

# ARISTA

## Global Settings Guide

### VeloCloud SASE

Version 6.0



<b>Headquarters</b>	<b>Support</b>	<b>Sales</b>
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
<a href="http://www.arista.com/en/">www.arista.com/en/</a>	<a href="mailto:support@arista.com">support@arista.com</a>	<a href="mailto:sales@arista.com">sales@arista.com</a>

© Copyright 2025 Arista Networks, Inc. All rights reserved. The information contained herein is subject to change without notice. The trademarks, logos, and service marks ("Marks") displayed in this documentation are the property of Arista Networks in the United States and other countries. Use of the Marks is subject to the Arista Networks Terms of Use Policy, available at [www.arista.com/en/terms-of-use](http://www.arista.com/en/terms-of-use). Use of marks belonging to other parties is for informational purposes only.

# Contents

**Chapter 1: VeloCloud Global Settings Guide..... 1**

**Chapter 2: Overview.....2**

**Chapter 3: User Management - Enterprise..... 3**

- 3.1 Users.....3
  - 3.1.1 Add New User..... 5
  - 3.1.2 API Tokens..... 7
- 3.2 Roles..... 9
  - 3.2.1 Add Role..... 12
- 3.3 Service Permissions..... 14
  - 3.3.1 New Permission..... 17
  - 3.3.2 List of User Privileges..... 18
- 3.4 Authentication..... 41
  - 3.4.1 Configure Azure Active Directory for Single Sign On.....46
  - 3.4.2 Configure Okta for Single Sign On.....51
  - 3.4.3 Configure OneLogin for Single Sign On.....55
  - 3.4.4 Configure PingIdentity for Single Sign On.....59

**Chapter 4: Enterprise Settings..... 62**

**Chapter 5: Configure Customers.....65**

- 5.1 Configure Partner Handoff..... 71
- 5.2 Configure Distributed Cost Calculation..... 79
- 5.3 Configure Path Calculation with Multiple DSCP Labels per Flow..... 82

**Chapter 6: References..... 85**

- 6.1 Related Documents..... 85

## 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.

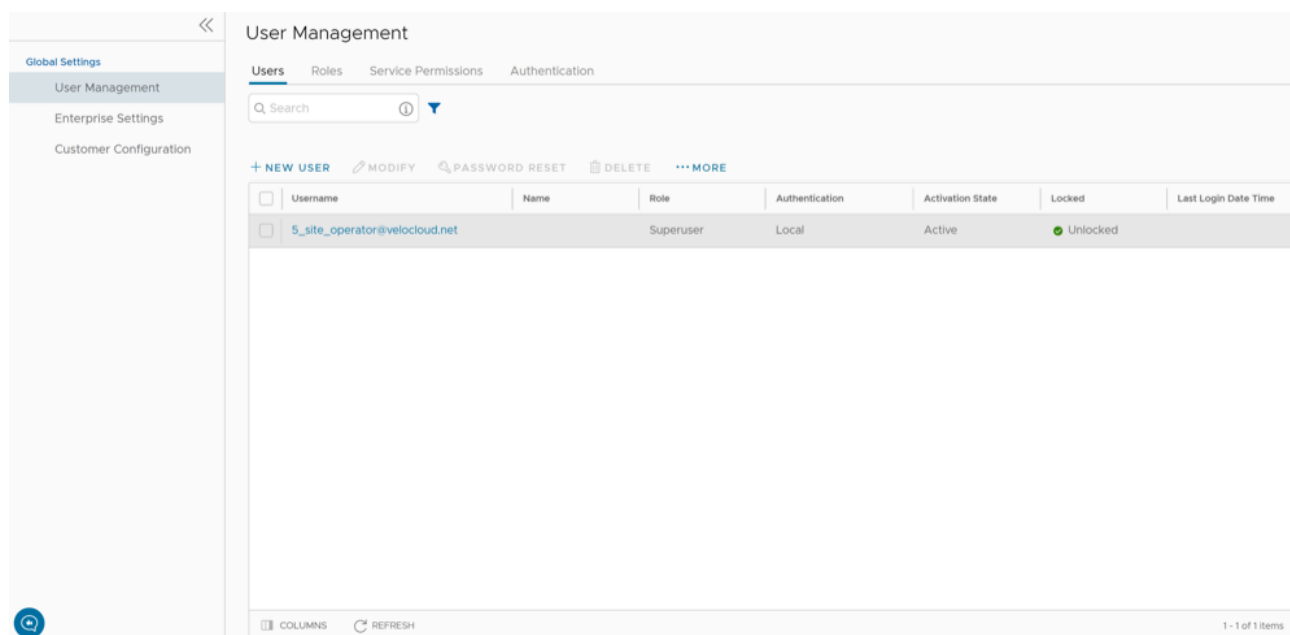
## Overview

Considering the number of services available in the Orchestrator, the Administration section has evolved from the SD-WAN service into its 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 the **SD-WAN** service. The features under **Global Settings** are shared across all services.

The following features reside under Enterprise **Global Settings**: **Global Settings** > **User Management**

**Figure 2-1: User Management**



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](#)
- [Enterprise Settings](#)
- [Configure Customers](#)



**Note:** This feature is available only for Operator users.

## User Management - Enterprise

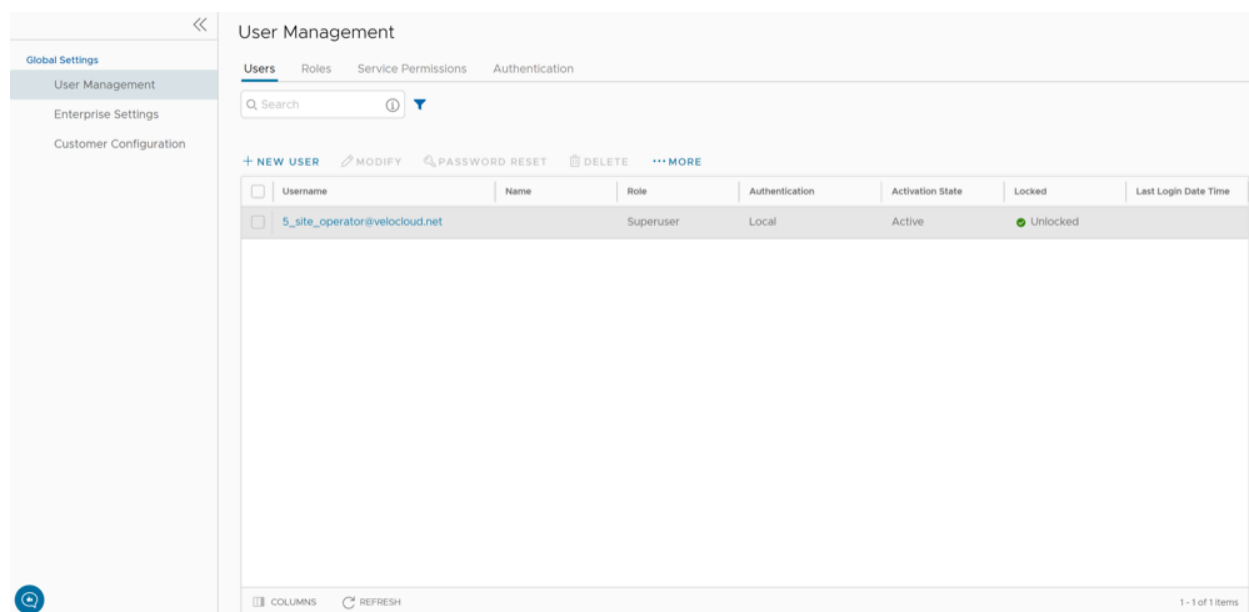
The User Management feature allows you to manage users, their roles, service permissions (formerly known as Role Customization), and authentication.

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**



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

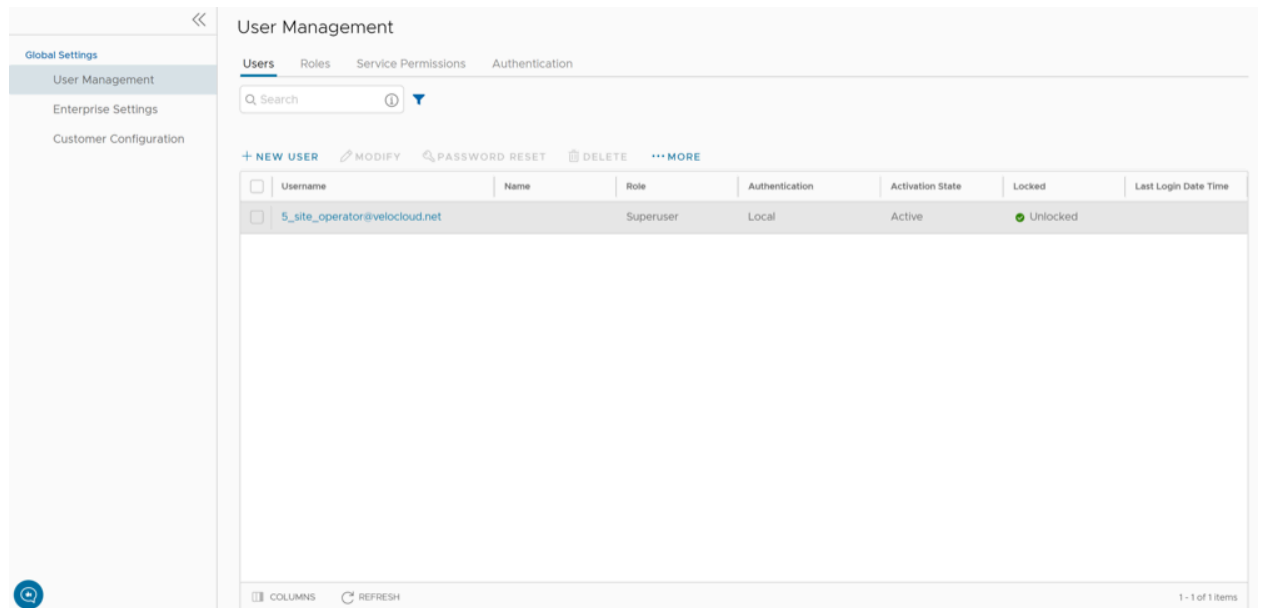
You can view the existing Admin users. Only Enterprise Superusers can create new Admin users with different roles, and configure API tokens for each Admin user.

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: Users Tab**



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

**Table 1: Users Tab- Options and Descriptions**

Option	Description
New User	Creates a new Admin user. For additional information, see <a href="#">Add New User</a> .
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 <b>Download</b> 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: Additional Options**

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

Only Enterprise Superusers 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, 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.

#### 4. Select New User.

Figure 3-3: New User

The screenshot displays a web interface for creating a new user, divided into three main sections:

- General Information:** This section is titled "User Name / Set Password / Contact Information". It includes fields for "Authentication" (Local/Remote), "Username", "Contact Email", "Password", "Confirm Password", "First Name", "Last Name", "Phone", and "Mobile Phone". A "NEXT" button is located at the bottom of this section.
- Role:** This section is titled "Role defines the permissions this user has in services available". It contains a search bar and a table of roles. The table has columns for "Role" and "Descriptions".

Role	Descriptions
Enterprise Standard Admin	Can view and manage network and security services
Enterprise Superuser	Can view, edit and create users, global settings, and has full access across all services
Enterprise Support	Can monitor Edges, activity, and initiate diagnostic actions in their network and can monitor their security service
Enterprise Read Only User	Read only view of their company's network services
Enterprise Security Admin	Can view and manage their security services. Has read only access to the network



A "NEXT" button is located at the bottom of this section.
- Edge Access:** This section is titled "SD-WAN Edge Access Privileges". It includes an "Access Level" dropdown (Basic/Privileged) and an "Add another user" checkbox. "ADD USER" and "CANCEL" buttons are at the bottom.

#### 5. 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- Options and Descriptions**

Option	Description
Authentication	<p>Select an authentication mode:</p> <ul style="list-style-type: none"> <li>• <b>Local:</b> This is the Native authentication mode, which is the default option.</li> <li>• <b>Remote:</b> This is the Non-Native authentication mode, which is a Single Sign On (SSO) authentication service that allows you to login to Orchestrator using one set of login credentials to access multiple applications.</li> </ul>
Username	Enter a username in the format of an email address.
Contact Email	The email address is auto-populated. You can edit it if required.
Password	<p>Enter a unique password.</p> <div style="border: 1px solid #00a0e3; padding: 5px; margin-top: 10px;">  <p><b>Note:</b> Starting from the 4.5 release, the use of the special character "&lt;" in the password is no longer supported. In cases where users have already used "&lt;" in their passwords in previous releases, they must remove it to save any changes on the page.</p> </div>
Confirm Password	Re-enter the password.
First Name	Enter the first name of the user. This field is optional.
Last Name	Enter the last name of the user. This field is optional.
Phone	Enter the phone number of the user. This field is optional.
Mobile Phone	Enter the mobile number of the user. This field is optional.
Role	Select a role that you want to assign to the user. For information on roles, see <a href="#">Roles</a> .
Edge Access	<p>Choose one of the following options:</p> <ul style="list-style-type: none"> <li>• <b>Basic:</b> Allows you to perform certain basic debug operations such as <code>ping</code>, <code>tcpdump</code>, <code>PCAP</code>, <code>remote diagnostics</code>, and so on.</li> <li>• <b>Privileged:</b> Grants you the root-level access to perform all basic debug operations along with Edge actions such as <code>restart</code>, <code>deactivate</code>, <code>reboot</code>, <code>hard reset</code>, and <code>shutdown</code>. In addition, you can access Linux shell.</li> </ul> <p>The default value is <b>Basic</b>.</p> <div style="border: 1px solid #00a0e3; padding: 5px; margin-top: 10px;">  <p><b>Note:</b> To configure this option, you must have a role that allows access to the <b>SD-WAN</b> service.</p> </div>

6. 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.
7. Click 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. For additional information, see [API Tokens](#).

