ARISTA

SASE

VeloCloud SD-WAN Global Settings Guide

Version 6.1

Arista.com

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

VeloCloud Global Settings Guide

The VeloCloud Global Settings guide provides information about features residing under the Enterprise Global Settings service. These features are shared across all services.

Chapter 2

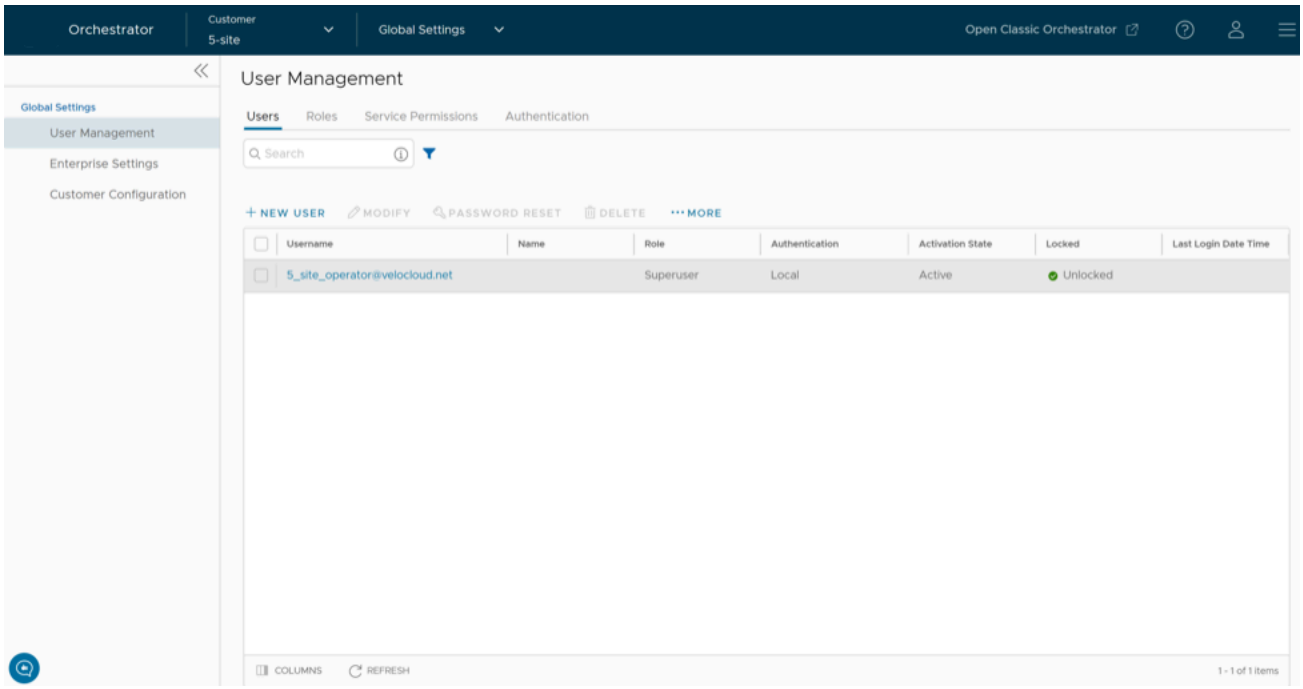
Overview

Considering the number of services available in the **Orchestrator**, the Administration section has evolved from the SD-WAN service into it's own centralized settings to be shared across services. Thus, the original Administration section is split into Global Settings and SD-WAN Settings. All Edge or SD-WAN specific settings are moved to Service Settings within the SD-WAN service, and all Administration related or shared settings across services are moved to the Global Settings service.

The **Enterprise Global Settings** service is located in the **Enterprise Applications** drop-down menu along with **SD-WAN** services. The features under **Global Settings** are shared across all services.

The following features reside under **Enterprise Global Settings**:

Figure 2-1: Global Settings Screen



Selecting the **Global Settings** service displays the **User Management** screen by default.

For additional information on each of these features, see the below topics:

- User Management
- Enterprise Settings
- Configure Customers

Note: This feature is available only for Operator users.

Chapter 3

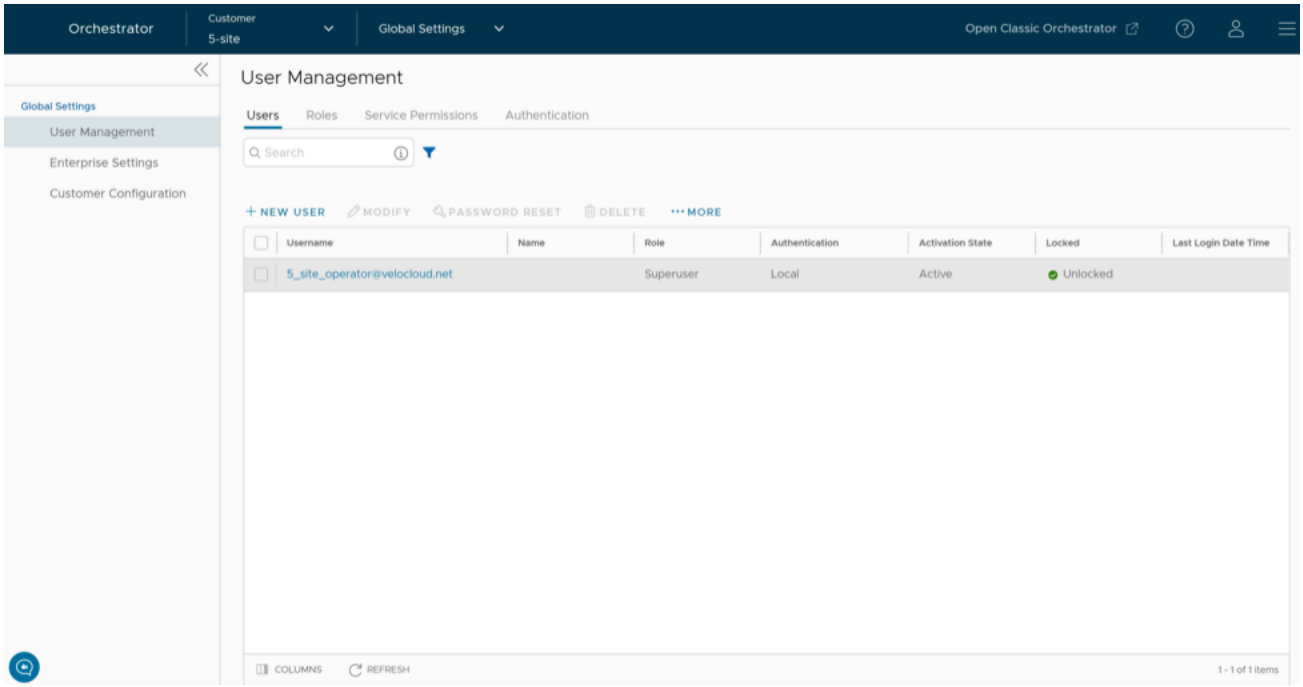
User Management

The **User Management** feature allows you to manage users, their roles, service permissions (formerly known as **Role Customization**), and authentication.

As an Enterprise Superuser, follow the below steps to access the **User Management** screen:

1. In the **Enterprise** portal, on the **Global Navigation** bar, expand the **Enterprise Applications** drop-down menu.
2. Select **Global Settings** service.
3. From the left menu, select **User Management**. The following screen is displayed:

Figure 3-1: User Management Screen



The **User Management** window displays four tabs: **Users**, **Roles**, **Service Permissions**, and **Authentication**.

For additional information on each of these tabs, see:

- Users
- Roles
- Service Permissions
- Authentication

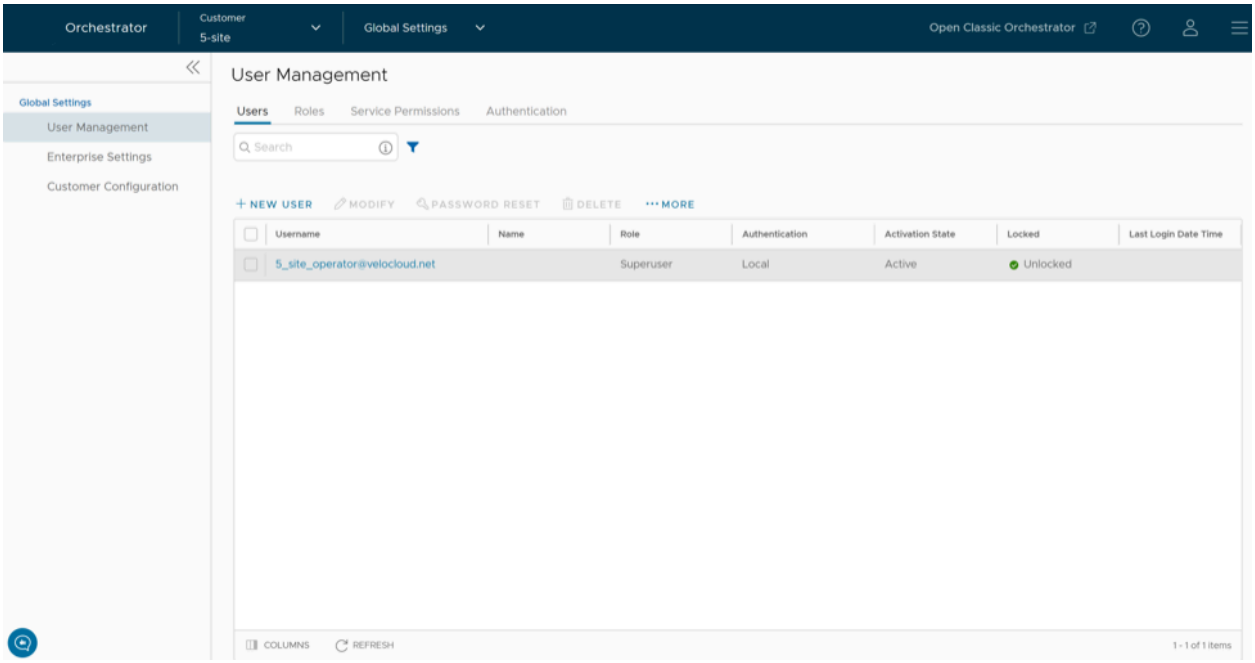
3.1 Users

You can view the existing Admin users. Only Enterprise Superusers can create new Admin users with different roles, and configure API tokens for each Admin user.

To access the **Users** tab:

1. In the **Enterprise** portal, on the **Global Navigation** bar, expand the **Enterprise Applications** drop-down menu.
2. Select **Global Settings** service.
3. From the left menu, select **User Management**. The **Users** tab is displayed by default.

   Figure 3-2: User Management > Users



4. On the **Users** screen, you can perform the following activities:

   Table 1: Users Option Descriptions

Option	Description
New User	Creates a new Admin user. For more information, see Add New User.
Modify	Allows you to modify the properties of the selected Admin user. You can also select the link to the username to modify the properties.
Password Reset	Sends an email to the selected user with a link to reset the password. You can also choose to freeze the account until the password is reset.
Delete	Deletes the selected user. You cannot delete the default users.
More	Select this option, and then select **Download** to download the details of all the users into a file in CSV format.

5. The following are the other options available in the **Users** tab:

Table 2: Users Additional Option Descriptions

Option	Description
Search	Enter a search term to search for the matching text across the table. Use the advanced search option to narrow down the search results.
Columns	Select the columns to be displayed or hidden on the page.
Refresh	Select to refresh the page to display the most current data.

3.1.1 Add New User

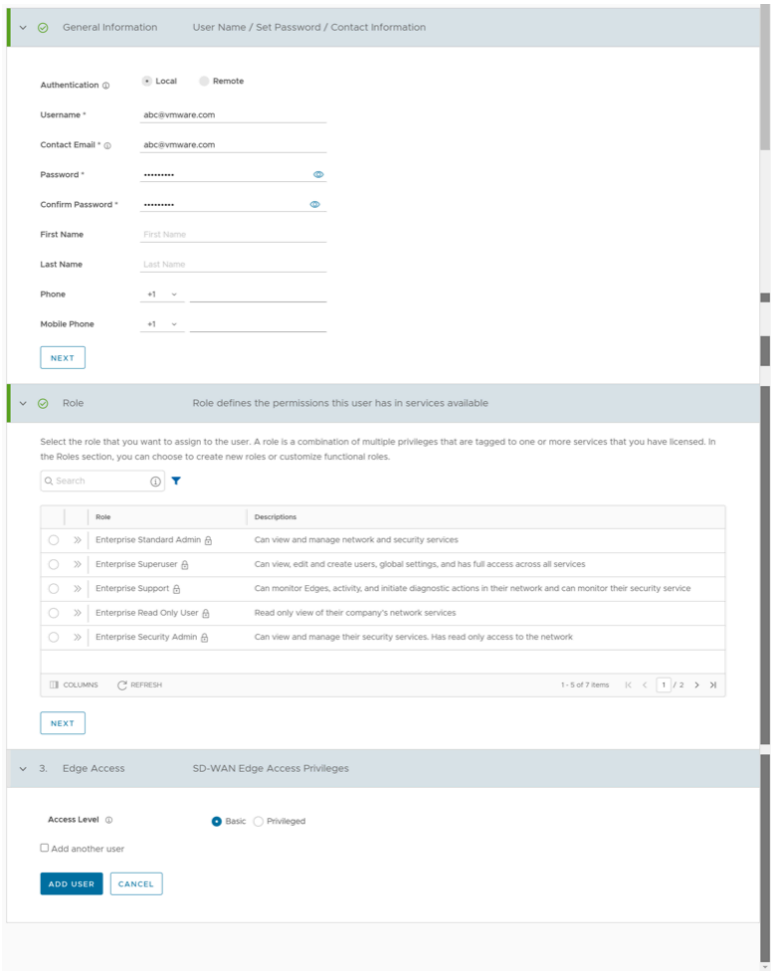
Standard Administrator Superusers and Standard Administrators can create new Admin users. The SSH username is automatically created for the user. To add a new user, perform the following steps:

Note: These steps are valid for all customers, though customers created in a 5.2.0 Orchestrator where they are not assigned to a Partner have certain limitations. These limitations are outlined in an Important note at the end of the article.

1. In the **Enterprise** portal, go to **Enterprise Applications** > **Global Settings**.
2. From the left menu, select **User Management**, and then select the **Users** tab.

3. Select **New User**.

Figure 3-3: User Management > New User



4. Enter the following details for the new user:

> **Note:** The **Next** button is activated only when you enter all the mandatory details in each section.

Table 3: New User Details

Option	Description
General information	Enter the required personal details of the user. **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.
Role	Select a role that you want to assign to the user. For information on roles, see the topic **Roles**.
Edge Access	Choose one of the following options: • **Basic**: Allows you to perform certain basic debug operations such as ping, tcpdump, pcap, remote diagnostics, and so on. • **Privileged**: Grants you the root-level access to perform all basic debug operations along with Edge actions such as restart, deactivate, reboot, hard reset, and shutdown. In addition, you can access linux shell. The default value is **Basic**.

5. Select the **Add another user** check box if you wish to create another user, and then select **Add User**. The new user appears in the **User Management** > **Users** page. Select the link to the user to view or modify the details. As an Enterprise Administrator, you can manage the Roles, Service Permissions, and API Tokens for the Enterprise users.

Note: Enterprise Administrator should manually delete inactive Identity Provider (IdP) users from the Orchestrator to prevent unauthorized access via API Token.

Important: Customers created on a Release 5.2.0 Orchestrator who are not assigned to a Partner are automatically configured for Single Sign On (SSO) using Cloud Services Platform (CSP) as the Identity Provider (IdP). As a result:

- New administrators are created by an administrator with a Superuser role through the CSP portal.
- There is one exception to this: the customer is permitted one administrator account with Native authentication (username/password) to allow them to access their portal in the event there is an issue with CSP authentication.
- For additional information about using CSP as an IdP in SD-WAN, see the topic *Configure CSP for Single Sign On*.

3.1.2 API Tokens

You can access the Orchestrator APIs using tokens instead of session-based authentication. As an Enterprise Superuser, you can manage the API tokens. You can create multiple API tokens for a user.

Note:

- For Enterprise Read Only users and MSP Business Specialist users, token-based authentication is not activated.

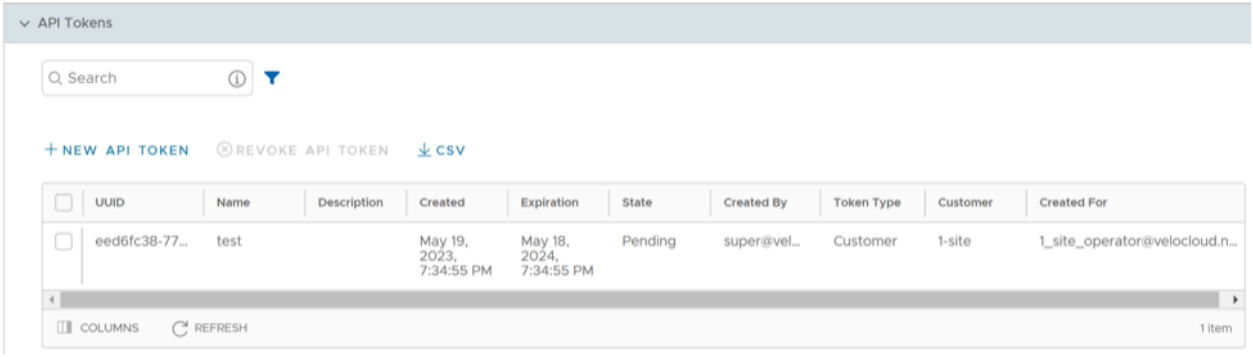
- Enterprise Superuser should manually delete inactive Identity Provider (IdP) users from the Orchestrator to prevent unauthorized access via API Token.

The users can create, revoke, and download the tokens based on their roles.

To manage the API tokens:

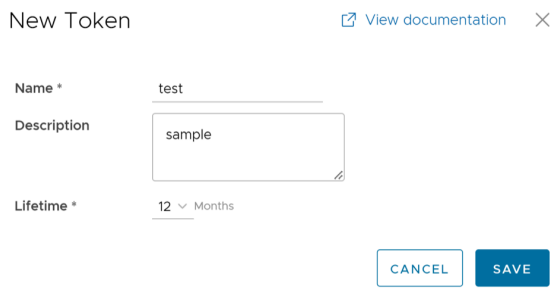
1. In the **Enterprise** portal, on the **Global Navigation** bar, expand the **Enterprise Applications** drop-down menu.
2. Select **Global Settings** service.
3. Navigate to **User Management** > **Users**.
4. Select a user and select **Modify** or select the link to the username. Go to the **API Tokens** section.

   Figure 3-4: Modifying API Tokens



5. Select **New API Token**.

   Figure 3-5: New API Tokens



6. In the **New Token** window, enter a **Name** and **Description** for the token, and then choose the **Lifetime** from the drop-down menu.
7. Select **Save**. The new token is displayed in the **API Tokens** table. Initially, the status of the token is displayed as **Pending**. Once you download it, the status changes to **Enabled**.
8. To download the token, select the token, and then select **Download API Token**.
9. To deactivate a token, select the token, and then select **Revoke API Token**. The status of the token is displayed as **Revoked**.
10. Select **CSV** to download the complete list of API tokens in a `.csv` file format.

11. When the Lifetime of the token is over, the status changes to **Expired**.

> **Note:** Only the user who is associated with a token can download it and after downloading, the ID of the token alone is displayed. You can download a token only once. After downloading the token, the user can send it as part of the Authorization Header of the request to access the Orchestrator API.

The following example shows a sample snippet of the code to access an API.

```
curl -k -H "Authorization: Token <Token>" -X POST https://vco/portal/ -d '{ "id": 1, "jsonrpc":
 "2.0", "method": "enterprise/getEnterpriseUsers", "params": { "enterpriseId": 1 }}'
```

The following are the other options available in the **API Tokens** section:

Table 4: API Tokens Option Descriptions

Option	Description
Search	Enter a search term to search for the matching text across the table. Use the advanced search option to narrow down the search results.
Columns	Select the columns to be displayed or hidden on the page.
Refresh	Select to refresh the page to display the most current data.

3.2 Roles

The Orchestrator consists of two types of roles.

> **Note:** Starting from the 5.1.0 release, **Functional Roles** are renamed as **Privileges**, and **Composite Roles** are renamed as **Roles**.

The roles are categorized as follows:

- **Privileges** – Privileges are a set of roles relevant to a functionality. A privilege can be tagged to one or more of the following services: SD-WAN and Global Settings. Users require privileges to carry out business processes. For example, a Customer support role in SD-WAN is a privilege required by an SD-WAN user to carry out various support activities. Every service defines such privileges based on its supported business functionality.
- **Roles**– The privileges from various categories can be grouped to form a role. By default, the following roles are available for a Customer:

Table 5: Role Services

Role	SD-WAN Service	Global Settings Service
Enterprise Standard Admin	SD-WAN Enterprise Admin	Global Settings Enterprise Admin
Enterprise Superuser	SD-WAN Enterprise Superuser	Global Settings Enterprise Superuser
Enterprise Support	SD-WAN Enterprise Support	Global Settings Enterprise Support
Enterprise Read Only User	SD-WAN Enterprise Read Only	Global Settings Enterprise Read Only
Enterprise Security Admin	SD-WAN Security Enterprise Admin	Global Settings Enterprise Admin
Enterprise Security Read Only	SD-WAN Security Enterprise Read Only	Global Settings Enterprise Read Only
Enterprise Network Admin	SD-WAN Enterprise Admin	Global Settings Enterprise Admin

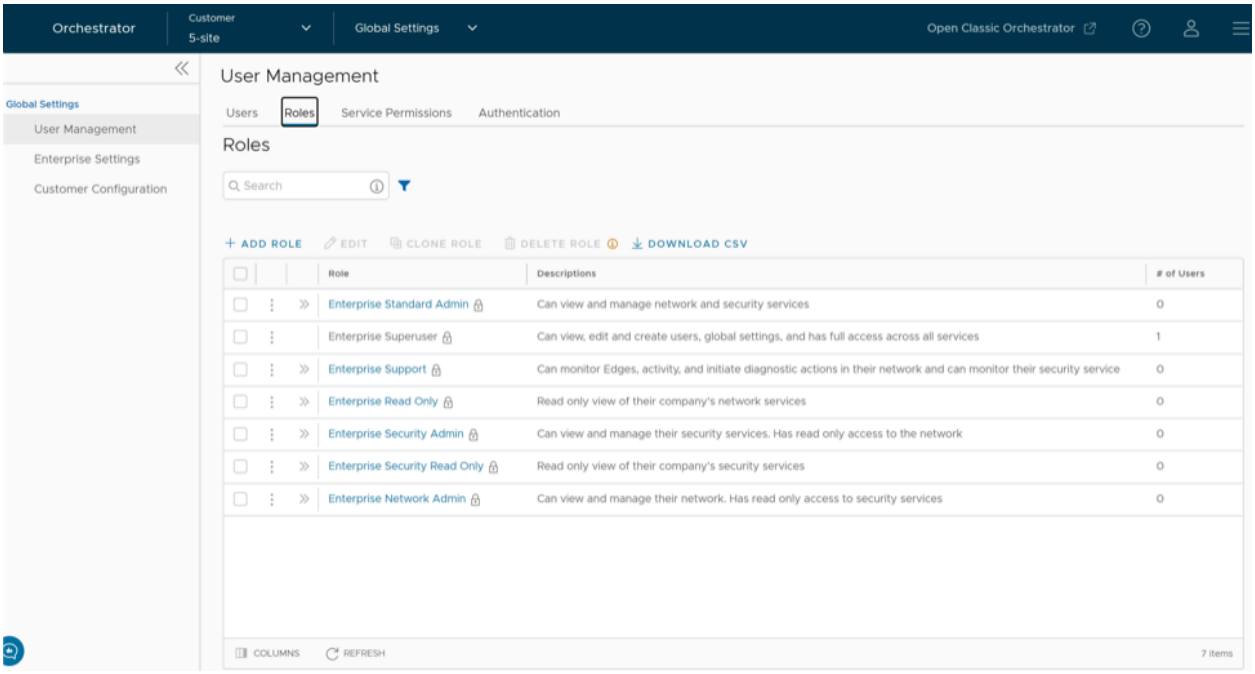
If required, you can customize the privileges of these roles. For additional information, see Service Permissions.

As a Customer, you can view the list of existing standard roles and their corresponding descriptions. You can add, edit, clone, or delete a new role. However, you cannot edit or delete a default role.

