Partner Guide

VeloCloud SD-WAN

Version 6.1

Arista.com

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

Contents

Chapter 1

About VeloCloud SD-WAN Partner Guide

The VeloCloud SD-WAN™ Partner Guide provides information about VeloCloud Edge Cloud Orchestrator including how to add and manage Customers who use VeloCloud SD-WAN.

Intended Audience

This guide is intended for Partners who are familiar with the Networking configurations and SD-WAN operations.

Here's a quick walkthrough of the user journey as a Partner Superuser:

1. Install SD-WAN Orchestrator
2. Configure SD-WAN Orchestrator Disaster Recovery
3. Install VeloCloud Partner Gateway
4. Partner Settings
5. Configure Partner Users
6. Manage Partner Customers
7. Configure Profiles
8. Manage Edge Licensing
9. Activate Edges
10. Configure Gateways and Gateway Pools
11. Monitor Partner Customers
12. Monitor and Troubleshoot Gateways

Chapter 2

What's New

Table 1: What's New in Version 6.1.0

Feature	Description
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 additional 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 VeloCloud SD-WAN versions, contact your VeloCloud representative.

Chapter 3

Introduction

As a Partner user, you can configure and manage the following:

- Partner Admin Users
- Partner Events
- Partner Settings
- Partner Authentication
- Enterprise Customers

Supported Browsers

The Orchestrator supports the following browsers:

Table 2: Browser Support

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 recommends Google Chrome or Mozilla Firefox.

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

Chapter 5

Using SSO Login for a Partner User

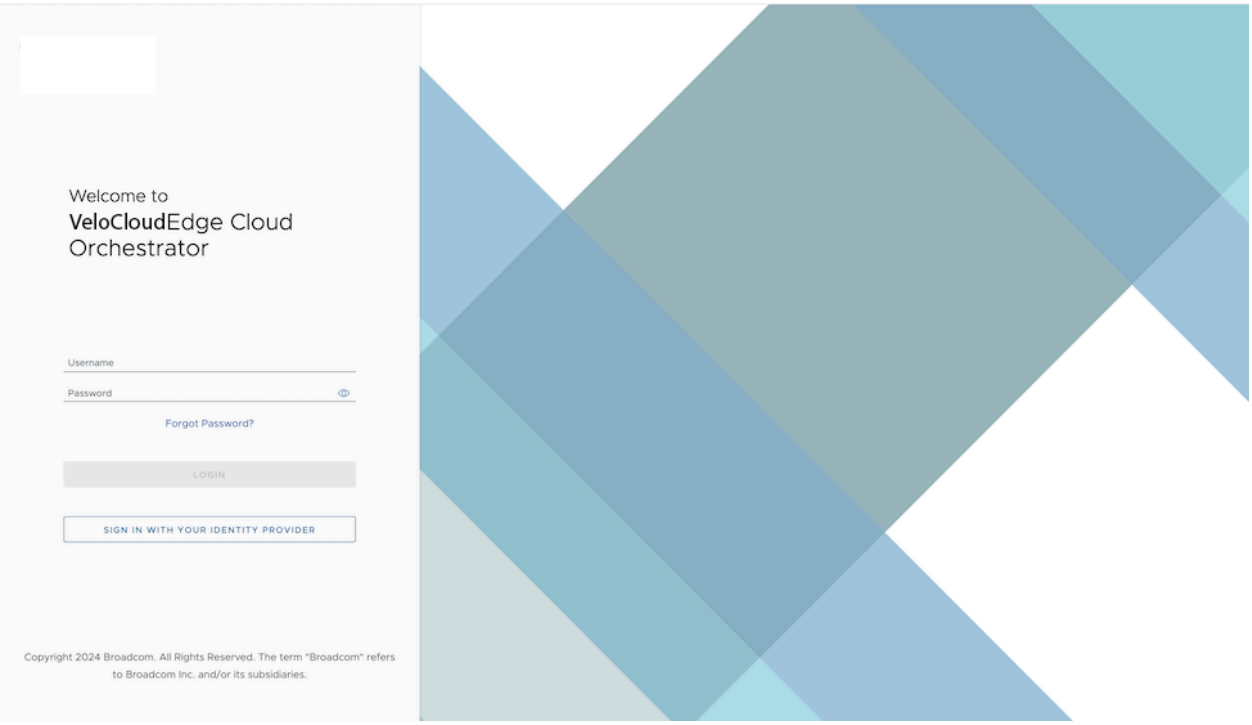
You can login to the Orchestrator with your local credentials or SSO, if set up at the Partner level. This section discusses how to log in to Orchestrator using Single Sign On (SSO) as a Partner user.

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

  For additional information, see Authentication.

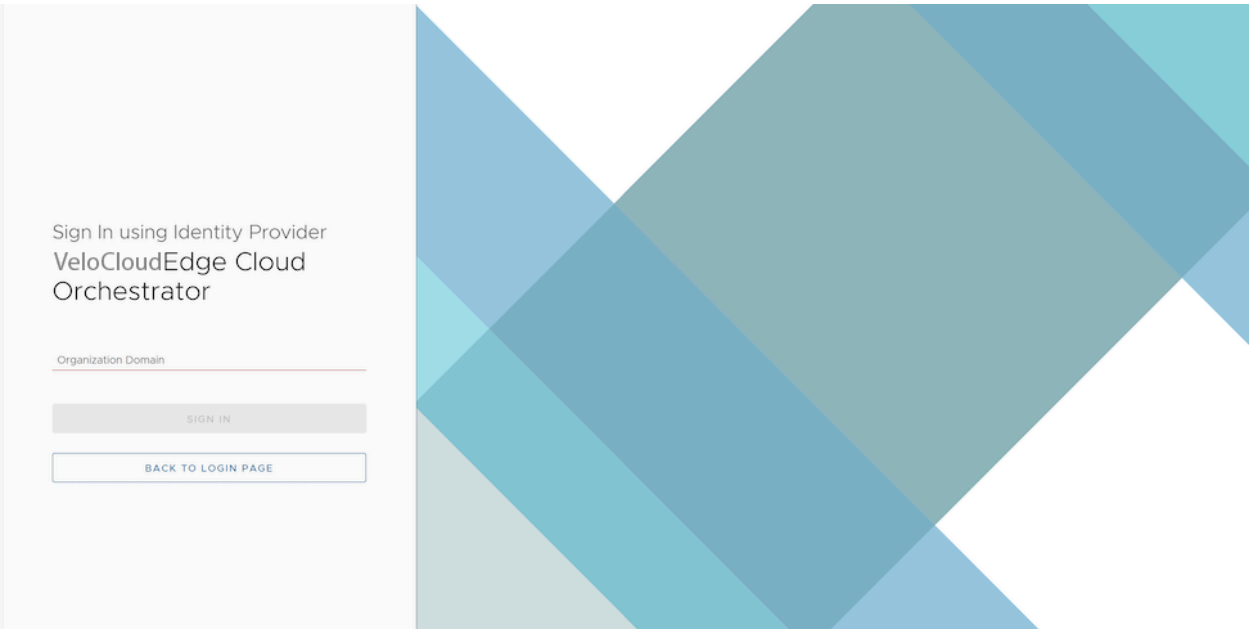
1. In a web browser, launch the **Orchestrator** application. The **VeloCloud SD-WAN Operations Console** screen appears.

   Figure 5-1: Orchestrator Login Screen



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

Figure 5-2: Signing In with Identity Provider



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.

> **Note:** Once the users log in to the Orchestrator using SSO, they cannot login again as native users.

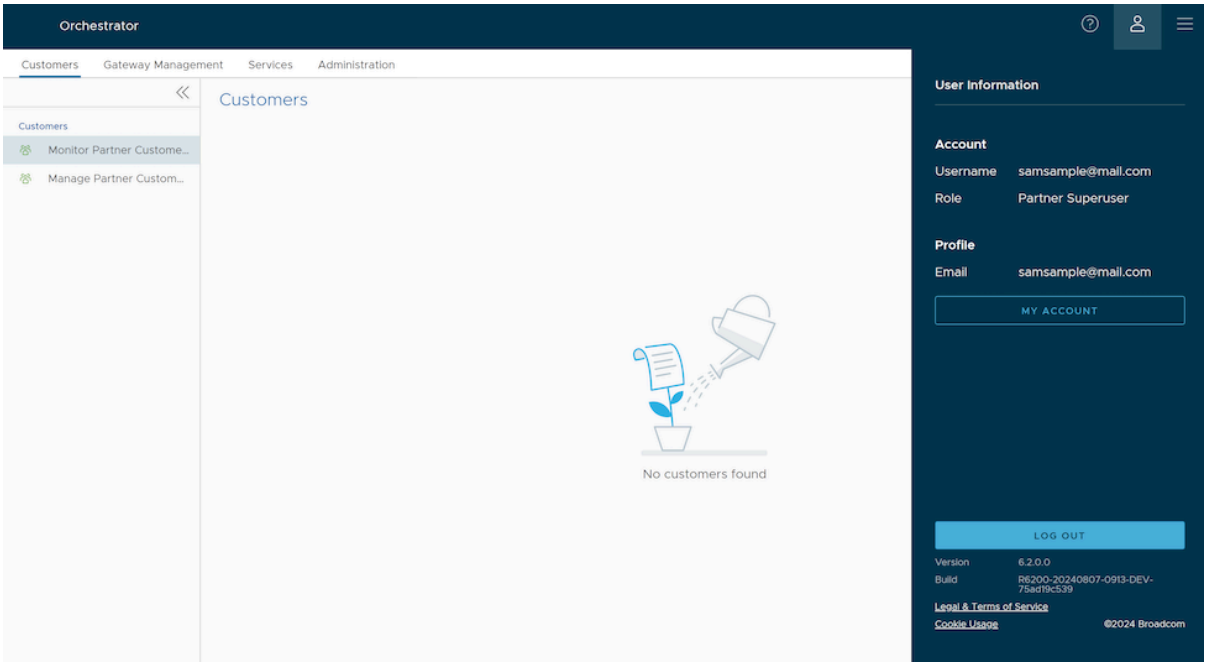
- Manage and monitor Partner customers
- Manage Partners and Partner settings
- Configure User Account details
- Manage Gateway pools and Gateways

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 VeloCloud trademark. For additional information, see Configure User Account details.

Figure 5-3: Displaying My Account



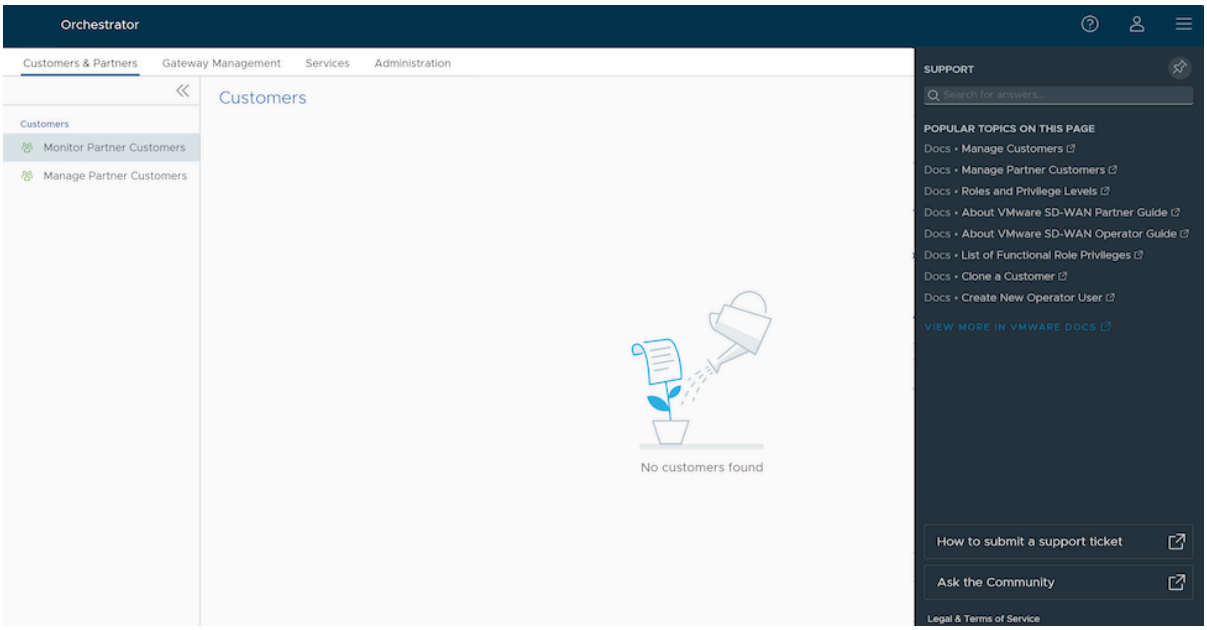
- Starting with the 5.4.0 release, the **In-product Contextual Help Panel** with context-sensitive user assistance is supported in the SD-WAN service of the Enterprise Orchestrator UI and as well as for the Operator and Partner levels. In the Global Navigation bar, select the **Question Mark** icon located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

Figure 5-4: Adding Feature Access

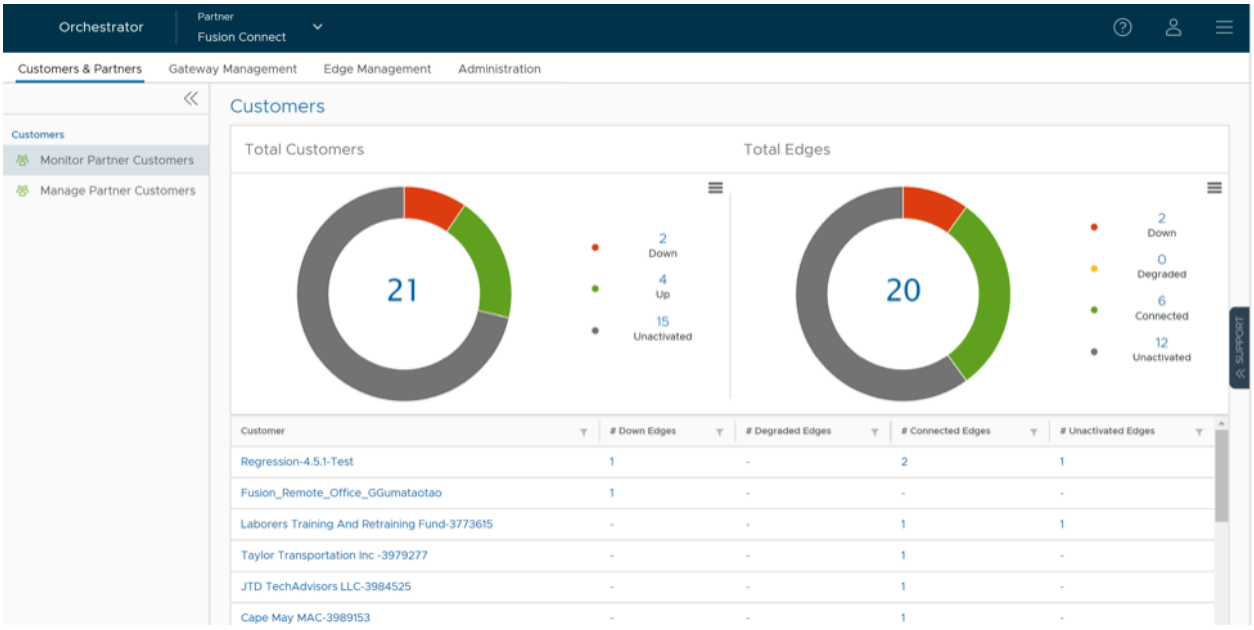


Monitor Partner Customers

As a Partner Administrator, you can monitor the status of your Customers along with the Edges connected to the Customers.