### 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:

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

**Figure 3-4: API Tokens**

UUID	Name	Description	Created	Expiration	State	Created By	Token Type	Customer	Created For
eed6fc38-77...	test		May 19, 2023, 7:34:55 PM	May 18, 2024, 7:34:55 PM	Pending	super@vel...	Customer	1-site	1_site_operator@velocloud.n...

- Select **New API Token**.

**Figure 3-5: New Token**

New Token [View documentation](#) ×

Name \*

Description

Lifetime \*  Months

- In the **New Token** window, enter a **Name** and **Description** for the token, and then choose the **Lifetime** from the drop-down menu.
- 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**.

9. To download the token, select the token, and then select **Download API Token**.
10. To deactivate a token, select the token, and then select **Revoke API Token**. The status of the token is displayed as **Revoked**.
11. Select **CSV** to download the complete list of API tokens in a .csv file format.
12. 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 } }'
```

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

**Table 4: Additional Options**

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: Enterprise Roles**

Role	SD-WAN Service	Cloud Web Security Service	Secure Access Service	Global Settings Service
Enterprise Standard Admin	SD-WAN Enterprise Admin	Cloud Web Security Enterprise Admin	Secure Access Enterprise Admin	Global Settings Enterprise Admin
Enterprise Superuser	SD-WAN Enterprise Superuser	Cloud Web Security Enterprise Superuser	Secure Access Enterprise Superuser	Global Settings Enterprise Superuser
Enterprise Support	SD-WAN Enterprise Support	Cloud Web Security Enterprise Read Only	Secure Access Enterprise Read Only	Global Settings Enterprise Support
Enterprise Read Only User	SD-WAN Enterprise Read Only	No privileges	No privileges	Global Settings Enterprise Read Only
Enterprise Security Admin	SD-WAN Security Enterprise Admin	Cloud Web Security Enterprise Admin	Secure Access Enterprise Admin	Global Settings Enterprise Admin
Enterprise Security Read Only	SD-WAN Security Enterprise Read Only	Cloud Web Security Enterprise Read Only	Secure Access Enterprise Read Only	Global Settings Enterprise Read Only
Enterprise Network Admin	SD-WAN Enterprise Admin	Cloud Web Security Enterprise Read Only	Secure Access Enterprise Read Only	Global Settings Enterprise Admin

If required, you can customize the privileges of these roles. For additional information, see [Service Permissions](#).

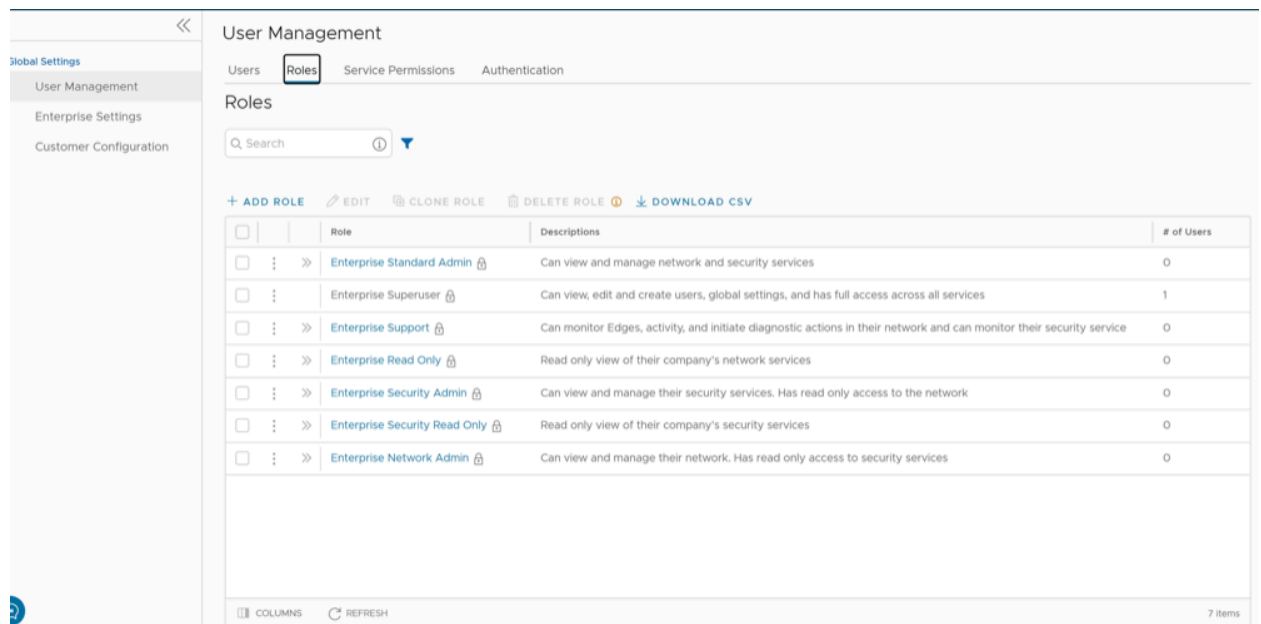
As a Customer, you can view the list of existing standard roles and their corresponding descriptions. You can add, edit, clone, or delete a new role. However, you cannot edit or delete a default role.

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 Tab**



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

**Table 6: Roles Tab- Options and Descriptions**

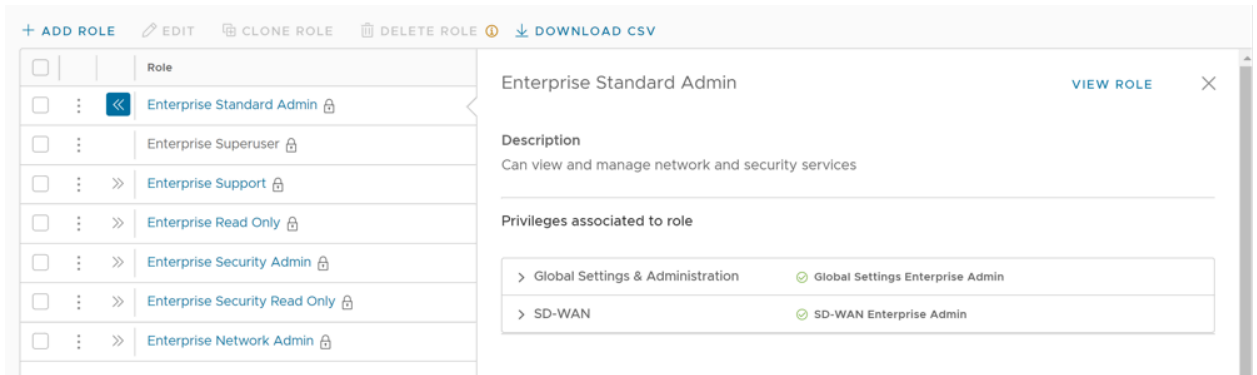
Option	Description
Add Role	Creates a new custom role. For additional information, see <a href="#">Add Role</a> .
Edit	Allows you to edit only the custom roles. You cannot edit the default roles. Also, you cannot edit or view the settings of a Superuser.
Clone Role	Creates a new custom role, by cloning 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: Open Icon**



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: Additional Options**

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: Add Role**

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

**Table 8: Add Role - Options and Descriptions**

Option	Description
<b>Role Details</b>	
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.
<b>Role Creation</b>	
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, <b>Global Settings Enterprise Read Only</b> 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 <b>No Privileges</b> .



**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.

#### 7. 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 Tab**

The screenshot shows the 'Service Permissions' tab within the 'User Management' section. The left sidebar contains navigation options: 'Global Settings', 'User Management', 'Enterprise Settings', and 'Customer Configuration'. The main content area has tabs for 'Users', 'Roles', 'Service Permissions', and 'Authentication'. Below the tabs, there is a 'Service' dropdown menu set to 'All'. A toolbar includes '+ NEW PERMISSION', 'EDIT', 'CLONE', 'PUBLISH PERMISSION', and '...MORE'. A table lists permissions with columns for 'Permission Name', 'Service', 'Role Associated', 'Last Modified', and 'Published'. One permission named 'test' is listed, associated with 'Global Settings' and 'Enterprise Superuser', last modified on 'Oct 3, 2022, 5:19:17 PM', and marked as 'Published'. At the bottom, there are 'COLUMNS' and 'REFRESH' buttons, and a '1 item' indicator.

Permission Name	Service	Role Associated	Last Modified	Published
test	Global Settings	Enterprise Superuser	Oct 3, 2022, 5:19:17 PM	Published


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


**Table 9: Service Permissions- Options and Descriptions**

Option	Description
Service	<p>Select the service from the drop-down menu. The available services are:</p> <ul style="list-style-type: none"> <li>• <b>All</b></li> <li>• <b>Global Settings</b></li> <li>• <b>SD-WAN</b></li> </ul> <p>Custom service permissions, if any, associated with the selected service are displayed. By default, all of the custom service permissions are displayed.</p>
New Permission	Allows you to create a new permission. For additional information, see <a href="#">New Permission</a> .
Edit	Allows you to edit the settings of the selected permission. You can also select the link to the <b>Permission Name</b> 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	<p>Allows you to select from the following additional options:</p> <ul style="list-style-type: none"> <li>• <b>Delete:</b> Deletes the selected permission. You cannot delete a permission if it is already in use.</li> </ul> <div style="border: 1px solid #add8e6; padding: 5px; margin: 5px 0;"> <p> <b>Note:</b> A permission can only be deleted if it is in a draft mode. The <b>Delete</b> 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 <b>Delete</b> option for the permission.</p> </div> <ul style="list-style-type: none"> <li>• <b>Download JSON:</b> Downloads the list of permissions into a file in JSON format.</li> <li>• <b>Upload Permission:</b> Allows you to upload a JSON file of a customized permission.</li> <li>• <b>Reset to System Default:</b> 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.</li> </ul>

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

**Table 10: Additional Options**

Option	Description
Columns	<p>Select the columns to be displayed or hidden on the page.</p> <div style="border: 1px solid #add8e6; padding: 5px; margin: 5px 0;"> <p> <b>Note:</b> The <b>Role Associated</b> column displays the Roles using the same Privilege Bundle.</p> </div>
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 Permission**

Service Permissions / test

test

Permission Details

Name \* test

Description

Service \* Global Settings

Privilege Bundle \* Global Settings Enterprise Superuser

Privileges [DOWNLOAD CSV](#)


Privileges	Description	Read	Create	Update	Delete	Feature
Authentication Service	Privilege controlling the creation and configuration of hosted 802.1x service providing LAN-side user authentication	<input checked="" type="checkbox"/> On	<input checked="" type="checkbox"/> On	<input checked="" type="checkbox"/> On	<input checked="" type="checkbox"/> On	
Cloud Security Service	Privilege controlling the creation and configuration of third party cloud security services to which traffic can be steered by business policy	<input checked="" type="checkbox"/> On	<input checked="" type="checkbox"/> On	<input checked="" type="checkbox"/> On	<input checked="" type="checkbox"/> On	
Cloud Subscription Service	Privilege granting the ability to view and manage the configuration of access to IAAS providers, such as Azure, AWS and Google Cloud	<input checked="" type="checkbox"/> On	<input checked="" type="checkbox"/> On	<input checked="" type="checkbox"/> On	<input checked="" type="checkbox"/> On	
Customer	Privilege granting the ability to view and manage Customers, from the Partner or Operator level	<input checked="" type="checkbox"/> On	<input type="checkbox"/> Off	<input checked="" type="checkbox"/> On	<input type="checkbox"/> Off	
Customer Alert Notification	Privilege granting the ability to view and manage customer alert configuration	<input checked="" type="checkbox"/> On	<input type="checkbox"/> Off	<input type="checkbox"/> Off	<input type="checkbox"/> Off	
Customer Authentication	Privilege granting the ability to view and manage customer authentication mode, for example SSO, Radius or Native	<input type="checkbox"/> Off	<input type="checkbox"/> Off	<input type="checkbox"/> Off	<input type="checkbox"/> Off	
Customer Delegation	Privilege granting the ability to view and manage the delegation of privileges from the customer to Partners or the Operator	<input checked="" type="checkbox"/> On	<input checked="" type="checkbox"/> On	<input checked="" type="checkbox"/> On	<input checked="" type="checkbox"/> On	
Customer Edge Settings	Privilege granting the ability to activate or deactivate Configuration Updates for an Edge.	<input checked="" type="checkbox"/> On	<input type="checkbox"/> Off	<input checked="" type="checkbox"/> On	<input type="checkbox"/> Off	
Customer General Information	Privilege granting the ability to choose a default certificate for an Edge, and activate or deactivate Secure Edge Access.	<input checked="" type="checkbox"/> On	<input type="checkbox"/> Off	<input checked="" type="checkbox"/> On	<input type="checkbox"/> Off	