To access the **Roles** tab:

1. In the **Enterprise** portal, on the **Global Navigation** bar, expand the **Enterprise Applications** drop-down menu.
2. Select **Global Settings** service.
3. From the left menu, select **User Management**, and then select the **Roles** tab. The following screen appears:

   Figure 3-6: Roles



4. On the **Roles** screen, you can perform the following activities:

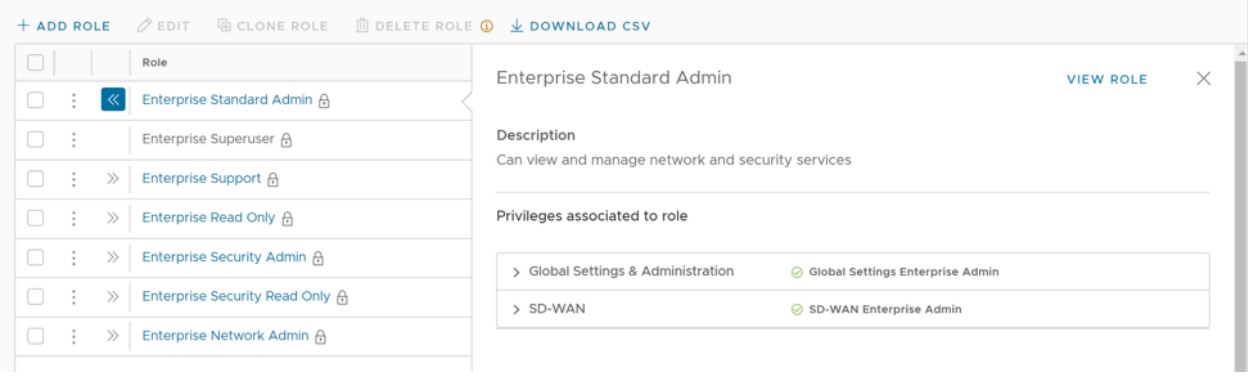
Table 6: Roles Option Descriptions

Option	Description
Add Role	Creates a new custom role. For additional information, see Add Role.
Edit	Allows you to edit only the custom roles. You cannot edit the default roles. Also, you cannot edit or view the settings of a Superuser.
Clone Role	Creates a new custom role, by cloning the existing settings from the selected role. You cannot clone the settings of a Superuser.
Delete Role	Deletes the selected role. You cannot delete the default roles. You can delete only custom composite roles. Ensure that you have removed all the users associated with the selected role, before deleting the role.
Download CSV	Downloads the details of the user roles into a file in CSV format.

Note: You can also access the **Edit**, **Clone Role**, and **Delete Role** options from the vertical ellipsis of the selected Role.

5. Select the **Open** icon " **>>**" displayed before the Role link, to view additional details about the selected Role, as shown below:

Figure 3-7: Role Details



6. Select the **View Role** link to view the privileges associated to the selected role for the activated services.

Note: By default, only **Global Settings & Administration** service is activated for a Customer. Only an Operator can activate an additional service.

7. The following are the other options available in the **Roles** tab:

Table 7: Roles Additional Option Descriptions

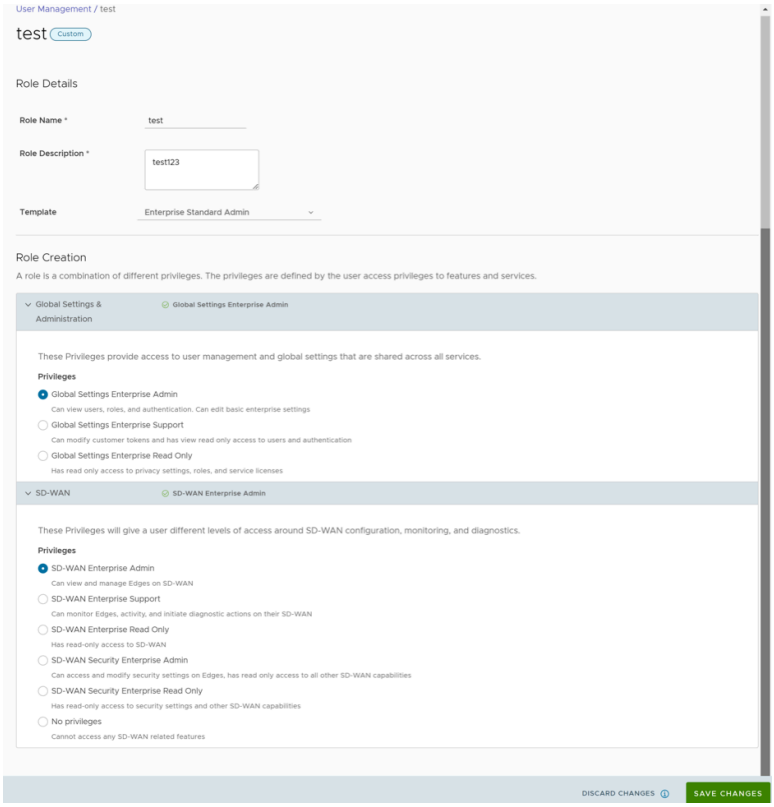
Option	Description
Search	Enter a search term to search for the matching text across the table. Use the advanced search option to narrow down the search results.
Columns	Select the columns to be displayed or hidden on the page.
Refresh	Select to refresh the page to display the most current data.

3.2.1 Add Role

To add a new role for a Customer, perform the following steps:

1. In the **Enterprise** portal, on the **Global Navigation** bar, expand the **Enterprise Applications** drop-down menu.
2. Select **Global Settings** service.
3. From the left menu, select **User Management**, and then select the **Roles** tab.
4. Select **Add Role**.

Figure 3-8: Adding Role



5. Enter the following details for the new custom role:

Table 8: New Custom Role Options

Option	Description
Role Details	
Role Name	Enter a name for the new role.
Role Description	Enter a description for the role.
Template	Optionally, select an existing role as template from the drop-down list. The privileges of the selected template are assigned to the new role.
Role Creation	
Global Settings & Administration	These privileges provide access to user management and global settings that are shared across all services. Choosing one of the privileges is mandatory. By default, **Global Settings Enterprise Read Only** is selected.
SD-WAN	These privileges provide the Enterprise Administrator with different levels of access around SD-WAN configuration, monitoring, and diagnostics. You can optionally choose an SD-WAN privilege. The default value is **No Privileges**.

Note: The **Role Creation** section displays the privileges only for which the Customer has licenses.

6. Select **Save Changes**. The new custom role appears in the **User Management** > **Roles** page. Select the link to the custom role to view the settings.

3.3 Service Permissions

Service Permissions allow an Administrator to granularly define actions (Read, Create, Update, and Delete) assigned to each Privilege (such as Cloud Security Service and Customer Segment configuration) within a Privilege Bundle.

Note: Starting from the 5.1.0 release, **Role Customization** is renamed to **Service Permissions**.

You can customize only the permissions and not the roles. When you customize a permission, the changes would impact the roles associated with it. For additional information, see Roles.

Only an Operator Superuser can activate the Service Permissions for an Enterprise Superuser. If the **Service Permissions** option is not available for you, contact your Operator.

The **Service Permissions** are applied to the privileges as follows:

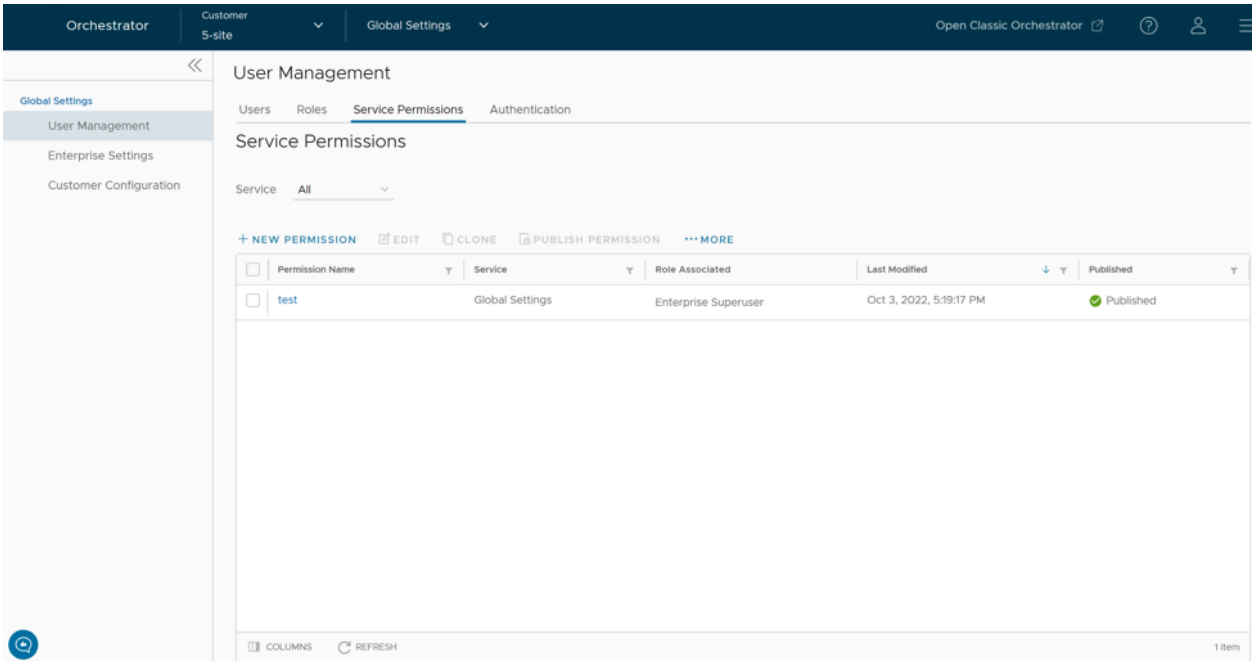
- The customizations done at the **Enterprise** level override the **Partner** or **Operator** level customizations.
- The customizations done at the **Partner** level override the **Operator** level customizations.
- Only when there are no customizations done at the **Partner** level or **Enterprise** level, the customizations made by the Operator are applied globally across all users in the **Orchestrator**.

Note: For information on user privileges, see List of User Privileges.

To access the **Service Permissions** tab:

1. In the **Enterprise** portal, on the **Global Navigation** bar, expand the **Enterprise Applications** drop-down menu.
2. Select **Global Settings** service.
3. From the left menu, select **User Management**, and then select the **Service Permissions** tab. The following screen appears:

   Figure 3-9: Service Permissions



4. On the **Service Permissions** screen, you can perform the following activities:

Table 9: Service Permissions Option Descriptions

Option	Description
Service	Select the service from the drop-down menu. The available services are: • **All** • **Global Settings** • **SD-WAN** • **Edge Compute** Custom service permissions, if any, associated with the selected service are displayed. By default, all of the custom service permissions are displayed.
New Permission	Allows you to create a new permission. For additional information, see New Permission.
Edit	Allows you to edit the settings of the selected permission. You can also select the link to the **Permission Name** to edit the settings.
Clone	Allows you to create a copy of the selected permission.
Publish Permission	Applies the customization available in the selected package to the existing permission. This option modifies the privileges only at the current level. If there are customizations available at the Operator level or a lower level for the same role, then the lower level takes precedence.
More	Allows you to select from the following additional options: • **Delete**: Deletes the selected permission. You cannot delete a permission if it is already in use. **Note:** A permission can only be deleted if it is in a draft mode. The **Delete** option is deactivated for a published permission. If you want to delete a published permission, you must reset the permission to system default, which changes it to draft mode and activates the **Delete** option for the permission. • **Download JSON**: Downloads the list of permissions into a file in JSON format. • **Upload Permission**: Allows you to upload a JSON file of a customized permission. • **Reset to System Default**: Allows you to reset the current published permissions to default settings. Only the permissions applied to the privileges in the current level (Operator, Partner, or Enterprise) of the Orchestrator are reset to the default settings. If Operators or Customers have customized their privileges in the Partner or Enterprise level in the Orchestrator, those settings remain the same.

5. The following are the other options available in the **Service Permissions** tab:

Table 10: Service Permissions Additional Options

Option	Description
Columns	Select and select the columns to be displayed or hidden on the page. **Note:** The **Role Associated** column displays the Roles using the same Privilege Bundle.
Refresh	Select to refresh the page to display the most current data.

Note:

- The Orchestrator does not support customization of multiple privilege bundles.
- Service Permissions are version dependent, and a service permission created on an Orchestrator using an earlier software release will not be compatible with an Orchestrator using a later release. For example, a service permission created on an Orchestrator that is running Release 3.4.x does not work properly if the Orchestrator is upgraded to a 4.x Release. Also, a service permission created on an Orchestrator running Release 3.4.x does not work properly when the Orchestrator is upgraded to 4.x.x Release. In such cases, the user must review and recreate the service permission for the newer release to ensure proper enforcement of all roles.

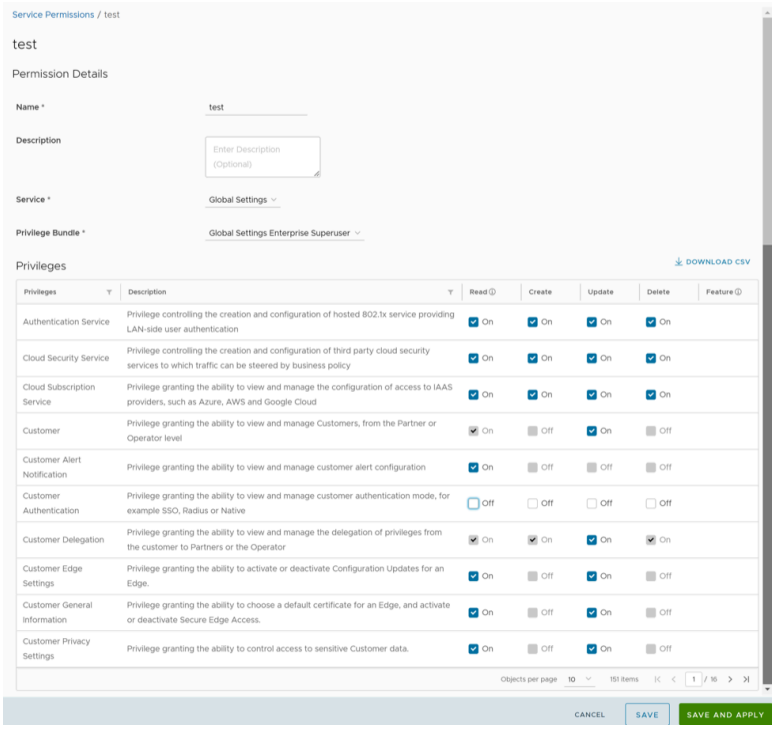
3.3.1 New Permission

You can customize the privileges and apply them to the existing permission in the Orchestrator.

To add a new permission, perform the following steps:

1. In the **Enterprise** portal, on the **Global Navigation** bar, expand the **Enterprise Applications** drop-down menu.
2. Select **Global Settings** service.
3. From the left menu, select **User Management**, and then select the **Service Permissions** tab.
4. Select **New Permission**. The following screen appears:

   Figure 3-10: New Service Permissions



5. Enter the following details to create a new permission:

Table 11: New Permission Option Descriptions

Option	Description
Name	Enter an appropriate name for the permission. **Note:** The permission name must be unique within the Orchestrator it is hosted upon.
Description	Enter a description. This field is optional.
Service	Select a service from the drop-down menu. The available services are: • **Global Settings** • **SD-WAN** • **Edge Compute**
Privilege Bundle	Select a privilege bundle from the drop-down menu. The privileges are populated depending on the selected **Service**.
Privileges	Displays the list of privileges based on the selected **Privilege Bundle**. You can edit only those privileges that are eligible for customization.

6. Select **Download CSV** to download the list of all privileges, their description, and associated actions, into a file in CSV format.
7. Select **Save** to save the new permission. Select **Save and Apply** to save and publish the permission.

Note: The **Save** and **Save and Apply** buttons are activated only after you modify the permissions.

The new permission is displayed on the **Service Permissions** page.

3.3.2 List of User Privileges

This section lists all the user privileges available in the **Enterprise** portal.

Below is a table listing the user privileges. The columns in the table indicate the following:

- **Allow Privilege** – Do the privileges have allow access?
- **Deny Privilege** – Do the privileges have deny access?
- **Customizable** – Is the privilege available for customization in the **Service Permissions** tab along with the **Create**, **Read**, **Update**, **Delete** customizations?

Note: The features that can be completely customized by an Enterprise Superuser have been listed in a separate table at the end of this topic.

Table 12: Permission Information

Navigation Path in the Enterprise Portal	Name of the Tab	Elements in the Tab	Name of the Privilege	Description	Allow Privilege	Deny Privilege	Customizable
Monitor > **Edges** > **Select Edge**	Overview						
			Read Edge	Grants ability to view and manage Edge objects and their properties in general	Yes	No	No
		Top Applications Top Categories Top Operating Systems Top Sources	Read Edge	Grants ability to view and manage Edge objects and their properties in general	Yes	No	No
			View Flow Stats	Grants ability to view collected flow statistics	Yes	Yes	Yes
	Sources		Read Edge	Grants ability to view and manage Edge objects and their properties in general	Yes	No	No
			View Edge Sources	Grants ability to view Monitor Edge Sources tab	Yes	Yes	Yes
		Devices	View User Identifiable Flow Stats	Grants ability to view potentially user identifiable flow source attributes	Yes	Yes	Yes
			Create Client Device Read Client Device	Controls visibility to unique identifiers (IP or MAC address) of LAN-side client devices	Yes	No	No
		Change Hostname	Update Client Device Delete Client Device Manage Client Device				
		Operating Systems	Create Client User Read Client User Update Client User Delete Client User Manage Client User	Controls visibility to potentially Personal Identifiable Information(PII) in flow statistics	Yes	No	No
	Applications Sources Destinations		Read Edge	Grants ability to view and manage Edge objects and their properties in general	Yes	No	No
			View Flow Stats	Grants ability to view collected flow statistics	Yes	Yes	Yes
	Events from this Edge		Read Customer Event	Grants ability to view customer level events	Yes	No	No
	Remote Actions		Read Remote Actions	Grants access to view and execute remote actions	No	Yes	Yes

Navigation Path in the Enterprise Portal	Name of the Tab	Elements in the Tab	Name of the Privilege	Description	Allow Privilege	Deny Privilege	Customizable
	Remote Actions Generate Diagnostic Bundle Remote Diagnostics		Read Diagnostics	Controls creation of and access to diagnostics bundles, both Edge and Gateway. Combine with Edge and Gateway privileges to control access to each type individually	Yes	Yes	Yes
	Generate Diagnostic Bundle		Create Diagnostic Bundle		No	Yes	Yes
	Remote Diagnostics		Read Remote Diagnostics	Privilege granting access to view and execute remote diagnostics	No	Yes	Yes
Monitor	Edges		Read Edge	Grants ability to view and manage Edge objects and their properties in general	Yes	No	No
		Edge Cluster	Read Edge Cluster	Controls the ability to create and configure Edge Clusters	No	Yes	Yes
	Network Services		Read Network Service	Grants ability to view and manage services with the Network Services configuration block	Yes	No	No
		Non SD-WAN Destinations via Gateway Non SD-WAN Destinations via Edge	Read Customer Event	Grants ability to view customer level events	Yes	No	No
		Non SD-WAN Destinations via Gateway Non SD-WAN Destinations via Edge	Read Non SD-WAN Destination via Gateway	Grants ability to view and manage Non SD-WAN Destinations via Gateway and Non SD-WAN Destinations via Edge	No	Yes	Yes
		BGP Gateway Neighbor State	Read Network Service	Grants ability to view and manage services with the Network Services configuration block	Yes	No	No
		BGP Edge Neighbor State	Read Edge	Grants ability to view and manage Edge objects and their properties in general	Yes	No	No
		Edge VNFs	Read VNF Network Service	Grants ability to manage VNF Network Services	No	Yes	Yes
		Edge Cluster	Read Edge Cluster	Controls the ability to create and configure Edge Clusters	No	Yes	Yes
	Routing		Read Network Addressing	Grants ability to view and manage address block configuration in the legacy Network profile mode	Yes	No	No
			Read Edge	Grants ability to view and manage Edge objects and their properties in general	Yes	No	No

Navigation Path in the Enterprise Portal	Name of the Tab	Elements in the Tab	Name of the Privilege	Description	Allow Privilege	Deny Privilege	Customizable
			View Customer Routing	Grants ability to view the customer Routing	Yes	No	No
	Alerts		Create Customer Alert	Grants ability to view and manage customer alert configuration and generated alerts	Yes	No	No
			Read Customer Alert			Yes	Yes
			Update Customer Alert				
			Delete Customer Alert			No	No
			Manage Customer Alert				
	Events		Create Customer Event	Grants ability to view customer level events	Yes	No	No
			Read Customer Event				
			Update Customer Event				
			Delete Customer Event				
			Manage Customer Event				
	Reports		Update Customer	Grants ability to view and manage Customers, from the Partner or Operator level	Yes	Yes	Yes
			Read Customer			No	No
	Firewall	Firewall Logging	View Firewall Logs	Grants ability to view collected firewall logs	Yes	Yes	Yes
			Read Edge	Grants ability to view and manage Edge objects and their properties in general	Yes	No	No
			Read Customer Event	Grants ability to view customer level events	Yes	No	No
Configure > **Edge** > **Select Edge**	Edge Overview		Edge Overview	Controls ability to view or modify Edge overview page	No	Yes	Yes
		Properties	Create Edge Overview Properties	Controls ability to view or change items within the properties section of the Edge overview page	No	Yes	Yes
			Read Edge Overview Properties			No	No
			Update Edge Overview Properties			Yes	Yes
			Delete Edge Overview Properties				
		Name	Read Edge Overview Properties Name	Controls ability to view or change Edge name on the Edge overview page	No	Yes	Yes
			Update Edge Overview Properties Name				

Navigation Path in the Enterprise Portal	Name of the Tab	Elements in the Tab	Name of the Privilege	Description	Allow Privilege	Deny Privilege	Customizable
		Description	Read Edge Overview Properties Description Update Edge Overview Properties Description	Controls ability to view or change Edge description on the Edge overview page	No	Yes	Yes
		Enable Alerts	Read Edge Overview Properties Enable Alerts Update Edge Overview Properties Enable Alerts	Controls ability to view or change Edge alert configuration on the Edge overview page	No	Yes	Yes
		Authentication Mode	Read Edge Overview Properties Auth Mode Update Edge Overview Properties Auth Mode	Controls ability to view or change Edge PKI configuration on the Edge overview page	No	Yes	Yes
			Read Customer PKI Update Customer PKI	Grants ability to view and manage enterprise PKI settings	Yes	No	No
		Serial Number	Read Edge Overview Properties Serial Number Update Edge Overview Properties Serial Number	Controls ability to view or change Edge serial number, prior to activation, on the Edge overview page	No	Yes	Yes
		Generate New Activation Key	Read Edge Overview Properties Activation Expiration Update Edge Overview Properties Activation Expiration	Controls ability to view or change the activation key expiration period on the Edge overview page	No	Yes	Yes
		Send Activation Email button	Create Edge Overview Properties Activation Email Read Edge Overview Properties Activation Email	Controls ability to generate an activation email on the Edge overview page	No	Yes	Yes
		Local Credentials	Read Overview Properties Local Credentials Update Overview Properties Local Credentials	Grants ability to view and configure Edge local credentials	No	Yes	Yes

Navigation Path in the Enterprise Portal	Name of the Tab	Elements in the Tab	Name of the Privilege	Description	Allow Privilege	Deny Privilege	Customizable
		View	Read Edge Update Edge	Grants ability to view and manage Edge objects and their properties in general	Yes	No	No
			Read Customer Keys Update Customer Keys	Grants ability to view and manage enterprise security keys such as Edge administrator credentials and IPSEC keys	Yes	Yes	Yes
		License	Read License Update License	Grants ability to view and manage Edge licensing	Yes	Yes	Yes
		Profile	Create Edge Overview Profile	Controls visibility and control of Edges assigned profile on the Edge overview page	No	Yes	Yes
			Read Edge Overview Profile			No	No
			Update Edge Overview Profile			Yes	Yes
			Delete Edge Overview Profile				
		RMA Reactivation	Create Edge	Grants ability to view and manage Edge objects and their properties in general	Yes	Yes	Yes
	Device						
		Authentication Settings	Create Edge Device Authentication Settings	Controls ability to view or change Edge Device Authentication Settings	No	Yes	Yes
			Read Edge Device Authentication Settings				
			Update Edge Device Authentication Settings				
			Delete Edge Device Authentication Settings				
		DNS Settings	Update Edge Device DNS Settings	Controls ability to view or change Edge Device DNS Settings	No	Yes	Yes
		Netflow Settings	Create Edge Device Netflow Settings	Controls ability to view or change Edge Device Netflow Settings	No	Yes	Yes
			Read Edge Device Netflow Settings				
			Update Edge Device Netflow Settings				
			Delete Edge Device Netflow Settings				
		LAN-Side NAT Rules	Update Edge Device LAN-Side NAT Rules	Controls ability to view or change Edge Device LAN-Side NAT Rules	No	Yes	Yes

