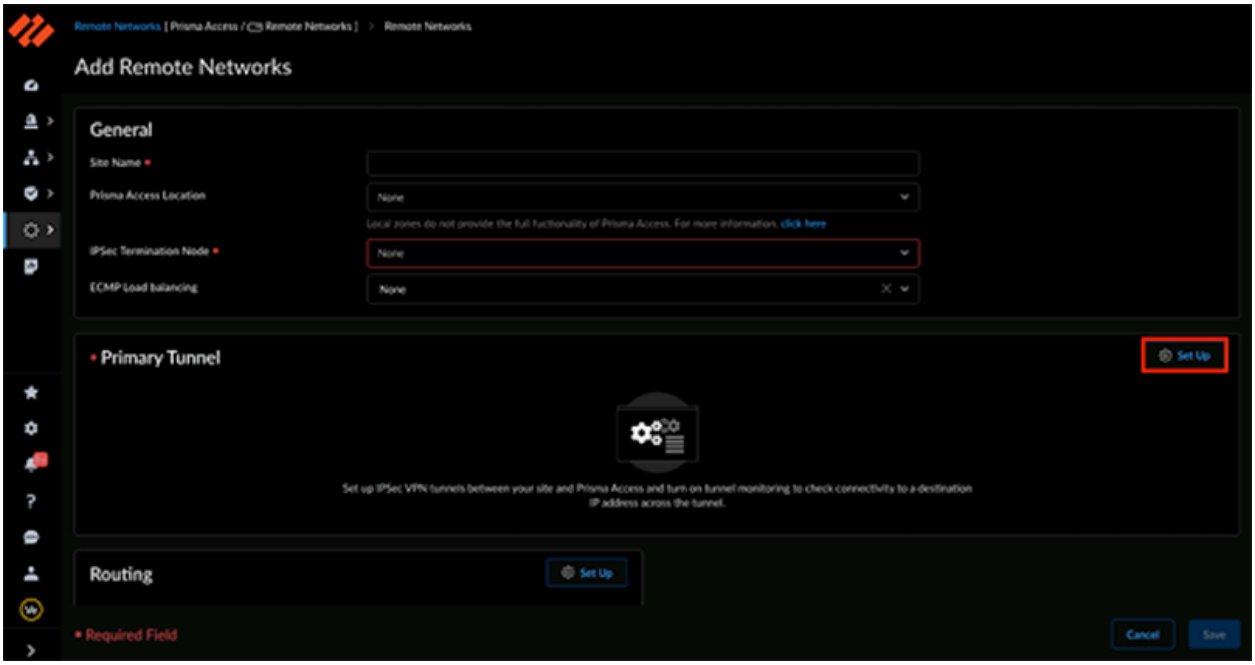
2. Navigate to **Workflows** > **Prisma Access Setup** > **Remote Networks** as shown in the above screenshot. The **Remote Networks Setup** screen appears.
3. Click **Add Remote Networks** in the top right corner of the **Remote Networks Setup** screen.

   Figure 3-2: Remote Networks Setup



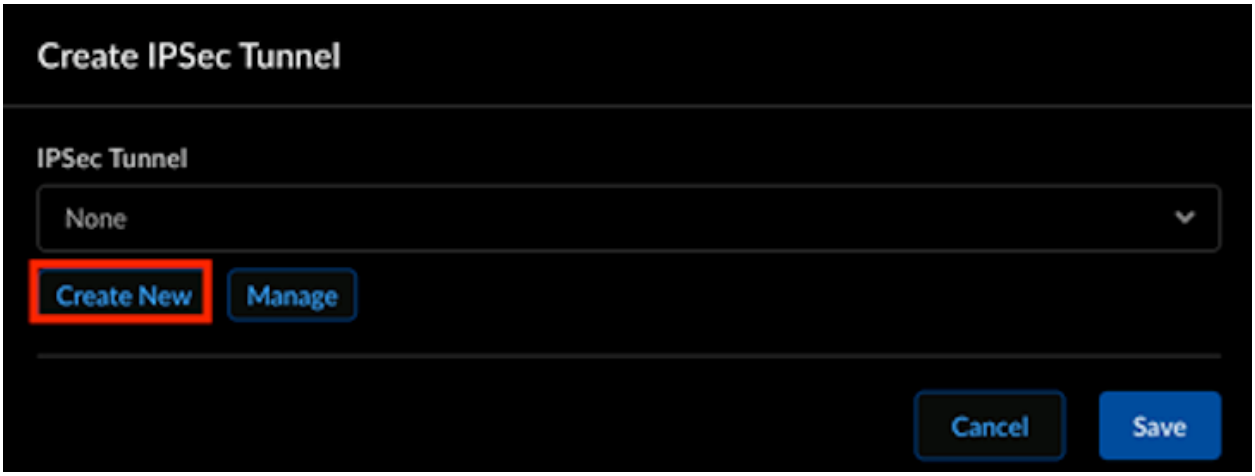
4. In the **Add Remote Networks** screen, ignore the mandatory fields and directly go to the **IKE** and **IPsec** profile configurations, by clicking **Set Up** in the **Primary Tunnel** section as shown below:

Figure 3-3: Add Remote Networks



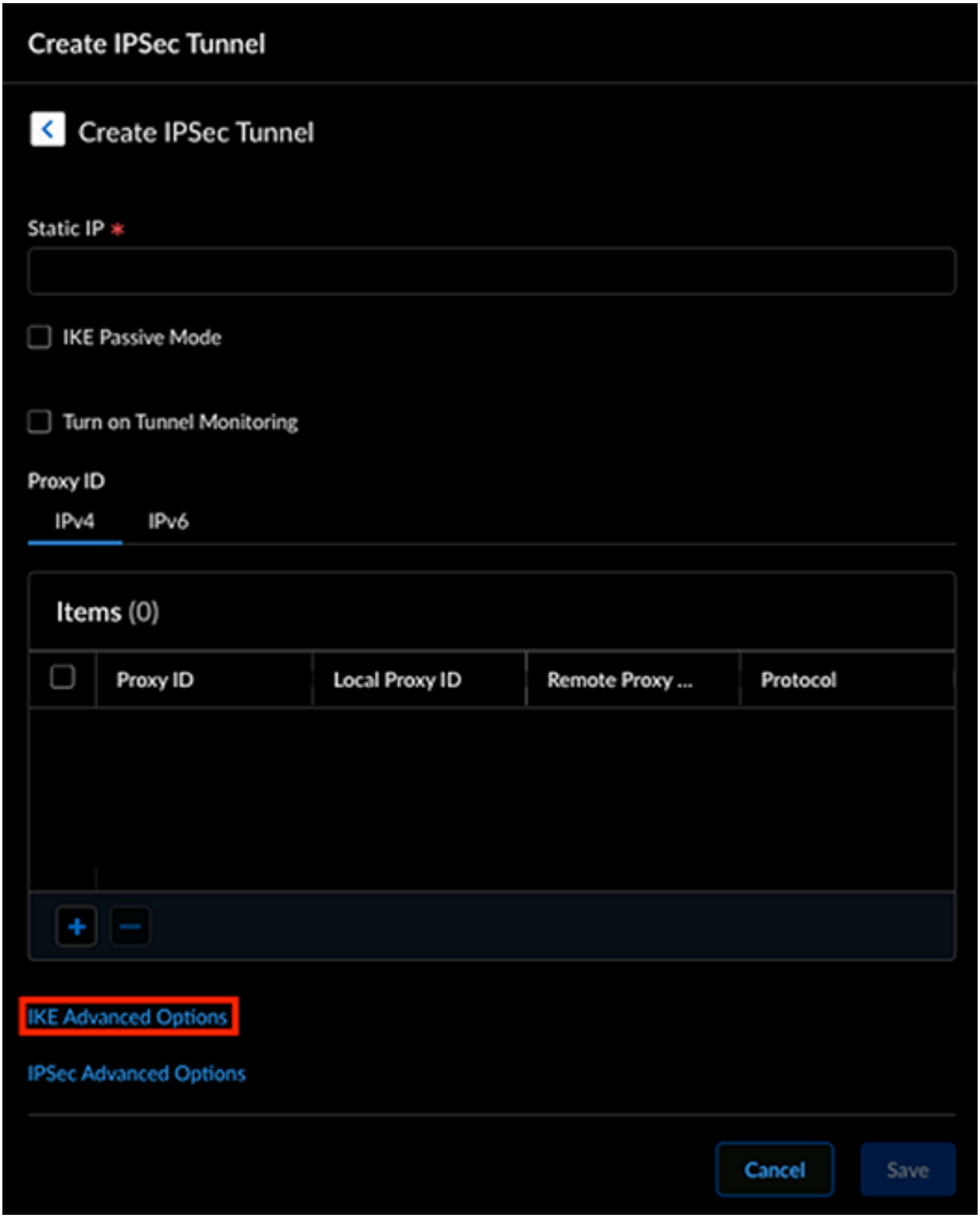
5. In the **Create IPsec Tunnel** screen, click **Create New**.