1. Login to the **Orchestrator** as a Partner. In the **Partner** portal, select **Monitor Partner Customers**. The **Customers** page appears.

   Figure 6-1: Monitor Partner Customers



2. The **Customers** page displays the Edges for all customers managed by this Partner as follows:

   Total Customers:

   - Customers managed by the Partner.
   - Number of Edges that are DOWN, DEGRADED, CONNECTED, and UNACTIVATED. Select the number to view the corresponding Customer details in 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 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, select the number of Edges link, to view the details of each Edge. Select the link to the Edge name to view additional details corresponding to the selected Edge. For additional information, see the *VeloCloud SD-WAN Administration Guide*.

Note: The option for Auto Refresh is not available. You can refresh the Window manually to view the current data.

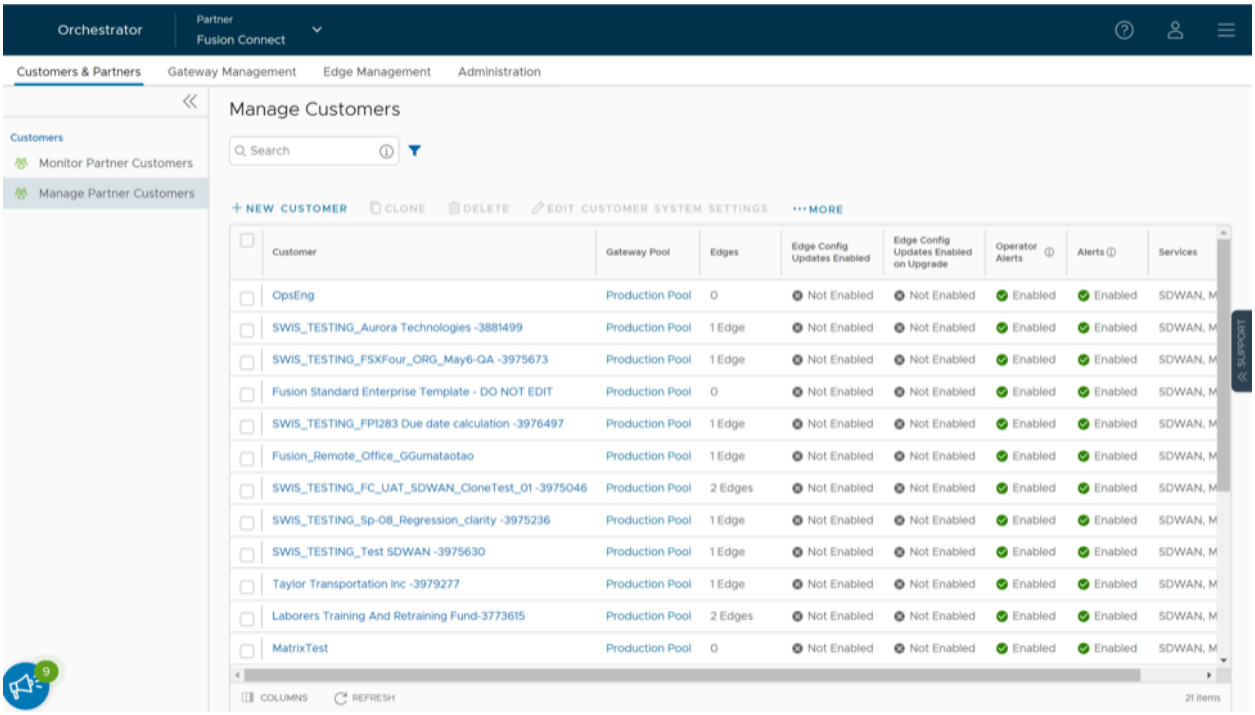
Manage Partner Customers

The Manage Partner Customers option allows you to create new Customers, configure the Customer capabilities, clone the existing configuration, and to configure other Customer settings. As a Partner Super User, you can choose the settings that the Partner Customer can modify.

1. Login to the **Orchestrator** as a Partner. In the **Partner** portal, go to **Customers & Partners** > **Manage Partners** and from the **Manage Partners** page, select a Partner.
2. Select **Manage Partner Customers**. The **Manage Customers** page appears.

> **Note:** You can also navigate to this page from the **Operator** portal, by selecting the link under the **Partner** column of a corresponding Customer. However, a Partner user does not have the same privileges as that of an Operator.

Figure 7-1: Manage Partner Customers



3. You can perform the following actions:

Table 3: Partner 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 Partner 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 Partner Customer.
Delete	Deletes the selected Customers. Enter the number of selected Customers in the pop-up window and select **Delete**. **Note:** Ensure that you have removed all the Edges associated with the selected Customer, before deleting the Customer.
Edit Customer System Settings	Allows you to edit the system settings for the customer. For additional information, see the " *Enterprise Settings*" section in the *VeloCloud SD-WAN Administration Guide*.
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*.

4. 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.
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.
Export All Customers	Exports the details of all the Customers in the Operator portal to a CSV file. The default separator used is comma (,) and you can choose to replace the separator with any other special character.
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 (,).

5. 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.

7.1 Create New Partner Customer

In the **Partner** portal of the *Orchestrator*, you can create new Customers and configure the Customer settings. You can temporarily deactivate creating new Customers, by setting the system property `session.options.disableCreateEnterpriseProxy` to `True`. You can use this option when Orchestrator exceeds the usage capacity.

1. Login to the **Orchestrator** as a Partner.
2. In the **Partner** portal, go to **Customers & Partners** > **Manage Partners** and from the **Manage Partners** page, select a **Partner**.
3. Select **Manage Partner Customers**. In the **Manage Customers** page appears, select **New Customer**.
4. On the **New Customer** page, configure the following details:
   a. Enter the **Customer Information** details in the following fields and select **Next**.

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

Figure 7-2: Configure Customer Information

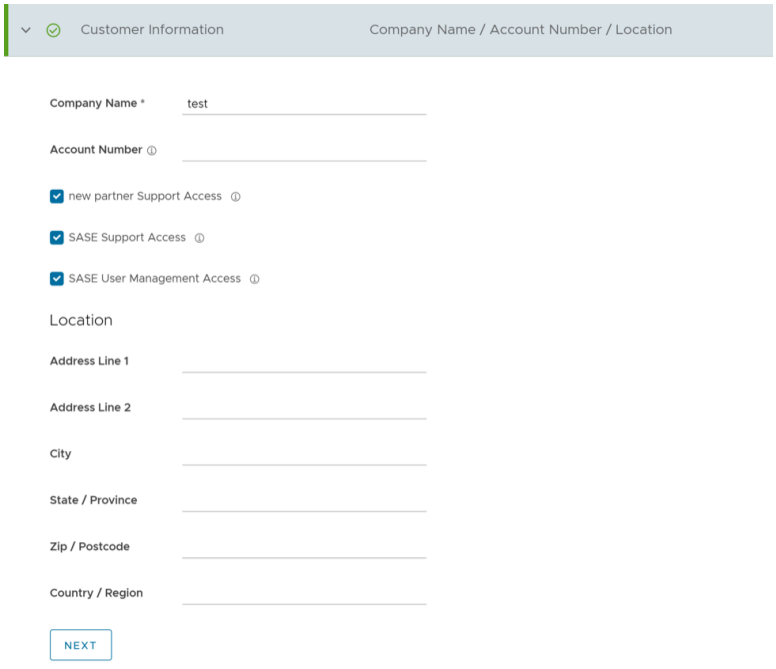


Table 6: Customer Information Option Descriptions

Option	Description
Company Name	Enter your company name.
Account Number	Enter a unique identifier for the Customer.
New Partner Support Access	Select the check box to allow the new Partner to view, configure, and troubleshoot the Customer's Edges.
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. Enter the **Administrative Account** details in the following fields and select **Next**.

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

Figure 7-3: Configure Administrative Account

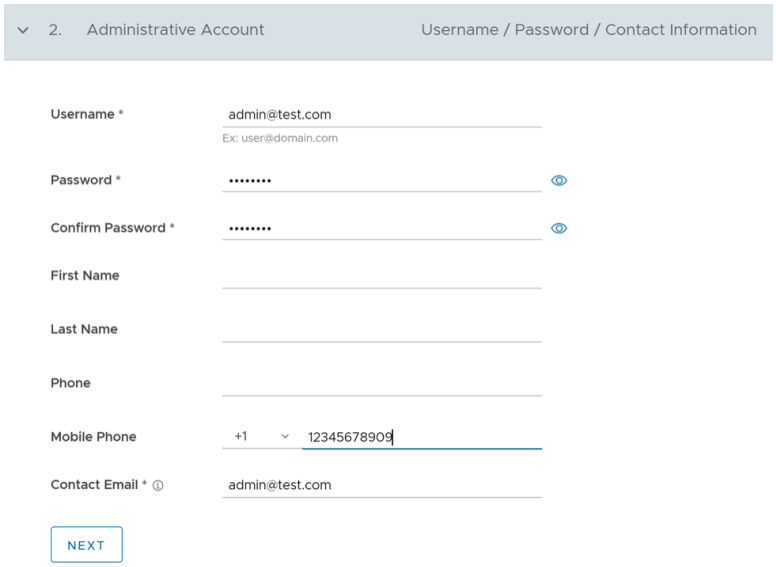


Table 7: Administrative Account Option Descriptions

Option	Description
Username	Enter the username in the `user@domain.com` format.
Password	Enter a password for the Administrator. **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.
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.

c. Under **Global Settings**, configure the Services as per your requirement:

Figure 7-4: Configure Services

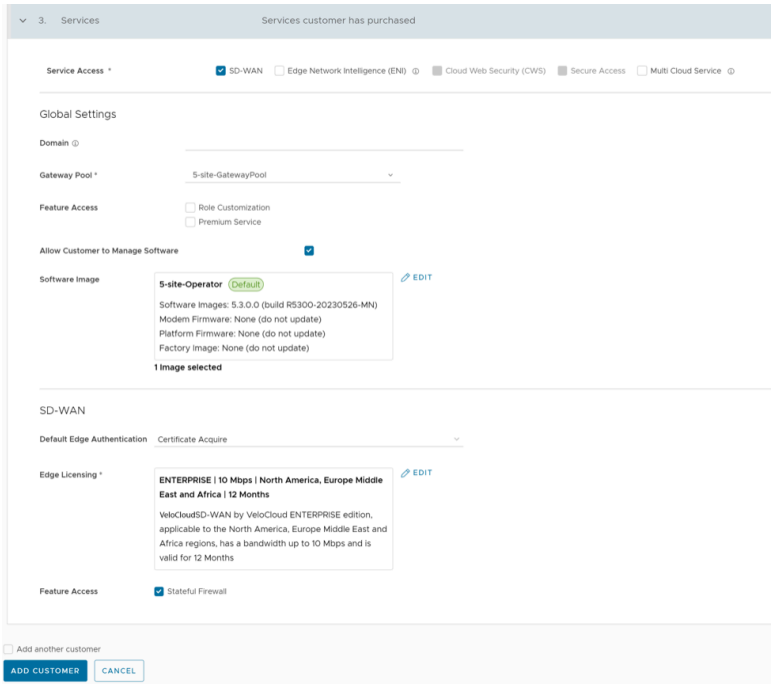


Table 8: Services Option Descriptions

Option	Description
Domain	Enter the domain name to be used to enable Single Sign On (SSO) authentication for the Orchestrator. This is also required to activate Edge Network Intelligence 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** filed 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. **Note:** You can remove an assigned image from an Enterprise, only if the image is not currently used by any Edge within the Enterprise.
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 the "Manage Operator Profiles" section in the *Arista VeloCloud SD-WAN Operator Guide*.

Service Access: This option is available above the global settings. 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`.

d. The **SD-WAN** service allows you to configure the following options:

Table 9: SD-WAN Service Option Descriptions

Option	Description
Default Edge Authentication	Choose the default option to authenticate the Edges associated with the Customer, from the drop-down list. • **Certificate Deactivated**: Edge uses a pre-shared key mode of authentication. • **Certificate Acquire**: This option is selected by default and instructs the Edge to acquire a certificate from the certificate authority of the Orchestrator, by generating a key pair and sending a certificate signing request to the Orchestrator. Once acquired, the Edge uses the certificate for authentication to the Orchestrator and for establishment of VCMP tunnels. **Note:** After acquiring the certificate, the option can be updated to **Certificate Required**. • **Certificate Required**: Edge uses the PKI certificate. Operators can change the certificate renewal time window for Edges using the system property `edge.certificate.renewal.window`.
Edge Licensing	Select **Add** and in the **Select Edge Licenses** pop-up window, select and assign the Edge licenses from the available list for the Enterprise. **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.

e. **Multi Cloud Service**: You can select this service only when **SD-WAN** is selected.