Navigation Path in the Enterprise Portal	Name of the Tab	Elements in the Tab	Name of the Privilege	Description	Allow Privilege	Deny Privilege	Customizable
		Voice Quality Monitoring Settings	Read Edge Device VQM Settings Update Edge Device VQM Settings	Controls ability to view or change Edge Device VQM Settings	No	Yes	Yes
		Syslog Settings	Read Edge Device Syslog Settings Update Edge Device Syslog Settings	Controls ability to view or change Edge Device Syslog Settings	No	Yes	Yes
		Static Route Settings	Update Edge Device Static Route Settings	Controls ability to view or change Edge Device Static Route Settings	No	Yes	Yes
		ICMP Probes	Read Edge Device ICMP Probes Update Edge Device ICMP Probes	Controls ability to view or change Edge Device ICMP Probes	No	Yes	Yes
		ICMP Responders	Read Edge Device ICMP Responders Update Edge Device ICMP Responders	Controls ability to view or change Edge Device ICMP Responders	No	Yes	Yes
		VRRP Settings	Update Edge Device VRRP Settings	Controls ability to view or change Edge Device VRRP Settings	No	Yes	Yes
		Cloud VPN	Read Edge Device Cloud VPN Update Edge Device Cloud VPN	Controls ability to view or change Edge Device Cloud VPN	No	Yes	Yes
		BFD Rules	Update Edge Device BFD Rules	Controls ability to view or change Edge Device BFD Rules	No	Yes	Yes
		BGP Settings	Read Edge Device BGP Settings Update Edge Device BGP Settings	Controls ability to view or change Edge Device BGP Settings	No	Yes	Yes
		Multicast Settings	Read Edge Device Multicast Settings Update Edge Device Multicast Settings	Controls ability to view or change Edge Device Multicast Settings	No	Yes	Yes
		Cloud Security Service	Read Edge Device Cloud Security Service Update Edge Device Cloud Security Service	Controls ability to view or change Edge Device Cloud Security Service	No	Yes	Yes

Navigation Path in the Enterprise Portal	Name of the Tab	Elements in the Tab	Name of the Privilege	Description	Allow Privilege	Deny Privilege	Customizable
		Gateway Handoff Assignment	Update Edge Device Gateway Handoff Assignment	Controls ability to view or change Edge Device Gateway Handoff Assignment	No	Yes	Yes
		High Availability	Create Edge Device High Availability	Controls ability to view or change Edge Device High Availability	No	Yes	Yes
			Read Edge Device High Availability				
			Update Edge Device High Availability				
			Delete Edge Device High Availability				
			Enable HA Standby Pair	Grants ability to configure standby HA	No	Yes	Yes
			Enable HA Cluster	Grants ability to configure HA Clustering	No	Yes	Yes
			Enable HA VRRP Pair	Grants ability to configure VRRP HA	No	Yes	Yes
		Configure VLAN	Read Edge Device Settings	Controls ability to view or change Edge Device Settings	No	Yes	Yes
		Management IP	Read Edge Device Management IP	Controls ability to view or change Edge Device Management IP	No	Yes	Yes
			Update Edge Device Management IP				
		Device Settings	Create Edge Device Settings	Controls ability to view or change Edge Device Settings	No	Yes	Yes
			Read Edge Device Settings				
			Update Edge Device Settings				
			Delete Edge Device Settings				
		Interface Settings	Update Edge Device Interface Settings	Controls ability to view or change Edge Device Interface Settings	No	Yes	Yes
		WAN Settings	Update Edge Device WAN Settings	Controls ability to view or change Edge Device WAN Settings	No	Yes	Yes
		Security VNF	Update Edge Device Security VNF	Controls ability to view or change Edge Device Security VNF	No	Yes	Yes
		Wi-Fi Radio Settings	Create Edge Device Wi-Fi Settings	Controls ability to view or change Edge Device Wi-Fi Settings	No	Yes	Yes
			Read Edge Device Wi-Fi Settings				
			Update Edge Device Wi-Fi Settings				

Navigation Path in the Enterprise Portal	Name of the Tab	Elements in the Tab	Name of the Privilege	Description	Allow Privilege	Deny Privilege	Customizable
			Delete Edge Device Wi-Fi Settings				
		Multi-Source QoS	Read Edge Device Cloud VPN QoS Settings	Controls ability to view or change Edge Device Cloud VPN QoS Settings	No	Yes	Yes
			Update Edge Device Cloud VPN QoS Settings				
		TACACS Settings	Create Network Service	Grants ability to view and manage services with the Network Services configuration block	Yes	Yes	Yes
			Read Network Service			No	No
			Update Network Service			Yes	Yes
			Delete Network Service				
			Create Customer Keys	Grants ability to view and manage enterprise security keys such as Edge administrator credentials and IPSEC keys	Yes	Yes	Yes
			Read Customer Keys				
			Update Customer Keys				
			Delete Customer Keys				
			Manage Customer Keys			No	No
		L2 Settings	Update Edge Device L2 Settings	Controls ability to view or change Edge Device L2 Settings	No	Yes	Yes
		SNMP Settings	Create Edge Device SNMP Settings	Controls ability to view or change Edge Device SNMP Settings	No	Yes	Yes
			Read Edge Device SNMP Settings				
			Update Edge Device SNMP Settings				
			Delete Edge Device SNMP Settings				
		NTP	Read Edge Device NTP Settings	Controls ability to view or change Edge Device NTP Settings	No	Yes	Yes
			Update Edge Device NTP Settings				
		Visibility Mode	Update Edge Device Config Visibility Mode	Controls ability to view or change Edge Device Config Visibility Mode	No	Yes	Yes
		Analytics Settings	Read Edge	Grants ability to view and manage Edge objects and their properties in general	Yes	No	No
			Update Edge				

Navigation Path in the Enterprise Portal	Name of the Tab	Elements in the Tab	Name of the Privilege	Description	Allow Privilege	Deny Privilege	Customizable
	Business Policy		Edge Business Policy	Controls ability to view or change Edge business policy page	No	Yes	Yes
		SD-WAN Overlay Rate Limit	Read Edge Business Policy Rate Limit	Controls the ability to read and update the rate limiting business policy feature	No	Yes	Yes
			Update Edge Business Policy Rate Limit				
		SD-WAN Overlay Rate Limit SD-WAN Traffic Class and Weight Mapping	Read Edge	Grants ability to view and manage Edge objects and their properties in general	Yes	No	No
			Read Customer Profile	Grants ability to view and edit enterprise configuration profiles	Yes	Yes	Yes
	Firewall		Edge Firewall	Controls ability to view or change Edge firewall page	No	Yes	Yes
		Firewall Logging Syslog Forwarding Stateful Firewall	Configure Edge Firewall Logging	Grants ability to configure Edges level firewall logging	No	Yes	Yes
			Read Edge	Grants ability to view and manage Edge objects and their properties in general	Yes	No	No
		Syslog Forwarding	View Syslog Forwarding	Grants ability to see Syslog forwarding	No	Yes	Yes
			Read Edge	Grants ability to view and manage Edge objects and their properties in general	Yes	No	No
		Stateful Firewall Settings Network & Flood Protection Settings Edge Access	Create Edge Firewall Edge Access	Privilege granting or denying visibility and control of an Edges Stateful Firewall Settings, Network & Flood Protection Settings and Edge Access on the Edge firewall page	No	Yes	Yes
			Read Edge Firewall Edge Access				
			Update Edge Firewall Edge Access				
			Delete Edge Firewall Edge Access				
	Events from this Edge		Read Customer Event	Grants ability to view customer level events	Yes	No	No
	Remote Actions		Read Remote Actions	Privilege granting access to view and execute remote actions	No	Yes	Yes
	Remote Actions Generate Diagnostic Bundle Remote Diagnostics		Read Diagnostics	Controls creation of and access to diagnostics bundles, both Edge and Gateway. Combine with Edge and Gateway privileges to control access to each type individually	Yes	Yes	Yes
	Generate Diagnostic Bundle		Create Diagnostic Bundle		No	Yes	Yes

Navigation Path in the Enterprise Portal	Name of the Tab	Elements in the Tab	Name of the Privilege	Description	Allow Privilege	Deny Privilege	Customizable
	Remote Diagnostics		Read Remote Diagnostics	Grants access to view and execute remote diagnostics	No	Yes	Yes
Configure > **Profiles** > **Select Profile**	Profile Overview		Profile Overview	Controls ability to view or change profile overview page	No	Yes	Yes
		Description	Create Profile Overview Description	Controls ability to view or change Profile Overview Description	No	Yes	Yes
			Read Profile Overview Description			No	No
			Update Profile Overview Description			Yes	Yes
			Delete Profile Overview Description				
		Local Credentials	Read Overview Properties Local Credentials	Grants ability to view and configure Edge local credentials	No	Yes	Yes
			Update Overview Properties Local Credentials				
	Device						
		Authentication Settings	Create Profile Device Authentication Settings	Controls ability to view or change Profile Device Authentication Settings	No	Yes	Yes
			Read Profile Device Authentication Settings				
			Update Profile Device Authentication Settings				
			Delete Profile Device Authentication Settings				
		DNS Settings	Update Profile Device DNS Settings	Controls ability to view or change Profile Device DNS Settings	No	Yes	Yes
		Netflow Settings	Create Profile Device Netflow Settings	Controls ability to view or change Profile Device Netflow Settings	No	Yes	Yes
			Read Profile Device Netflow Settings				
			Update Profile Device Netflow Settings				
			Delete Profile Device Netflow Settings				
		LAN-Side NAT Rules	Update Profile Device LAN-Side NAT Rules	Controls ability to view or change Profile Device LAN-Side NAT Rules	No	Yes	Yes

Navigation Path in the Enterprise Portal	Name of the Tab	Elements in the Tab	Name of the Privilege	Description	Allow Privilege	Deny Privilege	Customizable
		Voice Quality Monitoring Settings	Read Profile Device VQM Settings Update Profile Device VQM Settings	Controls ability to view or change Profile Device VQM Settings	No	Yes	Yes
		Syslog Settings	Read Profile Device Syslog Settings Update Profile Device Syslog Settings	Controls ability to view or change Profile Device Syslog Settings	No	Yes	Yes
		Cloud VPN	Read Profile Device Cloud VPN Update Profile Device Cloud VPN	Controls ability to view or change Profile Device Cloud VPN	No	Yes	Yes
		BFD Rules	Update Profile Device BFD Rules	Controls ability to view or change Profile Device BFD Rules	No	Yes	Yes
		OSPF Areas	Read Profile Device OSPF Settings Update Profile Device OSPF Settings	Controls ability to view or change Profile Device OSPF Settings	No	Yes	Yes
		BGP Settings	Read Profile Device BGP Settings Update Profile Device BGP Settings	Controls ability to view or change Profile Device BGP Settings	No	Yes	Yes
		Multicast Settings	Read Profile Device Multicast Settings Update Profile Device Multicast Settings	Controls ability to view or change Profile Device Multicast Settings	No	Yes	Yes
		Cloud Security Service	Read Profile Device Cloud Security Service Update Profile Device Cloud Security Service	Controls ability to view or change Profile Device Cloud Security Service	No	Yes	Yes
		Gateway Handoff Assignment	Update Profile Device Gateway Handoff Assignment	Controls ability to view or change Profile Device Gateway Handoff Assignment	No	Yes	Yes
		Configure VLAN	Read Profile Device Settings	Controls ability to view or change Profile Device Settings	No	Yes	Yes
		Management IP	Read Profile Device Management IP Update Profile Device Management IP	Controls ability to view or change Profile Device Management IP	No	Yes	Yes

Navigation Path in the Enterprise Portal	Name of the Tab	Elements in the Tab	Name of the Privilege	Description	Allow Privilege	Deny Privilege	Customizable
		Device Settings	Create Profile Device Settings Read Profile Device Settings Update Profile Device Settings Delete Profile Device Settings	Controls ability to view or change Profile Device Settings	No	Yes	Yes
		Interface Settings	Update Profile Device Interface Settings	Controls ability to view or change Profile Device Interface Settings	No	Yes	Yes
		Wi-Fi Radio Settings	Create Profile Device Wi-Fi Settings Read Profile Device Wi-Fi Settings Update Profile Device Wi-Fi Settings Delete Profile Device Wi-Fi Settings	Controls ability to view or change Profile Device Wi-Fi Settings	No	Yes	Yes
		L2 Settings	Update Profile Device L2 Settings	Controls ability to view or change Profile Device L2 Settings	No	Yes	Yes
		Multi-Source QoS	Read Profile Device Cloud VPN QoS Settings Update Profile Device Cloud VPN QoS Settings	Controls ability to view or change Profile Device Cloud VPN QoS Settings	No	Yes	Yes
		SNMP Settings	Create Profile Device SNMP Settings Read Profile Device SNMP Settings Update Profile Device SNMP Settings Delete Profile Device SNMP Settings	Controls ability to view or change Profile Device SNMP Settings	No	Yes	Yes
		NTP	Read Profile Device NTP Settings Update Profile Device NTP Settings	Controls ability to view or change Profile Device NTP Settings	No	Yes	Yes
		Visibility Mode	Update Profile Device Config Visibility Mode	Controls ability to view or change Profile Device Config Visibility Mode	No	Yes	Yes

Navigation Path in the Enterprise Portal	Name of the Tab	Elements in the Tab	Name of the Privilege	Description	Allow Privilege	Deny Privilege	Customizable
		Analytics Settings	Read Profile Device Analytics Settings	Controls ability to view or change Profile Device Analytics Settings	No	Yes	Yes
			Update Profile Device Analytics Settings				
			Create Profile Device Network Settings	Controls ability to view or change Profile Device Network Settings	No	Yes	Yes
			Read Profile Device Network Settings				
			Update Profile Device Network Settings				
			Delete Profile Device Network Settings				
	Business Policy		Profile Business Policy	Controls ability to view or change profile business policy page	No	Yes	Yes
		SD-WAN Overlay Rate Limit	Read Profile Business Policy Rate Limit	Controls the ability to read and update the rate limiting business policy feature	No	Yes	Yes
			Update Profile Business Policy Rate Limit				
	Firewall		Profile Firewall	Controls ability to view or change profile firewall page	No	Yes	Yes
		Firewall Logging Syslog Forwarding Stateful Firewall	Configure Profile Firewall Logging	Grants ability to configure profile level firewall logging	No	Yes	Yes
			Read Edge	Grants ability to view and manage Edge objects and their properties in general	Yes	No	No
			Read Edge	Grants ability to view and manage Edge objects and their properties in general	Yes	No	No
		Stateful Firewall Settings Network & Flood Protection Settings Edge Access	Create Edge Firewall Edge Access	Controls visibility and control of Stateful Firewall Settings, Network & Flood Protection Settings, and Edge Access on the profile firewall page	No	Yes	Yes
			Read Edge Firewall Edge Access			No	No
			Update Edge Firewall Edge Access			Yes	Yes
			Delete Edge Firewall Edge Access				
Configure	Edges		Create Edge	Grants ability to view and manage Edge objects and their properties in general	Yes	Yes	Yes
			Read Edge			No	No
			Update Edge				
			Delete Edge			Yes	Yes
			Manage Edge			No	No

Navigation Path in the Enterprise Portal	Name of the Tab	Elements in the Tab	Name of the Privilege	Description	Allow Privilege	Deny Privilege	Customizable
			Read Customer Profile	Grants ability to view and edit enterprise configuration profiles	Yes	Yes	Yes
	New Edge >	Authentication	Create Customer PKI	Grants ability to view and manage enterprise PKI settings	Yes	No	No
	Select Edge/ Edges >	Local Credentials	Read Overview Properties Local Credentials	Grants ability to view and configure Edge local credentials	No	Yes	Yes
			Update Overview Properties Local Credentials				
	Select Edge/ Edges >	Assign Profile	Assign Edge Profile	Grants ability to assign profiles to Edges	No	Yes	Yes
	Select Edge/ Edges >	Update Pre-Notifications	Update Edge Overview Properties Enable Alerts	Controls ability to view or change Edge alert configuration on the Edge overview page	No	Yes	Yes
	Select Edge/ Edges >	Assign Edge License					
	Select Edge/ Edges >	Update Customer Alerts					
		Edge Cluster	Read Edge Cluster	Grants ability to view Edge clusters	No	Yes	Yes
		Create Cloud Edge	Create DMZ Gateway	Grants ability to create DMZ Gateways	No	Yes	Yes
	Profiles		Create Customer Profile	Grants ability to view and edit enterprise configuration profiles	Yes	Yes	Yes
			Read Customer Profile				
			Update Customer Profile				
			Delete Customer Profile				
			Manage Customer Profile			No	No
		Duplicate Profile	Duplicate Customer Profile	Grants ability to edit duplicate customer level profiles	No	Yes	Yes
			Create Profile	Grants access to view and manage profiles at any level	No	Yes	Yes
			Read Profile				
			Update Profile				
			Delete Profile				
	Object Groups		Create Object Group	Grants ability to manage Object Group	Yes	Yes	Yes
			Read Object Group				
			Update Object Group				
			Delete Object Group				
			Manage Object Group			No	No
			Read Customer Profile	Grants ability to view and edit enterprise configuration profiles	Yes	Yes	Yes

Navigation Path in the Enterprise Portal	Name of the Tab	Elements in the Tab	Name of the Privilege	Description	Allow Privilege	Deny Privilege	Customizable
	Segments/ Networks		Create Network Addressing	Grants ability to view and manage address block configuration in the legacy Network profile mode	Yes	Yes	Yes
			Read Network Addressing			No	No
			Update Network Addressing			Yes	Yes
			Delete Network Addressing				
			Manage Network Addressing			No	No
			Create Customer Segment	Grants ability to view and manage the creation of segments and their assignment to configuration profiles	No	Yes	Yes
			Read Customer Segment				
			Update Customer Segment				
			Delete Customer Segment				
	Overlay Flow Control		Create Overlay Flow Control	Grants ability to view and manage data and configuration presented on the Overlay Flow Control page	No	Yes	Yes
			Read Overlay Flow Control				
			Update Overlay Flow Control				
			Delete Overlay Flow Control				
			Read Customer Profile	Grants ability to view and edit enterprise configuration profiles	Yes	Yes	Yes
			Update Customer Profile				
	Network Services		Create Network Service	Grants ability to view and manage services with the Network Services configuration block	Yes	Yes	Yes
			Read Network Service			No	No
			Update Network Service			Yes	Yes
			Delete Network Service				
			Manage Network Service			No	No
			Create Customer Keys	Grants ability to view and manage enterprise security keys such as Edge administrator credentials and IPSEC keys	Yes	Yes	Yes
			Read Customer Keys				
			Update Customer Keys				
			Read Customer Profile	Grants ability to view and edit enterprise configuration profiles	Yes	Yes	Yes
		Edge Cluster	Create Edge Cluster	Controls the ability to create and configure Edge Clusters	No	Yes	Yes
			Read Edge Cluster				

Navigation Path in the Enterprise Portal	Name of the Tab	Elements in the Tab	Name of the Privilege	Description	Allow Privilege	Deny Privilege	Customizable
			Update Edge Cluster				
			Delete Edge Cluster				
		Cloud VPN Hubs	Create VPN Hub Network Service	Grants ability to manage VPN Hubs as Network Services	No	Yes	Yes
			Read VPN Hub Network Service				
			Update VPN Hub Network Service				
			Delete VPN Hub Network Service				
		Non SD-WAN Destinations via Gateway Non SD-WAN Destinations via Edge	Create Non SD-WAN Destination via Gateway	Grants ability to view and manage Non SD-WAN Destinations via Gateway and Non SD-WAN Destinations via Edge	No	Yes	Yes
			Read Non SD-WAN Destination via Gateway				
			Update Non SD-WAN Destination via Gateway				
			Delete Non SD-WAN Destination via Gateway				
		Cloud Security Service	Create Cloud Security Service	Controls creation and configuration of third party cloud security services to which the traffic can be steered by business policy	No	Yes	Yes
			Read Cloud Security Service				
			Update Cloud Security Service				
			Delete Cloud Security Service				
		VNFs	Create VNF Network Service	Grants ability to manage VNF Network Services	No	Yes	Yes
			Read VNF Network Service				
			Update VNF Network Service				
			Delete VNF Network Service				
		VNF Licenses	Create VNF License Network Service	Grants ability to manage VNF licenses with Network Services	No	Yes	Yes
			Read VNF License Network Service				
			Update VNF License Network Service				
			Delete VNF License Network Service				
		DNS Services	Create DNS Network Service	Controls the ability to create and configure DNS services for use in profiles	No	Yes	Yes
			Read DNS Network Service				
			Update DNS Network Service				

Navigation Path in the Enterprise Portal	Name of the Tab	Elements in the Tab	Name of the Privilege	Description	Allow Privilege	Deny Privilege	Customizable
			Delete DNS Network Service				
		Private Network Names	Create Private Network Name Network Service	Grants ability to manage Private Network Name with Network Services	No	Yes	Yes
			Read Private Network Name Network Service				
			Update Private Network Name Network Service				
			Delete Private Network Name Network Service				
		Authentication Services	Create Authentication Service	Controls the creation and configuration of hosted 802.1x service providing LAN-side user authentication	No	Yes	Yes
			Read Authentication Service				
			Update Authentication Service				
			Delete Authentication Service				
		TACACS Services	Create Network Service	Grants ability to view and manage services with the Network Services configuration block	Yes	Yes	Yes
			Read Network Service			No	No
			Update Network Service			Yes	Yes
			Delete Network Service				
			Create Customer Keys	Grants ability to view and manage enterprise security keys such as Edge administrator credentials and IPSEC keys	Yes	Yes	Yes
			Read Customer Keys				
			Update Customer Keys				
			Delete Customer Keys				
			Manage Customer Keys			No	No
		Cloud Subscriptions	Create Cloud Subscription Service	Grants ability to view and manage the configuration of access to IAAS providers, such as Azure, AWS and Google Cloud	No	Yes	Yes
			Read Cloud Subscription Service				
			Update Cloud Subscription Service				
			Delete Cloud Subscription Service				

Navigation Path in the Enterprise Portal	Name of the Tab	Elements in the Tab	Name of the Privilege	Description	Allow Privilege	Deny Privilege	Customizable
	Alerts & Notifications		Read Customer Alert Notification	Grants ability to view and manage customer alert configuration	No	Yes	Yes
			Create Customer Alert	Grants ability to view and manage customer alert configuration and generated alerts	Yes	No	No
			Read Customer Alert			Yes	Yes
			Update Customer Alert				
			Delete Customer Alert			No	No
			Manage Customer Alert				
		SMS Alert	Update Customer SMS Alert	Grants ability to configure SMS alerts at the customer level	No	Yes	Yes
	Customer		Update Enterprise	Grants ability to view and manage Customers, from the Partner or Operator level	Yes	Yes	Yes
		Other Settings	Read User Agreement	Privilege granting access to configure the customer user agreement feature	Yes	No	No
			Update User Agreement				
Test & Troubleshoot			Read Diagnostics	Controls creation of and access to diagnostics bundles, both Edge and Gateway. Combine with Edge and Gateway privileges to control access to each type individually	Yes	Yes	Yes
	Remote Diagnostics		Create Remote Diagnostics	Grants access to view and execute remote diagnostics	No	No	No
			Read Remote Diagnostics			Yes	Yes
			Update Remote Diagnostics			No	No
			Delete Remote Diagnostics				
			Manage Remote Diagnostics			Yes	Yes
		Gateway	Remote Cloud Traffic Routing		No	Yes	Yes
		Reset USB Modem	Remote Reset USB Modem	Grants ability to execute the Edge USB modem reset remote action	No	Yes	Yes
		Scan for nearby Wi-Fi	Remote Scan for Wi-Fi Access Points	Grants ability to execute the Edge Wi-Fi scan remote action	No	Yes	Yes
		VPN Test	Remote VPN Test	Grants ability to execute the Edge VPN test remote action	No	Yes	Yes

Navigation Path in the Enterprise Portal	Name of the Tab	Elements in the Tab	Name of the Privilege	Description	Allow Privilege	Deny Privilege	Customizable
	Remote Actions		Create Remote Actions	Grants access to view and execute remote actions	No	Yes	Yes
			Read Remote Actions				
			Update Remote Actions				
			Delete Remote Actions				
		Select Edge > Shutdown button	Shutdown Edge	Grants ability to execute the Edge shutdown remote action	No	Yes	Yes
		Select Edge > Deactivate button	Deactivate Edge	Grants ability to execute the deactivate Edge remote action	No	Yes	Yes
	Diagnostic Bundles/Packet Capture	404 resource not found page	Create Diagnostics	Controls creation of and access to diagnostics bundles, both Edge and Gateway. Combine with Edge and Gateway privileges to control access to each type individually	Yes	Yes	Yes
			Read Diagnostics				
			Update Diagnostics				
			Delete Diagnostics				
			Manage Diagnostics			No	No
		Request Diagnostic Bundle	Create Diagnostic Bundle	Grants ability to view and request Diagnostic bundles as part of remote diagnostics functionality	No	Yes	Yes
	Diagnostic Bundles/Packet Capture	404 resource not found page	Read Diagnostic Bundle				
			Update Diagnostic Bundle				
		Delete Diagnostic Bundle	Delete Diagnostic Bundle				
		Request PCAP Bundle	Create PCAP Bundle	Grants ability to view and request PCAP bundles as part of remote diagnostics functionality	No	Yes	Yes
	Diagnostic Bundles/Packet Capture	404 resource not found page	Read PCAP Bundle				
			Update PCAP Bundle			No	No
			Delete PCAP Bundle			Yes	Yes
	Diagnostic Bundles/Packet Capture	404 resource not found page	Manage PCAP Bundle				
		Download Diagnostic Bundle	Download Edge Diagnostics	Grants ability to download Edge Diagnostics	No	Yes	Yes
Administration							

Navigation Path in the Enterprise Portal	Name of the Tab	Elements in the Tab	Name of the Privilege	Description	Allow Privilege	Deny Privilege	Customizable
	System Settings		Read Customer Delegation	Grants ability to view and manage the delegation of privileges from the customer to Partners or the Operator	Yes	Yes	Yes
	General Information >	General Information	Read Customer General Information Update Customer General Information	Controls visibility and control of Customer General Information on the System Settings General Information page	No	Yes	Yes
		Default Edge Authentication	Read Customer PKI Update Customer PKI	Grants ability to view and manage enterprise PKI settings	Yes	No	No
		Edge Configuration	Read Customer Edge Settings Update Customer Edge Settings	Controls visibility and control of Customer Edge Settings on the System Settings General Information page	No	Yes	Yes
		Privacy Settings	Read Customer Privacy Settings Update Customer Privacy Settings	Controls visibility and control of Customer Privacy Settings on the System Settings General Information page	No	Yes	Yes
		Privacy Settings > Enforce PCI	Update Customer User	Grants ability to view and manage Customer administrators	Yes	Yes	Yes
		Contact Information	Read System Settings Contact Info Update System Settings Contact Info	Controls visibility and control of System Settings Contact Info on the System Settings General Information page	No	Yes	Yes
	Authentication		Create Customer Authentication Read Customer Authentication Update Customer Authentication Delete Customer Authentication Manage Customer Authentication	Grants ability to view and manage customer authentication mode, for example SSO, Radius or Native	Yes	Yes	Yes
		API Tokens	Read Customer Token Update Customer Token	Grants ability to view and manage authentication tokens at the Customer level	Yes	No	No
	Administrators		Create Customer User Read Customer User Update Customer User	Grants ability to view and manage Customer administrators	Yes	Yes	Yes

Navigation Path in the Enterprise Portal	Name of the Tab	Elements in the Tab	Name of the Privilege	Description	Allow Privilege	Deny Privilege	Customizable
			Delete Customer User				
			Manage Customer User			No	No
	Select Enterprise User >	API Tokens	Create Customer Token	Grants ability to view and manage authentication tokens at the Customer level	Yes	No	No
			Read Customer Token				
			Update Customer Token				
			Delete Customer Token				
			Manage Customer Token				
	Service Permissions		Create Service Permissions Package	Grants access to manage Service Permissions packages	Yes	No	No
			Read Service Permissions Package				
			Update Service Permissions Package				
			Delete Service Permissions Package				
			Manage Service Permissions Package				
	Edge Licensing		Create License	Grants ability to view and manage Edge licensing	Yes	No	No
			Read License			Yes	Yes
			Update License				
			Delete License			No	No
			Manage License				
VeloCloud Support Access Role			Create Customer Delegation	Grants ability to view and manage the delegation of privileges from the customer to Partners or the Operator	Yes	Yes	Yes
			Read Customer Delegation				
			Update Customer Delegation				
			Delete Customer Delegation				
			Manage Customer Delegation			No	No

When the corresponding user privilege is denied, the Orchestrator window displays the `404 resource not found` error.