Customer Privacy Settings	Privilege granting the ability to control access to sensitive Customer data.	<input checked="" type="checkbox"/> On	<input type="checkbox"/> Off	<input checked="" type="checkbox"/> On	<input type="checkbox"/> Off	

Objects per page 10 151 Items 1 / 16


CANCEL SAVE SAVE AND APPLY

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

**Table 11: New Permission- Options and Descriptions**

Option	Description
Name	Enter an appropriate name for the permission. <div data-bbox="667 302 1508 373"> <b>Note:</b> The permission name must be unique within the Orchestrator it is hosted upon.</div>
Description	Enter a description. This field is optional.
Service	Select a service from the drop-down menu. The available services are: <ul style="list-style-type: none"><li>• <b>Global Settings</b></li><li>• <b>SD-WAN</b></li></ul>
Privilege Bundle	Select a privilege bundle from the drop-down menu. The privileges are populated depending on the selected <b>Service</b> .
Privileges	Displays the list of privileges based on the selected <b>Privilege Bundle</b> . 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: List of User Privileges

Navigation Path in the Enterprise Portal	Name of the Tab	Elements in the Tab	Name of the Privilege	Description	Allow Privilege	Deny Privilege	Customizable		
<b>Monitor &gt; Edges &gt; Select Edge</b>	Overview		Read Edge	Grants ability to view and manage Edge objects and their properties in general	Yes	No	No		
		Top Applications Top Categories	Read Edge	Grants ability to view and manage Edge objects and their properties in general	Yes	No	No		
		Top Operating Systems	View Flow Stats	Grants ability to view collected flow statistics	Yes	Yes	Yes		
		Top Sources							
	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	
		Change Hostname		Create Client Device	Controls visibility to unique identifiers (IP or MAC address) of LAN-side client devices	Yes	No	No	
				Read Client Device					
				Update Client Device					
				Delete Client Device					
		Operating Systems		Manage Client Device					
				Create Client User	Controls visibility to potentially Personal Identifiable Information(PII) in flow statistics	Yes	No	No	
				Read Client User					
				Update Client User					
		Applications Sources Destinations		Delete Client User					
			Manage Client User						
			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
Monitor	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
			Create Diagnostic Bundle		No	Yes	Yes
			Read Remote Diagnostics	Privilege granting access to view and execute remote diagnostics	No	Yes	Yes
	Edges	Edge Cluster	Read Edge	Grants ability to view and manage Edge objects and their properties in general	Yes	No	No
			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
			Read Customer Event	Grants ability to view customer level events	Yes	No	No
			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
			Read Non SD-WAN Destination via Edge				
			Read Network Service	Grants ability to view and manage services with the Network Services configuration block	Yes	No	No
			Read Edge	Grants ability to view and manage Edge objects and their properties in general	Yes	No	No
			Read VNF Network Service	Grants ability to manage VNF Network Services	No	Yes	Yes
	Routing		Read Edge Cluster	Controls the ability to create and configure Edge Clusters	No	Yes	Yes
			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	
Configure > Edge > Select Edge	Alerts		View Customer Routing	Grants ability to view the customer Routing	Yes	No	No	
			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	
	Edge Overview	Properties	Edge Overview	Controls ability to view or modify Edge overview page	No	Yes	Yes	
			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	
		Name		Update Edge Overview Properties			Yes	Yes
				Delete Edge Overview Properties				
				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	Controls ability to view or change Edge description on the Edge overview page	No	Yes	Yes
			Update Edge Overview Properties Description				
	Enable Alerts		Read Edge Overview Properties Enable Alerts	Controls ability to view or change Edge alert configuration on the Edge overview page	No	Yes	Yes
			Update Edge Overview Properties Enable Alerts				
	Authentication Mode		Read Edge Overview Properties Auth Mode	Controls ability to view or change Edge PKI configuration on the Edge overview page	No	Yes	Yes
			Update Edge Overview Properties Auth Mode				
			Read Customer PKI	Grants ability to view and manage enterprise PKI settings	Yes	No	No
			Update Customer PKI				
	Serial Number		Read 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
			Update Edge Overview Properties Serial Number				
	Generate New Activation Key		Read Edge Overview Properties Activation Expiration	Controls ability to view or change the activation key expiration period on the Edge overview page	No	Yes	Yes
			Update Edge Overview Properties Activation Expiration				
	Send Activation Email button		Create Edge Overview Properties Activation Email	Controls ability to generate an activation email on the Edge overview page	No	Yes	Yes
			Read Edge Overview Properties Activation Email				
	Local Credentials		Read Overview Properties Local Credentials	Grants ability to view and configure Edge local credentials	No	Yes	Yes
			Update Overview Properties Local Credentials				

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 Read Edge Overview Profile Update Edge Overview Profile Delete Edge Overview Profile	Controls visibility and control of Edges assigned profile on the Edge overview page	No	Yes No Yes	Yes No Yes
	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 Read Edge Device Authentication Settings Update Edge Device Authentication Settings Delete Edge Device Authentication Settings	Controls ability to view or change Edge Device Authentication Settings	No	Yes	Yes
	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 Read Edge Device Netflow Settings Update Edge Device Netflow Settings Delete Edge Device Netflow Settings	Controls ability to view or change Edge Device Netflow Settings	No	Yes	Yes
	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	Voice Quality Monitoring Settings	Read Edge Device VQM Settings	Controls ability to view or change Edge Device VQM Settings	No	Yes	Yes
			Update Edge Device VQM Settings				
	Syslog Settings	Syslog Settings	Read Edge Device Syslog Settings	Controls ability to view or change Edge Device Syslog Settings	No	Yes	Yes
			Update Edge Device Syslog Settings				
	Static Route Settings	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	ICMP Probes	Read Edge Device ICMP Probes	Controls ability to view or change Edge Device ICMP Probes	No	Yes	Yes
			Update Edge Device ICMP Probes				
	ICMP Responders	ICMP Responders	Read Edge Device ICMP Responders	Controls ability to view or change Edge Device ICMP Responders	No	Yes	Yes
			Update Edge Device ICMP Responders				
	VRRP Settings	VRRP Settings	Update Edge Device VRRP Settings	Controls ability to view or change Edge Device VRRP Settings	No	Yes	Yes
	Cloud VPN	Cloud VPN	Read Edge Device Cloud VPN	Controls ability to view or change Edge Device Cloud VPN	No	Yes	Yes
			Update Edge Device Cloud VPN				
	BFD Rules	BFD Rules	Update Edge Device BFD Rules	Controls ability to view or change Edge Device BFD Rules	No	Yes	Yes
	BGP Settings	BGP Settings	Read Edge Device BGP Settings	Controls ability to view or change Edge Device BGP Settings	No	Yes	Yes
			Update Edge Device BGP Settings				
	Multicast Settings	Multicast Settings	Read Edge Device Multicast Settings	Controls ability to view or change Edge Device Multicast Settings	No	Yes	Yes
			Update Edge Device Multicast Settings				
	Cloud Security Service	Cloud Security Service	Read Edge Device Cloud Security Service	Controls ability to view or change Edge Device Cloud Security Service	No	Yes	Yes
			Update Edge Device Cloud Security 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
		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	Read Edge Device High Availability	Controls ability to view or change Edge Device High Availability	No	Yes	Yes
		Update Edge Device High Availability	Delete Edge Device High Availability				
		Enable HA Standby Pair	Enable HA Cluster	Grants ability to configure standby HA	No	Yes	Yes
		Enable HA VRRP Pair		Grants ability to configure HA Clustering	No	Yes	Yes
	Configure VLAN	Read Edge Device Settings		Grants ability to configure VRRP HA	No	Yes	Yes
	Management IP	Read Edge Device Management IP	Update Edge Device Management IP	Controls ability to view or change Edge Device Management IP	No	Yes	Yes
	Device Settings	Create Edge Device Settings	Read Edge Device Settings	Controls ability to view or change Edge Device Settings	No	Yes	Yes
		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	Read Edge Device Wi-Fi Settings	Controls ability to view or change Edge Device Wi-Fi Settings	No	Yes	Yes
		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 Update Edge Business Policy Rate Limit	Controls the ability to read and update the rate limiting business policy feature	No	Yes	Yes
		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 Read Edge Firewall Edge Access Update Edge Firewall Edge Access Delete 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
	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	
<b>Configure &gt; Profiles &gt; Select Profile</b>	Remote Diagnostics		Read Remote Diagnostics	Grants access to view and execute remote diagnostics	No	Yes	Yes	
	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	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	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	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	BFD Rules	Update Profile Device BFD Rules	Controls ability to view or change Profile Device BFD Rules	No	Yes	Yes
