

ARISTA

Operator Guide

VeloCloud SD-WAN

Version 6.1



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

© Copyright 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. Use of marks belonging to other parties is for informational purposes only.

Contents

Chapter 1: Arista VeloCloud SD-WAN Operator Guide..... 1

Chapter 2: About the Arista VeloCloud SD-WAN Operator Guide..... 2

Chapter 3: Overview of Arista VeloCloud Orchestrator..... 3

Chapter 4: Supported Browsers..... 4

Chapter 5: What's New..... 5

Chapter 6: Using SSO Login for an Operator User..... 6

**Chapter 7: Configure Advisory Notice and Consent Warning Message
for Orchestrator..... 10**

Chapter 8: Monitor Customers..... 12

Chapter 9: Manage Customers..... 14

 9.1 Create New Customer..... 15

 9.2 Clone a Customer..... 19

 9.3 Configure Customers..... 21

 9.3.1 Configure Hand-off Operator..... 28

 9.3.2 Configure Distributed Cost Calculation..... 36

 9.3.3 Configure Path Calculation with Multiple DSCP Labels per Flow..... 39

Chapter 10: Manage Partners..... 42

 10.1 Create New Partner..... 43

 10.2 Configure Partner..... 45

Chapter 11: Partner Settings..... 48

Chapter 12: Manage Operators..... 50

 12.1 Monitor Operator Events..... 50

 12.2 Manage Operator Profiles..... 51

Chapter 13: User Management Operator..... 60

13.1 Users.....	60
13.1.1 Add New User.....	62
13.1.2 API Tokens.....	63
13.2 Roles.....	65
13.2.1 Add Role.....	67
13.2.2 Enterprise Security Admin Role.....	69
13.3 Service Permissions.....	71
13.3.1 New Permission.....	74
13.3.2 List of User Privileges.....	76
13.4 Authentication.....	82
13.4.1 Configure Azure Active Directory for Single Sign On.....	93
13.4.2 Configure Okta for Single Sign On.....	98
13.4.3 Configure OneLogin for Single Sign On.....	102
13.4.4 Configure PingIdentity for Single Sign On.....	105
Chapter 14: Manage User Agreements.....	108
Chapter 15: Manage Gateway Pools and Gateways.....	112
15.1 Manage Gateway Pools.....	112
15.1.1 Create New Gateway Pool.....	114
15.1.2 Clone a Gateway Pool.....	116
15.1.3 Configure Gateway Pools.....	116
15.2 Manage Gateways.....	118
15.2.1 Create New Gateway.....	120
15.2.2 Configure Gateways.....	123
15.2.3 Upgrade Orchestrator for Dual Stack Support.....	129
15.2.4 Configure IPv6 Address on Gateways.....	129
15.2.5 Partner Gateways.....	131
15.2.6 Monitor Gateways.....	136
15.3 SD-WAN Gateway Migration.....	140
15.3.1 Limitations of VeloCloud Gateway Migration.....	141
15.3.2 Quiesce Gateways.....	142
15.3.3 Decommission Quiesced Gateways.....	143
15.4 Diagnostic Bundles for Gateways.....	144
15.4.1 Request Diagnostic Bundles for Gateways.....	144
15.4.2 Request Packet Capture Bundle for Gateways.....	147
Chapter 16: Platform and Modem Firmware and Factory Images.....	149
Chapter 17: Software Images.....	152
Chapter 18: Edge Licensing.....	154
18.1 Manage Edge Licenses for Partners.....	156
18.2 Manage Edge Licenses for Customers.....	157
Chapter 19: Application Maps.....	160
Chapter 20: Edge Management.....	165

Chapter 21: Access SD-WAN Edges Using Key-Based Authentication.....	168
21.1 Add SSH Key.....	168
21.2 Revoke SSH Keys.....	169
For Other Operator Users.....	169
21.3 Enable Secure Edge Access for an Enterprise.....	170
21.4 Secure Edge CLI Commands.....	170
21.4.1 Sample Outputs.....	173
Chapter 22: Configure User Account Details.....	175
Chapter 23: Orchestrator Diagnostics.....	181
Diagnostic Bundles.....	181
Database Statistics.....	184
Chapter 24: Orchestrator Upgrade with New Orchestrator UI.....	187
Chapter 25: Replication.....	191
Chapter 26: System Properties.....	192
Chapter 27: External Certificate Authority.....	194
Configure External CA.....	196
Sample External CA Configuration.....	200
Monitoring External CA.....	201
Appendix A: Appendix.....	203
A.1 Operator-Level Orchestrator Alerts and Events.....	203
Appendix B: References.....	210
B.1 Related Documents.....	210

Arista VeloCloud SD-WAN Operator Guide

The Arista VeloCloud SD-WAN™ Operator Guide provides information about Orchestrator, including how to configure and manage Customers and Partners who use the Orchestrator.

About the Arista VeloCloud SD-WAN Operator Guide

The Arista VeloCloud SD-WAN™ Operator Guide provides information about Arista VeloCloud Edge Cloud Orchestrator, including how to configure and manage Customers and Partners who use the Orchestrator.

Intended Audience

This guide is intended for Operators and Service Providers, who are familiar with the Networking and SD-WAN operations.

Here's a quick walkthrough of the user journey as an Operator super user:

1. Install SD-WAN Orchestrator
2. Configure SD-WAN Orchestrator Disaster Recovery
3. Upload Software Images
4. Configure System Properties
5. Configure Operator Users
6. Configure Operator Profiles
7. Configure Customers
8. Configure Partners
9. Configure User Agreements
10. Manage Edge Licensing
11. Provision Edges
12. Configure Gateways and Gateway Pools
13. Configure Profiles
14. Monitor Customers
15. Monitor and Troubleshoot Gateways
16. Troubleshoot SD-WAN Orchestrator

Overview of Arista VeloCloud Orchestrator

Arista VeloCloud Orchestrator provides centralized, enterprise-wide installation, configuration, and real time monitoring, in addition to orchestrating the data flow through the cloud network.

The Orchestrator is available as web-based user interface, where you can configure and manage the following:

- Customers
- Partners
- Operator Users
- Gateways and Gateway Pools
- Orchestrator Authentication Modes

Supported Browsers

The Orchestrator supports the following browsers:

Table 1: Supported Browsers

Browsers Qualified	Browser Version
Google Chrome	77 – 79.0.3945.130
Mozilla Firefox	69.0.2- 72.0.2
Microsoft Edge	42.17134.1.0- 44.18362.449.0
Apple Safari	12.1.2-13.0.3



Note: For the best experience, Arista VeloCloud recommends Google Chrome or Mozilla Firefox.



Note: Starting from Arista VeloCloud SD-WAN version 4.0.0, the support for Internet Explorer has been deprecated.

What's New

What's New in Version 6.1.0

Table 2: New Features

Feature	Description
Enterprise Security Admin Role	Customization of the Enterprise Security Admin role is enhanced to separate network and security actions. This customization allows you to configure only the Firewall settings at Profile and Edge level. All other SD-WAN configurations become read-only for an Enterprise Security Admin role. For more information, see Enterprise Security Admin Role .
Multiple Identity Providers (IdP) for Orchestrator Single Sign On	This feature allows Partners and Service Providers the option to login as Operators on their Dedicated Orchestrator using Single Sign On (SSO). Previously, since a Dedicated Orchestrator is managed by VeloCloud, the Edge Operations team already configured their own SSO IdP for logging in, and this forces the Partner to rely on Native Authentication (username/password) to login as an Operator user. With this feature, VeloCloud can allocate an additional IdP for the Partner or Service Provider. For more information, see Authentication .
VCMP Tunnel Management based on Authentication mode change	The behavior of Edge and Gateway is enhanced based on different combinations of authentication mode changes. For more information, see Configure Gateways .

Release Notes

For information on all the new/modified features for 6.1.0, see *VeloCloud SD-WAN 6.1.0 Release Notes*.

Previous VeloCloud SD-WAN Versions

To get product documentation for previous versions of VeloCloud SD-WAN, contact your Arista representative.

Using SSO Login for an Operator User

Describes how to log in to Orchestrator using Single Sign On (SSO) as an Operator user.

- Ensure you have configured the SSO authentication in Orchestrator.
- Ensure you have set up users, roles, and OIDC application for the SSO in your preferred IDPs.

For additional information, see [Authentication](#).

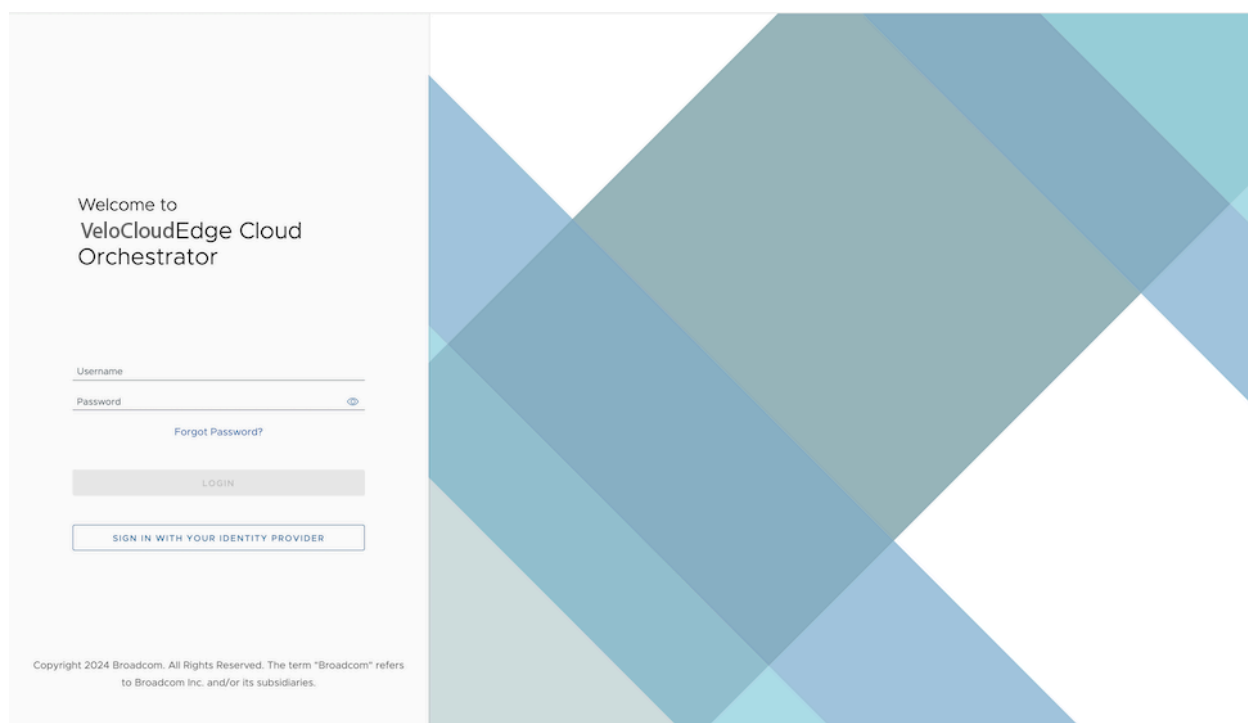


Note: If other authentication mechanisms fail, there must always be a native Operator Superuser as a system fallback.

To login into Orchestrator using the SSO as an Operator user:

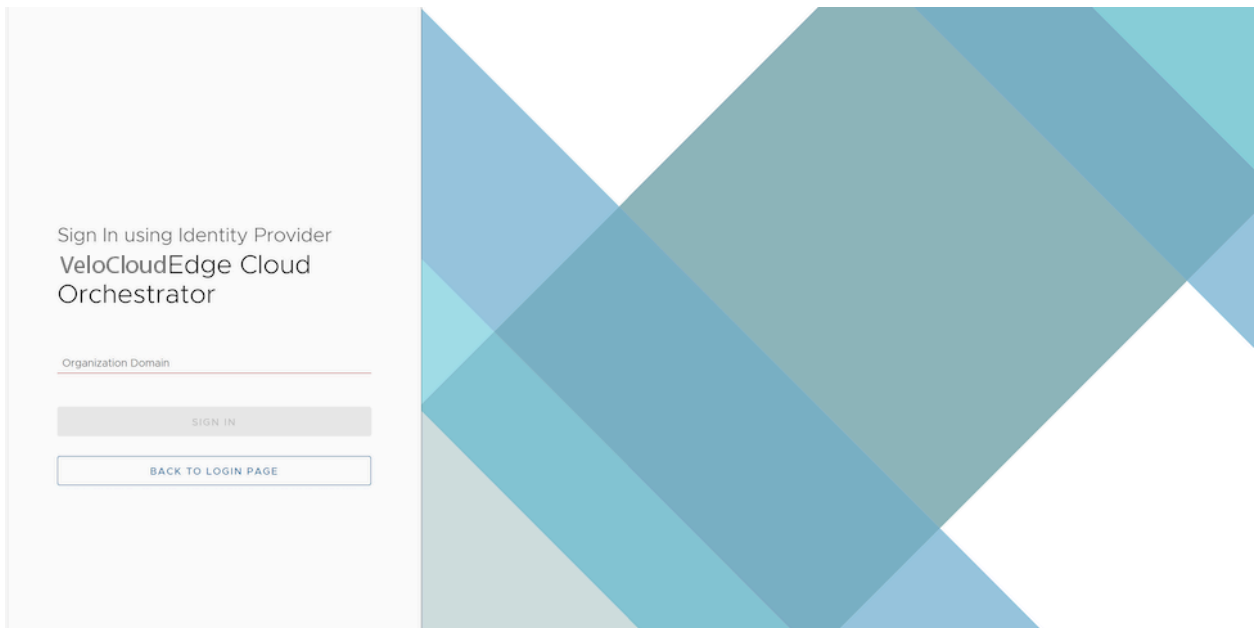
1. In a web browser, launch the Orchestrator application as an Operator user.

Figure 6-1: Displaying the VeloCloud Orchestrator Login Page



2. Select **Sign In With Your Identity Provider**.

Figure 6-2: Signing in with Your Identity



3. In the **Organization Domain** text box, enter the domain name used for the SSO configuration and select **Sign In**. The IdP configured for the SSO authenticates the user and redirects the user to the configured Orchestrator URL.



Note: Once the users log in to the Orchestrator using the SSO, they are not allowed to log in again as native users.

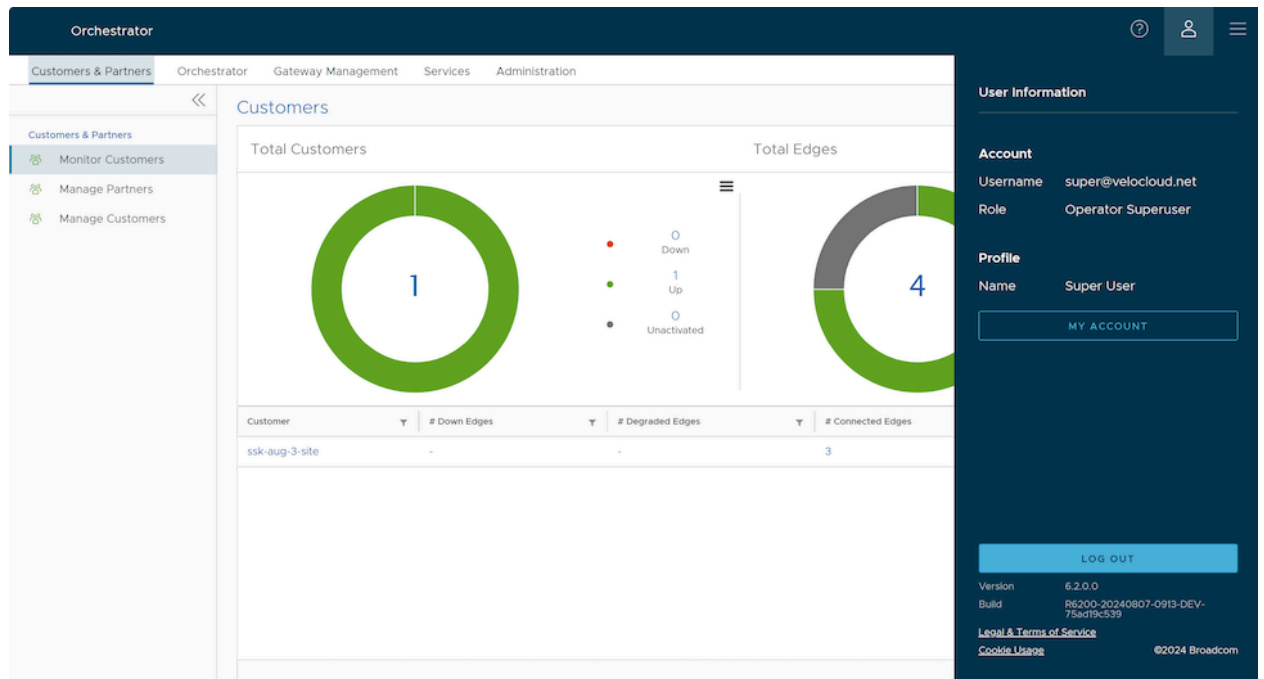
- Manage Customers and Partner
- Manage Operators
- Configure User Account details
- Manage Gateway pools and Gateways
- Manage Software and Firmware images

Additionally, in the Orchestrator home page, you can access the following features from the Global Navigation bar:

- The user can select the **User** icon located at the top right of the screen to access the **My Account** page. The **My Account** page allows users to configure basic user information, SSH keys, and API tokens. Users can also view the current user's role, associated privileges, and additional information such as version

number, build number, legal and terms information, cookie usage, and Arista trademark. For additional information, see [Configure User Account Details](#).

Figure 6-3: Displaying Orchestrator



- Starting with the 5.4.0 release, the **In-product Contextual Help Panel** with context-sensitive user assistance is supported in the SD-WAN service of the Enterprise Orchestrator UI and as well as for the Operator and Partner levels. In the Global Navigation bar, select the **Question Mark** icon located at the top right of the screen to access the Support panel.

The Support panel allows users across all levels to access helpful and important information such as Question-Based Lists (QBLs), Knowledge base links, Ask the Community link, how to file a support ticket, and other related documentation from within the Orchestrator UI page itself. This makes it easier for the user to learn our product without having to navigate to another site for guidance or contact the Support Team.



Note: By default, the Support Panel is not available to all Customers. You can activate this feature for a Customer by navigating to the **Global Settings > Customer Configuration >**

Additional Configuration > Global > Feature Access page. For additional information, see [Configure Customers](#).

Figure 6-4: Displaying the Support Panel

The screenshot displays the VMware SD-WAN Orchestrator interface. The top navigation bar includes 'Orchestrator', 'Customer custftest', and 'SD-WAN'. Below this, the main navigation menu has 'Monitor', 'Configure', 'Diagnostics', and 'Service Settings'. The 'Monitor' section is active, showing a sidebar with 'Network Overview', 'Edges', 'Network Services', 'Routing', 'Alerts', 'Events', and 'Reports'. The main content area is titled 'Network Overview' and is divided into 'Activated Edges' and 'Links'. Both sections show a large '0' in a circle, indicating no data is present. A table below the 'Activated Edges' section has columns for 'Edge Name', 'Status', 'Secrets Encryption', 'HA (Mode)', 'Cluster Name', and 'Links'. The table is empty, and a message 'No edges for this network found' is displayed with an icon of a watering can. The right sidebar is the 'SUPPORT' panel, featuring a search bar, 'POPULAR TOPICS' with several help links, and buttons for 'Knowledge Base' and 'Ask the Community'.

Configure Advisory Notice and Consent Warning Message for Orchestrator

As an Operator user, you can configure and display a Security Administrator-specified advisory notice and consent warning message regarding the use of Orchestrator for Operators, Partners, and Enterprises.

To configure the consent warning message:

1. In the **Operator** portal, go to **System Properties**.
2. Search and locate the `login.warning.banner.message` system property.
3. Select the system property, and then select **Actions > Modify System Property**. The **Modify System Property ...** page appears.

Figure 7-1: Modifying System Properties

Modify System Property...

Name:

Data Type:

Value:

```
{
  "msg": "The use of this system is restricted to authorized users only. Unauthorized access, use, or modification of this computer system or of the data contained herein or in transit to/from this system constitutes a violation of Title 18, United States Code, Section 1030 and state criminal and civil laws. These systems and equipment are subject to monitoring to ensure proper performance of applicable system and security features. Such monitoring may result in the acquisition, recording and analysis of all data being"
}
```

Value is Password: Yes - No

Value is Read-only: Yes - No

Description:

4. Ensure that the **Data Type** field is set to **JSON**.
5. In the **Value** text area, the default value is as follows:

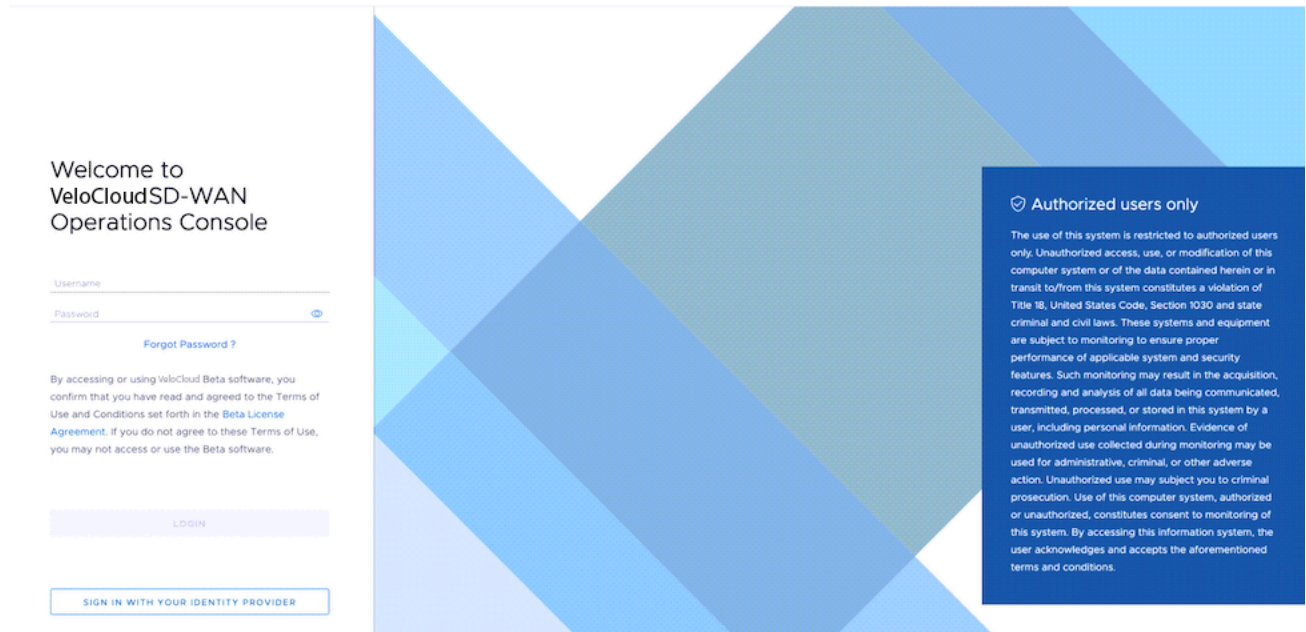
```
{ "msg": "" }
```

In the "msg" variable, type the required warning message between "".

6. Ensure that the **Value is Password** and **Value is Read-only** fields are set to **No**.
7. Select **Update**.

The warning message displays in the Orchestrator prior to user login for Operator, Partner, and Enterprise.

Figure 7-2: Displaying the Operations Console

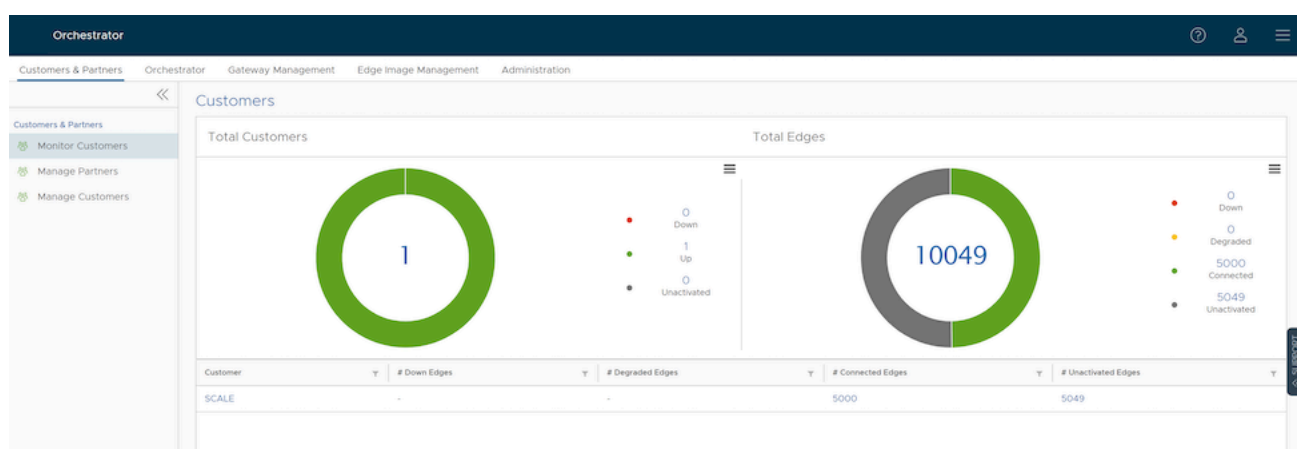


Monitor Customers

As an Operator user, you can monitor the status of your Customers along with the Edges connected to the Customers.

Log into the Arista **VeloCloud Edge Cloud Orchestrator** as an Operator user. In the **SD-WAN** service of the **Operator** portal, select **Customers & Partners > Monitor Customers**.

Figure 8-1: Monitoring Customers



The **Customers** page displays the following details:

Total Customers

- Customers managed by the Operator.
- Number of Customers that are UP, DOWN, and UNACTIVATED. Select the number to view the corresponding Customer details at the bottom panel.
- In the bottom panel, select the link to the Customer name to navigate to the Enterprise portal, where you can view and configure other settings corresponding to the selected customer. For additional information, see the *VeloCloud SD-WAN Administration Guide*.

Total Edges

- Edges associated with the Customers.
- Number of Edges that are DOWN, DEGRADED, CONNECTED, and UNACTIVATED. Select the number to view the corresponding details of the Edges in the bottom panel.
- In the bottom panel, place the mouse cursor on the Down Arrow displayed next to the number of Edges, to view the details of each Edge. Select the link to the Edge name to navigate to the Enterprise Monitoring portal, where you can view additional details corresponding to the selected Edge. For additional information, see the *VeloCloud SD-WAN Administration Guide*.



Note: The Orchestrator UI does not provide the option for auto refresh. You must refresh the window manually to view the current data.

Manage Customers

The Manage Customers option allows you to create new Customers, configure the Customer capabilities, clone the existing configuration, and to configure other Customer settings.


1. In the **Operator** portal, navigate to **Customers & Partners > Manage Customers**.

Figure 9-1: Manage Customers

Customer	Partner	Gateway Pool	Edges	Edge Config Updates Enabled	Edge Config Updates Enabled on Upgrade	Operator Alerts	Alerts	Services
5-site		5-site-GatewayPool	5 Edges	Enabled	Not Enabled	Enabled	Enabled	SDWAN, ADMIN
<input checked="" type="checkbox"/>		5-site-GatewayPool	0	Enabled	Not Enabled	Enabled	Enabled	SDWAN, ADMIN

2. You can perform the following actions:

Table 3: Manage Customers Option Descriptions


Option	Description
Search	Enter a search term to search for the matching text across the table. Use the advanced search option to narrow down the search results.
New Customer	Select this option to add a new Customer. For additional information, see Create New Customer .
Clone	Clones the existing configurations of the selected Customer. You can select any of the additional clone attributes. For additional information, see Clone a Customer .
Delete	Deletes the selected Customers. Enter the number of selected Customers in the pop-up window, and then select Delete .
	<div style="border: 1px solid #ccc; padding: 5px; background-color: #e6f2ff;"> <p> Note: Ensure that you have removed all the Edges associated with the selected Customer, before deleting the Customer.</p> </div>
Edit Customer System Settings	Allows you to edit the system settings for the customer. For additional information, see the "Enterprise Settings" section in the <i>VeloCloud SD-WAN Administration Guide</i> .
Stage to Bastion	Select to stage a Customer to the Bastion Orchestrator.



Note: **Stage to Bastion** and **Unstage from Bastion** options are available only when the Bastion Orchestrator feature is activated using the `session.options.enableBastionOrchestrator` system property. For additional information, see *Bastion Orchestrator Configuration Guide*.

3. Select **More** to perform the following actions:

Table 4: Additional Option Descriptions

Option	Description
Unstage from Bastion	Removes a Customer from the Bastion Orchestrator.
Edit Customer Edge Management	Allows to edit the Edge Management feature for the selected Customers.
Transfer to Partner	Assigns the selected Customer to a Partner. You can select an existing Partner from the drop-down list.
Release from Partner	Releases the selected Customer from the Partner.
Send Support Email	Sends customer support messages to the selected Customer.
Assign Operator Profile	Adds an Operator Profile for the selected Customers.
 Note: This option is available only for an Enterprise with an activated Edge Image Management feature.	
Update Edge Image Management	Activates or deactivates the Edge Image Management feature for the selected Customers.
Update Operator Alerts	Activates or deactivates the Operator alerts for the selected Customers.
Update Customer Alerts	Activates or deactivates the Customer alerts for the selected Customers.
Rebalance Gateways	Rebalances the Gateways of Edges associated with the selected Customer.
Export All Customers	Exports the details of all the Customers in the Operator portal to a CSV file. The default separator used is a comma (,).
Export Customers Edge Inventory	Exports the inventory details of all the Edges associated with all the Customers to a CSV file. The default separator used is a comma (,).

4. Following are the other options available in the **Manage Customers** area:

Table 5: Additional Manage Customers Option Descriptions

Option	Description
Columns	Select this option and select the check boxes to view the required columns.
Refresh	Select this option to refresh the page.

9.1 Create New Customer

In the **Operator** portal, you can create Customers and configure the Customer settings. Only Operator Super Users and Operator Standard Admins can create a new Customer. As an Operator Super User, you can temporarily deactivate creating new Customers, by setting the system property `session.options.disableCreateEnterprise` to `True`. You can use this option when Orchestrator exceeds the usage capacity.

1. In the **Operator** portal, go to **Customers & Partners > Manage Customers**, and then select **New Customer**. The **New Customer** page displays the following sections:

a. Configure customer information.

Figure 9-2: Configuring Customer Information

1. Customer Information Company Name / Account Number / Location

Company Name * vmware

Account Number @

SASE Support Access @

SASE User Management Access @

Location

Address Line 1 97, Columbia Place

Address Line 2

City Swindon

State / Province Wiltshire

Zip / Postcode 560108

Country / Region test

NEXT

Enter the details in the following fields and select **Next**.



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

Table 6: Customer Information Field Descriptions

Option	Description
Company Name	Enter your company name.
Account Number	Enter a unique identifier for the Customer.
SASE Support Access	This check box is selected by default, and grants access to the Arista Support to view, configure, and troubleshoot the Edges connected to the Customer. For security reasons, the Support cannot access or view the user identifiable information.
SASE User Management Access	Select the check box to allow the Arista Support to assist in User Management. The User Management includes options to create users, reset password, and configure other settings. In this case, the Support has access to user identifiable information.
Location	Enter relevant address details in the respective fields.

b. Configure administrative account details.

Figure 9-3: Adding an Administrative Account

2. Administrative Account
Username / Password / Contact Information

Username *
Ex: user@domain.com

Password *

Confirm Password *

First Name

Last Name

Phone

Mobile Phone

Contact Email *

Enter the details in the following fields and select **Next**.

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

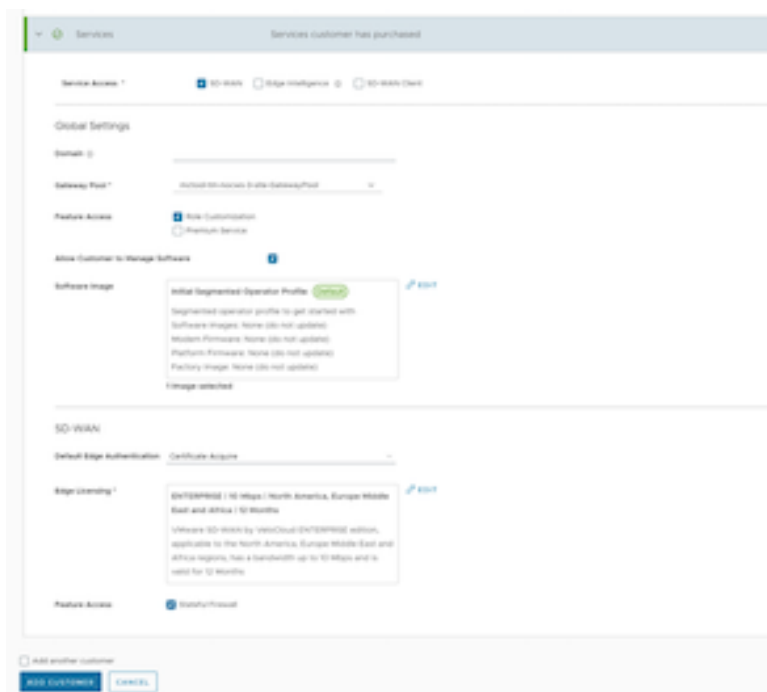
Table 7: Administrative Account Field Descriptions

Option	Description
Username	Enter the username in the user@domain.com format.
Password	Enter a password for the Administrator.
Confirm Password	Re-enter the password.
First Name	Enter the first name.
Last Name	Enter the last name.
Phone	Enter a valid phone number.
Mobile Phone	Enter a valid mobile number.
Contact Email	Enter the email address. The alerts on service status are sent to this email address.

Note: Starting from the 4.5 release, the use of the special character "<" in the password is no longer supported. In cases where users have already used "<" in their passwords in previous releases, they must remove it to save any changes on the page.


- c. Configure services as needed.

Figure 9-4: Adding Services



Configure the following global settings:

Table 8: Services Field Descriptions

Option	Description
Domain	Enter the domain name to be used to activate Single Sign On (SSO) authentication for the Orchestrator. This field is required when Edge Intelligence is activated for the Customer.
Gateway Pool	Select an existing Gateway pool from the drop-down list. For additional information, see Manage Gateway Pools .
Feature Access	You can select either Role Customization or Premium Service , or both the check boxes.
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. Once selected, the Software Image field is displayed. Select Add and in the Select Software/Firmware Images pop-up window, select and assign the software/firmware images from the available list for the Enterprise. Select Done to add the selected images to the Software Image list. <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> Note: You can remove an assigned image from an Enterprise, only if the image is not currently used by any Edge within the Enterprise.</div> For additional information, see Platform and Modem Firmware and Factory Images and Software Images .
Operator Profile	Select an Operator profile to be associated with the Customer from the available drop-down list. This field is not available if Allow Customer to Manage Software is selected. For additional information on Operator profiles, see Manage Operator Profiles .



Service Access: This option is available above the **Global Settings** section. You can choose the services that the Customer can access along with the roles and permissions available for the selected service.



Note: This option is available only when the system property `session.options.enableServiceLicenses` is set as `True`.

- **SD-WAN-** When you select this service, the following options are available:

Table 9: SD-WAN Option Descriptions

Option	Description
Default Edge Authentication	<p>Choose the default option to authenticate the Edges associated with the Customer, from the drop-down list.</p> <ul style="list-style-type: none"> • Certificate Deactivated: Edge uses a pre-shared key mode of authentication. • Certificate Acquire: This option is selected by default and instructs the Edge to acquire a certificate from the certificate authority of the Orchestrator, by generating a key pair and sending a certificate signing request to the Orchestrator. Once acquired, the Edge uses the certificate for authentication to the Orchestrator and for establishment of VCMP tunnels. <div data-bbox="781 821 1536 894" style="border: 1px solid #ccc; padding: 5px;"> <p> Note: After acquiring the certificate, the option can be updated to Certificate Required.</p> </div> <ul style="list-style-type: none"> • Certificate Required: 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>.
Edge Licensing	<p>Select Add and in the Select Edge Licenses pop-up window, select and assign the Edge licenses from the available list for the Enterprise.</p> <div data-bbox="740 1129 1536 1262" style="border: 1px solid #ccc; padding: 5px;"> <p> Note: The license types can be used on multiple Edges. It is recommended to provide your customers with access to all types of licenses to match their edition and region.</p> <p>For additional information, see Edge Licensing.</p> </div>
Feature Access	<p>Select the Stateful Firewall check box to override the Stateful Firewall settings activated on the Enterprise Edge.</p>

2. After entering all the details, select **Add Customer**. If you want to add another customer, you can select the **Add another Customer** before selecting **Add Customer**. The new Customer name displays on the **Customers** page. You can select the Customer name to navigate to the Enterprise portal and add configurations to the Customer.

For additional information, see [Configure Customers](#).

9.2 Clone a Customer

You can clone the configurations from an existing customer and create a new customer with the cloned settings.

Only Operator Super users and MSP Super users can clone a customer.

By default, the following configurations are cloned from the selected customer:

- Enterprise configuration profiles
- Enterprise network services and objects like:
 - DNS services
 - Private network names
 - Network Segments
- Customer capabilities
- Edge authentication scheme
- Address groups and Port groups



Note: **Distributed Cost Calculation** is not copied to the cloned Enterprise.

You cannot clone an Enterprise if it consists of the following:

- Profile with Edge references like hubs, clusters, and so on
- Profile containing Partner Gateway References
- Cloud Security Service enabled
- Non SD-WAN Destinations
- VNF or VNF licenses
- Authentication services
- NetFlow objects like collectors or filters

1. Log into the Arista Edge Cloud Orchestrator as an Operator user. Navigate to **Customers & Partners > Manage Customers**.
2. In the **Customers** page, select the customer you want to clone, and then select **Clone**.

The **Clone Customer** page appears.

Figure 9-5: Clone Scale Customer

3. Configure the **Customer Information**, **Administrative Account** details, and **Services**. For additional information, see [Create New Customer](#).
4. Select **Add Customer**.

The new customer name is displayed in the **Customers** page. The customer is already configured with the cloned settings. You can select the customer name to navigate to the Enterprise portal and add or modify the configurations. For additional information about customer configurations and settings, see [Configure Customers](#).

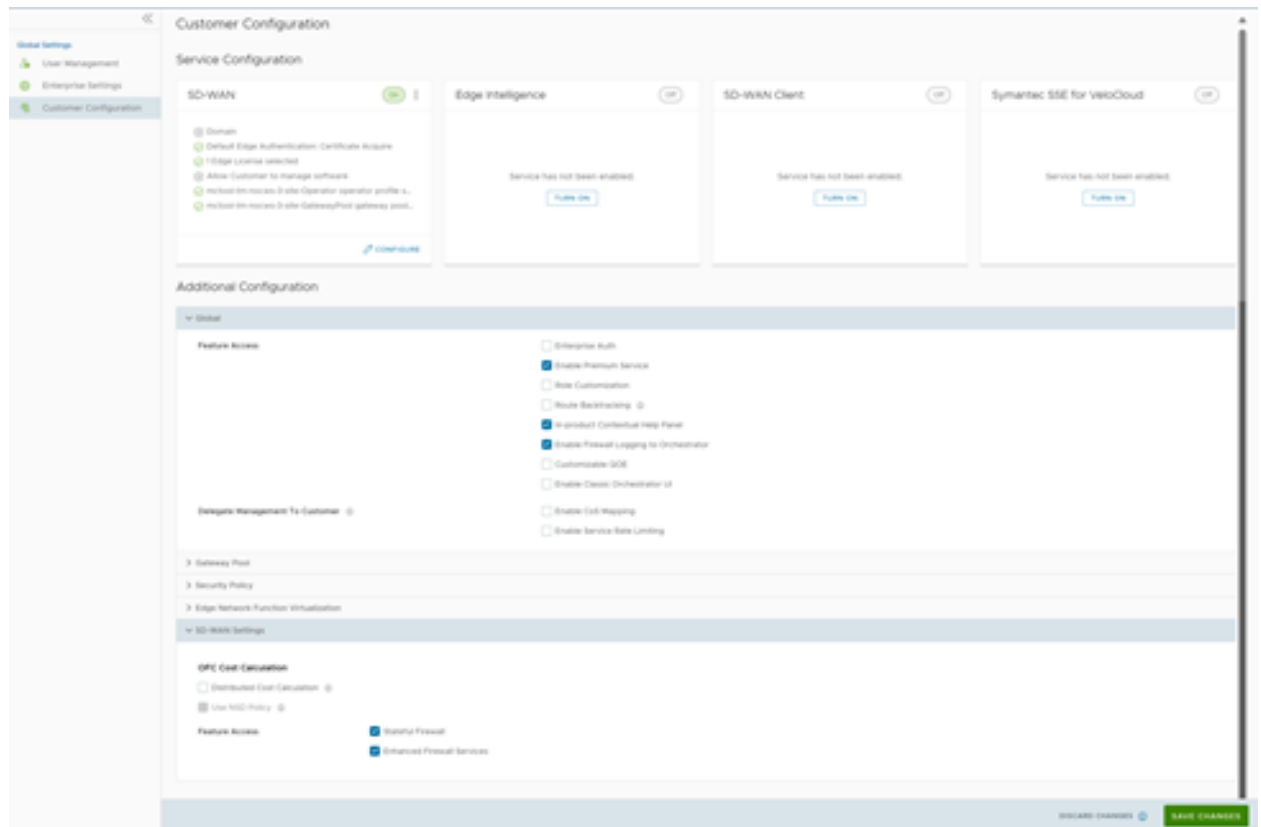
9.3 Configure Customers

After creating a Customer, configure the feature options and settings that the Customer can access. As an Operator, you can choose the settings the Customer can modify.

1. 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 directly from the Operator portal, by following the steps below:
2. In the monitoring and configuration options page, select a Customer, and from the top header, select **SD-WAN > Global Settings**.
3. From the left menu, select **Customer Configuration**.

The following page is displayed:

Figure 9-6: Customer Configuration



Service Configuration section includes the **SD-WAN** service:

4. 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 of the tile to configure the respective service. The tile displays the configuration summary.



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



5. Selecting the **Configure** option displays the following pop-up window. Configure the settings, and then select **Update**.

Figure 9-7: SD-WAN Configuration

SD-WAN Configuration ×


Domain * ⓘ	<input type="text" value="5-site"/>
Default Edge Authentication	<input type="text" value="Certificate Acquire"/> ▾
Edge Licensing *	<div style="border: 1px solid #ccc; padding: 5px; min-height: 40px;">0 Edge Licenses selected</div> + ADD
Allow Customer to manage software ⓘ	<input type="checkbox"/>
Operator Profile *	<input type="text" value="5-site-Operator"/> ▾
Maximum Number of Segments *	<input type="text" value="16"/>

Table 10: 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">• Certificate Deactivated: Edge uses a pre-shared key mode of authentication.• Certificate Acquire: This option is selected by default and instructs the Edge to acquire a certificate from the certificate authority of the Orchestrator, by generating a key pair and sending a certificate signing request to the Orchestrator. Once acquired, the Edge uses the certificate for authentication to the Orchestrator and for establishment of VCMP tunnels. <div data-bbox="703 583 1511 661" style="border: 1px solid #0070C0; padding: 5px;"><p> Note: After acquiring the certificate, the option can be updated to Certificate Required.</p></div> <ul style="list-style-type: none">• Certificate Required: 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>.
Edge Licensing	<p>The existing Edge Licenses are displayed. Select Add to add or remove the licenses.</p> <div data-bbox="665 869 1511 963" style="border: 1px solid #0070C0; padding: 5px;"><p> Note: The license types can be used on multiple Edges. It is recommended to provide your Customers with access to all types of licenses to match their edition and region. For additional information, see Edge Licensing.</p></div>
Allow Customer to Manage Software	Select the check box if you want to allow an Enterprise Superuser to manage the software images available for the Enterprise. For additional information, see the topic <i>Edge Image Management</i> in the <i>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 Allow Customer to Manage Software is selected. For additional information on Operator profiles, see Manage Operator Profiles .
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 .



6. Users can configure the additional configuration settings available on the **Customer Configuration** page:

Table 11: Customer Configuration- Options and Descriptions

Option	Description
Global	<p>User Agreement Display</p> <p>Select either of the following from the drop-down menu:</p> <ul style="list-style-type: none"> • Inherit • Override to Hide • Override to Show
Feature Access	<div data-bbox="667 506 1510 583" style="border: 1px solid #0070C0; padding: 5px; margin-bottom: 10px;">  Note: </div> <p>This field is available only when the system property <code>session.options.enableUserAgreements</code> is set to True.</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"> • Enterprise Auth: By default, only the Operator can activate or deactivate two-factor authentication for an Enterprise. When you select this check box, the Enterprise Admins can configure the two-factor authentication on their own. This option also controls the activation and deactivation of Single Sign On (SSO). • Enable Premium Service: This option is selected by default. Premium Service refers to the On-Demand Remediation feature that is a core part of SD-WAN's Dynamic Multipath Optimization (DMPO). DMPO is used for all traffic that traverses a VeloCloud Gateway. When Premium Service is selected, the Gateway uses Forward Error Correction (FEC) for customer traffic impacted by high levels of WAN link jitter or loss, and which cannot be steered to a better quality WAN link. When Premium Service is not selected, traffic still traverses the VeloCloud Gateway and benefit 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>. • Role Customization: Allows an Enterprise Super user to customize the role privileges for other Enterprise users. • Route Backtracking: Allows the device to choose the best route in the order of prefix length. • In-product Contextual Help Panel: Provides access to the 'In Product Help' panel integrated within the Orchestrator. This feature is deactivated by default. An Operator must activate this option for the Enterprise Customers. • Enable Firewall Logging to Orchestrator: By default, Edges cannot send their Firewall logs to the Orchestrator. Select this check box to allow an Edge to send the Firewall logs to the Orchestrator. • Customizable QoE: Allows the Customer to configure the minimum and maximum latency threshold values for Voice, Video, and Transactional application categories of an Edge. • Enable Classic Orchestrator UI: Allows the Customer to switch from the Angular Orchestrator UI to the Classic Orchestrator UI. This option is available only when the system property <code>session.options.enableClassicOrchestrator</code> is set to True.

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"> • Enable CoS Mapping: Allows to configure CoS mapping while configuring a business policy. • Enable Service Rate Limiting: Allows to rate limit services in a business policy.
Gateway Pool	
Current Gateway Pool	Displays the current Gateway pool associated with the selected Customer. If required, you can choose a different Gateway pool available in the drop-down menu and select Save Changes .
Gateways in this Pool	Displays the Gateway details in the current pool.
Partner Hand Off	Activating the Gateway Pool option displays the Configure Hand Off section. If the Gateways available in the Gateway pool have been assigned with Partner Gateway role, you can handoff the Gateways to Partners.
Security Policy	
Hash	<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 Turn off GCM check box, you can select one of the following as the authentication algorithm for the VPN header, from the drop-down menu:</p> <ul style="list-style-type: none"> • SHA 1 • SHA 256 • SHA 384 • SHA 512
Encryption	Select either AES 128 or AES 256 as the AES algorithm's key size to encrypt data. The default encryption algorithm mode is AES 128 .
DH Group	Select the Diffie-Hellman (DH) Group algorithm to be used when exchanging a pre-shared key. The DH Group sets the strength of the algorithm in bits. The supported DH Groups are 2, 5, 14, 15, 16, 19, 20, and 21.
	<div style="border: 1px solid black; padding: 5px;"> <p>Note:</p> <ul style="list-style-type: none"> • DH Groups 19, 20, and 21 are available starting from Release 5.2.0. • 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 Hash and select an authentication algorithm for the VPN header.
IPSec SA Lifetime Time(min)	Time when Internet Security Protocol (IPSec) rekeying is initiated for Edges. The minimum IPsec lifetime is 3 minutes and maximum IPsec lifetime is 480 minutes. The default value is 480 minutes.
	<div style="border: 1px solid black; padding: 5px;"> <p>Note: It is not recommended to configure low lifetime value for IPsec (less than 10 minutes), as it can cause traffic interruption in some deployments due to rekeys. The low lifetime values are for debugging purposes only.</p> </div>

Option	Description
IKE SA Lifetime(min)	<p>Time when Internet Key Exchange (IKE) rekeying is initiated for Edges. The minimum IKE lifetime is 10 minutes and maximum IKE lifetime is 1440 minutes. The default value is 1440 minutes.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>Note: It is not recommended to configure low lifetime values IKE (less than 30 minutes), as it can cause traffic interruption in some deployments due to rekeys. The low lifetime values are for debugging purposes only.</p> </div>
Secure Default Route Override	<p>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.</p>
Edge Network Function Virtualization:	<p>Allows to activate NFV on the Edges and allows Customers to deploy third party VNFs on service ready Edge platforms. Currently, the service ready Edge platform models are 520v and 840. As an Operator User, when you activate the Edge NFV, the Customers can configure and deploy VNFs and VNF licenses from their network services.</p>
Edge NFV	<p>Select this option to activate the ability to deploy VNFs on Edges. After deploying one or additional VNFs on Edges, you cannot deactivate this option.</p>
Security VNFs	<p>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>VeloCloud SD-WAN Administration Guide</i>.</p>
SD-WAN Settings	
OFC Cost Calculation	<p>Select the required check box:</p> <ul style="list-style-type: none"> Distributed Cost Calculation: Select this check box to delegate route cost calculation to Edges/Gateways. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>Note: This option is available only for the Edges/Gateways with version 3.4.0 and later. After activating Distributed Cost Calculation, it is recommended to refresh the routes by navigating to Configure > Overlay Flow Control in the SD-WAN service of the Enterprise portal. For additional information, see Configure Distributed Cost Calculation.</p> </div> Use NSD Policy: Select this check box to use NSD policy for route cost calculation to Edges/Gateways. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>Note: 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 Include DSCP value as part of flow lookup check box to include DSCP values as part of flow look-up and path calculation. For additional information, see Configure Path Calculation with Multiple DSCP Labels per Flow.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>Note: This field is available only when the system property <code>session.options.enableFlowParametersConfig</code> is set to True.</p> </div>
Feature Access	
Stateful Firewall	<p>Select the Stateful Firewall check box to override the Stateful Firewall settings activated on the Enterprise Edge.</p>

Option	Description
Enhanced Firewall Services	<p>Select the Enhanced Firewall Services check box to activate the Enhanced Firewall Services using the Firewall functionality in Arista Edge Cloud Orchestrator.</p> <div data-bbox="667 268 1511 342" style="border: 1px solid #add8e6; padding: 5px;"> <p> Note: 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 1511 541" style="border: 1px solid #add8e6; padding: 5px;"> <p> Note: Unselecting this option will only deactivate the EFS feature in the UI. To deactivate the EFS feature for an existing customer, you must first deactivate the EFS feature in the SD-WAN service of the Enterprise portal by navigating to Configure > Profiles/Edges > Firewall > Firewall Feature Control > Enhanced Security and then by unselecting this check box in Global Settings.</p> </div> <p>For additional information about configuring the various Enhanced Security Services and associating to a Firewall rule, see the topic <i>Configure Enhanced Security Services</i> in the <i>Arista VeloCloud SD-WAN Administration Guide</i>.</p>

7. Select **Save Changes**.

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.

9.3.1 Configure Hand-off Operator

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 9-8: Gateway 2

The screenshot displays the 'Gateway Management' interface for 'Gateway - 2'. The page is divided into several sections:

- Properties:**
 - Name:** Gateway - 2
 - Description:** Enter Description
 - Gateway Roles:**
 - Data Plane
 - Control Plane
 - Secure VPN Gateway
 - Partner Gateway** (highlighted with a red box)
 - CDE
 - Cloud Web Security
- Contact & Location:**
 - Contact Name:** Super User
 - Contact Email:** super@velocloud.net
 - Contact Phone:**
 - Location:** Lat, Lng: 37.403, -122.117
- Status:**
 - Administration:** Never Activated
 - Service State:** In Service
 - Gateway Authentication Mode:** Certificate Acquire
 - IPv4 Address:** 192.168.150.2
 - IPv6 Address:**

A map is visible in the bottom right corner, showing the location of the gateway.