Below table provides a list of customizable feature privileges:

Table 13: Customizable Feature Privileges

Navigation Path in the Enterprise Portal	Name of the Tab	Name of the Privilege	Description
Configure > **Edges** > **Select Edges**	Overview	Assign Edge Profile	Grants ability to assign a Profile to Edges
Configure > **Edges** > **Select Edges**	Firewall	Configure Edge Firewall Logging	Grants ability to configure Edge level firewall logging
Configure > **Profiles** > **Select Profile**	Firewall	Configure Profile Firewall Logging	Grants ability to configure Profile level firewall logging
Diagnostics > **Remote Actions**	Select Edge > Deactivate	Deactivate Edge	Grants ability to reset the device configuration to its factory default state
Global Settings > **Enterprise Settings** > **Information Privacy Settings** > **SD-WAN PC**	Enforce PCI Compliance	Deny PCI Operations	Denies access to sensitive Customer data including PCAPs, etc. on the Edges and Gateways, for all users
Diagnostics > **Diagnostic Bundles**	Select Edge > Download Bundle	Download Edge Diagnostics	Grants ability to download Edge Diagnostics
s**Gateway Management** > **Diagnostic Bundles**	Select Gateway > Download Bundle	Download Gateway Diagnostics	Grants ability to download Gateway Diagnostics
Configure > **Profiles**	Duplicate	Duplicate Customer Profile	Grants ability to edit duplicate customer level Profiles
Configure > **Segments/ Configure** > **Profiles/ Configure** > **Edges**	Segments drop-down menu	Edit Tab Segments	Grants ability to edit within the Segments tab
Configure > **Edges** > **Select Edge**	Device	Enable HA Cluster	Grants ability to configure HA Clustering
Configure > **Edges** > **Select Edge**	Device	Enable HA Active/Standby Pair	Grants ability to configure active/ standby HA
Configure > **Edges** > **Select Edge**	Device	Enable HA VRRP Pair	Grants ability to configure VRRP HA
Diagnostics > **Remote Diagnostics**	Clear ARP Cache	Remote Clear ARP Cache	Grants ability to clear the ARP cache for a given interface
Diagnostics > **Remote Diagnostics** > **Gateway**	Cloud Traffic Routing (drop-down menu)	Remote Cloud Traffic Routing	Grants ability to route cloud traffic remotely
Diagnostics > **Remote Diagnostics**	DNS/DHCP Service Restart	Remote DNS/DHCP Restart	Grants ability to restart the DNS/ DHCP service
Diagnostics > **Remote Diagnostics**	Flush Flows	Remote Flush Flows	Grants ability to flush the Flow table, causing user traffic to be re-classified
Diagnostics > **Remote Diagnostics**	Flush NAT	Remote Flush NAT	Grants ability to flush the NAT table
Diagnostics > **Remote Diagnostics** > **LTE SIM Switchover**	LTE Switch SIM Slot **Note:** This is for 610-LTE and 710 5G devices only.	Remote LTE Switch SIM Slot	Grants ability to activate the SIM Switchover feature. After the test is successful, you can check the status from **Monitor** > **Edges** > **Overview tab**
Diagnostics > **Remote Diagnostics**	List Paths	Remote List Paths	Grants ability to view the list of active paths between local WAN links and each peer
Diagnostics > **Remote Diagnostics**	List current IKE Child SAs	Remote List current IKE Child SAs	Grants ability to use filters to view the exact Child SAs you want to see
Diagnostics > **Remote Diagnostics**	List current IKE SAs	Remote List Current IKE SAs	Grants ability to use filters to view the exact SAs you want to see
Diagnostics > **Remote Diagnostics**	MIBs for Edge	Remote MIBS for Edge	Grants ability to dump Edge MIBs
Diagnostics > **Remote Diagnostics**	NAT Table Dump	Remote NAT Table Dump	Grants ability to view the contents of the NAT table
Diagnostics > **Remote Diagnostics**	Select Edge > Rebalance Hub Cluster	Remote Rebalance Hub Cluster	Grants ability to either redistribute Spokes in Hub Cluster or redistribute Spokes excluding this Hub

Navigation Path in the Enterprise Portal	Name of the Tab	Name of the Privilege	Description
Diagnostics > **Remote Diagnostics**	Select Edge (with SFP module) > Reset SFP Firmware Configuration	Remote Reset SFP Firmware Configuration	Grants ability to reset the SFP Firmware Configuration
Diagnostics > **Remote Actions**	Reset USB Modem	Remote Reset USB Modem	Grants ability to execute the Edge USB modem reset remote action
Diagnostics > **Remote Diagnostics**	Scan for Wi-Fi Access Points	Remote Scan for Wi-Fi Access Points	Grants ability to scan the Wi-Fi functionality for the VeloCloud Edge
Diagnostics > **Remote Diagnostics**	System Information	Remote System Information	Grants ability to view system information such as system load, recent WAN stability statistics, monitoring services
Diagnostics > **Remote Diagnostics**	VPN Test	Remote VPN Test	Grants ability to execute the Edge VPN test remote action
Diagnostics > **Remote Diagnostics**	WAN Link Bandwidth Test	Remote WAN link Bandwidth Test	Grants ability to re-test the bandwidth of a WAN link
Diagnostics > **Remote Actions**	Select Edge > Shutdown	Shutdown Edge	Grants ability to execute the Edge shutdown remote action
Service Settings > **Alerts & Notifications**	Notifications > Email/SMS	Update Customer SMS Alert	Grants ability to configure SMS alerts at the customer level
Monitor > **Edges** > **Select Edge**	Top Sources	View Edge Sources	Grants ability to view Monitor Edge Sources tab
Monitor > **Firewall**	Firewall Logging	View Firewall Logs	Grants ability to view collected firewall logs
Monitor > **Edges** > **Select Edge**	Top Sources	View Flow Stats	Grants ability to view collected flow statistics
Monitor > **Firewall Logs**	Firewall Logs	View Profile Firewall Logging	Grants ability to view the details of firewall logs originating from Arista VeloCloud Edges
Configure > **Profiles**	Firewall	View Stateful Firewall	Grants ability to view collected flow statistics
Configure > **Profiles**	Firewall tab > Configure Firewall > Syslog Forwarding	View Syslog Forwarding	Grants ability to view logs that are forwarded to a configured syslog collector
Operator portal > **Gateway Management**	Gateways	View Tab Gateway List	Grants ability to view the Gateway list tab
Operator portal > **Administration**	Operator Profiles	View Tab Operator Profile	Grants ability to view and configure settings within the Operator Profile menu tab
Monitor > **Edges** > **Select Edge**	Top Sources	View User Identifiable Flow Stats	Grants ability to view potentially user identifiable flow source attributes

3.4 Authentication

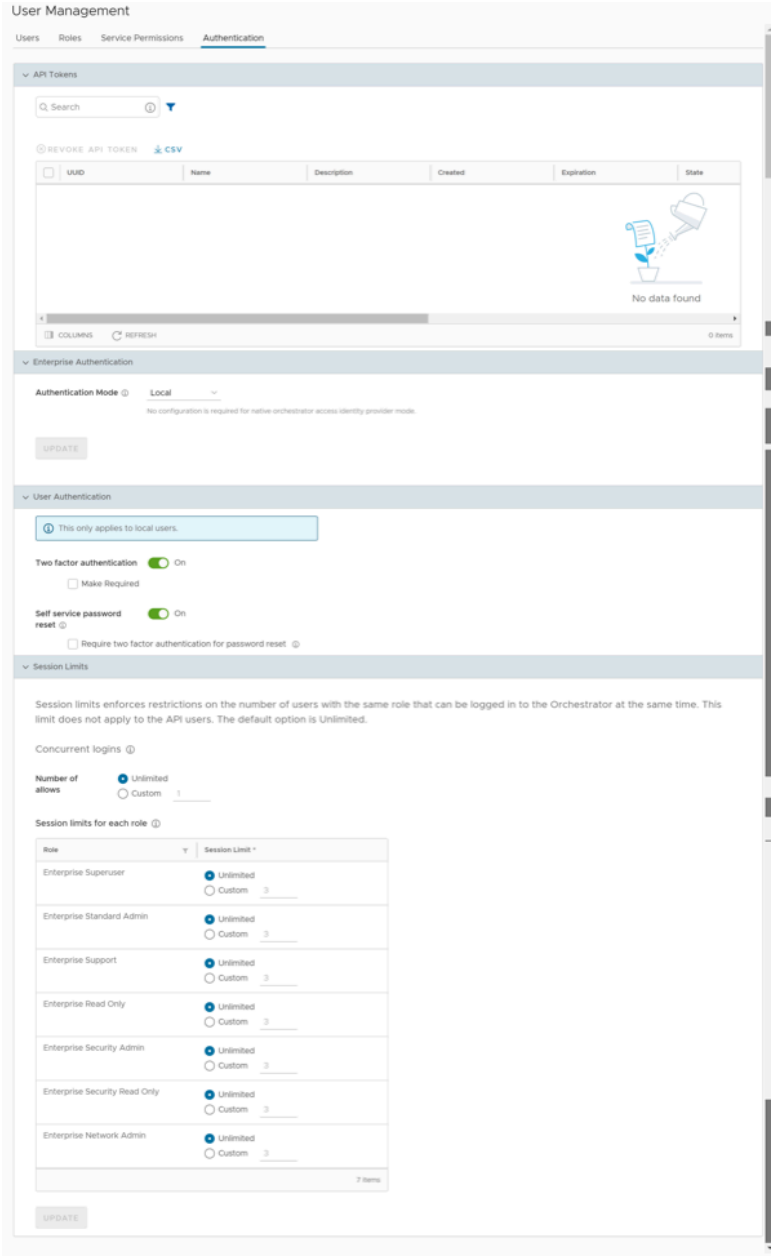
The Authentication feature allows you to set the authentication mode for an Enterprise user and view the existing API tokens.

To access the **Authentication** tab:

1. In the **Enterprise** portal, on the **Global Navigation** bar, expand the **Enterprise Applications** drop-down menu.
2. Select **Global Settings** service.

3. From the left menu, select **User Management**, and then select the **Authentication** tab. The following screen appears:

Figure 3-11: Authentication



API Tokens

You can access the **Orchestrator** APIs using token-based authentication, irrespective of the authentication mode. You can view the API tokens issued to the Enterprise users. If required, you can revoke the API tokens.

By default, the API Tokens are activated. If you want to deactivate them, contact your Operator.

Note: Enterprise Administrator should manually delete inactive Identity Provider (IdP) users from the Orchestrator to prevent unauthorized access via API Token.

The following are the options available in this section:

Table 14: API Tokens Option Descriptions

Option	Description
Search	Enter a search term to search for the matching text across the table. Use the advanced search option to narrow down the search results.
Revoke API Token	Select the token and select this option to revoke it. Only an Operator Super User or the user associated with an API token can revoke the token.
CSV	Select this option to download the complete list of API tokens in a `.csv` file format.
Columns	Select the columns to be displayed or hidden on the page.
Refresh	Select to refresh the page to display the most current data.

For information on creating and downloading API tokens, see API Tokens.

Enterprise Authentication

Select one of the following Authentication modes:

- **Local**: This is the default option and does not require any additional configuration.
- **Single Sign-On**: Single Sign-On (SSO) is a session and user authentication service that allows users to log in to multiple applications and websites with one set of credentials. Integrating an SSO service with Orchestrator enables Orchestrator to authenticate users from OpenID Connect (OIDC)-based Identity Providers (IdPs).

  For information on how to configure Single Sign On for Enterprise User, see Enterprise Settings.

  To enable Single Sign On (SSO) for Orchestrator, you must enter the Orchestrator application details into the Identity Provider (IdP). Select each of the following links for step-by-step instructions to configure the following supported IdPs:

  - Azure AD
  - Okta
  - OneLogin
  - PingIdentity

You can configure the following options when you select the **Authentication Mode** as **Single Sign-on**.

Figure 3-12: Enterprise Authentication Option Descriptions

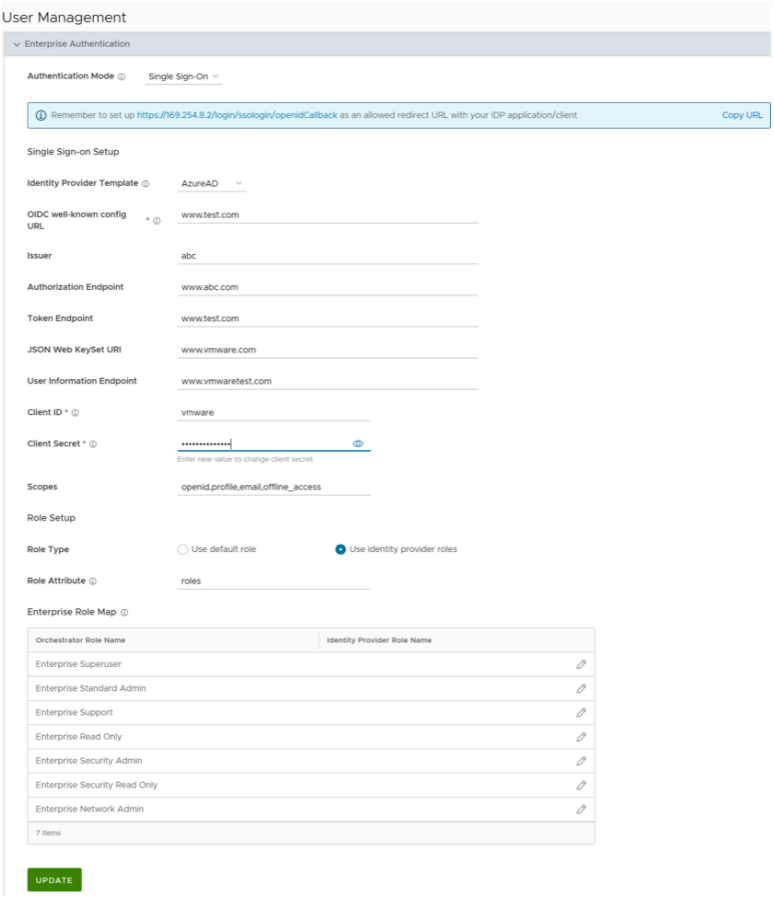


Table 15: Enterprise Authentication Option Descriptions

Option	Description
Identity Provider Template	From the drop-down menu, select your preferred Identity Provider (IdP) that you have configured for Single Sign On. This pre-populates fields specific to your IdP. **Note:** You can also manually configure your own IdPs by selecting **Others** from the drop-down menu.
Organization Id	This field is available only when you select the **CSP** template. Enter the Organization ID provided by the IdP in the format: `/csp/gateway/am/api/orgs/<full organization ID>`. When you sign in to CSP, you can view the organization ID you are logged into by selecting on your username. This information also appears under Organization details. Use the "Long Organization ID".
OIDC well-known config URL	Enter the OpenID Connect (OIDC) configuration URL for your IdP. For example, the URL format for Okta will be: `https://{oauth-provider-url}/.well-known/openid-configuration`.
Issuer	This field is auto-populated based on your selected IdP.
Authorization Endpoint	This field is auto-populated based on your selected IdP.
Token Endpoint	This field is auto-populated based on your selected IdP.
JSON Web KeySet URI	This field is auto-populated based on your selected IdP.
User Information Endpoint	This field is auto-populated based on your selected IdP.
Client ID	Enter the client identifier provided by your IdP.
Client Secret	Enter the client secret code provided by your IdP, that is used by the client to exchange an authorization code for a token.
Scopes	This field is auto-populated based on your selected IdP.
Role Type	Select one of the following two options: • Use default role • Use identity provider roles
Role Attribute	Enter the name of the attribute set in the IdP to return roles.
Enterprise Role Map	Map the IdP-provided roles to each of the Enterprise user roles.

Select **Update** to save the entered values. The SSO authentication setup is complete in the **Orchestrator**.

User Authentication

You can choose to activate or deactivate the **Two factor authentication** feature for the user. The **Self service password reset** allows you to change the password using a link on the Login page.

Note: This feature can be activated only for those users whose mobile phone numbers are associated with their user accounts.

Session Limits

Note: To view this section, an Operator user must navigate to **Orchestrator** > **System Properties**, and set the value of the system property `session.options.enableSessionTracking` to **True**.

The following are the options available in this section:

Table 16: Session Limits Option Descriptions

Option	Description
Concurrent logins	Allows you to set a limit on concurrent logins per user. By default, **Unlimited** is selected, indicating that unlimited concurrent logins are allowed for the user.
Session limits for each role	Allows you to set a limit on the number of concurrent sessions based on user role. By default, **Unlimited** is selected, indicating that unlimited sessions are allowed for the role. **Note:** The roles that are already created by the Enterprise in the **Roles** tab, are displayed in this section.

Select **Update** to save the selected values.

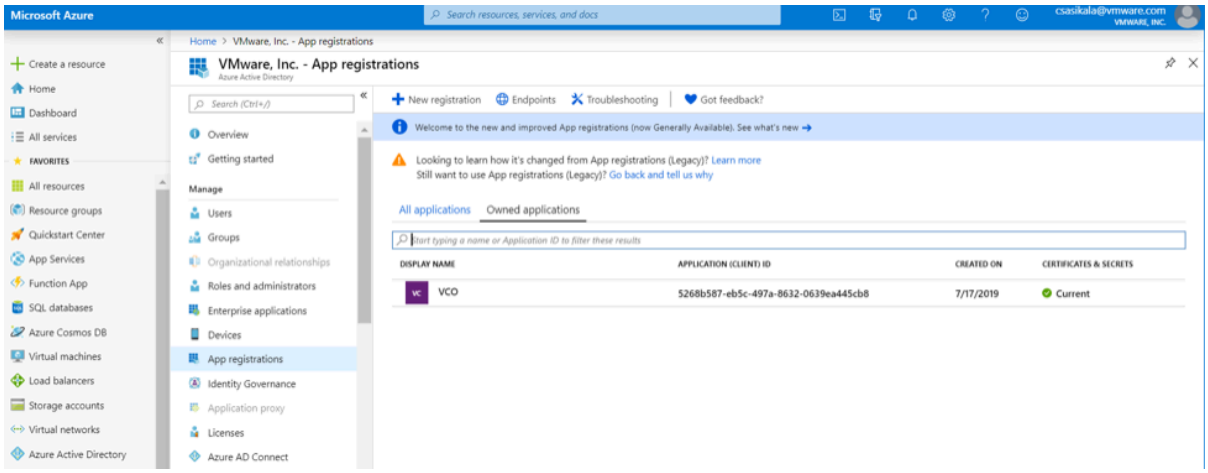
3.4.1 Configure Azure Active Directory for Single Sign On

To set up an OpenID Connect (OIDC)-based application in Microsoft Azure Active Directory (AzureAD) for Single Sign On (SSO), perform the following steps.

Ensure you have an AzureAD account to sign in.

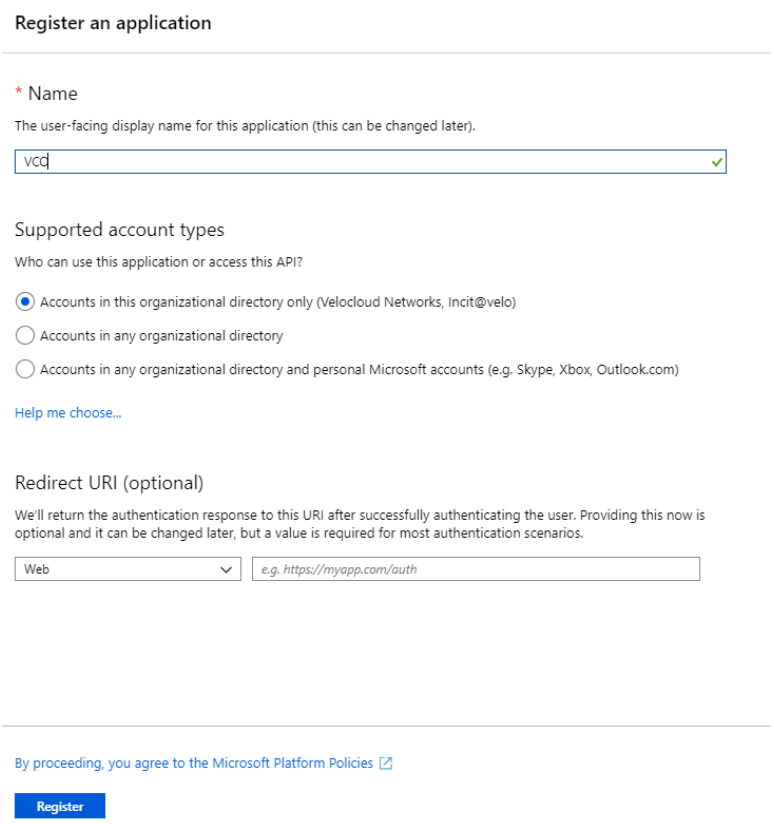
1. Log in to your Microsoft Azure account as an Admin user. The **Microsoft Azure** home screen appears.
2. To create a new application:
   a. Search and select the **Azure Active Directory** service.

Figure 3-13: Microsoft Azure



b. Go to **App registration** > **New registration**. The **Register an application** screen appears.

Figure 3-14: Register an Application



c. In the **Name** field, enter the name for your Orchestrator application.

d. In the **Redirect URL** field, enter the redirect URL that your **Orchestrator** application uses as the callback endpoint.

In the **Orchestrator** application, at the bottom of the **Configure Authentication** screen, you can find the redirect URL link. Ideally, the Orchestrator redirect URL will be in this format: **`https://<Orchestrator URL>/login/ssologin/openidCallback`**.