Figure 3-4: Create IPsec Tunnel



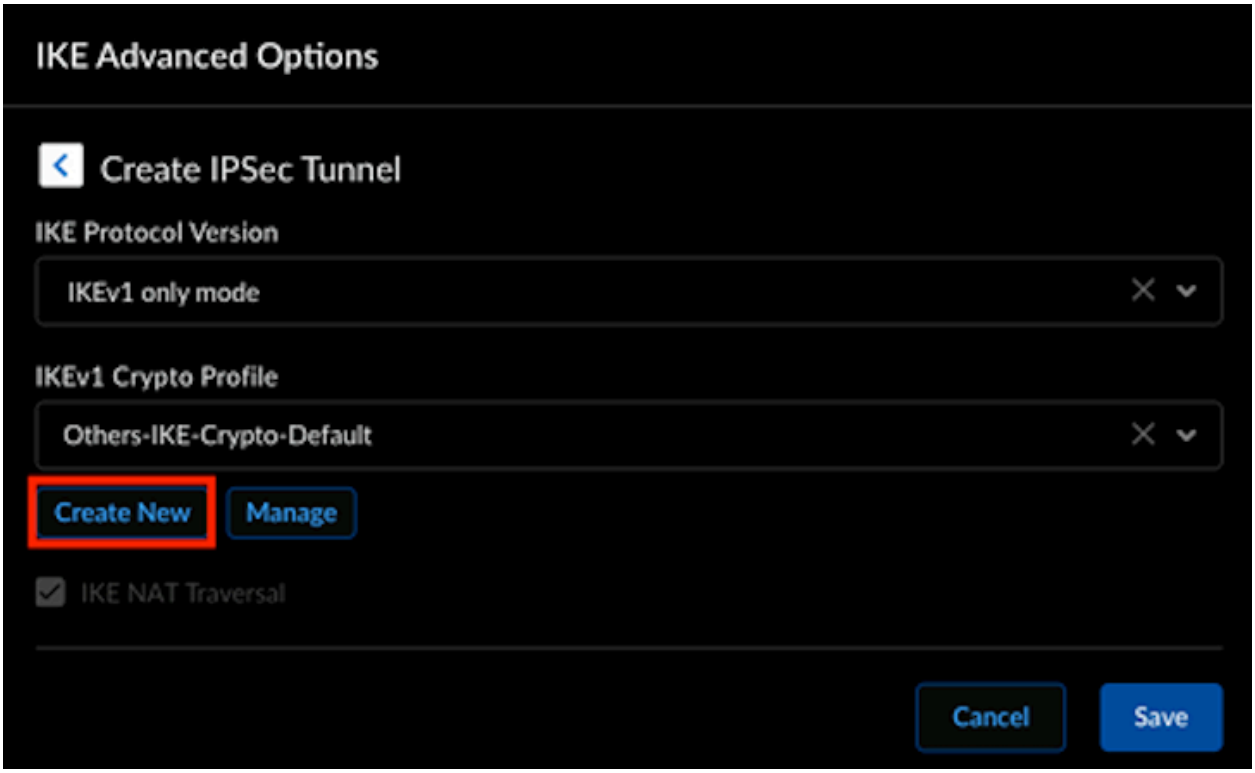
6. Ignore all the mandatory fields and scroll down to the bottom of this screen. Click **IKE Advanced Options**.