To configure the handoff settings, perform the following steps:

1. Log in to the **Orchestrator** as an Operator user.
2. Navigate to **Customers & Partners > Manage Customers**.
3. In the **Manage Customers** window, select the link of the desired customer.
4. Go to **Global Settings > Customer Configuration**.
5. In the **Customer Configuration** window, scroll down to **Additional Configuration** and expand the **Gateway Pool** area.
6. Turn on the **Partner Hand Off** toggle button.

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

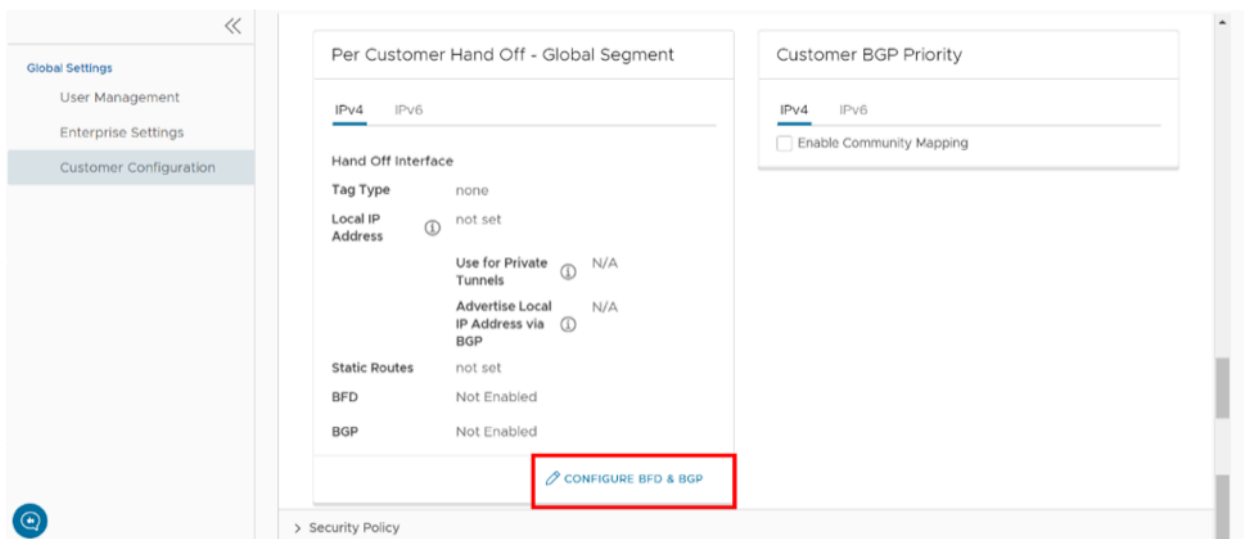
Figure 9-9: Configure Hand Off

Table 12: Configure Hand Off

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

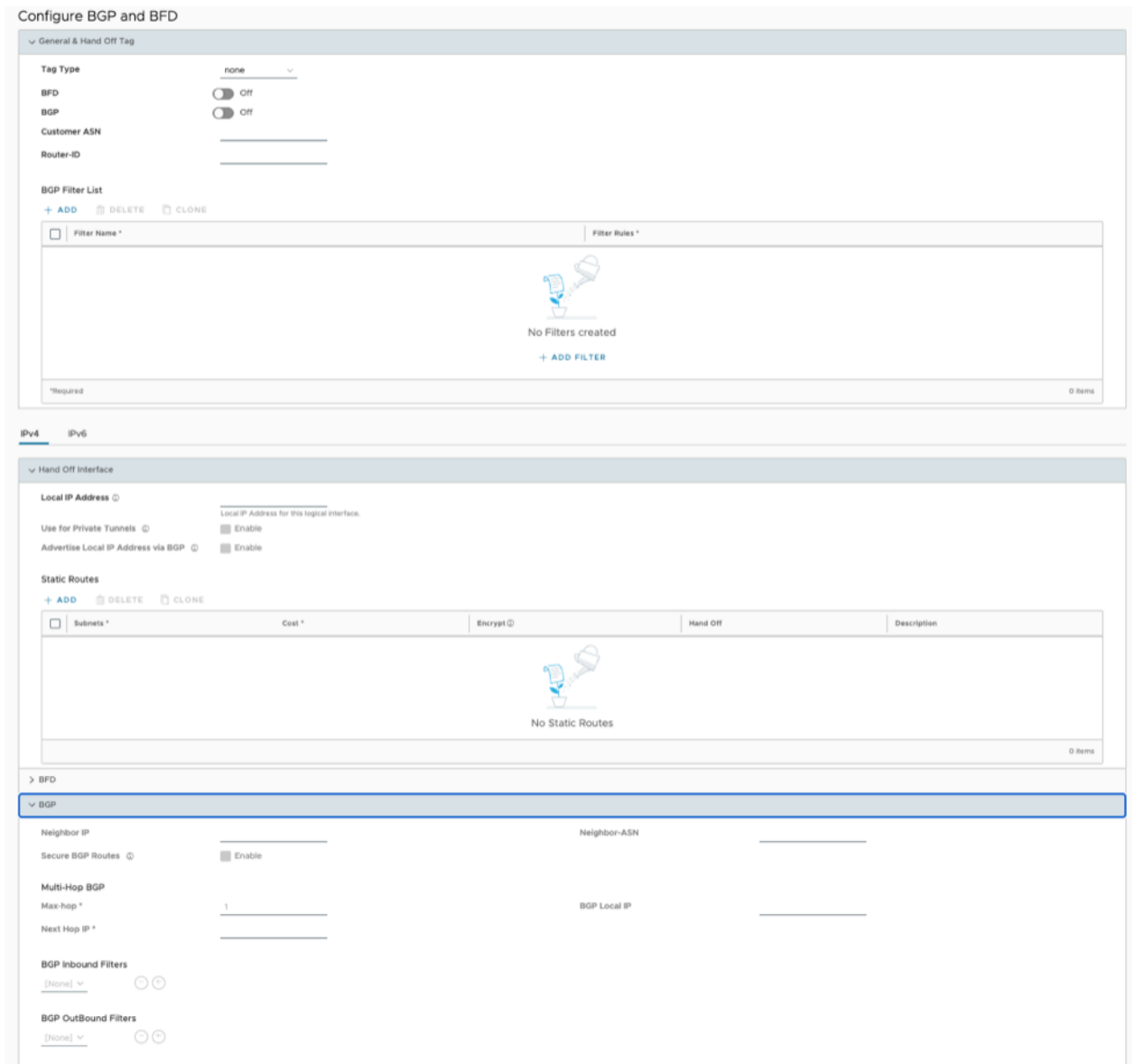
- At the bottom of the **Per Customer Hand Off – Global Segment** area, select the **Configure BFD & BGP** link, as shown in the image below.

Figure 9-10: Per Customer Hand Off



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

Figure 9-11: Configure BGP and BFD



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

Figure 9-12: BGP Activation






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

Table 13: BGP Configuration

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



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

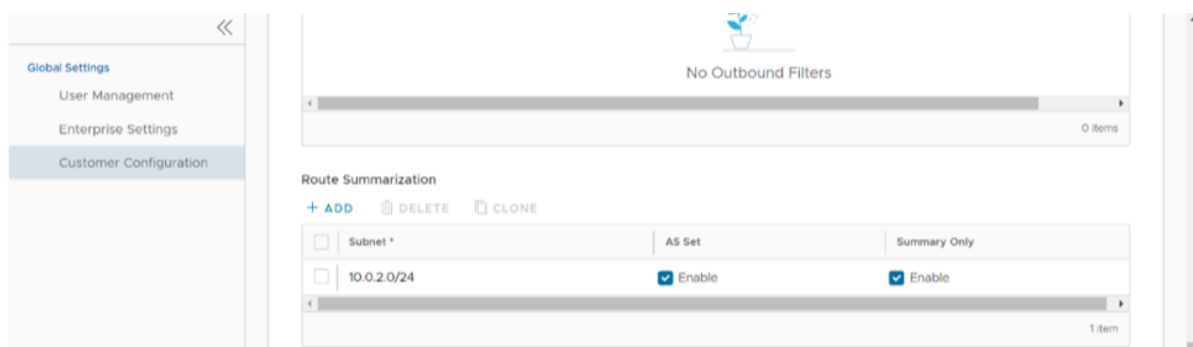
Option	Description
Next Hop IP	<p>Enter the next-hop IP address to be used by BGP to reach the multi-hop BGP peer.</p> <div style="border: 1px solid #00a0e3; padding: 5px;">  Note: This option is available only for multi-hop eBGP with Max-hop count greater than 1. </div>
Neighbor-ASN	Enter the Autonomous System Number of the Neighbor network.
BGP Local IP	<p>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.</p> <div style="border: 1px solid #00a0e3; padding: 5px;">  Note: The BGP Local IP address must be from a different subnet than a handoff IP address. </div> <p>If you do not enter any value, the IP address of the Hand Off Interface is used as the source IP address.</p>
BGP Filter List	Configure BGP filters.
BGP Inbound Filters	Assign filter to inbound.
BGP Outbound Filters	Assign filter to outbound.
BGP Optional Settings	
BFD	Select the check box to subscribe to the BFD session.
Router-ID	Enter the Router ID to identify the BGP Router.
Keep Alive	Enter the BGP Keep Alive time in seconds. The default timer is 60 seconds.
Hold Timers	Enter the BGP Hold time in seconds. The default timer is 180 seconds.
Turn off AS-PATH Carry Over	Select the check box to turn off AS-PATH carry over, which influences the outbound AS-PATH to make the L3-routers prefer a path towards a PE. If you select this option, ensure to tune your network to avoid routing loops. It is recommended not to select this check box.
MD5 Auth	Select the check box to activate BGP MD5 authentication. This option is used in a legacy network or federal network, and is used as a security guard for BGP peering.
MD5 Password	Enter a password for MD5 authentication.
	<div style="border: 1px solid #00a0e3; padding: 5px;">  Note: Starting from the 4.5 release, the use of the special character "<" in the password is no longer supported. In cases where users have already used "<" in their passwords in previous releases, they must remove it to save any changes on the page. </div>

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

- a. If applicable, configure for Route Summarization.

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

Figure 9-13: Route Summarization



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

Table 14: Route Summarization

Option	Description
+Add	Select +Add to add a new row in the Route Summarization area.
Subnet column	Under the Subnet column, enter the IP subnet.
AS Set column	Generate AS set path information from the summarized routes (while advertising the summarized route to the peer). Under the AS Set column, select the Yes check box if applicable.
Summary Only column	Under the Summary Only column, select the Yes check box to allow only the summarized route to be sent.

Note: To add additional rows to configure Route Summarization, select **+Add**. To Clone or Delete a route summarization, use the appropriate buttons, located next to **+Add**.

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

9.3.2 Configure Distributed Cost Calculation

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

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

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

Note:

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

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

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

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

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

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

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

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



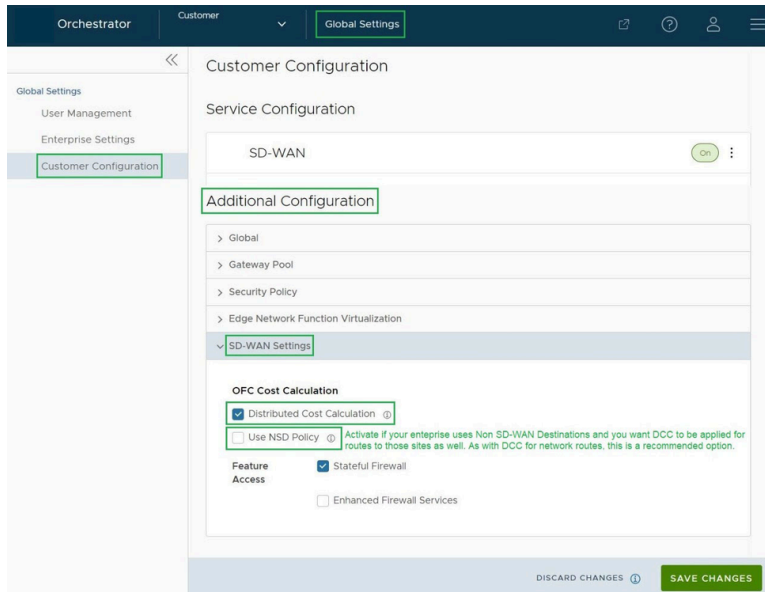
Note: It is recommended to enable Distributed Cost Calculation in a maintenance window to minimize the impact on the Customer Enterprise.

To configure Distributed Cost Calculation for a customer, perform the following steps:

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

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

Figure 9-14: Customer Configuration



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



- 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.

Note:

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 Administration Guide*.

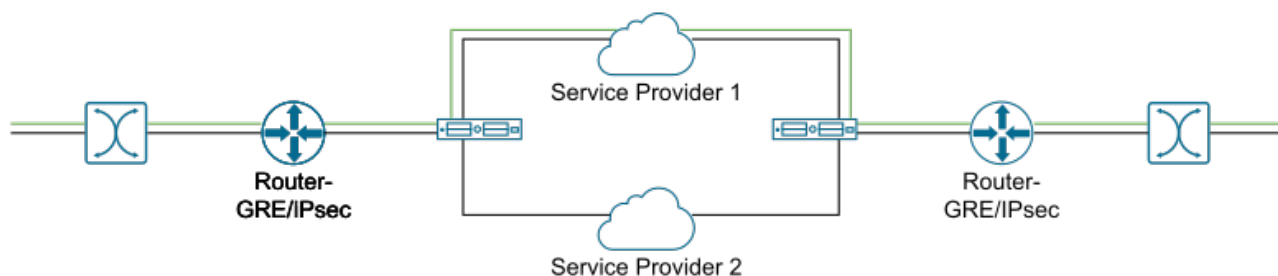
9.3.3 Configure Path Calculation with Multiple DSCP Labels per Flow

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 9-15: Encapsulation and Encryption Device



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



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

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



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

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

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

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

Limitations:

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

You can use this option for On-Premise deployment where Gateway is used only for control plane functionality and not for data plane traffic.

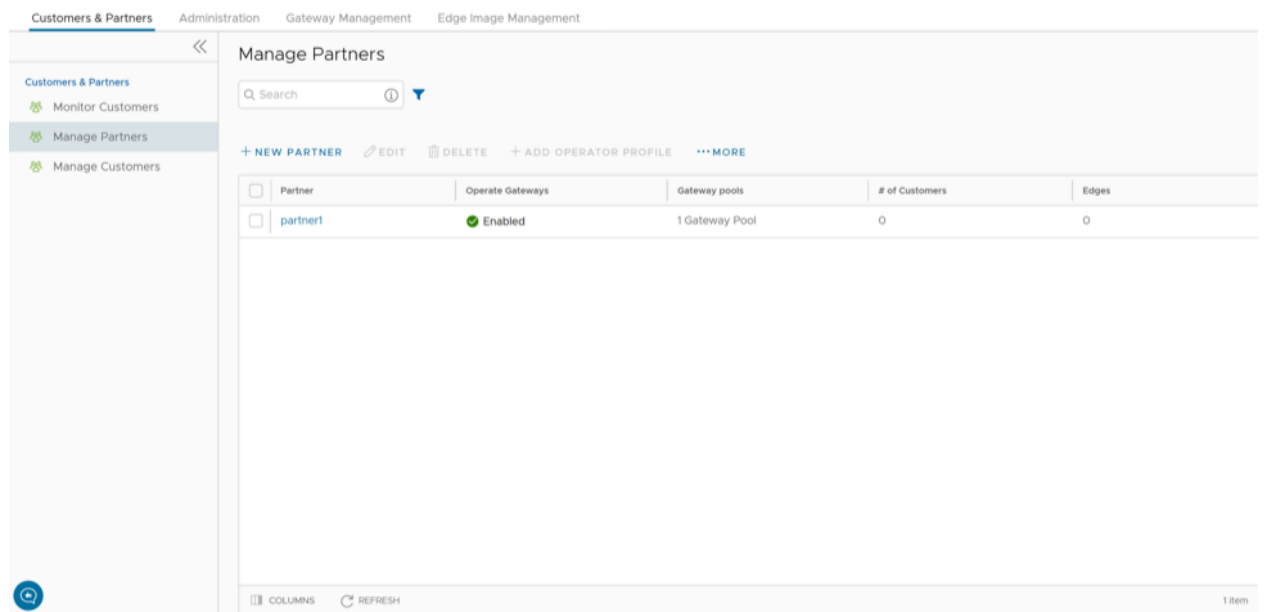
- The path calculation with multiple DSCP labels per Flow is intended only for GRE or IPSec traffic. The direct Internet traffic does not carry multiple DSCP labels within a single flow.
- After you enable the path calculation option, when the traffic flow consists of packets with same five-tuple information but different DSCP markings, LAN side NAT might not work as expected.

Manage Partners

The **Manage Partners** option allows you to create new Partners, who can independently manage a group of Customers.

1. Log into the **VeloCloud Orchestrator** as an Operator user. In the **SD-WAN** service of the **Operator** portal, select **Manage Partners**.

Figure 10-1: Manage Partners




The screenshot displays the 'Manage Partners' interface. At the top, there are navigation tabs: 'Customers & Partners', 'Administration', 'Gateway Management', and 'Edge Image Management'. The left sidebar shows 'Customers & Partners' with sub-items: 'Monitor Customers', 'Manage Partners' (highlighted), and 'Manage Customers'. The main content area is titled 'Manage Partners' and includes a search bar, a '+ NEW PARTNER' button, and action buttons for 'EDIT', 'DELETE', '+ ADD OPERATOR PROFILE', and '...MORE'. Below this is a table with the following data:

Partner	Operate Gateways	Gateway pools	# of Customers	Edges
partner1	Enabled	1 Gateway Pool	0	0

At the bottom of the interface, there are 'COLUMNS' and 'REFRESH' buttons, and a '1 Item' indicator.

2. You can perform the following actions:

Table 15: Manage Partners Option Descriptions

Option	Description
Search	Enter a search term to search for the matching text across the table. Use the advanced search option to narrow down the search results.
New Partner	Select this option to add a new Partner. For additional information, see Create New Partner .
Edit	This option takes you to the Partner Overview page in the Partner portal, where you can edit the Partner Capabilities , Available Software Images , and Gateway Pool of the selected Partner. For additional information, see Configure Partner .
Delete	Deletes the selected Partners. Enter the number of selected Partners in the pop-up window, and then select Delete .
	<div style="border: 1px solid #0070C0; padding: 5px;">  Note: Ensure that you have removed all the Customers associated to the selected Partner, before deleting the Partner. </div>
Add Operator Profile	Assigns an Operator profile to the selected Partners, which specifies the network settings managed by Orchestrator. In the Add Profiles to Selected Partners pop-up window, select a profile and select the arrow to add it. Select Save . For additional information, see Manage Operator Profiles .
More	Select this option, and then select Download to download the list of Partners' profiles in a CSV format.

3. Following are the other options available in the Manage Partners area:

Table 16: Additional Manage Partners Option Descriptions

Option	Description
Columns	Select the check boxes to view the required columns.
Refresh	Select this option to refresh the page.

10.1 Create New Partner

In the **Operator** portal, you can create Partners and configure the settings, so that the Partners can manage a group of Customers on their own.

Only Operator Superusers, Standard Operators, and Business Specialist Operators can create a new Partner.



Note: As an Operator Super User, you can temporarily deactivate creating new partners by setting the system property `session.options.disableCreateEnterpriseProxy` to `True`. You can use this option when Orchestrator exceeds the usage capacity.

1. Log into the **VeloCloud Orchestrator** as an Operator user. In the **Operator** portal, go to **Customers & Partners > Manage Partners**, and then select **New Partner**.

Figure 10-2: Create New Partner

The screenshot shows the 'New Partner' form in the VeloCloud Orchestrator. The form is divided into three sections, each with a 'NEXT' button at the bottom.

- Partner Information** (Name / Domain / Address):
 - Name: test
 - Domain: [empty]
 - SASE Support Access
 - Grant Gateway Management Access
 - Location:
 - Address Line 1: 97 Columbia Place
 - Address Line 2: Campbell Park
 - City: Milton Keynes
 - State / Province: [empty]
 - Country: United Kingdom
 - Zip / Postcode: [empty]
- Initial Partner Admin Account** (Username / Contact Information / Password):
 - Initial Partner Admin Account: [empty]
 - Username: abc@vmware.com
 - Password: [masked]
 - Confirm: [masked]
 - First Name: [empty]
 - Last Name: [empty]
 - Phone: [empty]
 - Mobile Phone: +1 -
 - Contact Email: abc@vmware.com
- 3. Default Properties** (Services customer has purchased):
 - Gateway Pool: Default Pool (gateway pool used when none is explicitly assigned to an enterprise)
 - Software Image: 5-site-Operator (Software Images: 5.1.0.0 (build R5100-20220625-M64-df6t5ddd))
 - Edge Licensing: ENTERPRISE | 10 Mbps | North America, Europe Middle East and Africa | 60 Months



At the bottom, there is a checkbox 'Add another partner' and two buttons: 'ADD PARTNER' and 'CANCEL'.

2. On the **New Partner** page, enter the following details:



Note: Select **Next** to go to the next section on the page. The **Next** button is activated only when you enter all the mandatory details in each section.

Table 17: Create New Partner Option Descriptions

Option	Description
Partner Information	
Name	Enter the Partner name.
Domain	Enter the domain name of the Partner.
SASE Support Access	This option is selected by default and grants access to the Arista Support to view, configure, and troubleshoot the settings of the Partner.
Grant Gateway Management Access	Select the check box to allow the Partner to create and manage the Gateways.
Location	Enter relevant address details in the respective fields.
Initial Partner Admin Account	
Username	Enter the username in the user@domain.com format.
Password	Enter a password for the Partner.
	<div style="border: 1px solid #ccc; padding: 5px;">  <p>Note: Starting from the 4.5 release, the use of the special character "<" in the password is no longer supported. In cases where users have already used "<" in their passwords in previous releases, they must remove it to save any changes on the page.</p> </div>
Confirm	Re-enter the password.
First Name, Last Name, Phone, Mobile Phone	Enter relevant details in the respective fields.
Contact Email	Enter the email address. The alerts on service status are sent to this email address.
Default Properties	
Gateway Pool	<p>Select Add to select the Gateway Pool from the available list. After adding the Gateway Pools, you can select Edit to add or remove the pools.</p> <p>For additional information on Gateway Pools, see Manage Gateway Pools.</p>
Software Image	Select Add to select the Software Image from the available list. After adding the Software Image, you can select Edit to add or remove the images. For additional information on Software Images, see Platform and Modem Firmware and Factory Images .
Edge Licensing	Select Add to select the Edge licenses from the available list. After adding the licenses, you can select Edit to add or remove the licenses. This option is available only when the value of System Property <code>session.options.enableEdgeLicensing</code> is set to <code>True</code> .
	<div style="border: 1px solid #ccc; padding: 5px;">  <p>Note: The license types can be used on multiple VeloCloud Edges. It is recommended to provide the Partners with access to all types of licenses to match their edition and region. For additional information, see Edge Licensing.</p> </div>

3. Select the **Add Another Partner** check box, to create another new Partner, or directly select the **Add Partner** button. The new Partner name is displayed on the **Manage Partners** page. You can select the Partner name to navigate to the Partner portal and add more configurations to the Partner. For additional information, see [Configure Partner](#).

10.2 Configure Partner

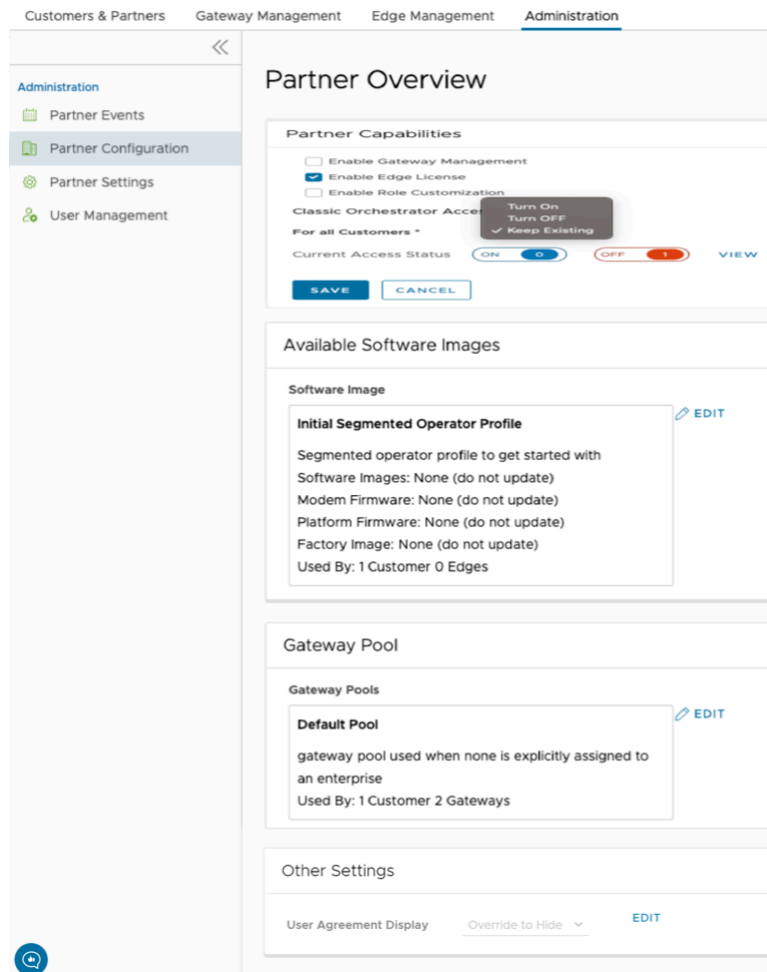
As an Operator Superuser and Operator Admin, when you create a new Partner, you are automatically redirected to the **Partner Overview** page, where you can configure Partner capabilities, Software images, Gateway pools, and other settings that the Partner can access.

To configure Partner information for an existing Partner:

1. In the **Operator** portal of the **VeloCloud Orchestrator**, select **Manage Partners**, and then select the Partner name to navigate to the Partner portal and add additional configurations to the Partner.




The **Partner Overview** page for the selected Partner appears.

Figure 10-3: Configure Partner



2. You can configure the following capabilities and settings for the selected Partner:

Table 18: Partner Configuration Option Descriptions

Option	Description
Partner Capabilities	<p>Selecting Edit allows you to select the following capabilities for the current Partner:</p> <ul style="list-style-type: none"> • Enable Gateway Management – Allows the Partner users to create, configure, and manage their own Gateways. • Enable Edge License – Allows the Partner users to manage their Edge Licenses. • Enable Role Customization – Allows a Partner Super user to customize the service permissions of other Partner users and Enterprise users of the Partner.
Classic Orchestrator Access	<p>Displays the Classic Orchestrator accessibility settings for the Partner Customers.</p> <p>For All Customers: An Operator can choose any one of the following options from the drop-down menu:</p> <ul style="list-style-type: none"> • Turn On: Allows Partner Customers to access the Classic Orchestrator. • Turn Off: Does not allow Partner Customers to access the Classic Orchestrator. • Keep Existing: This option indicates no change to the settings. <p>Current Access Status: Displays the access information (On/Off) for the existing Partner Customers. Select View to view the list of names and statuses of the Partner Customers.</p> <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;">  Note: You must refresh the page to see the Classic Orchestrator UI button at the top right of the screen. </div>
Available Software Images	<p>Displays all the software images assigned to the Partner. Select Edit to add or remove the software images in the list.</p> <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;">  Note: You cannot remove the software images that are assigned to a Customer. </div>
Gateway Pool	<p>Displays the Gateway pools associated with the selected Partner. Select Edit to add or remove the Gateway pools in the list.</p> <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;">  Note: You cannot remove the Gateway Pools that are assigned to a Customer. </div>
Other Settings	<p>Displays the settings of the User Agreement only if you have activated the User Agreement feature. By default, the User Agreement feature is not activated. To enable the User Agreement feature, navigate to the System Properties in the Operator portal, and set the value of the <code>session.options.enableUserAgreements</code> system property as <code>True</code>.</p> <p>You can choose to override the default display settings of the User Agreement, by selecting the Edit button and selecting relevant option from the User Agreement Display drop-down menu. By default, the Customer inherits the display mode set in the system properties.</p>

3. After configuring the required Partner details, select **Save Changes**.

Partner Settings

As an Operator, you can configure Partner specific information such as name, primary location, and primary contact.

1. In the **Operator** portal, select **Manage Partners**, and then select the link to a Partner name for which you wish to edit the settings.
2. From the top menu, select **Administration**, and then from the left menu, select **Partner Settings**.

Figure 11-1: Configure Partner Settings

Partner Settings

General Information

Name * abc

Domain Enter domain
Example: vmware

Description Enter Description (Optional)

Information Privacy Settings

Operator Support Access

Allow Support Access On
VMware Support is granted access to view your events. Granting VMware Support access to your customers is individually set at the customer level.

Partner Business Contact Information

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

Primary Business Contact

Contact Name test123

Contact Email test@velocloud.com

Phone +1 12345678990

Mobile Phone +1 12345678990

Primary Business Location

Address Line 1 97, Columbia Place

Address Line 2

City Bangalore

State / Province Karnataka


Zip / Postcode 560008

Country / Region India

DISCARD CHANGES

3. You can edit the following settings on this screen:

Table 19: Partner Settings Option Descriptions

Option	Description
Name	You can edit the Partner name.
Domain	You can edit the Partner domain name.
Description	Enter a description. This field is optional.
Operator Support Access	This option is activated by default, indicating that Arista Support can view Partner level events. <div data-bbox="667 449 1508 541" style="border: 1px solid #0070C0; padding: 5px;"> Note: When deactivated, the Operator can no longer edit the settings of the selected Partner. Only the Partner can activate this setting from the Partner portal.</div>
Partner business contact information	Enter information of the primary person in charge of licensing, business reports, logistics, shipping, Edge auto-activation, etc.

4. Select Save Changes.

Manage Operators

In the Operator portal, you can configure and manage Operator Profiles and Operator Users. You can also view the events triggered by Operators.

12.1 Monitor Operator Events

Displays a list of events generated within the Orchestrator at the Operator level. These events help to determine the status of VeloCloud System.

To view the Operator events using the Orchestrator UI, select **Administration > Operator Events**.

Figure 12-1: Monitor Operator Events

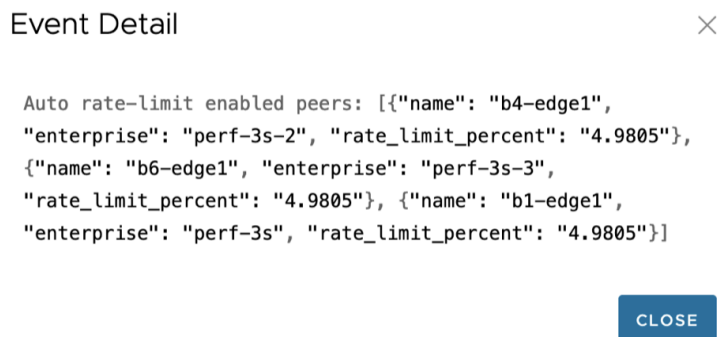
Event	User	Gateway	Severity	Time	Message
Auto Rate-Limit Disabled		gateway-1	Warning	Jan 25, 2023, 1:44:09 PM	Gateway auto rate-limit condition has been restored
Auto Rate-Limit Enabled		gateway-1	Warning	Jan 25, 2023, 1:34:19 PM	Gateway auto rate-limit has been enabled on 3 peers
Auto Rate-Limit Disabled		gateway-1	Warning	Jan 25, 2023, 1:33:38 PM	Gateway auto rate-limit condition has been restored
Auto Rate-Limit Enabled		gateway-1	Warning	Jan 25, 2023, 1:32:43 PM	Gateway auto rate-limit has been enabled on 3 peers
Auto Rate-Limit Enabled		gateway-1	Warning	Jan 25, 2023, 1:29:20 PM	Gateway auto rate-limit has been enabled on 2 peers
Auto Rate-Limit Enabled		gateway-1	Warning	Jan 25, 2023, 1:24:22 PM	Gateway auto rate-limit has been enabled on 3 peers

The **Events** page displays the recent Operator events. You can select the link to an event to view additional details about the selected event.

When the auto rate-limit capability is activated on a Gateways, the Gateway will drop packets if it detects that certain Edges are sending large amount of traffic which might be causing the Gateway to be unstable. The

event message includes the information about the list of Edges to which the Gateway is applying the auto rate limit and the rate limit percentage.

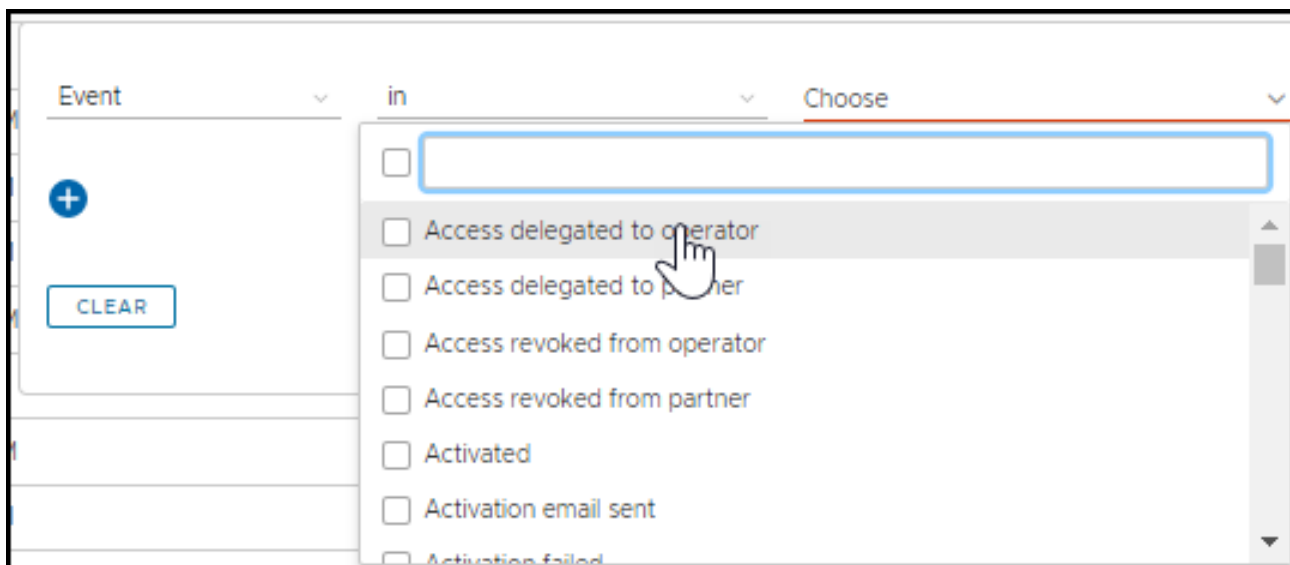
Figure 12-2: Event Detail



At the top of the page, you can choose a specific time period to view the details of events for the selected duration.

In the **Search** field, enter a term to search for specific details. Select the **Filter** icon to filter the view by a specific criteria. In the Filter, choose **Event**, and then select the drop-down arrow next to the field to view the list of Operator Events available and to filter by specific Events.

Figure 12-3: Search Event



Select the **CSV** option to download a report of the events in CSV format.



Note: For detailed information about alerts and events generated within the Orchestrator at the Operator level, see [Operator-Level Orchestrator Alerts and Events](#).

12.2 Manage Operator Profiles

An Operator Profile is used to specify the network settings managed by **Orchestrator**. After you create a Customer or Partner, you can assign an Operator profile to them.

Operators can upload, modify, or delete the following firmware and factory images in the Orchestrator UI:

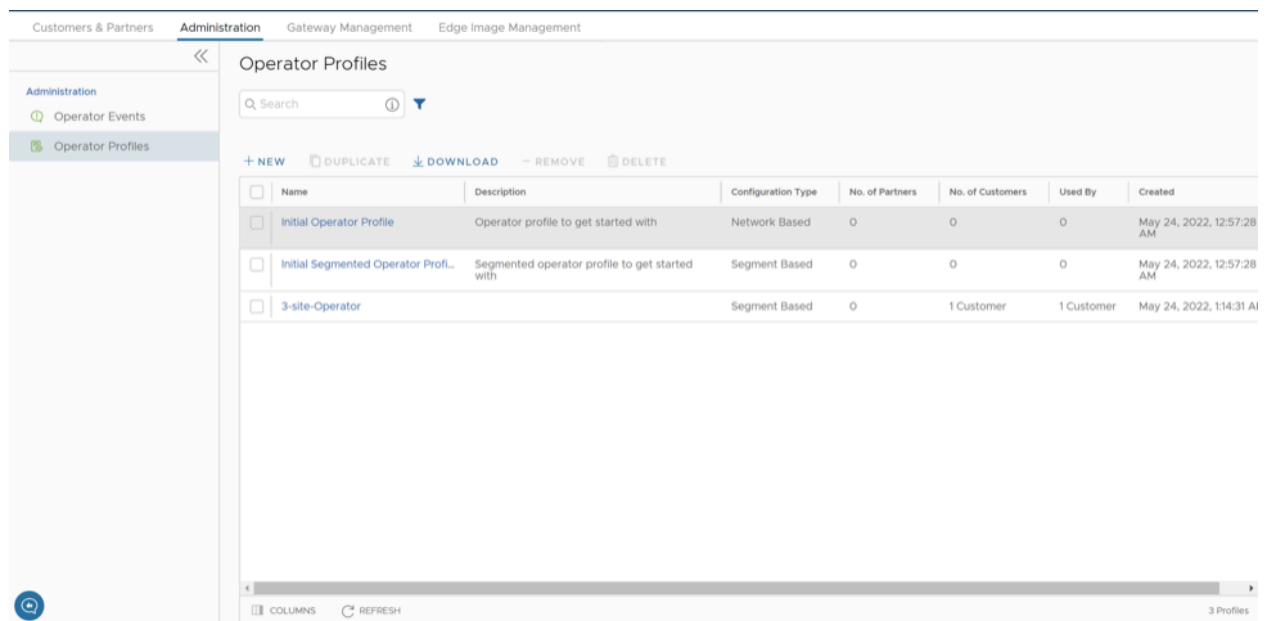
- Firmware Platform images for 6x0, 7x0, and 3x00 (3400/3800/3810) Edge device models
- Firmware Modem images for 510-LTE (Edge 510LTE-AE, Edge 510LTE-AP) and 610-LTE (Edge 610LTE-AM, Edge 61LTE-RW)
- Factory images for all physical VeloCloud Edge devices

With the 5.2 release, updating the Factory image and Platform firmware on High-availability (HA) Edges is supported. Steps and requirements are described in the appropriate sections in the procedure below.

See [Platform and Modem Firmware and Factory Images](#) for additional information.

1. In the **Operator** portal, from the top menu, select **Administration > Operator Profiles**. The **Operator Profiles** page displays the available profiles.

Figure 12-4: Operator Profiles



<input type="checkbox"/>	Name	Description	Configuration Type	No. of Partners	No. of Customers	Used By	Created
<input type="checkbox"/>	Initial Operator Profile	Operator profile to get started with	Network Based	0	0	0	May 24, 2022, 12:57:28 AM
<input type="checkbox"/>	Initial Segmented Operator Prof...	Segmented operator profile to get started with	Segment Based	0	0	0	May 24, 2022, 12:57:28 AM
<input type="checkbox"/>	3-site-Operator		Segment Based	0	1 Customer	1 Customer	May 24, 2022, 1:14:31 AM



Note: The Operator profiles that contain a deprecated image are flagged to notify the user that the software version of the profile contains a deprecated software image.

2. As an Operator user, you can perform the following actions on this page:

Table 20: Operator Profiles- Options and Descriptions

Option	Description
Search	Enter a search term to search for a matching text across the page. You can use the Advanced Search option to narrow down the search results.
New	Select this option to create a new Operator Profile. Enter the desired name and description in the dialog and select Create .
Duplicate	Select this option to create a copy of the selected Operator Profile. You can update the name and description.
Download	Select this option to download the csv file containing a list of all or the selected Operator Profiles.
Remove	Select this option to remove the selected Operator Profile(s) from all the associated Partners and Customers. You can complete this action only after you enter the correct number of profiles selected.
Delete	Select this option to delete the selected profile(s). You can complete this action only after you enter the correct number of profiles selected.
Columns	You can select the desired columns to be displayed in the table.
Refresh	Select this option to refresh the page.



Note: You cannot delete a profile that has already been assigned to a Customer or Partner.



Note: You cannot delete a profile that has already been assigned to a Customer or Partner.

- To update an existing Operator Profile, select the link to that Operator Profile name. The selected Operator Profile page appears, as shown in the image below.

Figure 12-5: Initial Operator Profile




The screenshot displays the configuration page for an Initial Operator Profile. The page is organized into several sections:

- Profile Settings:** Includes a 'Name' field with the value 'Initial Operator Profile' and a 'Description' field with the value 'Operator profile to get started with'. A note below the description states: 'If this profile is in a Partner's list of assigned profiles, this description will help them decide which to use for their Customers.'
- Management Settings:** A table of configuration parameters:

Orchestrator Address	IP Address	Heartbeat Interval (s) *	30
Orchestrator IPv4 Address	10.81.114.61	Time Slice Interval (s) *	300
Orchestrator IPv6 Address		Stats Upload Interval (s) *	300
- Gateway Selection:** Features a 'Gateway Mode' section with radio buttons for 'Dynamic' (selected) and 'Static'.
- Application Map Assignment:** Includes a 'JSON File' field with the value 'Initial Application Map Mon Oct 10 2022 06:38:03 G...'. Below this is a 'Software Version' section with a toggle switch set to 'Off'.
- Firmware Version:** A section with a blue informational box: 'Configure this section only when any specific firmware image updates are to be pushed to edges. This configuration is not required otherwise. Note: This selection is applicable only for edges version >= 5.0.0.0'. Below this are three rows, each with a toggle switch set to 'Off':
 - Modem Firmware
 - Platform Firmware
 - Factory Firmware

- You can configure the existing settings of the selected Profile. See table below.

Table 21: Initial Operator Profile- Options and Descriptions

Option	Description
Profile Settings	
Name	Edit the existing name of the Operator Profile.
Description	Edit the existing description of the Operator Profile.
Management Settings	
Orchestrator Address	Choose to use either FQDN or IP address as the Orchestrator Address. If you select FQDN, enter the FQDN address.
Orchestrator IPv4 Address	Enter the IPv4 address to be used as Orchestrator Address.
Orchestrator IPv6 Address	Enter the IPv6 address to be used as Orchestrator Address.
Heartbeat Interval (s)	Displays the time interval between the heartbeat messages sent from the Orchestrator to Edges. The default value is 30 seconds and minimum interval must be 10 seconds. If an Edge does not receive two heartbeats continuously, then the Edge is marked as Down.
	 Note: When you modify the heartbeat interval, make sure to update the Edge Offline Alert Notification Delay time accordingly, to avoid sending unnecessary alerts.
Time Slice Interval (s)	Displays the time interval over which the monitoring data is collected for a flow. The default value is 300 seconds.
Stats Upload Interval (s)	Displays the time interval for uploading the monitoring data. All the data for each Timeslice is collected during the Stats Upload Interval and then uploaded. The default value is 300 seconds.
Gateway Selection	
Gateway Mode	<p>By default, the Gateway selection is Dynamic and the VeloCloud Gateways are chosen dynamically from the Gateway Pool. Ensure that the Gateway Pool consists of at least two VeloCloud Gateways, for the Gateway selection to be efficient.</p> <p>Select the check box to make the Gateway selection as Static. For the Static Gateway selection, you must specify the Primary Gateway. You can also enter an optional Secondary Gateway.</p>
	 Note: Use the Static Gateway Selection only for testing or debugging purposes. You must not use this option for Edge-to- Edge VPN or Partner handoff configurations.
Application Map Assignment	
JSON File	By default, the initial Application Map is assigned to the Operator Profile. You can choose a different Application Map from the drop-down list. For additional information, see Application Maps .
Software Version: You can choose to push the latest Software Image to the Edges. By default, no updates are applied to the devices. Activate the toggle button to display the following fields.	
Version	Choose the Software Image from the drop-down list. For additional information on the Software Images, see Software Images .
Update Duration	Select the Update Duration check box, and then enter the duration time in minutes. When you activate this option, the Orchestrator updates all the devices associated with the Enterprise customer within the specified time duration.
Firmware Version	
	 Note: This section is available only for Edge versions 5.0.0 and above. This section is activated only when we deactivate the Software Version section.

The 5.1.0 release introduces the functionality for Operators to manage image upgrades for both Platform firmware, Modem firmware, and Factory Default images. (See table below for specific device requirements.

See the table below for device requirements and a description of both software types.

Table 22: Device Requirements

Software Type	Device Requirements	Components of the Edge that will be Updated
Modem Firmware	For the 5.1.0 release and later: 510-LTE (EDGE 510LTE-AE, EDGE510LTE-AP) and 610-LTE (EDGE610LTE-AM, EDGE61LTE-RW)	Carrier firmware and configuration files
Platform Firmware	For the 5.0.0 release, only Edge 6x0 devices are supported. For the 5.1.0 release, EDGE3400/ EDGE3800/ EDGE3810 models are also supported. Starting from the 5.2.4 release, Edge 7x0 devices are supported.	<ul style="list-style-type: none"> • BIOS (Basic Input/Output System) • CPLD (Complex Programmable Logic Device) • PIC (Programmable Intelligent Compute)
Factory Default (MR): Edge 500, Edge 5x0, Edge 6x0, Edge 7x0	For the 5.0.0 and later releases: all Edge devices.	Default factory image will be updated.

Note:

- It is important that you update the software version first. Then, after completion, update the firmware (Platform or Modem), and then update the factory default. Do not update the software version, the firmware, and the factory default at the same time. Also, only update one component at a time.



CAUTION: For the "Factory Image Update" feature, only use images that have been officially distributed as supported Factory Image versions. Do not use any other software update images with this feature. At any given time, Arista has an official **current** Factory Image version that is distributed from activate-sdwan.arista.com. Any other version (older or newer, supported or unsupported) that is installed as a **factory image** will be automatically updated to this version the next time the Edge is in an unactivated state and connected to the Internet.

- For releases prior to 5.0.0, the Operator Profile update will be a success, but the Firmware images will not be applied on the Orchestrator. No events will be generated, as the Orchestrator does not have a supported software version.
- For the 5.0.0 release and later, the Operator Profile update will be a success, and the Orchestrator will update the Firmware and Factory image components.

See the table below for a compatibility matrix of supported images for the supported Edge devices.

Table 23: Supported Images

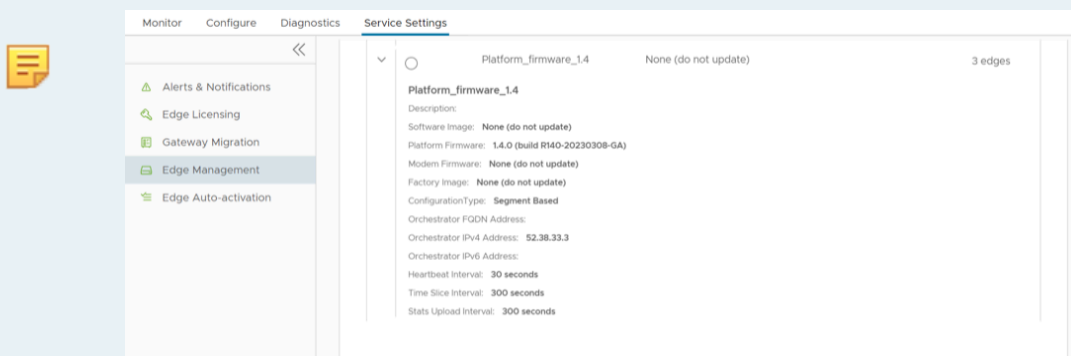
Device Family	Software Image (Device Family)	Platform Firmware (Device Family)	Modem Firmware (Device Family)	Factory Default (Device Family)
• EDGE 6x0	• EDGE 6X0	EDGE 6X0	610-LTE	• EDGE 6X0
EDGE 3x00	• EDGE 8X0 • EDGE 1000 • EDGE 3X00	Edge 3X00	NA	• EDGE 8X0 • EDGE 1000 • EDGE 3X00
510LTE	• Edge 510LTE-AE • Edge 510LTE-AP	NA	• Edge 510LTE-AE • Edge 510LTE-AP	Edge 5X0
610-LTE	• Edge 610LTE-AM • Edge 61LTE-RW	Edge 6X0	• Edge 610LTE-AM • Edge 61LTE-RW	Edge 6X0
EDGE 7x0 (EDGE 710-W, EDGE 710-5G, EDGE 720, EDGE 740)	EDGE 7x0	EDGE 7x0	EDGE 7x0	EDGE 7x0

The Operator can create multiple different profiles and select profiles with various combinations to manage different types of Firmware updates to be applied to Edges. See the notes below for additional information.

Note:

- Before an Operator can update and manage the Platform Firmware for 6X0 Edge devices and Factory Default images for all devices, the Edge and Orchestrator software version must first be updated to 5.0.0 or later.
- In the 5.0.0 release, the Operator Profile name will display as an image bundle (software and firmware) that lists the details of the Firmware images tagged in the Operator profile. (To view this setting, go to **Edge Management > Service Settings**). See image below.

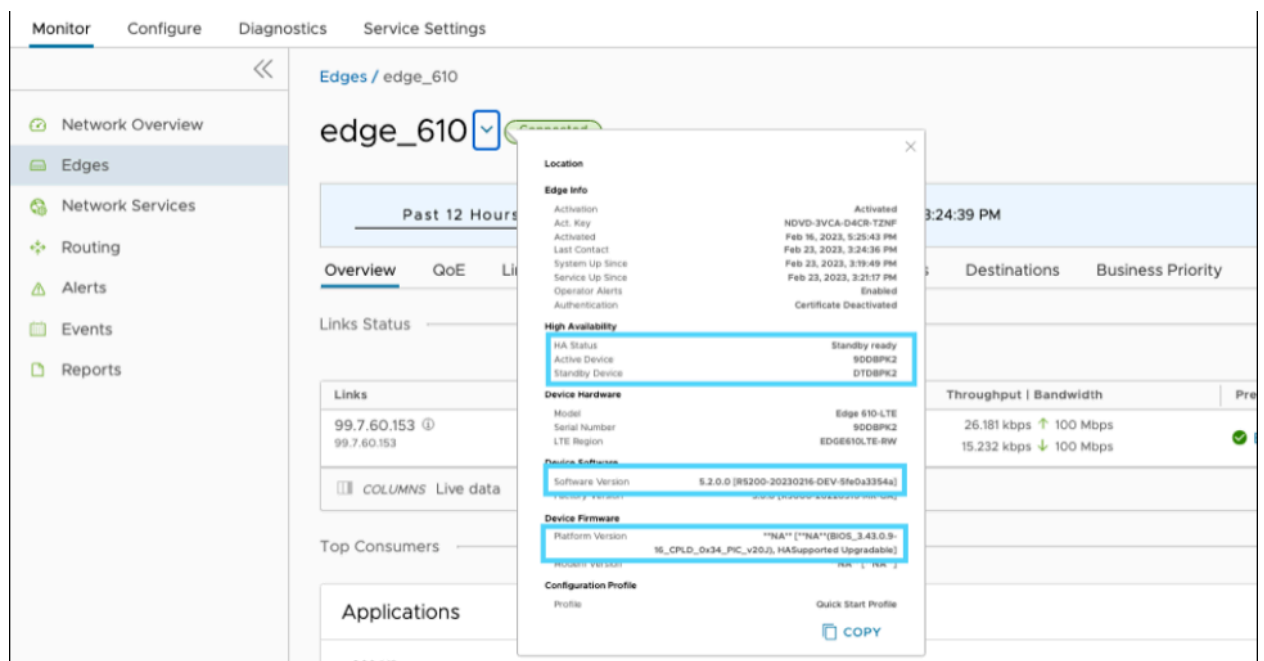
Figure 12-6: Service Settings



- All Factory and Firmware upgrades are limited to post activation.