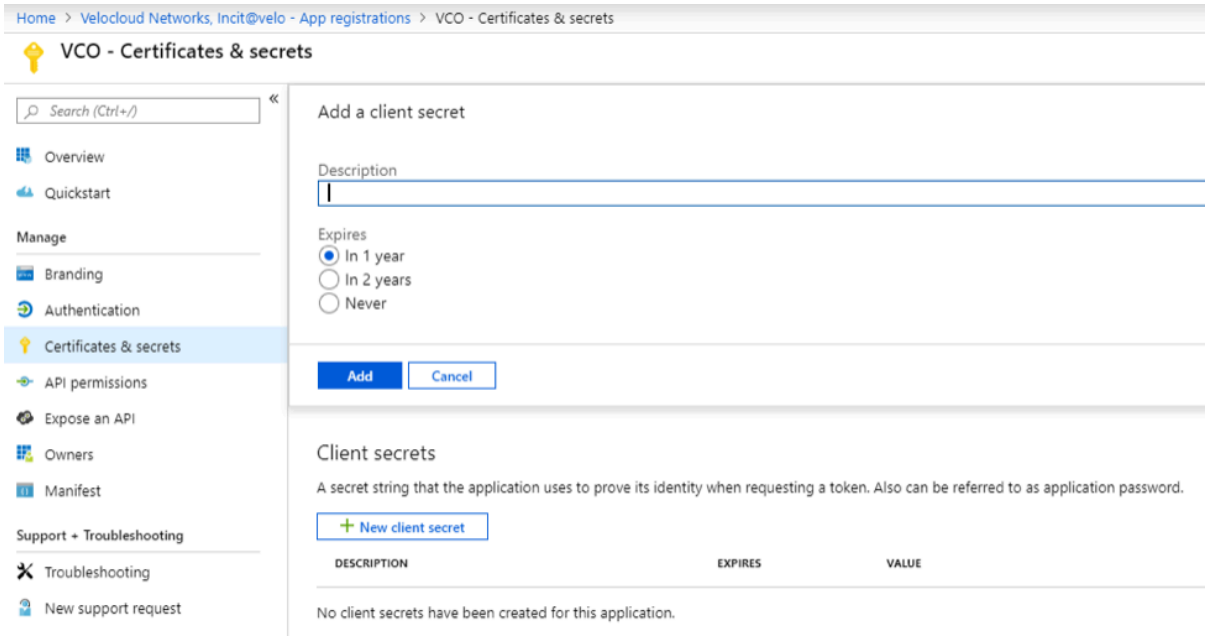
e. Select **Register**. Your **Orchestrator** application will be registered and displayed in the **All applications** and **Owned applications** tabs. Make sure to note down the **Client ID/Application ID** to be used during the SSO configuration in Orchestrator.

f. Select **Endpoints** and copy the well-known OIDC configuration URL to be used during the SSO configuration in Orchestrator.

g. To create a client secret for your **Orchestrator** application, on the **Owned applications** tab, select your **Orchestrator** application.

h. Go to **Certificates & secrets** > **New client secret**. The **Add a client secret** screen appears.

Figure 3-15: Adding a Client Secret

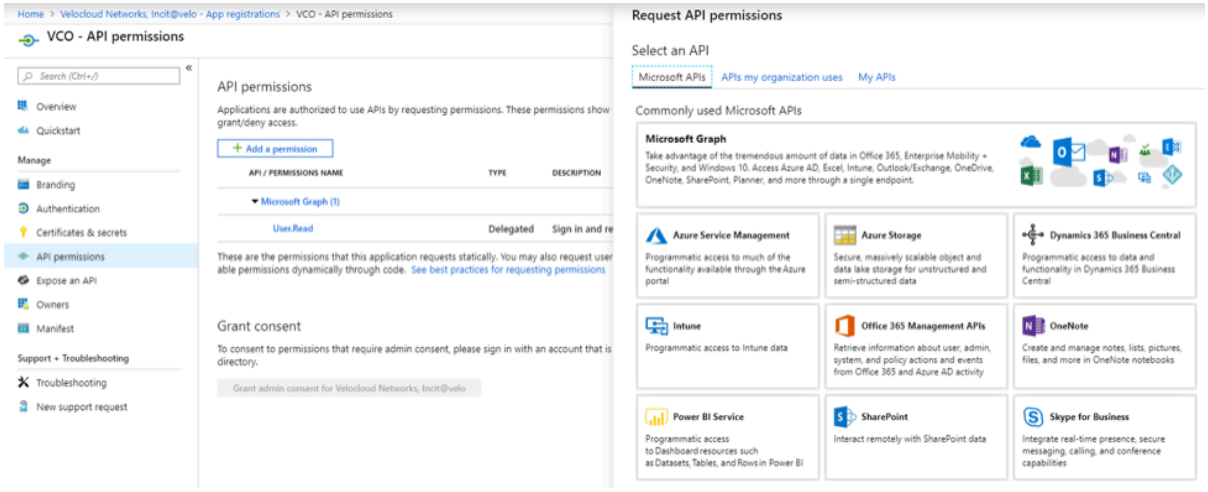


i. Provide details such as description and expiry value for the secret and select **Add**.

The client secret is created for the application. Note down the new client secret value to be used during the SSO configuration in Orchestrator.

j. To configure permissions for your **Orchestrator** application, select your **Orchestrator** application and go to **API permissions** > **Add a permission**. The **Request API permissions** screen appears.

Figure 3-16: Adding API Permissions



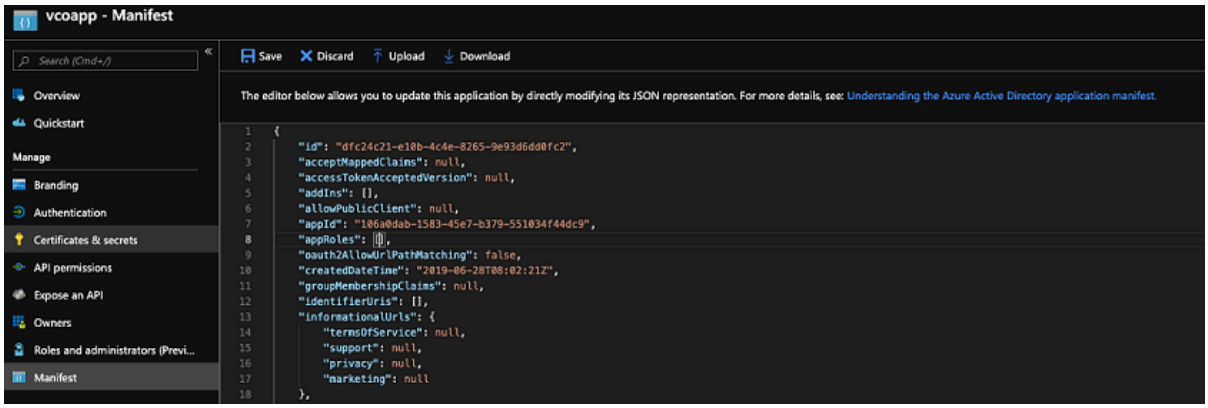
k. Select **Microsoft Graph** and select **Application permissions** as the type of permission for your application.

l. Under **Select permissions**, from the **Directory** drop-down menu, select **Directory.Read.All**, and from the **User** drop-down menu, select **User.Read.All**.

m. Select **Add permissions**.

n. To add and save roles in the manifest, select your **Orchestrator** application and from the application **Overview** screen, select **Manifest**. A web-based manifest editor opens, allowing you to edit the manifest within the portal. Optionally, you can select **Download** to edit the manifest locally, and then use **Upload** to reapply it to your application.

Figure 3-17: Viewing the Manifest



o. In the manifest, search for the appRoles array and add one or more role objects as shown in the following example and select **Save**.

> **Note:** The value property from appRoles must be added to the **Identity Provider Role Name** column of the **Role Map** table, located in the **Authentication** tab, in order to map the roles correctly.

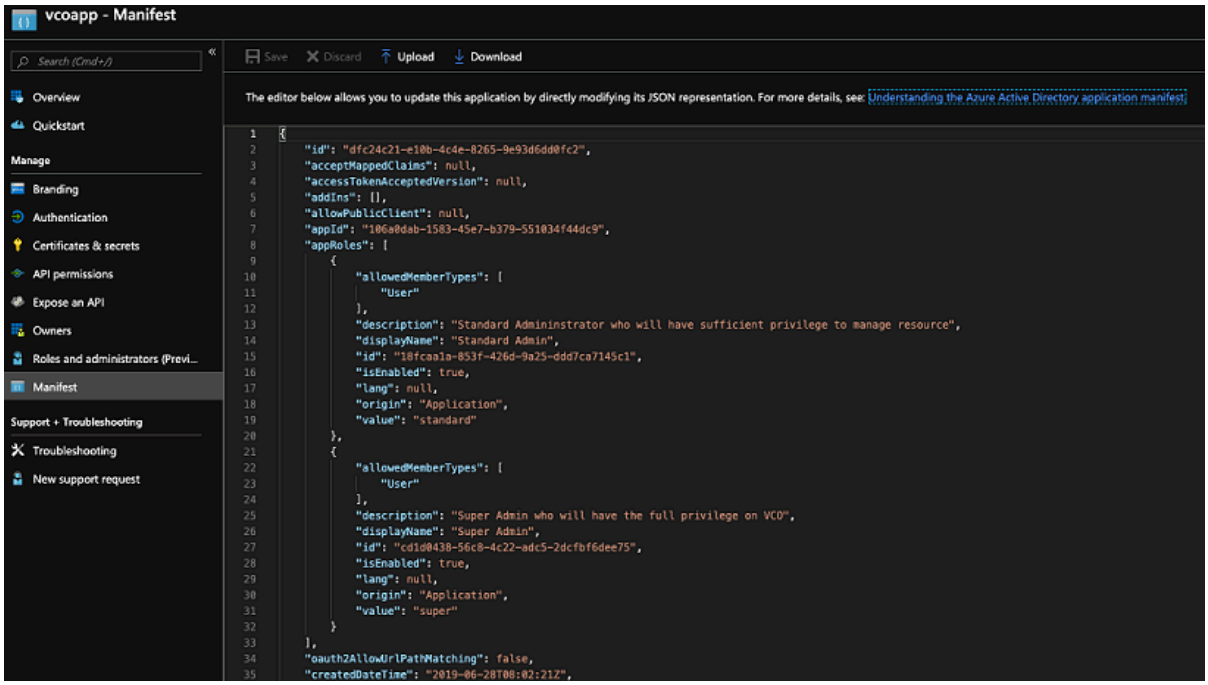
Sample role objects

```
{ "allowedMemberTypes": [ "User" ], "description": "Standard Administrator who will
 have sufficient privilege to manage resource", "displayName": "Standard Admin", "id":
 "18fcaa1a-853f-426d-9a25-ddd7ca7145c1", "isEnabled": true, "lang": null, "origin":
 "Application", "value": "standard" }, { "allowedMemberTypes": [ "User" ], "description"
: "Super Admin who will have the full privilege on Orchestrator", "displayName": "Super
 Admin", "id": "cd1d0438-56c8-4c22-adc5-2dcfbf6dee75", "isEnabled": true, "lang": null,
 "origin": "Application", "value": "superuser" }
```

> **Note:** Make sure to set id to a newly generated Global Unique Identifier (GUID) value. You can generate GUIDs online using web-based tools (for example, https://www.guidgen.com/), or by running the following commands:
>
> - Linux/OSX- uuidgen

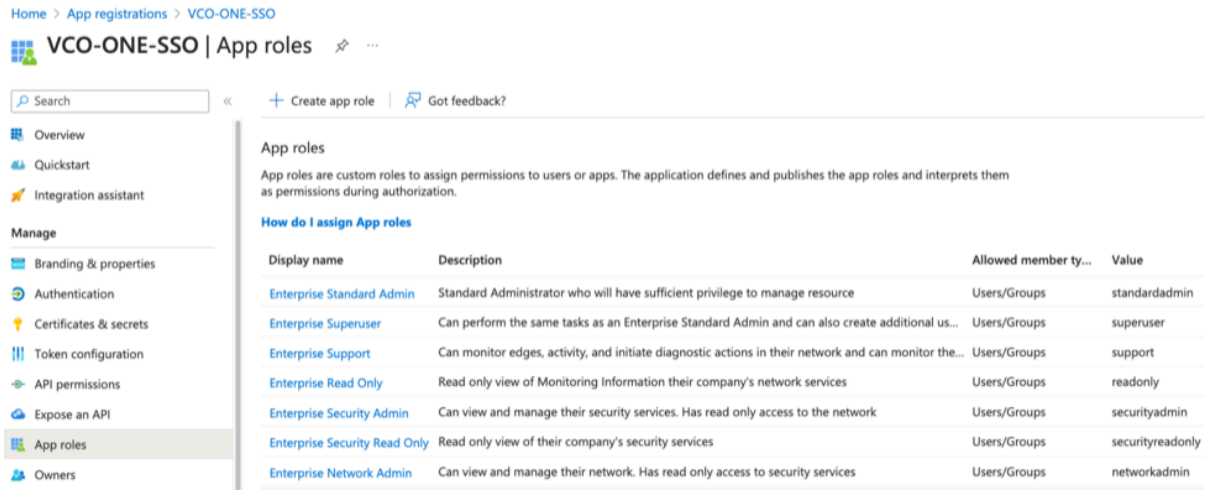
- Windows- powershell [guid]::NewGuid()

Figure 3-18: Manifest



Roles are manually set up in the Orchestrator, and must match the ones configured in the **Microsoft Azure** portal.

Figure 3-19: App Roles



3. To assign groups and users to your Orchestrator application:
   a. Go to **Azure Active Directory** > **Enterprise applications**.
   b. Search and select your Orchestrator application.
   c. Select **Users and groups** and assign users and groups to the application.

d. Select **Submit**.

You have completed setting up an OIDC-based application in AzureAD for SSO. Configure Single Sign On in Orchestrator.

3.4.2 Configure Okta for Single Sign On

To support OpenID Connect (OIDC)-based Single Sign On (SSO) from Okta, you must first set up an application in Okta. To set up an OIDC-based application in Okta for SSO, perform the steps on this procedure.

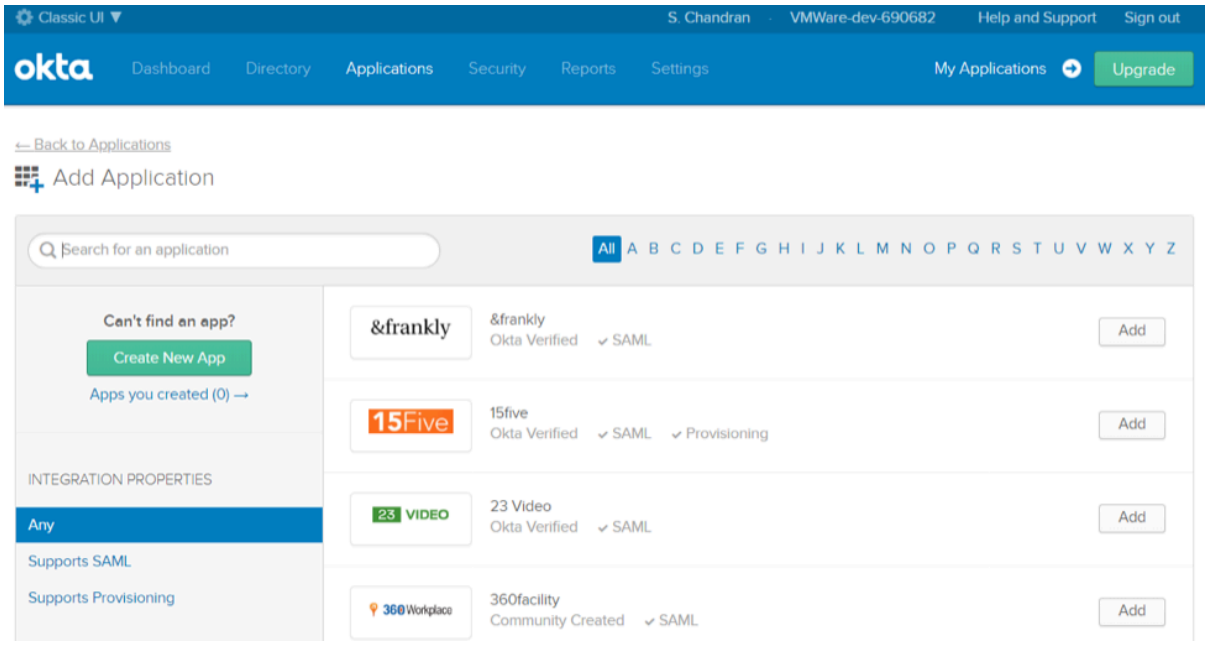
Ensure you have an Okta account to sign in.

1. Log in to your Okta account as an Admin user. The **Okta** home screen appears.

> **Note:** If you are in the **Developer Console** view, then you must switch to the **Classic UI** view by selecting **Classic UI** from the **Developer Console** drop-down list.

2. To create a new application:
   a. In the upper navigation bar, select **Applications** > **Add Application**. The **Add Application** screen appears.

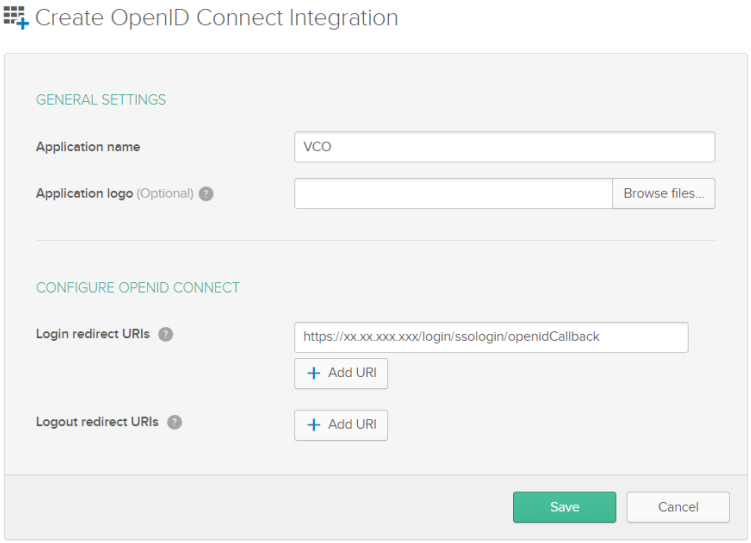
Figure 3-20: Adding an Application to Okta



   b. Select **Create New App**. The **Create a New Application Integration** dialog box appears.
   c. From the **Platform** drop-drop menu, select **Web**.

d. Select **OpenID Connect** as the Sign on method and select **Create**. The **Create OpenID Connect Integration** screen appears.

Figure 3-21: Creating an OpenID Connect Integration



e. Under the **General Settings** area, in the **Application name** text box, enter the name for your application.

f. Under the **CONFIGURE OPENID CONNECT** area, in the **Login redirect URIs** text box, enter the redirect URL that your Orchestrator application uses as the callback endpoint.

In the **Orchestrator** application, at the bottom of the **Configure Authentication** screen, you can find the redirect URL link. Ideally, the Orchestrator redirect URL will be in this format: **`https://<Orchestrator URL>/login/ssologin/openidCallback`**.

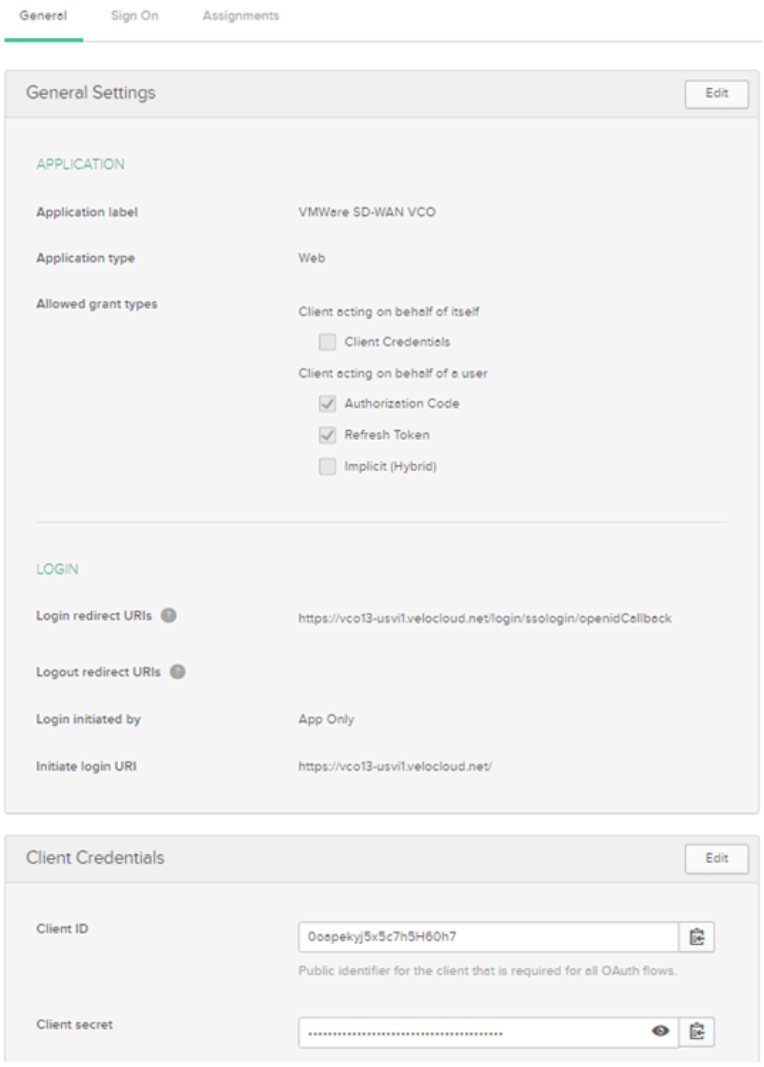
g. Select **Save**. The newly created application page appears.

h. On the **General** tab, select **Edit** and select **Refresh Token** for Allowed grant types, and select **Save**.

Note down the Client Credentials (Client ID and Client Secret) to be used during the SSO configuration in

Orchestrator.

Figure 3-22: Configuring General Settings



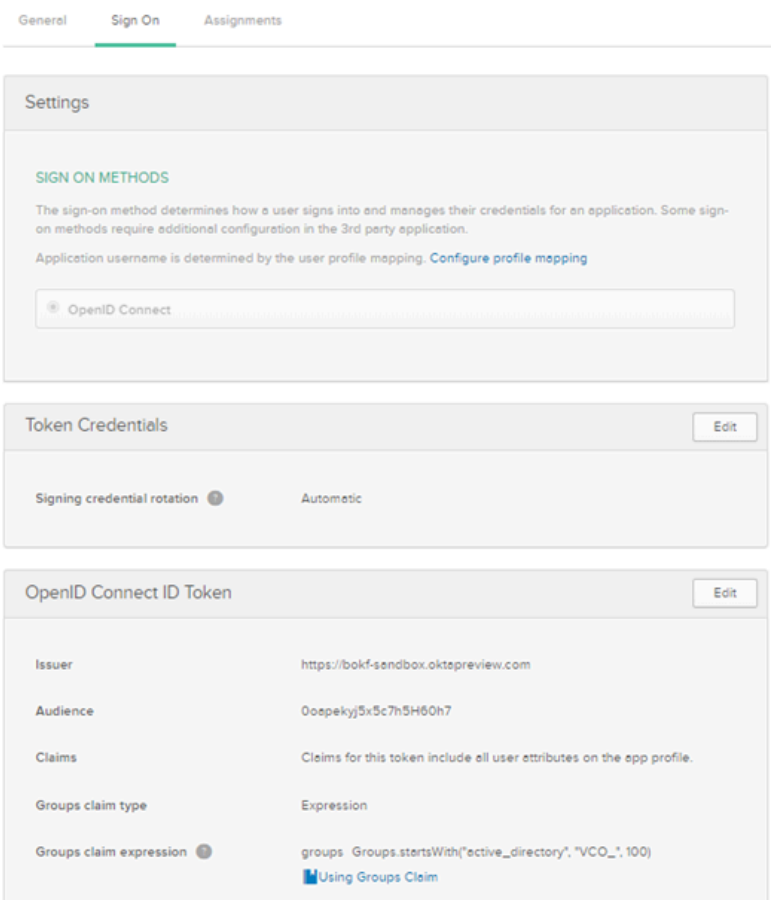
i. Select the **Sign On** tab and under the **OpenID Connect ID Token** area, select **Edit**.

j. From the **Groups claim type** drop-down menu, select **Expression**. By default, Groups claim type is set to **Filter**.

k. In the **Groups claim expression** textbox, enter the claim name that will be used in the token, and an Okta input expression statement that evaluates the token.

l. Select **Save**. The application is setup in IDP. You can assign user groups and users to your Orchestrator application.