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

7.2 Clone a Partner Customer

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

Note: Only Partner Super Users and Partner Standard Admins can clone a Partner 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

- Edge authentication scheme
- Address groups and Port groups

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

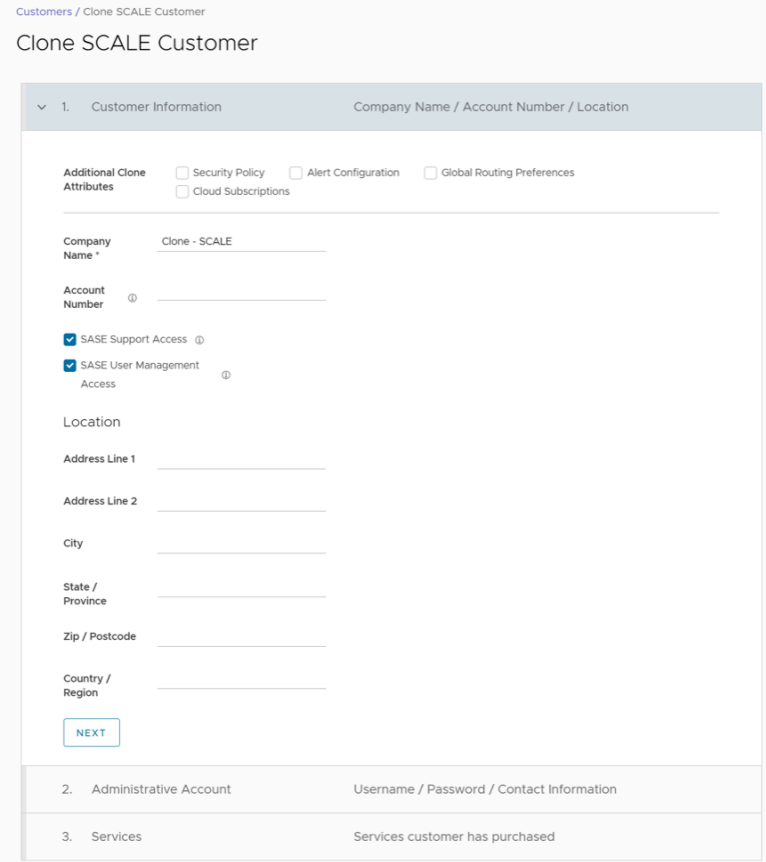
You cannot clone an Enterprise if it consists of the following:

- 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. Login to the **Orchestrator** as a Partner and navigate to **Manage Customers**.
2. On the **Manage Customers** page, select the customer you want to clone, and then select **Clone**.

The **Clone Customer** page appears.

Figure 7-5: Clone Customer



3. Configure the **Customer Information** and **Administrative Account** details, and **Services**. For additional information, see Create New Partner Customer.
4. Select **Add Customer**.

   The new customer name is displayed on the **Manage 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.

7.3 Configure Partner Customers

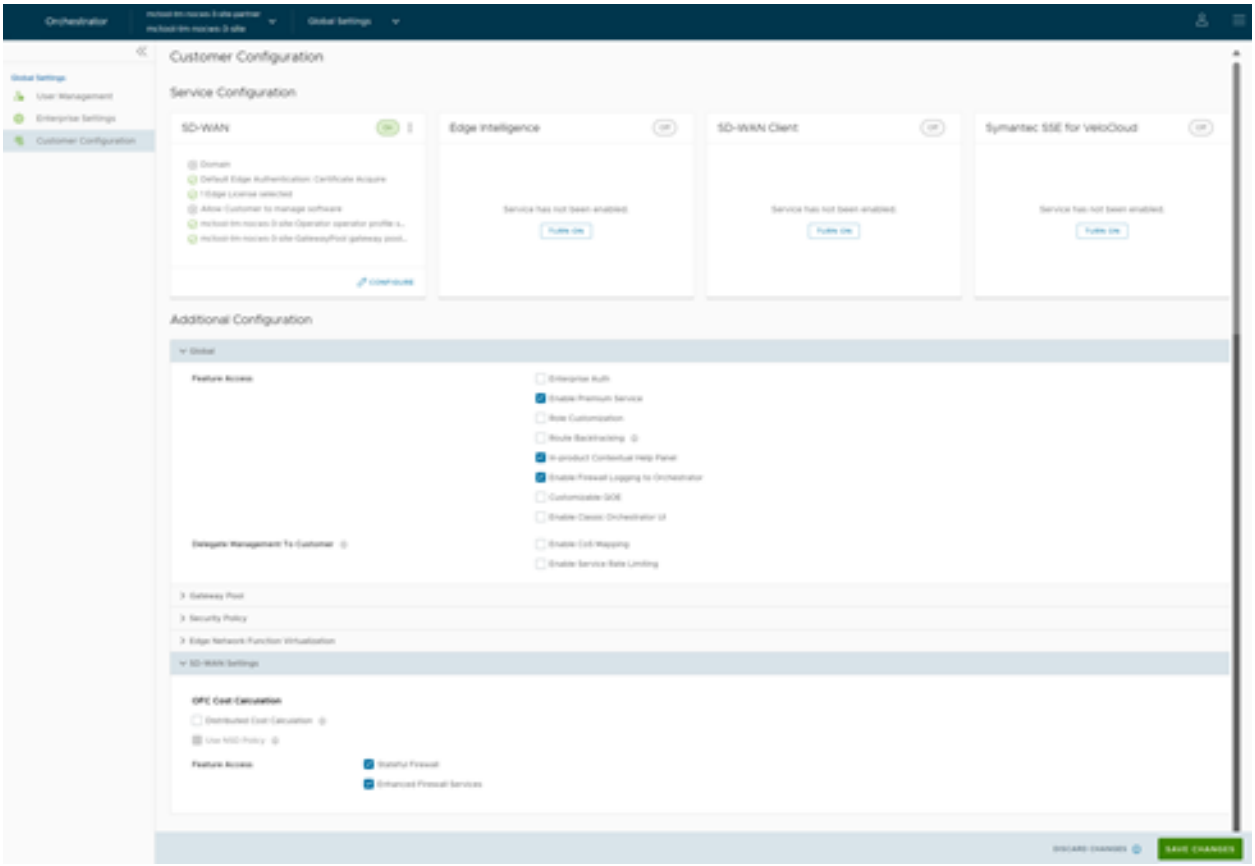
After creating a Customer, configure the feature options and settings that the Customer can access. As a Partner Super User, you can choose the settings the Partner Customer can modify.

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 Configuration page by following the below steps:

1. Login to the Orchestrator as a Partner.
2. In the **Partner** portal, select a Partner Customer, and from the top header, select **SD-WAN** > **Global Settings**.

3. From the left menu, select **Customer Configuration**.

Figure 7-6: Customer Configuration



4. In the **Service Configuration** section, under **SD-WAN**, select **Configure** to configure SD-WAN settings, and then select **Update**.

Figure 7-7: SD-WAN Configuration

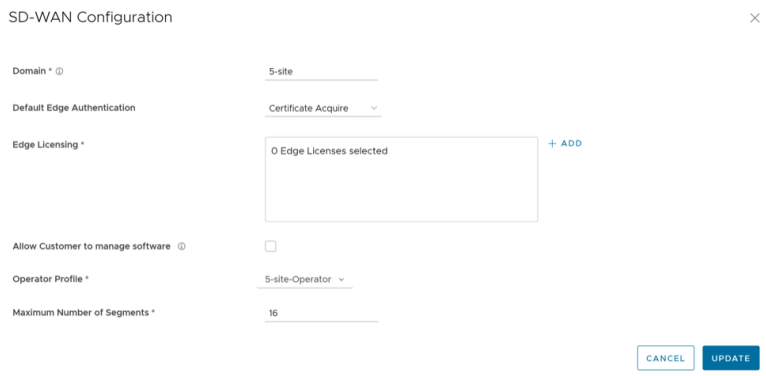


Table 10: SD-WAN Configuration Option Descriptions

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

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

Table 11: Additional Configuration Settings

Option	Description
Global	
User Agreement Display	Select either of the following from the drop-down menu: • Inherit • Override to Hide • Override to Show  **Note:** This field is available only when the system property `session.options.enableUserAgreements` is set to **True**.
Feature Access	Provides access to the selected features. Select one or additional check boxes from the below list to activate these features for the Partner Customer: • **Enterprise Auth**: By default, only the Operator can activate or deactivate two-factor authentication for an Enterprise. When you select this check box, the Enterprise Admins can configure the two-factor authentication on their own. • **Enable Premium Service**: Provides access to the available premium services. This option is selected by default. • **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 Help Panel integrated with the Orchestrator. This feature is deactivated by default. A Partner Admin must activate this option for the Partner Customers. • **Enable Firewall Logging to Orchestrator**: By default, Edges cannot send their Firewall logs to the Orchestrator. Select this check box to allow an Edge to send the Firewall logs to the Orchestrator. • **Customizable QoE**: Allows the Customer to configure the minimum and maximum latency threshold values for Voice, Video, and Transactional application categories of an Edge. • **Enable Classic Orchestrator UI**: Allows the Customer to switch from the Angular Orchestrator UI to the Classic Orchestrator UI. This option is available only when the system property `session.options.enableClassicOrchestrator` is set to **True**.
Delegate Management To Customer	Allows the Partner Customer to modify the settings of the selected property. Following two properties are always visible to the Partner Customers: • **Enable CoS Mapping**: Allows to configure CoS mapping while configuring a business policy. • **Enable Service Rate Limiting**: Allows to rate limit services in a business policy.

Option	Description
Gateway Pool	
Current Gateway Pool	Select the Gateway pool from the drop-down menu.
Gateways in this Pool	Displays the Gateway details in the current pool.
Partner Hand Off	Activating this option displays the **Configure Hand Off** section. For details, see Configure Partner Handoff.
Security Policy	
Hash	By default, there is no authentication algorithm configured for the VPN header as AES-GCM is an authenticated encryption algorithm. When you select the **Turn off GCM** check box, you can select one of the following as the authentication algorithm for the VPN header, from the drop-down menu: • SHA 1 • SHA 256 • SHA 384 • SHA 512
Encryption	Select either **AES 128** or **AES 256** as the AES algorithm's key size to encrypt data. The default encryption algorithm mode is **AES 128**.
DH Group	Select the Diffie-Hellman (DH) Group algorithm to be used when exchanging a pre-shared key. The DH Group sets the strength of the algorithm in bits. The supported DH Groups are 2, 5, 14, 15, 16, 19, 20, and 21.  **Note:** • 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.
PFS	Select the Perfect Forward Secrecy (PFS) level for additional security. The supported PFS levels are 2, 5, 14, 15, and 16. By default, PFS is deactivated.
Turn off GCM	Select this check box to activate **Hash** and select an authentication algorithm for the VPN header.
IPSec SA Lifetime Time(min)	Time when Internet Security Protocol (IPSec) rekeying is initiated for Edges. The minimum IPsec lifetime is 3 minutes and maximum IPsec lifetime is 480 minutes. The default value is **480** minutes.  **Note:** It is not recommended to configure low lifetime value for IPsec (less than 10 minutes), as it can cause traffic interruption in some deployments due to rekeys. The low lifetime values are for debugging purposes only.
IKE SA Lifetime(min)	Time when Internet Key Exchange (IKE) rekeying is initiated for Edges. The minimum IKE lifetime is 10 minutes and maximum IKE lifetime is 1440 minutes. The default value is *1440* minutes.  **Note:** It is not recommended to configure low lifetime values IKE (less than 30 minutes), as it can cause traffic interruption in some deployments due to rekeys. The low lifetime values are for debugging purposes only.

Option	Description
Secure Default Route Override	Select the check box so that the destination of traffic matching a secure default route (either Static Route or BGP Route) from a Partner Gateway can be overridden using Business Policy. **Note:** For instructions on how to activate secure routing on an Edge, refer to Configure Partner Handoff. For additional information about configuring a Network Service for Business Policy rule, refer to the "Configure Network Service for Business Policy Rule" in the *VeloCloud SD-WAN Administration Guide*.
Edge Network Function Virtualization	
Edge NFV	Select this option to activate the ability to deploy VNFs on Edges. After deploying one or more VNFs on Edges, you cannot deactivate this option.
Security VNFs	Select the relevant check boxes, to deploy the corresponding security VNFs on Edges.
SD-WAN Settings	
OFC Cost Calculation	Select the required check box: • **Distributed Cost Calculation**: Select this check box to delegate route cost calculation to Edges/Gateways. **Note:** This option is available only for the Edges/ Gateways with version 3.4.0 and later. • **Use NSD Policy**: Select this check box to use NSD policy for route cost calculation to Edges/Gateways. **Note:** This option is available only for the Edges/ Gateways with version 4.2.0 and later.
Multiple-DSCP tags per Flow Path Calculation	Select the check box to include the DSCP value as part of flow look-up. **Note:** This field is available only when the system property `session.options.enableFlowParametersConfig` is set to **True**.
Feature Access	Select **Stateful Firewall** or **Advanced Threat Protection** check box to override the corresponding settings activated on the Enterprise Edge.

6. Select **Save Changes**.

Note: When you modify the **Security Policy** settings, the changes may cause interruptions to the current services. In addition, these settings may reduce overall throughput and increase the time required for VCMP tunnel setup, which may impact branch to branch dynamic tunnel setup times and recovery from Edge failure in a cluster.

7.3.1 Configure Partner Handoff

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

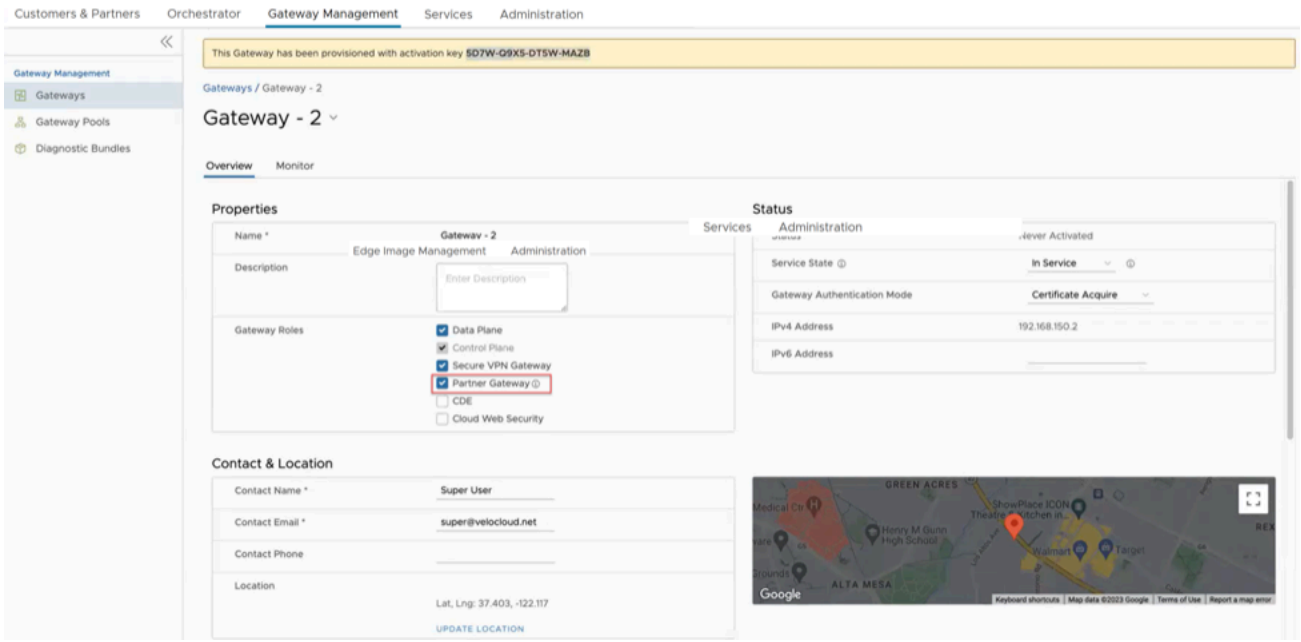
Ensure that the Gateway to be handed off to the Production Orchestrator is assigned with Partner Gateway Role and Static Routes configured as per your topology requirements.