Figure 3-5: Scroll to IKE Advanced Options



7. Click **Create New** on the **IKE Advanced Options** screen.

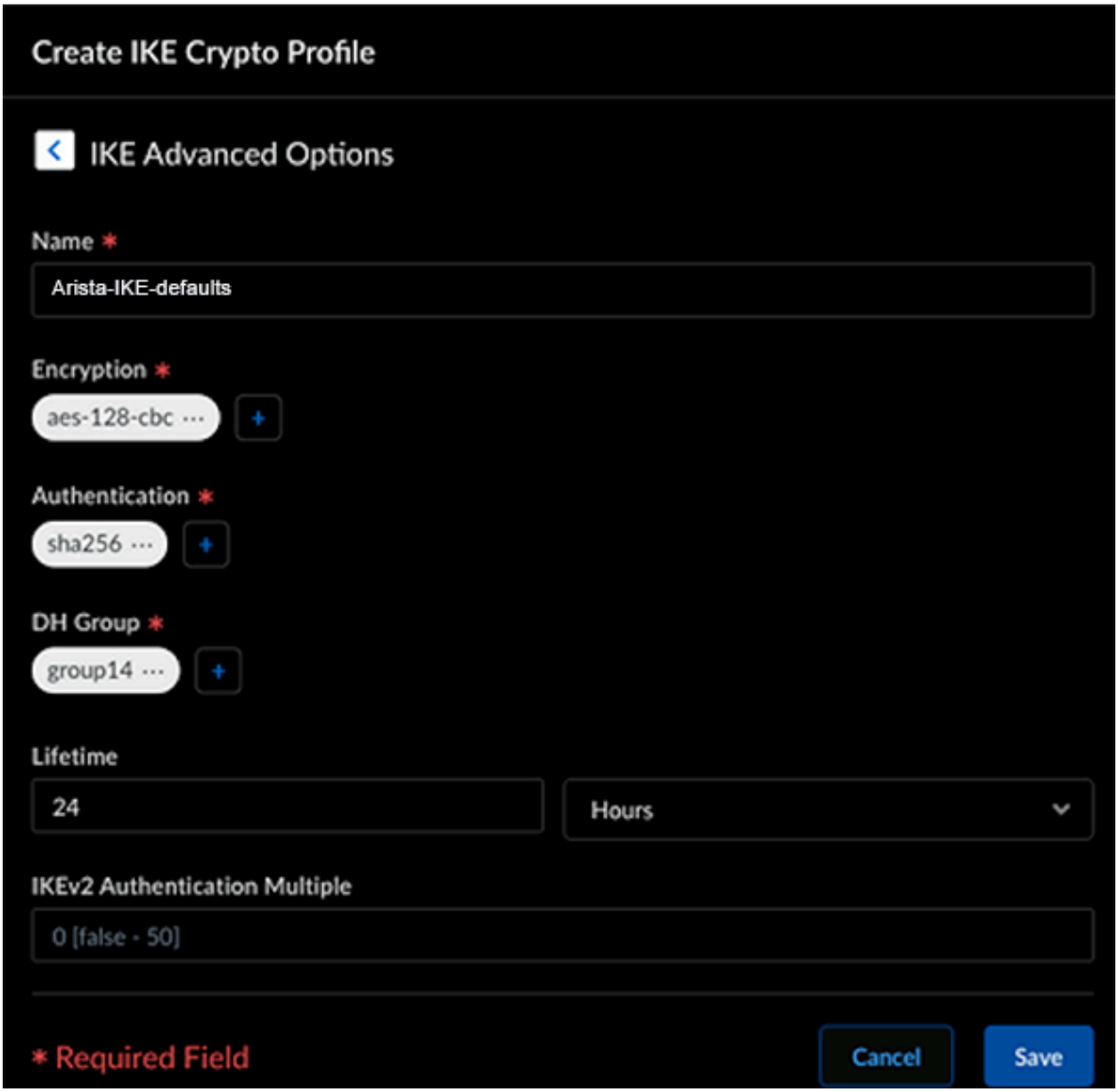
Figure 3-6: IKE Advanced Options



Note: Ignore all the pre-configured options. You must create a new **IKE** profile to be used for the VeloCloud SSE automation.