Figure 3-23: Configuring Settings



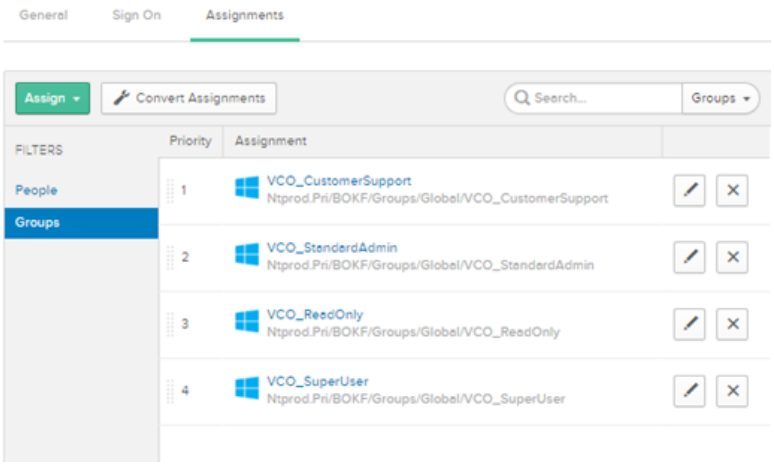
3. To assign groups and users to your Orchestrator application:

   a. Go to **Application** and select your **Orchestrator** application link.

   b. On the **Assignments** tab, from the **Assign** drop-down menu, select **Assign to Groups** or **Assign to People**. The **Assign** > **Application** > **Assign to Groups** or **Assign** > **Application** > **Assign to People** dialog box appears.

c. Select **Assign** next to available user groups or users you want to assign the Orchestrator application and select **Done**. The users or user groups assigned to the Orchestrator application will be displayed.

Figure 3-24: Assigning the Configuration



You have completed setting up an OIDC-based application in Okta for SSO.

3.4.3 Configure One Login for Single Sign On

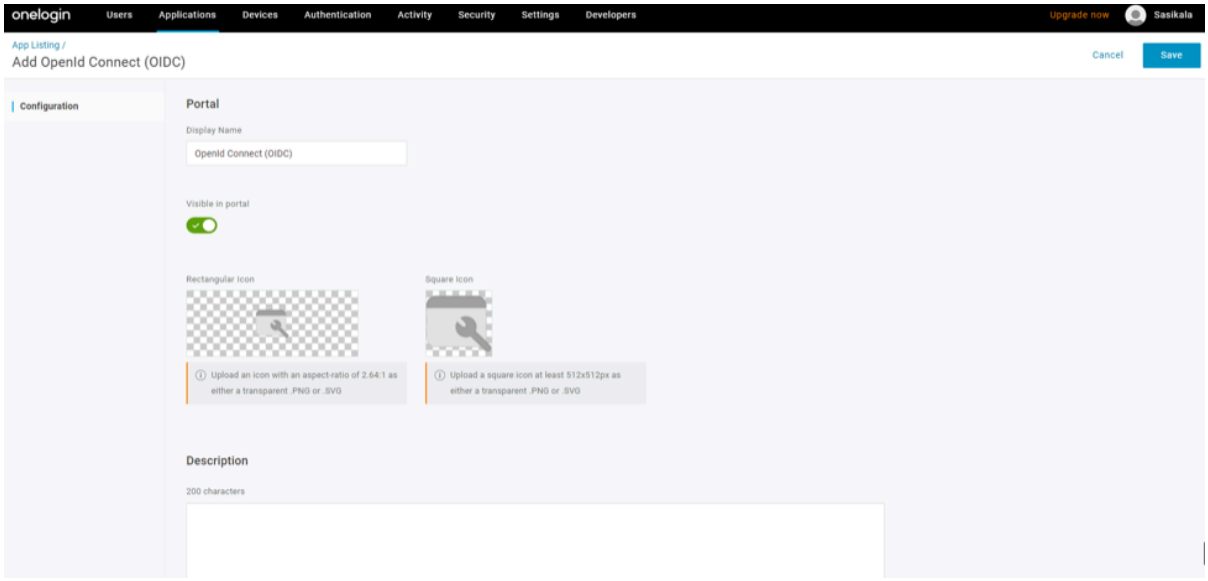
To set up an OpenID Connect (OIDC)-based application in OneLogin for Single Sign On (SSO), perform the steps below:

Ensure you have an OneLogin account to sign in.

1. Log in to your OneLogin account as an Admin user. The **OneLogin** home screen appears.
2. To create a new application:
   a. In the upper navigation bar, select **Apps** > **Add Apps**.

b. In the **Find Applications** text box, search for “**OpenId Connect**” or “**oidc**” and then select the **OpenId Connect (OIDC)** app. The **Add OpenId Connect (OIDC)** screen appears.

Figure 3-25: Add OpenID Connect

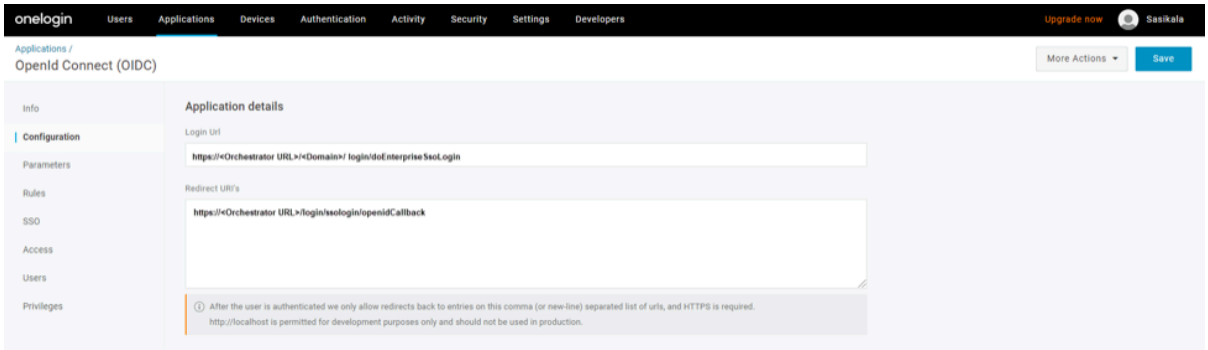


c. In the **Display Name** text box, enter the name for your application and select **Save**.

d. On the **Configuration** tab, enter the Login URL (auto-login URL for SSO) and the Redirect URI that Orchestrator uses as the callback endpoint, and select **Save**.

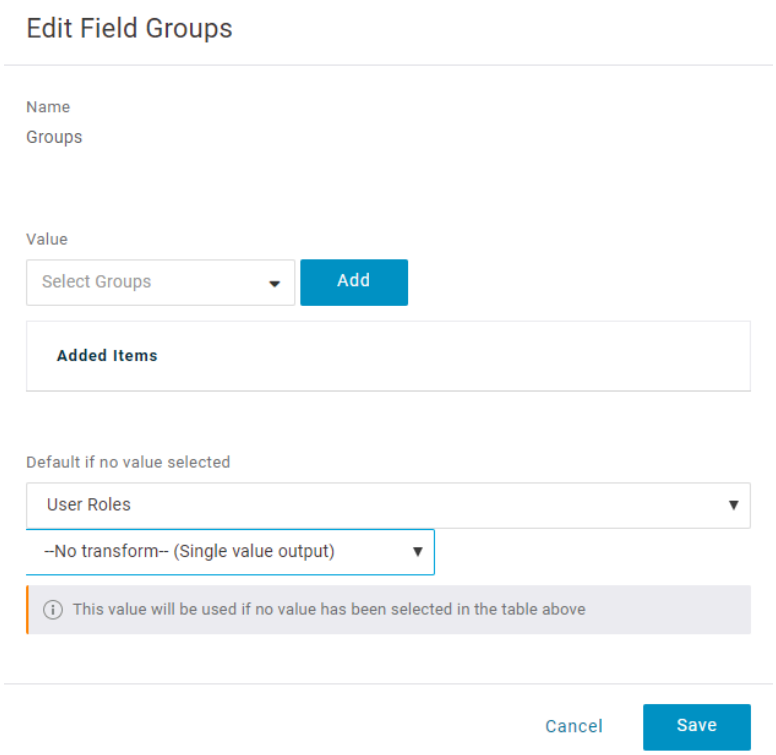
- **Login URL**- The login URL will be in this format: **`https://<Orchestrator URL>/<Domain>/login/doEnterpriseSsoLogin`**. Where, ***Domain*** is the domain name of your Enterprise that you must have already set up to enable SSO authentication for the Orchestrator. You can get the Domain name from the **Enterprise portal** > **Administration** > **System Settings** > **General Information** page.
- **Redirect URI's**- The Orchestrator redirect URL will be in this format: **`https://<Orchestrator URL>/login/ssologin/openidCallback`**. In the Orchestrator application, at the bottom of the **Authentication** screen, you can find the redirect URL link.

Figure 3-26: Configuring OpenID Connect



e. On the **Parameters** tab, under **OpenId Connect (OIDC)**, double select **Groups**. The **Edit Field Groups** popup appears.

Figure 3-27: Editing Field Groups



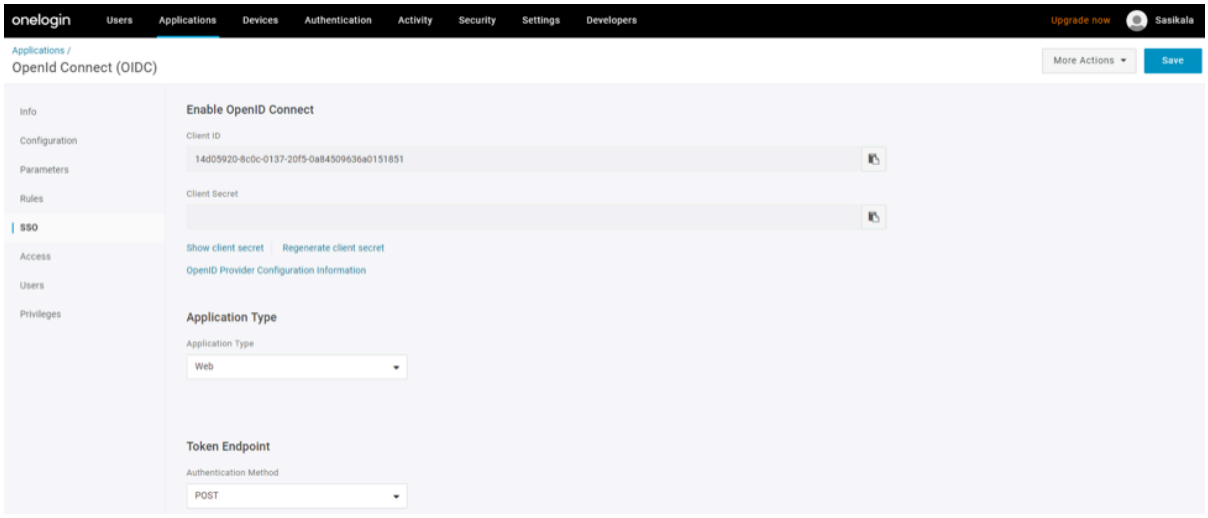
f. Configure **User Roles** with value "***--No transform--(Single value output)***" to be sent in groups attribute and select **Save**.

g. On the **SSO** tab, from the **Application Type** drop-down menu, select **Web**.

h. From the **Authentication Method** drop-down menu, select **POST** as the Token Endpoint and select **Save**.

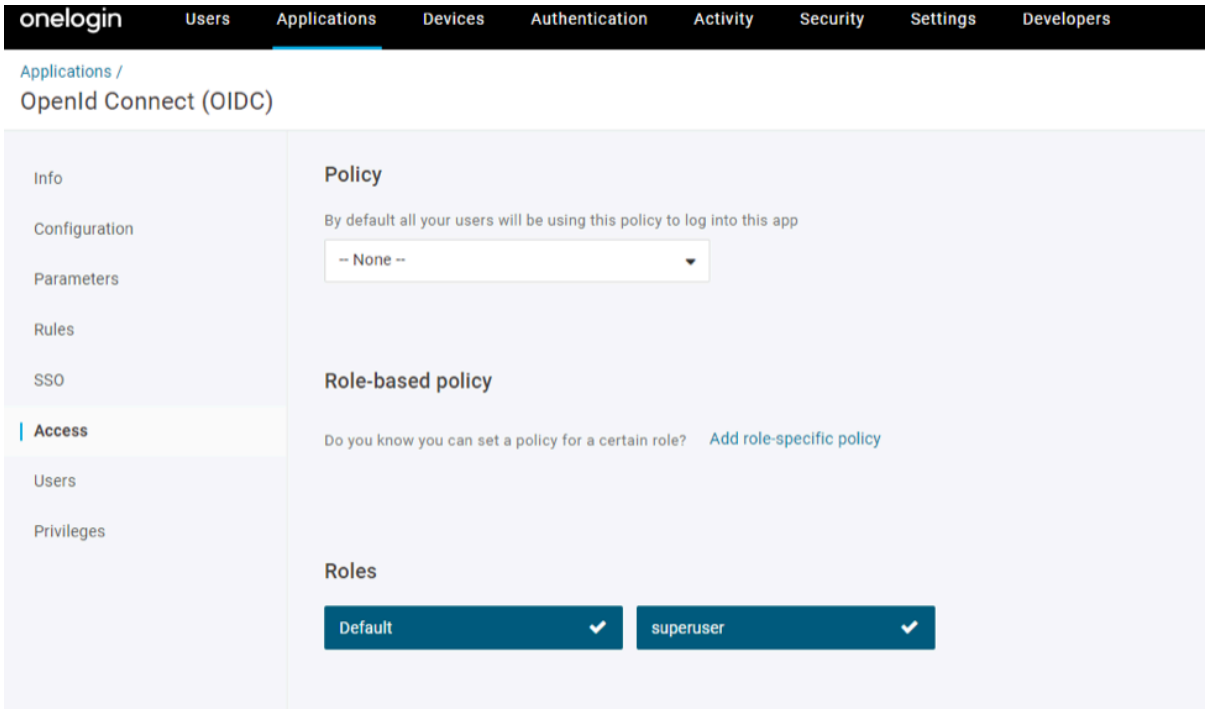
Also, note down the Client Credentials (Client ID and Client Secret) to be used during the SSO configuration in Orchestrator.

Figure 3-28: Configuring the Authentication Method



i. On the **Access** tab, choose the roles that will be allowed to login and select **Save**.

Figure 3-29: Access



3. To add roles and users to your Orchestrator application:

   a. Select **Users** and select a user.

   b. On the **Application** tab, from the **Roles** drop-down menu, on the left, select a role to be mapped to the user.

c. Select **Save Users**.

You have completed setting up an OIDC-based application in OneLogin for SSO.

3.4.4 Configure Ping Identity for Single Sign On

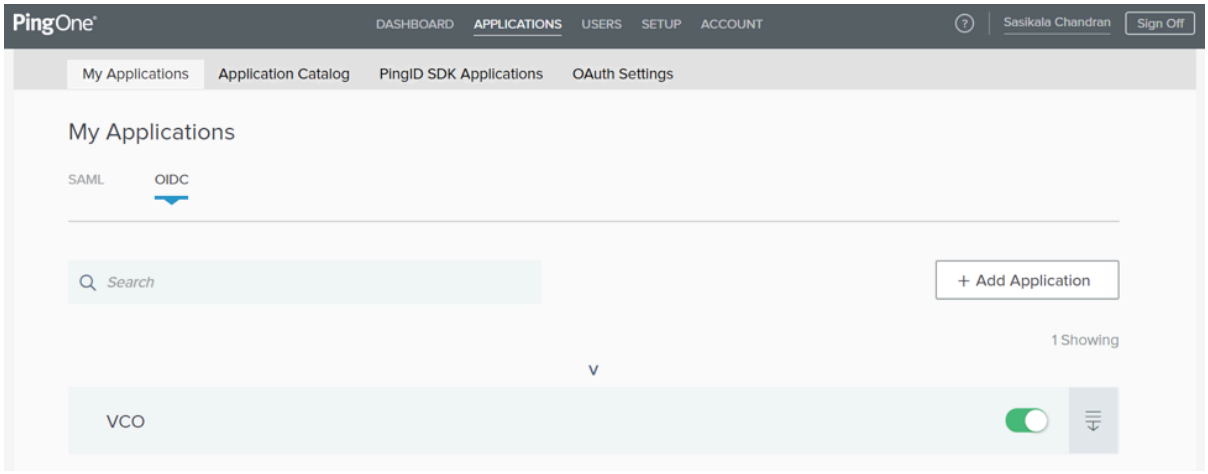
To set up an OpenID Connect (OIDC)-based application in Ping Identity for Single Sign On (SSO), perform the steps on this procedure.

Ensure you have a PingOne account to sign in.

Note: Currently, Orchestrator supports PingOne as the Identity Partner (IDP); however, any PingIdentity product supporting OIDC can be easily configured.

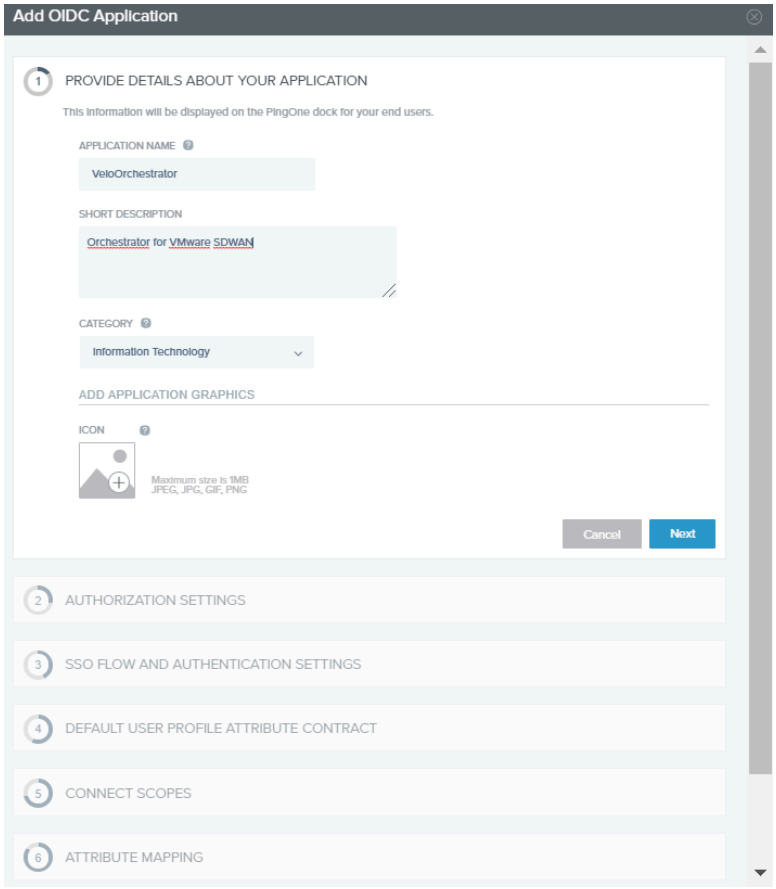
1. Log in to your PingOne account as an Admin user. The **PingOne** home screen appears.
2. To create a new application:
   a. In the upper navigation bar, click **Applications**.

Figure 3-30: My Applications



b. On the **My Applications** tab, select **OIDC** and then click **Add Application**. The **Add OIDC Application** pop-up window appears.

Figure 3-31: Adding an OIDC Application



c. Provide basic details such as name, short description, and category for the application and click **Next**.

d. Under **AUTHORIZATION SETTINGS**, select **Authorization Code** as the allowed grant types and click **Next**.

   Also, note down the Discovery URL and Client Credentials (Client ID and Client Secret) to be used during the SSO configuration in Orchestrator.

e. Under **SSO FLOW AND AUTHENTICATION SETTINGS**, provide valid values for Start SSO URL and Redirect URL and click **Next**.

   In the Orchestrator application, at the bottom of the **Configure Authentication** screen, you can find the redirect URL link. Ideally, the Orchestrator redirect URL will be in this format: **`https://<Orchestrator URL>/login/ssologin/openidCallback`**. The Start SSO URL will be in this format: **`https://<Orchestrator URL>/<domain name>/login/doEnterpriseSsoLogin`**.

f. Under **DEFAULT USER PROFILE ATTRIBUTE CONTRACT**, click **Add Attribute** to add additional user profile attributes.

g. In the **Attribute Name** text box, enter ***group_membership*** and then select the **Required** checkbox, and select **Next**.

> **Note:** The ***group_membership*** attribute is required to retrieve roles from PingOne.

h. Under **CONNECT SCOPES**, select the scopes that can be requested for your Orchestrator application during authentication and click **Next**.

i. Under **Attribute Mapping**, map your identity repository attributes to the claims available to your Orchestrator application.

> **Note:** The minimum required mappings for the integration to work are email, given_name, family_name, phone_number, sub, and group_membership (mapped to member Of).

j. Under **Group Access**, select all user groups that should have access to your Orchestrator application and click **Done**. The application will be added to your account and will be available in the **My Application** screen.

You have completed setting up an OIDC-based application in PingOne for SSO.

Chapter 4

Enterprise Settings

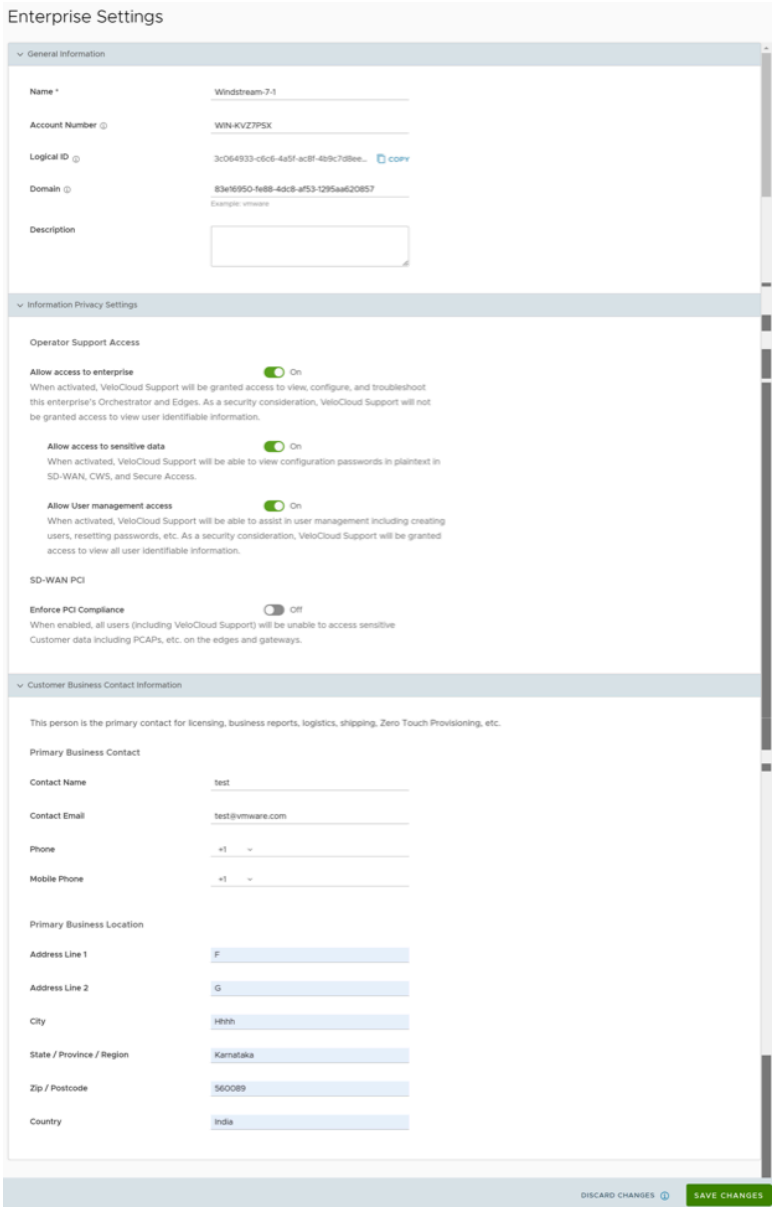
The **Enterprise Settings** option allows you to configure the user information, privacy settings, and primary contact details for the Enterprise users.

Follow the below steps to configure **Enterprise Settings**:

1. In the **Enterprise** portal, on the **Global Navigation** bar, expand the **Enterprise Applications** drop-down menu.
2. Select **Global Settings** service.

3. From the left menu, select **Enterprise Settings**. The following screen appears:

Figure 4-1: Enterprise Settings Screen



4. You can configure the following parameters, and then select **Save Changes**:

Table 17: Enterprise Settings Option Descriptions

Option	Description
General Information	
Name	Enter the name of the new Customer. This field is mandatory.
Account Number	Enter the account number for the Customer.
Logical ID	Displays a unique identifier. You can copy this unique ID to be used by the APIs.
Domain	The domain name is used to activate the SSO authentication for the Orchestrator and to turn on the Edge Intelligence.  **Note:** Modifying the domain after configuration, affects the EI integration with the Orchestrator.
Description	Enter a description. This field is optional.
Information Privacy Settings	Use the toggle button to allow or deny access to sensitive data and user management. Turn on the **Enforce PCI Compliance** to prevent operations that are disallowed for PCI compliance reasons. Currently, the only operation this option prevents is the ability to request PCAP Diagnostic Bundles from the Edge.
Customer Business Contact Information	Enter primary contact details of the Customer such as contact name, email address, phone number, location details etc.