In the Orchestrator portal, 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.

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 screen shot.

The Production Orchestrator address is advertised as secure routes by configuring subnets or static routes for the Partner Gateway. For additional information on how to configure static routes, see *Configure Gateways* section in the *Arista VeloCloud SD-WAN Operator Guide*.

Figure 7-8: Configure Partner Gateway



To configure the handoff settings, perform the following steps:

1. Log in to the **Orchestrator** as a Partner 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:

Figure 7-9: Configure Partner Hand Off

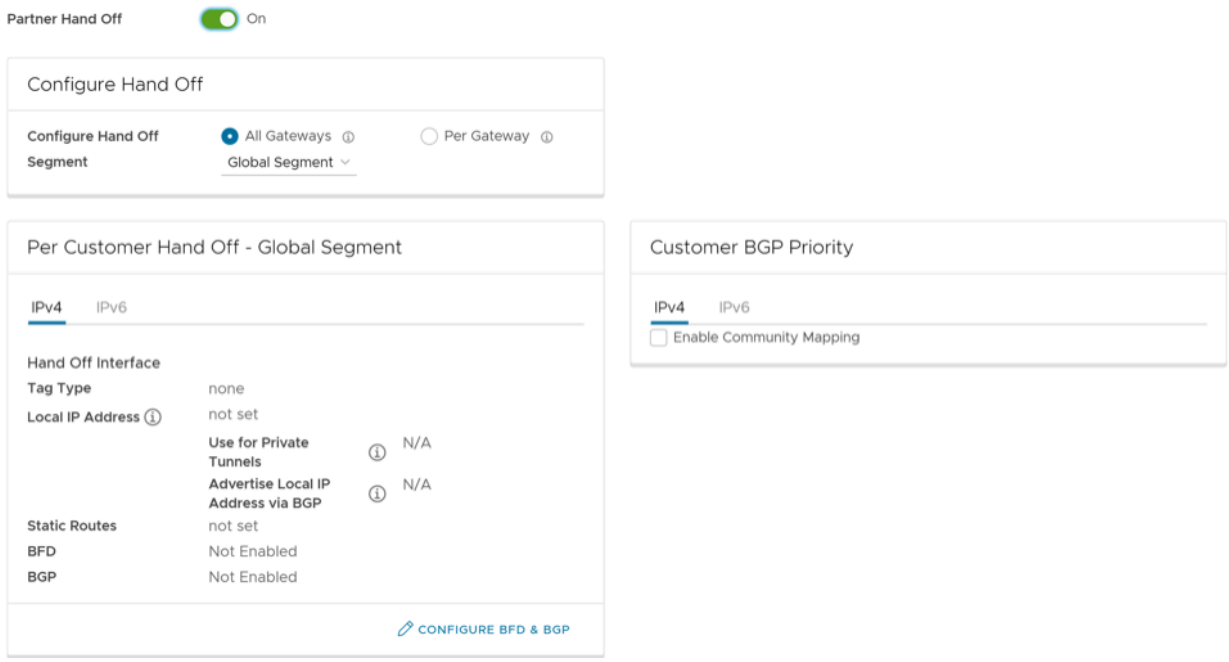
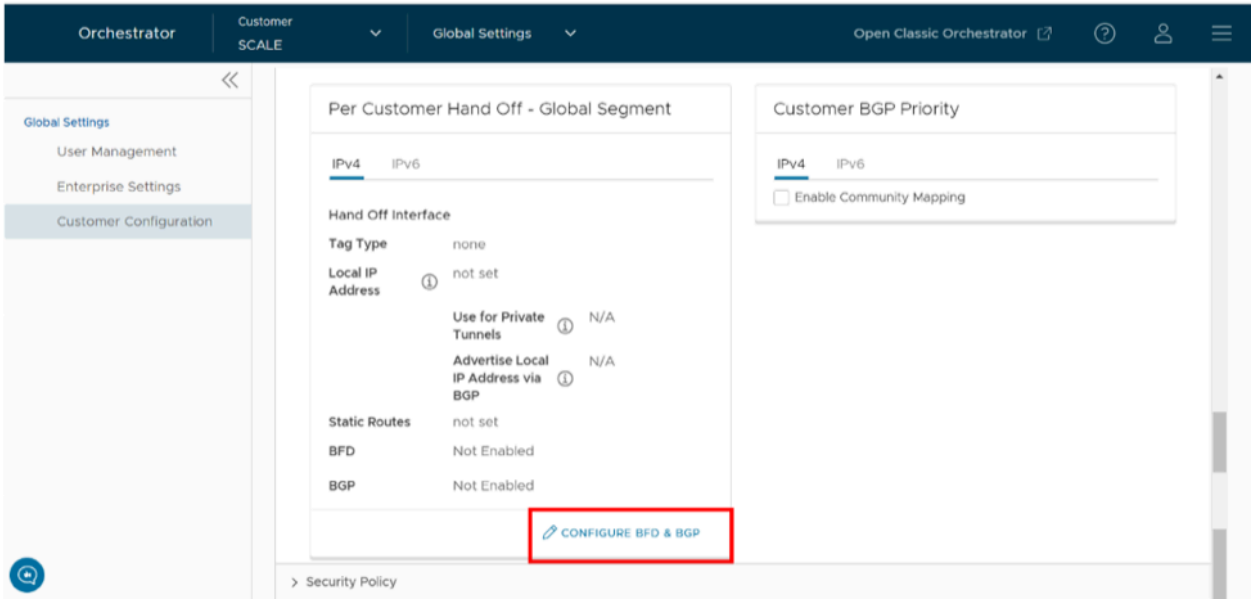


Table 12: Partner Hand Off Option Descriptions

Option	Description
Configure Hand Off	By default, the hand off configuration is applied to all the Gateways. If you want to configure a specific Gateway, choose **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.

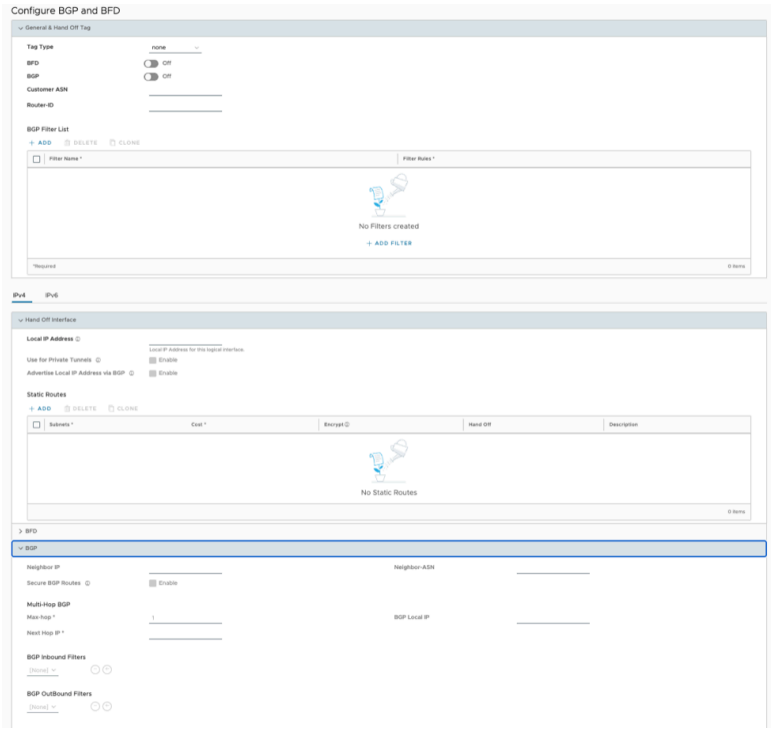
8. At the bottom of the **Per Customer Hand Off – Global Segment** area, select the **Configure BFD & BGP** link, as shown in the following image.

Figure 7-10: Configure BFD and BGP Settings for Handoff Interface



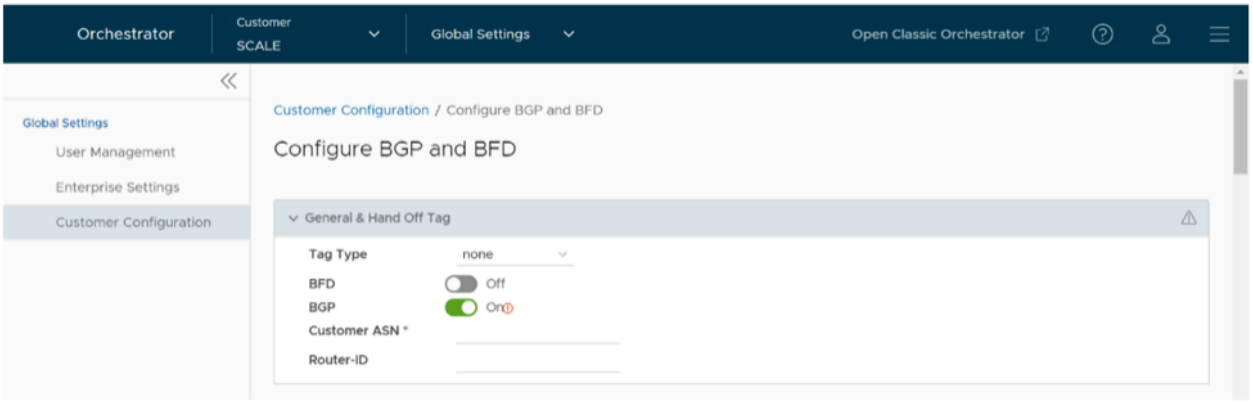
The **Configure BGP and BFD** screen displays.

Figure 7-11: Configure BGP and BFD



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

Figure 7-12: General & Hand Off Tag Settings



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

Table 13: BGP Partner Hand Off Option Descriptions

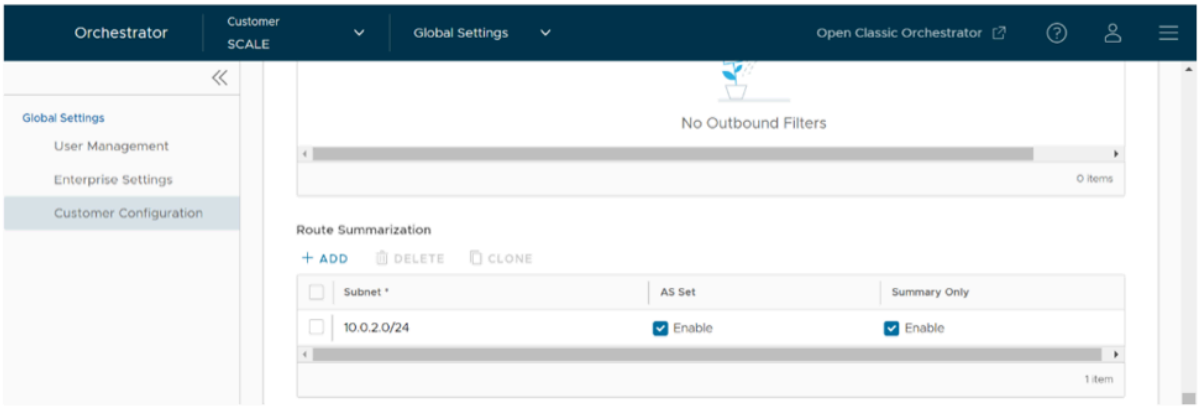
Option	Description
Hand Off Tag	
Tag Type	Choose the tag type, which is the encapsulation, in which the Gateway hands off customer traffic to the Router. The following are the types of tags available: • **None**: Untagged. Choose this during single tenant hand off or a hand off towards shared services VRF. • **802.1Q**: Single VLAN tag • **802.1ad / QinQ(0x8100) / QinQ(0x9100)**: Dual VLAN tag
Customer ASN	Enter the Customer Autonomous System Number.
Hand Off Interface: You can configure the following settings for IPv4 and IPv6.	
Local IP Address	Enter the Local IP address for the logical Hand Off interface.
Use for Private Tunnels	Select the check box so that private WAN links connect to the private IP address of the Partner Gateway. If private WAN connectivity is activated on a Gateway, the Orchestrator audits to ensure that the local IP address is unique for each Gateway within an Enterprise.
Advertise Local IP Address via BGP	Select the check box to automatically advertise the private WAN IP of the Partner Gateway through BGP. The connectivity is provided using the existing Local IP address.
Static Routes: You can add, delete, or clone a static route.	
Subnets	Enter the IP address of the Static Route Subnet that the Gateway should advertise to the Edge.
Cost	Enter the cost to apply 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.

Option	Description
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.
Next Hop IP	Enter the next-hop IP address to be used by BGP to reach the multi-hop BGP peer. **Note:** This option is available only for multi-hop eBGP with Max-hop count greater than 1.
Neighbor-ASN	Enter the Autonomous System Number of the Neighbor network.
BGP Local IP	Local IP address is the equivalent of a loopback IP address. Enter an IP address that the BGP neighborships can use as the source IP address for the outgoing BGP packets. **Note:** The BGP Local IP address must be from a different subnet than a handoff IP address. If you do not enter any value, the IP address of the **Hand Off Interface** is used as the source IP address.
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. **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.

11. If applicable, configure Route Summarization.

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

Figure 7-13: Configure Route Summarization



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

Table 14: Route Summarization Option Descriptions

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

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

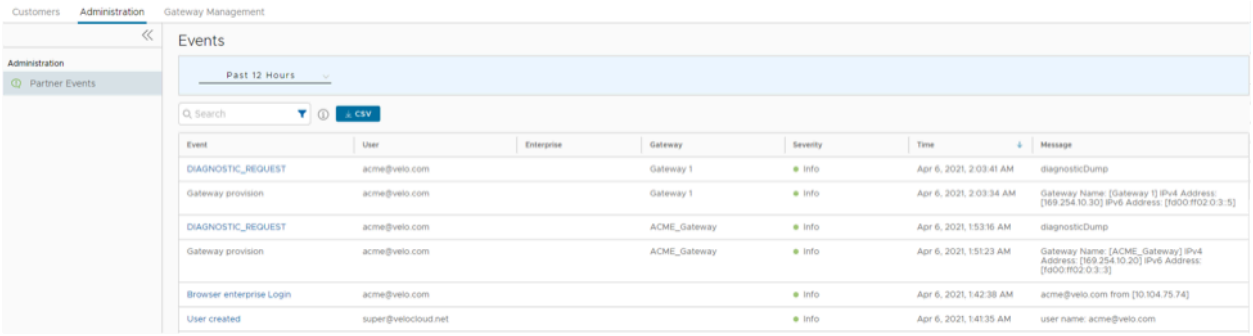
c. Select **Update** to save the settings.