8. Clicking **Create New** displays the following screen:

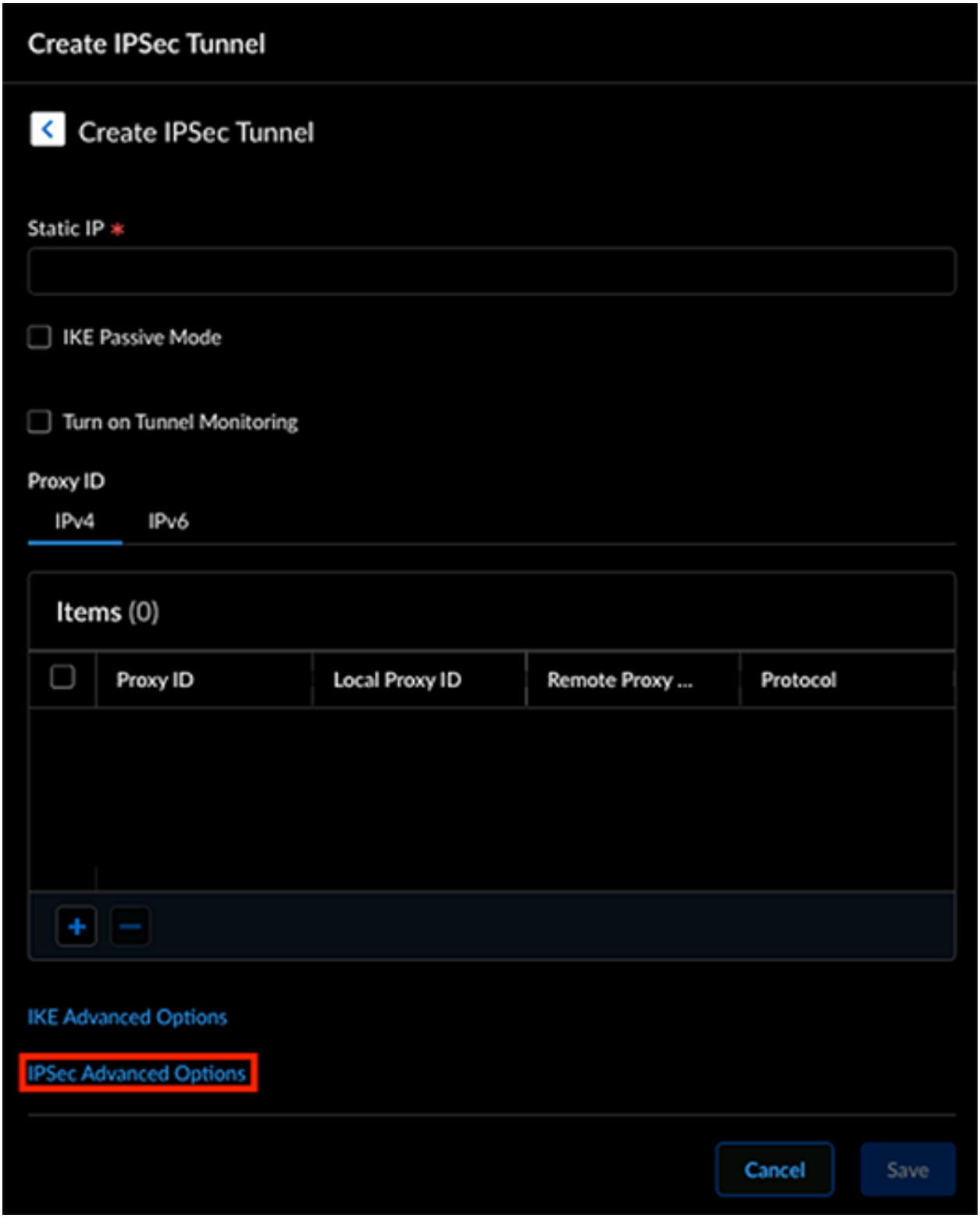
Figure 3-7: Create IKE Crypto Profile



9. Enter the values based on the template provided in the prerequisites section, and then click **Save**.
10. Click **Save** on the **IKE Advanced Options** screen to save the **IKE** profile.
    This step takes you back to the **Create IPsec Tunnel** screen.