	OSPF Areas	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	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	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	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	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	Configure VLAN	Read Profile Device Settings	Controls ability to view or change Profile Device Settings	No	Yes	Yes
	Management IP	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	Controls ability to view or change Profile Device Settings	No	Yes	Yes
			Read Profile Device Settings				
			Update Profile Device Settings				
			Delete Profile Device Settings				
		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	Controls ability to view or change Profile Device Wi-Fi Settings	No	Yes	Yes
			Read Profile Device Wi-Fi Settings				
			Update Profile Device Wi-Fi Settings				
			Delete Profile Device Wi-Fi Settings				
		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	Controls ability to view or change Profile Device Cloud VPN QoS Settings	No	Yes	Yes
			Update Profile Device Cloud VPN QoS Settings				
		SNMP Settings	Create Profile Device SNMP Settings	Controls ability to view or change Profile Device SNMP Settings	No	Yes	Yes
			Read Profile Device SNMP Settings				
			Update Profile Device SNMP Settings				
			Delete Profile Device SNMP Settings				
		NTP	Read Profile Device NTP Settings	Controls ability to view or change Profile Device NTP Settings	No	Yes	Yes
			Update Profile Device NTP Settings				
		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				
<b>Configure</b>	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	Controls ability to view or change Edge alert configuration on the Edge overview page	No	Yes	Yes
	Select Edge/ Edges >	Assign Edge License	Enable Alerts				
	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		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
	Non SD-WAN Destinations via Edge		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	
<b>Test &amp; Troubleshoot</b>	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				
		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/Package 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				
		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/Package 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/Package Capture	404 resource not found page	Read PCAP Bundle				
			Update PCAP Bundle			No	No
			Delete PCAP Bundle			Yes	Yes
	Diagnostic Bundles/Package 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	Controls visibility and control of Customer General Information on the System Settings General Information page	No	Yes	Yes
			Update Customer General Information				
	Default Edge Authentication		Read Customer PKI	Grants ability to view and manage enterprise PKI settings	Yes	No	No
			Update Customer PKI				
	Edge Configuration		Read Customer Edge Settings	Controls visibility and control of Customer Edge Settings on the System Settings General Information page	No	Yes	Yes
			Update Customer Edge Settings				
	Privacy Settings		Read Customer Privacy Settings	Controls visibility and control of Customer Privacy Settings on the System Settings General Information page	No	Yes	Yes
			Update Customer Privacy Settings				
	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	Controls visibility and control of System Settings Contact Info on the System Settings General Information page	No	Yes	Yes
			Update System Settings Contact Info				
	Authentication		Create Customer Authentication	Grants ability to view and manage customer authentication mode, for example SSO, Radius or Native	Yes	Yes	Yes
			Read Customer Authentication				
			Update Customer Authentication				
			Delete Customer Authentication				
			Manage Customer Authentication				
	API Tokens		Read Customer Token	Grants ability to view and manage authentication tokens at the Customer level	Yes	No	No
			Update Customer Token				
	Administrators		Create Customer User	Grants ability to view and manage Customer administrators	Yes	Yes	Yes
			Read Customer User				
			Update Customer User				

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
sGateway 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	Remote LTE Switch SIM Slot	Grants ability to activate the SIM Switchover feature. After the test is successful, you can check the status from <b>Monitor &gt; Edges &gt; Overview tab</b>
	<div style="border: 1px solid black; padding: 5px; width: fit-content;">  <b>Note:</b> This is for 610-LTE and 710 5G devices only.         </div>		
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 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

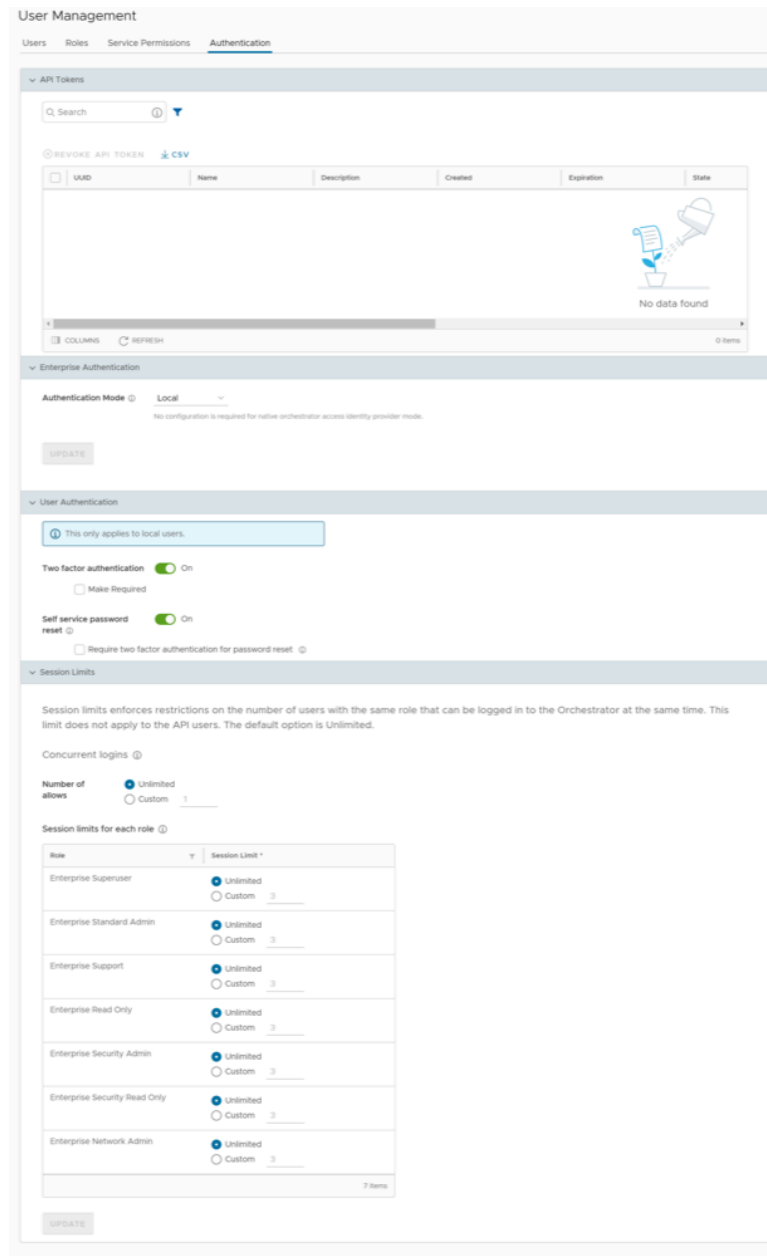
The Authentication feature allows you to set the authentication mode for an Enterprise user and view the existing API tokens.

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 Tab**



- 4. 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: Authentication Tab- Options and 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](#).

**5. 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). Click 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: Single Sign-on Authentication Mode**

User Management

Enterprise Authentication

Authentication Mode: Single Sign-On

Remember to set up <https://69.254.8.2/login/ssologin/openidCallback> as an allowed redirect URL with your IDP application/client. [Copy URL](#)

Single Sign-on Setup

Identity Provider Template: AzureAD

OIDC well-known config URL:

Issuer:

Authorization Endpoint:

Token Endpoint:

JSON Web KeySet URI:

User Information Endpoint:

Client ID:

Client Secret:  [Copy](#)  
Enter new value to change client secret

Scopes:

Role Setup

Role Type:  Use default role  Use identity provider roles

Role Attribute:


Enterprise Role Map

Orchestrator Role Name	Identity Provider Role Name
Enterprise Superuser	<input type="text"/>
Enterprise Standard Admin	<input type="text"/>
Enterprise Support	<input type="text"/>
Enterprise Read Only	<input type="text"/>
Enterprise Security Admin	<input type="text"/>
Enterprise Security Read Only	<input type="text"/>
Enterprise Network Admin	<input type="text"/>

7 items


[UPDATE](#)

**Table 15: Single Sign-on Authentication Mode- Options and 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.  <div data-bbox="703 323 1500 401" style="border: 1px solid #0070C0; padding: 5px;">  <b>Note:</b> You can also manually configure your own IdPs by selecting <b>Others</b> from the drop-down menu. </div>
OIDC well-known config URL	Enter the OpenID Connect (OIDC) configuration URL for your IdP. For example, the URL format for Okta will be: <code>https://{oauth-provider-url}/.well-known/openid-configuration</code> .
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: <ul style="list-style-type: none"> <li>• Use default role</li> <li>• Use identity provider roles</li> </ul>
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.

- 6. User Authentication:** You can choose to activate or deactivate **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.


**7. 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- Options and Descriptions**

Option	Description
Concurrent logins	Allows you to set a limit on concurrent logins per user. By default, <b>Unlimited</b> 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, <b>Unlimited</b> 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.

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

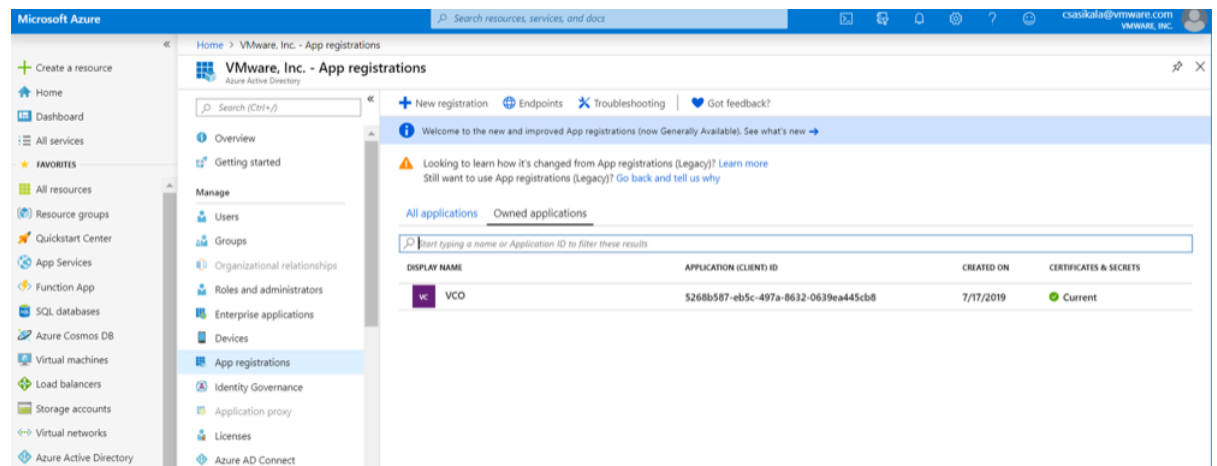
### 3.4.1 Configure Azure Active Directory for Single Sign On

Ensure you have an Azure AD account to sign in.

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

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: Azure Active Directory**



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

**Figure 3-14: Register an application**

Register an application

---

**\* Name**  
The user-facing display name for this application (this can be changed later).

✓

**Supported account types**  
Who can use this application or access this API?

Accounts in this organizational directory only (Velocloud Networks, Incit@velo)  
 Accounts in any organizational directory  
 Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)

[Help me choose...](#)

**Redirect URI (optional)**  
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

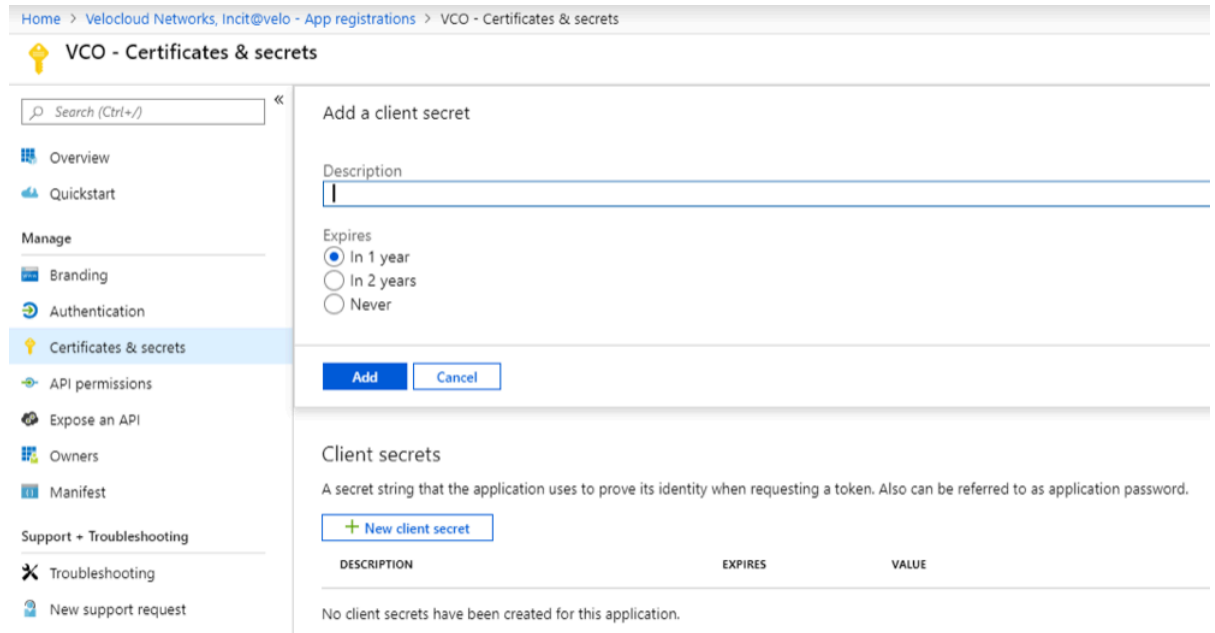
---

By proceeding, you agree to the [Microsoft Platform Policies](#)

- 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. 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`.
- f. 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.
- g. Select **Endpoints** and copy the well-known OIDC configuration URL to be used during the SSO configuration in Orchestrator.
- h. To create a client secret for your Orchestrator application, on the **Owned applications** tab, select your Orchestrator application.

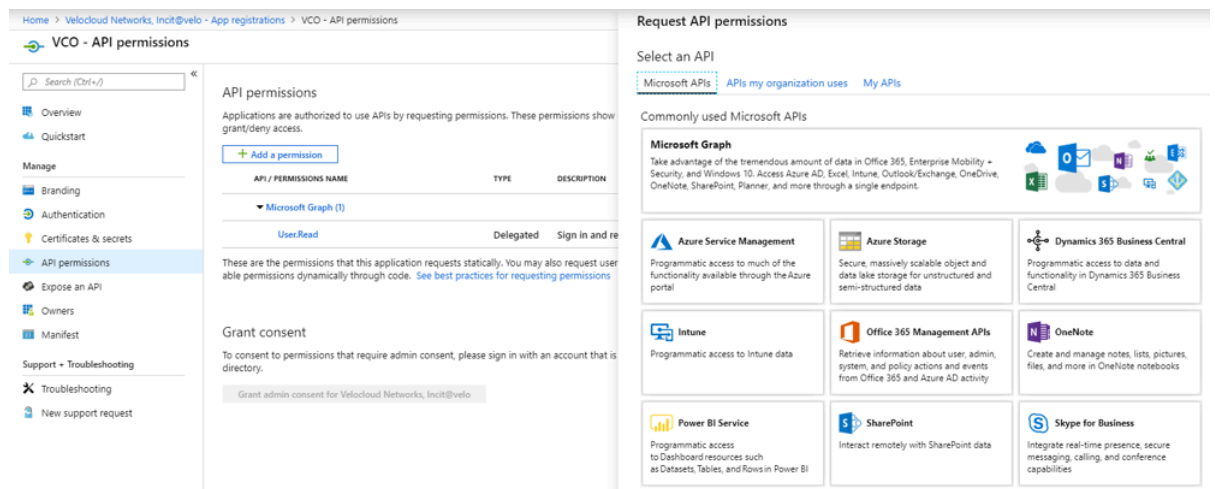
- i. Go to **Certificates & secrets > New client secret**. The **Add a client secret** screen appears.

**Figure 3-15: Add a Client Secret**



- j. 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.
- k. 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.

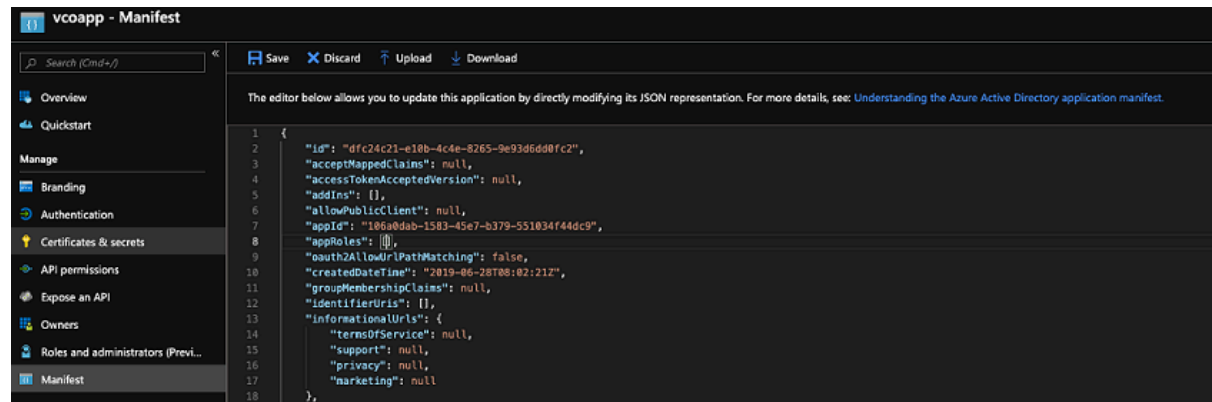
**Figure 3-16: Request API permissions**




- l. Select **Microsoft Graph** and select **Application permissions** as the type of permission for your application.
- m. Under **Select permissions**, from the **Directory** drop-down menu, select **Directory.Read.All** and from the **User** drop-down menu, select **User.Read.All**.

- n. Select **Add permissions**.
- o. 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: Manifest**




- p. 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": "18fcaala-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