Monitor Events

The Partner super user and Partner admin user can view the partner events.

1. Select **Administration** > **Partner Events** to view the events.

   Figure 8-1: Monitor Partner Events

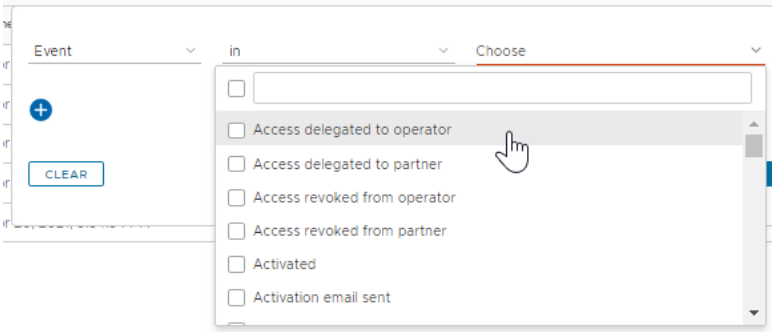


   The page displays the recent events. You can click the link to the events to view additional details.

> **Note:** The **Events** Page displays a maximum of 2048 Events. To view specific Events, you can use the Filter option.

2. At the top of the page, you can choose a specific time period to view the details of events for the selected duration.
3. 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 click the drop-down arrow next to the field to view the list of Partner Events available and to filter by specific Events.

   Figure 8-2: Search Events using Filter



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

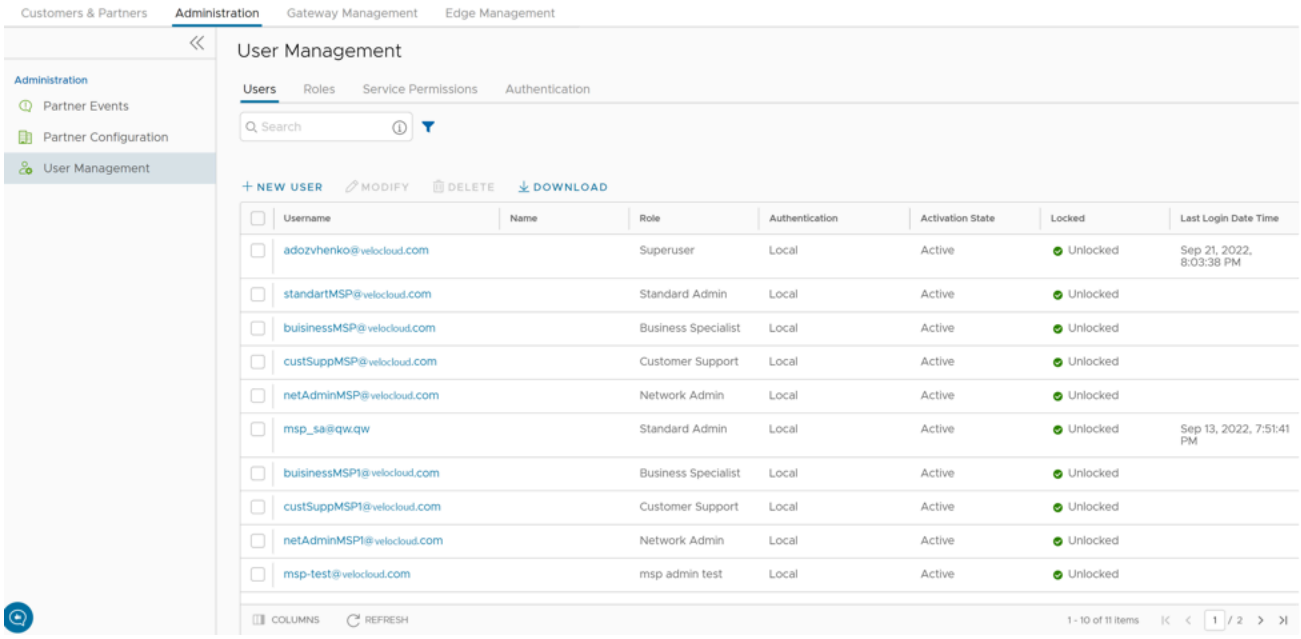
Chapter 9

User Management - Partner

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

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

Figure 9-1: User Management- Partner



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

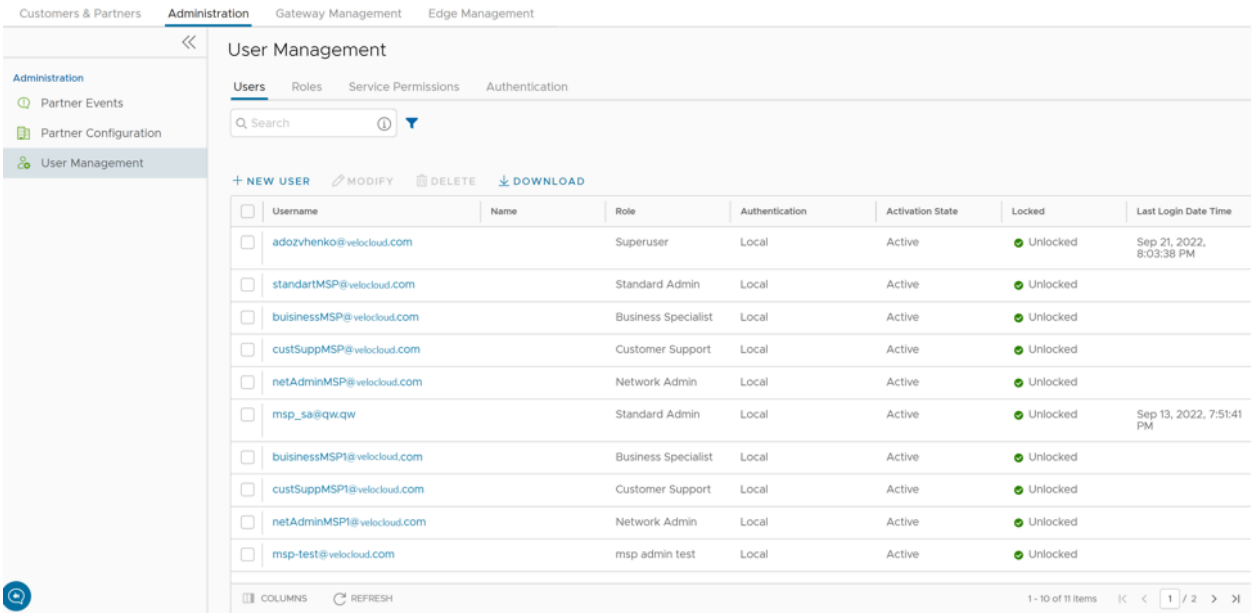
9.1 Users

As a Partner, you can view the list of existing users and their corresponding details. You can add, modify, or delete a user. However, you cannot delete a default user.

To access the **Users** tab:

1. Login to the **Orchestrator** as a Partner.
2. In the **Partner** portal, select **Administration** from the top menu.
3. From the left menu, select **User Management**. The **Users** tab is displayed by default.

Figure 9-2: Users- Partner



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

Table 15: Users Tab- Options and Descriptions

Option	Description
New User	Creates a new user. For additional information, see Add New User.
Modify	Allows you to modify the properties of the selected Partner user. You can change the **Activation State** of the selected Partner user. You can also modify the user details by selecting the username link.
Delete	Deletes the selected user. You cannot delete the default users.
Download	Select this option to download the details of all the users into a file in CSV format.

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

Table 16: Users Tab- Additional Settings

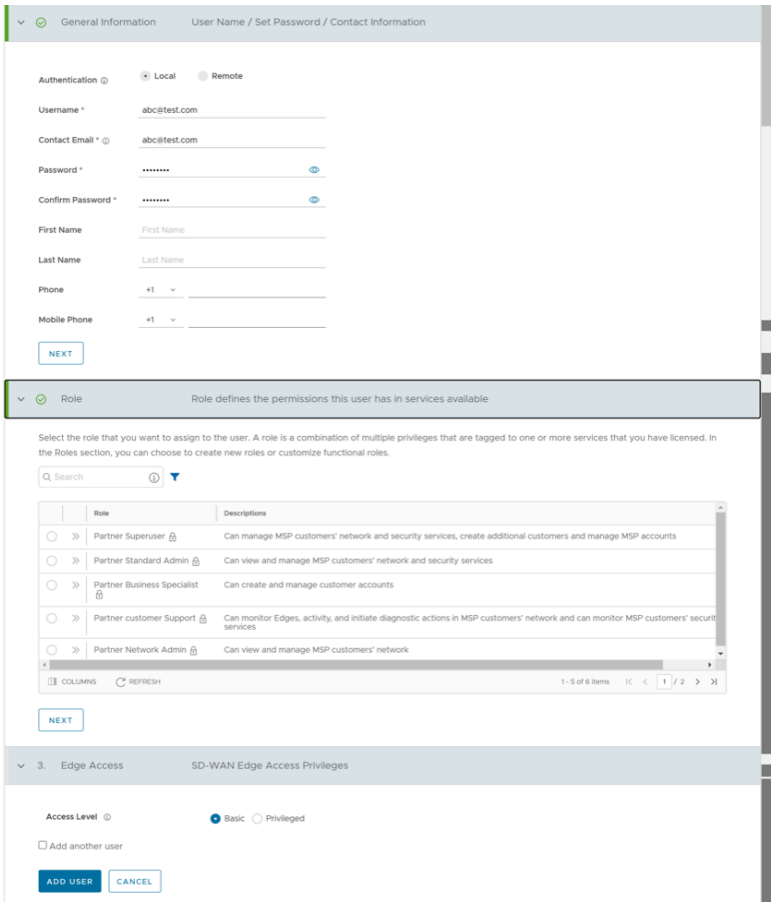
Option	Description
Search	Enter a search term to search for the matching text across the table. Use the advanced search option to narrow down the search results.
Columns	Select the columns to be displayed or hidden on the page.
Refresh	Select to refresh the page to display the most current data.

9.1.1 Add New User

In the **Partner** portal of the **Orchestrator**, you can add new users and configure the user settings. To add a new user, perform the following steps:

1. Login to the **Orchestrator** as a Partner.
2. In the **Partner** portal, select **Administration** from the top menu.
3. From the left menu, select **User Management**. The **Users** tab is displayed by default.
4. Select **New User**.

Figure 9-3: Add New User



5. Enter the following details for the new user:

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

Table 17: 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	Choose one of the following options: • **Basic**: Allows you to perform certain basic debug operations such as ping, tcpdump, PCAP, remote diagnostics, and so on. • **Privileged**: Grants you the root-level access to perform all basic debug operations along with Edge actions such as restart, deactivate, reboot, hard reset, and shutdown. In addition, you can access Linux shell. The default value is **Basic**.

6. Select the **Add another user** check box if you wish to create another user, and then select **Add User**. The new user appears in the **User Management** > > **Users** page. Select the link to the user to view or modify the details. As a Partner Administrator, you can manage the Roles, Service Permissions, and API Tokens for the Partner users. For additional information on API Tokens, see API Tokens.

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

9.1.2 API Tokens

The users can access the Orchestrator APIs using tokens instead of session-based authentication. As Partner Super User, you can manage the API tokens for your enterprise users. You can create multiple API tokens for a user.

Any user can create tokens based on the privileges they have been assigned to their user roles, except the Business Specialist users.

The users can perform the following actions, based on their roles:

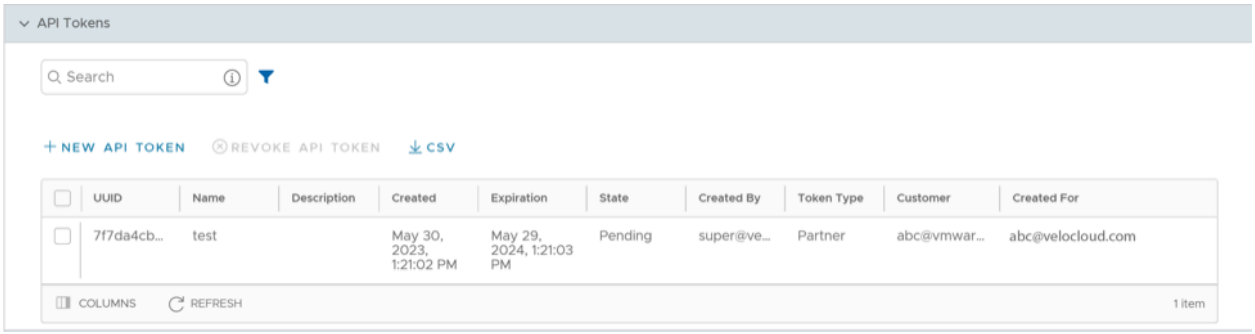
- Enterprise users can Create, Download, and Revoke tokens for them.
- Partner Super users can manage tokens of Enterprise users, if the Enterprise user has delegated user permissions to the Partner.
- Partner Super users can only create and revoke the tokens for other users.
- Users can download only their own tokens and cannot download other users' tokens.

To manage the API tokens:

1. Login to the **Orchestrator** as a Partner and 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 9-4: API Tokens



3. Select **New API Token**.

Figure 9-5: New Token

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 deactivate a token, select the token, and then select **Revoke API Token**. The status of the token is displayed as **Revoked**.
7. Select **CSV** to download the complete list of API tokens in a .csv file format.
8. 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.