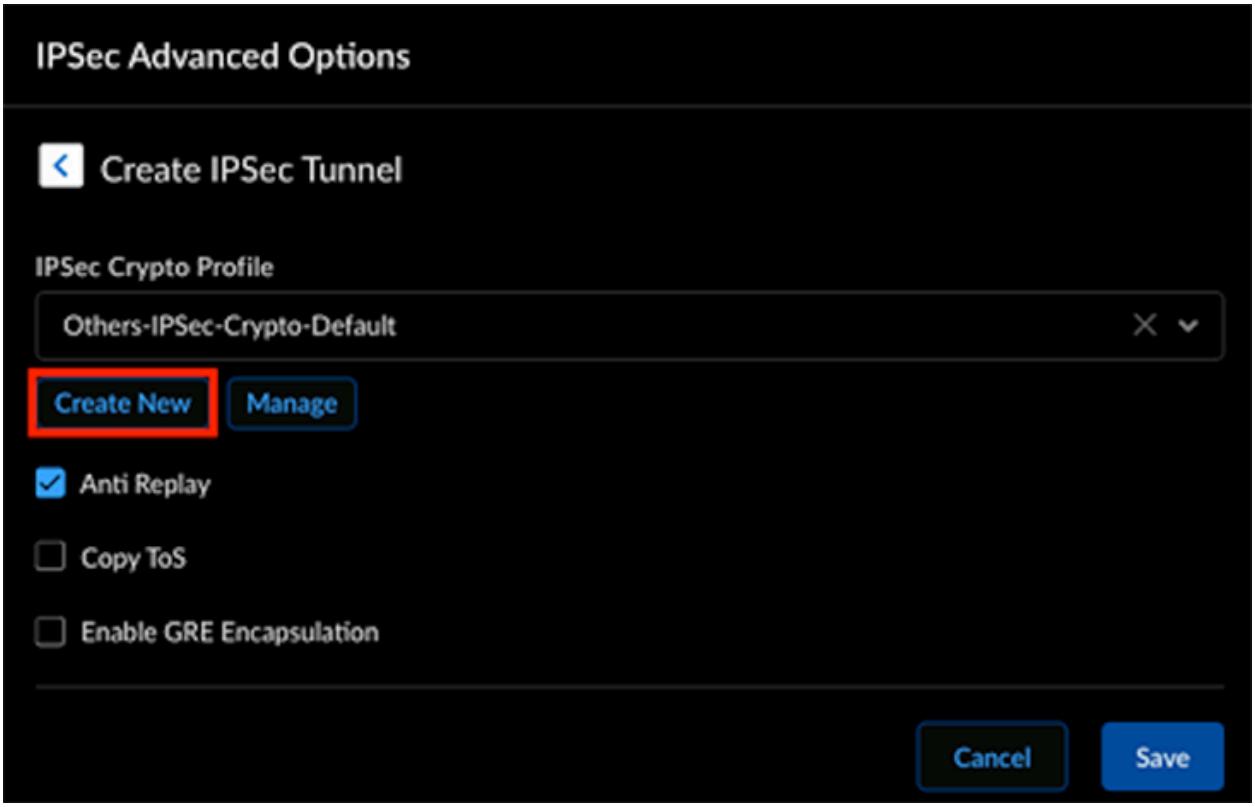
11. On the **Create IPsec Tunnel** screen, click **IPsec Advanced Options** as shown below:

Figure 3-8: Scroll to IPsec Advanced Options



12. Click **Create New** on the **IPsec Advanced Options** screen.

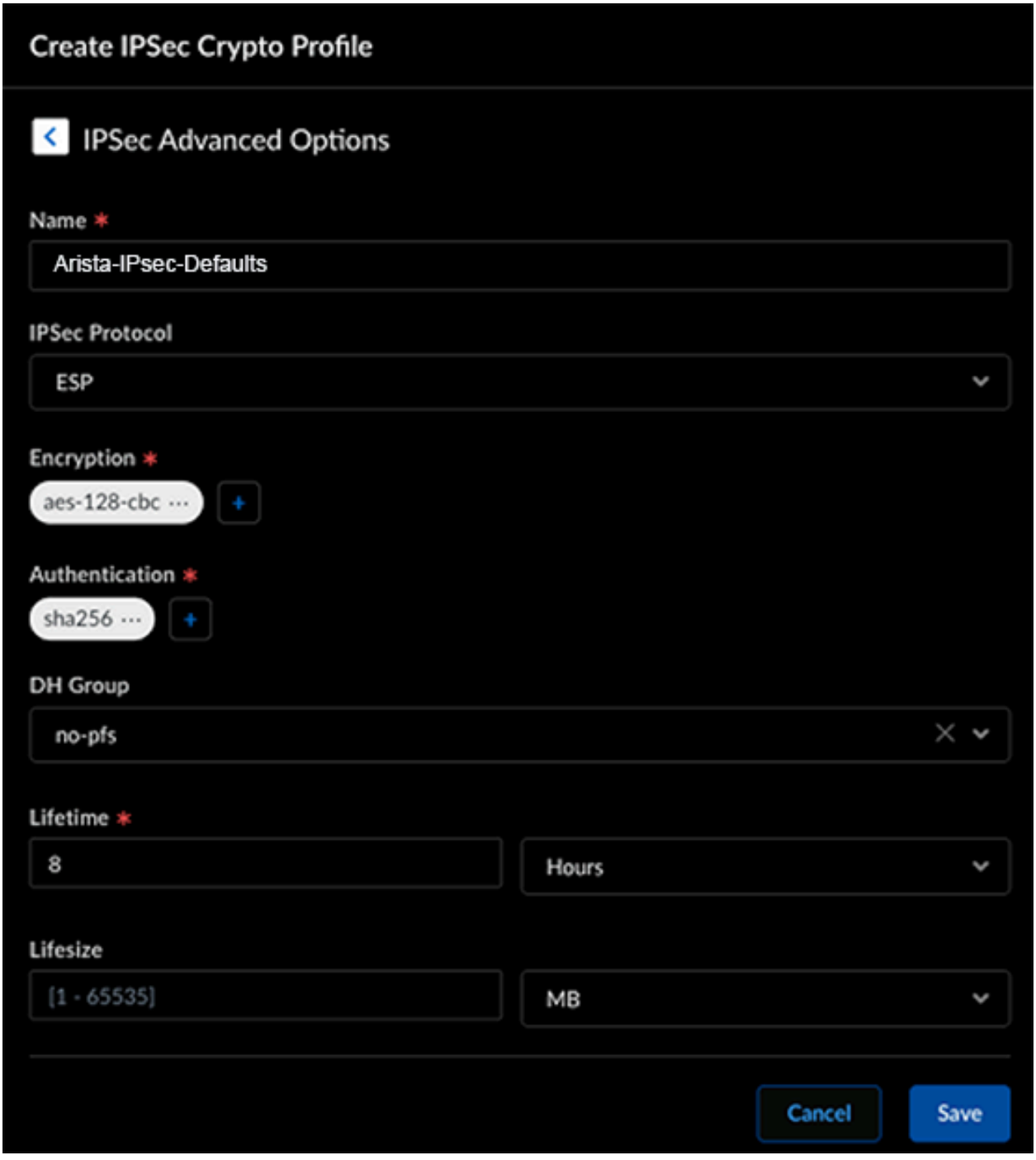
Figure 3-9: IPsec Advanced Options



Note: Ignore all the pre-configured options. You must create a new **IPsec** profile to be used for the VeloCloud SSE automation.

13. Clicking **Create New** displays the following screen:

Figure 3-10: Create IPSec Crypto Profile



14. Enter the values based on the template provided in the prerequisites section, and then click **Save**.
15. Click **Save** on the **IPsec Advanced Options** screen to save the **IPsec** profile.

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).

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:

- Configure SSE for Pan Prisma
- *VeloCloud SD-WAN Configuration Guide SSE for Symantec*