- The 5.0.0 software image can be used to update the Factory default image on the Edge if the 5.0.0 or greater release image is uploaded from the “Software tab.” The software will be updated. If the image is uploaded from “Firmware tab,” the Factory Default image will be updated. Platform Firmware images can be uploaded only from the “Firmware tab.”
- The Platform Firmware upgrade takes at least 10 minutes to complete and includes multiple Edge reboots where the Edge will display as offline.
- For the 5.2 release, updating the Factory image and Platform firmware on HA (High-availability) Edges is supported. For updating Modem firmware on HA Edges, follow the steps below.
 - 1- The Edges must be unconfigured from HA.
 - 2- Apply the Modem firmware.
 - 3- Reconfigure to HA mode.

Figure 12-7: Edge Details



5. In the **Software Version** section, select the **Version** drop-down menu. Select the software image and select **Save Changes**. To update a Platform Firmware, a 5.0.0 or above software version for an Edge 6X0 or Edge 3X00 must be applied. To update Modem Firmware, a 5.0.0 or above software version for an Edge 510-LTE (Edge 510LTE-AE, Edge 510LTE-AP) or 610-LTE (Edge 610LTE-AM, Edge 61LTE-RW) must be applied.

Note:



- It is important that you update the software version first. Then, after completion, update the Factory image or Platform or Modem Firmware. Do not update the software version and the firmware at the same time.
- The **Version** drop-down menu displays the software images that are deprecated with a flag, but you will not be able to select the deprecated images.

For the selected profile, the usage information such as number of customers using the profile and software version used by the profile, appears at the left-hand bottom of the page.

If a Software Version 5.0.0 and above for an Edge 6X0 is selected from the Software Version drop-down menu, the **Firmware** section will be available for upgrade. If a software version lower than 5.0.0 is selected, or when a software image bundle for a Virtual Edge is selected, the Firmware section is grayed out.

6. Select **Save Changes**.
7. In the **Software Version** section, uncheck the Software Version check box and select **Save Changes**.
8. In the **Firmware** section, check the Platform Firmware and/or Factory Image check boxes in the appropriate sections and choose an image from the drop-down menu. See important note below.



Note: The **Firmware** image section can be configured for the software version 5.0.0 and greater and for 6X0 Edge devices.

9. Select **Reapply** to force re-update of the selected software image for the Edges associated with the selected Operator Profile.
10. Select **Save Changes**.

Related Links

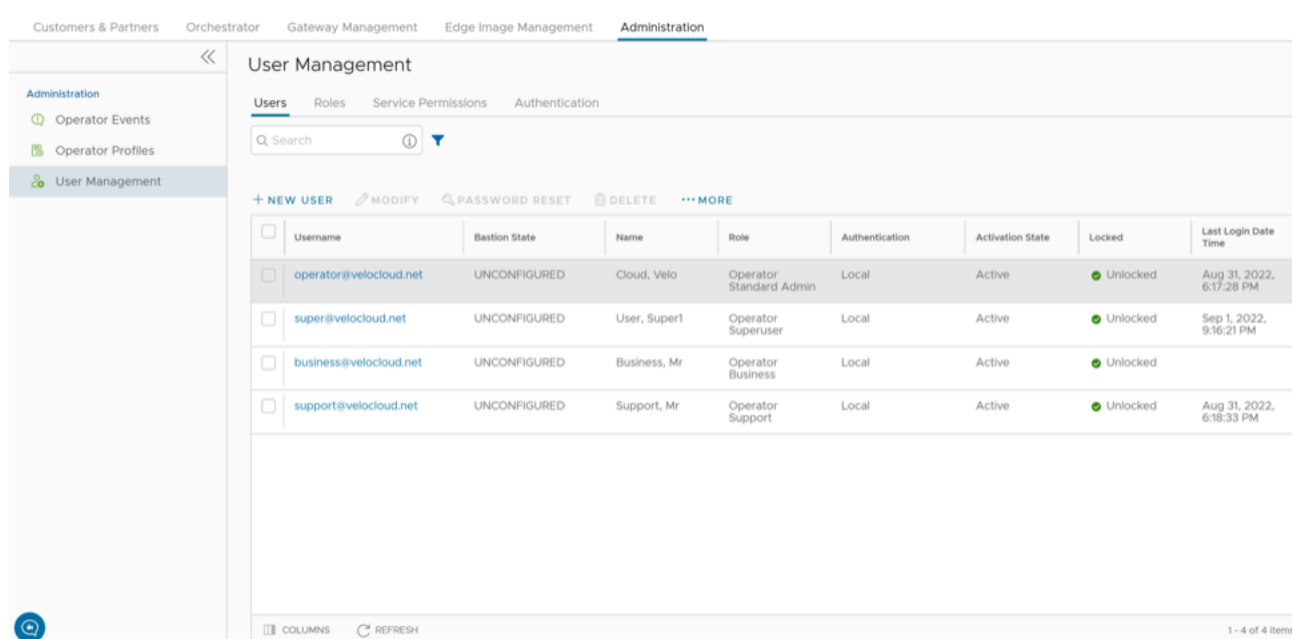
- To assign a profile for a new customer, see [Create New Customer](#).
- To change the profile for an existing customer, see [Configure Customers](#).
- To assign a profile for a partner, see [Manage Partners](#).

User Management Operator

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

As an Operator, you can access this feature from the Operator portal, by navigating to **Administration > User Management**. The following screen is displayed:

Figure 13-1: User Management- Operator



The screenshot shows the 'User Management' interface with the 'Users' tab selected. The interface includes a navigation menu on the left, a search bar, and a table of users. The table has columns for Username, Bastion State, Name, Role, Authentication, Activation State, Locked, and Last Login Date Time. There are four users listed in the table.

Username	Bastion State	Name	Role	Authentication	Activation State	Locked	Last Login Date Time
operator@velocloud.net	UNCONFIGURED	Cloud, Velo	Operator Standard Admin	Local	Active	Unlocked	Aug 31, 2022, 6:17:28 PM
super@velocloud.net	UNCONFIGURED	User, Superl	Operator Superuser	Local	Active	Unlocked	Sep 1, 2022, 9:16:21 PM
business@velocloud.net	UNCONFIGURED	Business, Mr	Operator Business	Local	Active	Unlocked	
support@velocloud.net	UNCONFIGURED	Support, Mr	Operator Support	Local	Active	Unlocked	Aug 31, 2022, 6:18:33 PM

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](#)

13.1 Users

As an Operator, you can view the list of existing users and their corresponding details. You can add, modify, or delete a user. However, you cannot modify or delete an Operator Super User. An Operator Super User can create new Operator users with different role privileges and configure API tokens for each Operator user.

To access the **Users** tab:

1. In the **Operator** portal, select **Administration** from the top menu.
2. From the left menu, select **User Management**.

The **Users** tab is displayed by default.

Figure 13-2: Users- Operator

Username	Bastion State	Name	Role	Authentication	Activation State	Locked	Last Login Date Time
operator@velocloud.net	UNCONFIGURED	Cloud, Velo	Operator Standard Admin	Local	Active	Unlocked	Aug 31, 2022, 6:17:28 PM
super@velocloud.net	UNCONFIGURED	User, Superl	Operator Superuser	Local	Active	Unlocked	Sep 1, 2022, 9:16:21 PM
business@velocloud.net	UNCONFIGURED	Business, Mr	Operator Business	Local	Active	Unlocked	
support@velocloud.net	UNCONFIGURED	Support, Mr	Operator Support	Local	Active	Unlocked	Aug 31, 2022, 6:18:33 PM

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

Table 24: Users Tab- Options and Descriptions

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

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

Table 25: Users Tab- 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.

13.1.1 Add New User

In the Operator portal, you can add new users and configure the user settings. Only Operator Super Users and Operator Standard Admins can add a new user. To add a new user, perform the following steps:

1. In the Operator portal, select **Administration** from the top menu.
2. From the left menu, select **User Management**. The **Users** tab is displayed by default.
3. Select **New User**. The following screen appears:

Figure 13-3: Add New User

The screenshot shows the 'Add New User' form in the Operator portal. The form is divided into three sections: 'General Information', 'Role', and 'Edge Access'.

General Information (User Name / Set Password / Contact Information):

- Authentication: Local, Remote
- Username: test@vmware.com
- Contact Email: test@vmware.com
- Password: [masked]
- Confirm Password: [masked]
- First Name: First Name
- Last Name: Last Name
- Phone: +1 [masked]
- Mobile Phone: +1 [masked]
- Next button

Role (Role defines the permissions this user has in services available):

Select the role that you want to assign to the user. A role is a combination of multiple privileges that are tagged to one or more services that you have licensed. In the Roles section, you can choose to create new roles or customize functional roles.

Role	Descriptions
<input type="radio"/> Operator Superuser	Can view, edit and create additional operators, global settings, and has full access across all services
<input type="radio"/> Operator Standard Admin	Can view and manage Operator customers' network and security services
<input type="radio"/> Operator Business	Can create and manage customer accounts
<input type="radio"/> Operator Support	Can monitor Edges and activity on the customers' network and security services

Columns: [icon] Refresh [icon] 1 - 4 of 4 items

Next button

3. Edge Access (SD-WAN Edge Access Privileges):


Access Level: Basic, Privileged


Add another user

Add User button, Cancel button

4. Enter the following details for the new user:

Table 26: Add New User- Options and Descriptions


Option	Description
General Information	Enter the required personal details of the user.
Role	Select a role that you want to assign to the user. For information on roles, see Roles .
Edge Access	<p>Ensure that you have Operator Super User role to modify the Access Level for the user. Choose one of the following options:</p> <ul style="list-style-type: none"> • Basic: Allows you to perform certain basic debug operations such as ping, tcpdump, PCAP, remote diagnostics, and so on. • Privileged: Grants you the root-level access to perform all basic debug operations along with Edge actions such as restart, deactivate, reboot, hard reset, and shutdown. In addition, you can access Linux shell. <p>The default value is Basic.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  Note: Only Operator Super Users can modify the default value to Privileged. </div>

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


5. Select the **Add another user** check box if you wish to create another user, and then select **Add User**. The new user appears in the **User Management > Users** page. Select the link to the user to view or modify the details.

13.1.2 API Tokens

You can access the Orchestrator APIs using tokens instead of session-based authentication. As an Operator 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.

By default, the API Tokens are activated. If you want to deactivate them, go to **System Properties** in the Operator portal, and set the value of the system property `session.options.enableApiTokenAuth` as **False**.

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

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

To manage the API tokens:

1. In the **Operator** portal, navigate to **Administration > User Management > Users**.

2. Select a user and select **Modify** or select the link to the username. Go to the **API Tokens** section.

Figure 13-4: API Tokens

<input type="checkbox"/>	UUID	Name	Description	Created	Expiration	State	Created By	Token Type	Customer	Created For
<input type="checkbox"/>	08655e51-a...	111		Aug 31, 2022, 8:11:30 PM	Aug 31, 2023, 8:11:30 PM	Enabled	super@velo...	Operator		super@velo...
<input type="checkbox"/>	e6313e59-d...	222		Aug 31, 2022, 8:13:55 PM	Aug 31, 2023, 8:13:56 PM	Enabled	super@velo...	Operator		super@velo...
<input type="checkbox"/>	67c4c354-6...	2323		Aug 31, 2022, 8:18:58 PM	Aug 31, 2023, 8:18:59 PM	Enabled	super@velo...	Operator		super@velo...
<input type="checkbox"/>	ba950228-9...	444		Aug 31, 2022, 8:24:28 PM	Aug 31, 2023, 8:24:28 PM	Enabled	super@velo...	Operator		super@velo...

3. Select **New API Token**.

Figure 13-5: New API Token


New Token [View documentation](#) ✕

Name *

Description

Lifetime * Months

4. In the **New Token** window, enter a **Name** and **Description** for the token, and then choose the **Lifetime** from the drop-down menu.
5. 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**.
6. To download the token, select the token, and then select **Download API Token**.
7. To deactivate a token, select the token, and then select **Revoke API Token**. The status of the token is displayed as **Revoked**.
8. Select **CSV** to download the complete list of API tokens in a .csv file format.
9. 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.

10. Similarly, you can configure additional properties and create API tokens for Partner Admins, Enterprise Customers, and Partner Customers. For additional information, see:

- 'Users' topic in the *Arista VeloCloud Global Settings Guide*

- 'Users' topic in the *Arista VeloCloud SD-WAN Partner Guide*

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

Table 27: API Tokens- 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.
Columns	Select the columns to be displayed or hidden on the page.
Refresh	Select to refresh the page to display the most current data.

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 } }'
```

13.2 Roles

The Orchestrator consists of two types of roles.



Note: Starting from the 5.1.0 release, **Functional Roles** are renamed as **Privileges**, and 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 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 an Operator user:

Table 28: Operator User Roles

Role	SD-WAN Service	Global Settings Service
Operator Standard Admin	SD-WAN Operator Admin	Global Settings Operator Admin
Operator Superuser	Full Access	Full Access
Operator Business	SD-WAN Operator Business	Global Settings Operator Business
Operator Support	SD-WAN Operator Support	Global Settings Operator Support

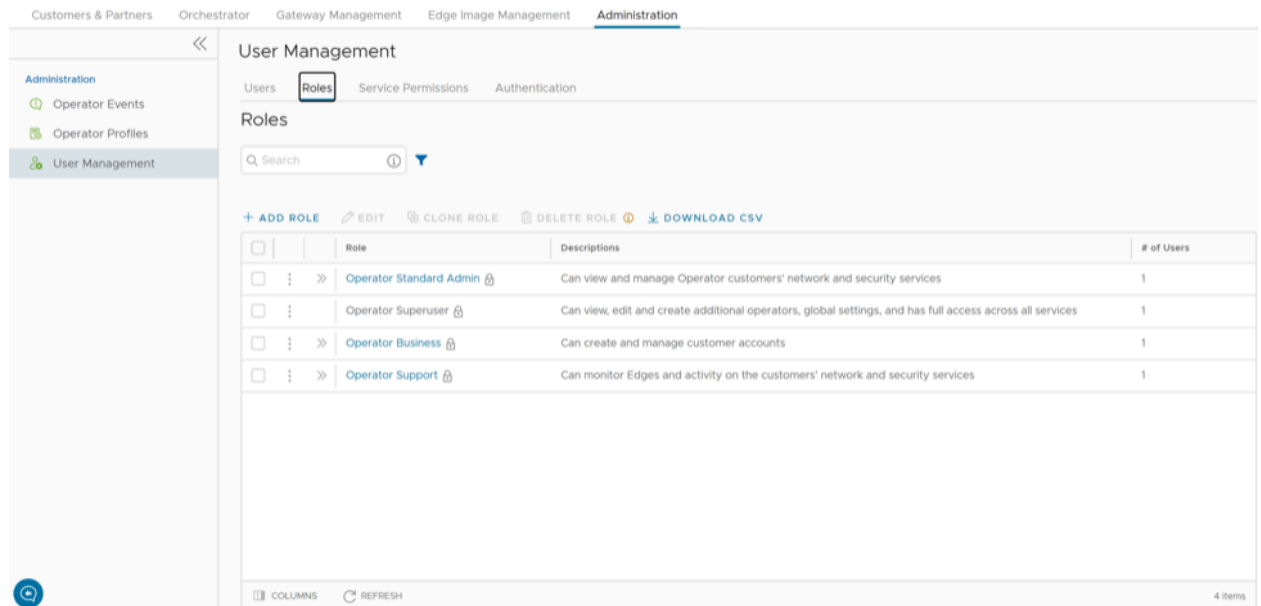
If required, you can customize the privileges of these roles. For additional information, see [Service Permissions](#).

As an Operator, 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 **Operator** portal, select **Administration** from the top menu.
2. From the left menu, select **User Management**, and then select the **Roles** tab. The following screen appears:

Figure 13-6: Roles- Operator



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

Table 29: Roles Tab- Options and Descriptions

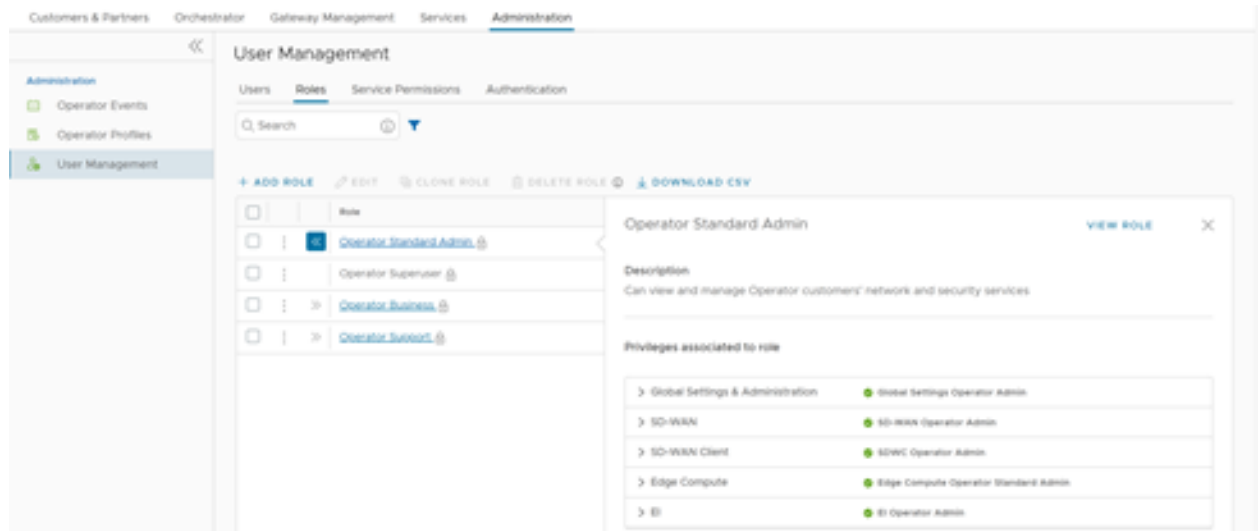
Option	Description
Add Role	Creates a new custom role. For additional information, see Add Role .
Edit	Allows you to edit only the custom roles. You cannot edit the default roles. Also, you cannot edit or view the settings of a Superuser.
Clone Role	Creates a new custom role, by cloning the existing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



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

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

Figure 13-7: Open Icon



5. Select the **View Role** link to view the privileges associated to the selected role for the following services:
 - Global Settings & Administration
 - SD-WAN
6. The following are the other options available in the **Roles** tab:

Table 30: Roles Tab- 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 and select the columns to be displayed or hidden on the page.
Refresh	Select to refresh the page to display the most current data.

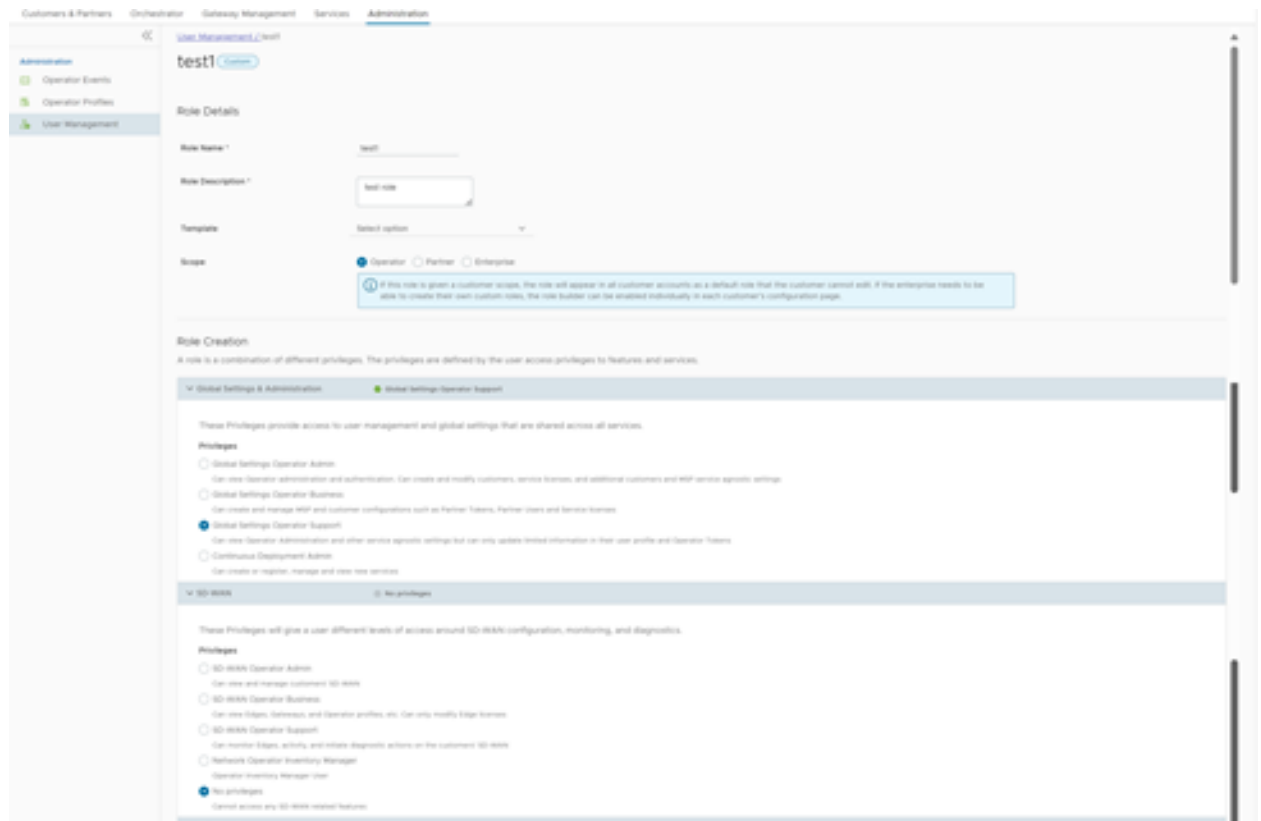
13.2.1 Add Role

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

1. In the **Operator** portal, select **Administration** from the top menu.
2. From the left menu, select **User Management**, and then select the **Roles** tab.

3. Select **Add Role**. The following screen appears:

Figure 13-8: Add Role



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

Table 31: Add Role- Options and Descriptions

Option	Description
Role Details	
Role Name	Enter a name for the new role.
Role Description	Enter a description for the role.
Template	Optionally, select an existing role as template from the drop-down list. The privileges of the selected template are assigned to the new role.
Scope	Select Operator , Partner , or Customer as the scope for the new role. The new role appears in all the accounts for the selected user, as a default role. If an Operator creates a role for a Partner, it appears in the Partner's roles' list and can be edited only by an Operator and a Partner user who has the required permissions.
Role Creation: The options in this section vary depending on the selected Scope .	
Global Settings & Administration	These privileges provide access to user management and global settings that are shared across all services. Choosing one of the privileges is mandatory. By default, Global Settings Operator Support is selected for the Operator scope.
SD-WAN	These privileges provide the Operator, Partner, or Enterprise Administrator with different levels of read and/or write access around SD-WAN configuration, monitoring, and diagnostics. You can optionally choose an SD-WAN privilege. The default value is No Privileges .

5. Select **Save Changes**.

The new custom role appears in the **User Management > Roles** page of the user, depending on the selected **Scope**. Select the link to the custom role to view the settings.

13.2.2 Enterprise Security Admin Role

Starting from the 6.1.0 release, customization of the Enterprise Security Admin role is enhanced to separate network and security actions. This customization allows you to configure only the Firewall settings at Profile and Edge level. All other SD-WAN configurations become read-only for an Enterprise Security Admin role.

The customization of the **Enterprise Security Admin** role can be achieved by creating the following two service permissions:

- SD-WAN Enterprise Security Admin
- Global Settings Enterprise Admin

You can either create these new permissions or directly upload these permissions using JSON files. Both these methods are explained below:

1. Create a Permission:

- In the **Operator** portal, select **Administration** from the top menu.
- From the left menu, select **User Management**, and then select the **Service Permissions** tab.
- Select **New Permission**. The following screen appears:

Figure 13-9: Enterprise Security Admin Role

The screenshot shows the 'Enterprise Security Admin' role configuration page. The 'Permission Details' section includes:

- Name:** Enterprise Security Admin
- Description:** Enter Description (Optional)
- Scope:** Enterprise (selected)
- Service:** SD-WAN
- Privilege Bundle:** SD-WAN Security Enterprise Admin

The 'Privileges' section contains a table with the following data:

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	On	On	On	On	On
Client Device	This privilege controls visibility to unique identifiers (IP or MAC address) of LAN-side client devices	On	Off	Off	Off	Off
Client User	This privilege controls visibility to potentially PII data in flow statistics	On	Off	Off	Off	Off
Cloud Security Service	Privilege controlling the creation and configuration of third party cloud security services to which traffic can be steered by business policy	On	On	On	On	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	On	On	On	On	On
Customer Alert Notification	Privilege granting the ability to view and manage customer alert configuration	On	Off	Off	Off	Off
Customer Edge Settings	Privilege granting the ability to activate or deactivate Configuration Updates for an Edge.	On	Off	On	Off	Off
Customer General Information	Privilege granting the ability to choose a default certificate for an Edge, and activate or deactivate Secure Edge Access.	On	Off	On	Off	Off
Customer Keys	Privilege granting the ability to view and manage enterprise security keys such as edge administrator credentials and IPSEC keys	On	Off	Off	Off	Off
Customer Privacy Settings	Privilege granting the ability to control access to sensitive Customer data.	On	Off	On	Off	Off

At the bottom of the page, there are buttons for 'CANCEL', 'SAVE', and 'SAVE AND APPLY'.

- Enter the following details to create a new permission:

Table 32: Enterprise Security Admin Role- Options and Descriptions

Option	Description
Name	Enter an appropriate name for the permission.
Description	Enter a description. This field is optional.
Scope	Select Enterprise as the scope.
Service	Select SD-WAN service to create the SD-WAN Enterprise Security Admin service permission. Select Global Settings service to create the Global Settings Enterprise Admin service permission.
Privilege Bundle	Select an appropriate privilege bundle from the drop-down menu. The privileges are populated depending on the selected Service .
Privileges	Displays the list of privileges based on the selected Privilege Bundle . You can edit only those privileges that are eligible for customization.



Note: Operator Superuser role is not available.

- e. Select **Download CSV** to download the list of all privileges, their description, and associated actions, into a file in CSV format.
- f. Select **Save** to save the new permission. Select **Save and Apply** to save and publish the permission. The new permission is displayed on the **Service Permissions** page.



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

2. Upload a Permission:

You can upload a service permission by navigating to **User Management > Service Permissions > More > Upload Permission**.

Below are the service permissions for **SD-WAN Enterprise Security** and **Global Settings Enterprise Admin** roles with the list of privileges:

SD-WAN Enterprise Security Admin

```
{ "roleCustomizations": [ { "forRoleId": 151, "addPrivileges": [ { "object": "EDGE_DEVICE_DEVICE_SETTINGS", "action": "UPDATE", "isDeny": 1 }, { "object": "EDGE_DEVICE_CLOUD_SECURITY_SERVICE", "action": "UPDATE", "isDeny": 1 }, { "object": "EDGE_DEVICE_GLOBAL_IPV6_SETTINGS", "action": "UPDATE", "isDeny": 1 }, { "object": "EDGE_DEVICE_L2_SETTINGS", "action": "UPDATE", "isDeny": 1 }, { "object": "EDGE_DEVICE_WIFI_SETTINGS", "action": "UPDATE", "isDeny": 1 }, { "object": "EDGE_DEVICE_CC_FIREWALL", "action": "UPDATE", "isDeny": 1 }, { "object": "EDGE_DEVICE_HIGH_AVAILABILITY", "action": "UPDATE", "isDeny": 1 }, { "object": "EDGE_DEVICE_CONFIG_VISIBILITY_MODE", "action": "UPDATE", "isDeny": 1 }, { "object": "EDGE_DEVICE_SNMP_SETTINGS", "action": "UPDATE", "isDeny": 1 }, { "object": "EDGE_DEVICE_SECURITY_VNF", "action": "UPDATE", "isDeny": 1 }, { "object": "EDGE_DEVICE_NTP_SETTINGS", "action": "UPDATE", "isDeny": 1 }, { "object": "EDGE_DEVICE_ANALYTICS_SETTINGS", "action": "UPDATE", "isDeny": 1 }, { "object": "PROFILE_DEVICE_DEVICE_SETTINGS", "action": "UPDATE", "isDeny": 1 }, { "object": "PROFILE_DEVICE_L2_SETTINGS", "action": "UPDATE", "isDeny": 1 }, { "object": "PROFILE_DEVICE_GLOBAL_IPV6_SETTINGS", "action": "UPDATE", "isDeny": 1 }, { "object": "PROFILE_DEVICE_WIFI_SETTINGS", "action": "UPDATE", "isDeny": 1 }, { "object": "PROFILE_DEVICE_CC_FIREWALL", "action": "UPDATE", "isDeny": 1 }, { "object": "PROFILE_DEVICE_CONFIG_VISIBILITY_MODE", "action": "UPDATE", "isDeny": 1 }, { "object": "PROFILE_DEVICE_NTP_SETTINGS", "action": "UPDATE", "isDeny": 1 }, { "object": "PROFILE_DEVICE_SNMP_SETTINGS", "action": "UPDATE", "isDeny": 1 }, { "object": "EDGE_OVERVIEW", "action": "UPDATE", "isDeny": 1 }, { "object": "PROFILE", "action": "CREATE", "isDeny": 1 }, { "object": "OVERLAY_FLOW_CONTROL",
```

```
"action": "UPDATE", "isDeny": 1 }, { "object": "EDGE_MANAGEMENT", "action": "UPDATE",
"isDeny": 1 }], "removePrivileges": [ ] } ] }
```

Global Settings Enterprise Admin