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

Table 18: API Tokens - Additional Settings

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 }}'
```

9.2 Roles

The **Orchestrator** consists of two types of roles.

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

The roles are categorized as follows:

- **Privileges** – Privileges are a set of roles relevant to a service. 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 a Partner administrator:

  Table 19: Partner User Roles

Role	SD-WAN Service	Global Settings Service
Partner Standard Admin	SD-WAN Partner Admin	Global Settings Partner Admin
Partner Security Admin	SD-WAN Security Partner Admin	Global Settings Partner Admin
Partner Network Admin	SD-WAN Partner Admin	Global Settings Partner Admin
Partner Superuser	Full Access	Full Access
Partner Business Specialist	SD-WAN Partner Business	Global Settings Partner Business
Partner Customer Support	SD-WAN Partner Support	Global Settings Partner Support

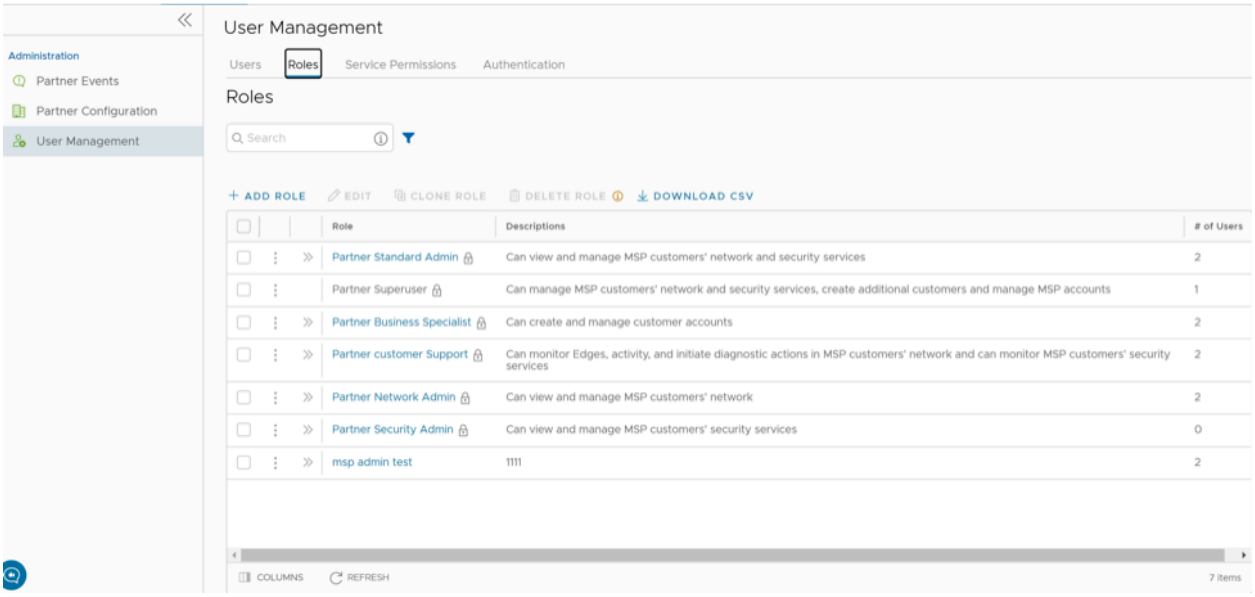
  If required, you can customize the privileges of these roles. For additional information, see Service Permissions.

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

To access the **Roles** tab:

1. Login to the **Orchestrator** as a Partner.
2. Select **Administration** from the top menu.
3. From the left menu, select **User Management**, and then select the **Roles** tab. The following screen appears:

Figure 9-6: Roles- Partner



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

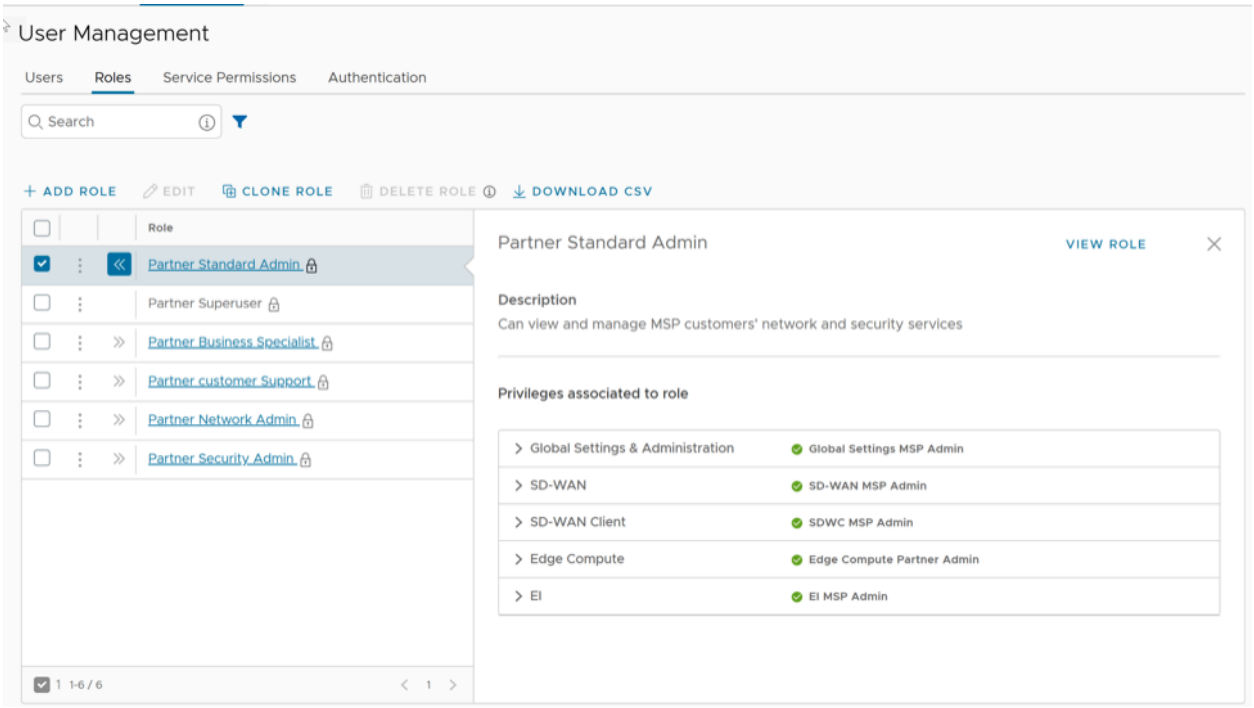
Table 20: Roles Tab- Options and Descriptions

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.

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

Figure 9-7: Open Icon



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

Table 21: Roles Tab- Additional Settings

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.

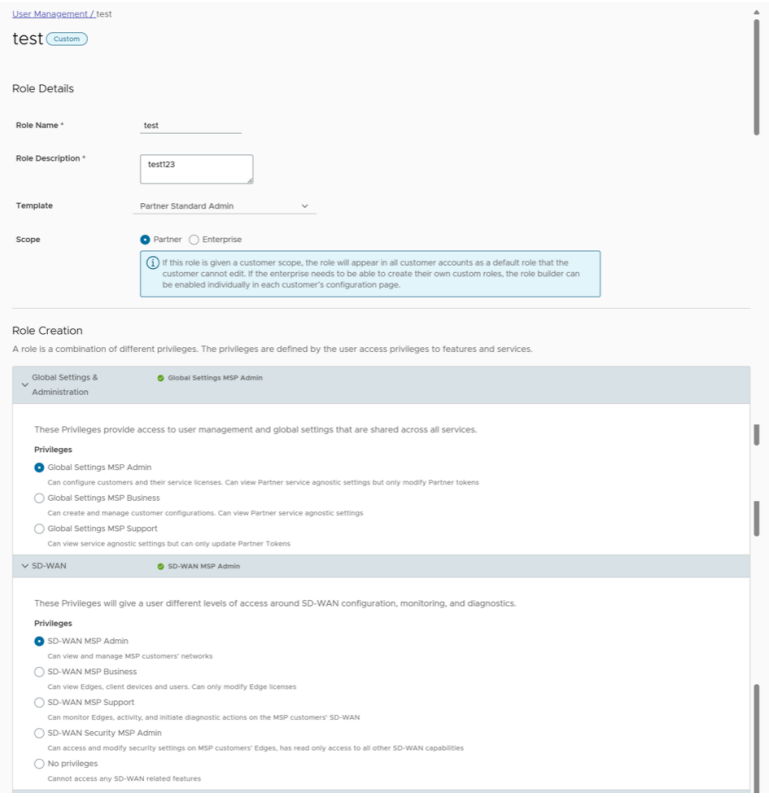
9.2.1 Add Role

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

1. Login to the **Orchestrator** as a Partner.
2. Select **Administration** from the top menu.
3. From the left menu, select **User Management**, and then select the **Roles** tab.

4. Select **Add Role**.

Figure 9-8: Add Role



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

Table 22: 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 either **Partner** or **Enterprise** as the scope for the new role. A role with the **Partner** scope can be applied to Partner level Administrators for the current Partner. A role with the **Enterprise** scope appears in the role list for all of the Partner's Customers.
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 MSP Support** is selected for the **Partner** scope. For the **Enterprise** scope, **Global Settings Enterprise Read Only** is selected by default.
SD-WAN	These privileges provide the 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**.

6. 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.

9.3 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**.
- Only an Operator Superuser can activate Role Customization for a Partner Superuser. If the Role Customization option is not available for you, contact your Operator.

When you customize a Service Permission, the changes 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.

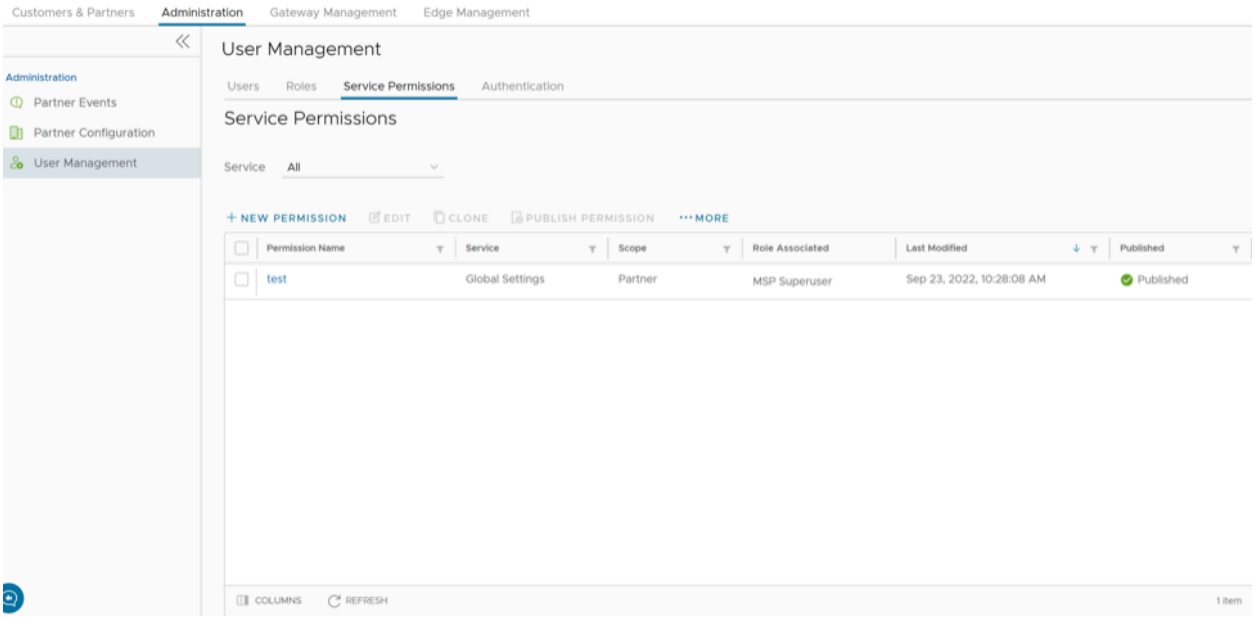
Note: For information on user privileges, see the topic **List of User Privileges**.

To access the **Service Permissions** tab:

1. Login to the **Orchestrator** as a Partner.
2. Select **Administration** from the top menu.

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

Figure 9-9: Service Permissions - Partner



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

Table 23: Service Permissions - Options and Descriptions

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

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

Table 24: Service Permissions - Additional Settings

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

Note: 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.

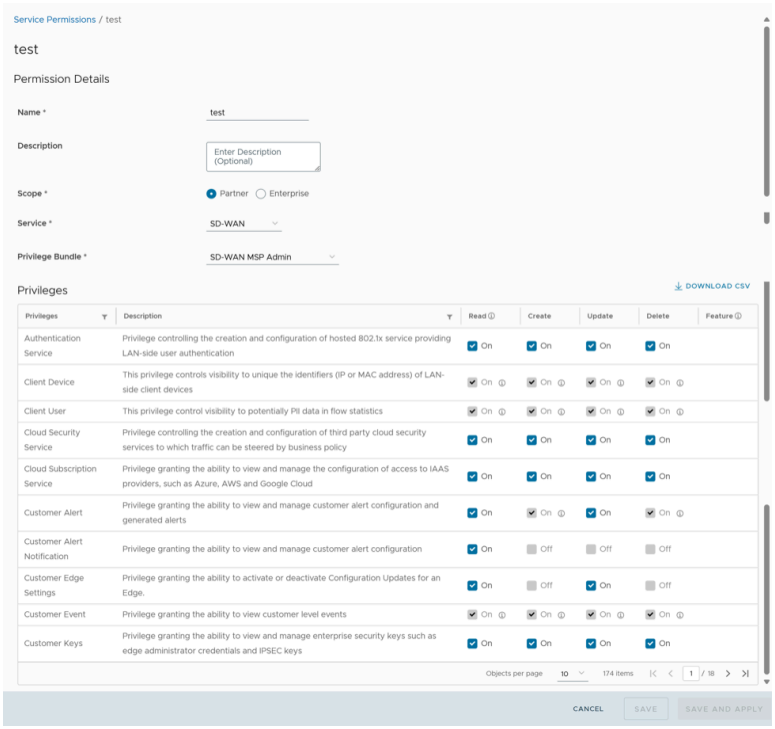
9.3.1 New Permission

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. Login to the **Orchestrator** as a Partner.
2. Select **Administration** from the top menu.
3. From the left menu, select **User Management**, and then select the **Service Permissions** tab.
4. Select **New Permission**. The following screen appears:

Figure 9-10: New Permission



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

Table 25: 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 **Partner** or **Enterprise** as the scope. A Partner can customize the permissions for Partners and Customers.
Service	Select a service from the drop-down menu. The available services are: • **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.

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

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

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

9.3.2 List of User Privileges

This section lists all the role privileges available in the Partner portal of the Orchestrator.

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 26: 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 Customers, from the Partner or Operator level	Yes	No	No
	Read Customer				
	Update Customer			Yes	Yes
	Delete Customer			No	No