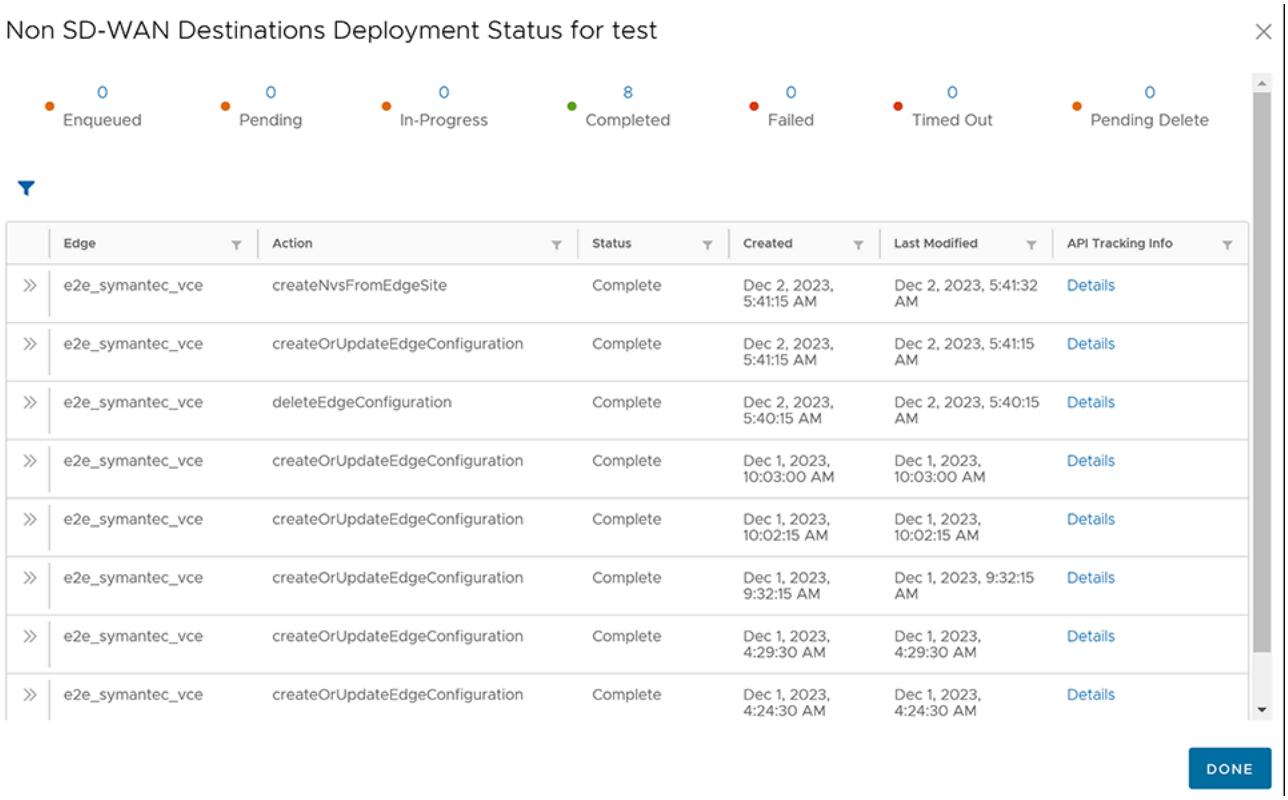
If you wish to edit the existing SSE integration, select the SSE integration from the list on the **Security Service Edge (SSE)** screen, and then click **Edit**. You can also click the SSE integration name link to edit it.

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

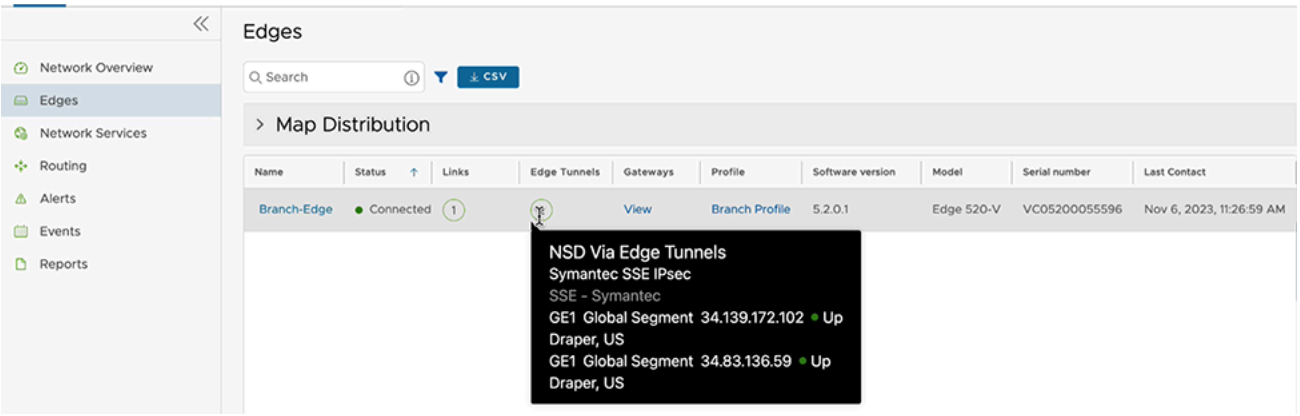


The actions `createOrUpdateEdgeConfiguration` and `deleteEdgeConfiguration` indicate the SSE automation to update the Orchestrator Edge Device settings. The other actions are for third-party automations.

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*