```

1  {
2    "id": "dfc24c21-e1bb-4c4e-8265-9e93d6dd0fc2",
3    "acceptMappedClaims": null,
4    "accessTokenAcceptedVersion": null,
5    "addins": [],
6    "allowPublicClient": null,
7    "appId": "186a0dab-1583-45e7-b379-551834f44dc9",
8    "appRoles": [
9      {
10       "allowedMemberTypes": [
11         "User"
12       ],
13       "description": "Standard Administrator who will have sufficient privilege to manage resource",
14       "displayName": "Standard Admin",
15       "id": "18fca1a-853f-426d-9a25-ddd7ca7145c1",
16       "isEnabled": true,
17       "lang": null,
18       "origin": "Application",
19       "value": "standard"
20     },
21     {
22       "allowedMemberTypes": [
23         "User"
24       ],
25       "description": "Super Admin who will have the full privilege on VCO",
26       "displayName": "Super Admin",
27       "id": "cd1a0438-56c8-4c22-adc5-2dcfbf6dee75",
28       "isEnabled": true,
29       "lang": null,
30       "origin": "Application",
31       "value": "super"
32     }
33   ],
34   "oauth2AllowUrlPathMatching": false,
35   "createdDateTime": "2019-06-28T08:02:21Z",

```

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

Figure 3-19: App Roles

Home > App registrations > VCO-ONE-SSO

VCO-ONE-SSO | App roles

App roles

App roles are custom roles to assign permissions to users or apps. The application defines and publishes the app roles and interprets them as permissions during authorization.

How do I assign App roles

Display name	Description	Allowed member ty...	Value
Enterprise Standard Admin	Standard Administrator who will have sufficient privilege to manage resource	Users/Groups	standardadmin
Enterprise Superuser	Can perform the same tasks as an Enterprise Standard Admin and can also create additional us...	Users/Groups	superuser
Enterprise Support	Can monitor edges, activity, and initiate diagnostic actions in their network and can monitor the...	Users/Groups	support
Enterprise Read Only	Read only view of Monitoring Information their company's network services	Users/Groups	readonly
Enterprise Security Admin	Can view and manage their security services. Has read only access to the network	Users/Groups	securityadmin
Enterprise Security Read Only	Read only view of their company's security services	Users/Groups	securityreadonly
Enterprise Network Admin	Can view and manage their network. Has read only access to security services	Users/Groups	networkadmin

- To assign groups and users to your Orchestrator application:
  - Go to **Azure Active Directory > Enterprise applications**.
  - Search and select your Orchestrator application.
  - 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 Azure AD for SSO.

Configure Single Sign On in the Orchestrator.

### 3.4.2 Configure Okta for Single Sign On

Ensure you have an Okta account to sign in.

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.

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: Add Application**

The screenshot displays the Okta 'Add Application' interface. At the top, the navigation bar includes 'Classic UI', user 'S. Chandran', and 'VMWare-dev-690682'. The main navigation bar contains 'Dashboard', 'Directory', 'Applications', 'Security', 'Reports', and 'Settings'. The 'Add Application' screen has a search bar and a 'Back to Applications' link. A sidebar on the left provides a 'Create New App' button and 'Integration Properties' (Any, Supports SAML, Supports Provisioning). The main content area lists applications: '&frankly' (Okta Verified, SAML), '15Five' (Okta Verified, SAML, Provisioning), '23 VIDEO' (Okta Verified, SAML), and '360 Workplace' (Community Created, SAML). Each application has an 'Add' button.

- b. Select **Create New App**. The **Create a New Application Integration** dialog box appears.
- c. From the **Platform** drop-down 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: Create OpenID Connect Integration**

 Create OpenID Connect Integration


**GENERAL SETTINGS**


Application name

Application logo (Optional) 

---

**CONFIGURE OPENID CONNECT**

Login redirect URIs 

Logout redirect URIs 

- 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.
- g. 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`
- h. Select **Save**. The newly created application page appears.

- i. 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.

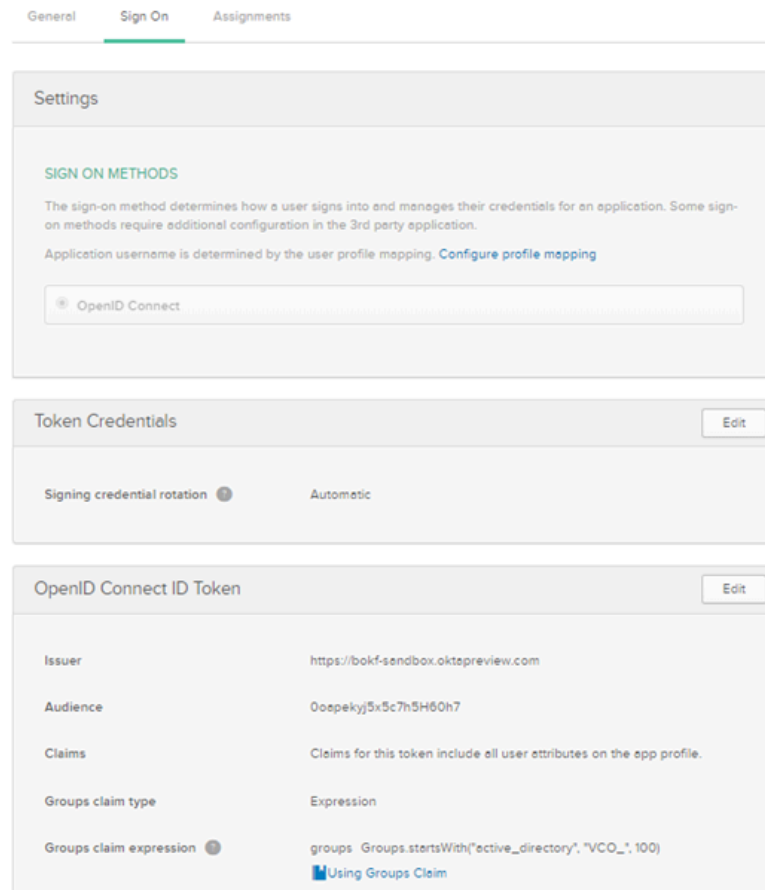
**Figure 3-22: Application**

The screenshot displays the 'Application' configuration page in a web interface. At the top, there are three tabs: 'General' (selected), 'Sign On', and 'Assignments'. Below the tabs is a 'General Settings' section with an 'Edit' button. This section is divided into two parts: 'APPLICATION' and 'LOGIN'. Under 'APPLICATION', the 'Application label' is 'VMWare SD-WAN VCO', the 'Application type' is 'Web', and 'Allowed grant types' includes 'Client acting on behalf of itself' (with 'Client Credentials' unchecked) and 'Client acting on behalf of a user' (with 'Authorization Code' and 'Refresh Token' checked, and 'Implicit (Hybrid)' unchecked). The 'LOGIN' section includes 'Login redirect URIs' (https://vco13-usv11.velocloud.net/login/ssologin/openidCallback), 'Logout redirect URIs', 'Login initiated by' (App Only), and 'Initiate login URI' (https://vco13-usv11.velocloud.net/). Below this is the 'Client Credentials' section, also with an 'Edit' button. It shows the 'Client ID' as '0ospekyj5x5c7h5H60h7' and the 'Client secret' as a masked field with a copy icon.

- j. Select the **Sign On** tab and under the **OpenID Connect ID Token** area, select **Edit**.
- k. From the **Groups claim type** drop-down menu, select **Expression**. By default, Groups claim type is set to **Filter**.
- l. In the **Groups claim expression** text box, enter the claim name that will be used in the token, and an Okta input expression statement that evaluates the token.

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

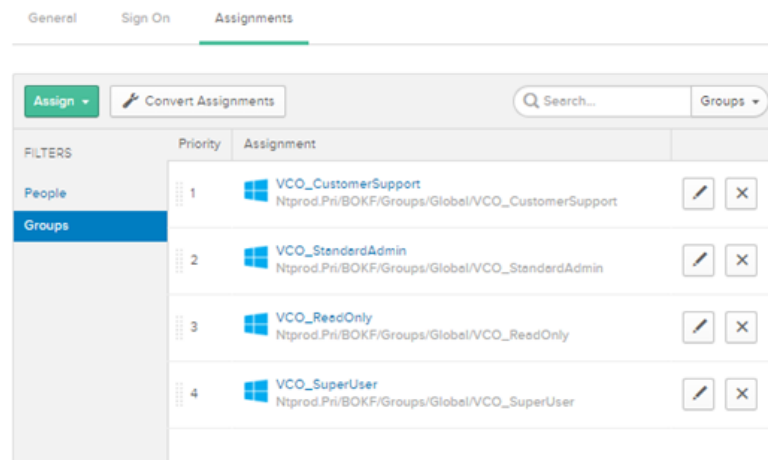
**Figure 3-23: Groups claim expression**



- 3. To assign groups and users to your Orchestrator application:
  - a. Go to **Application > Applications** 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 Name> to Groups** or **Assign <Application Name> 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: Groups tab**



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

Configure Single Sign On in the Orchestrator.

### 3.4.3 Configure OneLogin for Single Sign On

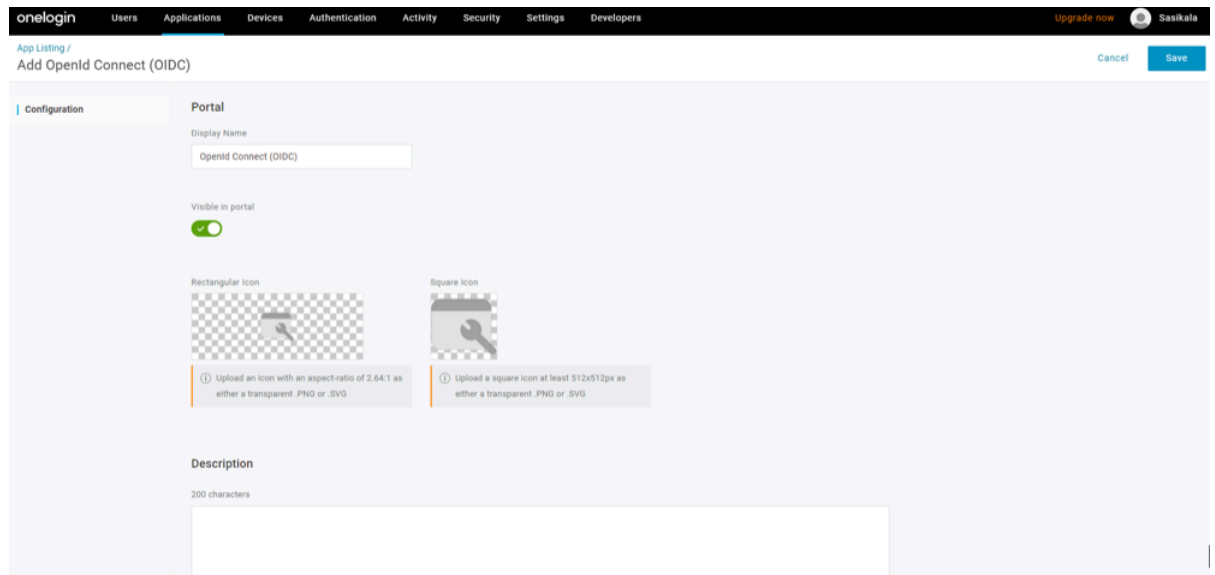
Ensure you have an OneLogin account to sign in.

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

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**.

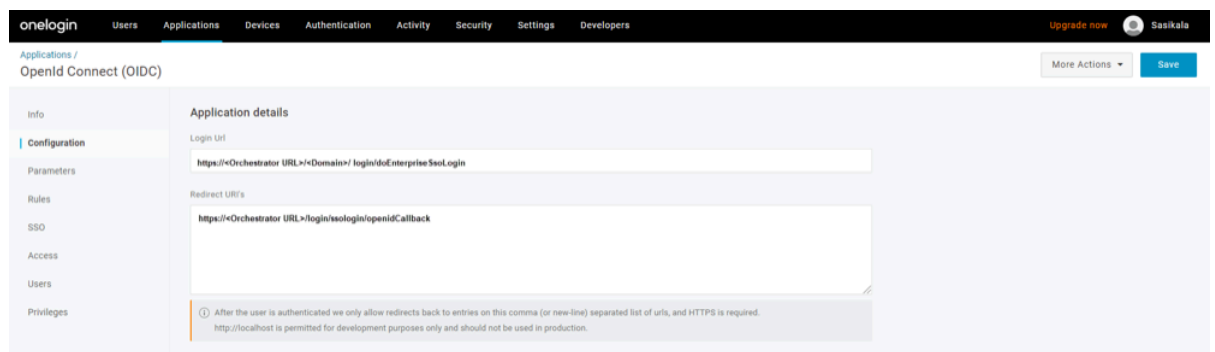
- b. In the **Find Applications** text box, search for “OpenId Connect” or “oidc” and then select the **OpenId Connect (OIDC)** app. The **Add OpenId Connect (OIDC)** screen appears.

**Figure 3-25: Add OpenId Connect (OIDC)**



- 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: Application Details**



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

**Figure 3-27: Edit Field Groups**

Edit Field Groups

---

Name  
Groups

Value

Select Groups

Added Items

Default if no value selected

User Roles

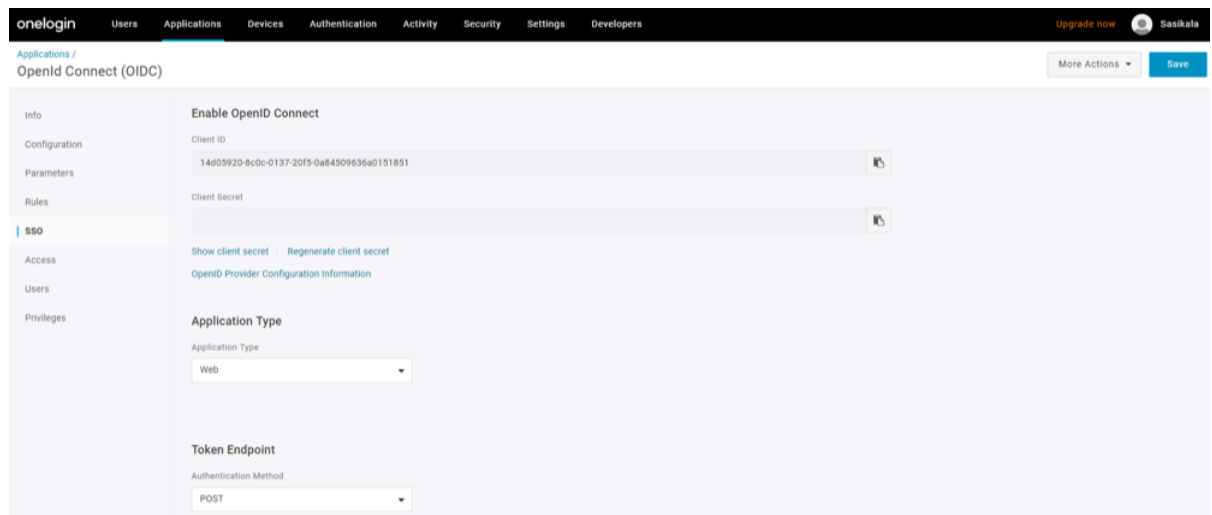
(i) This value will be used if no value has been selected in the table above

---

- 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**.

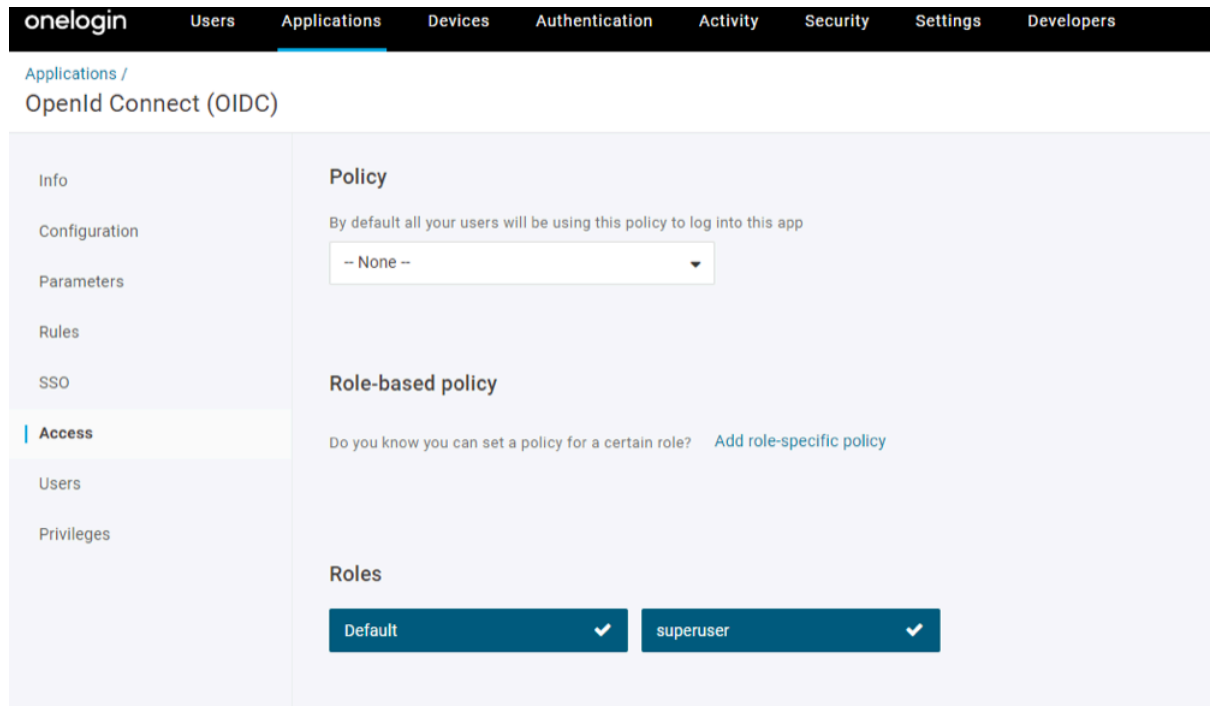
- h. From the **Authentication Method** drop-down menu, select **POST** as the Token Endpoint and select **Save**. Note down the Client Credentials (Client ID and Client Secret) to be used during the SSO configuration in Orchestrator.

**Figure 3-28: Application Type**



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

**Figure 3-29: Access tab**



- 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.