	Manage Customer				
Partner Events	Create Partner Event	Grants access to view Partner events	Yes	No	No
	Read Partner Event			Yes	Yes
	Update Partner Event			No	No
	Delete Partner Event				
	Manage Partner Event				
Partner Admins	Create Partner User	Grants access to view and configure Partner administrators	Yes	No	No
	Read Partner User			Yes	Yes
	Update Partner User			No	No
	Delete Partner User				
	Manage Partner User				
Partner Admins > API Tokens	Create Partner Token	Grants ability to view and manage operator authentication tokens	Yes	No	No
	Read Partner Token				
	Update Partner Token				
	Delete Partner Token				
	Manage Partner Token				
Service Permissions	Create Service Permissions Package	Grants access to manage Service Permissions packages	Yes	No	No
	Read Service Permissions Package				
	Update Service Permissions Package				
	Delete Service Permissions Package				
	Manage Service Permissions Package				
Partner Overview	Update Partner	Grants access to view and Partners	Yes	No	No

Feature	Name of the Privilege	Description	Allow Privilege	Deny Privilege	Customizable
Partner Overview > Other Settings	Read User Agreement	Grants access to configure the customer user agreement feature	Yes	No	No
	Update User Agreement				
Partner Settings	Read Partner Delegation	Grants ability to view and edit the delegation of Partner privileges to the Operator	Yes	No	No
Partner Settings > General Information > Privacy Settings	Read Customer Delegation	Grants ability to view and manage the delegation of privileges from the customer to Partners or the Operator	Yes	Yes	Yes
	Update Customer Delegation				No
Partner Settings > Authentication	Create Partner Authentication	Grants ability to view and edit Partner authentication mode and associated configuration	Yes	No	No
	Read Partner Authentication				
	Update Partner Authentication				
	Delete Partner Authentication				
	Manage Partner Authentication				
Partner Settings > Authentication > API Tokens	Create Partner Token	Grants ability to view and manage operator authentication tokens	Yes	No	No
	Read Partner Token				
	Update Partner Token				
	Delete Partner Token				
	Manage Partner Token				
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				
Gateway Pools Gateways Gateway Diagnostic bundles	Create Gateway	Grants ability to view and manage Gateways, from the Partner or Operator level	Yes	Yes	Yes
	Read Gateway				
	Update Gateway				
	Delete Gateway				
	Manage Gateway				
	View Tab Gateway List	Grants ability to view the Gateway list tab	No	Yes	Yes
Gateway Diagnostic Bundles > Download Diagnostic Bundles	Download Gateway Diagnostics	Grants ability to download Gateway Diagnostics	No	Yes	Yes

Feature	Name of the Privilege	Description	Allow Privilege	Deny Privilege	Customizable
VeloCloud Support Access Role	Create Partner Delegation Read Partner Delegation Update Partner Delegation Delete Partner Delegation Manage Partner Delegation	Grants ability to view and edit the delegation of Partner privileges to the Operator	Yes	No	No

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

Below table provides a list of customizable feature privileges:

Table 27: 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 **Note:** This is for 610-LTE devices only.	Remote LTE Switch SIM Slot	Grants ability to activate the SIM Switchover feature. After the test is successful, you can check the status from Monitor > Edges > Overview tab
Diagnostics > Remote Diagnostics	List Paths	Remote List Paths	Grants ability to view the list of active paths between local WAN links and each peer
Diagnostics > Remote Diagnostics	List current IKE Child SAs	Remote List current IKE Child SAs	Grants ability to use filters to view the exact Child SAs you want to see

Navigation Path in the Enterprise Portal	Name of the Tab	Name of the Privilege	Description
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
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 SD-WAN 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 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

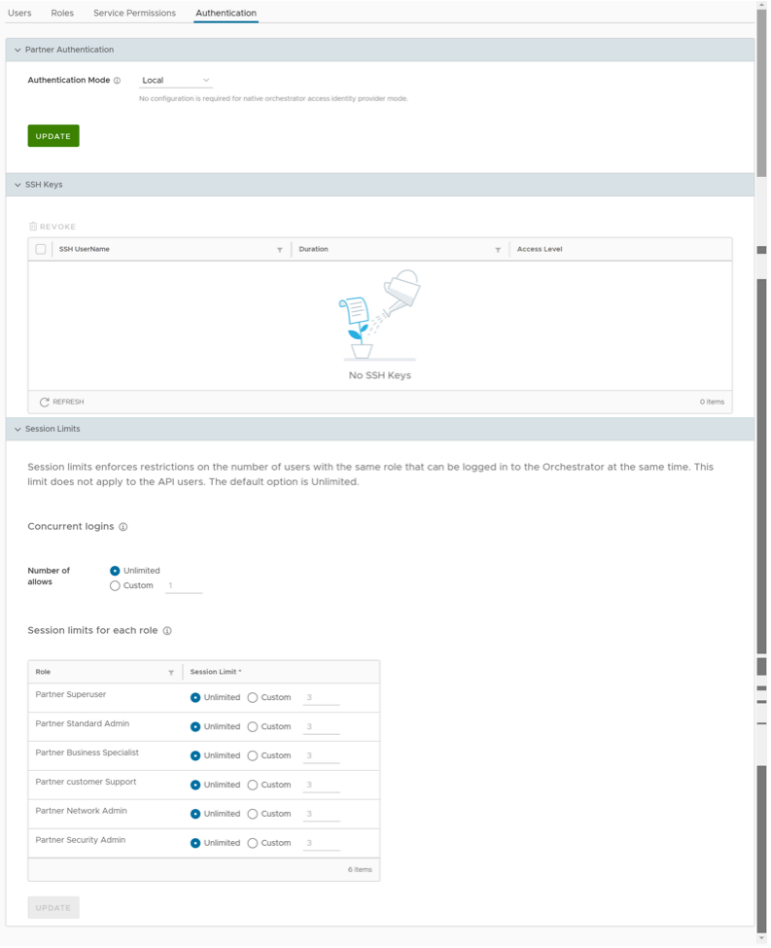
9.4 Authentication

The Authentication feature allows you to set the authentication mode for a Partner and an Enterprise user.

To access the **Authentication** tab:

1. Login to the **Orchestrator** as a Partner and from the top menu, select **Administration** from the top menu.
2. From the left menu, select **User Management**, and then select the **Authentication** tab. The following screen appears:

   Figure 9-11: Authentication- Partner



3. **Partner Authentication**:

   Select one of the following Authentication modes:

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

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

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

Figure 9-12: Single Sign-on Mode

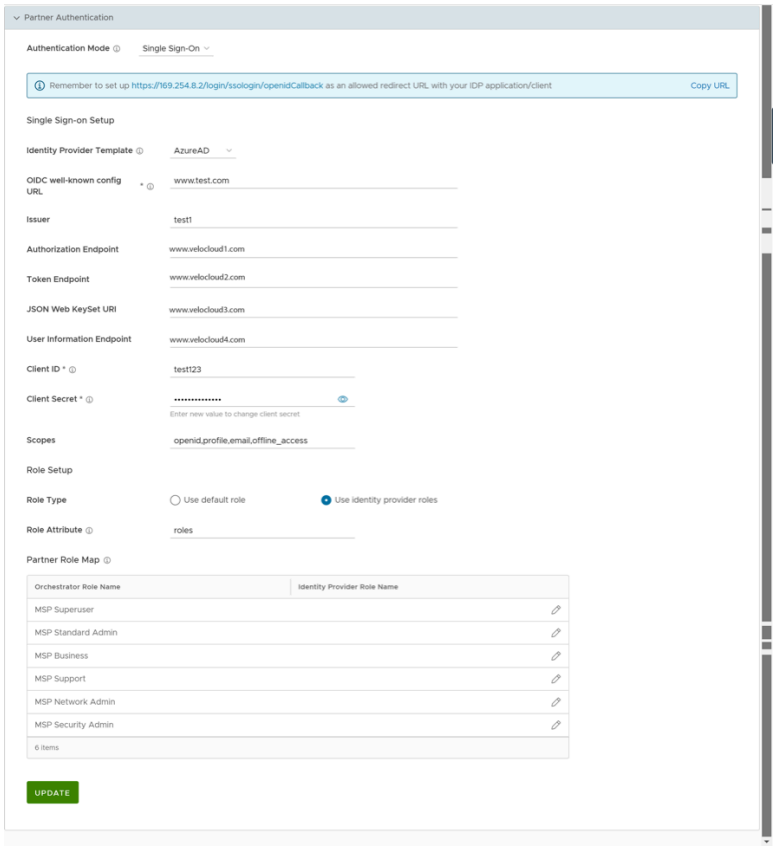


Table 28: Single Sign-on Mode- Options and Descriptions

Option	Description
Identity Provider Template	From the drop-down menu, select your preferred Identity Provider (IdP) that you have configured for Single Sign On. This pre-populates fields specific to your IdP. **Note:** You can also manually configure your own IdPs by selecting **Others** from the drop-down menu.
OIDC well-known config URL	Enter the OpenID Connect (OIDC) configuration URL for your IdP. For example, the URL format for Okta will be: `https://{oauth-provider-url}/.well-known/openid-configuration`.