```
{ "roleCustomizations": [ { "forRoleId": 551, "addPrivileges": [ { "object": "SYSTEM_SETTI
NGS_GENERAL_INFO", "action": "UPDATE", "isDeny": 1 } ], "removePrivileges": [ ] } ],
"networkId": 1 }
```

For additional information, see [Service Permissions](#).

13.3 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 as **Service Permissions**.
- To activate this feature, an Operator must navigate to **Global Settings > Customer Configuration > Additional Configuration > Feature Access**, and then check the **Role Customization** check box.

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 the topic **Roles**.

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.



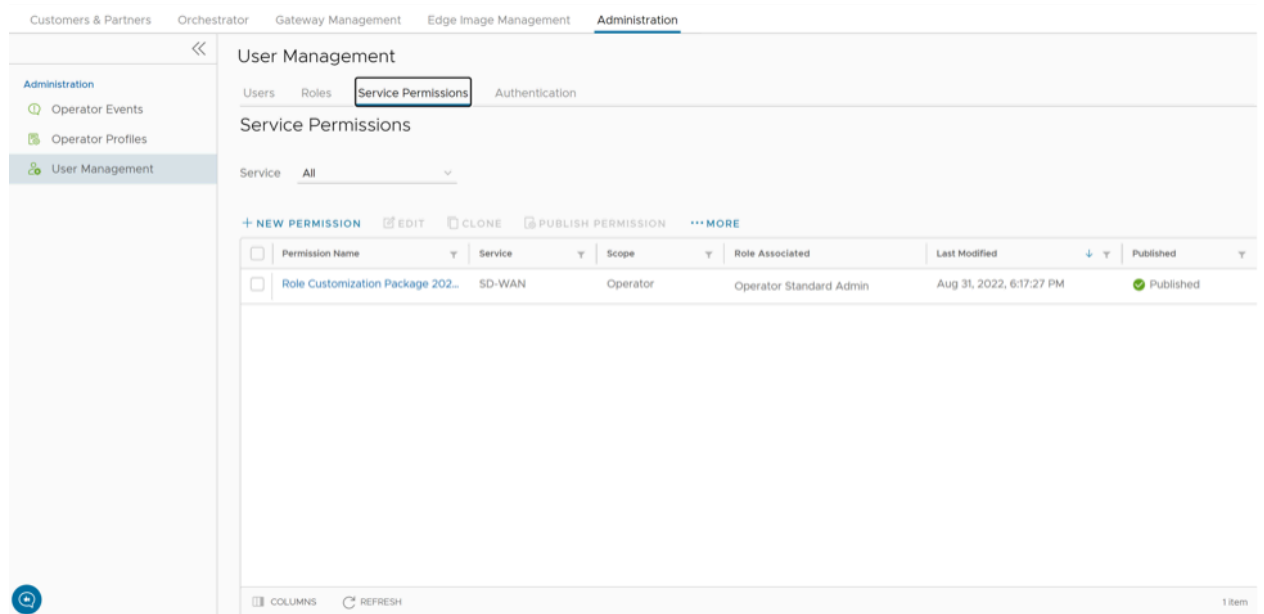
Note: For information on user privileges, see the topic **List of User Privileges**.

To access the **Service Permissions** tab:

- In the **Operator** Portal, select **Administration** from the top menu.


- From the left menu, select **User Management**, and then select the **Service Permissions** tab. The following screen appears:

Figure 13-10: Service Permissions- Operator




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

Table 33: 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"> • All • Global Settings • SD-WAN • Edge Compute <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 the topic New Permission .
Edit	Allows you to edit the settings of the selected permission. You can also select the link to the Permission Name to edit the settings.
Clone	Allows you to create a copy of the selected permission.
Publish Permission	Applies the customization available in the selected package to the existing permission. This option modifies the privileges only at the current level. If there are customizations available at the Operator level or a lower level for the same role, then the lower level takes precedence.
More	<p>Allows you to select from the following additional options:</p> <ul style="list-style-type: none"> • Delete: Deletes the selected permission. You cannot delete a permission if it is already in use. <div data-bbox="701 1001 1510 1146" style="border: 1px solid #0070C0; padding: 5px; margin: 5px 0;"> <p> Note: A permission can only be deleted if it is in a draft mode. The Delete option is deactivated for a published permission. If you want to delete a published permission, you must reset the permission to system default, which changes it to draft mode and activates the Delete option for the permission.</p> </div> <ul style="list-style-type: none"> • Download JSON: Downloads the list of permissions into a file in JSON format. • Upload Permission: Allows you to upload a JSON file of a customized permission. • Reset to System Default: Allows you to reset the current published permissions to default settings. Only the permissions applied to the privileges in the current level (Operator, Partner, or Enterprise) of the Orchestrator are reset to the default settings. If Operators or Customers have customized their privileges in the Partner or Enterprise level in the Orchestrator, those settings remain the same.

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

Table 34: Service Permissions- Additional Options and Descriptions

Option	Description
Columns	<p>Select the columns to be displayed or hidden on the page.</p> <div data-bbox="665 1682 1510 1759" style="border: 1px solid #0070C0; padding: 5px; margin: 5px 0;"> <p> Note: The Role Associated column displays the Roles using the same Privilege Bundle.</p> </div>
Refresh	Select to refresh the page to display the most current data.



Note: 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.

13.3.1 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 **Operator** portal, select **Administration** from the top menu.
2. From the left menu, select **User Management**, and then select the **Service Permissions** tab.

3. Select **New Permission**. The following screen appears:

Figure 13-11: New Permission

Service Permissions / test

test

Permission Details

Name *

Description

Scope * Operator Partner Enterprise

Service *

Privilege Bundle *

[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	
Bastion VCO	This privilege controls access to Bastion VCO configuration and monitoring information	<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 Alert	Privilege granting the ability to view and manage customer alert configuration and generated alerts	<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 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 Keys	Privilege granting the ability to view and manage enterprise security keys such as edge administrator credentials and IPSEC keys	<input checked="" type="checkbox"/> On	<input checked="" type="checkbox"/> On	<input checked="" type="checkbox"/> On	<input checked="" type="checkbox"/> On	
Customer PKI	Privilege granting the ability to view and manage enterprise PKI settings	<input checked="" type="checkbox"/> On	<input type="checkbox"/> Off	<input type="checkbox"/> Off	<input type="checkbox"/> Off	
Customer Profile	Privilege granting the ability to view and edit enterprise configuration profiles	<input checked="" type="checkbox"/> On	<input checked="" type="checkbox"/> On	<input checked="" type="checkbox"/> On	<input checked="" type="checkbox"/> On	

Objects per page 172 Items / 18

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

Table 35: New Permission- Options and Descriptions

Option	Description
Name	Enter an appropriate name for the permission.
Description	Enter a description. This field is optional.
Scope	Select Operator , Partner , or Enterprise as the scope. An Operator can apply the permissions for Operators, Partners, and Customers.
Service	Select a service from the drop-down menu. The available services are: <ul style="list-style-type: none">• Global Settings• SD-WAN
Privilege Bundle	Select a privilege bundle from the drop-down menu. The privileges are populated depending on the selected Service .
Privileges	Displays the list of privileges based on the selected Privilege Bundle . You can edit only those privileges that are eligible for customization.



Note: Operator Superuser role cannot be customized.

5. Select **Download CSV** to download the list of all privileges, their description, and associated actions, into a file in CSV format.
6. 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.

13.3.2 List of User Privileges

This section discusses all the privileges available in the Operator **portal**.

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?

Table 36: List of User Privileges

Feature	Name of the Privilege	Description	Allow Privilege	Deny Privilege	Customizable
Manage Customers	Create Customer	Grants ability to view and manage Enterprise Customers as an Operator or a Partner	Yes	No	No
	Read Customer				
	Update Customer				
	Delete Customer				
	Manage Customer				
Manage Partners	Create Partner	Grants ability to view and manage Partners	Yes	No	No
	Read Partner				
	Update Partner				
	Delete Partner				
	Manage Partner				
Software Images	Create Software Package	Grants access to upload and assign Edge Software Images and Application Maps	Yes	Yes	Yes
	Read Software Package				
	Update Software Package				
	Delete Software Package				
	Manage Software Package				
System Properties	Create System Property	Grants access to view and manage System Properties	Yes	Yes	No
	Read System Property				
	Update System Property				
	Delete System Property				
	Manage System Property				
	Edit Restricted System Properties	Controls the ability of user to edit restricted system properties	Yes	No	No
Operator Events	Create Operator Event	Grants ability to view Operator events	Yes	Yes	Yes
	Read Operator Event				
	Update Operator Event				
	Delete Operator Event				
	Manage Operator Event				
Operator Profiles	Create Operator Profile	Grants ability to view and manage Operator profiles	Yes	Yes	Yes
	Read Operator Profile				
	Update Operator Profile				
	Delete Operator Profile				
	Manage Operator Profile				
	View Tab Operator Profile	Controls ability of the user to view and configure within the Operator profile menu	No	Yes	Yes
Operator Users	Create Operator User	Grants ability to view and manage Operator administrative users	Yes	Yes	No
	Read Operator User				
	Update Operator User				
	Delete Operator User				
	Manage Operator User				
Operator Users > API Tokens	Create Operator Token	Grants ability to view and manage the operator Authentication Tokens	Yes	No	No
	Read Operator Token				
	Update Operator Token				

Feature	Name of the Privilege	Description	Allow Privilege	Deny Privilege	Customizable
	Delete Operator Token				
	Manage Operator Token				
Gateway Pools Gateways Gateway Diagnostic bundles	Create Gateway	Grants ability to view and manage Gateway pools and Gateways as an Operator or a Partner	Yes	Yes	Yes
	Read Gateway				
	Update Gateway				
	Delete Gateway				
	Manage Gateway				
	View Tab Gateway List	Controls the ability of user to view the list of Gateways	No	Yes	Yes
Gateways > New Gateway	Create Operator PKI	Grants ability to view and manage Operator level PKI configuration including Gateway certificates and certificate authority	Yes	Yes	No
Gateway > Gateway Authentication Mode	Read Operator PKI				Yes
	Update Operator PKI				No
	Manage Operator PKI				Yes
Gateway Diagnostic Bundles > Download Diagnostic Bundles	Download Gateway Diagnostics	Grants ability to download Gateway Diagnostics	No	Yes	Yes
Application Maps	Create Software Package	Grants access to upload and assign Edge software images and Application Maps	Yes	Yes	Yes
	Read Software Package				
	Update Software Package				
	Delete Software Package				
	Manage Software Package				
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				
CA Summary > Gateway Certificates > Revoke Certificate	Read Operator PKI	Grants ability to view and manage operator level PKI configuration including Gateway certificates and certificate authority	Yes	Yes	Yes
	Delete Operator PKI				No
	Manage Operator PKI				Yes
	Read Customer PKI	Grants ability to view and manage Enterprise PKI settings	Yes	No	No
	Delete Customer PKI				
	Manage Customer PKI				
Orchestrator Authentication > Operator Authentication	Create Operator Authentication	Grants ability to view and manage Operator authentication mode, like SSO, RADIUS, or Native	Yes	Yes	Yes
	Read Operator Authentication				

Feature	Name of the Privilege	Description	Allow Privilege	Deny Privilege	Customizable
Orchestrator Authentication > Enterprise Authentication	Update Operator Authentication				
	Delete Operator Authentication				
	Manage Operator Authentication				
	Create Customer Authentication	Grants ability to view and manage Customer authentication mode, like RADIUS or Native	Yes	Yes	Yes
	Read Customer Authentication				
	Update Customer Authentication				
	Delete Customer Authentication				
Replication	Manage Customer Authentication				
	Create Replication	Grants access to view and configure Orchestrator disaster recovery	Yes	Yes	No
	Read Replication				Yes
	Update Replication				No
	Delete Replication				
Orchestrator Diagnostics > Diagnostic Bundles	Manage Replication				Yes
	Create Orchestrator Diagnostics	Grants access to request and view Orchestrator diagnostic bundles	Yes	Yes	Yes
	Read Orchestrator Diagnostics				
	Update Orchestrator Diagnostics				
	Delete Orchestrator Diagnostics				
Orchestrator Diagnostics > Database Statistics	Manage Orchestrator Diagnostics				
	Create Software Package	Grants access to upload and assign Edge software images and Application Maps	Yes	Yes	Yes
	Read Software Package				
	Update Software Package				
	Delete Software Package				
Orchestrator Upgrade for Standalone	Manage Software Package				
	Create Replication	Grants access to view and configure Orchestrator disaster recovery	Yes	Yes	No
	Read Replication				Yes
	Update Replication				No
	Delete Replication				
Orchestrator Upgrade for DR Setup	Manage Replication				Yes
	Create User Agreement	Grants access to configure the customer user agreement	Yes	No	No
	Read User Agreement				
	Update User Agreement				
	Delete User Agreement				
User Agreements	Manage User Agreement				

Feature	Name of the Privilege	Description	Allow Privilege	Deny Privilege	Customizable
Orchestrator Owners Manage Orchestrators Edge Inventory	Create Edge Inventory	Grants ability to view and manage Edge inventory as needed for Redirect configuration	Yes	No	No
	Read Edge Inventory				
	Update Edge Inventory				
	Delete Edge Inventory				
	Manage Edge Inventory				

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 37: List of Customizable Privileges

Navigation Path in the Enterprise Portal	Name of the Tab	Name of the Privilege	Description
Configure > Edges > Select Edge	Overview	Assign Edge Profile	Grants ability to assign a Profile to Edges
Configure > Edges > Select Edge	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 PCI	Enforce PCI Compliance	Deny PCI Operations	Denies access to sensitive Customer data including PCAPs, etc. on the Edges and Gateways, for all users including Arista Support
Diagnostics > Diagnostic Bundles	Select Edge > Download Bundle	Download Edge Diagnostics	Grants ability to download Edge Diagnostics
Gateway Management > Diagnostic Bundles	Select Gateway > Download Bundle	Download Gateway Diagnostics	Grants ability to download Gateway Diagnostics
Configure > Profiles	Duplicate	Duplicate Customer Profile	Grants ability to edit duplicate customer level Profiles
Configure > Segments / Configure > Profiles > Configure > Edges	Segments drop-down menu	Edit Tab Segments	Grants ability to edit within the Segments tab
Configure > Edges > Select Edge	Device	Enable HA Cluster	Grants ability to configure HA Clustering
Configure > Edges > Select Edge	Device	Enable HA Active/Standby Pair	Grants ability to configure active/standby HA
Configure > Edges > Select Edge	Device	Enable HA VRRP Pair	Grants ability to configure VRRP HA
Diagnostics > Remote Diagnostics	Clear ARP Cache	Remote Clear ARP Cache	Grants ability to clear the ARP cache for a given interface
Diagnostics > Remote Diagnostics > Gateway	Cloud Traffic Routing (drop-down menu)	Remote Cloud Traffic Routing	Grants ability to route cloud traffic remotely
Diagnostics > Remote Diagnostics	DNS/DHCP Service Restart	Remote DNS/DHCP Restart	Grants ability to restart the DNS/DHCP service
Diagnostics > Remote Diagnostics	Flush Flows	Remote Flush Flows	Grants ability to flush the Flow table, causing user traffic to be re-classified
Diagnostics > Remote Diagnostics	Flush NAT	Remote Flush NAT	Grants ability to flush the NAT table
Diagnostics > Remote Diagnostics > LTE SIM Switchover	LTE Switch SIM Slot	Remote LTE Switch SIM Slot	Grants ability to activate the SIM Switchover feature. After the test is successful, you can check the status from Monitor > Edges > Overview tab
	 Note: This is for 610-LTE and 710 5G devices only.		
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
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

Navigation Path in the Enterprise Portal	Name of the Tab	Name of the Privilege	Description
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

13.4 Authentication

The Authentication feature allows you to set the authentication modes for both, Operators and Enterprise users. You can also view the existing API tokens.

To access the **Authentication** tab:

1. In the **Operator** portal, select **Administration** from the top menu.

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

Figure 13-12: Authentication- Operator

The screenshot displays the 'User Management' interface with the 'Authentication' tab selected. The left sidebar shows the navigation menu with 'User Management' highlighted. The main content area is divided into several sections:

- API Tokens:** A table listing issued tokens. The table has columns for Uuid, Name, Description, Created, Expiration, and State. There are 9 items listed.
- Operator Authentication:** A section with a dropdown menu for 'Authentication Mode' set to 'Local'. Below it, a note states 'No configuration is required for native orchestrator access identity provider mode.' and an 'UPDATE' button.
- Enterprise Authentication:** A section with a dropdown menu for 'Authentication Mode' set to 'Local'. Below it, a note states 'No configuration is required for native orchestrator access identity provider mode.' and a blue box with text: 'Specific authentication configurations can be overridden inside the enterprise under global settings in the user access management page.' and an 'UPDATE' button.
- SSH Keys:** A section with a 'REVOKE' button and a table of SSH keys. The table has columns for Ssh UserName, Duration, and Access Level. There is 1 item listed.
- Session Limits:** A section with a description: 'Session limits enforces restrictions on the number of users with the same role that can be logged in to the Orchestrator at the same time. This limit does not apply to the API users. The default option is Unlimited.' It includes a 'Concurrent logins' section with a radio button for 'Unlimited' selected and a 'Session limits for each role' table.

Role	Session Limit
Operator Supervisor	Unlimited
Operator Standard Admin	Unlimited
Operator Business	Unlimited
Operator Support	Unlimited

API Tokens

You can access the Orchestrator APIs using token-based authentication, irrespective of the authentication mode. Operator Administrators with right permissions can view the API tokens issued to Orchestrator users, including tokens issued to the Partner and Customer users. If required, an Operator Administrator can revoke the API tokens.

By default, the API Tokens are activated. If you want to deactivate them, go to **Orchestrator > System Properties**, and set the value of the system property `session.options.enableApiTokenAuth` as **False**.



Note: An Operator Super User 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 38: API Tokens- 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.

As an Operator Super User, you can manage the API tokens for Enterprise users. For information on creating and downloading API tokens, see [API Tokens](#).

Operator Authentication / 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:** Operator users with Superuser permission can set up and configure Single Sign On (SSO) in Orchestrator. 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 the Orchestrator to authenticate users from an OpenID Connect (OIDC)-based Identity Providers (IdPs).



Note:

Beginning in Release 6.1.0, the Orchestrator is capable of having multiple IdPs configured so that a Partner on their Dedicated Orchestrator can configure an IdP independently of the VeloCloud SD-WAN TechOPS team. As a result the Partner with Operator level access can log into their Dedicated Orchestrator with an integrated Single Sign-On service.

Pre-requisites:

- Ensure that you have the Operator Superuser permission.
- Before setting up the SSO authentication in Orchestrator, make sure that you have set up Users, Service Permissions, and OpenID connect (OIDC) application for Orchestrator in your preferred identity provider's website.



Note:

- **Single Sign-On** mode is available only for **Operator Authentication** in the Operator portal.
- Token-based authentication is deactivated for SSO users.

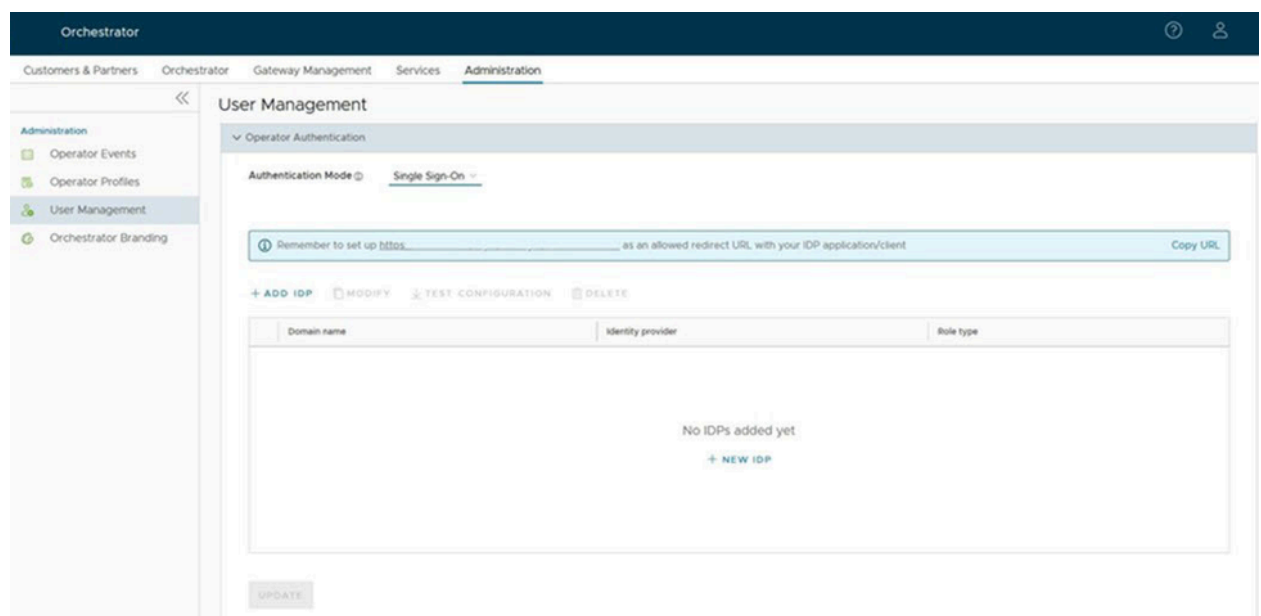
To enable Single Sign On (SSO) for Orchestrator, you must enter the Orchestrator application details into the Identity Provider (IdP). Select each of the following links for step-by-step instructions to configure the following supported IdPs:

- [Configure Azure Active Directory for Single Sign On](#)
- [Configure Okta for Single Sign On](#)
- [Configure OneLogin for Single Sign On](#)
- [Configure PingIdentity for Single Sign On](#)

The Operator Authentication Screen for Single Sign-On with Optional Multiple IdPs

With the new Multiple IdP feature in Release 6.1.0 the Single Sign-On screen changes from displaying one configuration screen for one Single Sign On account to displaying a table where multiple IdPs can be configured and tracked.

Figure 13-13: Single Sign-On Authentication Mode



With this new format, a Superuser Operator must select **+ NEW IDP** to add an IdP. Only then will the **Single Sign-On Setup** screen appear for configuring that particular IdP.

The workflow for configuring a Single Sign-On changes slightly with a user seeing two screens.

Single Sign-On Setup Screen

Figure 13-14: Single Sign-On Setup

Setup IDP

1 Single Sign-On Setup

2 Role Setup

Single Sign-On Setup

Domain Name: Test

Identity Provider Template: Okta

OIDC well-known config URL: https://.well-known/openid-config

Issuer: https://.okta.com

Authorization Endpoint: https://.okta.com/authorize

Token Endpoint: https://.okta.com/token

JSON Web KeySet URI: https://.okta.com/keys

User Information Endpoint: https://.okta.com/userinfo

Client ID: 12o4n

Client Secret: *****

CANCEL NEXT

Once you are on the **Single Sign-On Setup** screen, you can configure the following options when you select the **Authentication Mode** as **Single Sign-on**.

Table 39: Single Sign-on- 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.
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.

Once the **Single Sign-On Setup** is complete, the Operator needs to configure the **Role Setup** section.

Figure 13-15: Role Setup - Use Default Role

The screenshot shows the 'Role Setup' configuration page. On the left, a sidebar titled 'Setup IDP' has two items: '1 Single Sign-On Setup' and '2 Role Setup', with '2 Role Setup' selected. The main content area is titled 'Role Setup' and contains the following options:

- Role Setup**
- Role Type**: Two radio buttons are present. The first, 'Use default role', is selected with a blue dot. The second, 'Use identity provider roles', is unselected.
- Allow Super User**: A checkbox that is checked.
- Default Role**: A text input field containing the value 'Operator Standard Admin'.

At the bottom right of the form, there are three buttons: 'CANCEL', 'BACK', and 'DONE'.

Figure 13-16: Role Setup - Use Identity Provider Roles (Default)

The screenshot shows the 'Role Setup' configuration page with 'Use identity provider roles' selected. The sidebar and 'Role Setup' title are the same as in Figure 13-15. The options are:

- Role Setup**
- Role Type**: Two radio buttons are present. The first, 'Use default role', is unselected. The second, 'Use identity provider roles', is selected with a blue dot.
- Allow Super User**: A checkbox that is checked.
- Role Attribute**: A text input field containing the value 'groups'.
- Operator Role Map**: A table with two columns: 'Orchestrator Role Name' and 'Identity Provider Role Name'. It contains four rows of data, each with an edit icon on the right.

Orchestrator Role Name	Identity Provider Role Name
Operator Superuser	
Operator Standard Admin	
Operator Business	
Operator Support	

At the bottom right of the form, there are three buttons: 'CANCEL', 'BACK', and 'DONE'.

Once you are on the **Role Setup** screen, you can configure the following options.

Table 40: Role Setup - Options and Descriptions

Role Type	Select one of the following two options: <ul style="list-style-type: none"> Use default role Use identity provider roles
Allow Super User	This option is for the Partner adding a second IdP. Uncheck this option as a Partner cannot have a Superuser role on a Dedicated Orchestrator managed by Arista VeloCloud. In addition, remove the Super User role on the Use identity provider roles screen.
Role Attribute	Enter the name of the attribute set in the IdP to return roles.
Operator Role Map	Map the IdP-provided roles to each of the Operator user roles.



CAUTION: If configuring a second IdP for a Partner on an Orchestrator hosted by VeloCloud (Dedicated Orchestrator) the configuration must not include an Operator Superuser role.

Role Setup for a Partner-added second IdP where the **Allow Super User** check box is unchecked. This screen also shows that if you enter Operator Superuser as a default role, the UI will throw an error when that box is unchecked. The Default Role should be Operator Standard Admin for Partner Operator users.

Figure 13-17: Allow Super User

Setup IDP

- 1 Single Sign-On Setup
- 2 Role Setup

Role Setup

Role Type

Use default role

Use identity provider roles

Allow Super User

Default Role

Operator Superuser ❗

Invalid

CANCEL BACK DONE

Role Setup for a Partner-added second IdP where the Operator Superuser role must be removed.

Figure 13-18: Role Setup

Setup IDP

- 1 Single Sign-On Setup
- 2 Role Setup

Role Setup

Role Type

Use default role

Use identity provider roles

Allow Super User

Role Attribute ⓘ

groups

Operator Role Map ⓘ

Orchestrator Role Name	Identity Provider Role Name
Operator Superuser	
Operator Standard Admin	
Operator Business	
Operator Support	

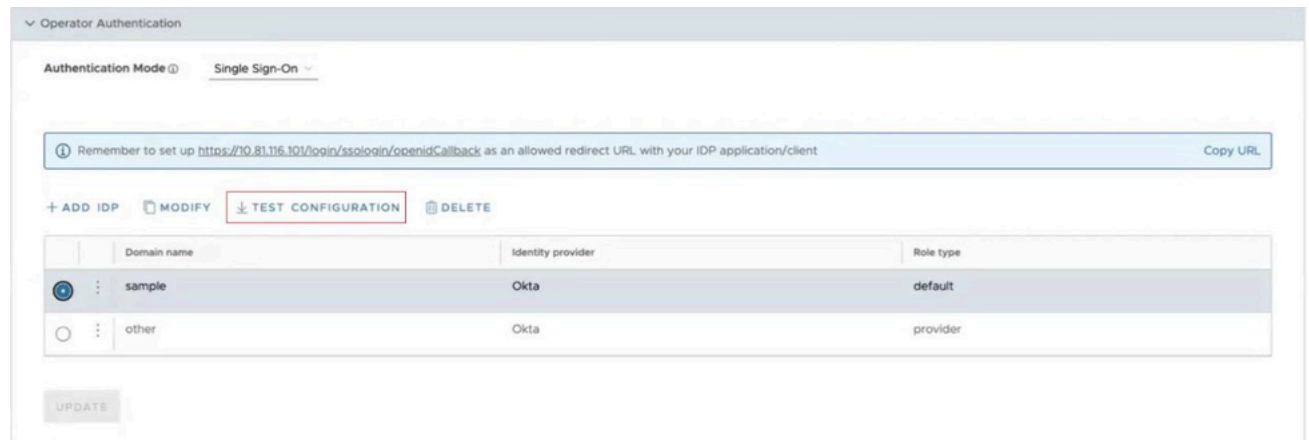
4 items

CANCEL BACK DONE

The Operator user can also test the configuration for a particular Single Sign-On/IdP configuration.

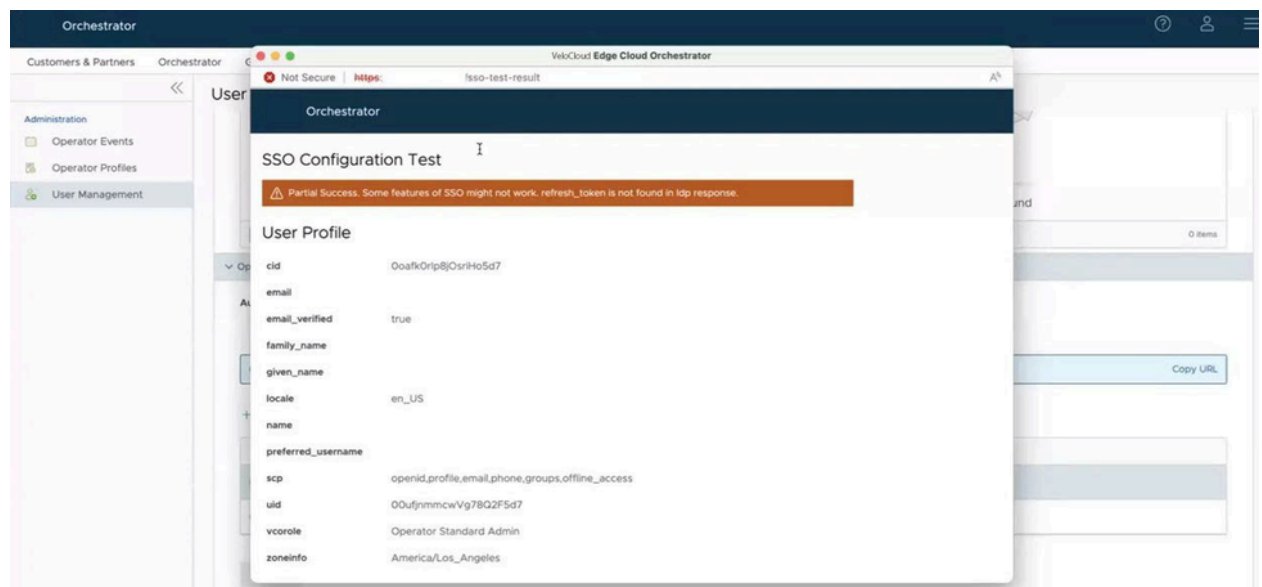
Test Configuration option for an SSO/IdP. Selecting on it runs the test.

Figure 13-19: Test Configuration



Successful SSO Configuration Test. The "Partial Success" message only indicates this configuration does not have a refresh token configured. It is still a valid configuration.

Figure 13-20: SSO Configuration Test

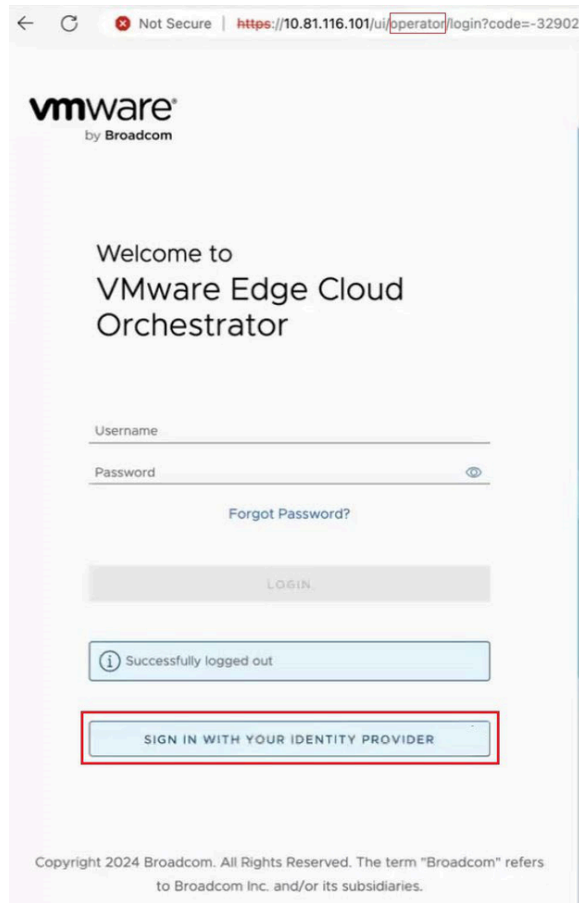


Logging in as a Partner with an Operator Role using your own IdP

A partner with an IdP configured can login to their Orchestrator by pulling up a browser and entering in the usual URL except they would add /operator to that URL. This pulls up the Operator login screen and includes a button **SIGN IN WITH YOUR IDENTITY PROVIDER**. On an Orchestrator with just one SSO IdP configured, selecting that button will log them in assuming the Operator user has the proper IdP credentials.

The Operator login screen. This screen will have '/operator' in the URL and include the 'Sign In With Your Identity Provider' button. Select on this button to move on to the SSO screen.

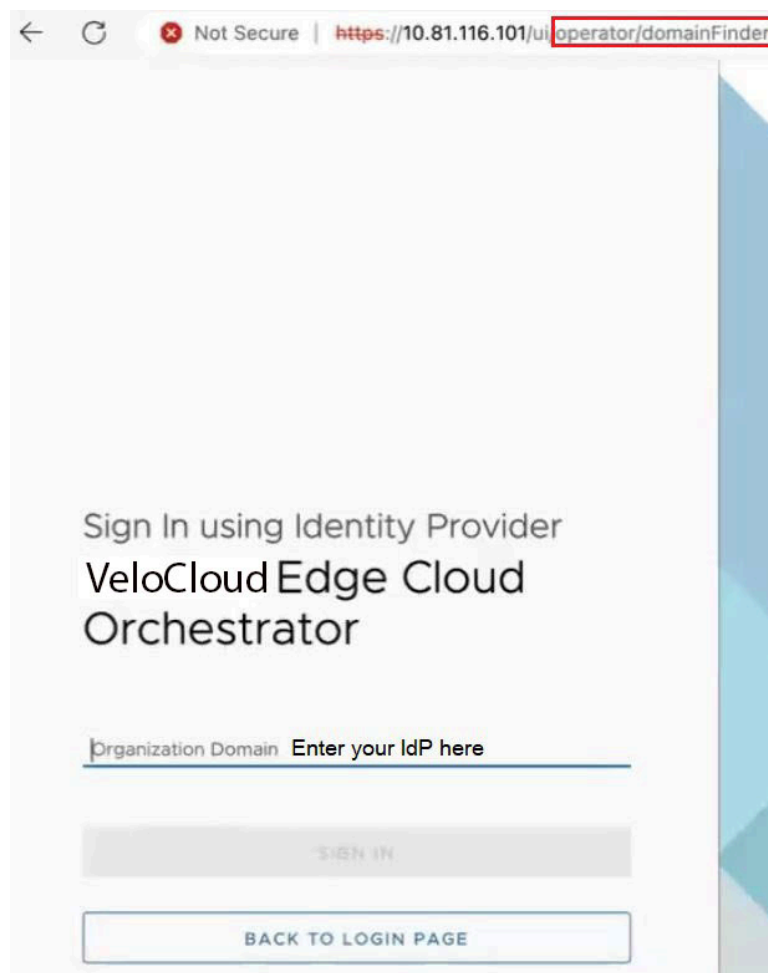
Figure 13-21: Operator Login Screen



On an Orchestrator with multiple IdPs configured, selecting that button takes you to a new screen for SSO sign-in. This is where the Partner Operator would enter in the **Domain Name** configured for the IdP. Once entered, select **Sign In** and you will be logged into the Orchestrator.

Where there are multiple IdPs configured, all users including the Partner would be moved to this screen. The URL will include the text string 'domainFinder', but where it reads Organization Domain, you actually enter your 'Domain Name' for the IdP as configured earlier.

Figure 13-22: Domain Name



Note: An easier method for a Partner using their own IdP is to bookmark the following their Orchestrator URL with this format: *https://orchestrator hostname or IP address/ui/operator/login?domain=IdP Domain Name*. This will automatically take you to the login screen and prepopulate the IdP Domain Name. For example for an Orchestrator with hostname `vcoll-usor1.velocloud.net` where the IdP Domain Name is **Acme**, the Partner Operator could bookmark: `https://vcoll-usor1.velocloud.net/ui/operator/login?domain=Acme` and when they selected that bookmark, the browser would still go to the Operator login screen. The difference is that now when they select **SIGN IN WITH YOUR IDENTITY PROVIDER**, the user is immediately logged in the Orchestrator with no extra step, as the domain is already provided in the URL.

For all configurations of an IdP, select **Update** to save the entered values. The SSO authentication setup is complete in the SD-WAN Orchestrator.

- **RADIUS:** Remote Authentication Dial-In User Service (RADIUS) is a client-server protocol that enables remote access servers to communicate with a central server. RADIUS authentication provides a centralized management for users. You can configure the Orchestrator Authentication in RADIUS mode,

so that the Operator and Enterprise Customers log into the portals using the RADIUS servers. Enter appropriate details in the following fields:

Figure 13-23: Radius Authentication Mode

Orchestrator Role Name	RADIUS Name *
Operator Superuser	VC_SUPER_USER
Operator Standard Admin	VC_ADMIN_USER
Operator Support	VC_SUPPORT_USER

- You can edit the **Protocol** value only in the **System Properties**. Navigate to **Orchestrator > System Properties**, and edit the protocol in the **Value** field of the system property `vco.operator.authentication.radius`.
- **Operator Domain** field is available only for Operators.
- In the **Operator Role Map / Enterprise Role Map** section, map the RADIUS server attributes to each of the Operator or Enterprise user roles. This role mapping is used to determine the role the users would be assigned when they login to the Orchestrator using the RADIUS server for the first time.
- Select **Update** to save the entered values.

SSH Keys

You can create only one SSH Key per user. Select the **User Information** icon located at the top right of the screen, and then select **My Account > SSH Keys** to create an SSH Key.

As an Operator, you can also revoke an SSH Key.

Select the **Refresh** option to refresh the section to display the most current data.

For additional information, see [Configure User Account Details](#).

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 41: Session Limits - Options and Descriptions

Option	Description
Concurrent logins	Allows you to set a limit on concurrent logins per user. By default, Unlimited is selected, indicating that unlimited concurrent logins are allowed for the user.
Session limits for each role	Allows you to set a limit on the number of concurrent sessions based on user role. By default, Unlimited is selected, indicating that unlimited sessions are allowed for the role.

Note: The roles that are already created by the Operator in the **Roles** tab, are displayed in this section.

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

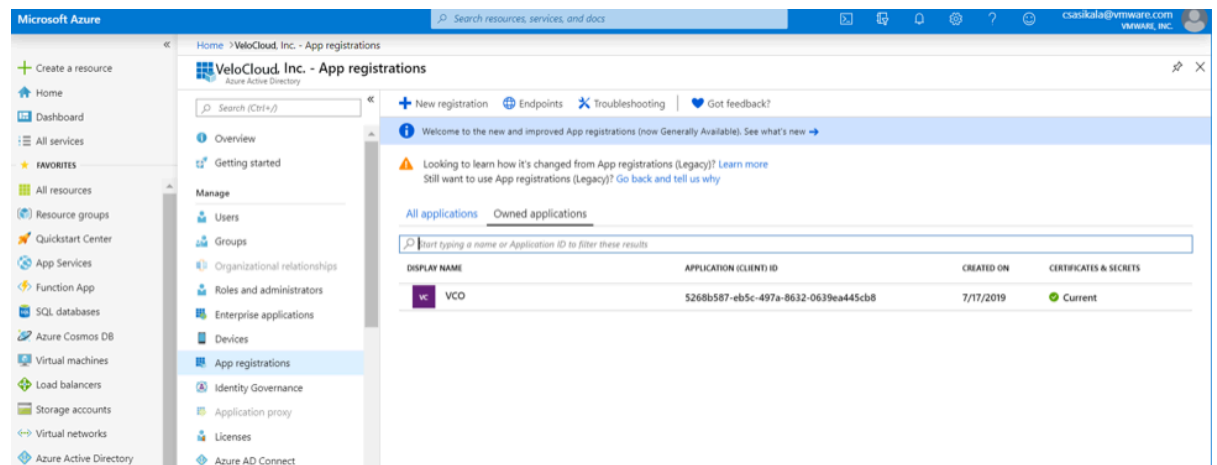
13.4.1 Configure Azure Active Directory for Single Sign On

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 13-24: Azure Active Directory



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

Figure 13-25: 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.

Web

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

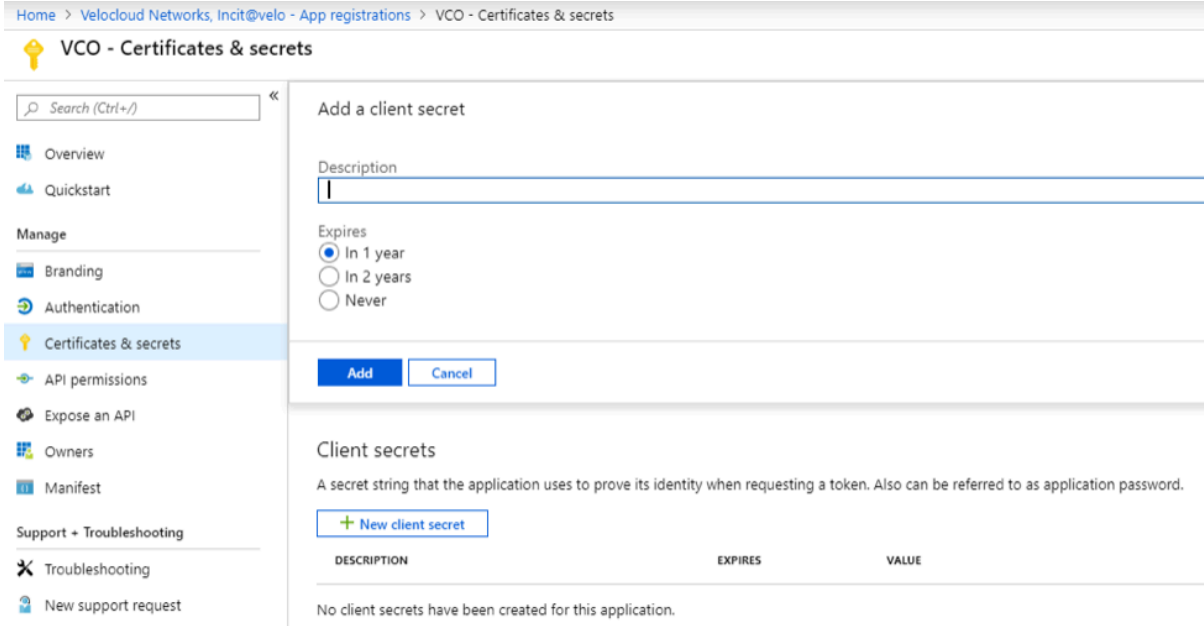
Register

- c. In the **Name** field, enter the name for your Orchestrator application.
- d. In the **Redirect URL** field, enter the redirect URL that your Orchestrator application uses as the callback endpoint.

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

- e. Select **Register**.
- f. Your Orchestrator application will be registered and displayed in the **All applications** and **Owned applications** tabs. 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 on your Orchestrator application.
- i. Go to **Certificates & secrets > New client secret**.
The **Add a client secret** screen appears.

Figure 13-26: Add a client secret



Home > Velocloud Networks, Incit@velo - App registrations > VCO - Certificates & secrets

VCO - Certificates & secrets

Search (Ctrl+/)

Overview

Quickstart

Manage

Branding

Authentication

Certificates & secrets

API permissions

Expose an API

Owners

Manifest

Support + Troubleshooting

Troubleshooting

New support request

Add a client secret

Description

Expires

In 1 year

In 2 years

Never

Add Cancel

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

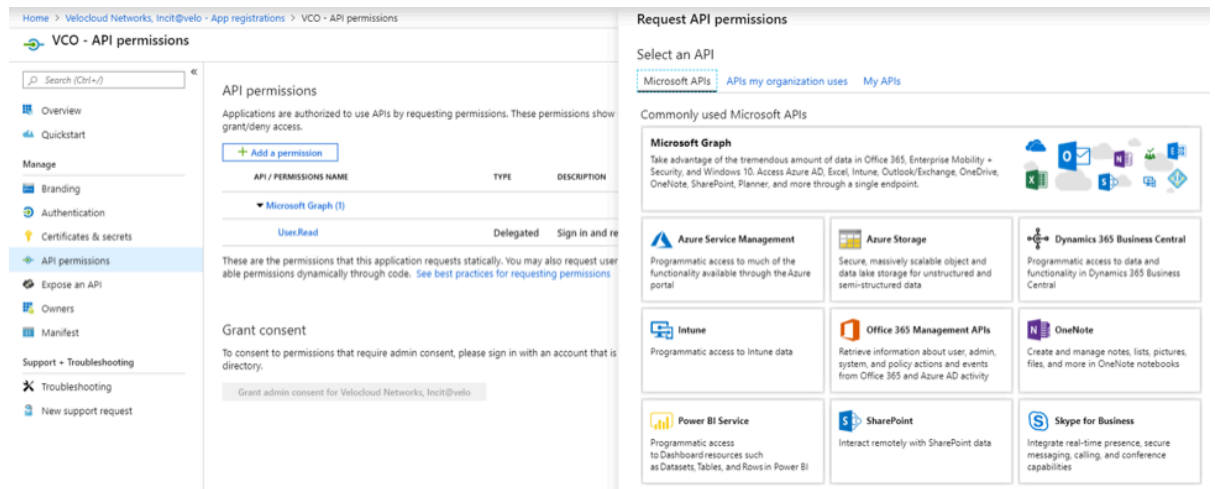
+ New client secret

DESCRIPTION	EXPIRES	VALUE
No client secrets have been created for this application.		

- 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 on your Orchestrator application and go to **API permissions > Add a permission**.

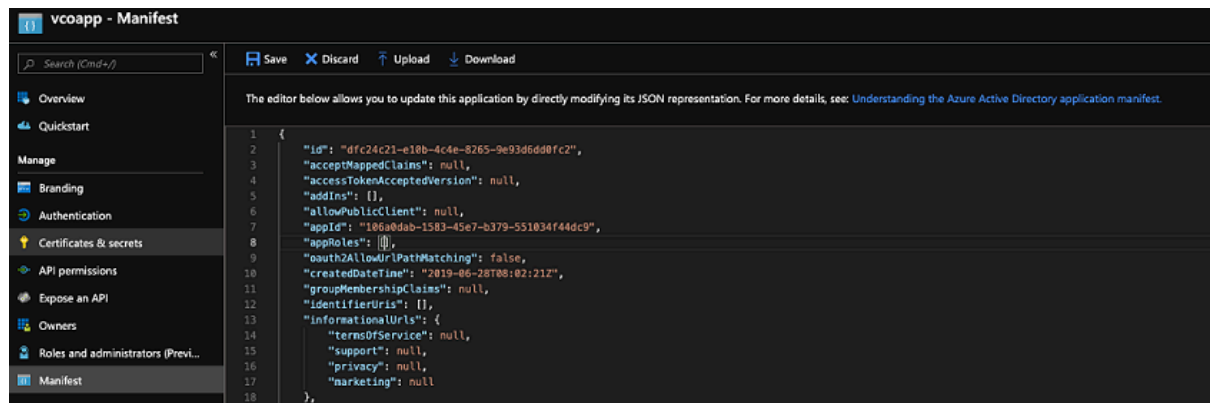
The Request API permissions screen appears.

Figure 13-27: Request API permissions



- i. 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 13-28: Manifest Editor



- 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()`

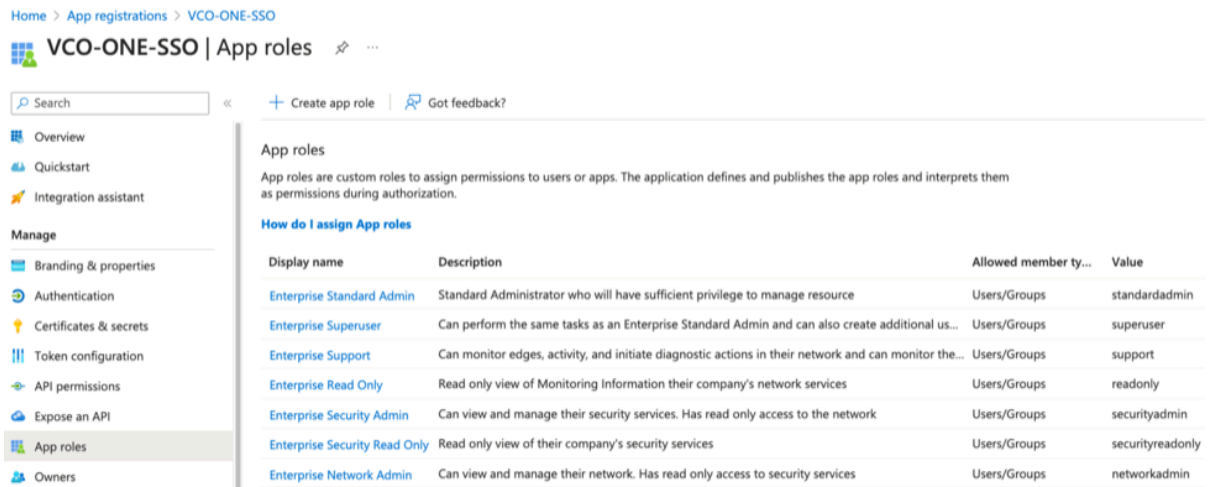
Figure 13-29: Manifest- Add Role Objects

The screenshot shows the 'vcoapp - Manifest' editor in the Azure portal. The left sidebar contains navigation options: Overview, Quickstart, Manage (with sub-items: Branding, Authentication, Certificates & secrets, API permissions, Expose an API, Owners, Roles and administrators (Previous), Manifest), Support + Troubleshooting, and New support request. The main editor area displays the following JSON code:

```
1 {
2   "id": "dfc24c21-e18b-4cde-8265-9e93d6dd0fc2",
3   "acceptMappedClaims": null,
4   "accessTokenAcceptedVersion": null,
5   "addins": [],
6   "allowPublicClient": null,
7   "appId": "186a8dab-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": "18fcaala-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": "cd1d0438-56c8-4c22-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",
```

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

Figure 13-30: App Roles



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

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

Configure Single Sign On in the Orchestrator.

13.4.2 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.

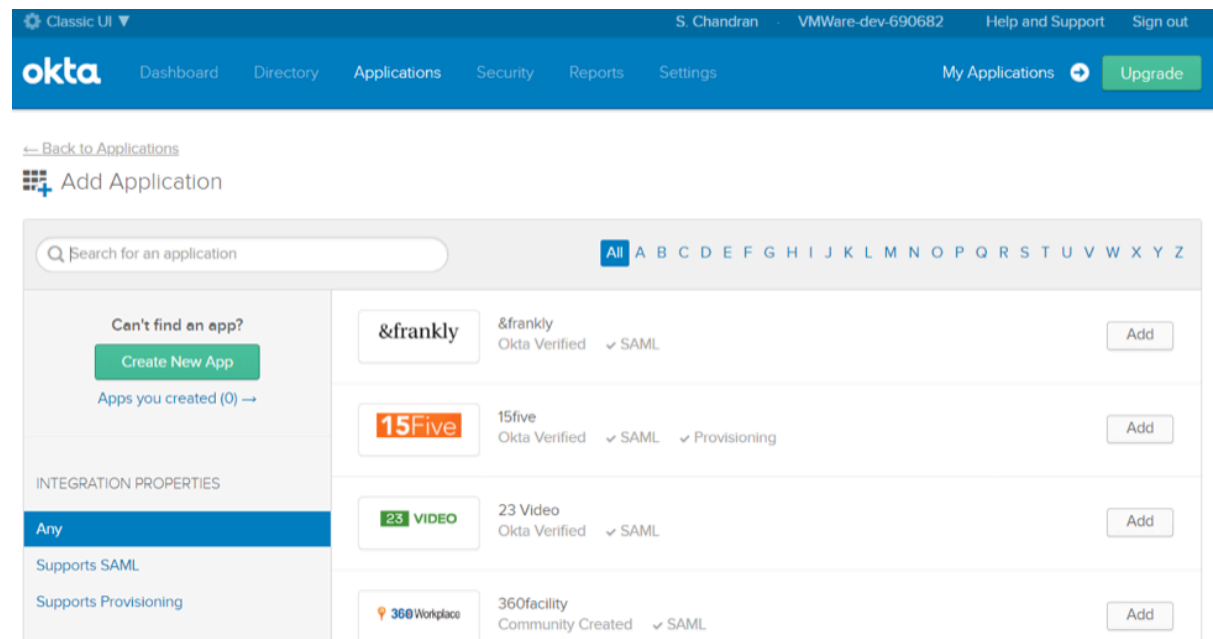


Note: If you are in the Developer Console view, then you must switch to the Classic UI view by selecting **Classic UI** from the **Developer Console** drop-down list.

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

The **Add Application** screen appears.

Figure 13-31: Add Application



b. Select **Create New App**.

The **Create a New Application Integration** dialog box appears.

c. From the **Platform** drop-drop menu, select **Web**.

d. Select **OpenID Connect** as the Sign on method and select **Create**.

The **Create OpenID Connect Integration** screen appears.

Figure 13-32: Create OpenID Connect Integration

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

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

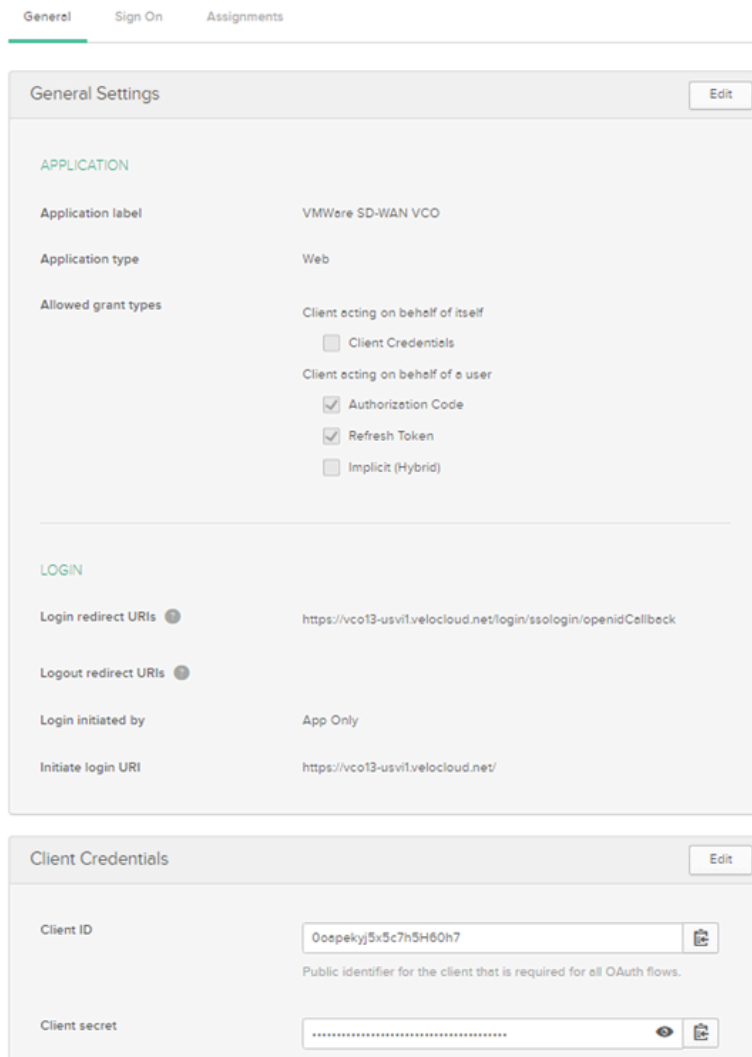
In the Orchestrator application, at the bottom of the **Configure Authentication** screen, you can find the redirect URL link. Ideally, the Orchestrator redirect URL will be in this format: `https://<Orchestrator URL>/login/ssologin/openidCallback`.

- g. Select **Save**.

The newly created application page appears.

- h. On the **General** tab, select **Edit** and select **Refresh Token** for Allowed grant types, and select **Save**. Note down the Client Credentials (Client ID and Client Secret) to be used during the SSO configuration in Orchestrator.

Figure 13-33: Client Credentials



- i. Select the **Sign On** tab and under the **OpenID Connect ID Token** area, select **Edit**.
- j. From the **Groups claim type** drop-down menu, select **Expression**. By default, Groups claim type is set to **Filter**.

- k. In the **Groups claim expression** textbox, enter the claim name that will be used in the token, and an Okta input expression statement that evaluates the token.
- l. Select **Save**.
The application is setup in IDP. You can assign user groups and users to your Orchestrator application.

Figure 13-34: Application is Setup

The screenshot displays the 'Sign On' configuration page for an application. At the top, there are three tabs: 'General', 'Sign On' (which is active), and 'Assignments'. Below the tabs, the page is organized into three main sections:

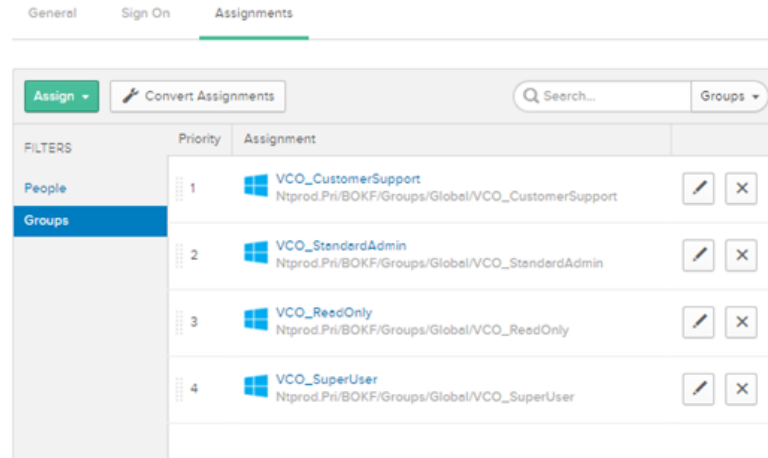
- Settings:** This section is titled 'SIGN ON METHODS'. It includes a descriptive paragraph about sign-on methods and a link to 'Configure profile mapping'. A radio button next to 'OpenID Connect' is selected.
- Token Credentials:** This section has an 'Edit' button. It shows 'Signing credential rotation' set to 'Automatic'.
- OpenID Connect ID Token:** This section also has an 'Edit' button and contains a table of configuration details:

Issuer	https://bokf-sandbox.oktapreview.com
Audience	0oapekyj5x5c7h5H60h7
Claims	Claims for this token include all user attributes on the app profile.
Groups claim type	Expression
Groups claim expression	groups Groups.startsWith("active_directory", "VCO_", 100) Using Groups Claim

- 3. To assign groups and users to your Orchestrator application:
 - a. Go to **Application > Assignments** 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 13-35: Assignments



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

Configure Single Sign-On in the Orchestrator.

13.4.3 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 13-36: 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 by navigating to **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 13-37: Application Details

- e. On the **Parameters** tab, under **OpenId Connect (OIDC)**, double select **Groups**.

The **Edit Field Groups** pop-up appears.

Figure 13-38: Edit Field Groups

Name
Groups

Value

Select Groups

Added Items

Default if no value selected

User Roles

--No transform-- (Single value output)

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

Cancel

- 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 13-39: Token Endpoint

onelogin Users Applications Devices Authentication Activity Security Settings Developers Upgrade now Sasikala

Applications / OpenId Connect (OIDC) More Actions

Info Enable OpenID Connect

Configuration Client ID
14d05920-8c0c-0137-20f5-0a84509636a0151851

Parameters Client Secret

Rules

SSO Show client secret Regenerate client secret

Access OpenID Provider Configuration Information

Users

Privileges

Application Type

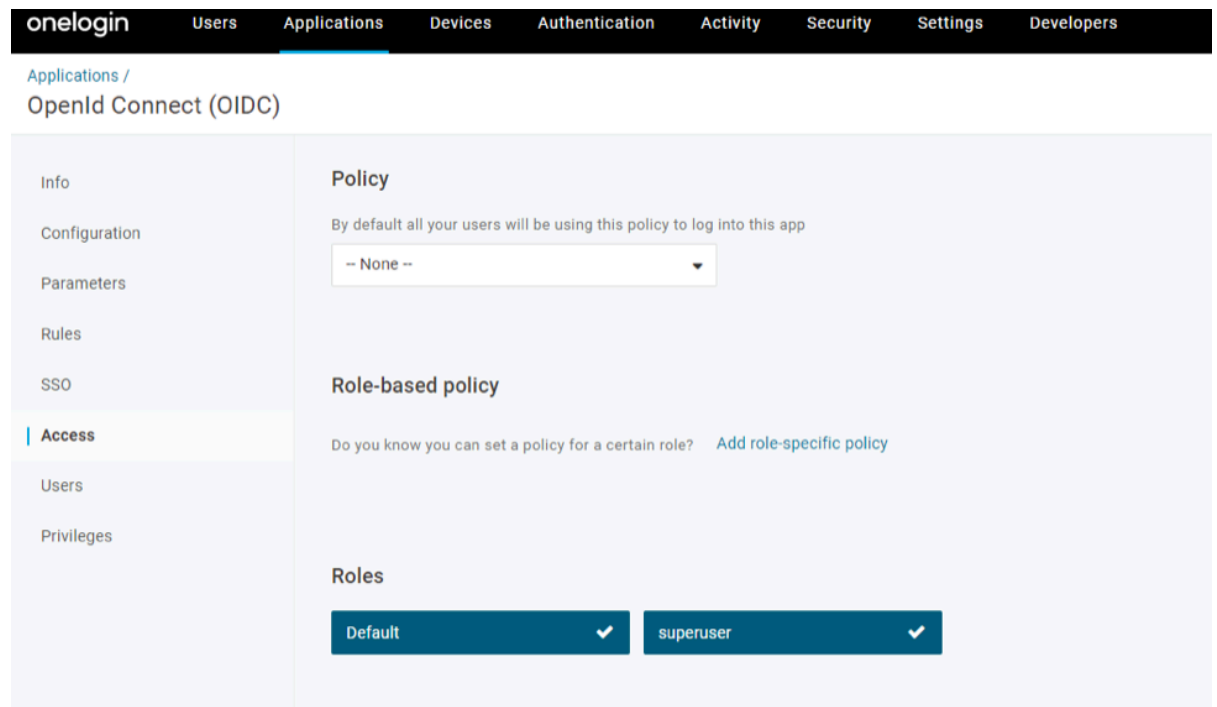
Application Type
Web

Token Endpoint

Authentication Method
POST

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

Figure 13-40: Access tab



3. To add roles and users to your Orchestrator application:
 - a. Select **Users > 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.

13.4.4 Configure PingIdentity for Single Sign On

Ensure you have a PingOne account to sign in.

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

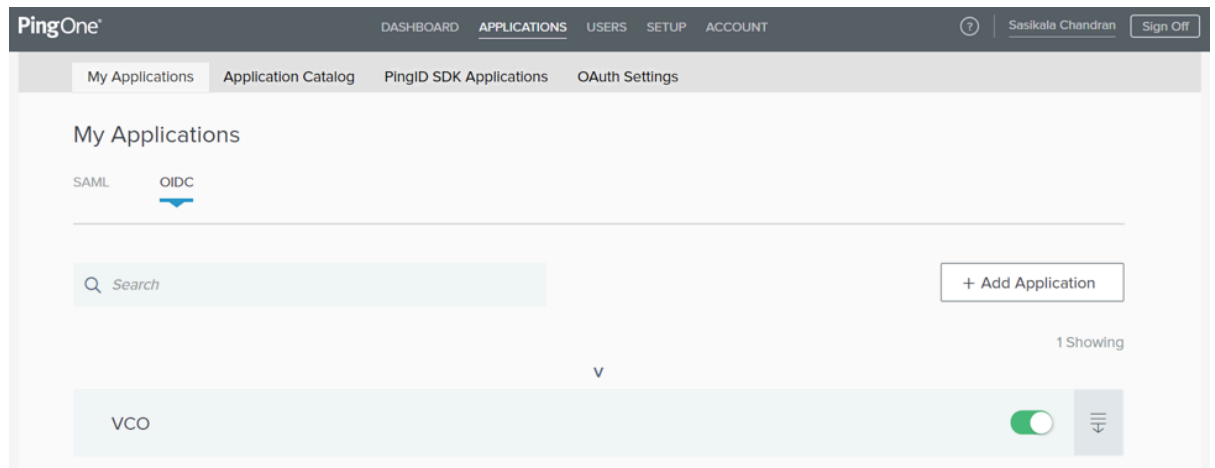


Note: Currently, Orchestrator supports PingOne as the Identity Partner (IDP); however, any PingIdentity product supporting OIDC can be easily configured.

1. Log in to your [PingOne](#) account as an Admin user.
The **PingOne** home screen appears.
2. To create a new application:

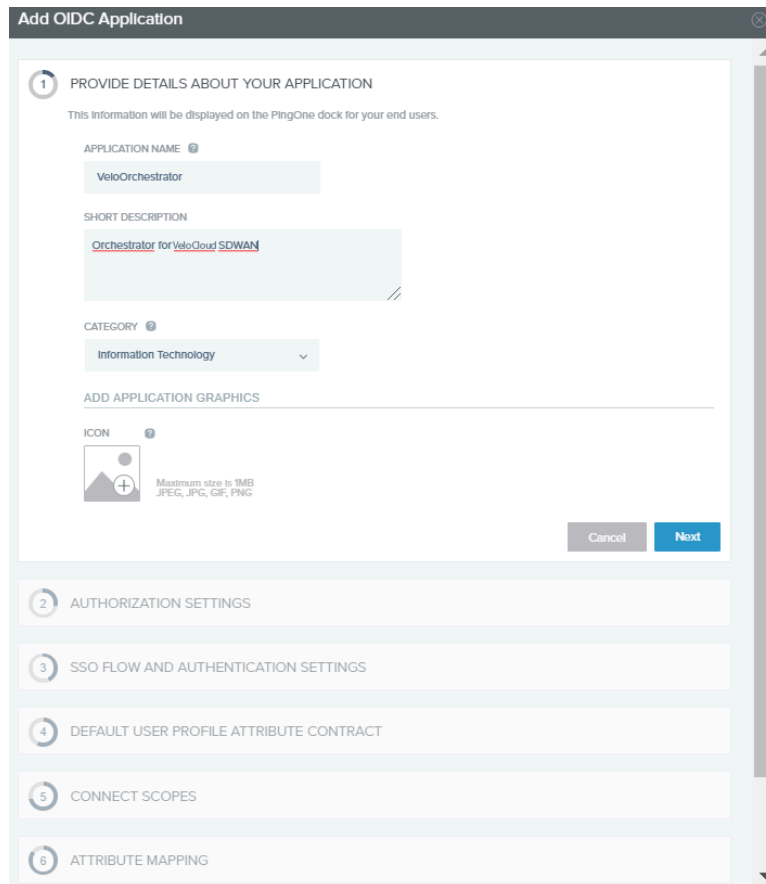
- a. In the upper navigation bar, select **Applications**.

Figure 13-41: My Applications



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

Figure 13-42: Add OIDC Application



- 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 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** checkbox, and select **Next**.



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

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

Manage User Agreements

Orchestrator allows an Operator Super User and Operator Standard Administrator to create and manage End User License Agreements. Only an Operator Super User can create an End User License Agreement.

1. In the Operator Portal, select **Administration** tab and from the left pane select **User Agreements** button.
2. By default, the User Agreement option is de-activated. To activate this option, navigate to the **System Properties** in the Operator portal, and set the value of the System Property `session.options.enableUserAgreements` as **True**. In addition, you can configure the display mode of the User Agreement by defining the Value of the System Property `vco.enterprise.userAgreement.display.mode` as follows:
 - **NONE** — The User Agreement is not displayed to any of the Enterprise Users. This is the default value.
 - **ALL** — The User Agreement is displayed to all the Enterprise Users.
 - **WITH_MSPS** — The User Agreement is displayed to all the Enterprise Users with MSPS.
 - **WITHOUT_MSPS** — The User Agreement is displayed to all the Enterprise Users without MSPS.

The above display settings are applied to all the Customers managed by the Operator. As an Operator, you can override these settings for each Enterprise Customer, as described in [Configure Customers](#).

Only an Enterprise Super User or Partner Super User can accept a license agreement, based on the System Property settings.

Once the properties mentioned above are set, the **User Agreement** page appears in Administration tab.

3. To create and manage User Agreement, select **Administration > User Agreements** tab in the **Operator** portal and perform the following actions:

Table 42: User Agreement- Options and Descriptions

Option	Description
New	Creates a new End User License Agreement.
Duplicate	Duplicates and creates a copy of the selected User Agreement.
Download	Downloads a copy of the User Agreement details.
Delete	Deletes the selected User Agreements.
Export Acceptance Report	Exports a report of all the customers who have accepted the User Agreements, to a CSV file.

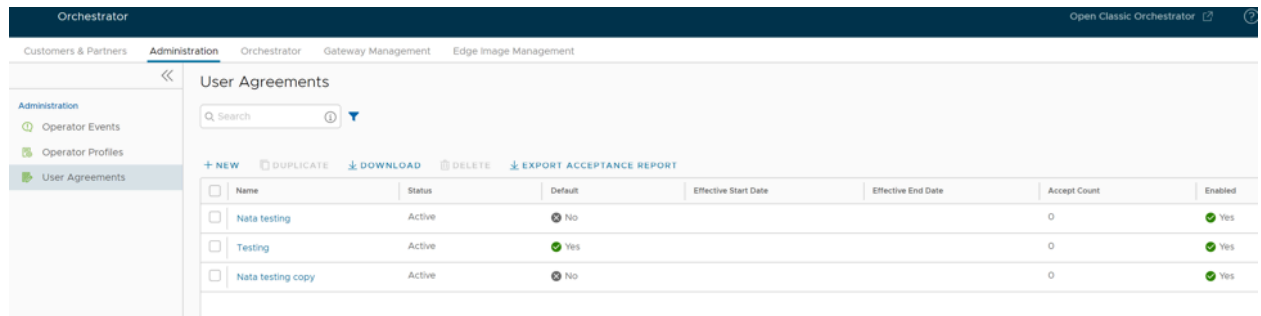


Note: To update, select the existing agreement in the table and update as required.

4. **Create a User Agreement:** Only Operator Superusers and Operator Standard Administrator can create a new user agreement. You can create multiple active user agreements and configure the default one from

the list of active user agreements. You can also choose and configure an active user agreement that you want to show for a particular customer.

Figure 14-1: User Agreements Screen



- a. In the **Administration** tab, select **User Agreements** and select **New**. The **User Agreement** dialog box appears.
- b. Enter the following information in the **User Agreement** dialog box:

Figure 14-2: Create a User Agreement

User Agreement ✕

Enabled

Default

Effective Start Date

Effective End Date

Dialog Title Text *

Dialog Body Text *

Copyright © 1998 - 2022 VMware, Inc. All rights reserved. This product is protected by copyright and intellectual property laws in the United States and other countries as well as by international treaties. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

This field supports [Common Mark](#)

Dialog Button Text *

Table 43: User Agreement- Options and Descriptions

Option	Description
Name	Enter the name for the user agreement.
Enabled	By default, this check box is selected. If unselected, the user agreement is Inactive.
Effective Start Date	Enter the date from which the user agreement is effective.
Effective End Date	Enter the date until which the user agreement is effective.
Dialog Title Text	Enter a title for the user agreement.
Dialog Body Text	Enter the descriptive user agreement text that would be visible to the Customer.
Dialog Button Text	Enter the text to be displayed on the button that the customer would select to accept the agreement.

c. Select Create.

The agreements get displayed on the **User Agreements** page.

Figure 14-3: User Agreement

User Agreement ×

Name *

Enabled

Effective Start Date

Effective End Date

Dialog Title Text *

Dialog Body Text *

Copyright © 1998 - 2022 VMware, Inc. All rights reserved. This product is protected by copyright and intellectual property laws in the United States and other countries as well as by international treaties. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

This field supports [Common Mark](#)

Dialog Button Text *

d. To delete an agreement, select an inactive agreement and select Delete.



Note: Active agreements cannot be deleted.



Note: When an Enterprise Superuser or Partner Superuser logs into the Orchestrator for the first time, a 'User Agreement' message pops up prompting the user to accept the agreement. The user must accept the agreement to get access to the Orchestrator. If the user does not accept the agreement, it gets automatically logged out.

Manage Gateway Pools and Gateways

Arista network consists of multiple service Gateways deployed at top tier network and cloud data centers. The Gateway provides the advantage of cloud-delivered services and optimized paths to all applications, branches, and data centers. Service providers can also deploy their own Partner Gateways in their private cloud infrastructure.

15.1 Manage Gateway Pools

A Gateway Pool is a group of Gateways.

Gateways can be organized into pools that are then assigned to a network. An unpopulated default Gateway pool is available after you install Orchestrator. If required, you can create additional Gateway pools.

As an Operator Super user and Operator Admin user, you can create, clone, manage, download, and delete Gateway pools created by both Operator and Partner users.



Note: Operator Business Specialist user and Operator IT support user can only view the configured Gateway pools and download the CSV file.

To manage Gateway pools, perform the following steps:

1. Log into the **Orchestrator** as an Operator Super user or Admin user.
2. In the Orchestrator UI, select the **Gateway Management** tab and go to **Gateway Pools** in the left navigation pane.

The **Gateway Pools** page appears.

Figure 15-1: Manage Gateway Pools

The screenshot shows the 'Gateway Pools' management interface. At the top, there are navigation tabs: 'Customers', 'Administration', 'Gateway Management' (selected), and 'Edge Image Management'. A left sidebar contains 'Gateway Management', 'Gateways', 'Gateway Pools' (selected), and 'Diagnostic Bundles'. The main area has a search bar and a 'Map Distribution' section. Below this is a table with the following data:


<input type="checkbox"/>	Name	Gateways	IP Version	Customers	Partner Gateway	Managed Pool [ⓘ]
<input type="checkbox"/>	5-site-GatewayPool	2	IPv4 and IPv6	1	None	<input checked="" type="radio"/> No
<input type="checkbox"/>	Default Pool	0	IPv4	0	None	<input checked="" type="radio"/> No

At the bottom of the table, there are controls for 'COLUMNS' and 'REFRESH', and a status indicator '2 Gateway Pools'.

3. To search a specific Gateway pool, enter a relevant search text in the **Search** box. For advanced search, select the **Filter** icon next to the **Search** box to filter the results by specific criteria.
4. The **Map Distribution** section is used for displaying the Gateways on a map. You can select the **+** and **-** buttons to zoom in and zoom out the map, respectively. In the **Gateway Pools** table, if you have selected any Gateway pools then only the Gateways in the selected pools are displayed on the map. Otherwise, all Gateways are displayed on the map.

The **Gateway Pools** table displays the existing Gateway pools with the following details.

Table 44: Gateway Pools Field Descriptions

Field	Description
Name	Specifies the name of the Gateway pool. When selecting a Gateway pool link in the Name column, the user gets redirected to the Gateway Pools Overview page.
Gateways	Specifies the number of Gateways available in the Gateway pool. When selecting a Gateway link in the Gateways column, the user gets redirected to the Gateway Overview page.
IP Version	Specifies whether the Gateway pool is enabled with IPv4 address or both the IPv4 and IPv6 addresses. <div style="border: 1px solid black; padding: 5px;"> Note: When assigning Gateways to the Gateway pool, ensure that the IP address type of the Gateway matches the IP address type of pool.</div>
Customers	Specifies the number of Enterprise Customers associated with the Gateway pool. When selecting a Customer link in the Customers column, a dialog opens with listed customers. If a user selects a customer then the user gets redirected to the Configure Customers page.
Partner Gateway	Specifies the status of the Partner Gateway. The following are the available options: <ul style="list-style-type: none">• None- Use this option when Enterprises assigned to this Gateway pool do not require Gateway Partner handoffs.• Allow- Use this option when the Gateway pool must support both Partner Gateways and Cloud Gateways.• Only (Partner Gateways)- Use this option when Edges in the Enterprise should not be assigned Cloud Gateways from the Gateway pool, but can use only the Gateway-1 and Gateway-2 that are set for the individual Edge.
Managed Pool	Specifies if a Partner can manage the Gateway pool.

On the **Gateway Pools** page, you can perform the following activities: **New Gateway Pool** – Creates a new Gateway pool. See [Create New Gateway Pool](#).

- **Clone** – Creates a new Gateway pool, by cloning the existing configurations from the selected Gateway pool. See [Clone a Gateway Pool](#).
- **Download**- Downloads the CSV file for all Gateway pools or the selected Gateway pool.
- **Delete** – Deletes the selected Gateway pool. You cannot delete a Gateway pool that is already being used by a Partner or an Enterprise Customer.
- You can also configure the existing Gateway pools by selecting the name link of the Gateway pool. See [Configure Gateway Pools](#).

15.1.1 Create New Gateway Pool


In addition to the default Gateway pool, you can create new Gateway pools and associate them with Enterprise Customers.

1. In the Orchestrator UI, select the **Gateway Management** tab and go to **Gateway Pools** in the left navigation pane. The **Gateway Pools** page appears.
2. Select **New Gateway Pool**.
3. In the **New Gateway Pool** dialog, configure the following details and select **Create**.

Figure 15-2: Create New Gateway Pool

Table 45: New Gateway Pool Field Descriptions

Field	Description
Name	Enter a name for the new Gateway pool.
Description	Enter a description for the Gateway pool.
Partner Gateway Hand Off	<p>This option determines the method to hand off the Gateways to Partners. Choose one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> • None – Select this option when Partner Gateway hand off is not required. • Allow – Select this option when you want the Gateway pool to support a mix of both the Partner Gateways and Cloud Gateways. • Only Partner Gateways – Select this option when Edges in the Enterprise should not be assigned with Cloud Gateways from the pool, and will only be assigned with the Gateways that are set for an individual Edge.
IP Version	<p>Choose one of the following address types with which the Gateway pool should be enabled:</p> <ul style="list-style-type: none"> • IPv4 – Allows to add IPv4 only Gateways. • IPv4 and IPv6 – Allows to add Gateways with IPv4 and IPv6 addresses.

 **Note:** If you want to use Edges with IPv6 support, then choose **IPv4 and IPv6**.

- Configure the Gateway pool by adding Gateways to the pool. See [Configure Gateway Pools](#).

15.1.2 Clone a Gateway Pool

You can clone the configurations from an existing Gateway pool and create a new Gateway pool with the cloned settings.

1. In the Orchestrator UI, select the **Gateway Management** tab and go to **Gateway Pools** in the left navigation pane. The **Gateway Pools** page appears.
2. In the **Gateway Pools** table, select the Gateway pool that you want to clone and select **Clone**. The **New Gateway Pool** dialog with the cloned settings appears.

Figure 15-3: Clone a Gateway Pool

New Gateway Pool

Name * Copy of VC GW pool

Description Enter Description (Optional)
Maximum 256 characters

Partner Gateway Hand Off ① Allow

IP Version *
 IPv4
 IPv4 and IPv6

CANCEL CREATE

3. The Gateway pool clones the existing configuration from the selected Gateway pool. If required, you can modify the details. For additional information on the options, see [Create New Gateway Pool](#).
 4. After updating the Gateway pool details, select **Create**.
- Configure the Gateway pool by adding Gateways to the pool. See [Configure Gateway Pools](#).

15.1.3 Configure Gateway Pools

After creating a Gateway pool, you can add Gateways to the pool and associate the pool to an Enterprise Customer.

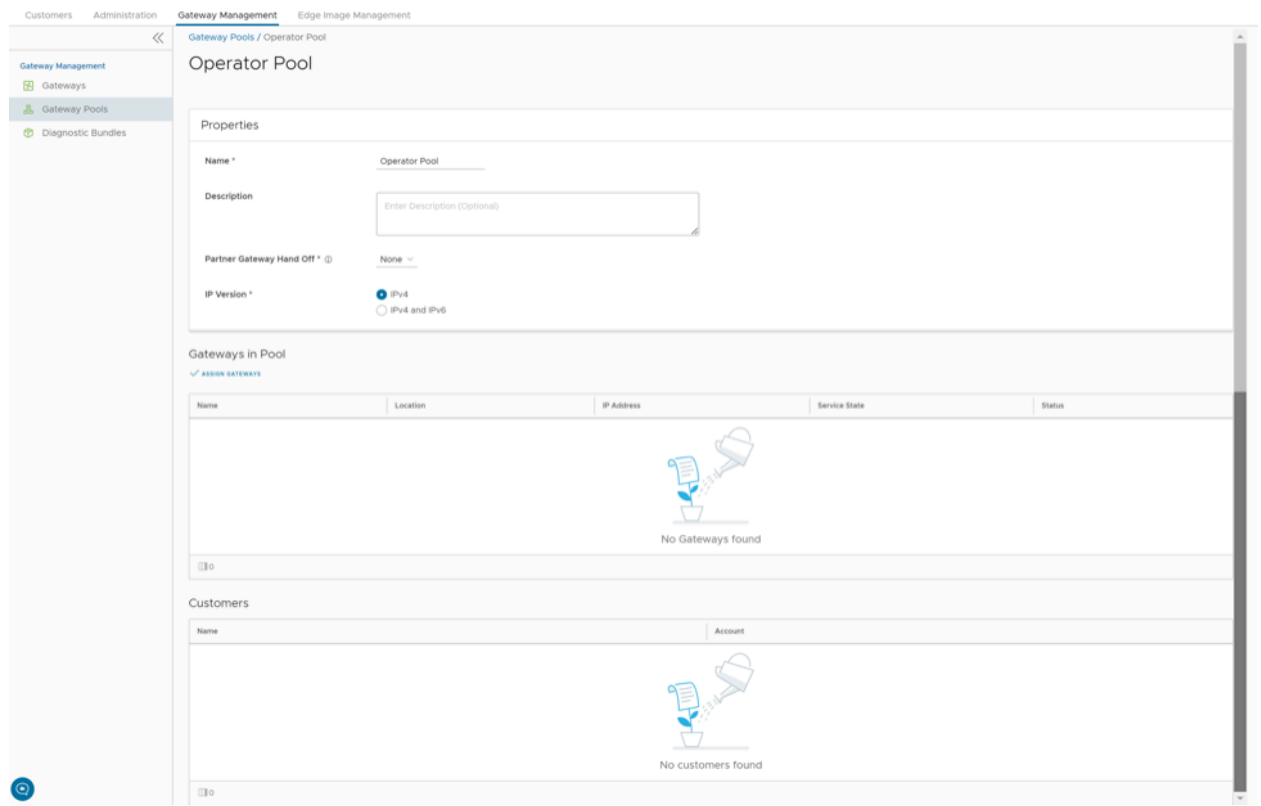
Whenever you create a new Gateway pool or clone a pool, you are redirected to the **Gateway Pool Overview** page to configure the properties of the pool.

To configure an existing Gateway pool:

1. In the Orchestrator UI, select the **Gateway Management** tab and go to **Gateway Pools** in the left navigation pane. The **Gateway Pools** page appears.
2. Select the name link to a Gateway pool that you want to configure.

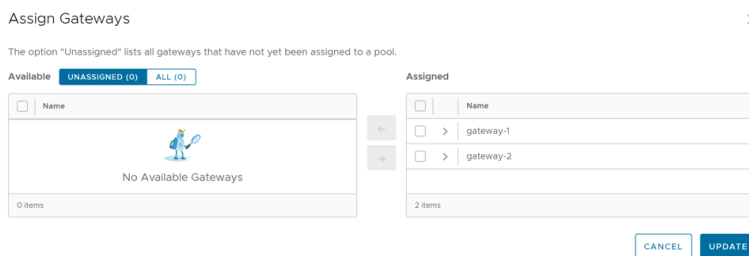
3. Configure the following details for the Gateway pool:

Figure 15-4: Configure Gateway Pools



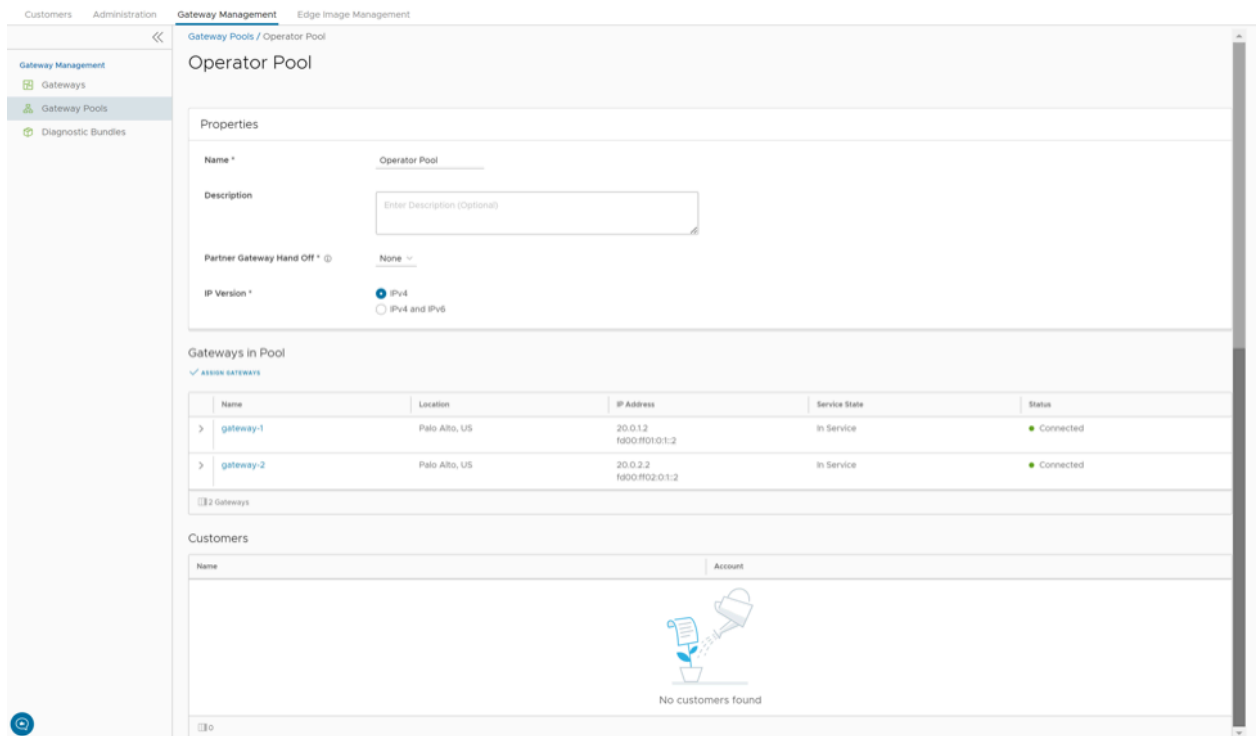
- In the **Properties** section, the existing Name, Description, Partner Gateway Hand Off details, and the Association Type are displayed. If required, you can modify these details.
- In the **Gateways in Pool** section, select **Manage** to add Gateways to the pool. The **Assign Gateways to Gateway pool** dialog appears.
- In the **Assign Gateways to Gateway pool** dialog, move the required Gateways from the **Available** pane to **Assigned** pane using the arrows and select **Update**.

Figure 15-5: Assign Gateways to Gateway pool



- The Gateways assigned to the selected Gateway pool are displayed as follows.

Figure 15-6: Gateways in Pool



- Select **Save Changes**.

The configured Gateway pools are displayed on the **Gateway Pools** page.

You can associate the Gateway pool to a Partner or an Enterprise Customer. The Edges available in the Enterprise are connected to the Gateways available in the pool.

Refer to the following links to associate the Gateway pool:

- For a new customer, see [Create New Customer](#).
- For an existing customer, see [Configure Customers](#).
- For a new Partner, see [Create New Partner](#).
- For an existing Partner, see [Configure Partner](#).

15.2 Manage Gateways

VeloCloud Gateways are a distributed network of gateways, deployed around the world or on-premises at service providers, provide scalability, redundancy and on-demand flexibility. The Gateways optimize data paths to all applications, branches, and data centers along with the ability to deliver network services to and from the cloud.

By default, the Gateways named as **gateway-1** and **gateway-2** are available when you install Orchestrator. If required, you can create additional Gateways.

As an Operator Super user and Operator Admin user, you can create, manage, and delete Gateways created by both Operator and Partner users.



Note: The Operator IT support user and Operator Business Specialist user can only view the configured Gateways.

To manage Gateways, perform the following steps:

1. Log into the **Orchestrator** as an Operator Super user or Admin user.
2. In the Orchestrator UI, select the **Gateway Management** tab and go to **Gateways** in the left navigation pane.

The **Gateways** page appears.

Figure 15-7: Manage Gateways

The screenshot shows the Orchestrator Gateway Management interface. The top navigation bar includes 'Orchestrator', 'Open Classic Orchestrator', and user icons. The main navigation pane on the left shows 'Gateway Management' with sub-items: 'Gateways', 'Gateway Pools', and 'Diagnostic Bundles'. The main content area is titled 'Gateways' and features a search box, a filter icon, and a 'csv' button. Below this is a 'Map Distribution' section. A table lists the gateways with columns for Name, Status, CPU, Memory, Edges, Service State, IP Address, and Location. The table contains four rows: gateway-1 (Connected, 38.81% CPU, 65.1% Memory, 5 Edges, In Service, 20.0.1.2), gateway-2 (Connected, 22.09% CPU, 65.1% Memory, 5 Edges, In Service, 20.0.2.2), N-CA (dev) (Offline, 0 Edges, In Service, 54.215.193.206), and SIN (dev) (Offline, 0 Edges, In Service, 54.254.157.221). At the bottom of the table, there are 'COLUMNS' and 'REFRESH' buttons, and a pagination indicator '1 - 4 of 4 items'.


	Name	Status	CPU	Memory	Edges	Service State	IP Address	Location
>	gateway-1	Connected	38.81%	65.1%	5 View	In Service	20.0.1.2 fd00:ff01:0:1:2	San Francisco, US
>	gateway-2	Connected	22.09%	65.1%	5 View	In Service	20.0.2.2 fd00:ff02:0:1:2	Palo Alto, US
>	N-CA (dev)	Offline			0 View	In Service	54.215.193.206	
>	SIN (dev)	Offline			0 View	In Service	54.254.157.221	

To search a specific Gateway, enter a relevant search text in the **Search** box. For advanced search, select the filter icon next to the **Search** box to filter the results by specific criteria.

The **Map Distribution** section is used for displaying the Gateways on a map. You can select the **+** and **-** buttons to zoom in and zoom out the map, respectively.


The **Gateways** table displays the existing Gateways with the following details.

Table 46: Gateways Field Descriptions

Field	Description
Name	Name of the Gateway
Status	Reflects the success or failure of periodic heartbeats sent by mgd to the Orchestrator and does not indicate the status of the data and control plane. The following are the possible statuses: <ul style="list-style-type: none">• Connected – Gateway is heart beating successfully to the Orchestrator.• Degraded – Orchestrator has not heard from the Gateway for at least one minute.• Offline – Orchestrator has not heard from the Gateway for at least two minutes.
CPU	Average CPU utilization of all the cores in the system at the time of the last heartbeat.
Memory	Percentage usage of the physical memory by all processes in the system as reported by <code>psutil.phymem_usage</code> at the time of the last heartbeat. This is similar to estimating the percentage of memory usage using the <code>free</code> command.
Edges	Number of Edges connected to the Gateway at the time of the last heartbeat. <div data-bbox="667 737 1511 856" style="border: 1px solid black; padding: 5px;"><p> Note: Select View next to the number of Edges, to view all the Edges assigned to the Gateway as well as their online/offline status on the Orchestrator. This option does not display the Edges that are actually connected to the Gateway.</p></div>
Service State	The user-configured service state of the Gateway and whether it is eligible to be assigned to new Edges.
IP Address	The public IP address that public WAN links of an Edge use to connect to the Gateway. This IP address is used to uniquely identify the Gateway. If the Gateway is enabled to accommodate both IPv4 and IPv6 addresses, this column displays both the IP addresses.
Location	Location of the Gateway from GeoIP (by default) or as manually entered by the user. This is used for geographic assignment of the Gateway to Edges and should be verified.

3. On the **Gateways** page, you can perform the following activities:

- **New Gateway** – Creates a new Gateway. See [Create New Gateway](#).
- **Delete Gateway** – Deletes the selected Gateway. You cannot delete a Gateway that is already being used by a Partner or an Enterprise Customer.
- **Stage to Bastion** - Stages a Gateway to the Bastion Orchestrator.
- **Unstage from Bastion** - Removes a Gateway from the Production Orchestrator.

 **Note:** **Stage to Bastion** and **Unstage from Bastion** options are available only when the Bastion Orchestrator feature is enabled using the `session.options.enableBastionOrchestrator` system property.

For additional information, see *Bastion Orchestrator Configuration Guide*.

- **Support Request** – Redirects to a Knowledge Base article that has instructions on how to file a support request.

15.2.1 Create New Gateway

In addition to the default Gateways, you can create Gateways and associate them with Enterprise Customers.

To create a Gateway, perform the following steps.

1. In the **Orchestrator** UI, select the **Gateway Management** tab and go to **Gateways** in the left navigation pane. The **Gateways** page appears.
2. Select **New Gateway**. The **New Gateway** dialog appears.
3. In the **New Gateway** dialog, configure the following details:

Figure 15-8: Create New Gateway

New Gateway ×




Property

Name *	<input type="text" value="GW1"/>
IPv4 Address *	<input type="text" value="12.1.1.1"/>
IPv6 Address	<input type="text" value="Enter IPv6"/>
Service State	<input type="text" value="Out Of Service"/>
Gateway Pool	<input type="text" value="Default Pool (IPv4)"/>
Authentication Mode	<input type="text" value="Certificate Acquire"/>

Site Contact

Contact Name *	<input type="text" value="Super User"/>
Contact Email *	<input type="text" value="super@velocloud.net"/>

Table 47: New Gateway Field Descriptions

Field	Description
Name	Enter a name for the new Gateway.
IPv4 Address	Enter the IPv4 address of the Gateway.
IPv6 Address	Enter the IPv6 address of the Gateway.
Service State	<p>Select the service state of the Gateway from the drop-down list. The following options are available:</p> <ul style="list-style-type: none"> • In Service- The Gateway is connected and available. • Out of Service- The Gateway is not connected. • Quiesced- The Gateway service is quiesced or paused. Select this state for backup or maintenance purposes. <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p> Note: The Quiesced and Out of Service states are only applicable for Cloud Gateway deployment.</p> </div>
Gateway Pool	Select the Gateway Pool from the drop-down list, to which the Gateway would be assigned.
Authentication Mode	<p>Select the authentication mode of the Gateway from the following available options:</p> <ul style="list-style-type: none"> • Certificate Not Required- Gateway uses a pre-shared key mode of authentication. • Certificate Acquire- This option is selected by default and instructs the Gateway 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 Gateway uses the certificate for authentication to the Orchestrator and for establishment of VCMP tunnels. <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p> Note: After acquiring the certificate, the option can be updated to Certificate Required.</p> </div> <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p> Note: With the Bastion Orchestrator feature enabled, the Gateways that are to be staged to Public Orchestrator should have the Authentication mode set to either Certificate Acquire or Certificate Required.</p> </div> <ul style="list-style-type: none"> • Certificate Required- Gateway uses the PKI certificate. Operators can change the certificate renewal time window for Gateways using the system properties.
Contact Name	Enter the name of the Site Contact.
Contact Email	Enter the Email ID of the Site Contact.

Note:

- Once you have created a Gateway, you cannot modify the IP addresses.
- Release 4.3.x and 4.4.x support Greenfield deployment of Gateways for IPv6. If you have upgraded a Gateway from a previous version earlier than 4.3.0, you cannot configure the upgraded Gateway with the IPv6 address.
- Release 4.5.0 supports both the Greenfield and Brownfield deployment of Gateways for IPv6. If you have upgraded a Gateway from a previous version earlier than 4.5.0, you can dynamically configure IPv6 address for the Gateway.

- IPv4/IPv6 dual-stack mode is not supported for Bastion Orchestrator configuration.

Once you create a new Gateway, you are redirected to the **Configure Gateways** page, where you can configure additional settings for the newly created Gateway.

To configure additional settings for the Gateway, see [Configure Gateways](#).

15.2.2 Configure Gateways

When you create a new Gateway, you are automatically redirected to the Configure Gateways page, where you can configure the properties and other additional settings for the Gateway.

To configure an existing Gateway:

1. In the **Operator** portal of the Orchestrator, select the **Gateway Management** tab and go to **Gateways** in the left navigation pane. The **Gateways** page displays the list of available Gateways.
2. Select the link to a Gateway that needs to be configured for additional settings. The details of the selected Gateway are displayed in the **Configure > Gateways** page.
3. In the **Overview** tab, you can configure the following details:

Figure 15-9: Configure Gateways Overview Screen

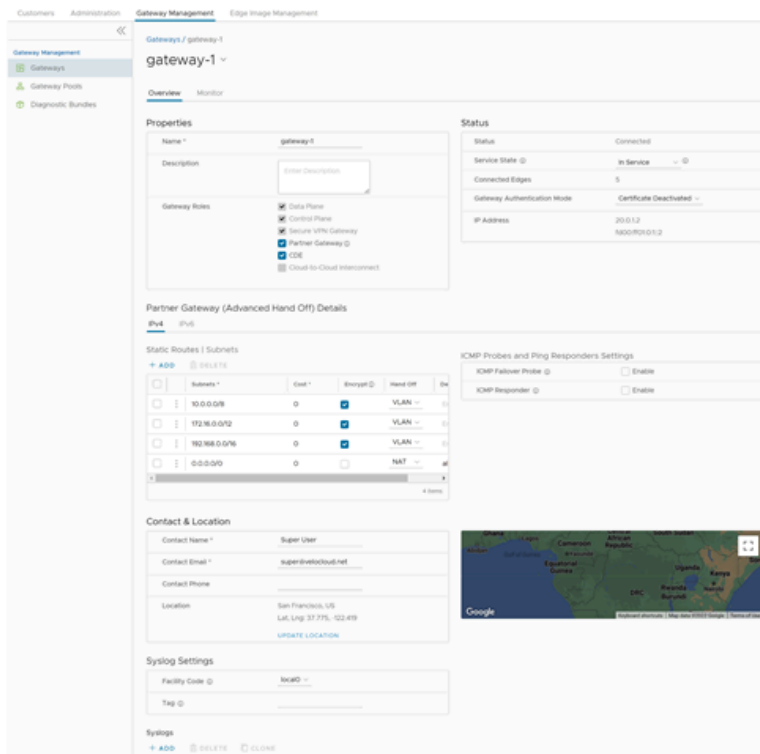







Table 48: Configure Gateways Field Descriptions


Option	Description
Properties	<p data-bbox="664 260 1503 310">Displays the existing Name and Description of the selected Gateway. If required, you can modify the information.</p> <p data-bbox="664 323 1190 350">You can also configure the Gateway Roles, as required:</p> <ul data-bbox="672 363 1503 850" style="list-style-type: none"><li data-bbox="672 363 1443 413">• Data Plane- Enables the Gateway to operate in the Data plane and is selected by default.<li data-bbox="672 438 1495 489">• Control Plane- Enables the Gateway to operate in the Control plane and is selected by default.<li data-bbox="672 514 1479 564">• Secure VPN Gateway- Select the option to use the Gateway to establish an IPsec tunnel to a Non SD-WAN Destination.<li data-bbox="672 590 1495 669">• Partner Gateway- Select the check box to allow the Gateway to be assigned as a Partner Gateway for Edges. If you select this option, configure the additional settings in the Partner Gateway (Advanced Handoff) Details section.<li data-bbox="672 695 1503 774">• CDE- Enables the Gateway to operate in Cardholder Data Environment (CDE) mode. Select this option to assign the Gateway for customers who require to transmit PCI traffic.<li data-bbox="672 800 1398 850">• Cloud-to-Cloud Interconnect- Select the option to enable cloud-to-cloud-interconnect (CCI) tunnels on the VeloCloud Gateways. <div data-bbox="703 863 1508 957" style="border: 1px solid #00a0e3; padding: 5px;"><p data-bbox="711 894 748 930"></p><p data-bbox="794 873 1419 947">Note: This Gateway Role option is shown if the <code>session.options.enableZscalerCci</code> system property is set to True.</p></div> <ul data-bbox="672 1010 1487 1087" style="list-style-type: none"><li data-bbox="672 1010 1487 1087">• Symantec Web Security Service: Enables the Gateway's Symantec Web Security Service capability. The Orchestrator assigns this Gateway to the Edge as WSS Primary Gateway or WSS Secondary Gateway. <div data-bbox="703 1100 1508 1176" style="border: 1px solid #00a0e3; padding: 5px;"><p data-bbox="711 1119 748 1155"></p><p data-bbox="794 1113 1450 1163">Note: This assignment works only when the Gateway Pool's Partner Gateway Handoff is not set to Only.</p></div>

Option	Description
Status	<p>You can configure the following details:</p> <ul style="list-style-type: none"> • Status- Displays the status of the Gateway which reflects the success or failure of periodic heartbeats sent to the Orchestrator. The following are the available statuses: <ul style="list-style-type: none"> • Connected- Gateway is heart beating successfully to the Orchestrator. • Degraded- Orchestrator has not heard from the Gateway for at least one minute. • Offline- Orchestrator has not heard from the Gateway for at least two minutes. • Service State- Select the Service State of the Gateway from the following available options: <ul style="list-style-type: none"> • In Service- The Gateway is connected, and it is available for Primary or secondary tunnel assignments. When the Service state of the Gateway is switched from the 'Out Of Service' to 'In Service' state, the Primary or Secondary assignments, Super Gateways, Edge-to-Edge routes are recalculated for each Enterprise using the Gateway. • Pending Service- The Gateway is connected, and it is pending for tunnel assignments. • Out of Service- The Gateway is not connected or not available for any assignments. All the existing assignments are removed. • Quiesced- The Gateway service is quiesced or paused. No new tunnels or NSD sites can be added to the Gateway. However, the existing assignments would still remain in the Gateway. Select this state for backup or maintenance purposes. <div data-bbox="740 919 1510 997" style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;">  Note: The Quiesced and Out of Service states are only applicable for Cloud Gateway deployment. </div> <p>When the Service state is Quiesced, Orchestrator provides a self-service migration functionality that allows you to migrate from your existing Gateway to a new Gateway without your Operator's support.</p> <p>For additional information, see Quiesce Gateways.</p> <div data-bbox="740 1192 1510 1270" style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;">  Note: Self-service migration is not supported on Partner Gateways. </div>
Connected Edges	<p>Displays the number of Edges connected to the Gateway. This option is displayed only when the Gateway is activated.</p>





Option	Description
Gateway Authentication Mode	<p>Select the authentication mode of the Gateway from the drop-down menu:</p> <ul style="list-style-type: none"> Certificate Deactivated- Gateway uses a pre-shared key mode of authentication. If you change the mode from Certificate Deactivated to: <ul style="list-style-type: none"> Certificate Acquire: Tunnels based on PSK mode are not impacted. Only tunnels with Gateways are impacted. These tunnels are reconnected based on certificate. All tunnels configured with PSK mode continue to stay active and no disruption is seen in the traffic. Certificate Required: The Orchestrator does not directly allow this change. You must first change the mode to Certificate Acquire, and then change it to Certificate Required. This helps avoiding heartbeat loss to the Orchestrator, when Edge is assigned a certificate. Certificate Acquire- This option is selected by default and instructs the Gateway 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 Gateway uses the certificate for authentication to the Orchestrator and for establishment of VCMP tunnels. If you change the mode from Certificate Acquire to: <ul style="list-style-type: none"> Certificate Deactivated: PSK based tunnels are not impacted. Tunnels with Gateways and all certificate-based tunnels are disconnected and reconnected based on PSK. Certificate Required: All peers configured with PSK mode are disconnected and cannot connect to the Hub. All current RSA tunnels stay active. <p>When the Hub is in Certificate Acquire mode, the tunnels based on the certificate are reestablished with new certificate. PSK based tunnels are not impacted.</p>

 **Note:** After acquiring the certificate, the option can be updated to **Certificate Required**.

- Certificate Required**- Gateway uses the PKI certificate. Operators can change the certificate renewal time window for Gateways using the system property `gateway.certificate.renewal.window`. If you change the mode from **Certificate Required** to:
 - Certificate Deactivated**: All peers with RSA tunnel are disconnected and cannot reconnect. All peers configured with PSK mode continue to stay active and no disruption is seen in the traffic.
 - Certificate Acquire**: All peers configured in PSK mode reconnect with Hub/ Gateway. All current RSA tunnels stay active.

 **Note:**

- When Gateway certificate is revoked, the Gateway does not receive certificate revocation list (CRL) as it loses TLS connection immediately. Anyway, the Gateway is still operable.
- The current QuickSec design checks CRL time validity. The CRL time validity must match with current time of Edges for the CRL to have impact on new established connection. To implement this, ensure to update Orchestrator time properly to match with date and time of Edges.

Option	Description								
IP Address	<p>Displays the public IP address that public WAN links of an Edge use to connect to the Gateway. This IP address is used to uniquely identify the Gateway. If you have configured the Gateway with both IPv4 and IPv6 addresses, this field displays both the IP addresses. If you have created IPv4 only Gateway or if there is an existing IPv4 Gateway upgraded from previous versions, you can enter the IPv6 address to support the dual stack. After you save the changes, the IPv6 address is not sent to the Edges immediately. You can trigger the rebalance operation to push the IPv6 address to the customer and the associated Edges manually or the IPv6 address is sent to the Edges during the next Control Plane update.</p> <div style="border: 1px solid #0070C0; padding: 5px; margin-bottom: 5px;"> <p> Note: Adding IPv6 address is a one-time activity and once you save the changes, you cannot modify the IP addresses.</p> </div> <div style="border: 1px solid #0070C0; padding: 5px;"> <p> CAUTION: An incorrectly configured IPv6 address, when pushed to Edges, might lead to failure of the IPv6 tunnelling to the IPv6 Gateway. In such cases, you need to deactivate the Gateway and create a new one to activate both the IPv4 and IPv6 addresses.</p> </div>								
Contact & Location	Displays the existing contact details. If required, you can modify the information.								
NSD IP Portability	<p>Beginning with the 6.0 Orchestrator release, selecting this option will activate NSD IP Portability for the Gateway. Portable NSD IPs allow an Operators to move NSD configurations to different Gateways in the POP without requiring the customer to reconfigure their tunnels. When the NSD Portability check box is selected, the Orchestrator fetches the following data such as SASE PoP name, NSD Virtual IPv4 Address, and NSD Virtual IPv6 Prefix currently assigned to the Gateway from the Global Services Manager (GSM) and displays it. Select Refresh POP to retrieve the current and updated data.</p> <div style="border: 1px solid #0070C0; padding: 5px; margin-bottom: 5px;"> <p> Note: For the "NSD Portability" feature to work as designed, the Operators must ensure that the Gateways are associated with the corresponding PoPs in GSM.</p> </div>								
<p>Figure 15-10: Activate NSD IP Portability</p> <div style="border: 1px solid #ccc; padding: 10px; margin-bottom: 10px;"> <p>NSD IP Portability</p> <p>REFRESH POP</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td>NSD Portability</td> <td style="text-align: right;"><input checked="" type="checkbox"/> Enabled</td> </tr> <tr> <td>SASE PoP</td> <td style="text-align: right;">Hapy_Palo_Alto</td> </tr> <tr> <td>NSD Virtual IPv4 Address</td> <td style="text-align: right;">1.1.1.1</td> </tr> <tr> <td>NSD Virtual IPv6 Prefix</td> <td style="text-align: right;">2:2:2:2</td> </tr> </table> </div> <div style="border: 1px solid #FFD700; padding: 10px;"> <p> Important: There are two important caveats with NSD IP Portability:</p> <ol style="list-style-type: none"> a. NSD peers must operate as an IKE responder. In the past, some configurations would permit an initiator-only setup, but that will no longer function. b. Peers must allow NAT-T (NAT Traversal). The current implementation of NSD Portable IP uses NAT which is internal to the POP. </div>		NSD Portability	<input checked="" type="checkbox"/> Enabled	SASE PoP	Hapy_Palo_Alto	NSD Virtual IPv4 Address	1.1.1.1	NSD Virtual IPv6 Prefix	2:2:2:2
NSD Portability	<input checked="" type="checkbox"/> Enabled								
SASE PoP	Hapy_Palo_Alto								
NSD Virtual IPv4 Address	1.1.1.1								
NSD Virtual IPv6 Prefix	2:2:2:2								
Syslog Settings	Beginning with the 4.5 release, Gateways can export NAT information via a remote syslog server or via telegraf to the desired destination.								
Customer Usage	Displays the usage details of different types of Gateways assigned to the customers.								
Pool Membership	Displays the details of the Gateway pools to which the current Gateway is assigned.								
Partner Gateway (Advanced Handoff) Details	This section is available only if you select the Partner Gateway check box. You can configure advanced handoff settings for the Partner Gateway. For additional information, see the <i>Partner Gateway (Advanced Handoff) Details</i> section below.								

4. After configuring the required details, select **Save Changes**.

Partner Gateway (Advanced Handoff) Details

You can configure the following advanced handoff settings for the Partner Gateway:



CAUTION: It is recommended not to push IPv6 configurations to Partner Gateways that are running with Software version earlier than 5.0.

Table 49: Partner Gateway Handoff Field Descriptions

Option	Description
Static Routes Subnets	Specify the subnets or routes that the Gateway should advertise to the Edge. This is global per Gateway and applies to ALL customers. With BGP, this section is used only if there is a shared subnet that all customers need to access and if NAT handoff is required. Remove the unused subnets from the Static Route list if you do not have any subnets that you need to advertise to the Edge and have the handoff of type NAT. You can select the IPv4 or IPv6 tab to configure the corresponding address type for the Subnets.
Subnets	Enter the IPv4 or IPv6 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 handoff type as VLAN or NAT.
Description	Optionally, enter a descriptive text for the static route.
ICMP Probes and Ping Responders Settings	
ICMP Failover Probe – The Gateway uses ICMP probe to check for the reachability of a particular IP address and notifies the Edge to failover to the secondary Gateway if the IP address is not reachable. This option supports only IPv4 addresses.	
VLAN Tagging	Select the VLAN tag from the drop-down list to apply to the ICMP probe packets. The following are the available options: <ul style="list-style-type: none">• None – Untagged• 802.1q – Single VLAN tag• 802.1ad / QinQ(0x8100) / QinQ(0x9100) – Dual VLAN tag
Destination IP address	Enter the IP address to be pinged.
Frequency	Enter the time interval, in seconds, to send the ping request. The range is from 1 to 60 seconds.
Threshold	Enter the number of times the ping replies can be missed to mark the routes as unreachable. The range is from 1 to 10.
ICMP Responder - Allows the Gateway to respond to the ICMP probe from the next hop router when the tunnels are up. This option supports only IPv4 addresses.	
IP address	Enter the virtual IP address that will respond to the ping requests.
Mode	Select one of the following modes from the drop-down list: <ul style="list-style-type: none">• Conditional – Gateway responds to the ICMP request only when the service is up and when at least one tunnel is up.• Always – Gateway always responds to the ICMP request from the peer.



Note: The ICMP probe parameters are optional and recommended only if you want to use ICMP to check the health of the Gateway. With BGP support on the Partner Gateway, using ICMP probe for

failover and route convergence is no longer required. For additional information on configuring BGP support and handoff settings for a Partner Gateway, see [Configure Hand-off Operator](#).

15.2.3 Upgrade Orchestrator for Dual Stack Support

To upgrade **Orchestrator** to release 5.0.0 to support dual stack, perform the following:

1. Upgrade Orchestrator to release 5.0.0.
2. Add IPv6 address in Orchestrator Shell. The following example shows a sample configuration:

```
vcadmin@vco:~$ cat /etc/netplan/50-cloud-init.yaml network: ethernet: eth0: addresses:
[169.254.8.2/29, 'fd00:aaaa:0:1::2/64'] routes: - {metric: 1, to: 0.0.0.0/0, via: 169.254.8.1}
- {metric: 1, to: '0::0/0', via: 'fd00:aaaa:0:1::1'} renderer: networkd version: 2
```

3. In the **Operator** portal, navigate to **Administration > Operator Profiles**, and select a Profile.
4. In the **Operator Profiles** page of the selected Profile, navigate to the **Management Settings** section and enter the IPv6 address configured in Orchestrator Shell.

Figure 15-11: Configure Dual Stack Support

The screenshot shows the Orchestrator web interface. The top navigation bar includes 'Customers & Partners', 'Orchestrator', 'Gateway Management', 'Edge Image Management', and 'Administration'. The left sidebar shows 'Administration' with sub-items: 'Operator Events', 'Operator Profiles', and 'User Management'. The main content area is titled 'Operator profile R510' and shows 'Used by 0 Customers'. The 'Profile Settings' section includes a 'Name' field with the value 'Operator profile R510' and a 'Description' field with the placeholder 'Enter Description (Optional)'. Below this is the 'Management Settings' section, which is expanded to show a table of settings:

Management Settings			
Orchestrator Address	IP Address	Heartbeat Interval (s) *	30
Orchestrator IPv4 Address	169.254.8.2	Time Slice Interval (s) *	300
Orchestrator IPv6 Address		Stats Upload Interval (s) *	300

Below the table is the 'Gateway Selection' section, which includes a 'Gateway Mode' field with radio buttons for 'Dynamic' (selected) and 'Static'.

5. Select **Save Changes**.

15.2.4 Configure IPv6 Address on Gateways

Ensure that the **Orchestrator** is running version 5.0.0 as described in [Upgrade Orchestrator for Dual Stack Support](#).

You can provision a Gateway with both IPv4 and IPv6 addresses.

1. Deploy VeloCloud Gateway on AWS.
Consider the following guidelines while deploying Gateways on AWS.

- While migrating Gateways on cloud, it is recommended to destroy and create new instance of Gateways with the IPv6 option enabled.
 - When a VeloCloud Gateway is freshly deployed with a AWS c5.4xlarge instance type from the AWS portal with IPv6 option selected, it is required to only use the static mode of IPv4/IPv6 address assignment on interfaces for the Gateway because VeloCloud SD-WAN does not support DHCP on the Gateway side.
2. Setup IPv6 Address on Gateways for a new deployment.
 - a. Create a Gateway pool with IP version type as **IPv4 and IPv6**.
 - b. Deploy a new Gateway with version 5.0.0. You can configure IPv4 and IPv6 addresses on public interface using netplan, if IPv6 is not available in metadata.

The following example shows a sample configuration:

```
vcadmin@vcg2:~$ cat /etc/netplan/50-cloud-init.yaml network: ethernet: eth0: addresses:
[169.254.10.2/29, 'fd00:ff01:0:1::2/64'] routes: - {metric: 1, to: 0.0.0.0/0, via:
169.254.10.1} - {metric: 1, to: '0::0/0', via: 'fd00:ff01:0:1::1'} eth1: addresses:
[101.101.101.11/24] routes: - {metric: 2, to: 0.0.0.0/0, via: 101.101.101.10} eth2:
addresses: [192.168.0.111/24] renderer: networkd version: 2 vcadmin@vcg2:~$
```

- c. After updating the netplan, run **sudo netplan apply** to apply the configuration.

```
vcadmin@vcg2:~$ sudo netplan apply vcadmin@vcg2:~$
```

- d. Activate the Gateway using IPv4 address of the Orchestrator. If the Orchestrator is provisioned with dual stack, you can activate the Gateway using either IPv4 or IPv6 address of the Orchestrator. After activating, the Orchestrator will push both the IPv4 and IPv6 information to Edges.
 - e. Upgrade the Software version of Edge to version 5.0.0. Once the Edges are upgraded, the Orchestrator enables options to setup IPv6-related device settings.
3. Setup IPv6 Address on Gateways upgraded from the previous release.
 - a. Upgrade the Gateways to release 5.0.0.
 - b. In Gateway shell, update the netplan configurations with IPv6 address. The following example shows a sample configuration:

```
vcadmin@vcg2:~$ cat /etc/netplan/50-cloud-init.yaml network: ethernet: eth0: addresses:
[169.254.10.2/29, 'fd00:ff01:0:1::2/64'] routes: - {metric: 1, to: 0.0.0.0/0, via:
169.254.10.1} - {metric: 1, to: '0::0/0', via: 'fd00:ff01:0:1::1'} eth1: addresses:
[101.101.101.11/24] routes: - {metric: 2, to: 0.0.0.0/0, via: 101.101.101.10} eth2:
addresses: [192.168.0.111/24] renderer: networkd version: 2 vcadmin@vcg2:~$ vcadmin@vcg2:~$
sudo netplan apply vcadmin@vcg2:~$
```

- c. In the **Orchestrator** portal, navigate to the **Gateways** page and select the upgraded IPv4 Gateway.
- d. In the **Overview** page of the selected Gateway, under the **Status** section enter the IPv6 address configured in the Gateway Shell.

For additional information, see [Configure Gateways](#).

4. The **Orchestrator** will push the IPv6 configurations to the Edges.
5. Upgrade the Software version of Edge to version 5.0.0. Once the Edges are upgraded, the Orchestrator enables options to setup IPv6-related device settings.
6. You must rebalance Gateways at the Edge level or for the entire Enterprise Customer, for the Edges to get the IPv6 information of Gateway from Orchestrator.

For additional information, refer to the following topics:

- [Manage Gateways](#)
- [Manage Gateway Pools](#)
- [Manage Operator Profiles](#)

15.2.5 Partner Gateways

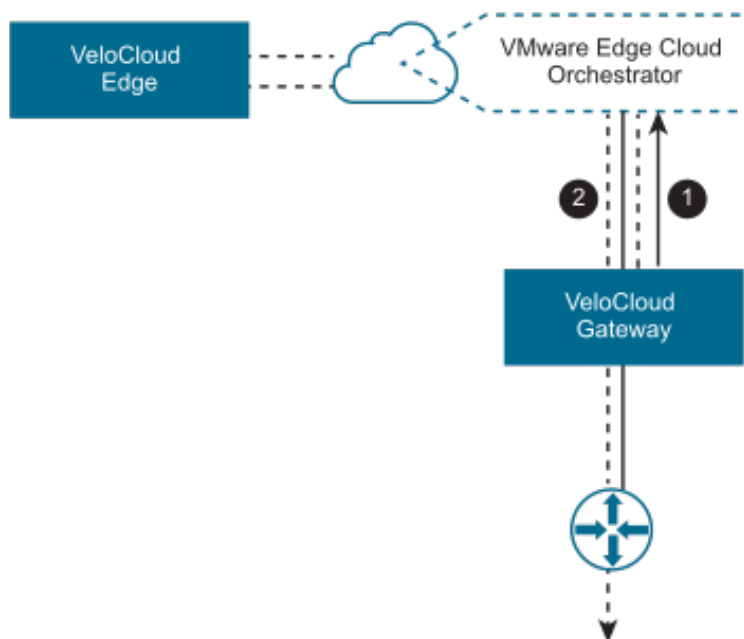
Partner Gateway can be configured with multiple subnets, each of which can be configured with a hand-off of NAT or VLAN. Each subnet can also be configured with a relative cost and whether the traffic should be encrypted or not.

The examples below illustrate two use cases for Partner Gateways configuration.

Gateway Configuration Use Case #1

In the following illustration, a Gateway is connected over VLAN/VRF mode to a VRF that has no access to the public Internet. However, the Partner Gateway must be able to contact the Orchestrator in the public cloud, and there must be a path to reach the cloud. The Gateway can selectively NAT certain traffic (such as the IP address of an Orchestrator, or the subnets used to reach public DNS servers) even though it is operating in VLAN/VRF mode.

Figure 15-12: Partner Gateway Configuration Use Case Topology 1



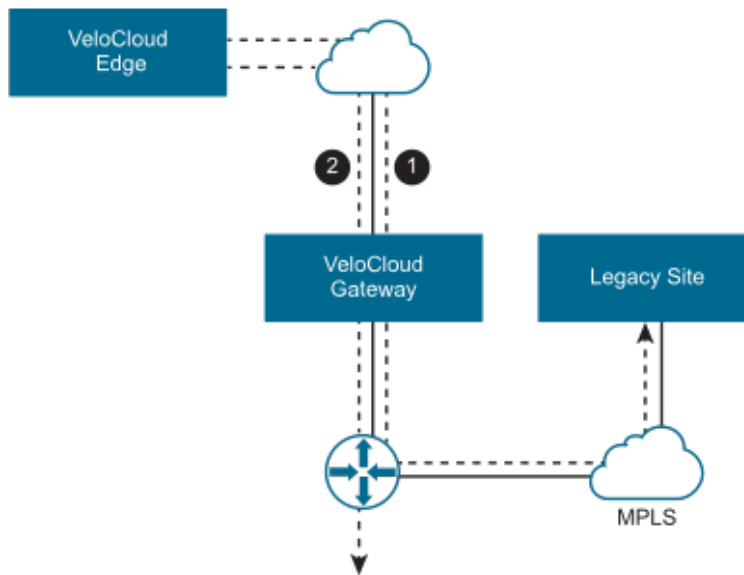
- #1- Orchestrator traffic is routed using IP addresses to NAT.
- #2- Corporate Traffic is routed through subnets to VLAN/VRF.

Gateway Configuration Use Case #2

It is common for a Partner Gateway to tie into a corporate network, providing connectivity to legacy sites. This need can occur even when not all corporate sites have been converted to Arista network. For this use case, it is necessary to specify traffic by subnet on the Partner Gateway. Each subnet can also be configured to encrypt network traffic.

The following illustration shows an example where only the traffic to legacy sites is encrypted. If the Gateway is already configured with a 0.0.0.0/0 subnet to allow all traffic (which is a common configuration), all that would be required is to add the private subnet for your legacy sites and mark it as encrypted.

Figure 15-13: Partner Gateway Configuration Use Case Topology 2



- #1- Subnet (e.g., 10.0.0.0/8) defined for Legacy Sites and marked for encryption. Traffic is transmitted between Edge and Gateway over the IPsec tunnel.
- #2- Remaining traffic is sent unencrypted to the Edge, and then to its final destination.

Note:



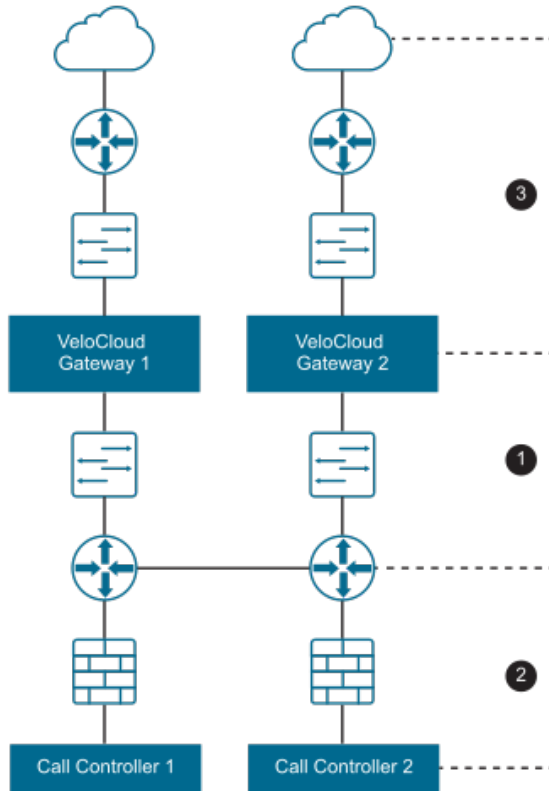
- For an IPsec tunnel via Partner Gateway, the VCMP tunnel failure causes the existing flows to timeout. The expected behavior for existing flows is to remain on the current path. Any new flow will begin to go (direct) causing the tunnel to remain down.
- Use application map flags `mustUseGateway` and `dropIfPartnerGatewayDown` to force or drop traffic through the Gateway until the path is restored. If these flags are not active, a flow flush is required once tunnel path is restored.

15.2.5.1 Partner Gateway Resiliency

The Partner Gateway provides resiliency by detecting failures and failing over to an alternate Partner Gateway. This includes the ability of a Partner Gateway to detect failure conditions and for the surrounding infrastructure to detect failures of the Gateway itself.

Consider the following Gateway topology:

Figure 15-14: Partner Gateway Topology



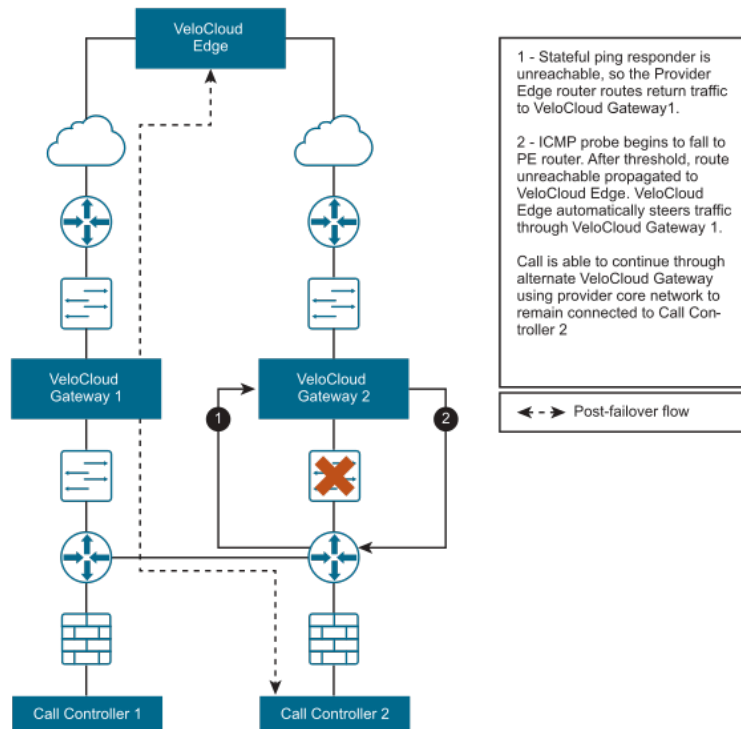
This figure shows three distinct failure zones:

Table 50: Gateway Failure Zones

Failure Zone	Component	Description
1	Provider Edge	The Provider Edge is one instance in which failure can be detected either from the Provider Edge router pinging the Gateway, or from the Gateway to the Provider Edge router.
2	Call Controller	The Gateway should be able to ping the Provider Edge router or Call Controller to verify connectivity.
3	WAN	The Gateway should have a stateful ping responder that responds only if the WAN zone is available.

The following figure shows a typical failure scenario that occurs between the Gateway and Provider Edge router and describes the activity that occurs.

Figure 15-15: Partner Gateway Failure Scenario



The Partner Gateway also supports configurable route costs to allow for more flexible failure scenarios. Finally, there is an additional hand-off type required where neither NAT nor VLAN tags are applied to the packets and they are simply passed through to the Provider Edge router.

15.2.5.2 ICMP Failover Probes

This section discusses ICMP failover probes.

In order to address a failure in zones #1 or #2 of the Gateway topology diagram, the Gateway supports the optional ability to send failover probes. These probes will ping a single destination IP address at the specified frequency. If the threshold for successive missed ping replies is exceeded, the VeloCloud Gateway will mark the Gateway's routes as unreachable. While the routes are marked as unreachable due to this probe failure state, probes continue to be sent. If the same threshold is exceeded for successive successful pings replies, the Gateway will mark the routes as reachable again.

Example Scenario

For example, consider the case in which a user has configured a frequency of two seconds and a threshold of three.

1. VeloCloud Edges connect to the primary Gateway. The primary Gateway marks routes as reachable.
2. The Primary Gateway fails to receive a reply for three successive probes (~6 seconds).
3. The Primary Gateway marks routes as unreachable and communicates this to all connected Edges.

4. Edges begin routing Gateway traffic via the alternate Gateway.
5. Connectivity is restored and the primary Gateway receives three successive replies from probes.
6. The Primary Gateway marks routes as reachable and communicates this to all connected Edges.
7. Edges route traffic back through the primary Gateway.

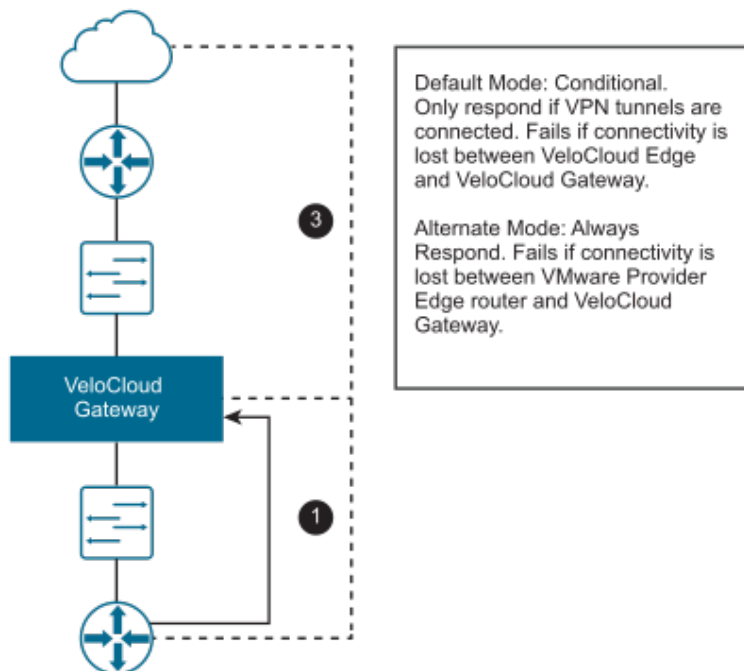
This could be used in failure scenario #1 to ping an IP address on the Provider Edge router itself. This could be used in failure scenario #2 to ping the actual Call Controller.

Stateful Ping Responder

To address a failure in zone #2 or #3 of the Partner Gateway topology diagram, the Gateway supports an optional stateful ping responder. This allows the configuration of a virtual IP address (which must be different from the interface IP address) within the Gateway that will, based on configuration, either respond to pings always (Gateway service is running) or conditionally based on WAN connectivity (the Gateway has VPN tunnels connected).

This can be used in failure scenario #1 by having the Provider Edge router ping the ping responder, as the Gateway becoming unreachable would cause the IP SLA on the Provider Edge router to fail. This could also be used in failure scenario #3 by having the Gateway only respond if VPN tunnels are connected- this is similar to the behavior with BGP (no clients connected means no client routes).

Figure 15-16: ICMP Failover Probes Scenario



The Partner Gateway will respond back to the Provider Edge (PE) router ICMP request based on the IP SLA configured in the PE router. The Stateful Ping Responder PE router should be configured as shown below with proper VLAN tag information.