Configure Single Sign On in the Orchestrator.

### 3.4.4 Configure PingIdentity for Single Sign On

Ensure you have a PingOne account to sign in.

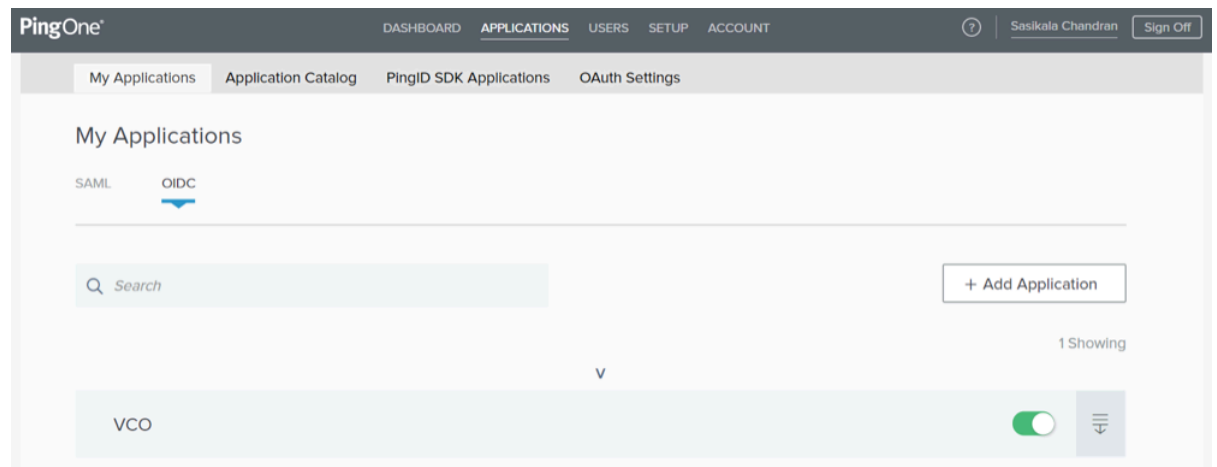


**Note:** Currently, Orchestrator supports PingOne as the Identity Partner (IDP). However, any PingIdentity product supporting OIDC can be easily configured.

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

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, select **Applications**.

**Figure 3-30: My Applications**



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

**Figure 3-31: Adding an OIDC Application**

The screenshot shows the 'Add OIDC Application' window with the following details:

- APPLICATION NAME:** VeloOrchestrator
- SHORT DESCRIPTION:** Orchestrator for VMware SD-WAN
- CATEGORY:** Information Technology
- ICON:** A placeholder icon with a plus sign and a note: 'Maximum size is 1MB JPEG, JPG, GIF, PNG'
- Buttons:** Cancel and Next
- Wizard Steps:**
  1. PROVIDE DETAILS ABOUT YOUR APPLICATION
  2. AUTHORIZATION SETTINGS
  3. SSO FLOW AND AUTHENTICATION SETTINGS
  4. DEFAULT USER PROFILE ATTRIBUTE CONTRACT
  5. CONNECT SCOPES
  6. ATTRIBUTE MAPPING

- c. Provide basic details such as name, short description, and category for the application and select **Next**.
- d. Under **AUTHORIZATION SETTINGS**, select **Authorization Code** as the allowed grant types and select **Next**. Note down the Discovery URL and Client Credentials (Client ID and Client Secret) to be used during the SSO configuration in the Orchestrator.
- e. Under **SSO FLOW AND AUTHENTICATION SETTINGS**, provide valid values for Start SSO URL and Redirect URL and select **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**, select **Add Attribute** to add additional user profile attributes.
- g. In the **Attribute Name** text box, enter `group_membership` and then select the **Required** check box, 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 select **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 memberOf).

- j. Under **Group Access**, select all user groups that should have access to your Orchestrator application and select **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.

Configure Single Sign On in Orchestrator.

# Enterprise Settings

---

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

To configure Enterprise 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.

- From the left menu, select **Enterprise Settings**. The **Enterprise Settings** screen appears.

**Figure 4-1: Enterprise Settings**

Enterprise Settings

General Information

Name \* Windstream-7-1

Account Number @ WIN-KVZ7PSX

Logical ID @ 3c064933-c66-4a5f-ac8f-4b9c789ee... [copy](#)

Domain @ 83e16950-fe88-4dc8-af53-1295aa20857  
Example: vmware

Description

Information Privacy Settings

Operator Support Access

Allow access to enterprise  On  
When activated, VeloCloud Support will be granted access to view, configure, and troubleshoot this enterprise's Orchestrator and Edges. As a security consideration, VeloCloud Support will not be granted access to view user identifiable information.

Allow access to sensitive data  On  
When activated, VeloCloud Support will be able to view configuration passwords in plaintext in SD-WAN, CWS, and Secure Access.

Allow User management access  On  
When activated, VeloCloud Support will be able to assist in user management including creating users, resetting passwords, etc. As a security consideration, VeloCloud Support will be granted access to view all user identifiable information.

SD-WAN PCI

Enforce PCI Compliance  Off  
When enabled, all users (including VeloCloud Support) will be unable to access sensitive Customer data including PCAPs, etc. on the edges and gateways.

Customer Business Contact Information

This person is the primary contact for licensing, business reports, logistics, shipping, Zero Touch Provisioning, etc.

Primary Business Contact

Contact Name test

Contact Email test@vmware.com

Phone +1

Mobile Phone +1

Primary Business Location

Address Line 1 F

Address Line 2 G

City Hhhh

State / Province / Region Karnataka


Zip / Postcode 560089

Country India

DISCARD CHANGES [?](#) **SAVE CHANGES**

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

**Table 17: Enterprise Settings Option Descriptions**

Option	Description
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. <div data-bbox="667 449 1510 527" style="border: 1px solid black; padding: 5px;"> <b>Note:</b> Modifying the domain after configuration, affects the EI integration with the Orchestrator.</div>
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 <b>Enforce PCI Compliance</b> 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 - Enterprise](#).

You can now log in to the VeloCloud Orchestrator using Single Sign On. For additional information, see the topic *Using Single Sign On Login for Enterprise Users* in *Arista VeloCloud SD-WAN Administration Guide*.

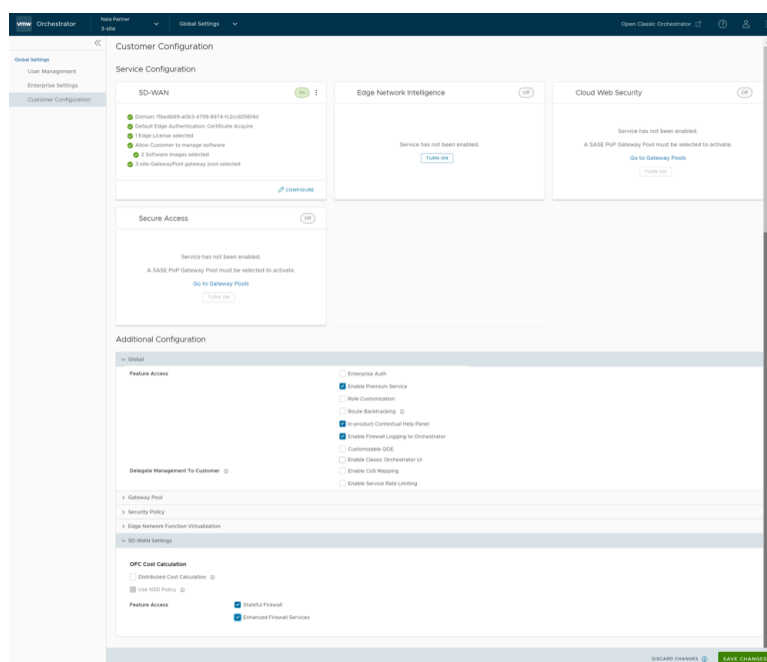
## Configure Customers

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 **Customer Configuration** page appears.

**Figure 5-1: Customer Configuration Page**



In the **Service Configuration** section, under **SD-WAN** select the **Turn On** button to activate the service. Select the vertical ellipsis present at the top right corner of the tile to turn off or configure that service.

You can also use the **Configure** option present at the bottom right corner to configure the service. Selecting the **Configure** option displays the following pop-up window. Configure the settings, and then select **Update**.

**Figure 5-2: Configuring SD-WAN**

**Table 18: SD-WAN Configuration Options and Descriptions**


Option	Description
Domain	Enter the domain name to be used to activate Single Sign On (SSO) authentication for the Orchestrator.
Default Edge Authentication	<p>Choose the default option to authenticate the Edges associated to the Customer, from the drop-down menu.</p> <ul style="list-style-type: none"> <li>• <b>Certificate Deactivated:</b> Edge uses a pre-shared key mode of authentication.</li> <li>• <b>Certificate Acquire:</b> 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.</li> </ul> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p> <b>Note:</b> After acquiring the certificate, the option can be updated to <b>Certificate Required</b>.</p> </div> <ul style="list-style-type: none"> <li>• <b>Certificate Required:</b> Edge uses the PKI certificate. Operators can change the certificate renewal time window for Edges using the system property <code>edge.certificate.renewal.window</code>.</li> </ul>
Edge Licensing	<p>The existing Edge Licenses are displayed. Select <b>Add</b> to add or remove the licenses.</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p> <b>Note:</b> 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 <i>Edge Licensing</i> in <i>Arista VeloCloud SD-WAN Administration Guide</i>.</p> </div>
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 <i>Edge Image Management</i> in <i>Arista VeloCloud SD-WAN Administration Guide</i> .
Operator Profile	Select an Operator profile to be associated with the Customer from the available drop-down menu. This field is not available if <b>Allow Customer to Manage Software</b> is selected. For additional information on Operator profiles, see the topic <i>Manage Operator Profiles</i> in <i>Arista VeloCloud SD-WAN Operator Guide</i> .
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.









**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**.



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

**Table 19: Customer Configuration Settings Options and Descriptions**


Option	Description
<b>Global</b>	
User Agreement Display	<p>Select either of the following from the drop-down menu:</p> <ul style="list-style-type: none"> <li>• Inherit</li> <li>• Override to Hide</li> <li>• Override to Show</li> </ul>