After you have configured the **Enterprise Settings**, you must set up the SSO Authentication. Before setting up the SSO authentication, you must set up Users and Roles. For additional information, see User Management.

Chapter 5

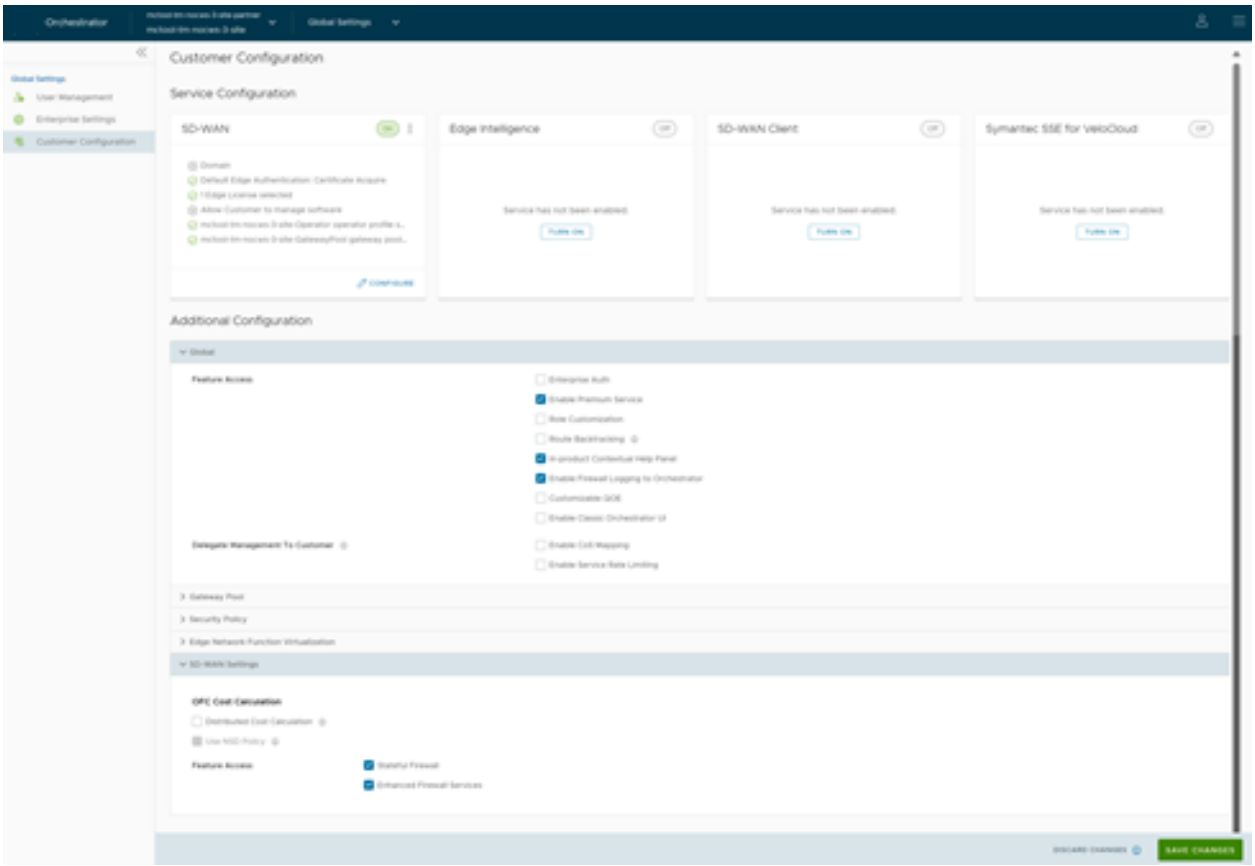
Configure Customers

After creating a Customer, configure the feature options and settings that the Customer can access. You can choose the settings the Customer can modify. Only an Operator user can configure Customer settings.

When you create a new Customer, you are redirected to the **Customer Configuration** page, where you can configure the Customer settings. You can also navigate to the **Customer Configuration** page by following the steps below:

1. In the **Enterprise** portal, on the **Global Navigation** bar, expand the **Enterprise Applications** drop-down menu.
2. Select **Global Settings** service.
3. From the left menu, select **Customer Configuration**. The following page is displayed:

   Figure 5-1: Global Settings- Customer Configuration



The **Service Configuration** section includes the following services:

- **SD-WAN**
- **Edge Intelligence**

- **SD-WAN Client**
- **Symantec SSE for VeloCloud**

Select the **Turn On** button to activate each service. Select the vertical ellipsis present at the top right corner of each tile to turn off or configure that service. You can also use the **Configure** option present at the bottom right corner of each tile to configure the respective service. Each tile displays the configuration summary.

Note: When you select **Turn off** option, a pop-up window appears asking for your confirmation. Select the check box and select **Turn Off Service**.

a. **SD-WAN**: Selecting the **Configure** option displays the following pop-up window. Configure the settings, and then select **Update**.

Figure 5-2: SD-WAN Configuration

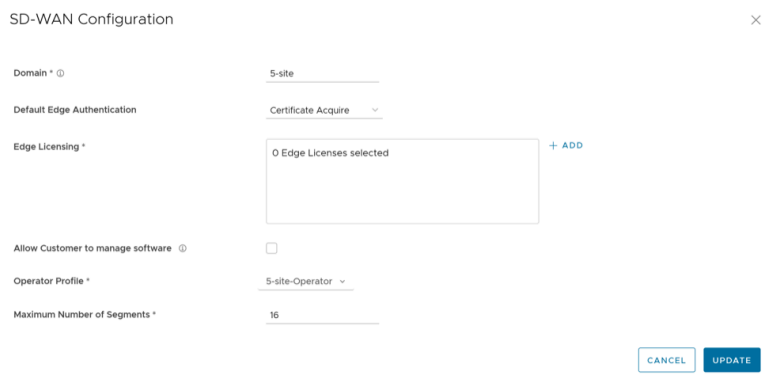


Table 18: SD-WAN Option Descriptions

Option	Description
Domain	Enter the domain name to be used to activate Single Sign On (SSO) authentication for the Orchestrator. This is also required to activate Edge Intelligence for the Customer.
Default Edge Authentication	Choose the default option to authenticate the Edges associated to the Customer, from the drop-down menu. • **Certificate Deactivated**: Edge uses a pre-shared key mode of authentication. • **Certificate Acquire**: This option is selected by default and instructs the Edge to acquire a certificate from the certificate authority of the Orchestrator, by generating a key pair and sending a certificate signing request to the Orchestrator. Once acquired, the Edge uses the certificate for authentication to the Orchestrator and for establishment of VCMP tunnels. **Note:** After acquiring the certificate, the option can be updated to **Certificate Required**. • **Certificate Required**: Edge uses the PKI certificate. Operators can change the certificate renewal time window for Edges using the system property `edge.certificate.renewal.window`.
Edge Licensing	The existing Edge Licenses are displayed. Select **Add** to add or remove the licenses. **Note:** The license types can be used on multiple Edges. It is recommended to provide your Customers with access to all types of licenses to match their edition and region. For additional information, see the topic *Edge Licensing* in *VeloCloud SD-WAN Administration Guide*.
Allow Customer to Manage Software	Select the check box if you want to allow an Enterprise Super User to manage the software images available for the Enterprise. For additional information, see the topic *Edge Image Management* in *VeloCloud SD-WAN Administration Guide*.
Operator Profile	Select an Operator profile to be associated with the Customer from the available drop-down menu. This field is not available if **Allow Customer to Manage Software** is selected. For additional information on Operator profiles, see the topic *Manage Operator Profiles* in *VeloCloud SD-WAN Administration Guide*
Maximum Number of Segments	Enter the maximum number of segments that can be configured. The valid range is 1 to 16.The default value is **16**.

b. **Edge Intelligence**: Selecting the **Configure** option displays the following pop-up window. Configure the settings, and then select **Update**.

Note: You can select this option only when the **SD-WAN** service is turned on.

Figure 5-3: Edge Intelligence Configuration

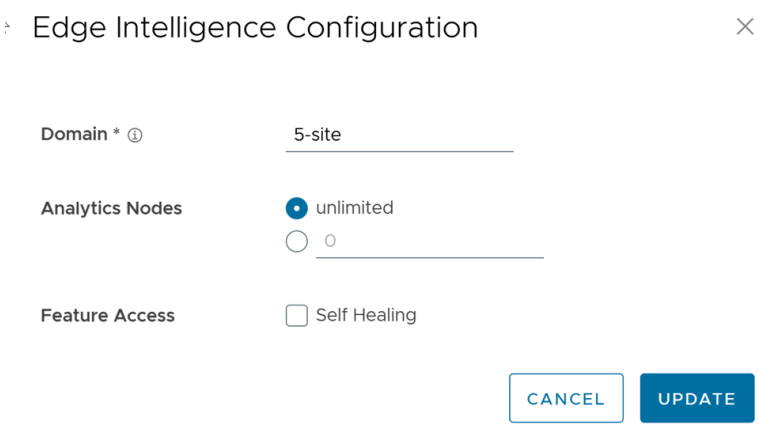


Table 19: Customer Configuration Option Descriptions

Option	Description
Domain	Enter the domain name to be used to activate Single Sign On (SSO) authentication for the Orchestrator. This is also required to activate Edge Intelligence for the Customer.
Analytics Nodes	Enter the maximum number of Edges that can be provisioned as Analytics Nodes. By default, **Unlimited** is selected.
Feature Access	Select the **Self Healing** check box to allow the Edge Intelligence to provide recommendations to improve performance.

c. **SD-WAN Client**: This service allows you to access the SD-WAN Client account. For additional information, see *VeloCloud SD-WAN Client Administrator Guide*.

d. **Symantec SSE for VeloCloud**: This service allows you to access the Symantec SSE for VeloCloud account. For additional information, see *Symantec SSE for VeloCloud User Guide*.

4. Following are the additional configuration settings available on the **Customer Configuration** page:

Table 20: Customer Configuration

Option	Description
Global	
User Agreement Display	Select either of the following from the drop-down menu: • Inherit • Override to Hide • Override to Show **Note:** This field is available only when the system property `session.options.enableUserAgreements` is set to **True**.
Feature Access	Provides access to the selected features. Select one or more check boxes from the below list to activate these features for the Customer: • **Enterprise Auth**: By default, only the Operator can activate or deactivate two-factor authentication for an Enterprise. When you select this check box, the Enterprise Admins can configure the two-factor authentication on their own. This option also controls the activation and deactivation of Single Sign On (SSO). • **Enable Premium Service**: This option is selected by default. Premium Service refers to the On-Demand Remediation feature that is a core part of SD-WAN's Dynamic Multipath Optimization (DMPO). DMPO is used for all traffic that traverses a VeloCloud Gateway. When Premium Service is selected, the Gateway uses Forward Error Correction (FEC) for customer traffic impacted by high levels of WAN link jitter or loss, and which cannot be steered to a better quality WAN link. When Premium Service is not selected, traffic still traverses the VeloCloud Gateway and benefits from other components of DMPO like Continuous Monitoring, Dynamic Application Steering, and Secure Traffic Transmission. However, traffic impacted by high levels of WAN link jitter or loss does not benefit from error correction by the Gateway. For more information, see the topic *Dynamic Multipath Optimization (DMPO)* in the *VeloCloud SD-WAN Administration Guide*. • **Role Customization**: Allows an Enterprise Super user to customize the role privileges for other Enterprise users. • **Route Backtracking**: Allows the device to choose the best route in the order of prefix length. • **In-product Contextual Help Panel**: Provides access to the 'In Product Help' panel integrated within the Orchestrator. This feature is deactivated by default. An Operator must activate this option for the Enterprise Customers. • **Enable Firewall Logging to Orchestrator**: By default, Edges cannot send their Firewall logs to the Orchestrator. Select this check box to allow an Edge to send the Firewall logs to the **Orchestrator**. • **Customizable QoE**: Allows the Customer to configure the minimum and maximum latency threshold values for Voice, Video, and Transactional application categories of an Edge. • **Enable Classic Orchestrator UI**: Allows the Customer to switch from the **Angular Orchestrator UI** to the **Classic Orchestrator UI**. This option is available only when the system property `session.options.enableClassicOrchestrator` is set to **True**.

Option	Description
Delegate Management To Customer	Allows the Customer to modify the settings of the selected property. Following two properties are always visible to the Customers: • **Enable CoS Mapping**: Allows to configure CoS mapping while configuring a business policy. • **Enable Service Rate Limiting**: Allows to rate limit services in a business policy.
Gateway Pool	
Current Gateway Pool	Displays the current Gateway pool associated with the selected Customer. If required, you can choose a different Gateway pool available in the drop-down menu and select **Save Changes**.
Gateways in this Pool	Displays the Gateway details in the current pool.
Partner Hand Off	Activating the **Gateway Pool** option displays the **Configure Hand Off** section. If the Gateways available in the Gateway pool have been assigned with Partner Gateway role, you can handoff the Gateways to Partners.
Security Policy	
Hash	By default, there is no authentication algorithm configured for the VPN header as AES-GCM is an authenticated encryption algorithm. When you select the **Turn off GCM** check box, you can select one of the following as the authentication algorithm for the VPN header, from the drop-down menu: • **SHA 1** • **SHA 256** • **SHA 384** • **SHA 512**
Encryption	Select either **AES 128** or **AES 256** as the AES algorithm's key size to encrypt data. The default encryption algorithm mode is **AES 128**.
DH Group	Select the Diffie-Hellman (DH) Group algorithm to be used when exchanging a pre-shared key. The DH Group sets the strength of the algorithm in bits. The supported DH Groups are 2, 5, 14, 15, 16, 19, 20, and 21. DH Groups 19, 20, and 21 are available starting in Release 5.2.0.  **Note:** It is recommended to use DH Group **14**, which is the default value.
PFS	Select the Perfect Forward Secrecy (PFS) level for additional security. The supported PFS Groups are 2, 5, 14, 15, 16, 19, 20, and 21. PFS Groups 19, 20, and 21 are available starting in Release 5.2.0. By default, PFS is deactivated.
Turn off GCM	Select this check box to activate **Hash** and select an authentication algorithm for the VPN header.
IPSec SA Lifetime Time(min)	Time when Internet Security Protocol (IPSec) rekeying is initiated for Edges. The minimum IPsec lifetime is 3 minutes and maximum IPsec lifetime is 480 minutes. The default value is `480` minutes.  **Note:** It is not recommended to configure low lifetime value for IPsec (less than 10 minutes), as it can cause traffic interruption in some deployments due to rekeys. The low lifetime values are for debugging purposes only.
IKE SA Lifetime(min)	Time when Internet Key Exchange (IKE) rekeying is initiated for Edges. The minimum IKE lifetime is 10 minutes and maximum IKE lifetime is 1440 minutes. The default value is `1440` minutes.  **Note:** It is not recommended to configure low lifetime values IKE (less than 30 minutes), as it can cause traffic interruption in some deployments due to rekeys. The low lifetime values are for debugging purposes only.

Option	Description
Secure Default Route Override	Select the check box so that the destination of traffic matching a secure default route (either Static Route or BGP Route) from a Partner Gateway can be overridden using Business Policy.
Edge Network Function Virtualization: Allows to activate NFV on the Edges and allows Customers to deploy third party VNFs on service ready Edge platforms. Currently, the service ready Edge platform models are 520v and 840. As an Operator User, when you activate the **Edge NFV**, the Customers can configure and deploy VNFs and VNF licenses from their network services.	
Edge NFV	Select this option to activate the ability to deploy VNFs on Edges. After deploying one or more VNFs on Edges, you cannot deactivate this option.
Security VNFs	Select the relevant check boxes, to deploy the corresponding security VNFs on Edges. For additional information, see the topic *Security VNFs* in the *VeloCloud SD-WAN Administration Guide*
SD-WAN Settings	
OFC Cost Calculation	Select the required check box: • **Distributed Cost Calculation**: Select this check box to delegate route cost calculation to Edges/Gateways. **Note:** This option is available only for the Edges/Gateways with version 3.4.0 and later. After activating **Distributed Cost Calculation**, it is recommended to refresh the routes by navigating to **Configure** > **Overlay Flow Control** in the **SD-WAN** service of the Enterprise portal.
Multiple-DSCP tags per Flow Path Calculation	This feature is used when the original user traffic is encapsulated in another tunnel (GRE/IPsec) and the DSCP labels are saved in the new IP header. The feature activates path calculation for a single flow (same source/destination) with multiple DSCP tags and offers path differentiations based on the DSCP values in the flow. Select the **Include DSCP value as part of flow lookup** check box to include DSCP values as part of flow look-up and path calculation. **Note:** This field is available only when the system property `session.options.enableFlowParametersConfig` is set to **True**.
Feature Access	
Stateful Firewall	Select the **Stateful Firewall** check box to override the Stateful Firewall settings activated on the Enterprise Edge.
Enhanced Firewall Services	Select the **Enhanced Firewall Services** check box to activate the Enhanced Firewall Services using the Firewall functionality in Edge Cloud Orchestrator. **Note:** For Enhanced Firewall Services (EFS) to work, ensure the Edge version is upgraded to 5.2.0.0. **Note:** Unselecting this option will only deactivate the EFS feature in the UI. To deactivate the EFS feature for an existing customer, you must first deactivate the EFS feature in the SD-WAN service of the Enterprise portal by navigating to **Configure** > **Profiles/Edges** > **Firewall** > **Enhanced Firewall Services** and then by unselecting this check box in Global Settings. For additional information about configuring Enhanced Firewall Services Policy rule, see the topic *Configure Enhanced Firewall Services* in the *VeloCloud SD-WAN Administration Guide*.

5. Select **Save Changes**.

Note: When you modify the **Security Policy** settings, the changes may cause interruptions to the current services. In addition, these settings may reduce overall throughput and increase the

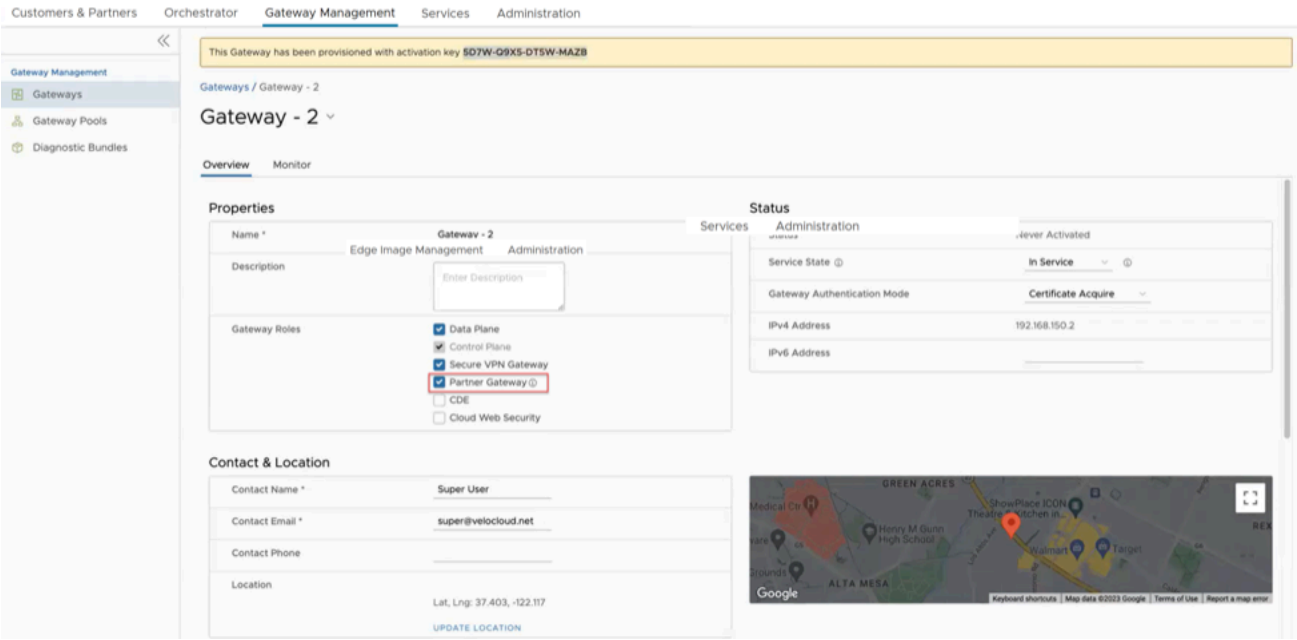
time required for VCMP tunnel setup, which may impact branch to branch dynamic tunnel setup times and recovery from Edge failure in a cluster.

5.1 Configure Partner Handoff

You can configure a Gateway to hand off to Partners. The Gateway acts as a Partner Gateway that enables you to configure the Hand off Interface, Static Routes, BGP, and other settings.

Ensure that the Gateway to be handed off is assigned with Partner Gateway role. In the Orchestrator portal (Operator or Partner), select **Gateways** and select the link to an existing Gateway. In the **Properties** section of the selected Gateway's Overview page, you can enable the **Partner Gateway** role as shown in the following screenshot:

Figure 5-4: Partner Gateway Management



Procedure:

To configure the Handoff settings, perform the following steps:

1. In the **Enterprise** portal, on the **Global Navigation** bar, expand the **Enterprise Applications** drop-down menu.
2. Select **Global Settings** service, and then from the left menu, select **Customer Configuration**.
3. In the **Customer Configuration** window, scroll down to **Additional Configuration** and expand the **Gateway Pool** area.
4. Turn on the **Partner Hand Off** toggle button.

5. In the **Configure Hand Off** area, configure the following fields in the table below:

Figure 5-5: Configure Partner Hand Off

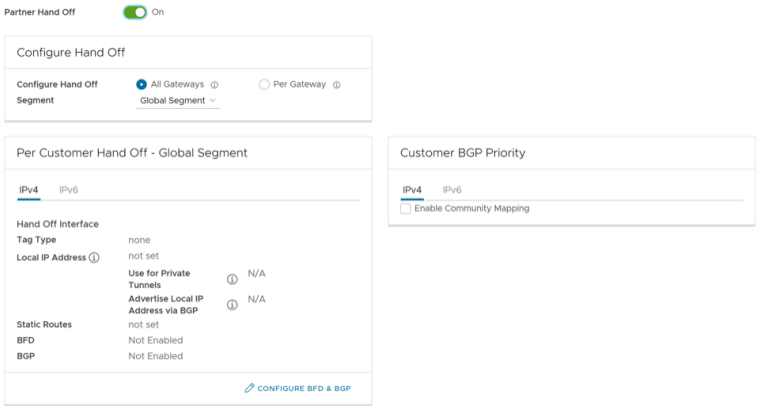
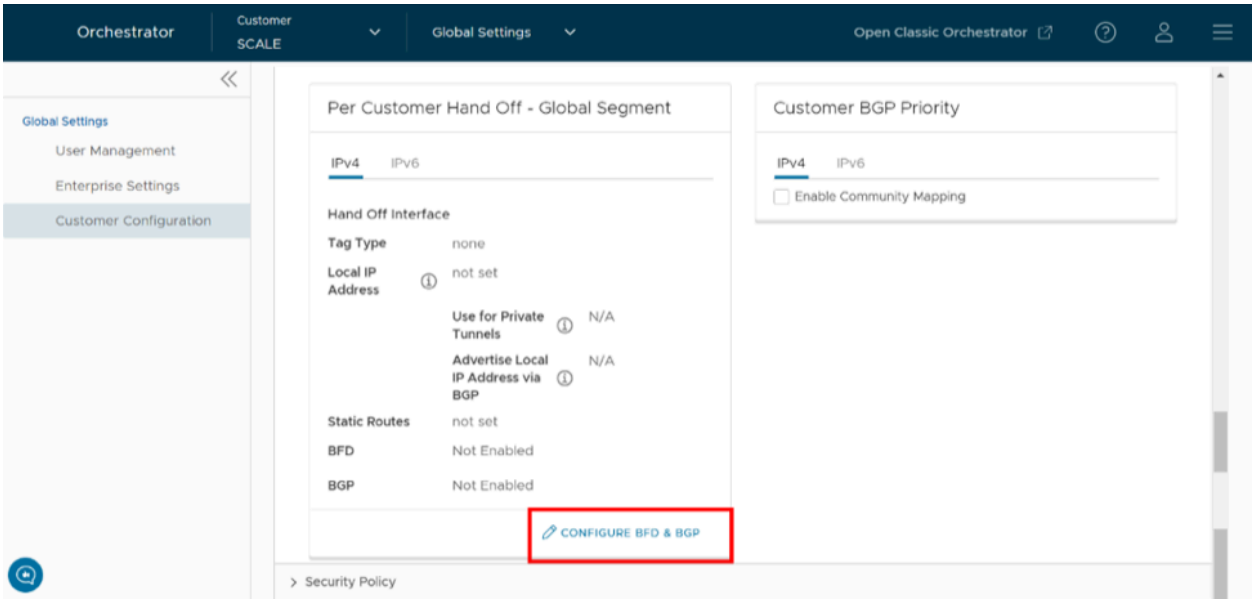


Table 21: Partner Handoff Option Descriptions

Option	Description
Configure Hand Off	By default, the hand off configuration is applied to all the Gateways. If you want to configure a specific Gateway, choose **Per Gateway**, and then select the Gateway from the drop-down list.
Segment	By default, **Global Segment** is selected, which means that the hand off configuration is applied to all the segments. If you want to configure a specific segment, select the segment from the drop-down menu.
Hand Off Interface	This section displays the values that are configured on the **Configure BGP and BFD** page.
Customer BGP Priority	Select the check box and configure the Community Mapping details.