```
!IP-SLA configuration to send ICMP request to gateway virtual IP ip sla 1 icmp-echo 192.168.10.10
source-ip 192.168.10.1 vrf CUSTOMER1 threshold 1000 timeout 1000 frequency 2 ip sla schedule
1 life forever start-time now !tracking the IP SLA for its reachability track 1 ip sla 1
```

```

reachability !all the routes will reachable only when SLA probe succeeds ip route vrf CUSTOMER1
0.0.0.0 0.0.0.0 192.168.11.101 track 1 ip route vrf CUSTOMER2 0.0.0.0 0.0.0.0 192.168.12.101
track 1 ip route vrf CUSTOMER1 10.0.0.0 255.0.0.0 192.168.10.10 track 1 ip route vrf CUSTOMER2
10.0.0.0 255.0.0.0 192.168.10.10 track 1 ip route vrf CUSTOMER1 192.168.100.0 255.255.255.0
192.168.10.10 track 1

```

Caveats When Using NAT Hand-off Mode

When using NAT hand-off mode, consider the following caveats:

- For VLAN hand-off mode, the Partner Gateway can listen on any IP if it is reachable to the PE router (including its interface IP). For NAT hand-off mode, the Partner Gateway will not respond if the ICMP request comes to its own interface (WAN) IP address.
- Reverse flow is not supported in the NAT hand-off mode.

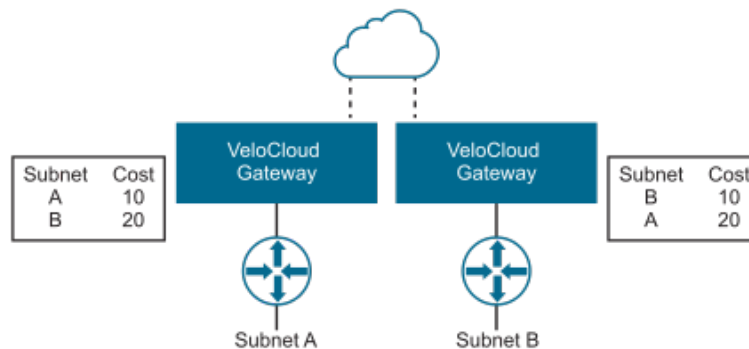
15.2.5.3 Active/Backup Subnets

This section describes how to configure active and backup subnets for a Partner Gateway.

Subnets on a Partner Gateway

Subnets configured on a Partner Gateway are input as subnets and optional descriptions. A Cost field is included to allow for weighting between routes. Lower-cost routes are preferred over higher-cost routes. The following figure shows Cost settings per subnet.

Figure 15-17: Cost Settings Per Subnet on a Partner Gateway



15.2.6 Monitor Gateways

You can monitor the status and network usage data of Gateways available in the **Operator** portal.

To monitor the Gateways:

1. In the **Operator** portal, select **Gateway Management > Gateways**.

- The **Gateways** page displays the list of available Gateways.

Figure 15-18: Gateways Screen

	Name	Status	CPU	Memory	Edges	Service State	IP Address	Location
<input type="checkbox"/>	gateway-1	Connected	38.81%	65.1%	5 View	In Service	20.0.1.2 fd00:ff01:0:1:2	San Francisco, US
<input type="checkbox"/>	gateway-2	Connected	22.09%	65.1%	5 View	In Service	20.0.2.2 fd00:ff02:0:1:2	Palo Alto, US
<input type="checkbox"/>	N-CA (dev)	Offline			0 View	In Service	54.215.193.206	
<input type="checkbox"/>	SIN (dev)	Offline			0 View	In Service	54.254.157.221	

- Select **Map Distribution** to expand and view the locations of the Gateways in the Map. By default, this view is collapsed.
- You can also select the arrows prior to each Gateways name to view more details. The page displays the following details:
 - Name** – Name of the Gateways.
 - Status** – Current status of the Gateways. The status may be one of the following: Connected, Degraded, Never Activated, Not in Use, Offline, Out of Service, or Quiesced.
 - CPU** – Percentage of CPU utilization by the Gateways.
 - Memory** – Percentage of memory utilization by the Gateways.
 - Edges** – Number of Edges connected to the Gateways.
 - Service State** – Service state of the Gateways. The state may be one of the following: Historical, In Service, Out of Service, Pending Service, or Quiesced.
 - IP Address** – The IP Address of the Gateways.
 - Location** – Location of the Gateways.
- In the **Search** field, enter a term to search for specific details. Select the **Filter** icon to filter the view by a specific criterion.
- Select the **CSV** option to download a report of the Gateways in the CSV format.

7. Select the link to a Gateway to view the details of the selected Gateway.

Figure 15-19: View Gateway Overview

The screenshot displays the 'gateway-1' Overview page. At the top, there are tabs for 'Overview' and 'Monitor'. The 'Overview' tab is active. The page is organized into several sections:

- Properties:** Name: gateway-1; Description: Enter Description; Gateway Roles: Data Plane (checked), Control Plane (checked), Secure VPN Gateway (checked), Partner Gateway (unchecked), CDE (unchecked).
- Status:** Status: Connected; Service State: Out Of Service; Connected Edges: 0; Gateway Authentication Mode: Certificate Deactivated; IP Address: 20.0.12, fd00::f010:1:2.
- Contact & Location:** Contact Name: Super User; Contact Email: super@velocloud.net; Contact Phone: ; Location: Palo Alto, US (Lat, Lng: 37.4, -122.142).
- Customer Usage:** A table with columns for Customer, Pool, and Gateway Type. It shows 'No customers found for this gateway'.
- Pool Membership:** A table with columns for Pool, Gateway, and Used By (Customers). It shows one entry: Pool: S-site-GatewayPool, Gateway: 2, Used By (Customers): 1.

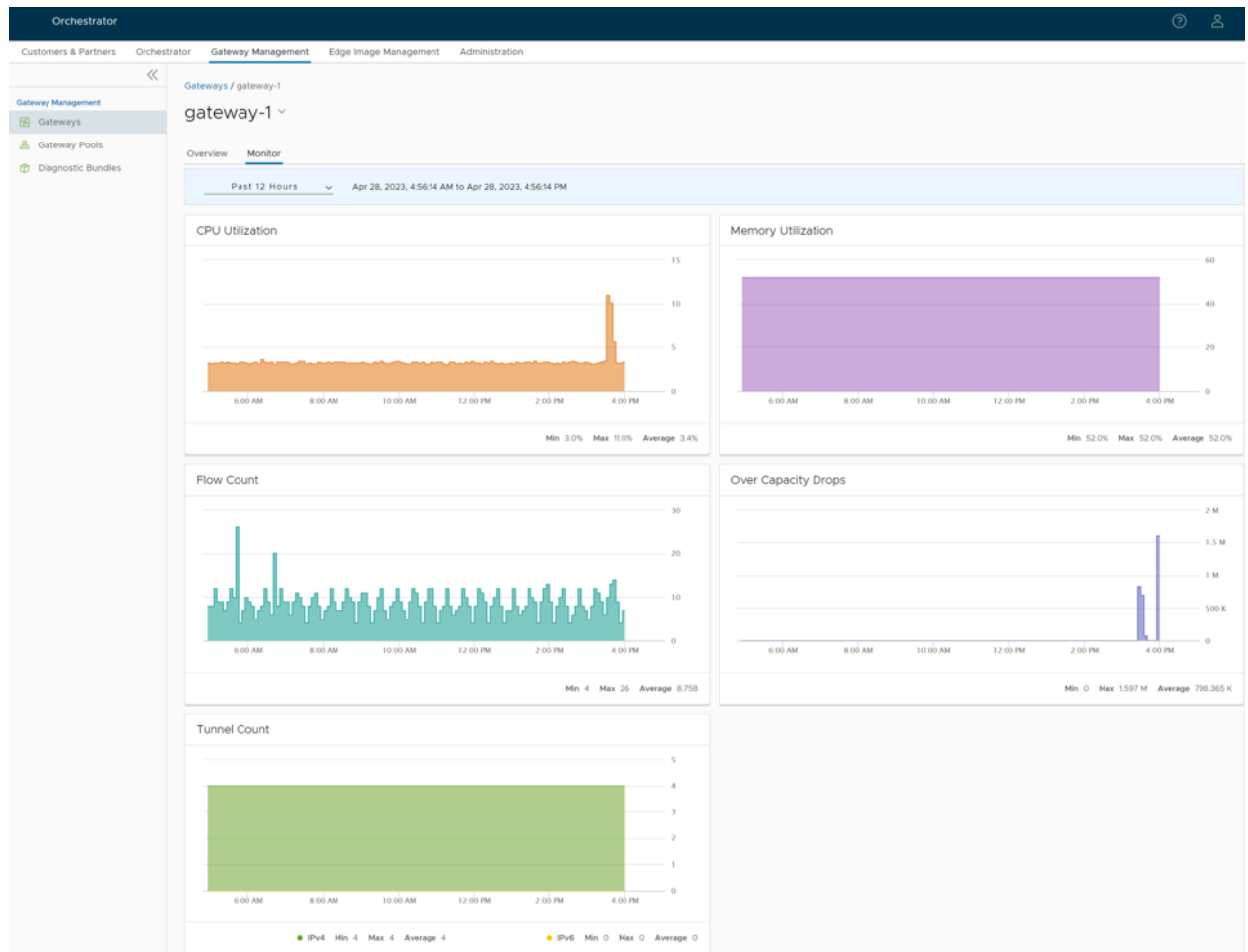
The **Overview** tab displays the properties, status, location, customer usage, and Gateway Pool of the selected Gateway.



Note: In the **Overview** tab, you can modify the **Name** and **Description** of the selected Gateway, and choose a different **Service State**. To configure the other options, navigate to the **Gateways** page in the Operator portal.

8. Select the **Monitor** tab to view the usage details of the selected Gateways.

Figure 15-20: Monitor Network Usage of Gateways



At the top of the page, you can choose a specific time period to view the details of the Gateway for the selected duration.

The page displays graphical representation of usage details of the following parameters for the period of selected time duration, along with the minimum, maximum, and average values.

- **CPU Percentage** – Percentage of usage of CPU.
- **Memory Usage** – Percentage of usage of memory.
- **Flow Counts** – Count of traffic flow.
- **Over Capacity Drops** – Total number of packets dropped due to over capacity since the last sync interval. Occasional drops are expected, usually caused by a large burst of traffic. However, a consistent increase in drops usually indicates a Gateway capacity issue.
- **Tunnel Count** – Count of tunnel sessions for both the IPv4 and IPv6 addresses.

Hover the mouse on the graphs to view additional details.

15.3 SD-WAN Gateway Migration

VeloCloud Orchestrator provides a self-service migration functionality that allows you to migrate from your existing Gateway to a new Gateway without your Operator's support.

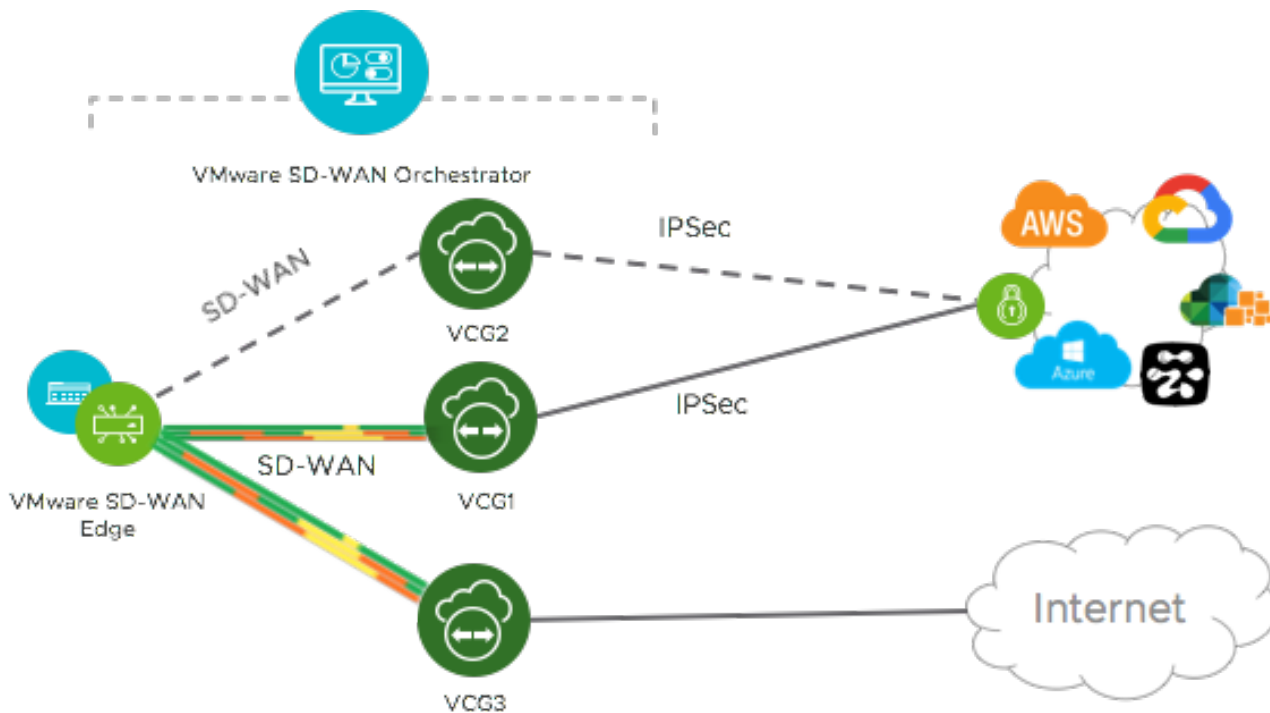
Gateway migration may be required in the following scenarios:

- Achieve operational efficiency.
- Decommission old Gateways.

Gateways are configured with specific roles. For example, a Gateway with data plane role is used to forward data plane traffic from source to destination. Similarly, a Gateway with Control Plane role is called a Super Gateway and is assigned to an Enterprise. Edges within the Enterprise are connected to the Super Gateway. Also, there is a Gateway with Secure VPN role that is used to establish an IPSec tunnel to a Non SD-WAN destination (NSD). The migration steps may vary based on the role configured for the Gateway. For additional information about the Gateway roles, see the "Configure Gateways" section in the *Arista VeloCloud SD-WAN Operator Guide*.

The following figure illustrates the migration process of the Secure VPN Gateway:

Figure 15-21: Secure VPN Gateway Migration Process

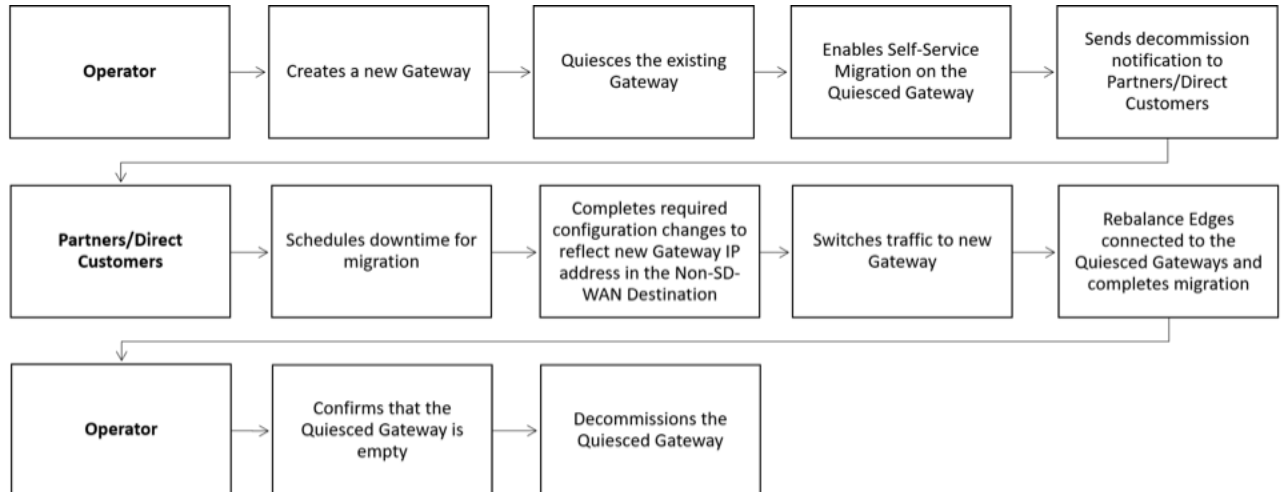


In this example, an SD-WAN Edge is connected to an NSD through a Secure VPN Gateway, VCG1. The VCG1 Gateway is planned to be decommissioned. Before decommissioning, a new Gateway, VCG2 is created. It is assigned with the same role and attached to the same Gateway pool as VCG1 so that VCG2 can be considered as a replacement to VCG1. The service state of VCG1 is changed to Quiesced. No new tunnels or NSDs can be added to VCG1. However, the existing assignments remain in VCG1. Configuration changes with respect to the IP address of VCG2 are made in the NSD, an IPSec tunnel is established

between VCG2 and NSD, and the traffic is switched from VCG1 to VCG2. After confirming that VCG1 is empty, it is decommissioned.

Following is the high-level workflow of Secure VPN Gateway migration based on the User roles:

Figure 15-22: Secure VPN Gateway Migration Workflow



15.3.1 Limitations of VeloCloud Gateway Migration

Keep in mind the following limitations when you migrate your Gateways:

- Self-service migration is not supported on Partner Gateways.
- There will be a minimum service disruption based on the time taken to switch Non SD-WAN Destinations (NSDs) from the quiesced Gateway to the new Gateway and to rebalance the Edges connected to the quiesced Gateway.
- If the NSD is configured with redundant Gateways and one of the Gateways is quiesced, the redundant Gateway cannot be the replacement Gateway for the quiesced Gateway.
- During self-service migration of a quiesced Gateway, the replacement Gateway must have the same Gateway Authentication mode as the quiesced Gateway.
- For a customer deploying a NSD via Gateway where BGP is configured on the NSD, if the customer migrates the NSD to a different Gateway using the Self-Service Gateway Migration feature on the Orchestrator, the BGP configurations are not migrated and all BGP sessions are dropped post-migration.

In this scenario, the existing Gateway assigned to the NSD is in a quiesced state and requires migration to another Gateway. The customer then navigates to **Service Settings > Gateway Migration** on the Orchestrator and initiates the **Gateway Migration** process to move their NSD to another Gateway. Post-migration, the BGP Local ASN & Router ID information is not populated on the new Gateway and results in NSD BGP sessions not coming up with all routes being lost and traffic using those routes is disrupted until the user manually recreates all BGP settings.

This is a Day 1 issue and while the **Gateway Migration** feature accounts for many critical NSD settings, the NSD's BGP settings that are not accounted for, and their loss post-migration is an expected behavior.

Workaround: The migration of a Gateway should be done in a maintenance window only. Prior to the migration, the user should document all BGP settings and be prepared to manually reconfigure these settings post-migration to minimize impact to customer users.

15.3.2 Quiesce Gateways

When you choose to decommission a Gateway, you must change the Gateway to Quiesced state so that no new tunnels or NSDs can be configured on the Gateway. Ensure that you have Operator Super User role to quiesce Gateways.

Before you quiesce the existing Gateway, ensure that you create a new Gateway as a replacement. Assign the new Gateway with the same role and attach it to the same Gateway pool as the existing Gateway. For instructions, see the “Configure Gateways” section in the *VeloCloud SD-WAN Operator Guide*. Also, review the [Limitations of VeloCloud Gateway Migration](#) before you proceed with quiescing the Gateway.



Note: Arista recommends you to use the self-service migration feature for NSD Gateway migration.

To quiesce the Gateway and enable self-service migration:

1. In the **Operator** portal, go to **Gateway Management**. The **Gateways** page lists the available Gateways.
2. Select the link of the Gateway that you want to quiesce. The details of the Gateway appears in the **Overview** tab.

Figure 15-23: Quiesce Gateways

The screenshot shows the Arista Orchestrator interface for managing a gateway. The main navigation bar includes 'Customers & Partners', 'Orchestrator', 'Gateway Management', 'Edge Image Management', and 'Administration'. The left sidebar shows 'Gateway Management' with sub-items: 'Gateways', 'Gateway Pools', and 'Diagnostic Bundles'. The main content area is titled 'gateway-1' and has two tabs: 'Overview' (selected) and 'Monitor'. The 'Overview' tab is divided into two sections: 'Properties' and 'Status'.
The 'Properties' section includes:
- Name: gateway-1
- Description: Enter Description
- Gateway Roles: Data Plane (checked), Control Plane (checked), Secure VPN Gateway (unchecked), Partner Gateway (unchecked), CDE (checked), Cloud Web Security (unchecked).
The 'Status' section includes:
- Status: Connected
- Service State: Quiesced (highlighted with a red box)
- Enable Self-Service Migration: checked
- New Gateway: gateway-5
- Migration Deadline: 05/31/2023
- Connected Edges: 5
- Gateway Authentication Mode: Certificate Deactivated
- IP Address: 20.1.0.2, fd00:ff01:0:1:2

3. In the **Status** section, from the **Service State** drop-down menu, select **Quiesced**.
4. Select the **Enable Self-Service Migration** check box.
5. From the **New Gateway** drop-down list, select the Gateway that you have created as a replacement to the Gateway that you are quiescing.

- In the **Migration Deadline** date picker, select a date by when you want the Partners or direct customers to complete the migration. Ensure that the date is within 60 days from the current date.
- Select **Save Changes**.

In the **Gateways** page, you can see that the **Service State** of the Gateway has changed to **Quiesced**.

Send decommission notification to Partners and direct customers who are impacted. The notification email provides the migration deadline and detailed instructions on how to migrate the Edges and NSDs from the quiesced Gateway to the new Gateway.

A notification icon is displayed for customers and Partners who have one or more Gateways that are in Quiesced service state. Also, a notification icon is displayed for Edges that are connected to a quiesced Gateway.



Note: Decommission notification email is sent only to direct customers and not to Partners' customers.

15.3.3 Decommission Quiesced Gateways

Before you decommission the quiesced Gateways, ensure that there are no Edges or NSDs connected to the Gateway.

In case there are Partners or direct customers who have not yet migrated from the quiesced Gateways, follow-up with them to ensure that they migrate from the quiesced Gateway. Verify that the quiesced Gateway is empty and then decommission it.

To decommission a quiesced Gateway:

- In the **Operator** portal, go to **Gateway Management**. The **Gateways** page lists the available Gateways.
- Select the link of the Gateway that you want to decommission. The details of the Gateway appears in the **Overview** tab.

Figure 15-24: Decommission Quiesced Gateways

The screenshot shows the Orchestrator interface for Gateway Management. The breadcrumb trail is Customers & Partners > Orchestrator > Gateway Management > Edge Image Management > Administration. The left sidebar shows Gateway Management > Gateways. The main content area shows the details for gateway-1. The Overview tab is active. The Properties section shows Name: gateway-1, Description: Enter Description, and Gateway Roles: Data Plane (checked), Control Plane (checked), Secure VPN Gateway (unchecked), Partner Gateway (unchecked), CDE (checked), and Cloud Web Security (unchecked). The Status section shows Status: Connected, Service State: Out Of Service (highlighted with a red box), Connected Edges: 5, Gateway Authentication Mode: Certificate Deactivated, and IP Address: 20.10.2, f500:f101:0:1:2.

- From the **Service State** drop-down list, select **Out Of Service**.
- Select **Save Changes**.

Ensure that you remove the Gateway from the Gateway pool and delete the Gateway from Orchestrator.

15.4 Diagnostic Bundles for Gateways

Run diagnostics for Gateways to collect diagnostic bundles and packet capture files for troubleshooting purpose.

- [Request Diagnostic Bundles for Gateways](#)
- [Request Packet Capture Bundle for Gateways](#)

15.4.1 Request Diagnostic Bundles for Gateways

Diagnostic bundles allow users to collect all the configuration files and log files from a specific VeloCloud Gateway into a consolidated zipped file. The data available in the diagnostic bundles can be used for troubleshooting the Gateways.

As an Operator Super user and Operator Admin user, you can create, manage, download, and delete diagnostic bundles for Gateways created by both Operator and Partner users.



Note: Operator Business Specialist user and Operator IT support users can only view the generated Diagnostic bundles and download the CSV file.

To generate a new Diagnostic bundle:

1. In the **Operator** portal, select the **Gateway Management** tab and select **Diagnostic Bundles** in the left navigation pane.

The **Diagnostic Bundles** page appears with the existing diagnostic bundles.

2. To generate a new Diagnostic bundle, select **Request Diagnostic Bundle**.

3. In the **Request Diagnostic Bundle** dialog, configure the following details and select **Submit**.

Figure 15-25: Request Diagnostic Bundle Dialog

Request Diagnostic Bundle

Target gateway-1

Reason for Generation For troubleshooting purpose

Core Limit No Limit

CLOSE SUBMIT

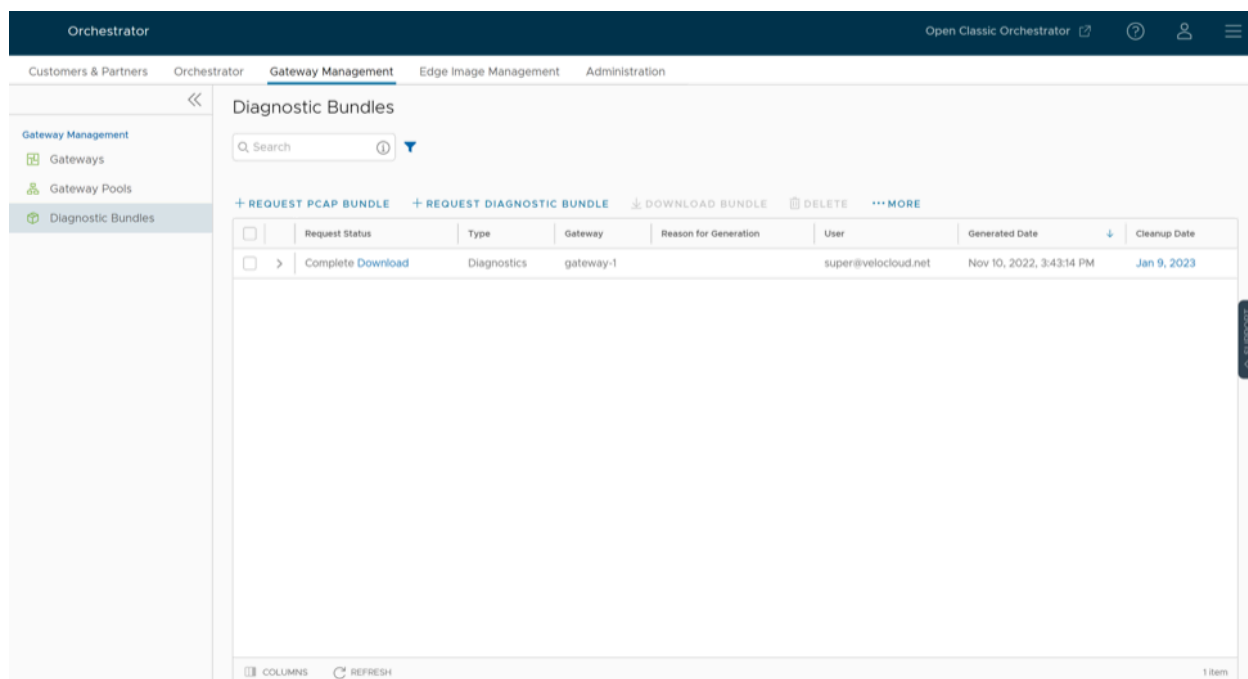
Table 51: Request Diagnostic Bundle Field Descriptions

Field	Description
Target	Select the target Gateway from the drop-down list. The data is collected from the selected Gateway.
Reason for Generation	Optionally, you can enter your reason for generating the bundle.
Core Limit	Select a Core Limit value from the drop-down, which is used to reduce the size of the uploaded bundle when the Internet connectivity is experiencing issues.

The **Diagnostic Bundles** page displays the details of the bundle being generated, along with the status.

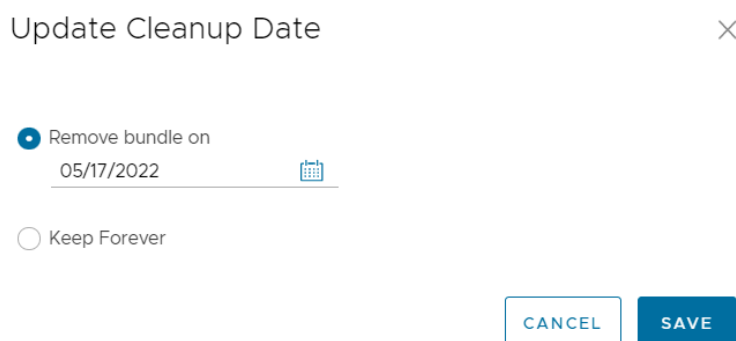
To search a specific diagnostic bundle, enter a relevant search text in the **Search** box. For advanced search, select the filter icon next to the **Search** box to filter the results by specific criteria.

Figure 15-26: Diagnostic Bundles Screen



4. You can download the generated Diagnostic bundles to troubleshoot an Edge.
5. To download a generated bundle, select the link next to **Complete** in the **Request Status** column or select the bundle and select **Download Bundle**. The bundle is downloaded as a ZIP file.
You can send the downloaded bundle to a Arista Support representative for debugging the data.
6. The completed bundles get deleted automatically on the date displayed in the **Cleanup Date** column. You can select the link to the **Cleanup Date** or choose the bundle and select **More > Update Cleanup Date** to modify the Date.

Figure 15-27: Update Cleanup Date Dialog



- a. In the **Update Cleanup Date** dialog, choose the date on which the selected Bundle would be deleted.
- b. If you want to retain the Bundle, select the **Keep Forever** check box, so that the Bundle does not get deleted automatically.

- c. To delete a bundle manually, select the bundle and select **Delete**.

15.4.2 Request Packet Capture Bundle for Gateways

The Packet Capture bundle collects the packets data of a network. These files are used in analyzing the network characteristics. You can use the data for debugging the network traffic and determining network status.

As an Operator Super user and Operator Admin user, you can create, manage, download, and delete Packet Capture (PCAP) bundles for Gateways created by both Operator and Partner users.



Note: Operator Business Specialist user and Operator IT support users can only view the generated PCAP bundles and download the CSV file.

To generate a PCAP bundle:

1. In the **Operator** portal, select the **Gateway Management** tab and select **Diagnostic Bundles** in the left navigation pane.

The **Diagnostic Bundles** page appears with the existing diagnostic bundles.

2. To generate a new PCAP bundle, select **Request PCAP Bundle**.
3. In the **Request PCAP Bundle** dialog, configure the following details and select **Generate**.

Figure 15-28: Request PCAP Bundle Dialog

Request PCAP Bundle
×

All inputs are required unless otherwise indicated. A minimum of one filter should be defined.

Target

gateway-1

Connectivity

eth0

Duration

5 seconds

Reason for Generation


Optional

PCAP FILTERS
ADVANCED FILTERS

IP2	▼	is	10.0.0.0/32	×
IP2: Port 2	▼	is	80	×

+

Table 52: Request PCAP Bundle Field Descriptions

Field	Description
Target	Choose the target Gateway from the drop-down list. The packets are collected from the selected Gateway.
Connectivity	Choose an Interface or an Edge ID from the drop-down list. The packets are collected on the selected Interface or Edge associated to the Gateway.
Duration	Choose the time in seconds. The packets are collected for the selected duration. The default value is 5 seconds.
Reason for Generation	Optionally, you can enter your reason for generating the bundle.
PCAP Filters	<p>You can define PCAP filters by which you want to control the PCAP data to be generated by choosing the following options:</p> <ul style="list-style-type: none">• IP1- Enter an IPv4 address, or IPv6 address, or Subnet mask.• IP2- Enter an IPv4 address, or IPv6 address, or Subnet mask.• IP1:Port1- Enter a Port ID associated with IP1.• IP2:Port2- Enter a Port ID associated with IP2.• Protocol- Select a protocol from the list. <div data-bbox="667 835 1508 911" style="border: 1px solid #add8e6; padding: 5px;"><p> Note: If you choose to use the PCAP filtering capability then you must define at least one filter.</p></div>
Advanced Filters	You can define free form filters by which you want to control the PCAP data to be generated.

The **Diagnostic Bundles** page displays the details of the PCAP bundle being generated, along with the status.

4. To download a generated bundle, select the link next to **Complete** in the **Request Status** column or select the bundle and select **Download Bundle**. The bundle is downloaded as a ZIP file.
5. The completed bundles get deleted automatically on the date displayed in the **Cleanup Date** column. You can select the link to the **Cleanup Date** or choose the bundle and select **More > Update Cleanup Date** to modify the Date.
6. To delete a bundle manually, select the bundle and select **Delete**.

Platform and Modem Firmware and Factory Images

Operators can upload, modify, or delete Platform and Modem Firmware images for specific Edge devices and Factory images for all physical VeloCloud Edge devices from the Orchestrator.

1. In the **Operator** portal, select the **Edge Image Management** tab.
2. To upload a Firmware image, select **Firmware** on the left panel under **Edge Image Management**. To upload a Software image, select **Software** on the left panel under **Edge Image Management**.

Note: Operators can upload, modify, or delete the following firmware and factory images:

- Firmware Platform images for 6x0, 7x0, and 3x00 (3400/3800/3810) Edge device models
- Firmware Modem images for 510-LTE (Edge 510LTE-AE, Edge 510LTE-AP) and 610-LTE (Edge 610LTE-AM, Edge 610LTE-RW)
- Factory images for all physical VeloCloud Edge devices



For additional information about uploading/managing Firmware images, see [Manage Operator Profiles](#).

3. In the appropriate screen (Firmware or Software depending upon which option you have chosen), select the **+Upload Image** link and choose an image file (ZIP format, file size less than 200MB) to upload from your local storage.

Note: It is important that you update the software version first. Then, after completion, update the firmware (Platform or Modem) and the factory default. Do not update the software version, the firmware, and the factory default at the same time.



4. After the file is successfully attached, select the **Done** button in the **File Upload** dialog.

The Orchestrator UI validates the package and uploads it to the portal. You can upload multiple Firmware and Software images to the portal. The uploaded packages are displayed on the appropriate page (**Firmware Images** or **Software Images**) based on your chosen image type.



Note: When **Firmware** is selected, note the **Image Type** column which indicates if the image is **Platform Firmware** or **Factory Default**.

Figure 16-1: Manage Firmware Images

Firmware Image	Used By Profile	Image Type	Size	Version	Build Number	Target
edge-platformupdate-EDGE5X0-x86_64-1.2.0-1-R120-20210926-QA-3ec24f5900.zip	1	platformima...	14.40 MB	1.2.0	R120-20210926-QA-3ec24f5900	EDGE6X0
edge-imageupdate-EDGE5X0-x86_64-5.0.0-1-R500-2021007-DEV-2795570ea5.zip	1	factoryimage	167.13 MB	5.0.0	R500-2021007-DEV-2795570e...	EDGE500
edge-imageupdate-EDGE5X0-x86_64-5.0.0-1-R500-2021007-DEV-2795570ea5.zip	1	factoryimage	167.13 MB	5.0.0	R500-2021007-DEV-2795570e...	EDGE5X0
edge-imageupdate-EDGE5X0-x86_64-5.0.0-1-R500-2021007-DEV-2795570ea5.zip	1	factoryimage	167.13 MB	5.0.0	R500-2021007-DEV-2795570e...	EDGE6X0

- To modify a Firmware or Software image, select an image from the appropriate page (Firmware or Software), and then select **Modify Image**. The **Modify Image** pop-up window appears.

Figure 16-2: Modify Image Window

Modify Image [Close]

Name edge1-imageupdate-VC_VM_Sample

Description [Empty text area]

File Name edge-imageupdate-EDGE5X0-x86_64-4.2.1-10-R421-20210304-QA-e2b61fd67d.zip

Size 144.31 MB

Version 4.2.1 (build R421-20210304-QA-e2b61fd67d)

Device Category Edge

Target Edge 500

Upload Hash 1094d707001730dea363702be14a516a8c56abb4

Deprecated

[CANCEL] [MODIFY]

- You can update the Name and Description of the Firmware or Software image package, if needed.
- If necessary, select the **Deprecated** check box to deprecate the Firmware or Software image and select the **Modify** button. The deprecated Firmware or Software image is flagged and appears in the respective page (Firmware Images or Software Images).



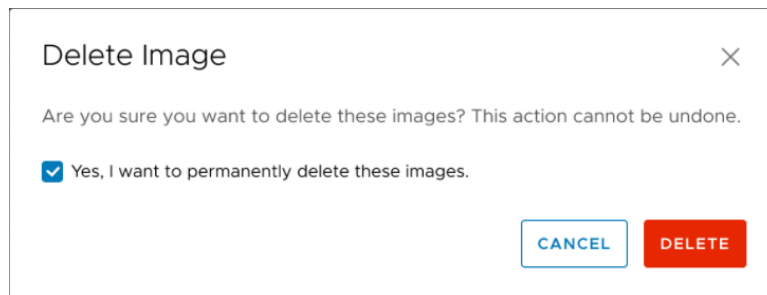
Note: The existing Operator Profiles that contain a deprecated image are also flagged to notify the user that the Firmware or Software version of the profile contains a deprecated software image.



Note: Once the image is deprecated, the image will not appear in the list of available firmware or software images, or versions to be assigned to Operator Profiles, or Customers or Edges.

8. To delete a package from the portal, select the image and select **Delete**.

Figure 16-3: Delete Image



To manage VeloCloud Edges within an Enterprise with a specific Software/Firmware image, see [Manage Operator Profiles](#).

Software Images

The Orchestrator portal allows Operator Super Users and Operator Standard Admins to manage the Software Images for the associated Edges.

As an Operator Super User, you can upload a new software image, modify the existing software images, and delete a software image associated with the Edges.

1. To upload a new software image, in the **Operator** portal, select **Services** at the top of the screen, and then select **Software** on the left side of the panel.

Figure 17-1: Manage Software Images

Software Image	Used By Profile	Size	Version	Build Number
edge-imageupdate-VC_VMDK-x86_64-4.2.2-223-R422-20220715-GA-8c452800b7.zip	1	137.6 MB	4.2.2	R422-20220715-GA-8c452800b7
edge-imageupdate-EDGE1000-x86_64-5.1.0.2-5827-R5102-20230310-GA-6ee0ca8b2d.zip	0	201.19 MB	5.1.0.2	R5102-20230310-GA-6ee0ca8b2d
edge-imageupdate-EDGE1000-x86_64-5.1.0.2-5827-R5102-20230310-GA-6ee0ca8b2d.zip	0	201.19 MB	5.1.0.2	R5102-20230310-GA-6ee0ca8b2d
edge-imageupdate-EDGE1000-x86_64-5.1.0.2-5827-R5102-20230310-GA-6ee0ca8b2d.zip	0	201.19 MB	5.1.0.2	R5102-20230310-GA-6ee0ca8b2d
edge-imageupdate-EDGE5XO-x86_64-5.1.0.2-5827-R5102-20230310-GA-6ee0ca8b2d.zip	0	199.81 MB	5.1.0.2	R5102-20230310-GA-6ee0ca8b2d
edge-imageupdate-EDGE5XO-x86_64-5.1.0.2-5827-R5102-20230310-GA-6ee0ca8b2d.zip	0	199.81 MB	5.1.0.2	R5102-20230310-GA-6ee0ca8b2d
edge-imageupdate-EDGE5XO-x86_64-5.1.0.2-5827-R5102-20230310-GA-6ee0ca8b2d.zip	0	199.81 MB	5.1.0.2	R5102-20230310-GA-6ee0ca8b2d
edge-imageupdate-VC_VMDK-x86_64-5.1.0.2-83770177-R5202-20230725-GA-6969b39047 (1).z...	1	175.35 MB	5.2.0.2	R5202-20230725-GA-6969b39047
edge-imageupdate-VC_VMDK-x86_64-5.4.0.0-97360204-R5400-20230915-GA-8b15963d67.zip	1	186.21 MB	5.4.0.0	R5400-20230915-GA-8b15963d67



Note: Starting from the 5.4.0 release, **Edge Image Management** is renamed to **Services**.

2. Select **Upload Image** and choose an Image file (ZIP format) to upload from your local storage. The Orchestrator validates the package and uploads it to the portal. You can upload multiple Software Images to the portal.
3. The uploaded packages are displayed in the **Software Images** page.
4. To modify an uploaded software image, select the link to the image name or select the image and select **Modify Image**. The **Modify Image** pop-up window appears.
5. You can update the Name and Description of the software image package, if needed.
6. Select the **Deprecated** check box to deprecate the software image and select **OK**. The deprecated software image is flagged and appears in the **Software Images** page.



Note: Once the image is deprecated, the image will not appear in the list of available software images or versions to be assigned to Operator Profiles, or Customers or Edges.



Note: The existing Operator Profiles that contain a deprecated image is also flagged to notify the user that the



Note: software version of the profile contains a deprecated software image.

7. To delete a package from the portal, select the image and select **Delete**.

To upgrade the Edges within an Enterprise with a specific Software Image, see [Manage Operator Profiles](#).

Edge Licensing

Only Operators can enable the Edge Licensing and assign the licenses to a Partner user. If the Edge Licensing is not enabled for you, contact your Operator.

The Edge Licensing feature is activated by default.

To deactivate Edge Licensing, in the **Operator** portal, go to **Orchestrator > System Properties**, and set the value of the system property `session.options.enableEdgeLicensing` to **False**.

The Edge Licenses are available with the following components:

Table 53: Edge Licensing Support Matrix

Component	Supported Attributes
Bandwidth	10M, 30M, 50M, 100M, 200M, 350M, 500M, 750M, 1G, 2G, 5G, 10G
Editions	Standard, Enterprise, Premium
Region	North America, Europe Middle East and Africa, Latin America, Asia Pacific
Term	12 months, 36 months, 60 months

An Operator can assign different types of Edge licenses from the 324 types of licenses available with various combinations.

Apart from the above list, Arista offers a trial version of license with the following attributes:

Table 54: Edge Licensing Trial Version

Component	Supported Attributes
Bandwidth	10 Gbps
Edition	POC
Region	North America, Europe Middle East and Africa, Asia Pacific and Latin America
Term	60 Months



Note: You can assign the **POC** license to a customer as a trial. When required, you can upgrade the license to any required Edition.

To access the Edge Licensing feature:

1. In the **Operator** portal, select **Services**, and then from the left menu, select **Edge Licensing**.



Note: Starting from the 5.4.0 release, **Edge Image Management** is renamed to **Services**.

Figure 18-1: Edge Licensing Screen

Edge Licensing

Q Search ⓘ ⌵

↓ DOWNLOAD REPORT

Name	Term	Bandwidth	Edition	Region	Partners Assigned	Customers Assigned	Edges Assigned	Activated Edges Count
ENTERPRISE 10 Mbps L...	60 Months	10 Mbps	Enterprise	North America, Europe...	0 VIEW	1 VIEW	0	0
ENTERPRISE 10 Mbps L...	12 Months	10 Mbps	Enterprise	Asia Pacific	0 VIEW	1 VIEW	0	0
ENTERPRISE 10 Mbps L...	36 Months	10 Mbps	Enterprise	Asia Pacific	0 VIEW	1 VIEW	0	0
ENTERPRISE 10 Mbps L...	60 Months	10 Mbps	Enterprise	Asia Pacific	0 VIEW	1 VIEW	0	0
ENTERPRISE 10 Mbps L...	12 Months	10 Mbps	Enterprise	Latin America	0 VIEW	1 VIEW	0	0
ENTERPRISE 10 Mbps L...	36 Months	10 Mbps	Enterprise	Latin America	0 VIEW	1 VIEW	0	0
ENTERPRISE 10 Mbps L...	60 Months	10 Mbps	Enterprise	Latin America	0 VIEW	1 VIEW	0	0
PREMIUM 10 Mbps N...	12 Months	10 Mbps	Premium	North America, Europe...	-	-	0	0

⌵ COLUMNS ↻ REFRESH

1 - 20 of 21 items | 1 / 2

2. You can view the following options on this page:

Table 55: Edge Licensing Option Descriptions

Option	Description
Search	Enter a term to search for a matching text across the table. You can select the advanced search option to use filters to narrow down the search results.
Download Report	Select this option to download a report of the licenses, associated customers, and Edges in a CSV format.
Columns	Select this option and select the columns to be displayed in the table.
Refresh	Select this option to refresh the displayed list of licenses.

3. Selecting the **View** link under the **Partners assigned** column, displays the Edge license details of the selected Partner.
4. Selecting the **View** link under the **Customers assigned** column, displays the Edge license details of the selected Customer.
- To assign Edge Licenses to new Partners, see [Create New Partner](#).
 - To manage and assign Edge Licenses to existing Partners, see [Manage Edge Licenses for Partners](#).
 - To assign Edge Licenses to new Customers, see [Create New Customer](#).
 - To manage and assign Edge Licenses to existing Customers, see [Manage Edge Licenses for Customers](#).

18.1 Manage Edge Licenses for Partners

An Operator can manage the Edge Licenses and assign them to Partners.

Following the below procedure to manage and assign Edge Licenses to existing partners. To assign Edge Licenses to new Partners, see [Create New Partner](#).

1. In the **Operator** portal, select **Manage Partners**.
2. Select the link to a Partner name to navigate to the **Partner** portal.
3. In the **Partner** portal, select **Edge Management**, and then from the left menu, select **Edge Licensing**.

Figure 18-2: Manage Edge Licenses for Partners

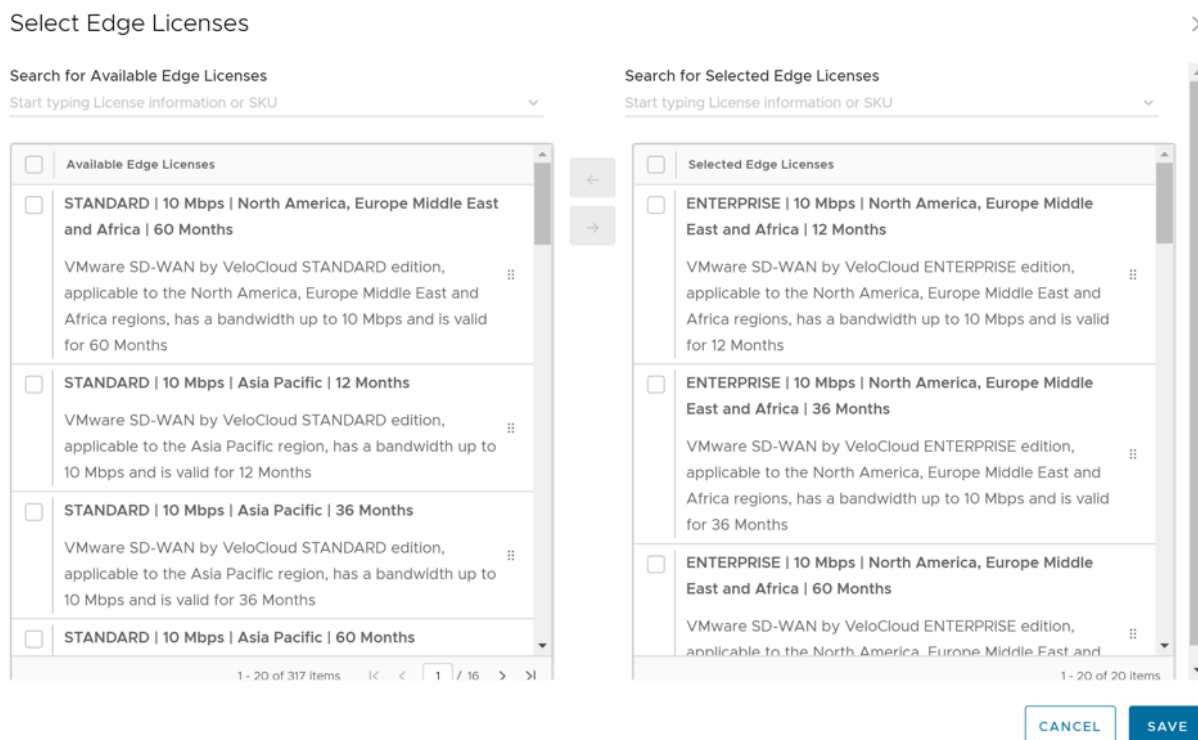
The screenshot shows the 'Edge Licensing' page in the Partner portal. The page has a top navigation bar with 'Monitor', 'Configure', 'Diagnostics', and 'Service Settings'. A left sidebar contains a menu with 'Alerts & Notifications', 'Edge Licensing' (selected), 'Gateway Migration', 'Edge Management', and 'Edge Auto-activation'. The main content area is titled 'Edge Licensing' and includes a search bar, a 'CSV' download button, and two links: 'MANAGE EDGE LICENSING' and 'DOWNLOAD REPORT'. Below these is a table with the following data:

Name	Term	Bandwidth	Edition	Region	Edges Assigned
STANDARD 10 Mbps North America, Europe Middle East and Africa 12 Months	12 Months	10 Mbps	Standard	North America, Europe, Middle East and Africa	1

At the bottom of the page, there are 'COLUMNS' and 'REFRESH' buttons, and a status indicator '1 - 1 of 1 items'.

4. Select **Manage Edge Licensing**.

Figure 18-3: Select and Assign Edge Licenses



5. In the **Select Edge Licenses** window, choose the relevant licenses based on the Bandwidth, Term, Edition, and Region.
6. Select **Save**.
The selected licenses are displayed in the **Edge Licensing** window.
7. Select **Download Report** to generate a report of the licenses along with the associated customers and Edges in a CSV format.

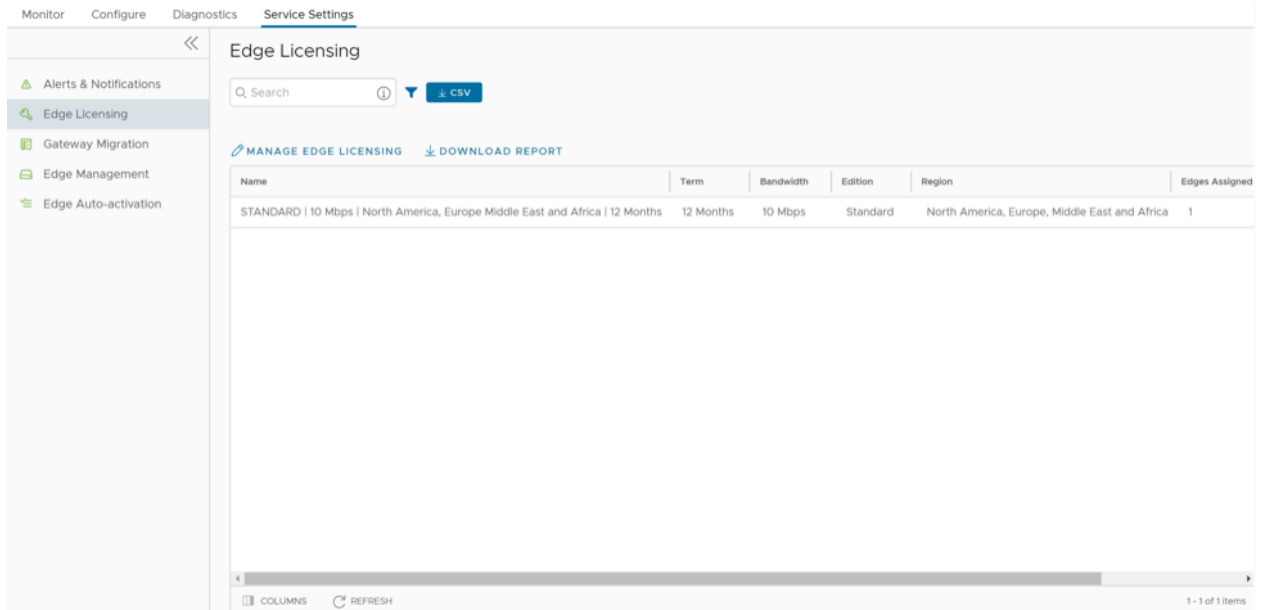
18.2 Manage Edge Licenses for Customers

An Operator can manage Edge Licenses and assign them to Customers.

1. In the **Operator** portal, select **Manage Customers**.
2. Select the link to a Customer name to navigate to the **Enterprise** portal.

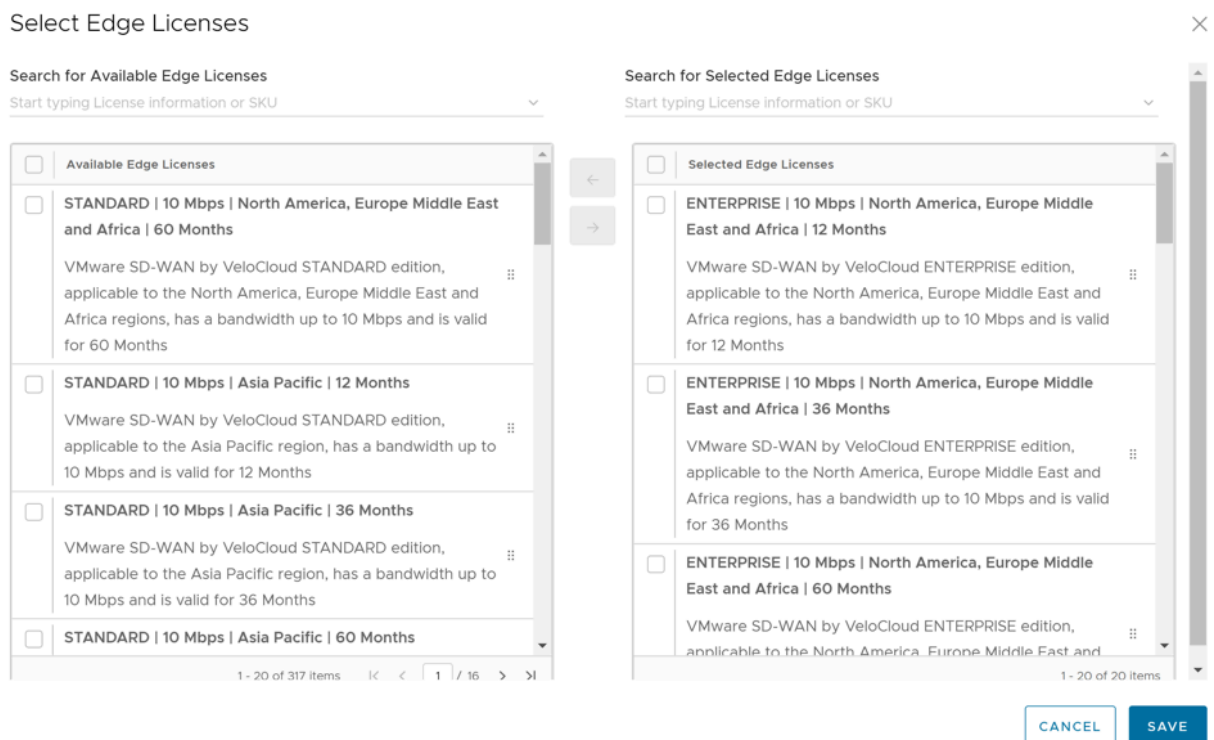
- In the **Enterprise** portal, select **Service Settings > Edge Licensing**.

Figure 18-4: Manage Edge Licenses for Customers



- Select **Manage Edge Licensing**.

Figure 18-5: Select and Assign Edge Licenses



- In the **Select Edge Licenses** window, choose the relevant licenses based on the Bandwidth, Term, Edition, Region, and then move them to the **Selected Edge Licenses** pane.



Note: Apart from the existing licenses, Arista offers a trial version of license with the Edition as **POC**. If you select a **POC** license, you cannot choose the other licenses.

6. Select **Save**. The selected licenses are displayed in the **Edge Licensing** window.



Note: If you have selected the **POC** license, you can select **Upgrade Edge License** to upgrade the license to the next level. Choose Standard, Enterprise or Premium Edition from the list. You cannot downgrade a License type to the previous Edition.

7. Select **Report** to generate a report of the licenses and the associated VeloCloud Edges in a CSV format.

When you create an Edge, you can choose and assign an Edge License from the drop-down list.

To assign a license to an existing Edge:

- In the **SD-WAN** service of the **Enterprise** portal, select **Configure > Edges**.
- To assign license to each Edge, select the link to the Edge, and then select the License in the **Properties** section of the **Edge Overview** page. You can also select the Edge, and then select **Assign Edge License** to assign the license.
- To assign a license to multiple Edges, select the appropriate Edges, select **Assign Edge License**, and then select the License.

Application Maps

The Application Maps are JSON files consisting of various Applications with definitions, which can be used while creating Business Policies.

From the **Operator** portal, select the **Services** tab, and then from the left navigation, select **Application Maps**. The following screen appears:

Figure 19-1: Manage Application Maps



Note: Starting from the 5.4.0 release, **Edge Image Management** is renamed to **Services**.

You can perform the following actions on this page:

- Upload Application Map
- Clone Application Map
- Refresh Application Map
- Push Application Map
- Edit Application Map
- Delete Application Map

Upload Application Map

VeloCloud SD-WAN provides an initial Application Map with possible applications. You can also upload your JSON file with Applications to be used in Business Policies.

- To upload a map file, select **Upload**.
- In the **File Upload** window, you can either drag and drop, or browse and choose the Application Map file to be uploaded.
- Select **Done**. The file is uploaded after the content is validated.

- The Application Map file is in JSON format and you can customize the applications as per your requirements. The following example illustrates a customized JSON file for the application bittorrent.