<p> <b>Note:</b></p>	
Feature Access	<p>This field is available only when the system property <code>session.options.enableUserAgreements</code> is set to <b>True</b>.</p> <p>Provides access to the selected features. Select one or more check boxes from the below list to activate these features for the Customer:</p> <ul style="list-style-type: none"> <li>• <b>Enterprise Auth:</b> 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).</li> <li>• <b>Enable Premium Service:</b> 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 additional information, see the topic <i>Dynamic Multipath Optimization (DMPO)</i> in the <i>Arista VeloCloud SD-WAN Administration Guide</i>.</li> <li>• <b>Role Customization:</b> Allows an Enterprise Super user to customize the role privileges for other Enterprise users.</li> <li>• <b>Route Backtracking:</b> Allows the device to choose the best route in the order of prefix length.</li> <li>• <b>In-product Contextual Help Panel:</b> 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.</li> <li>• <b>Enable Firewall Logging to Orchestrator:</b> 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.</li> <li>• <b>Customizable QoS:</b> Allows the Customer to configure the minimum and maximum latency threshold values for Voice, Video, and Transactional application categories of an Edge.</li> <li>• <b>Enable Classic Orchestrator UI:</b> Allows the Customer to switch from the Angular Orchestrator UI to the Classic Orchestrator UI. This option is available only when the system property <code>session.options.enableClassicOrchestrator</code> is set to <b>True</b>.</li> </ul>

Option	Description
Delegate Management To Customer	<p>Allows the Customer to modify the settings of the selected property. Following two properties are always visible to the Customers:</p> <ul style="list-style-type: none"> <li>• <b>Enable CoS Mapping:</b> Allows to configure CoS mapping while configuring a business policy.</li> <li>• <b>Enable Service Rate Limiting:</b> Allows to rate limit services in a business policy.</li> </ul>
<b>Gateway Pool</b>	
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 <b>Save Changes</b> .
Gateways in this Pool	Displays the Gateway details in the current pool.
Partner Hand Off	Activating the <b>Gateway Pool</b> option displays the <b>Configure Hand Off</b> section. If the Gateways available in the Gateway pool have been assigned with Partner Gateway role, you can handoff the Gateways to Partners. For details, see <a href="#">Configure Partner Handoff</a> .
<b>Security Policy</b>	
Hash	<p>By default, there is no authentication algorithm configured for the VPN header as AES-GCM is an authenticated encryption algorithm. When you select the <b>Turn off GCM</b> check box, you can select one of the following as the authentication algorithm for the VPN header, from the drop-down menu:</p> <ul style="list-style-type: none"> <li>• SHA 1</li> <li>• SHA 256</li> <li>• SHA 384</li> <li>• SHA 512</li> </ul>
Encryption	Select either <b>AES 128</b> or <b>AES 256</b> as the AES algorithm's key size to encrypt data. The default encryption algorithm mode is <b>AES 128</b> .
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.
<div style="border: 1px solid #00a0e3; padding: 5px;">  <b>Note:</b> It is recommended to use DH Group 14, which is the default value.         </div>	
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 <b>Hash</b> and select an authentication algorithm for the VPN header.
IPsec SA Lifetime Time(min)	Time when Internet Security Protocol (IPsec) re-keying is initiated for Edges. The minimum IPsec lifetime is 3 minutes and maximum IPsec lifetime is 480 minutes. The default value is <b>480</b> minutes.
<div style="border: 1px solid #00a0e3; padding: 5px;">  <b>Note:</b> 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 re-keys. The low lifetime values are for debugging purposes only.         </div>	
IKE SA Lifetime(min)	Time when Internet Key Exchange (IKE) re-keying is initiated for Edges. The minimum IKE lifetime is 10 minutes and maximum IKE lifetime is 1440 minutes. The default value is 1440 minutes.
<div style="border: 1px solid #00a0e3; padding: 5px;">  <b>Note:</b> 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 re-keys. The low lifetime values are for debugging purposes only.         </div>	

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 <b>Edge NFV</b> , 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 <i>Security VNFs</i> in the <i>Arista VeloCloud SD-WAN Administration Guide</i> .
<b>SD-WAN Settings</b>	
OFC Cost Calculation	<p>Select the required check box:</p> <ul style="list-style-type: none"> <li> <b>Distributed Cost Calculation:</b> Select this check box to delegate route cost calculation to Edges/Gateways. </li> </ul> <div style="border: 1px solid #00a0e3; padding: 5px; margin: 5px 0;"> <p> <b>Note:</b> This option is available only for the Edges/Gateways with version 3.4.0 and later. After activating <b>Distributed Cost Calculation</b>, it is recommended to refresh the routes by navigating to <b>Configure &gt; Overlay Flow Control</b> in the <b>SD-WAN</b> service of the Enterprise portal. For additional information, see <a href="#">Configure Distributed Cost Calculation</a>.</p> </div> <ul style="list-style-type: none"> <li> <b>Use NSD Policy:</b> Select this check box to use NSD policy for route cost calculation to Edges/Gateways. </li> </ul> <div style="border: 1px solid #00a0e3; padding: 5px; margin: 5px 0;"> <p> <b>Note:</b> This option is available only for the Edges/Gateways with version 4.2.0 and later.</p> </div>
Multiple-DSCP tags per Flow Path Calculation	<p>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.</p> <p>Select the <b>Include DSCP value as part of flow lookup</b> check box to include DSCP values as part of flow look-up and path calculation. For additional information, see <a href="#">Configure Path Calculation with Multiple DSCP Labels per Flow</a>.</p> <div style="border: 1px solid #00a0e3; padding: 5px; margin: 5px 0;"> <p> <b>Note:</b> This field is available only when the system property <code>session.options.enableFlowParametersConfig</code> is set to <b>True</b>.</p> </div>
<b>Feature Access</b>	
Stateful Firewall	Select the <b>Stateful Firewall</b> check box to override the Stateful Firewall settings activated on the Enterprise Edge.

Option	Description
Enhanced Firewall Services	<p>Select the <b>Enhanced Firewall Services</b> check box to activate the Enhanced Firewall Services using the Firewall functionality in the Orchestrator.</p> <div data-bbox="667 264 1508 342" style="border: 1px solid #add8e6; padding: 5px;"> <p> <b>Note:</b> For Enhanced Firewall Services (EFS) to work, ensure the Edge version is upgraded to 5.2.0.0.</p> </div> <div data-bbox="667 369 1508 512" style="border: 1px solid #add8e6; padding: 5px;"> <p> <b>Note:</b> Deselecting 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 <b>Configure &gt; Profiles/Edges &gt; Firewall &gt; Enhanced Firewall Services</b> and then by deselecting this check box in Global Settings.</p> </div> <p>For additional information about configuring Enhanced Firewall Services Policy rule, see the topic <i>Configure Enhanced Firewall Services</i> in the <i>Arista VeloCloud SD-WAN Administration Guide</i>.</p>

## 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.

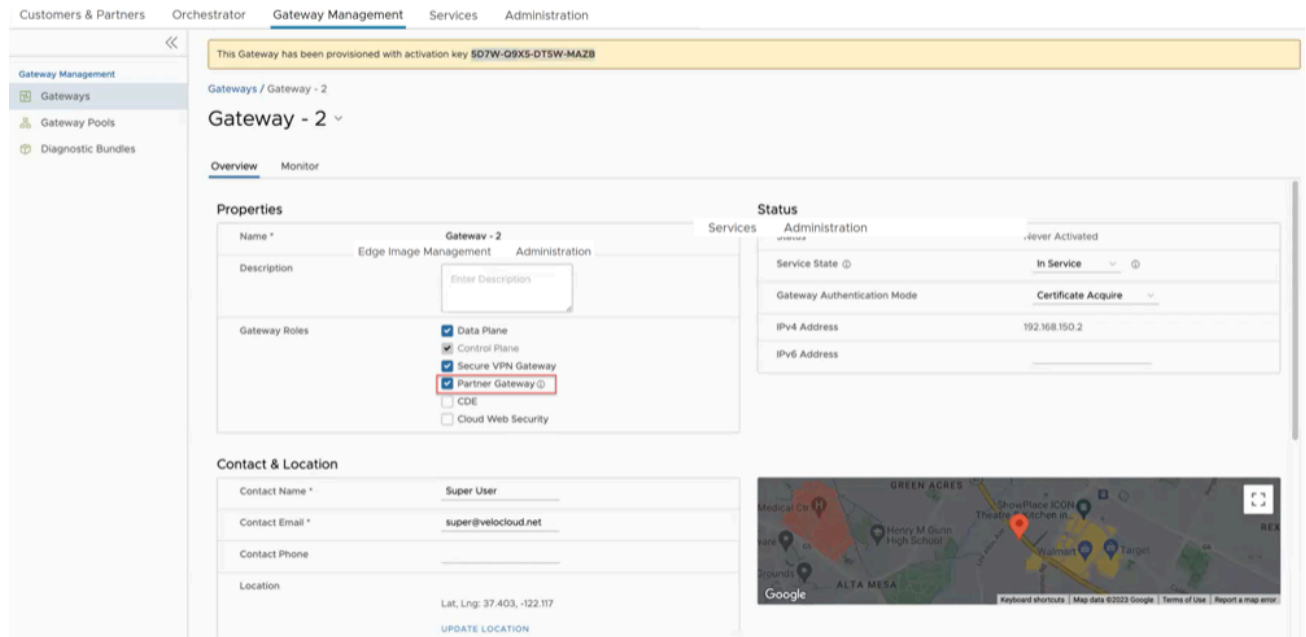
## 5.1 Configure Partner Handoff

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 5-3: Configure Partner Handoff**

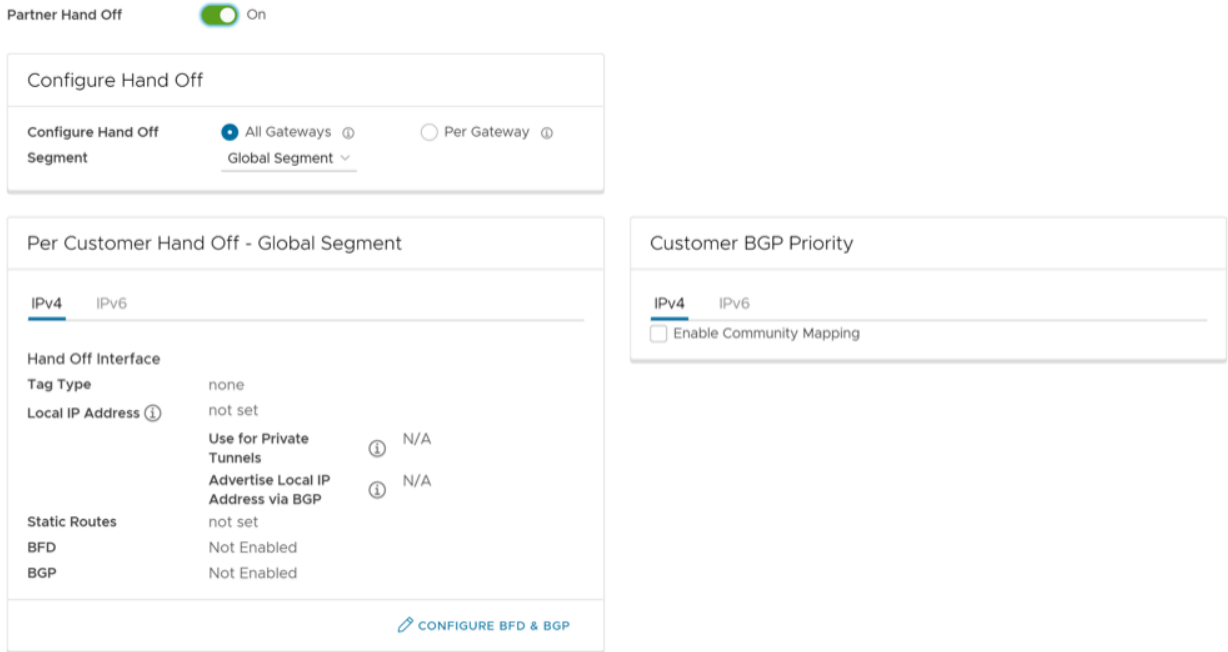


To configure the Handoff settings, perform the following steps:

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:

**Figure 5-4: Configure Partner Hand Off**

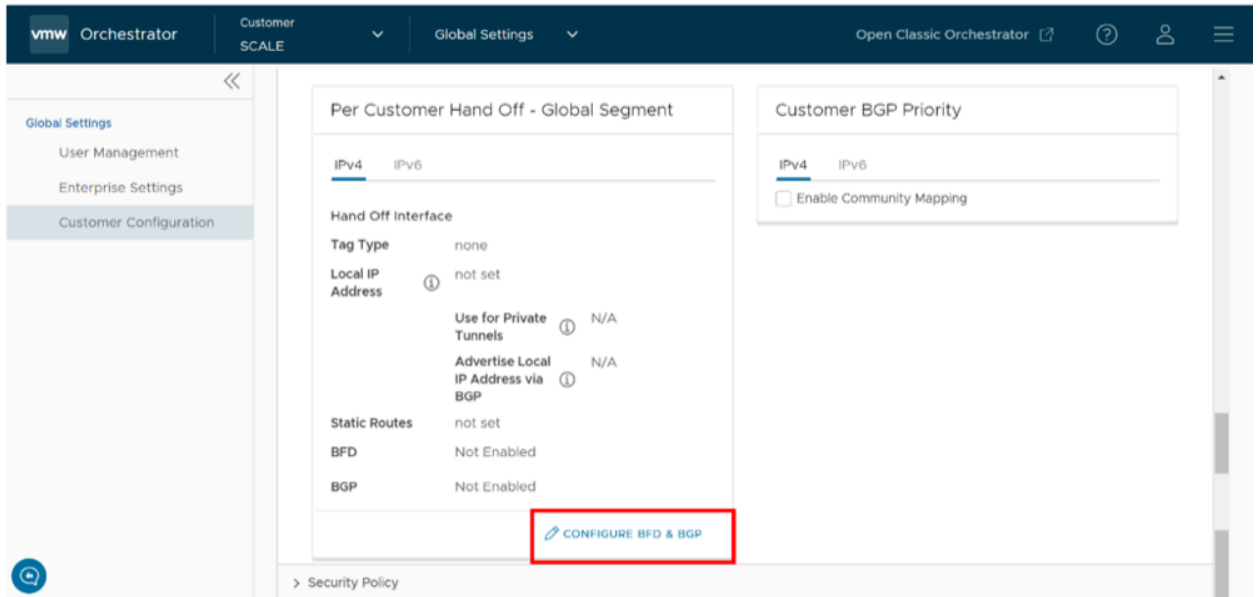