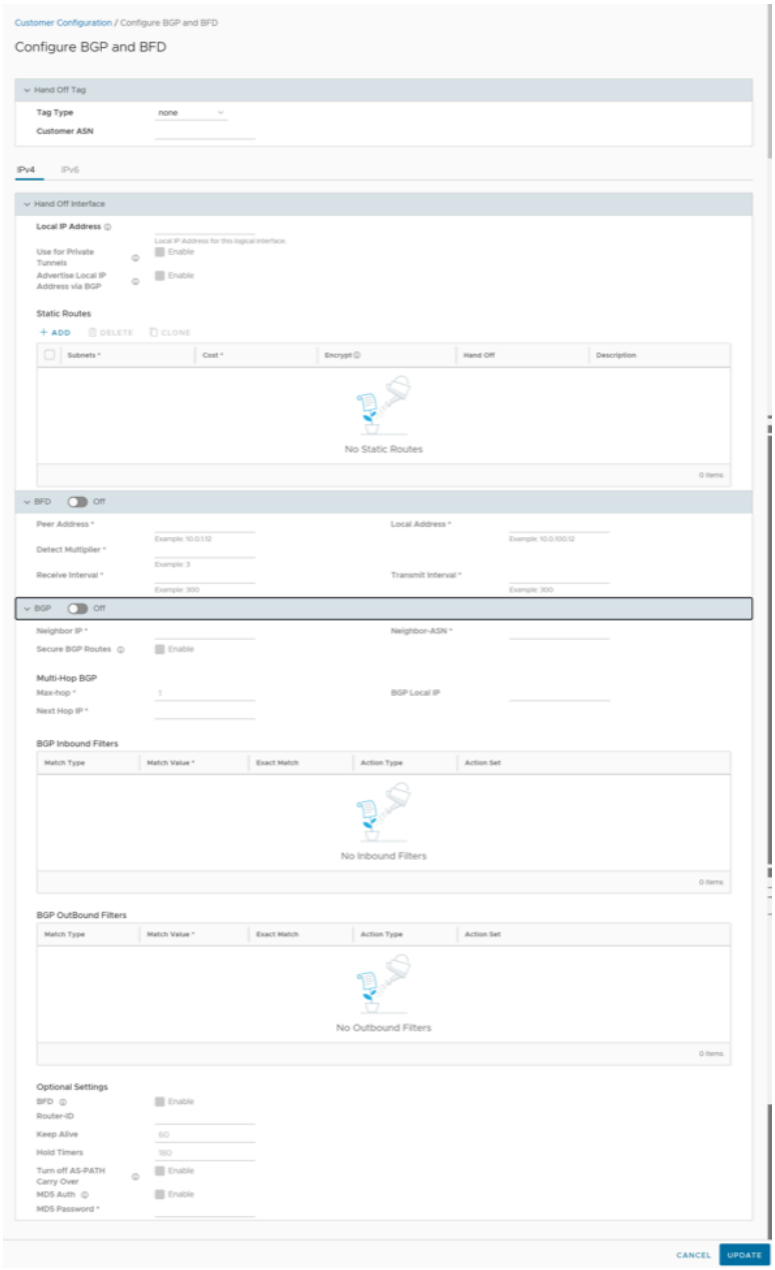
6. At the bottom of the **Per Customer Hand Off – Global Segment** area, select the **Configure BFD & BGP** link, as shown in the image below.

Figure 5-6: Per Customer Hand Off – Global Segment



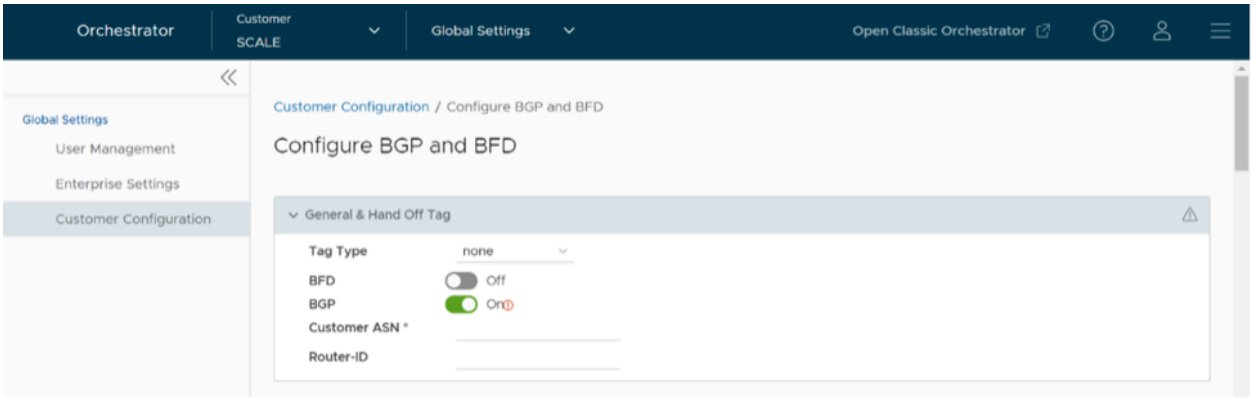
The **Configure BGP and BFD** screen displays, as shown in the image below.

Figure 5-7: Configure BFD and BGP



7. Open the **General & Hand Off Tag** section and turn the **BGP** option to the **On** position. See figure below.

Figure 5-8: General & Hand Off Tag



8. Scroll down to the **BGP** section and select the arrow to display the **BGP** section.
9. Configure the fields in the table below.

Table 22: General & Hand Off Tag Option Descriptions

Option	Description
Hand Off Tag	
Tag Type	Choose the tag type, which is the encapsulation, in which the Gateway hands off customer traffic to the Router. The following are the types of tags available: • **None**: Untagged. Choose this during single tenant hand off or a hand off towards shared services VRF. • **802.1Q**: Single VLAN tag • **802.1ad / QinQ(0x8100) / QinQ(0x9100)**: Dual VLAN tag
Customer ASN	Enter the Customer Autonomous System Number.
Hand Off Interface: You can configure the following settings for IPv4 and IPv6.	
Local IP Address	Enter the Local IP address for the logical Hand Off interface.
Use for Private Tunnels	Select the check box so that private WAN links connect to the private IP address of the Partner Gateway. If private WAN connectivity is activated on a Gateway, the Orchestrator audits to ensure that the local IP address is unique for each Gateway within an Enterprise.
Advertise Local IP Address via BGP	Select the check box to automatically advertise the private WAN IP of the Partner Gateway through BGP. The connectivity is provided using the existing Local IP address.
Static Routes: You can add, delete, or clone a static route.	
Subnets	Enter the IP address of the Static Route Subnet that the Gateway should advertise to the Edge.
Cost	Enter the cost to apply weight age on the routes. The range is from 0 to 255.
Encrypt	Select the check box to encrypt the traffic between Edge and Gateway.
Hand off	Select the hand off type as either **VLAN** or **NAT**.
Description	Enter a descriptive text for the static route. This field is optional.
BFD: Turn the toggle button to On to activate this section.	
Peer Address	Enter the IP address of the remote peer to initiate a BFD session.
Detect Multiplier	Enter the detection time multiplier. The remote transmission interval is multiplied by this value to determine the detection timer for connection loss. The range is from 3 to 50.
Receive Interval	Enter the minimum time interval, in milliseconds, at which the system can receive the control packets from the BFD peer. The range is from 300 to 60000 milliseconds.
Local Address	Enter a locally configured IP address for the peer listener. This address is used to send the packets.
Transmit Interval	Enter the minimum time interval, in milliseconds, at which the system can send the control packets from the BFD peer. The range is from 300 to 60000 milliseconds.
BGP: Turn the toggle button to On to activate this section.	
Neighbor IP	Enter the IP address of the configured BGP neighbor network.
Secure BGP Routes	Select the check box to allow encryption for data-forwarding over BGP routes.
Max-hop	Enter the number of maximum hops to allow multi-hop for the BGP peers. The range for Max-hop is from 1 to 255, and the default value is **1**. **Note:** This field is available only for eBGP neighbors, when the local ASN and the neighboring ASN are different.

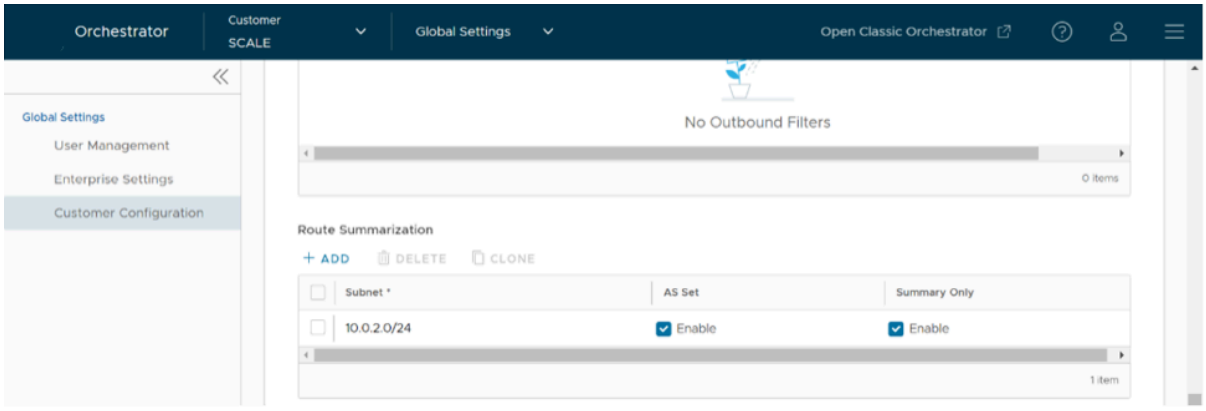
Option	Description
Next Hop IP	Enter the next-hop IP address to be used by BGP to reach the multi-hop BGP peer. **Note:** This option is available only for multi-hop eBGP with Max-hop count greater than 1.
Neighbor-ASN	Enter the Autonomous System Number of the Neighbor network.
BGP Local IP	Local IP address is the equivalent of a loopback IP address. Enter an IP address that the BGP neighborships can use as the source IP address for the outgoing BGP packets. If you do not enter any value, the IP address of the **Hand Off Interface** is used as the source IP address.
BGP Inbound Filters	Displays the BGP inbound filters.
BGP Outbound Filters	Displays the BGP outbound filters.
BGP Optional Settings	
BFD	Select the check box to subscribe to the BFD session.
Router-ID	Enter the Router ID to identify the BGP Router.
Keep Alive	Enter the BGP Keep Alive time in seconds. The default timer is **60** seconds.
Hold Timers	Enter the BGP Hold time in seconds. The default timer is **180** seconds.
Turn off AS-PATH Carry Over	Select the check box to turn off AS-PATH carry over, which influences the outbound AS-PATH to make the L3-routers prefer a path towards a PE. If you select this option, ensure to tune your network to avoid routing loops. It is recommended not to select this check box.
MD5 Auth	Select the check box to activate BGP MD5 authentication. This option is used in a legacy network or federal network, and is used as a security guard for BGP peering.
MD5 Password	Enter a password for MD5 authentication. **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.

Route Summarization is new for the 5.2 release. For an overview, use case, and black hole routing details for Route Summarization, see the section titled, *Route Summarization* in the *VeloCloud SD-WAN Administration Guide*. For Route Summarization configuration details, follow the steps below:

a. If applicable, configure for Route Summarization.

b. Scroll down to the **Route Summarization** area in the **BGP** section.

Figure 5-9: Route Summarization Screen



c. Configure the Route Summarization fields, as described in the table below:

Table 23: Route Summarization Options

Option	Description
+Add	Select **+Add** to add a new row in the **Route Summarization** area. **Note:** To add additional rows to configure Route Summarization, select **+Add**. To Clone or Delete a route summarization, use the appropriate buttons, located next to **+Add**.
Subnet column	Under the **Subnet** column, enter the IP subnet.
AS Set column	Generate AS set path information from the summarized routes (while advertising the summarized route to the peer). Under the **AS Set** column, select the **Yes** check box if applicable.
Summary Only column	Under the **Summary Only** column, select the **Yes** check box to allow only the summarized route to be sent.

d. Select **Update** to save the settings.

5.2 Configure Distributed Cost Calculation

By default, the **Orchestrator** is actively involved in learning the dynamic routes. VMware SD-WAN Edges and Gateways rely on the **Orchestrator** to calculate initial route preferences and return them to the Edge and Gateway. The Distributed Cost Calculation feature enables you to distribute the route cost calculation to the Edges and Gateways. Only an Operator user can configure Customer settings, including Distributed Cost Calculation.

Ensure the following before you enable the Distributed Cost Calculation feature.

- All the Edges and Gateways must use software version 3.4.0 or later.
- The software image associated with the Operator Profile must use version 3.4.0 or later.

Note:

Anybody experiencing an issue with **Orchestrator** based route calculation needs **Distributed Cost Calculation** enabled.

This default method of involving the Orchestrator in both dynamic route calculation and the distribution of those routes to Edges and Gateways has the following drawbacks:

- If the Orchestrator is under a high load, the route convergence time is significantly high (for example, as much as 40 seconds for 2000+ routes), as the **Orchestrator** takes that time to calculate the preference for all the synchronized routes and returns those preferences to the Edges and Gateways.
- Using the **Orchestrator** for route calculation means that new dynamic routes learned while the Orchestrator was unreachable are not advertised until the Orchestrator becomes reachable again.

When a customer enterprise uses Distributed Cost Calculation, the **Orchestrator** is no longer actively involved in the route preference calculation and instead routes are properly inserted in order by the Edge and Gateway instantly upon learning them and then convey these preferences to the **Orchestrator**.

When you choose to enable Distributed Cost Calculation for the Edges and Gateways, the feature provides the following benefits:

- Minimizes the impact on route learning when an **Orchestrator** is unreachable.
- Route convergence time is reduced from minutes to seconds in large networks with thousands of dynamic routes.
- Network delays are significantly reduced.
- Provides instantaneous Data Plane convergence.
- Supports enhanced re-ordering and pinning of routes on the Overlay Flow Control.
- Provides an option to refresh routes in the **Overlay Flow Control** page. Whenever there is a change in the Overlay Flow Control policy, the Refresh Routes option applies the changes to the existing routes immediately, without the need to restart the Edge or Gateway.

Enabling Distributed Cost Calculation has the following impacts on the Customer Enterprise network:

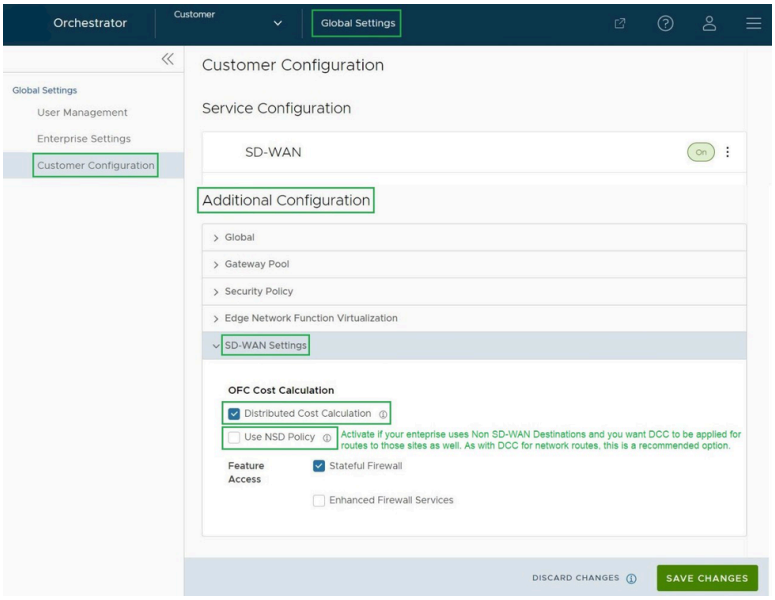
- All the local dynamic routes are refreshed, and the preference and advertise action of these routes are updated. This updated information is advertised to the Gateway, Orchestrator, and eventually across the Enterprise. The customer's network needs to completely rebuild the route table, which for most customer deployments will take less than 5 seconds. A large scale customer deployment (like 100,000+ routes) may take up to 2 minutes. During the time the route table is being rebuilt, customer traffic for all sites is impacted.
- Any existing flow using these routes can potentially be affected due to the change in the routing entries.

Note: It is recommended to enable Distributed Cost Calculation in a maintenance window to minimize the impact on the Customer Enterprise.

To configure Distributed Cost Calculation for a customer:

1. In the Operator portal, navigate to **Manage Customers**.
2. Select a customer and either select **Edit Customer System Settings** or select the link to the customer.

3. In the **Enterprise** portal, go to **Global Settings** > **Customer Configuration**.
4. **Figure 5-10: Distributed Cost Calculation**



5. In the **Customer Configuration** page, navigate to the **Additional Configuration** > **SD-WAN Settings** > **OFC Cost Calculation** section and configure the following:
   - Select the **Distributed Cost Calculation** checkbox to delegate the cost calculation of routes to Edges and Gateways.
   - Select the **Use NSD Policy** checkbox to use the Non SD-WAN Destination policy for route cost calculation of Edges and Gateways. This option is available only for Edges and Gateways that are running Software version 4.3.0 or later.
6. Select **Save Changes**.

Note: After enabling **Distributed Cost Calculation**, it is recommended to refresh the routes in the **Overlay Flow Control** page in the **SD-WAN** service of the **Enterprise** portal.

Note: When an Enterprise has **Distributed Cost Calculation** activated and a user tries to deactivate the software update in the **Operator Profile** page, then the user must ensure that, in future, no Edges in the Enterprise are downgraded to software image versions lower than 3.4.0. If one or more Edges in the Enterprise is using software image version below 3.4.0, the Enterprise traffic may take a sub-optimal path. The sub-optimal path will be corrected only when the Edge is upgraded to 3.4.0 or later versions.

The following are some of the scenarios in which the software versions can change and the user must make sure the Edges are using the software image version 3.4.0 or later:

- Factory Reset- When an Edge is reset to factory settings, it restores the software version of the Edge to factory image version which can be below 3.4.0.
- Edge Activation- When an Edge is activated, it may come up with software versions below 3.4.0.

Once **Distributed Cost Calculation** is activated, all the dynamic routes are assigned with new preferences and advertise action based on the Distributed Cost Calculation and the new information is propagated across the Enterprise Network.

The **Orchestrator** is no longer actively involved in the route preference calculation and instead the routes are properly inserted in order by the Edge and Gateway instantly upon learning them and then these preferences are conveyed to the **Orchestrator**.

The Overlay Flow Control policy is sent to Edges and Gateways in Control Plane Configuration updates. Edges and Gateways send the routes with computed cost and advertise action to the Orchestrator. Edges and Gateways handle the order of the routes based on the cost and route attributes.

To view a summary of all the routes in your network, select **Configure** > **Overlay Flow Control** in the **SD-WAN** service of the **Enterprise** portal. You can view the routes and advertise action in the **Overlay Flow Control** page. For additional information, see the topic *Overlay Flow Control* in the *VeloCloud Administration Guide*.

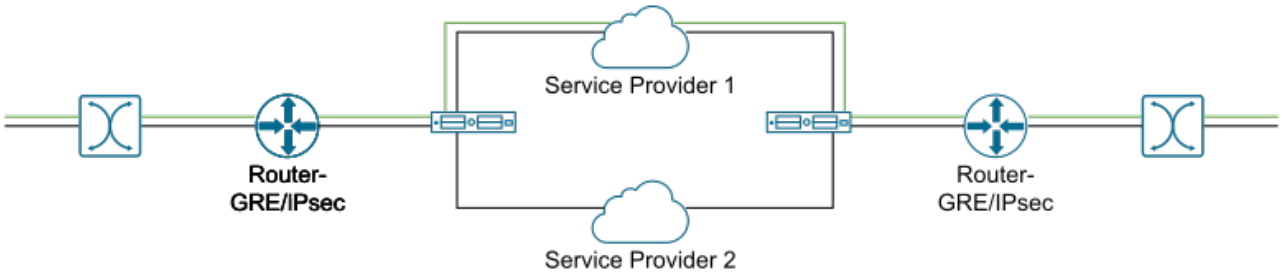
5.3 Configure Path Calculation with Multiple DSCP Labels per Flow

An Edge classifies a traffic flow based on the first packets in the flow. You can create business policies with application based on Differentiated Service Code Point (DSCP) and with different DSCP markings to determine the flow treatment.

By default, an Edge classifies a flow based on the first few packets received in the flow. Business Policy and QoS marking determine the flow treatment. Once the flow is classified, an entry with five tuple information of the flow is created in the flow cache table. Subsequent packets in the flow will use the five-tuple lookup against the flow cache table.

For network topologies with Layer 3 network devices doing encapsulation and/or encryption before the traffic arrives at the Edge, this creates a challenge for the Edge to forward traffic based on the Business Policy. The traffic from the end users is multiplexed into single flow with the same source and destination IP addresses, and protocols by the Layer 3 encapsulation/encryption device, as illustrated in the following image.

Figure 5-11: Single Flow Traffic



The impact of multiplexing end user flows into a single tunnel creates polarization of flow forwarding using the five tuples of flow cache table, which results in WAN links not being utilized.

The Path Calculation with Multiple DSCP Labels per Flow allows the DSCP value to be included, in addition to the five tuples, as part of the flow cache table lookup. Use the path calculation with multiple DSCP tags

when the original user traffic is encapsulated in another tunnel like GRE or IPsec, and DSCP labels are preserved in the new IP header. This option enables path calculation for a single flow with multiple DSCP labels, which consists of same source and destination IP addresses, and offers path differentiations based on the DSCP labels in the flow.

When you enable the **Multiple-DSCP tags per Flow Path Calculation**, the Edges can differentiate the traffic flows based on the DSCP marked labels.

To enable Multiple-DSCP tags per Flow Path Calculation:

1. In the **Operator** portal, select **Orchestrator** > **System Properties**.
2. Select **New**.
3. In the **New System Property** window, create a system property with the following parameters:
   - **Name**: *session.options.enableFlowParametersConfig*
   - **Data Type**: *Boolean*
   - **Value**: *True*
4. Select **Save Changes**.
5. In the **Operator** portal, navigate to **Global Settings** > **Customer Configuration** > .
6. In the **Customer Configuration** page, go to the additional configuration settings section, and then under **SD-WAN settings**, select the **Include DSCP value as part of flow lookup** check box for **Multiple-DSCP tags per Flow Path Calculation**.

   Note: This option is available only when the system property `session.options.enableFlowParametersConfig` is set to **True**.

7. Select **Save Changes**.
8. In the Edges, different flows are created based on different DSCP labels.

Note: When you select **Include DSCP value as part of flow lookup**, the inter-operability with previous versions is undefined.

While configuring the business policy for an Edge, you can choose to match a DSCP label for an application. For additional information, see the topic *Configure Business Policy Rule* in the *VeloCloud Administration Guide*.

When traffic arrives at the Edge, if the traffic flow matches with the selected application and DSCP tag, then the corresponding action is performed.

You can create more business policies with different DSCP labels to match with different traffic flows and apply different treatments for those flows. For additional information on business policies, see the *VeloCloud SD-WAN Administration Guide.*

Limitations:

- The path calculation with multiple DSCP labels per Flow is not applicable for the Gateways. You can enable this option only for Edge-to-Edge tunnels, where Edge-to-Edge can be any of the following:
  - Edge-to-Edge through Hub
  - Spoke-to-Hub
  - Dynamic Branch-to-Branch

  You can use this option for On-Premise deployment where Gateway is used only for control plane functionality and not for data plane traffic.
- The path calculation with multiple DSCP labels per Flow is intended only for GRE or IPSec traffic. The direct Internet traffic does not carry multiple DSCP labels within a single flow.
- After you enable the path calculation option, when the traffic flow consists of packets with same five-tuple information but different DSCP markings, LAN side NAT might not work as expected.

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 Partner Guide*
- *Arista VeloCloud SD-WAN Gateway Monitoring Guide*
- *Arista VeloCloud SD-WAN Troubleshooting Guide*
- *Arista VeloCloud SD-WAN Orchestrator Deployment and Monitoring Guide*
- *Arista VeloCloud SD-WAN Design Guide for Enhanced Firewall Services*
- *Arista VeloCloud SD-WAN API*
- *Arista VeloCloud Portal API*