```
{ "id": 15, "name": "APP_BITTORRENT", "displayName": "bittorrent", "class": 14, "description"
: "BitTorrent is a peer-to-peer protocol. [Note: bittorrent is also known as kadmelia.]",
"knownIpPortMapping": {}, "protocolPortMapping": {}, "doNotSlowLearn": 1, "mustNotUseGateway":
1 }
```

Clone Application Map

You can create a new Application Map by cloning an existing Application Map.

- Select an existing Application Map, and then select **Clone**.
- In the **Clone Application Map** window, enter a new name and description for the Application.
- Select **Clone**.

Refresh Application Map

You can update the Application definitions, managed by third party SaaS providers, listed in the Application Map.

- Select one or more Application Maps, and then select **Refresh**. The **Refresh Application Maps** window appears, which lists the details of the selected Application Map(s) and Profile Count associated with the selected Application Map(s).
- Select **Refresh** to refresh the selected Application Map(s).



Note: The Application map Refresh operation serves to update application definitions managed by third party SaaS providers (for example Microsoft Office365®). It does not push those updates to associated Edges. After Refresh, use the Push function to update Edges assigned to a selected application map.

Push Application Map

You can push the latest updates of the Application definitions available in the Application Maps to the associated VeloCloud Edges.

- Select an Application Map, and then select **Push**.
- Select **Push to Edges** to update the latest Application definitions available in the selected Application Map.



Note: This option pushes the Application definitions only when any updates are available.



Important: When you change an application map and push those changes to the Edges from the Orchestrator, all Edge flows are flushed. This is done to ensure all Edge flows apply the updated version of the application map. As a result, you should only push an update to a custom application map in a maintenance window which minimizes disruption from an Edge flow flush.



Note: On Hosted Orchestrators, the Cloud Operations team updates and pushes all application maps on the first Saturday of each month. The application map refresh operation serves to update application definitions managed by third-party SaaS providers (for example, Microsoft 365). The updates and pushes are scheduled to minimize the disruption to customer traffic and are as follows:

Table 56: Push Application Map Definitions to Edges Scheduler

Region	Local Time	UTC Time	Day of the Month
Asia Pacific	02:00	18:00 UTC	1st Saturday of the month
Europe	02:00	00:00 UTC	1st Saturday of the month
North America	02:00	08:00 UTC	1st Saturday of the month

As noted earlier, an application map refresh and push will flush all flows for the Edges associated with that map and customers should anticipate this in the monthly maintenance window when it is performed.

Edit Application Map

You can add or update the application details available in the existing Application Maps.

- Select an Application Map, and then select **More > Edit** to edit the associated Application.
- Select **Add** to add a new application along with the ID. Update details like **Name**, **Display Name**, **Description**, **Category**, **TCP Ports**, **UDP Ports**, and **IP/Subnets**.
- Select **Delete** to delete the selected application.

- Select **Save Changes** to save the entered details.

Figure 19-2: Edit Application Map



Delete Application Map

You can delete a selected Application Map, but you cannot delete a map that has been assigned to an Operator profile.

- Select an Application Map and then select **More > Delete**.
- Enter the **Number of Application maps selected** and select **Delete**.

Edge Management

Edge Management feature allows you to configure general settings, authentication, and encryption for an Edge. It allows you to activate or deactivate configuration updates for an Edge. You can also select a default Software & Firmware Image.

1. In the **Operator** portal, on the **Monitor Customers** screen, select a Customer name.
2. From the top menu, select **Service Settings**, and then from the left menu, select **Edge Management**.
3. You can configure the following options and select **Save Changes**.

Figure 20-1: Edge Management

Edge Management

General Edge Settings

Edge Link Down Limit ⓘ Customize (default 1 day)
 Number of days

Edge Authentication

Default Certificate Certificate Acquire Certificate Deactivated Certificate Required

Edge Authentication ⓘ ACTIVATE SECURE EDGE ACCESS

Device Secret Encryption

Enable Encrypt Device Secrets ⓘ ENABLE FOR ALL EDGES

Configuration Updates

Enable Edge Configuration Updates On
When this option is set to on, configuration updates are actively pushed to Edges. When this option is turned off, pending configuration changes are paused until the setting is turned back on. Note: Edge configuration updates are disabled by default during Orchestrator upgrades.




Enable Configuration Updates Post-Upgrade Off
This option allows the customer to control when post-Orchestrator upgrade configuration changes are applied to their Edges. During an Orchestrator upgrade, the Operator managing the upgrade pauses all Edge configuration updates automatically, and after the upgrade the Operator resumes these Edge configuration updates. When this option is turned off, the customer prevents the Operator from automatically resuming Edge configuration updates after the Orchestrator is upgraded, and these Edge configuration updates would only resume once the customer turned this setting back on.

Software & Firmware Images

Is Default?	Operator Profile	Software & Firmware Images	Description	Used by
<input checked="" type="checkbox"/>	3-site-Operator	5.2.0.0 (build R5200-20230323-MH-feOc2...		0
<p>3-site-Operator</p> <p>Description:</p> <p>Software Image: 5.2.0.0 (build R5200-20230323-MH-feOc25d5f)</p> <p>Platform Firmware: None (do not update)</p> <p>Modem Firmware: None (do not update)</p> <p>Factory Image: None (do not update)</p> <p>ConfigurationType: Segment Based</p> <p>Orchestrator PGDN Address:</p> <p>Orchestrator IPv4 Address: 10.81.117.120</p> <p>Orchestrator IPv6 Address:</p> <p>Heartbeat Interval: 5 seconds</p> <p>Time Slice Interval: 30 seconds</p> <p>Stats Upload Interval: 30 seconds</p>				

1 - 1 of 1 items

Table 57: Edge Management- Options and Descriptions

Option	Description
General Edge Settings	
Edge Link Down Limit	You can set this value for each Edge by selecting the Customize check box. This overrides the value set through the system property <code>edge.link.show.limit.sec</code> .
Number of days	Enter a value in the range 1 to 365 . The default value is 1 .
Edge Authentication	
Default Certificate	<p>Choose the default option to authenticate the Edges associated to the Customer.</p> <ul style="list-style-type: none"> Certificate Acquire: This option 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 the establishment of VCMP tunnels. <div style="border: 1px solid #00a0e3; padding: 5px; margin: 5px 0;">  Note: Only after acquiring the certificate, the option can be updated to Certificate Required. </div> <ul style="list-style-type: none"> Certificate Deactivated: This option instructs the Edge to use a pre-shared key mode of authentication. Certificate Required: This option is selected by default, and it instructs the Edge to use the PKI certificate. Operators can change the certificate renewal time window for Edges using system properties. For additional information, contact your Operator. <div style="border: 1px solid #00a0e3; padding: 5px; margin: 5px 0;">  Note: On selecting Save Changes, you are asked to confirm if the selected Edge authentication setting is applicable to all the impacted Edges or only the new Edges. By default, Apply to all Edges check box is selected. </div>
Edge Authentication	Select the Activate Secure Edge Access button to allow the user to access Edges using Password-based or Key-based authentication. You can activate this option only once. But you can switch to either Password-based or Key-based authentication any number of times. For additional details, see Configure User Account Details .
Device Secret Encryption	
Enable Encrypt Device Secrets	Select the Enable For All Edges button to activate device secret encryption for all the Edges in the current Enterprise. This action causes restart of all the Edges. However, Edges which already have this feature activated are not affected.
<div style="border: 1px solid #00a0e3; padding: 5px; margin: 5px 0;">  Note: You can activate this option for individual Edges at the time of creating a new Edge. For additional information, see the topic <i>Provision a New Edge</i> in the <i>Arista VeloCloud SD-WAN Administration Guide</i>. </div>	
Configuration Updates	
Disable Edge Configuration Updates	By default, this option is activated. This option allows you to actively push the configuration updates to Edges. Slide the toggle button to turn it Off.
Enable Configuration Updates Post-Upgrade	By default, this option is deactivated. This option allows you to control when post-Orchestrator upgrade configuration changes are applied to their Edges. Slide the toggle button to turn it On.

4. **Software & Firmware Images:** To view this section, an Operator user must follow the below steps.
 - a. Navigate to the **Global Settings** service of the Enterprise portal.
 - b. Go to **Customer Configuration > SD-WAN Configuration**.
 - c. Select the **Allow Customer to manage software** check box.



Note: Only an Operator user can add, delete, or edit an image.

For additional information, see the topics [Platform and Modem Firmware and Factory Images](#) and [Software Images](#).

Access SD-WAN Edges Using Key-Based Authentication

This section discusses details about how to enable key-based authentication, add SSH keys, and access Edges in a more secure way.

The Secure Shell (SSH) key-based authentication is a secure and robust authentication method to access VeloCloud Edges. It provides a strong, encrypted verification and communication process between users and Edges. The use of SSH keys bypasses the need to manually enter login credentials and automates the secure access to Edges.

Note:



- Both the Edge and the Orchestrator must be using Release 5.0.0 or later for this feature to be available.
- Users with Operator Business or Business Specialist account roles cannot access Edges using key-based authentication.

Perform the following tasks to access Edges using key-based authentication:

1. Configure privileges for a user to access Edges in a secure manner.
You must choose **Basic** access level for the user. You can configure the access level when you create a new user and choose to modify it at a later point in time. Ensure that you have Superuser role to modify the access level for a user. For additional information, see [Add New User](#).
2. Generate a new pair of SSH keys or import an existing SSH key.
See [Add SSH Key](#)
3. Enable key-based authentication to access Edges.
See [Enable Secure Edge Access for an Enterprise Operator](#).

21.1 Add SSH Key

When using key-based authentication to access Edges, a pair of SSH keys are generated: Public and Private.

The public key is stored in the database and is shared with the Edges. The private key is downloaded to your computer, and you can use this key along with the SSH username to access Edges. You can generate only one pair of SSH keys at a time. If you need to add a new pair of SSH keys, you must delete the existing pair and then generate a new pair. If a previously generated private key is lost, you cannot recover it from the Orchestrator. You must delete the key and then add a new key to gain access. For details about how to delete SSH keys, see [Revoke SSH Keys](#).

Based on their roles, users can perform the following actions:

- All users, except users with Operator Business or Business Specialist account roles, can create and revoke SSH keys for themselves.

- Operator Super users can manage SSH keys of other Operator users, Partner users, and Enterprise users, if the Partner user and Enterprise user have delegated user permissions to the Operator.
- Partner Super users can manage SSH keys of other Partner users and Enterprise users, if the Enterprise user has delegated user permissions to the Partner.
- Enterprise Super users can manage the SSH keys of all the users within that Enterprise.
- Super users can only view and revoke the SSH keys for other users.



Note: Enterprise and Partners customers without SD-WAN service access will not be able to configure or view SSH keys related details.

To add a SSH key:

1. In the **Enterprise** portal, select the **User** icon that appears at the top-right side of the Window. The **User Information** panel appears.
2. Select **Add SSH Key**. The **Add SSH Key** pop-up window appears.
3. Select one of the following options to add the SSH key:
 - **Generate Key:** Use this option to generate a new pair of public and private SSH keys. Note that the generated key gets downloaded automatically. The default file format in which the SSH key is generated is `.pem`. If you are using a Windows operating system, ensure that you convert the file format from `.pem` to `.ppk`, and then import the key. For instructions to convert `.pem` to `.ppk`, see <https://puttygen.com/convert-pem-to-ppk>.
 - **Import Key:** Use this option to paste or enter the public key if you already have a pair of SSH keys.
4. In the **PassPhrase** field, you can choose to enter a unique passphrase to further safeguard the private key stored on your computer.



Note: This is an optional field and is available only if you have selected the **Generate Key** option.

5. In the **Duration** drop-down list, select the number of days by when the SSH key must expire.
6. Select **Add Key**.

Ensure that you enable secure Edge access for the Enterprise and switch the authentication mode from Password-based to Key-based. See [Enable Secure Edge Access for an Enterprise Operator](#).

21.2 Revoke SSH Keys

Ensure that you have Super User role to delete the SSH keys for other users.

To revoke your SSH key:

1. In the **Orchestrator**, select the **User** icon that appears at the top-right side of the Window. The **User Information** panel appears.
2. Select **Revoke SSH Key**.

For Other Operator Users

To revoke the SSH keys of other Operator users:

1. In the **Operator** portal, go to **Orchestrator Authentication**.
2. In the **SSH Keys** area, select the SSH usernames for which you want to delete the SSH keys.
3. Select **Actions > Revoke SSH Key**.

The SSH keys for a user are automatically deleted when:

- You change the user role to Operator Business or Business Specialist because these roles cannot access Edges using key-based authentication.
- You delete a user from the Orchestrator.



Note: When a user is deleted or deactivated from the external SSO providers, the user can no longer access the Orchestrator. But the user's Secure Edge Access keys remain active until the user is explicitly deleted from the Orchestrator as well. Therefore, you must first delete the user from the IdP, before deleting from the Orchestrator.

21.3 Enable Secure Edge Access for an Enterprise

After adding the SSH key, you must switch the authentication mode from Password-based, which is the default mode to Key-based to access Edges using the SSH username and SSH key. The SSH username is automatically created when you create a new user.

To enable secure Edge access:

1. In the **SD-WAN** service of the **Enterprise** portal, go to **Service Settings > Edge Management**.
2. Select the **Enable Secure Edge Access** check box to allow the user to access Edges using Key-based authentication. Once you have activated Secure Edge Access, you cannot deactivate it.



Note: Only Operator users can enable secure Edge access for an Enterprise.

3. Select **Switch to Key-Based Authentication** and confirm your selection.



Note: Ensure that you have Super User role to switch the authentication mode.

Use the SSH keys to securely login to the Edge's CLI and run the required commands. See [Secure Edge CLI Commands](#).

21.4 Secure Edge CLI Commands

Based on the Access Level configured, you can run the following CLI commands:



Note: Run the `help <command name>` to view a brief description of the command.

Table 58: Secure Edge Commands

Commands	Description	Access Level = Basic	Access Level = Privileged
Interaction Commands			
help	Displays a list of available commands.	Yes	Yes
pagination	Paginates the output.	Yes	Yes
clear	Clears the screen.	Yes	Yes
EOF	Exits the secure Edge CLI.	Yes	Yes
Debug Commands			
edgeinfo	Displays the Edge's hardware and firmware information. For a sample output of the command, see edgeinfo .	Yes	Yes
seainfo	Displays details about the secure Edge access of the user. For a sample output of the command, see seainfo .	Yes	Yes
ping, ping6	Pings a URL or an IP address.	Yes	Yes
tcpdump	Displays TCP/IP and other packets being transmitted or received over a network to which the Edge is attached. For a sample output of the command, see tcpdump .	Yes	Yes
pcap	Captures the packet data pulled from the network traffic and prints the data to a file. For a sample output of the command, see pcap .	Yes	Yes
debug	Runs the debug commands for Edges. Run <code>debug-h</code> to view a list of available commands and options. For a sample output of one of the debug commands, see debug --dpmk_ports_dump .	Yes	Yes
diag	Runs the remote diagnostics commands. Run <code>diag -h</code> to view a list of available commands and options. For a sample output of one of the diag commands, see diag ARP_DUMP .	Yes	Yes
ifstatus	Fetches the status of all interfaces. For a sample output of the command, see ifstatus .	Yes	Yes
getwanconfig	Fetches the configuration details of all WAN interfaces. Use the logical names such as "GE3" or "GE4" as arguments to fetch the configuration details of that interface. Do not use the physical names such as "ge3" or "ge4" of the WAN interfaces. For example, run <code>getwanconfig GE3</code> to view the configuration details of the GE3 WAN interface. Run the <code>ifstatus</code> command to know the interface name mappings. For a sample output of the command, see getwanconfig .	Yes	Yes
Configuration Command			
setwanconfig	Configures WAN interfaces (wired interfaces only). Run <code>setwanconfig -h</code> to view configuration options.	Yes	Yes
Edge Actions Commands			
deactivate	Deactivates the Edges and reapplies the initial default configuration.	No	Yes
restart	Restarts the SD-WAN service.	No	Yes

Commands	Description	Access Level = Basic	Access Level = Privileged
reboot	Reboots the Edge.	No	Yes
shutdown	Powers off the Edge.	No	Yes
hardreset	Deactivates the Edges, restores the Edge's default configuration, and restores original software version.	No	Yes
edged	Activates or deactivates the Edge processes.	No	Yes
restartdhcpserver	Restarts the DHCP server.	No	Yes
Linux Shell Command			
shell	Takes you into the Linux shell. Type exit to return to the secure Edge CLI.	No	Yes

21.4.1 Sample Outputs

This section provides the sample outputs of some of the commands that can be run in a secure Edge CLI.

edgeinfo

```
o10test_velocloud_net:velocli> edgeinfo Model: vmware Serial: VMware-420efa0d2a6ccb35-9b
9bee2f04f74b32 Build Version: 5.0.0 Build Date: 2021-12-07_20-17-40 Build rev: R500-20211207-
MN-8f5954619c Build Hash: 8f5954619c643360455d8ada8e49def34faa688d
```

seainfo

```
o10test_velocloud_net:velocli> seainfo { "rootlocked": false, "seouserinfo": { "o2super_velo
cloud_net": { "expiry": 1641600000000, "privilege": "BASIC" } } }
```

tcpdump

```
o10test_velocloud_net:velocli> tcpdump -nnpi eth0 -c 10 reading from file -, link-type EN10MB
(Ethernet) 09:45:12.297381 IP6 fd00:1:1:2::2.2426 > fd00:ff01:0:1::2.2426: UDP, length 21
09:45:12.300520 IP6 fd00:ff01:0:1::2.2426 > fd00:1:1:2::2.2426: UDP, length 21 09:45:12.399077
IP6 fd00:1:1:2::2.2426 > fd00:ff01:0:1::2.2426: UDP, length 21 09:45:12.401382 IP6 fd00:ff01:0:1
::2.2426 > fd00:1:1:2::2.2426: UDP, length 21 09:45:12.442927 IP6 fd00:1:1:2::2.2426 >
fd00:ff01:0:1::2.2426: UDP, length 83 09:45:12.444745 IP6 fd00:ff01:0:1::2.2426 > fd00:1:1:2::2
.2426: UDP, length 83 09:45:12.476765 IP6 fd00:ff01:0:1::2.2426 > fd00:1:1:2::2.2426: UDP, length
64 09:45:12.515696 IP6 fd00:ff02:0:1::2.2426 > fd00:1:1:2::2.2426: UDP, length 21
```

pcap

```
o10test_velocloud_net:velocli> pcap -nnpi eth4 -c 10 The capture will be saved to file
o10test_velocloud_net_2021-12-09_09-57-50.pcap o10test_velocloud_net:velocli> tcpdump: listening
on eth4, link-type EN10MB (Ethernet), capture size 262144 bytes 10 packets captured 10 packets
received by filter 0 packets dropped by kernel
```

debug

```
o10test_velocloud_net:velocli> debug --dpdk ports_dump name port link ignore strip speed duplex
autoneg driver ge3 0 1 0 1 1000 1 1 igb ge6 4 0 2 1 0 0 1 ixgbe ge5 5 0 2 1 0 0 1 ixgbe ge4 1
0 2 1 0 0 0 igb sfp2 2 0 2 1 0 0 1 ixgbe sfp1 3 0 2 1 0 0 1 ixgbe net_vhost0 6 0 0 1 10000 1 0
net_vhost1 7 0 0 1 10000 1 0
```

diag

```
o10test_velocloud_net:velocli> diag ARP_DUMP --count 10 Stale Timeout: 2min | Dead Timeout: 25min
| Cleanup Timeout: 240min GE3 192.168.1.254 7c:12:61:70:2f:d0 ALIVE 1s LAN-VLAN1 10.10.1.137
b2:84:f7:c1:d3:a5 ALIVE 34s
```

ifstatus

```
o10test:velocli> ifstatus { "deviceBoardName": "EDGE620-CPU", "deviceInfo": [], "edgeActivated":
true, "edgeSerial": "HRPGPK2", "edgeSoftware": { "buildNumber": "R500-20210821-DEV-301514018f
\n", "version": "5.0.0\n" }, "edgedDisabled": false, "interfaceStatus": { "GE1": { "autonegotiat
ion": true, "duplex": "Unknown! (255)", "haActiveSerialNumber": "", "haEnabled": false,
"haStandbySerialNumber": "", "ifindex": 4, "internet": false, "ip": "", "is_sfp": false,
"isp": "", "linkDetected": false, "logical_id": "", "mac": "18:5a:58:1e:f9:22", "netmask":
"", "physicalName": "ge1", "reachabilityIp": "8.8.8.8", "service": false, "speed": "Unkn",
"state": "DEAD", "stats": { "bpsOfBestPathRx": 0, "bpsOfBestPathTx": 0 }, "type": "LAN" }, "GE2":
{ "autonegotiation": true, "duplex": "Unknown! (255)", "haActiveSerialNumber": "", "haEnabled":
false, ... .. } ] }
```

getwanconfig

```
o10test_velocloud_net:velocli> getwanconfig GE3 { "details": { "autonegotiation": "on", "driver":
"dppdk", "duplex": "", "gateway": "169.254.7.9", "ip": "169.254.7.10", "is_sfp": false,
"linkDetected": true, "mac": "00:50:56:8e:46:de", "netmask": "255.255.255.248", "password":
"", "proto": "static", "speed": "", "username": "", "v4Disable": false, "v6Disable": false,
"v6Gateway": "fd00:1:1:1::1", "v6Ip": "fd00:1:1:1::2", "v6Prefixlen": 64, "v6Proto": "static",
"vlanId": "" }, "status": "OK" }
```

Configure User Account Details

The **My Account** page allows you to configure basic user information, SSH keys, and API tokens. You can also view the current user's role and the associated privileges.

Ensure to configure privileges for a user to access Edges in a secure manner. You must choose **Basic** access level for the user. You can configure the access level when you create a new user (under User Management), and choose to modify it at a later point in time. Ensure that you have Superuser role to modify the access level for a user.

To access the **My Account** page, follow the below steps:

1. Select the **User** icon in the **Global Navigation** located at the top right of the screen. The **User Information** panel is displayed as shown below:

Figure 22-1: User Information

The screenshot displays the VMware Orchestrator interface. On the right, the **User Information** panel is open, showing the following details:

- Account:** Username: super@velocloud.net, Role: Operator Superuser
- Profile:** Name: Super User
- Buttons:** MY ACCOUNT, LOG OUT
- Footer:** Version: 5.4.0.0, Build: RS400-20230914-0655-GA-928cc4c19, Legal & Terms of Service, Cookie Usage, ©2023 VMware

The background shows the **Customers** dashboard. It features two donut charts: **Total Customers** (1) and **Total Edges** (10). A legend indicates 0 Down, 1 Up, and 0 Unactivated. Below the charts is a table with the following data:


Customer	# Down Edges	# Degraded Edges	# Connected Edges
5-site-cluster	-	-	10

2. Select the **My Account** button. The following screen appears:

Figure 22-2: Profile Tab

3. The **Profile** tab is displayed by default. You can update the following basic user details:

Table 59: Profile Tab- Options and Descriptions

Option	Description
Username	Displays the username and it is a read-only field.
Contact Email	Enter the primary contact email address of the user.
Current Password	Enter the current password.
New Password	Enter the new password.
	<div style="border: 1px solid black; padding: 5px;"> <p> Note: Starting from the 4.5 release, the use of the special character "<" in the password is no longer supported. In cases where users have already used "<" in their passwords in previous releases, they must remove it to save any changes on the page.</p> </div>
Confirm Password	Re-enter the new password.
First Name	Enter the first name of the user.
Last Name	Enter the last name of the user.
Phone	Enter the primary phone number of the user.
Mobile Phone	Enter the mobile number of the user along with the country code.

- Select the **Role** tab to view the existing user role and description. It also displays the privileges associated with the user role.

Figure 22-3: Role & Privileges tab

My Account

Profile **Role & Privileges** API Tokens SSH Keys

Role
Operator Superuser

Description
Can view, edit and create additional operators, global settings, and has full access across all services

Privileges associated to role

> Global Settings & Administration	✔ Global Settings Operator Superuser
> SD-WAN	✔ SD-WAN Operator Superuser
> Cloud Web Security	✔ Cloud Web Security Operator Superuser
> Secure Access	✔ Secure Access Operator Superuser
> Multi Cloud	✔ MCS Operator Superuser
> App Catalog	✔ App Catalog Operator Superuser

Privileges

Edge Access
Basic ⓘ

- Select the **API Tokens** tab. The following screen is displayed.

Figure 22-4: API Tokens tab

My Account

Profile Role & Privileges **API Tokens** SSH Keys

New Token

Name * test

Description test123

Lifetime * 12 Months

GENERATE KEY CANCEL

- Enter a **Name** and **Description** for the token, and then choose the **Lifetime** from the drop-down menu.
- Select **Generate Key**.
- Select the **SSH Keys** tab to configure a Secure Shell (SSH) key-based authentication.

The SSH key-based authentication is a secure and robust authentication method to access VeloCloud Edges. It provides a strong, encrypted verification and communication process between users and Edges. The use of SSH keys bypasses the need to manually enter login credentials and automates the secure access to Edges.

Note:



- Both the Edge and the Orchestrator must be using Release 5.0.0 or later for this feature to be available.
- Users with Operator Business or Business Specialist account roles cannot access Edges using key-based authentication.

When using key-based authentication to access Edges, a pair of SSH keys are generated- Public and Private.

The public key is stored in the database and is shared with the Edges. The private key is downloaded to your computer, and you can use this key along with the SSH username to access Edges. You can generate only one pair of SSH keys at a time. If you need to add a new pair of SSH keys, you must delete the existing pair and then generate a new pair. If a previously generated private key is lost, you cannot recover it from the Orchestrator. You must delete the key and then add a new key to gain access.

Based on their roles, users can perform the following actions:

- All users, except users with Operator Business or Business Specialist account roles, can create and revoke SSH keys for themselves.
- Operator Super users can manage SSH keys of other Operator users, Partner users, and Enterprise users, if the Partner user and Enterprise user have delegated user permissions to the Operator.
- Partner Super users can manage SSH keys of other Partner users and Enterprise users, if the Enterprise user has delegated user permissions to the Partner.
- Enterprise Super users can manage the SSH keys of all the users within that Enterprise.
- Super users can only view and revoke the SSH keys for other users.



Note: Enterprise and Partners Customers without SD-WAN service access are not able to configure or view SSH keys related details.

Select the **SSH Keys** tab, and then select the **Generate Key** button. The following screen appears:

Figure 22-5: SSH Keys tab

My Account ×

Profile Role & Privileges API Tokens SSH Keys

Generate SSH Key

User Name *
o2super_velocloud_net

Actions *
 Generate Key Enter Key

Enter Key


Duration * ⓘ
 30 Days

ⓘ The default file format is .pem (for use with OpenSSH). If you are using a Windows OS, ensure that you convert the file format from .pem to .ppk.

Table 60: SSH Keys Tab- Options and Descriptions

Option	Description
User Name	Displays the username and it is a read-only field.
Actions	<p>Select either one of the following options:</p> <ul style="list-style-type: none"> Generate key: Use this option to generate a new pair of public and private SSH keys. <div data-bbox="703 1077 1510 1224" style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;"> <p>Note: The generated key gets downloaded automatically. The default file format in which the SSH key is generated is .pem. If you are using a Windows operating system, ensure that you convert the file format from .pem to .ppk, and then import the key. For instructions to convert .pem to .ppk, see Convert Pem to Ppk File Using PuTTYgen.</p> </div> Enter key: Use this option to paste or enter the public key if you already have a pair of SSH keys.
PassPhrase	<p>If the Generate key option is selected, then you have to enter a unique passphrase to further safeguard the private key stored on your computer.</p> <div data-bbox="665 1434 1510 1507" style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;"> <p>Note: This is an optional field and is available only if you select the Generate Key action.</p> </div>
Duration	Select the number of days by when the SSH key must expire.

9. Select Generate Key.

 **Note:** Only one SSH Key can be created per user.

- 10.** To deactivate an SSH token, select the **Revoke** button. A pop-up window appears, to confirm the revoke operation. Select the check box, and then select **Revoke** to permanently revoke the key.

The SSH keys for a user are automatically deleted when:

- You change the user role to Operator Business or Business Specialist because these roles cannot access Edges using key-based authentication.
- You delete a user from the Orchestrator.



Note: When a user is deleted or deactivated from the external SSO providers, the user can no longer access the Orchestrator. But the user's Secure Edge Access keys remain active until the user is explicitly deleted from the Orchestrator as well. Therefore, you must first delete the user from the IdP, before deleting from the Orchestrator.

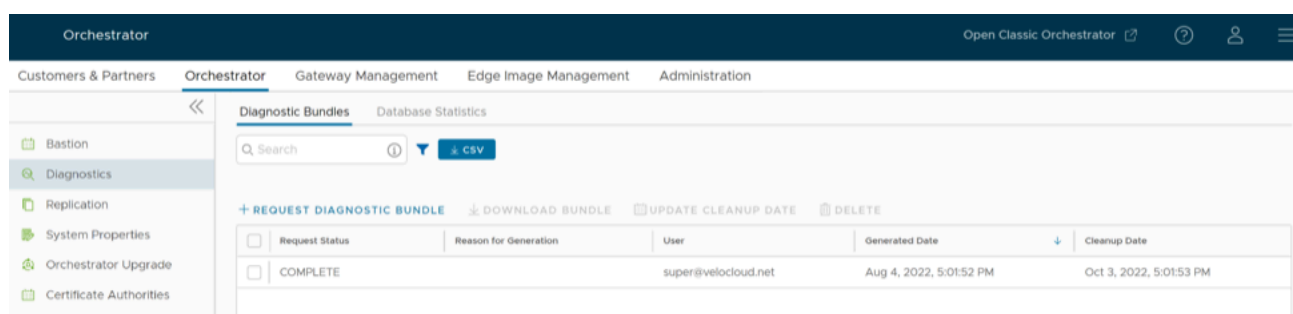
Ensure that you enable secure Edge access for the Enterprise and switch the authentication mode from Password-based to Key-based. See [Enable Secure Edge Access for an Enterprise](#).

Orchestrator Diagnostics

The Orchestrator Diagnostics bundle is a collection of diagnostic information to troubleshoot the Orchestrator. For Orchestrator on-prem installation, Operators can collect the Orchestrator Diagnostic bundle from the Orchestrator user interface and provide it to the Arista Support team for offline analysis and troubleshooting.

In the **Operator** portal, navigate to **Orchestrator > System Properties**, and then set the system property `session.options.enableBastionOrchestrator` to `True` to view the **Diagnostics** tab.

Figure 23-1: Configure Orchestrator Diagnostics



The following are the options available to troubleshoot Orchestrator Diagnostics:

- **Diagnostic Bundles:** Request and download a diagnostic bundle.
- **Database Statistics:** Provides read-only access view of some of the information from a diagnostic bundle.

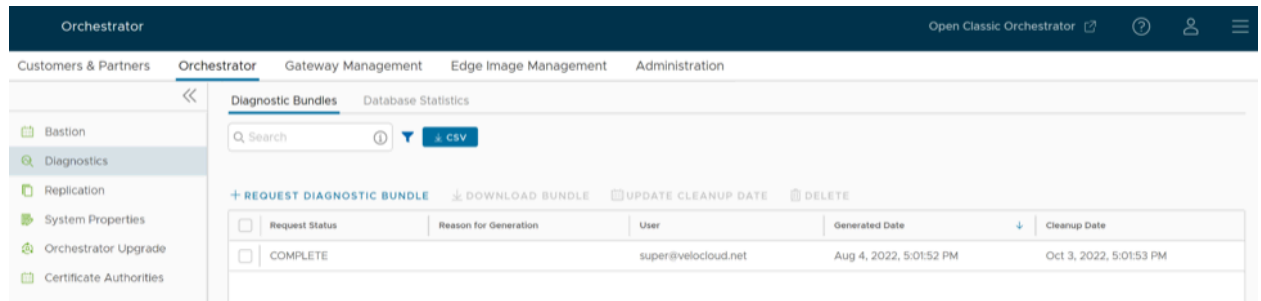
Diagnostic Bundles

To access the diagnostic bundles perform the following steps:

1. In **Operator** portal, select the **Orchestrator** tab.
2. In the left navigation pane, select **Diagnostics**.

The **Diagnostic Bundles** page appears with the existing diagnostic bundles.

Figure 23-2: Diagnostic Bundles



The **Orchestrator Diagnostics** table grid includes the following information:

Table 61: Orchestrator Diagnostics Field Descriptions

Field	Description
Request Status	<p>The following are the request status:</p> <ul style="list-style-type: none"> • Complete • In Progress <p>If a bundle has not completed the download, the In Progress status appears.</p>
Reason for Generation	The specific reason given for generating a diagnostic bundle. Select the Request Diagnostic Bundle button to include a description of the bundle.
User	The individual logged into the VeloCloud Orchestrator.
Generated	The date and time when the diagnostic bundle request was sent.
Update Cleanup Date	The default Cleanup Date is three months after the generated date, when the bundle will be automatically deleted. If you wish to extend the cleanup date, then select the bundle and then select this option to make the required changes. For additional information, see the Update Cleanup Date section below.

3. To generate a new Diagnostic bundle perform the following steps:
 - a. Select the **Request Diagnostic Bundle** button.

- b. In the **Request Diagnostic Bundle** dialog, enter the reason for generation.

Figure 23-3: Request Diagnostic Bundle

- c. Select **Submit**.

The **Diagnostic Bundles** page displays the details of the bundle being generated, along with the status.

To search a specific diagnostic bundle, enter a relevant search text in the **Search** box. For advanced search, select the **Filter** icon next to the **Search** box to filter the results by specific criteria.

4. To download a generated bundle, select the required check box in the **Request Status** column and select **Download Bundle**. The bundle is downloaded as a ZIP file.

You can send the downloaded bundle to a Arista Support representative for debugging the data.

5. The completed bundles get deleted automatically on the date displayed in the column called **Cleanup Date**. To update the cleanup date of a generated bundle, select the required check box in the **Request Status** column and select **Update Cleanup Date**.

In the **Update Cleanup Date** pop-up window, choose the date on which the selected bundles should be deleted and select **Update**.

Figure 23-4: Update Cleanup Date

Select the **Keep Forever** check box to retain the bundle, so that the bundle does not get deleted automatically.

The Orchestrator Diagnostics table grid updates to reflect the changes to the Cleanup Date.

6. To delete a bundle manually, select the required check box in the **Request Status** column and select **Delete**.

Database Statistics

The Database Statistics tab provides read-only access view of the information from a diagnostic bundle. To view it, select **Database Statistics** option available at the top of the window.

If you require additional information, go to the **Diagnostic Bundles** tab, request a diagnostic bundle, and download it locally.

Table 62: Database Statistics Field Descriptions

Field	Description
Database Sizes	Sizes of the Orchestrator databases.
Database Table Statistics	Statistical details of all tables in the Orchestrator database.
Database Storage Info	Storage details of the mounted locations.
Database Process List	The top 20 records of long-running SQL queries.
Database Status Variable	The status variables of the MySQL server
Database System Variable	System variables of the MySQL server.
Database Engine Status	The InnoDB engine status of the MySQL server.

Orchestrator Upgrade with New Orchestrator UI

This section discusses the prerequisites and steps required to upgrade a Orchestrator. Orchestrator allows you to configure and send a banner message about an upcoming Orchestrator upgrade. The banner is displayed to users the next time they login to the Orchestrator. You can customize the banner message and visibility for the users.

To upgrade a Orchestrator, perform the following steps:

1. Configure Orchestrator Upgrade Announcement
2. Prepare Orchestrator Upgrade
3. Complete Orchestrator Upgrade

1. Configure Orchestrator Upgrade Announcement

The **Upgrade Announcement** area enables you to configure and send a message about an upcoming upgrade. To send an Orchestrator Upgrade announcement, perform the following steps:

- a. In the **Operator** portal, select the **Orchestrator** tab, and go to **Orchestrator Upgrade** in the left navigation pane. The **Orchestrator Upgrade** screen appears.

Figure 24-1: Configure Upgrade Announcement Details

Customers & Partners Administration **Orchestrator** Gateway Management Edge Image Management

Orchestrator Upgrade

← Bastion System Properties **Orchestrator Upgrade**

ⓘ Currently there is no "Upcoming Orchestrator Upgrade Notification" or "Orchestrator Upgrade In Progress" announcement configured.

1. Use the Upgrade Announcement section to configure a message that will be displayed to users who have visibility when they next login about an upcoming upgrade.
2. Use "Prepare Orchestrator Upgrade" before commencing the upgrade, this will (a) Pause the application of configuration updates to edges during the upgrade, at the global level and by default at the enterprise level and (b) Display the system configured message as the banner message while the upgrade is in progress.
3. Once the Orchestrator Upgrade is completed, Use "Complete Orchestrator Upgrade" to re-enable the application of configuration updates to edges at the global level. By default, the application of configuration updates to edges continues to be paused at the enterprise level until subsequent enterprise-level changes.

Upgrade Announcement

Banner Message *

Orchestrator upgrade planned on MM/DD/YYYY @ 00:00AM PST. Application of configuration updates to edges will be deactivated during upgrade.

(max 512 chars)

Visibility

Operator only

Operator/Partner

Operator/Partner/Customer

Select which users have visibility to the banner

ANNOUNCE ORCHESTRATOR UPGRADE UNANNOUNCE ORCHESTRATOR UPGRADE

e.g. Orchestrator upgrade planned on 4/7/2018 @ 2:00AM PST. Application of configuration updates to edges will be paused during upgrade.

Upgrade Actions

PREPARE ORCHESTRATOR UPGRADE COMPLETE ORCHESTRATOR UPGRADE

- b. Under **Upgrade Announcement** set the banner message and visibility for the users.

Table 63: Upgrade Announcement Option Descriptions

Option	Description
Banner Message	Enter the required Banner Message in the text box to announce the status of an upcoming upgrade. A pop-up message appears indicating that you have successfully created your announcement, and your banner message displays at the top of the Orchestrator.
Visibility	You can choose the banner Visibility for the users. By default, Operator only is selected.

- c. Select the **Announce Orchestrator Upgrade** button to display the banner message.

A pop-up message appears indicating that you have successfully created your announcement, and that your banner message displays at the top of the Orchestrator.

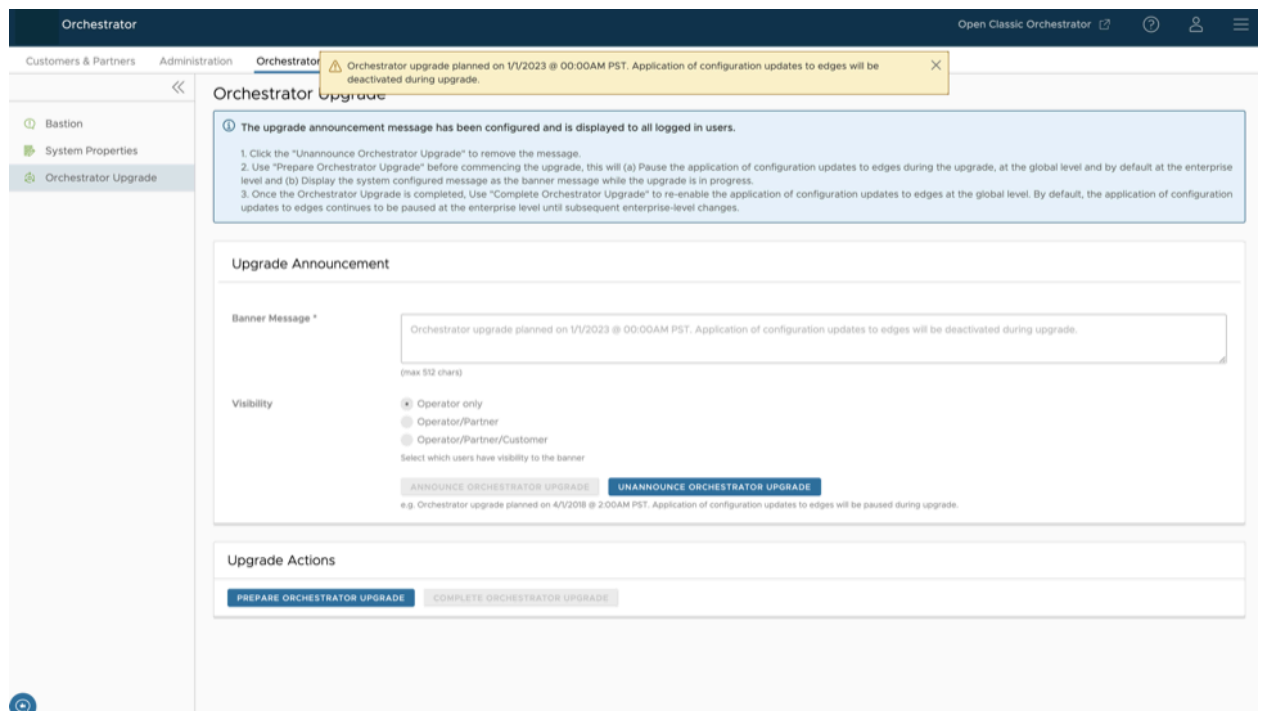
- d. If you want to remove the announcement from the Orchestrator, select the **Unannounced Orchestrator Upgrade** button.

A pop-up message appears indicating that you have successfully unannounced the Orchestrator upgrade.

2. Prepare Orchestrator Upgrade

After you have configured the Orchestrator upgrade banner message and visibility for the users, select the **Prepare Orchestrator Upgrade** button. This pauses the application of the configuration updates of Edges during the upgrade, at the global level and by default at the enterprise level. It displays the system configured message as the banner message while the upgrade is in progress.

Figure 24-2: Prepare Orchestrator Upgrade



Contact the Arista Support team to prepare for the Orchestrator upgrade.

- a. Collect the following information prior to contacting Support:

- Provide the current and target Orchestrator versions, for example: current version (i.e. 2.5.2 GA-20180430), target version (3.3.2 p2).



Note: For the current version, this information can be found on the top, right corner of the Orchestrator by selecting the **Help** icon.

- Provide a screenshot of the replication dashboard of the Orchestrator as shown below.
- Hypervisor Type and version (i.e. vSphere 6.7)
- Commands from the Orchestrator:



Note: Commands must be run as root (e.g. '`sudo <command>`' or '`sudo -i`').

- Run the script `/opt/vc/scripts/vco_upgrade_check.sh` to check:
 - LVM layout
 - Memory Information
 - CPU Information
 - Kernel Parameters
 - Some system properties
 - ssh configurations
 - Mysql schema and database sizes
 - File_store locations and sizes
- Copy of `/var/log`