**Table 20: Partner Hand Off Option Descriptions**

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 <b>Per Gateway</b> , and then select the Gateway from the drop-down list.
Segment	By default, <b>Global Segment</b> 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 <b>Configure BGP and BFD</b> page.
Customer BGP Priority	Select the check box and configure the Community Mapping details.

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

**Figure 5-5: Configure BFD and BGP Settings for Handoff Interface**



The **Configure BGP and BFD** screen displays.

**Figure 5-6: Configure BGP and BFD**

Customer Configuration / Configure BGP and BFD

### Configure BGP and BFD

**Hand Off Tag**

Tag Type: none

Customer ASN: \_\_\_\_\_

**IPv4** | IPv6

**Hand Off Interface**

Local IP Address: \_\_\_\_\_

Local IP Address for this logical interface:  Enable

Use for Private Tunnels:  Enable

Advertise Local IP Address via BGP:  Enable

**Static Routes**

+ ADD | DELETE | CLONE

Subnets *	Cost *	Encrypt	Hand Off	Description
No Static Routes				

0 items

**BFD**  Off

Peer Address: \_\_\_\_\_ Local Address: \_\_\_\_\_

Detect Multiplier: \_\_\_\_\_ Example: 3

Receive Interval: \_\_\_\_\_ Example: 300

Transmit Interval: \_\_\_\_\_ Example: 300

**BGP**  Off

Neighbor IP: \_\_\_\_\_ Neighbor-ASN: \_\_\_\_\_

Secure BGP Routes:  Enable

**Multi-Hop BGP**

Max-hop: 1 BGP Local IP: \_\_\_\_\_

Next Hop IP: \_\_\_\_\_

**BGP Inbound Filters**

Match Type	Match Value *	Exact Match	Action Type	Action Set
No Inbound Filters				

0 items

**BGP Outbound Filters**

Match Type	Match Value *	Exact Match	Action Type	Action Set
No Outbound Filters				

0 items

**Optional Settings**

BFD:  Enable

Router-ID: \_\_\_\_\_

Keep Alive: 60

Hold Timers: 180

Turn off AS-PATH Carry Over:  Enable

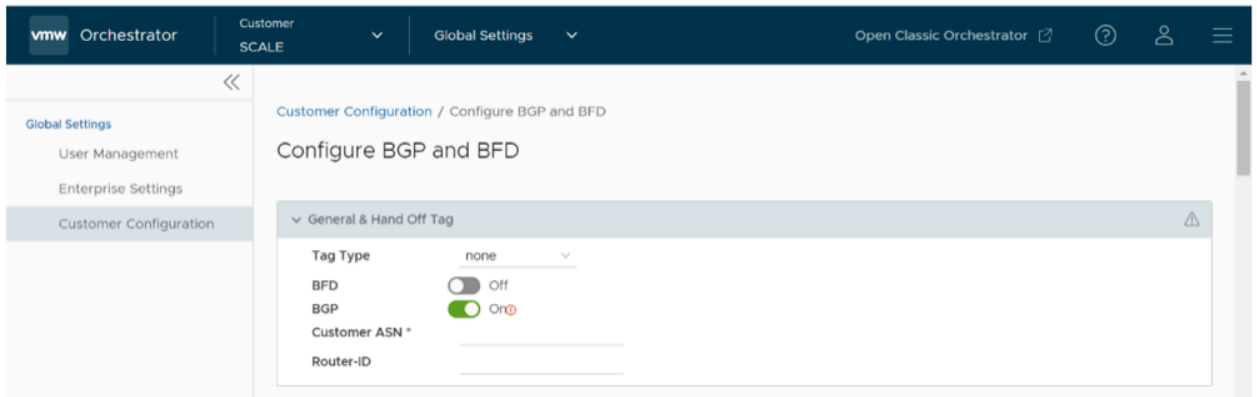
MDS Auth:  Enable

MDS Password: \_\_\_\_\_

CANCEL UPDATE

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

**Figure 5-7: General & Hand Off Tag Settings**





8. Scroll down to the **BGP** section and select the arrow to display the **BGP** section and configure the following settings:

**Table 21: BGP Partner Hand Off Option Descriptions**

Option	Description
<b>Hand Off Tag</b>	
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: <ul style="list-style-type: none"> <li>• <b>None</b>: Untagged. Choose this during single tenant hand off or a hand off towards shared services VRF.</li> <li>• <b>802.1Q</b>: Single VLAN tag</li> <li>• <b>802.1ad / QinQ(0x8100) / QinQ(0x9100)</b>: Dual VLAN tag</li> </ul>
Customer ASN	Enter the Customer Autonomous System Number.
<b>Hand Off Interface: You can configure the following settings for IPv4 and IPv6.</b>	
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.
<b>Static Routes: You can add, delete, or clone a static route.</b>	
Subnets	Enter the IP address of the Static Route Subnet that the Gateway should advertise to the Edge.
Cost	Enter the cost to apply weightage 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 <b>VLAN</b> or <b>NAT</b> .
Description	Enter a descriptive text for the static route. This field is optional.
<b>BFD: Turn the toggle button to On to activate this section.</b>	
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.
<b>BGP: Turn the toggle button to On to activate this section.</b>	
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.

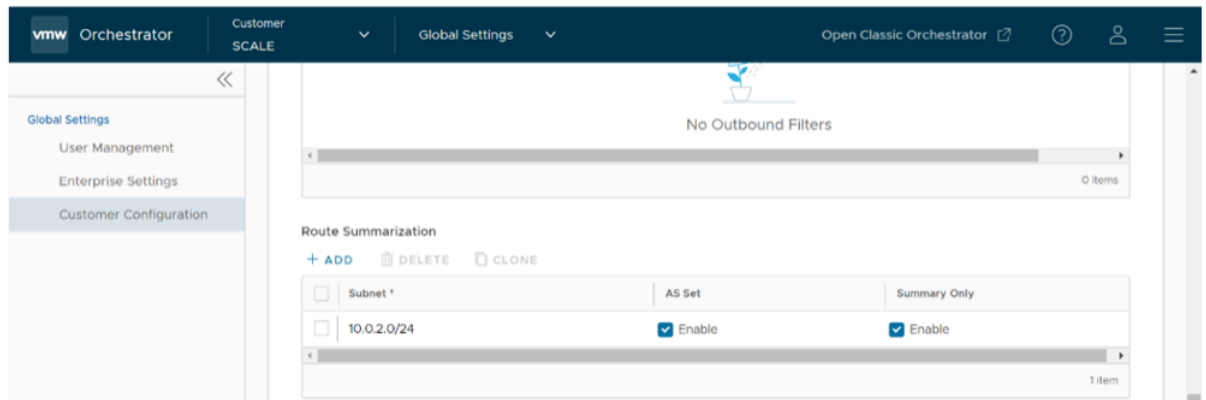


**Note:** This field is available only for eBGP neighbors, when the local ASN and the neighboring ASN are different.

Option	Description
Next Hop IP	Enter the next-hop IP address to be used by BGP to reach the multi-hop BGP peer.  <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <b>Note:</b> This option is available only for multi-hop eBGP with Max-hop count greater than 1. </div>
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 <b>Hand Off Interface</b> 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 <b>60</b> seconds.
Hold Timers	Enter the BGP Hold time in seconds. The default timer is <b>180</b> 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.  <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <b>Note:</b> Starting from the 4.5 release, the use of the special character "&lt;" in the password is no longer supported. In cases where users have already used "&lt;" in their passwords in previous releases, they must remove it to save any changes on the page. </div>


9. If applicable, configure Route Summarization.
  - a. Scroll down to the **Route Summarization** area in the **BGP** section.

**Figure 5-8: Configure Route Summarization**



- b. Configure the Route Summarization fields, as described in the following table:

**Table 22: Route Summarization Option Descriptions**

Option	Description
+Add	Select <b>+Add</b> to add a new row in the <b>Route Summarization</b> area.
	<div style="border: 1px solid #00a0e3; padding: 5px;">  <b>Note:</b> To add additional rows to configure Route Summarization, select <b>+Add</b>. To Clone or Delete a route summarization, use the appropriate buttons, located next to <b>+Add</b>. </div>
Subnet column	Under the <b>Subnet</b> 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 <b>AS Set</b> column, select the <b>Yes</b> check box if applicable.
Summary Only column	Under the <b>Summary Only</b> column, select the <b>Yes</b> check box to allow only the summarized route to be sent.

For an overview, use case, and black hole routing details for Route Summarization, see the section titled, *Route Summarization* in the *Arista VeloCloud SD-WAN Administration Guide*.

- c. Select **Update** to save the settings.

## 5.2 Configure Distributed Cost Calculation

By default, the Orchestrator is actively involved in learning the dynamic routes. VeloCloud 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 activate 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.



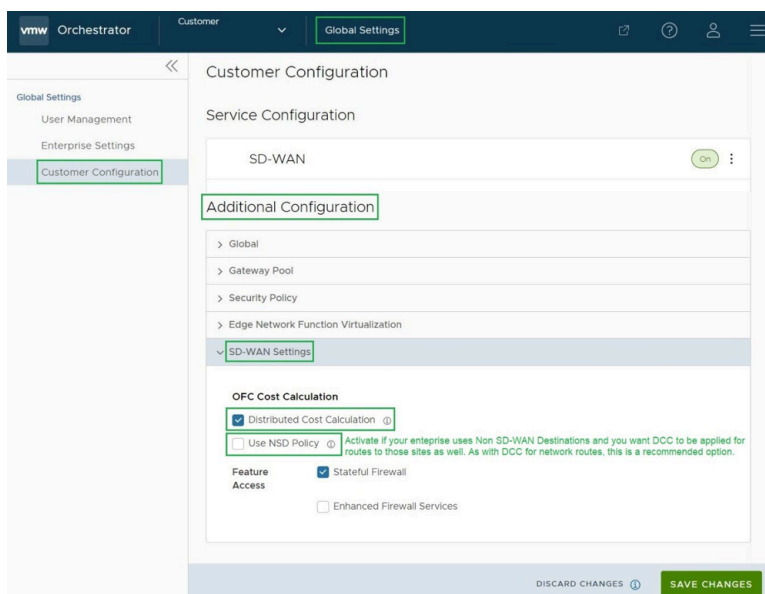
**Note:** It is recommended to enable Distributed Cost Calculation in a maintenance window to minimize the impact on the Customer Enterprise.

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.

- In the **Enterprise** portal, go to **Global Settings > Customer Configuration**.

**Figure 5-9: Configure Distributed Cost Calculation**



- 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** check box to delegate the cost calculation of routes to Edges and Gateways.
  - Select the **Use NSD Policy** check box 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.
- 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 *Arista VeloCloud SD-WAN Administration Guide*.

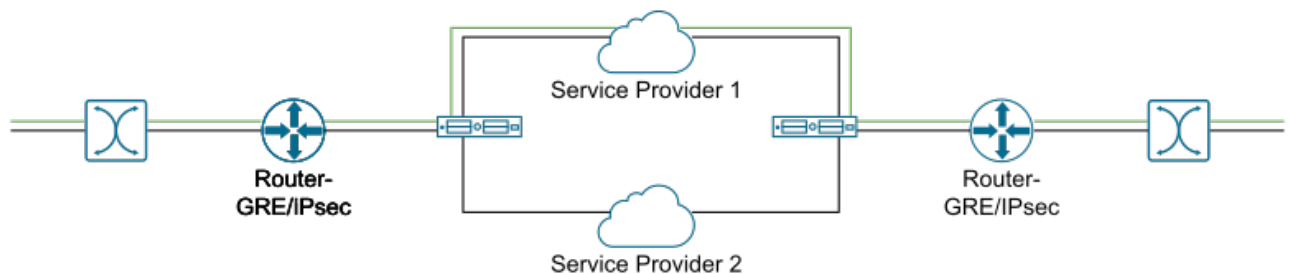
### 5.3 Configure Path Calculation with Multiple DSCP Labels per Flow

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 5-10: Single Flow Traffic Network Topology**



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, perform the following steps:

1. Create a new system property.
  - a. In the **Operator** portal, select **Orchestrator > System Properties**.
  - b. Select **New**.
  - c. In the **New System Property** window, create a system property with the following parameters:
    - **Name:** *session.options.enableFlowParametersConfig*
    - **Data Type:** *Boolean*
    - **Value:** *True*
  - d. Select **Save Changes**.
2. In the **Enterprise** portal, navigate to **Global Settings > Customer Configuration**.
3. 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**.

4. Select **Save Changes**.

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 *Arista VeloCloud SD-WAN 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 additional business policies with different DSCP labels to match with different traffic flows and apply different treatments for those flows.

#### 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.

## References

---

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