```
tar -czf /store/log-`date +%Y%M%S`.tar.gz --newer-mtime="36 hours ago" /var/log
```

- From the Standby Orchestrator:

```
sudo mysql --defaults-extra-file=/etc/mysql/velocloud.cnf velocloud -e 'SHOW SLAVE STATUS \G'
```

- From the Active Orchestrator:

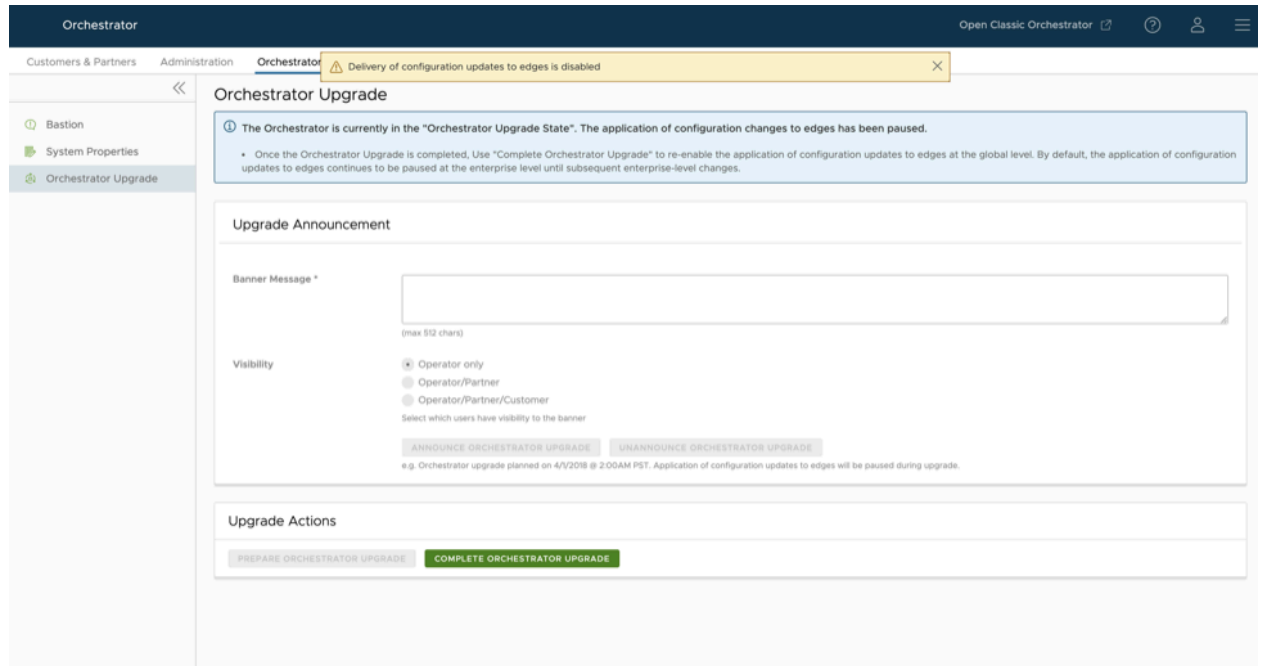
```
sudo mysql --defaults-extra-file=/etc/mysql/velocloud.cnf velocloud -e 'SHOW MASTER STATUS \G'
```

- Contact Arista Support with the above-mentioned information for assistance with the Orchestrator upgrade.

3. Complete Orchestrator Upgrade

After you have complete the Orchestrator upgrade, select the **Complete Orchestrator Upgrade** button under **Upgrade Actions**. This re-enables the application of the configuration updates of Edges at the global level.

Figure 24-3: Complete Orchestrator Upgrade



To verify that the status of the upgrade is complete, run the following command to display the correct version number for all the packages:

```
dpkg -l | grep vco
```

When you are logged in as an Operator, you can confirm if the same version displays by selecting the **Help** icon at the top right corner of the page.

Replication

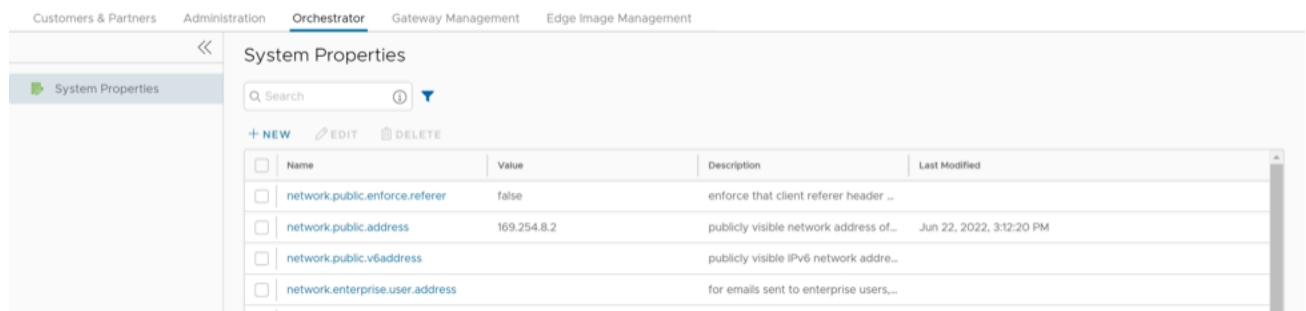
Information regarding how to set up VeloCloud Orchestrator Replication, also known as disaster recovery (DR), is available in the section *Configure VeloCloud Orchestrator Disaster Recovery* of the *Arista VeloCloud Orchestrator Deployment and Monitoring Guide*.

System Properties

Arista provides System Properties to configure various features and options available in the Orchestrator portal.

In the Operator portal, navigate to the **System Properties** page, which lists the available pre-defined system properties. See List of System Properties, which lists some of the system properties that you can modify as an Operator.

Figure 26-1: System Properties



The screenshot shows the 'System Properties' page in the Orchestrator portal. The page has a navigation bar with 'Customers & Partners', 'Administration', 'Orchestrator', 'Gateway Management', and 'Edge Image Management'. The 'System Properties' page title is displayed, along with a search bar and a '+ NEW' button. Below the search bar are 'EDIT' and 'DELETE' icons. The main content is a table with the following data:

Name	Value	Description	Last Modified
network.public.enforce.referrer	false	enforce that client referer header ...	
network.public.address	169.254.8.2	publicly visible network address of...	Jun 22, 2022, 3:12:20 PM
network.public.v6address		publicly visible IPv6 network addre...	
network.enterprise.user.address		for emails sent to enterprise users...	

To configure the system properties:

1. Select **New System Property** to add a new property.

2. In the **New System Property** window, configure the following parameters:

Figure 26-2: New System Property

Table 64: New System Property - Options and Descriptions

Option	Description
Name	Enter the Name for the new system property.
Data Type	Choose the required Data Type from the drop-down menu.
Value	Enter the Value for the property according to the data type.
Value is Password	Select Yes or No as required.
Value is Read-only	Select Yes or No for as required.
Description	Enter the Description for the new system property.

3. Select **Save Changes**.
4. You can use the **Search** field to find a specific system property.

See the section titled, *List of System Properties* in the *Arista VeloCloud Orchestrator Deployment and Monitoring Guide*, which lists some of the system properties that you can modify as an Operator.



Note: It is recommended to contact Arista Support before making changes to the system properties.

External Certificate Authority

The External Certificate Authority (CA) feature is for large enterprises and government customers who deploy an on-premise Orchestrator and have a requirement to use their own certificate authority (CA) rather than the default self-signed Orchestrator certificate authority. This section covers how to enable and configure External CA.

When External CA is configured, instead of the Orchestrator receiving a certificate signing request (CSR) and issuing the device certificates itself, the Orchestrator is required to pass the CSR to an external CA for issuance of the certificate. The device certificate will be returned to the Orchestrator and sent to the Edge or Gateway.

A customer using this feature would be expected to have deployed a commercial certificate authority, for example from PrimeKey (EJBCA PKI), or in some cases, may have implemented their own proprietary CA.

Beginning with Release 5.1.0, an Orchestrator where external CA is activated may be configured with two new API-ready modes:

- **Manual Mode** provides support for any certificate authority and provides flexibility and control with the user manually performing each step in the certificate process.
- **Asynchronous Mode** provides support for any certificate authority with the ability to script the manual steps and automating the recurring tasks.

These modes are added to **Synchronous or Automated Mode**, which was the first mode introduced in Release 4.3.0. With Synchronous mode, the Orchestrator integrates directly with an external CA (which, for Release 4.3.0 and forward, offered PrimeKey EJBCA PKI as the only available external certificate authority) and through REST APIs for certificate request, renewal, and revocation.

Enable External CA: The External CA feature is enabled through two System Properties. Enabling these system properties may only be done by an Operator with a Superuser role.

Note:



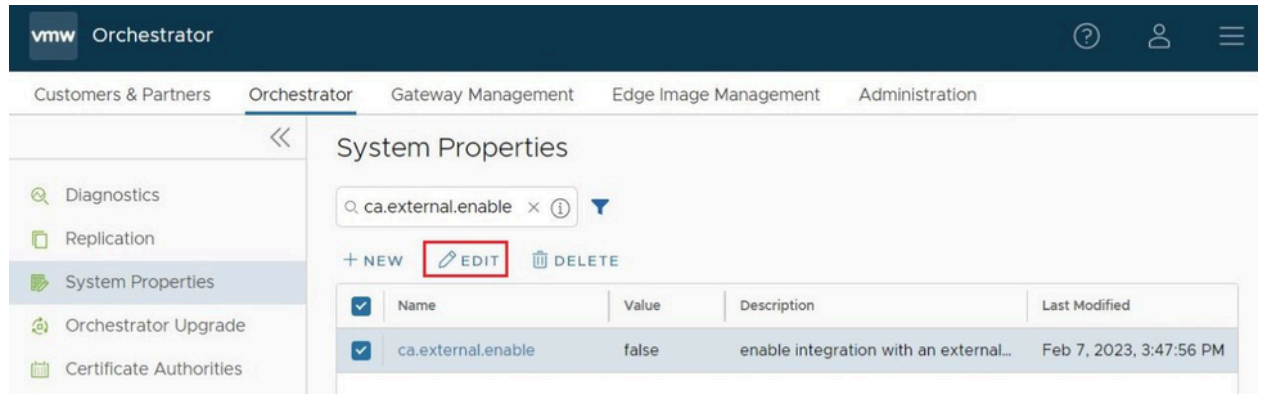
The first system property that must be enabled is `ca.external.configuration`. This property is manually created with a JSON data type and the JSON is populated consistent with the example seen below in the Sample External CA Configuration section.

Only after `ca.external.configuration` is created and enabled, should the Operator enable the second system property: `ca.external.enable`.

1. On the Orchestrator UI select **System Properties**.

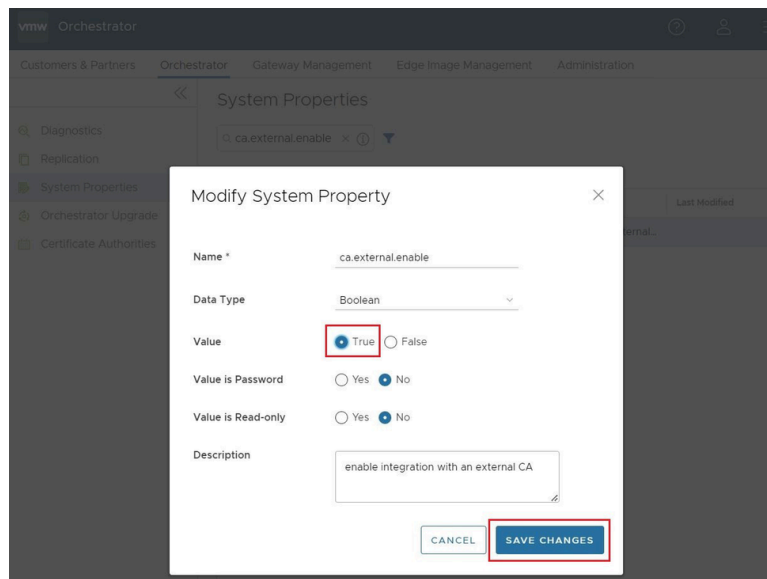
- Using the search box on the **System Properties** page enter `ca.external.enable` as shown in the images below.

Figure 27-1: System Properties



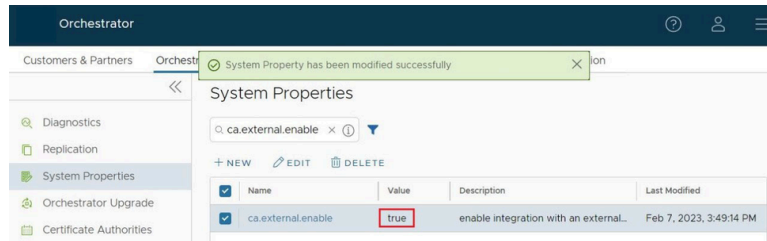
- Once the `ca.external.enable` property is located, either select on that property or check the box and select **Edit**.
- Change the `ca.external.enable` property to **True** and select **Save Changes** to complete the change as shown in the image below.

Figure 27-2: Modify System Property



The **System Property** page displays a confirmation that the property was successfully modified, and will now show that `ca.external.enable` is **True**.

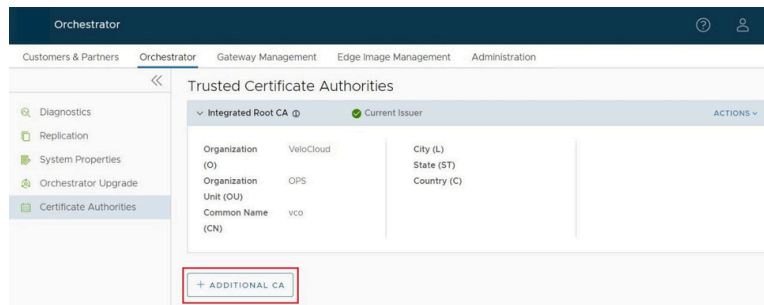
Figure 27-3: System Property Confirmation



Configure External CA

Having activated the External CA System Property, the Operator can now select on **Orchestrator > Certificate Authorities** to begin configuring an external certificate authority.

Figure 27-4: Certificate Authorities

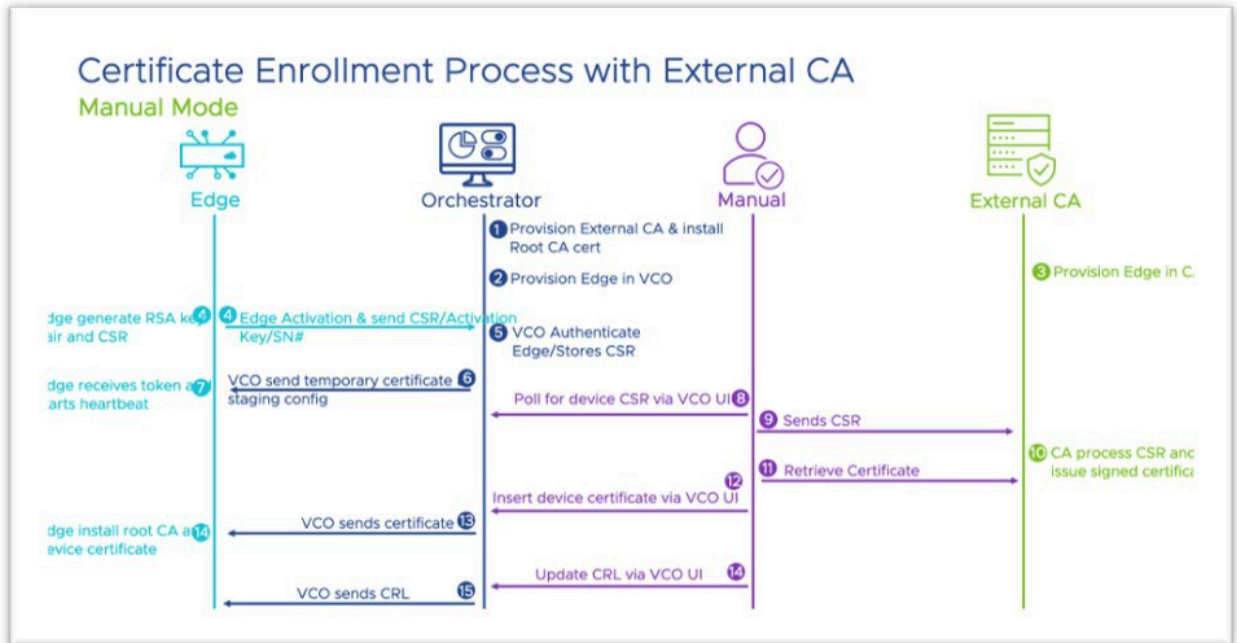


Configuring External CA can be done using one of three modes:

- **Automated (Synchronous):** With **Automated** mode, only one external certificate authority is supported: PrimeKey EJBCA PKI.

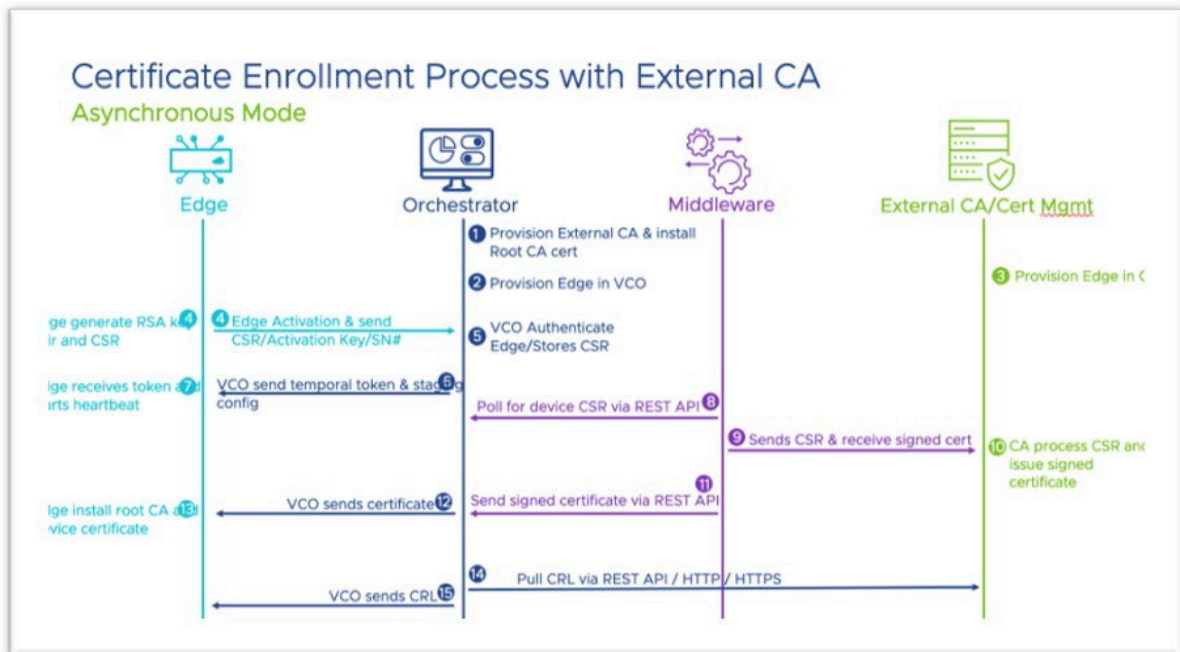
- **Manual:** Manual mode provides support for any certificate authority and provides flexibility and control with the user manually performing each step in the certificate process.

Figure 27-5: Certificate Enrollment Process- Manual Mode



- **Asynchronous:** Asynchronous Mode provides support for any certificate authority with the ability to script the manual steps while automating the recurring tasks.

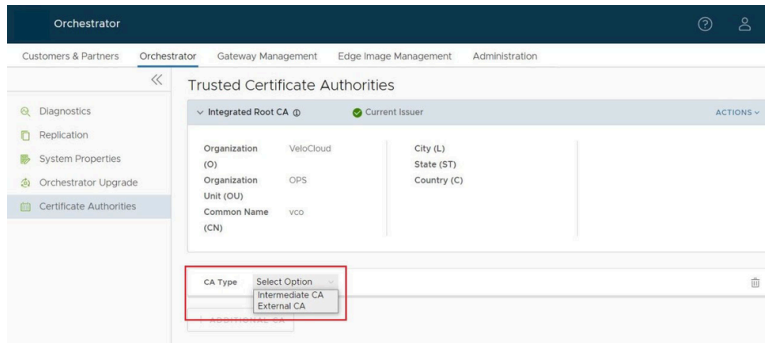
Figure 27-6: Certificate Enrollment Process- Asynchronous Mode



1. On the **Orchestrator > Certificate Authorities** page, select on **+ Additional CA**.

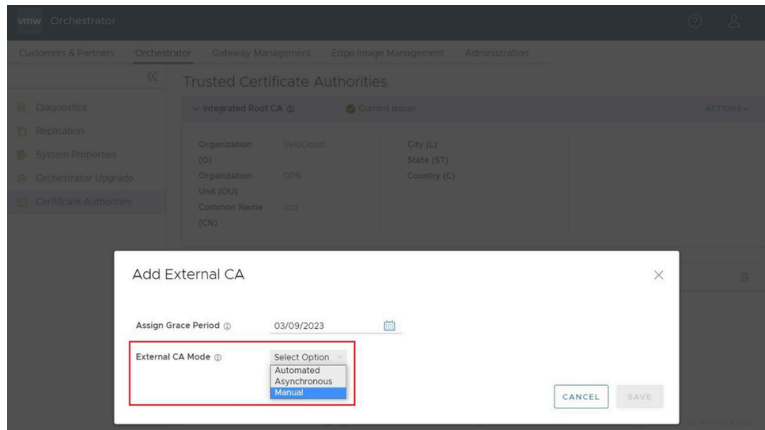
2. After selecting **+ Additional CA**, the UI will change to **CA Type** with a drop down menu with the options of **Intermediate CA** and **External CA**. Select **External CA**.

Figure 27-7: CA Types



3. Once **External CA** is selected, the screen changes to the **Add External CA** screen where an Operator can choose between the three previously mentioned **External CA Modes**: **Automated (Synchronous)**, **Asynchronous**, and **Manual**.

Figure 27-8: External CA Mode



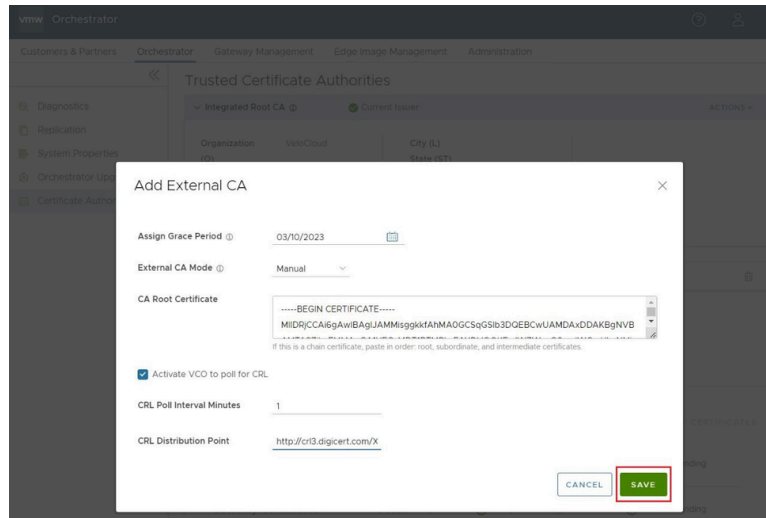
4. Having selected a CA Mode, the **Add External CA** screen changes to allow additional configuration of the external CA. This is where the Operator would paste in the **CA Root Certificate**.

By checking the box for **Activate VCO to poll for CRL**, the Operator elects to have the Orchestrator to conduct certificate revocation checks using the Certificate Revocation List (CRL). If this option is checked, two additional configuration parameters appear to be configured by the Operator:

- a. **CRL Poll Interval in Minutes** determines how often in minutes the Orchestrator will conduct certificate revocation checking against the latest CRL.

- b. **CRL Distribution Point** is the URL where the Orchestrator retrieves the latest CRL.

Figure 27-9: Add External CA



5. Once the Operator has filled out all the required fields, they would select **Save**.
6. Once an external CA is configured the Operator will have newly available options to **Import CRL** and **Download CRL**.

Figure 27-10: Import CRL

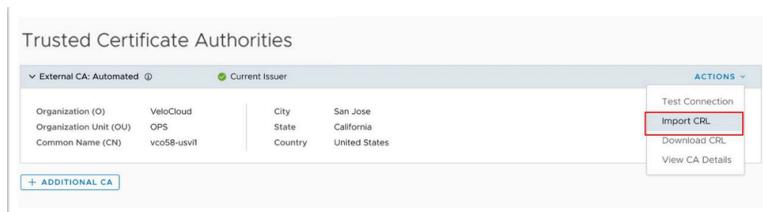


Figure 27-11: Download CRL



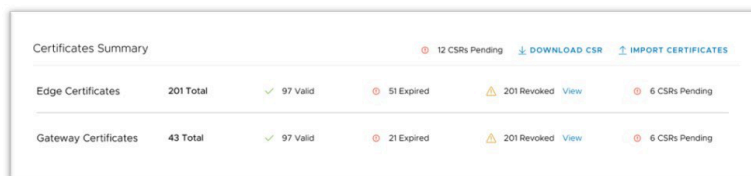

```
+Gcn66b99HgEyIjojqGc1dYzkZVHQuFH7RINFU//1OmnrN\ nmb6JgJNGgbdPKKHdWrFwrGpCiz1c44yznlkVWFrMdbLAlB
+luLpb8Xka7Hq5qzZn\nLVC007Q483FBa8Lkg+RXQjIxYXgx4wkiV600UyKPlpwnSLMJvUUBmIM/By11h8xR\nyKIIZn7rc
5wA4aKcfnJ9CUVfKcJtUPZffOwlvMt8bDZfaloiF20Z0KydJyAst13Z\nQbsMvcA6747aQQ25JD4tid5rDeRDb2bYi7nLl
+l1Nnhm5ZB4qGgnaXGj3oFDoN0R\n+kEK69D1ZRNUdn4=\n-----END CERTIFICATE-----", "apiCertificate":
"-----BEGIN CERTIFICATE-----\nMIIEKzCCApOgAwIBAgIUM83EYfZz4vi4tyleOJr+n6wMksAwDQYJKoZIhvcN
AQEL\nBQAwZiIxZiZhbGogKiaJk/IsZAEBDBNylTA1OTVhMTNjMTUzZDc2YWU1MRUwEwYD\nvQOQDDAxNYW5hZ2VtZW5
0QOExHjAcBgNVBAsMFwFtaS0wMmE0NDc0YzFmNzQ5NDZh\nODE0MDIGAlUECgwraXAtMTAtODEtMTI1LlTEZmI5lcy13
ZXN0LTUyZ29tCHV0ZS5p\nbnRlcm5hbDaeFw0yMTAyMDUwMDA1MTRaFw0yNjAyMDUwMDA1MTNAMBUXEzARBGNV\nnBAM
MCNl1cGvyQWRtaW4wggeiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQc/\nrPdG0oY89GGUgHbV9iG3n3Y1mPBmQ
+iVbVKYD3YpM7fG+KnVQTdJLrYoH5vP71VY\nnQj9H6pjxq0Bh53Mse2F19UE/Gew6IZiRd2OK9yM1xRKH7hjPB3tqFlA98mar
+BYA\nGPhapmq+sSFz6TS2ssToUllG8QgJeMxh6+vSP/Ca90+HiDB7TqEcufVv6lrL7sfKqfyQ5YzITKm7IGDQfdCiorwnd
vdl11NB+vviiYsk1fEW8gvRUu7wMRlzmPwxnUxd\nKmb/b7+065md7+FlkqU6EzYMQ/224ZJonwJfzmNT01AGt4aaJD
NKnl15wV22xqqQ\nnZvA6nrkBd+06pUwVTen1AgMBAAGjdTBzMAwGAlUdEwEB/wQCMAAwHwYDVR0jBBGw\nnFoAUafBBZ
NwmFvrP7Chj1ML14f8bjCcwEwYDVR0lBAwwCgYIKwYBBQUHAwIWhgYD\nnVR0OBByEFFj+bk/epA/jPXZywy1D4XV5sW
lMMA4GA1UdDwEB/wQEAWIF4DANBgkq\nnhkiG9w0BAQsFAAAQYEAARNN08PUMCAWI+wLpu4FRuApRJRwN7U07D2ZDirV
5a7pq\nn1CCbREe34EYmbLydqUCMHS8xJ1Pun5ER3E5YfZck7wJ9y2h8giB703cjx/wWkax\nnNEkz/Is634XZzeIRNf
1TmV9/71LnFUBDJjHYFPNzyw6CBT\nVn/nl1LQ9o3SvbbzLQ\nnCcdcpFm1rxku0UOuCaQgOSuLn5nqTFCNi4Sx40shg8w
Drc1AUuv+yX09dM2G+27h\nndCJrkqHwbtWQMY2s0BdTiQ6TMyJrsvTCTQ67vqRtdJuSqOw/CnPNso2/1srkNWC\nnI1
7mQzq6+2ayQBxsm6xuhXD0InORB+flq/QhY+CQIaTLyLezVITo0bZhe0TpnqYK\nn1INUWjxI8mCBBiXZZ9zxybyOqzZo
uZcNH12OCEqU8altfyW0EpGYClemRTGxXboDK\nn+uEwKH6sngYmK60Usni4WIKBvZV2dJa5o8RhuCUFhwBJ2aHuiTq8
6RLrazJBE3wa\nnGvp10ZmGYmond3aBOYu\nn-----END CERTIFICATE-----", "apiKey": "-----BEGIN PRIVATE
KEY-----\nMIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQC/rPdG0oY89GGU\nngHbV9iG3n3Y1mPB
mQ+iVbVKYD3YpM7fG+KnVQTdJLrYoH5vP71VY\nnQj9H6pjxq0Bh\nn53Mse2F19UE/Gew6IZiRd2OK9yM1xRKH7hjPB3tq
FlA98mar+BYAGPhapmq+sSFz\nn6TS2ssToUllG8QgJeMxh6+vSP/Ca90+HiDB7TqEcufVv6lrL7sfKqfyQ5YzITKm7\
nIGDQfdCiorwndvdl11NB+vviiYsk1fEW8gvRUu7wMRlzmPwxnUxd\nKmb/b7+065md7+FlkqU6EzYMQ/224ZJonwJf
zmNT01AGt4aaJD\nNKnl15wV22xqqQZvA6nrkBd+06\nnpUwVTen1AgMBAAEcggEAL5DVVnp0/JhqxMbydptbd613UMqW0
bgFdkIgnrKrkIL4\nnlSrrpPPHq/4PDzr02C9dd4cNHCQwKzzjv8gHkWDW5U3tEKM2t6BRs7usdLZqwvOy\nnaxAfKPTa
4BNEe3L1nrR0hTatHxXQRJ1BX3nebn5D1iGlbRDwfsValwZMYCmjStiS\nnZNYs71vrXrMfYfYUnyJGDCZsBDRdSb41cQ
J0GmwMd2B8AE5I0spMz2Y5FM0ZcddX\nnLdCLeLonz1LCTNzaXyhdDBCQ8ecWrSWJZ8REhTlK/wsTtPbLi10xIAemcLxxZTJQRC
\n0tyWzA2z190hmpJs3of7geGvDcDwRu/MgvuH31MFwQKBGQDxbHm/982/txuB440+\nnMm+x/Ma5HzZg018sMdH0wQ5qJyD/
lrgz2Ik79FqmFPh016LcekA0zGri+4PiRVr\nnAlY9pLFdegIY6jJpvJxJH+kQ00xEdEUSZ100aAn4dlSHaX3wg+SBjON
iZxs0eQ9m\nnrMDKYT7LE3F5indOimDCug2GoQKBGQDLp5FPvA3uWh5Lff14yhVb0T1oiyeiqe01\nny107LkCI0s002/
M7U0gWXd2XNqAr98RKFtVsbF9gZxsKXtVdI+Vsd1lxGGfNZXmM\nnwodSK9zIeL4Eve7mRtcB/ZDjtgQ0Um2YeVFXZr
EacQoopYo7B4pwjpmIq/40w3\nn0lhXOXEm1QKBGQDPkd9/8LQCwJEy9Q1sS3sDQf0uDyr2xgkz+0W0NQSkuOeuCE0p
\nrmQXmzKREhip7fIFtEpd2t+PdoZmlgsK+uJhL6ebYhpJh5p+1L6elIQThkhNmDuy\nnvgoW01i30jN7xPSWBSBC9xo
Vkea0ZAGc2q0Lk96kRXxL7oQzkaAvjD2y4QKBgHEE\nneQaSmIJO/8tuXLNsbYTDqNTVlgKvZoloit+fv3+pk4y+2dnr
2RQxu9GcIns2EsDj\nn3cQpXCHEgKrr0ZFZTwaFy6JscQcNRFFd0Ehjmj44rEK8LqTnlkz4f8KuHz/O3JZ\nne+qe0zN
71iPzKXVHLOZ65ivtzVNM8y9NtrsdCj/dAoGBAJNM0+fbt3i1e1+U/jOQ\nnKwD8vBVwsJEZ0UspoxETTAnu0sgIUBRE
CVhn/BQ5ja3HusRadRsKb7ROlyjnRuC7\nnnR/wM//oENnRm50hEi40cFp0eAOx7XQOUuE08XhUMYXp00mOC01NwOftL
0WdG6Bk\nnSNV2aPx+2+DGSZEVbuLXviHs\nn-----END PRIVATE KEY-----", "host": "ip-10-81-125-132.us-west-
2.compute.internal", "port": "443", "distinguishedName": "UID=r-0595a13c153d76ae5,cN=ManagementC
A,OU=ami-02a4474c1f74940a8,O=ip-10-81-125-132.us-west-2.compute.internal", "certificateProfile":
"ENDUSER", "endEntityProfile": "EMPTY" } }
```

Monitoring External CA

Monitoring certificates is done on the same **Orchestrator > Certificate Authorities** page.

The **Certificates Summary** page provides an Operator with a visual status of key indicators for their certificates' life cycle. The Operator would also import certificates and download CSRs in this section.

Figure 27-13: Certificates Summary



In the **Certificates** section, the Operator can download a complete list of all Edge or Gateway certificates in the .csv format.

Figure 27-14: Certificates

The screenshot shows a web interface titled "Certificates". It is divided into two sections: "Edge Certificates" and "Gateway Certificates". Each section has a "DOWNLOAD CSV" link and a table with columns for selection, name, serial number, issued/expiration dates, and a "View Certificate" link. Both tables currently show "0 items".

<input type="checkbox"/>	Enterprise	Edge Name	Serial number	Issued On	Expires On	View Certificate
COLUMNS 0 items						

<input type="checkbox"/>	Network	Gateway Name	Issued On	Expires On	View Certificate
COLUMNS 0 items					

An Operator, Partner, or Customer administrator can also examine a particular Edge's certificate by navigating to **Configure > Edge > Overview**.

Limitations

- External CA can only be enabled on an On-Premise Orchestrator managed by a single customer. This feature is not available on Orchestrators.
- On an Orchestrator using Release 3.4.0 up to 5.0.0, this feature can only use PrimeKey EJBCA PKI as an external CA.

Appendix

A.1 Operator-Level Orchestrator Alerts and Events

Describes a summary of alerts and events generated within the VeloCloud Orchestrator at the Operator level.

The document provides details about all Operator-level Orchestrator events. Although these events are stored within the Orchestrator and displayed on the Orchestrator UI, most of them are generated by either an Gateway and/or one of its running components (MGD, PROCMON, and so on) with the exception of a few which are generated by the Orchestrator itself. You can configure notifications/alerts for events in Orchestrator only.

The following table provides an explanation for each of the columns in the "Operator-level Orchestrator Events" table:

Table 65: Column Details of Operator-level Orchestrator Events

Column name	Details
EVENT	Unique name of the event
DISPLAYED ON ORCHESTRATOR UI AS	Specifies how the event is displayed on the Orchestrator.
SEVERITY	The severity with which this event is usually generated.
GENERATED BY	The VeloCloud SD-WAN component generating the notification can be one of the following: <ul style="list-style-type: none"> Orchestrator Gateway
GENERATED WHEN	Technical reason(s) and circumstances under which this event is generated.
RELEASE ADDED IN	The release this event was first added. If not specified, this event existed prior to release 2.5.
DEPRECATED	Specifies if the event is deprecated from a specific release.

Table 66: Operator-level Orchestrator Events

EVENT	DISPLAYED ON ORCHESTRATOR UI AS	SEVERITY	GENERATED BY	GENERATED WHEN	RELEASE ADDED IN	DEPRECATED
GATEWAY_UP	Gateway up	INFO	Orchestrator	A Gateway restores after losing connectivity with the Orchestrator.		
GATEWAY_DOWN	Gateway down	INFO	Orchestrator	A Gateway fails to communicate after losing connectivity with the Orchestrator.		
GATEWAY_LARGE_PKT_SIZE	Packet size limit exceeded	INFO	Gateway	The packet size limit incoming from a Gateway's peer exceeded.		
GATEWAY_SERVICE_FAILED	Gateway service failed	ERROR	Gateway	The GWD service on the Gateway fails.		
GATEWAY_BFD_NEIGHBOR_UP	BFD session established to Gateway neighbor	INFO	Gateway	A Gateway BFD neighbor comes back up		
GATEWAY_BFD_NEIGHBOR_DOWN	Gateway BFD neighbor unavailable	INFO	Gateway	A Gateway BFD neighbor comes back down		
GATEWAY_ICMP_PROBE_UNSTABLE	Gateway: ICMP probe unstable	ALERT	Gateway	The ICMP probe goes down on Partner Gateway.		
GATEWAY_REBALANCE	Gateways rebalanced	INFO	Orchestrator			
PROXY_ENABLE_OPERATOR_ACCESS	Partner access delegated to operator	INFO	Orchestrator			
PROXY_DISABLE_OPERATOR_ACCESS	Partner access revoked to operator	INFO	Orchestrator			
VRF_ROUTE_MAP_RULES_MAX_LIMIT_HIT	VRF route map rules limit exceeded	WARNING	Gateway	The VRF Inbound/ Outbound route map maximum limit exceeded (32).		
VRF_LIMIT_EXCEEDED	VRF limit exceeded	ALERT	Gateway	The VRF entries configured exceeded maximum limit (1000).		
ENABLE_EXTERNAL_CA	External CA Enabled	CRITICAL	Orchestrator	The ca.external.enable property is set to true.	4.3.0	
DISABLE_EXTERNAL_CA	External CA Disabled	CRITICAL	Orchestrator	The ca.external.enable property is set to false.	4.3.0	
INSERT_EXTERNAL_CA	External CA Inserted	CRITICAL	Orchestrator	External CA is inserted into the VELOCITY_CLOUD_CERTIFICATE_AUTHORITY table and becomes a trusted issuer.	4.3.0	
CREATE_COMPOSITE_ROLE	Composite Role Created	INFO	Orchestrator	A composite role is created by an Enterprise, Partner, or Operator.	4.5.0	
UPDATE_COMPOSITE_ROLE	Composite Role Updated	INFO	Orchestrator	A composite role is updated by an Enterprise, Partner, or Operator.	4.5.0	
DELETE_COMPOSITE_ROLE	Composite Role Deleted	INFO	Orchestrator	A composite role is deleted by an Enterprise, Partner, or Operator.	4.5.0	

EVENT	DISPLAYED ON ORCHESTRATOR UI AS	SEVERITY	GENERATED BY	GENERATED WHEN	RELEASE ADDED IN	DEPRECATED
CA_VALIDATION	CA validation failure	ALERT	Orchestrator	The CA certificate attributes are rejected.	5.0.0	
EI_ACTIVATION_CONFIG_SENT	EI activation config sent	INFO	Orchestrator	The activation config has been successfully sent to the EI server.	5.0.0	
Auto_Rate_Limit_Enabled	Auto Rate-Limit Enabled	WARNING	Gateway	The auto rate-limit capability is activated on Gateways if the Gateway detects that certain Edges are sending large amount of traffic which might be causing the Gateway to be unstable and drop packets. The event message includes the information about the list of Edges (Enterprise, Rate Limit Percentage) on which the auto rate-limit is activated.	5.2.0	
Auto_Rate_Limit_Disabled	Auto Rate-Limit Disabled	WARNING	Gateway	Gateway auto rate-limit condition is restored.	5.2.0	
SELF_HEALING_REPORT	anomaly_type: <Remote Route inconsistency>, num_routes_recovered:<number>, shr state: <DONE>	ALERT	Gateway	Generated when routes are detected as missing from a customer enterprise connected to a Gateway, and the Gateway corrects this issue by using the Self-Healing Routing feature to recover the missing routes.	5.2.0	
POLL_IDPS_SIGNATURE_FAIL	Failure in poll job that queries and downloads signature file from GSM	ERROR	Orchestrator	When Orchestrator backend poll job has failed to retrieve or download suricata signature from GSM and update profiles with the new signature metadata.	5.2.0	
IDPS_SIGNATURE_VCO_VERSION_CHECK_FAIL	Querying existing signature version from local DB failed	ERROR	Orchestrator	When Orchestrator backend poll job has failed to retrieve existing suricata signature version from Orchestrator's local database.	5.2.0	
IDPS_SIGNATURE_GSM_VERSION_CHECK_FAIL	Querying signature metadata from GSM failed	ERROR	Orchestrator	When Orchestrator backend poll job has failed to retrieve existing suricata signature metadata (that includes signature version) from GSM.	5.2.0	

EVENT	DISPLAYED ON ORCHESTRATOR UI AS	SEVERITY	GENERATED BY	GENERATED WHEN	RELEASE ADDED IN	DEPRECATED
IDPS_SIGNATURE_SKIP_DOWNLOAD_NO_UPDATE	Skipping signature download due to no change in signature version	INFO	Orchestrator	When Orchestrator backend poll job skips downloading suricata signature file due to no change in suricata signature file version.	5.2.0	
IDPS_SIGNATURE_STORE_FAILURE_NO_PATH	Filestore path not set to store signature file	ERROR	Orchestrator	When Orchestrator backend poll job fails to store suricata signature file due to filestore path not being set.	5.2.0	
IDPS_SIGNATURE_DOWNLOAD_SUCCESS	Successfully downloaded signature file from GSM	INFO	Orchestrator	When Orchestrator backend poll job successfully downloads suricata signature file from GSM.	5.2.0	
IDPS_SIGNATURE_DOWNLOAD_FAILURE	Failed to download signature file from GSM	ERROR	Orchestrator	When Orchestrator backend poll job fails to download suricata signature file from GSM.	5.2.0	
IDPS_SIGNATURE_STORE_SUCCESS	Successfully stored the signature file in filestore	INFO	Orchestrator	When Orchestrator backend poll job successfully stores the suricata signature file in local file store.	5.2.0	
IDPS_SIGNATURE_STORE_SIGNATURE_FAILURE	Failed to store the signature file in filestore	ERROR	Orchestrator	When Orchestrator backend poll job fails to store the suricata signature file in local file store.	5.2.0	
IDPS_SIGNATURE_METADATA_INSERT_SUCCESS	Successfully added metadata of the signature file to local DB	INFO	Orchestrator	When Orchestrator backend poll job successfully adds metadata of the suricata signature file to local DB.	5.2.0	
IDPS_SIGNATURE_METADATA_INSERT_FAILURE	Failure to add metadata of the signature file to local DB	ERROR	Orchestrator	When Orchestrator backend poll job fails to add metadata of the suricata signature file to local DB.	5.2.0	
POLL_URL_CATEGORIES_FAIL	POLL_URL_CATEGORIES_FAIL	ERROR	Orchestrator	Generated when Orchestrator URL categories poll job fails.	6.0.0	
URL_CATEGORIES_STORE_SUCCESS	URL_CATEGORIES_STORE_SUCCESS	INFO	Orchestrator	Generated when Orchestrator URL categories are stored successfully.	6.0.0	
URL_CATEGORIES_STORE_FAILURE	URL_CATEGORIES_STORE_FAILURE	ERROR	Orchestrator	Generated when Orchestrator URL categories storage job fails.	6.0.0	
VCO_ENTERPRISE_NTICS_LICENSE_REQUEST_FAILED	VCO_ENTERPRISE_NTICS_LICENSE_REQUEST_FAILED	ERROR	Orchestrator	Generated when Orchestrator Enterprise NTICS license request fails.	6.0.0	

EVENT	DISPLAYED ON ORCHESTRATOR UI AS	SEVERITY	GENERATED BY	GENERATED WHEN	RELEASE ADDED IN	DEPRECATED
VCO_ENTERPRISE_NTICS_LICENSE_REQUEST_SUCCEEDED	NTICS License request succeeded	INFO	Orchestrator	Generated when Orchestrator Enterprise NTICS license request succeeds.	6.0.0	

Gateway Capacity Events

Currently, the Gateway assignment is based on Geo-proximity and doesn't take Gateway capacity health metrics into account. To improve the Edge-to-Gateway assignment the capacity health metrics (Edge Count, Tunnel Count, PKI Activated Tunnel Count, Flow count, NAT Count, Packet Queue Watermark, and Packet Drops) are monitored periodically based on warning and critical thresholds. When any of the metrics count is above the defined warning and critical thresholds, Gateway capacity events are generated and reported to the Orchestrator. These events provide the Operator and Partners a clear visibility about the Gateway health for making intelligent and correct Gateway assignments.

The following are the Gateway capacity events generated based on the capacity threshold limits.

Table 67: Gateway Capacity Events

Metric	Trigger	Event	Severity	Message	Event Detail
Edge Count	Above Warning Threshold. The Warning threshold value is 90% of following Supported values: <ul style="list-style-type: none"> 4 CPU, 32G MEM - 2000 8 CPU, 32G MEM - 4000 	GATEWAY_DEGRADED	NOTICE	Over capacity alert due to high number of connected Edges as Gateway has crossed warning threshold.	<ul style="list-style-type: none"> 4 CPU: The number of connected Edges is above the warning threshold (1800). 8 CPU: The number of connected Edges is above the warning threshold (3600).
Edge Count	Above Critical Threshold. The Critical threshold value is 95% of following Supported values: <ul style="list-style-type: none"> 4 CPU, 32G MEM - 2000 8 CPU, 32G MEM - 4000 	GATEWAY_CRITICAL	NOTICE	Over capacity alert due to high number of connected Edges as Gateway has crossed critical threshold.	<ul style="list-style-type: none"> 4 CPU: The number of connected Edges is above the critical threshold (1900). 8 CPU: The number of connected Edges is above the critical threshold (3800).
Edge Count	Below Warning Threshold	GATEWAY_STABLE	INFO	Over capacity condition due to high number of connected Edges restored.	The number of connected Edges is within the acceptable threshold.
Tunnel Count	Above Warning Threshold. The Warning threshold value is 90% of following Supported values: <ul style="list-style-type: none"> 4 CPU, 32G MEM - 3000 8 CPU, 32G MEM - 6000 	GATEWAY_DEGRADED	NOTICE	Over capacity alert due to high number of tunnels.	<ul style="list-style-type: none"> 4 CPU: The number of tunnels is above the warning threshold (2700). 8 CPU: The number of tunnels is above the warning threshold (5400).
Tunnel Count	Above Critical Threshold. The Critical threshold value is 95% of following Supported values: <ul style="list-style-type: none"> 4 CPU, 32G MEM - 3000 8 CPU, 32G MEM - 6000 	GATEWAY_CRITICAL	NOTICE	Over capacity alert due to high number of tunnels.	<ul style="list-style-type: none"> 4 CPU: The number of tunnels is above the critical threshold (2850). 8 CPU: The number of tunnels is above the critical threshold (5700).
Tunnel Count	Below Warning Threshold	GATEWAY_STABLE	INFO	Over capacity condition due to high number of tunnels restored.	The number of tunnels is within the acceptable threshold.
Flow Count	Above Warning Threshold. The Warning threshold value is 50% of Supported value 1920000.	GATEWAY_DEGRADED	NOTICE	Over capacity alert due to high number of flows.	The number of flows is above the warning threshold (960000).
Flow Count	Above Critical Threshold. The Critical threshold value is 75% of Supported value 1920000.	GATEWAY_CRITICAL	NOTICE	Over capacity alert due to high number of flows.	The number of flows is above the critical threshold (1440000).
Flow Count	Below Warning Threshold	GATEWAY_STABLE	INFO	Over capacity condition due to high number of flows restored.	The number of flows is within the acceptable threshold.
NAT Entries Count	Above Warning Threshold. The Warning threshold value is 50% of Supported value 1920000.	GATEWAY_DEGRADED	NOTICE	Over capacity alert due to high number of NAT entries.	The number of NAT entries is above the warning threshold (960000).
NAT Entries Count	Above Critical Threshold. The Critical threshold value is 75% of Supported value 1920000.	GATEWAY_CRITICAL	NOTICE	Over capacity alert due to high number of NAT entries.	The number of NAT entries is above the critical threshold (1440000).

Metric	Trigger	Event	Severity	Message	Event Detail
NAT Entries Count	Below Warning Threshold	GATEWAY_STABLE	INFO	Over capacity condition due to high number of NAT entries restored.	The number of NAT entries is within the acceptable threshold.
Packet Queue Watermark	Above Critical Threshold	GATEWAY_CRITICAL	NOTICE	Over capacity alert due to high packet queue watermark.	The packet queue watermark is above the critical threshold (6000) for 5 consecutive seconds.
Packet Queue Watermark	Above Warning Threshold	GATEWAY_DEGRADED	NOTICE	Over capacity alert due to high packet queue watermark.	The packet queue watermark is above the warning threshold (2000) for 10 consecutive seconds.
Packet Queue Watermark	Below Warning Threshold	GATEWAY_STABLE	INFO	Over capacity condition due to high packet queue watermark restored.	The packet queue watermark is within the acceptable threshold.
Packet Drop Count	Above Critical Threshold	GATEWAY_CRITICAL	NOTICE	Over capacity alert due to high number of packet drops.	The number of packet drops is above the critical threshold (2000) for 5 consecutive seconds.
Packet Drop Count	Above Warning Threshold	GATEWAY_DEGRADED	NOTICE	Over capacity alert due to high number of packet drops.	The number of packet drops is above the warning threshold (500) for 10 consecutive seconds.
Packet Drop Count	Below Warning Threshold	GATEWAY_STABLE	INFO	Over capacity condition due to high number of packet drops restored.	The number of packet drops is within the acceptable threshold.

References

B.1 Related Documents

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

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