Issuer	This field is auto-populated based on your selected IdP.
Authorization Endpoint	This field is auto-populated based on your selected IdP.
Token Endpoint	This field is auto-populated based on your selected IdP.
JSON Web Key Set URI	This field is auto-populated based on your selected IdP.
User Information Endpoint	This field is auto-populated based on your selected IdP.
Client ID	Enter the client identifier provided by your IdP.
Client Secret	Enter the client secret code provided by your IdP, that is used by the client to exchange an authorization code for a token.
Scopes	This field is auto-populated based on your selected IdP.
Role Type	Choose one of the following two options: • Use default role • Use identity provider roles
Role Attribute	Enter the name of the attribute set in the IdP to return roles.
Partner Role Map	Map the IdP-provided roles to each of the Partner user roles.

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

4. **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 a Partner, 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.

5. **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 29: 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 Partner in the **Roles** tab, are displayed in this section.

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

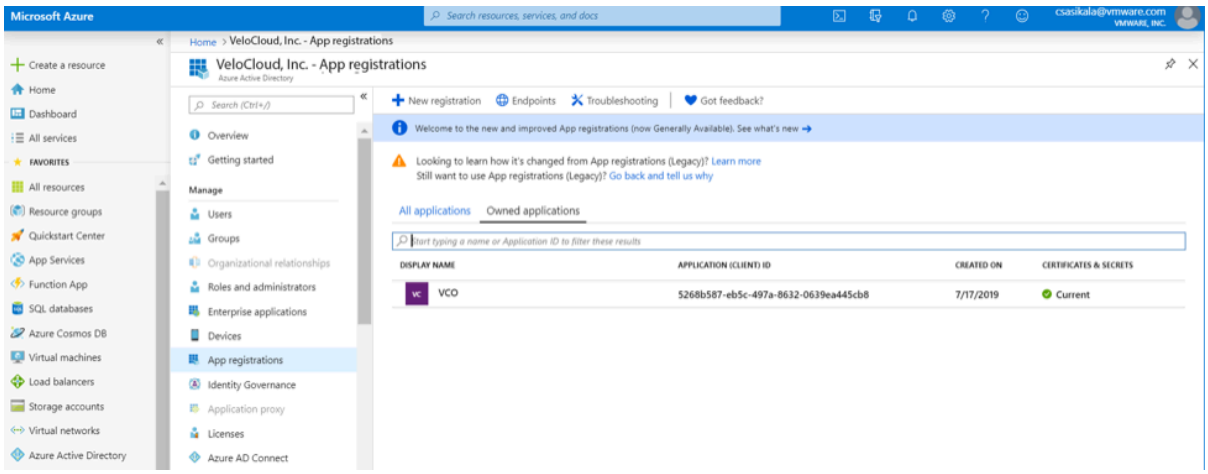
9.4.1 Configure Azure Active Directory for Single Sign On

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.

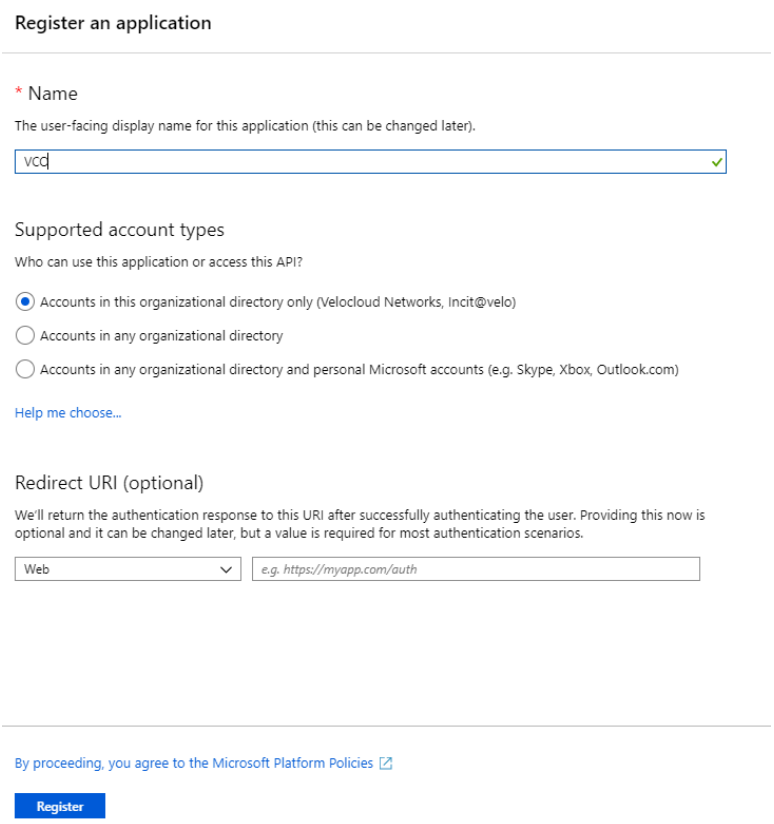
1. Log in to your Microsoft Azure account as an Admin user. The **Microsoft Azure** home screen appears.
2. To create a new application:
   a. Search and select the **Azure Active Directory** service.

Figure 9-13: Azure Active Directory



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

Figure 9-14: Register an application



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

d. In the **Redirect URL** field, enter the redirect URL that your Orchestrator application uses as the callback endpoint. In the Orchestrator application, at the bottom of the **Configure Authentication** screen, you can find the redirect URL link. Ideally, the Orchestrator redirect URL will be in this format: `https://<Orchestrator URL>/login/ssologin/openidCallback`.

e. In the **Redirect URL** field, enter the redirect URL that your Orchestrator application uses as the callback endpoint. In the Orchestrator application, at the bottom of the **Configure Authentication** screen, you can find the redirect URL link. Ideally, the Orchestrator redirect URL will be in this format: `https://<Orchestrator URL>/login/ssologin/openidCallback`.

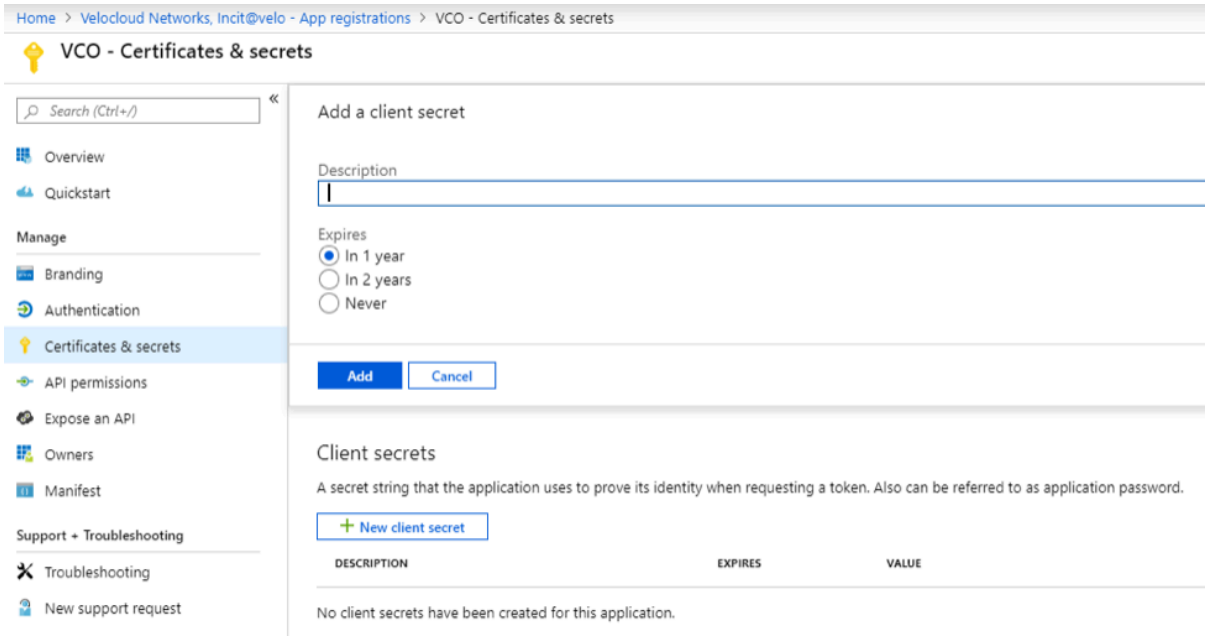
f. Select **Register**. Your Orchestrator application will be registered and displayed in the **All applications** and **Owned applications** tabs. Make sure to note down the Client ID/Application ID to be used during the SSO configuration in Orchestrator.

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

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

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

Figure 9-15: Add a client secret

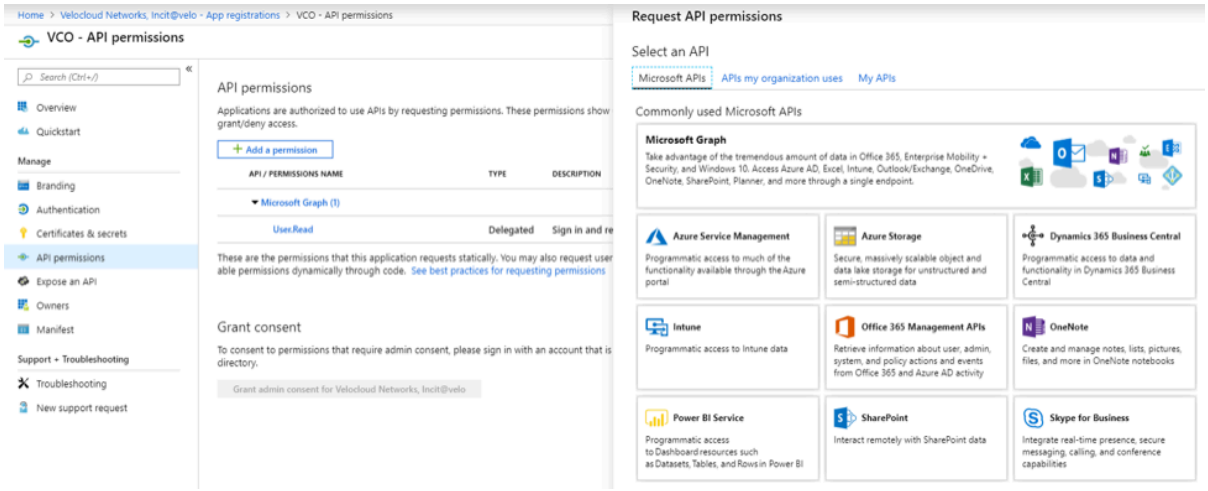


j. Provide details such as description and expiry value for the secret and select **Add**.

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

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

Figure 9-16: Request API permissions



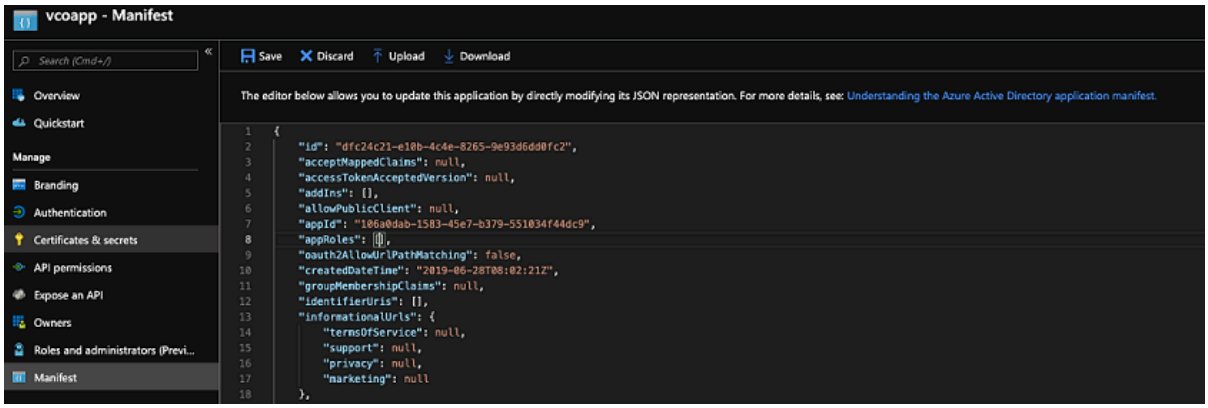
l. Select **Microsoft Graph** and select **Application permissions** as the type of permission for your application.

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

n. Select **Add permissions**.

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

Figure 9-17: Manifest



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

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

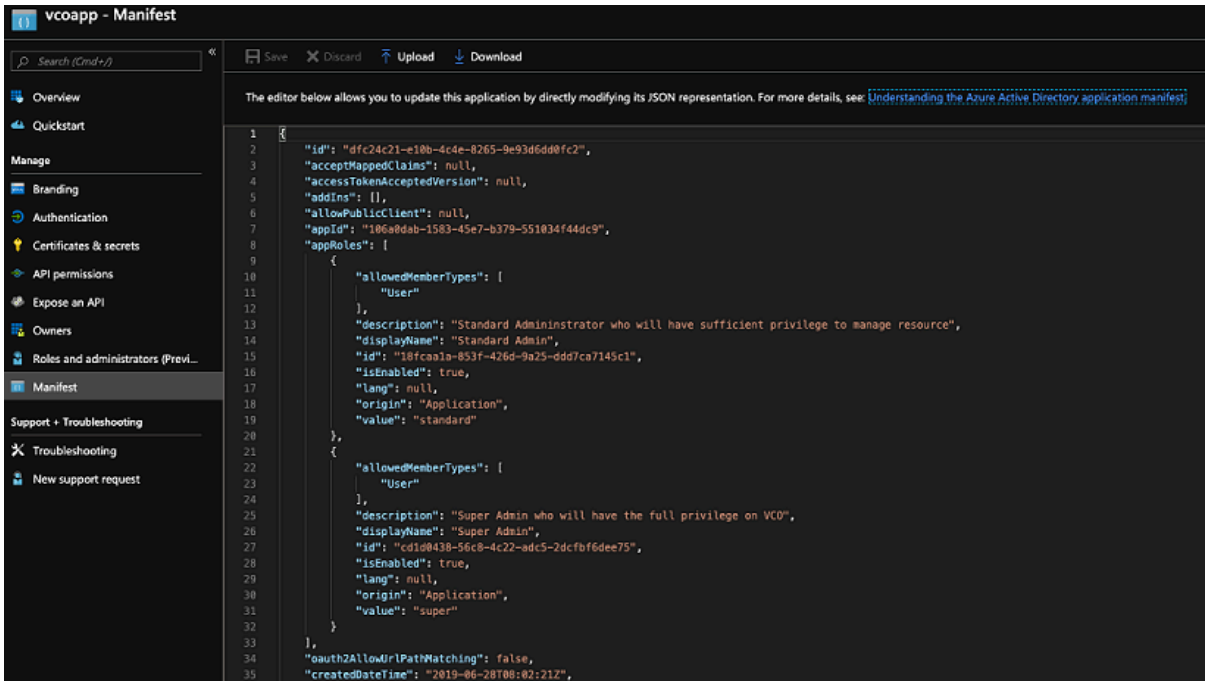
Sample role objects:

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

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

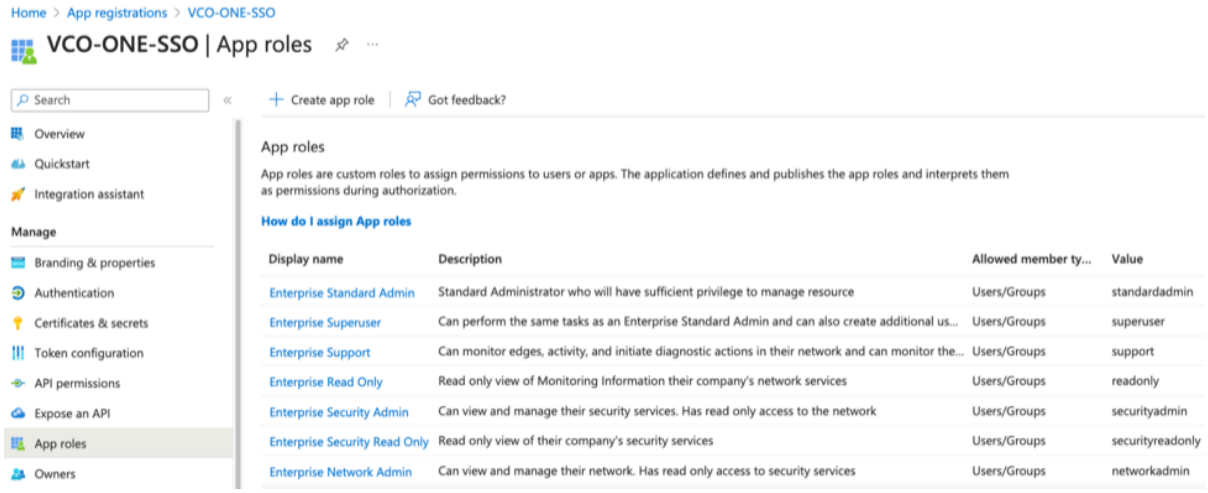
- Windows - powershell [guid]::NewGuid()

Figure 9-18: Manifest



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

Figure 9-19: App Roles



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

a. Go to **Azure Active Directory** > **Enterprise applications**.

b. Search and select your Orchestrator application.

c. Select **Users and groups** and assign users and groups to the application.

d. Select **Submit**.

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

Configure Single Sign On in the Orchestrator.

9.4.2 Configure Okta for Single Sign On

Ensure you have an Okta account to sign in.

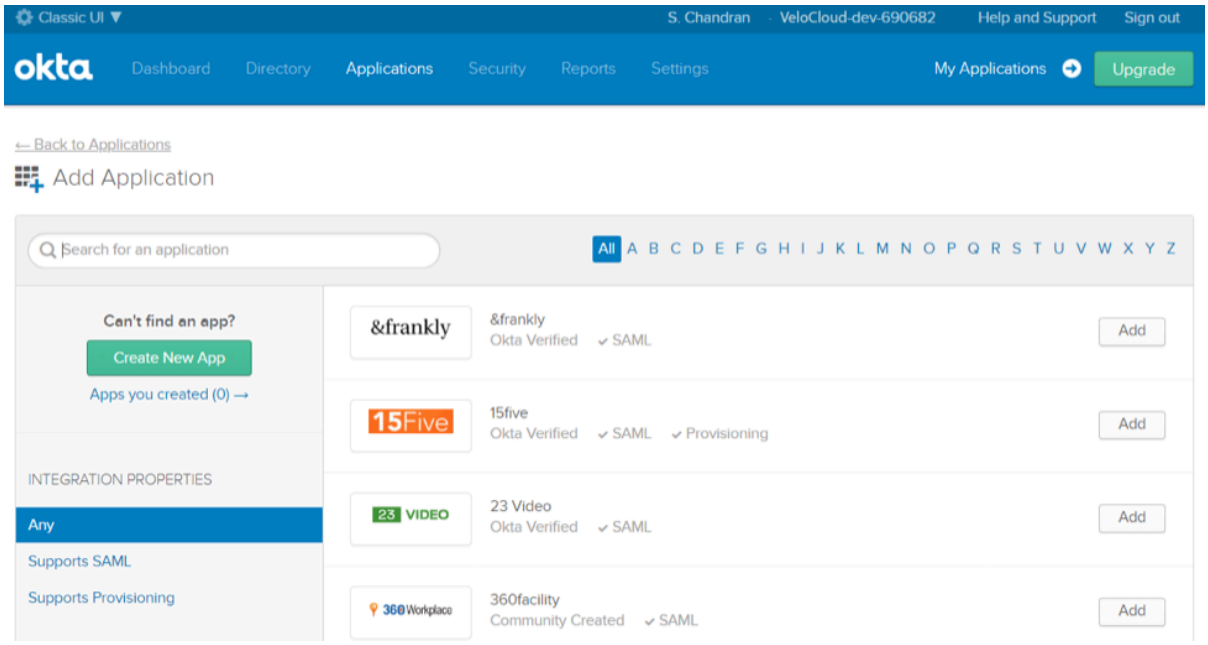
To support OpenID Connect (OIDC)-based Single Sign On (SSO) from Okta, you must first set up an application in Okta. To set up an OIDC-based application in Okta for SSO, perform the steps on this procedure.

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 9-20: Add Application

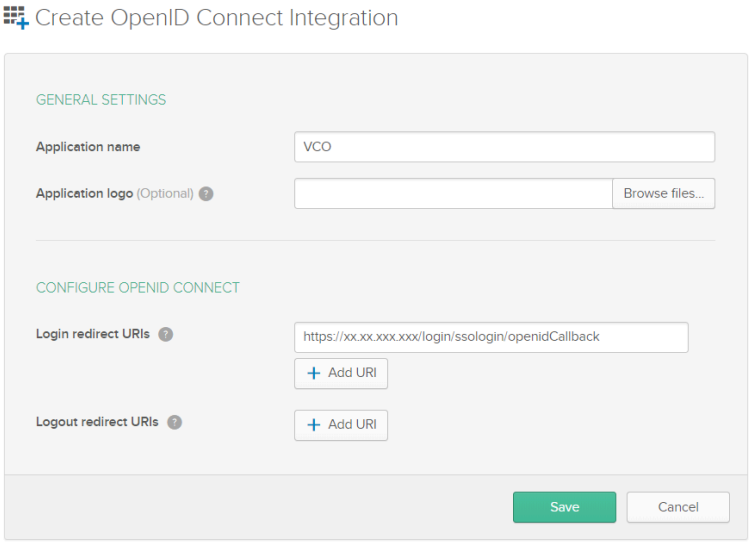


   b. Select **Create New App**. The **Create a New Application Integration** dialog box appears.

   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 9-21: Create OpenID Connect Integration



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

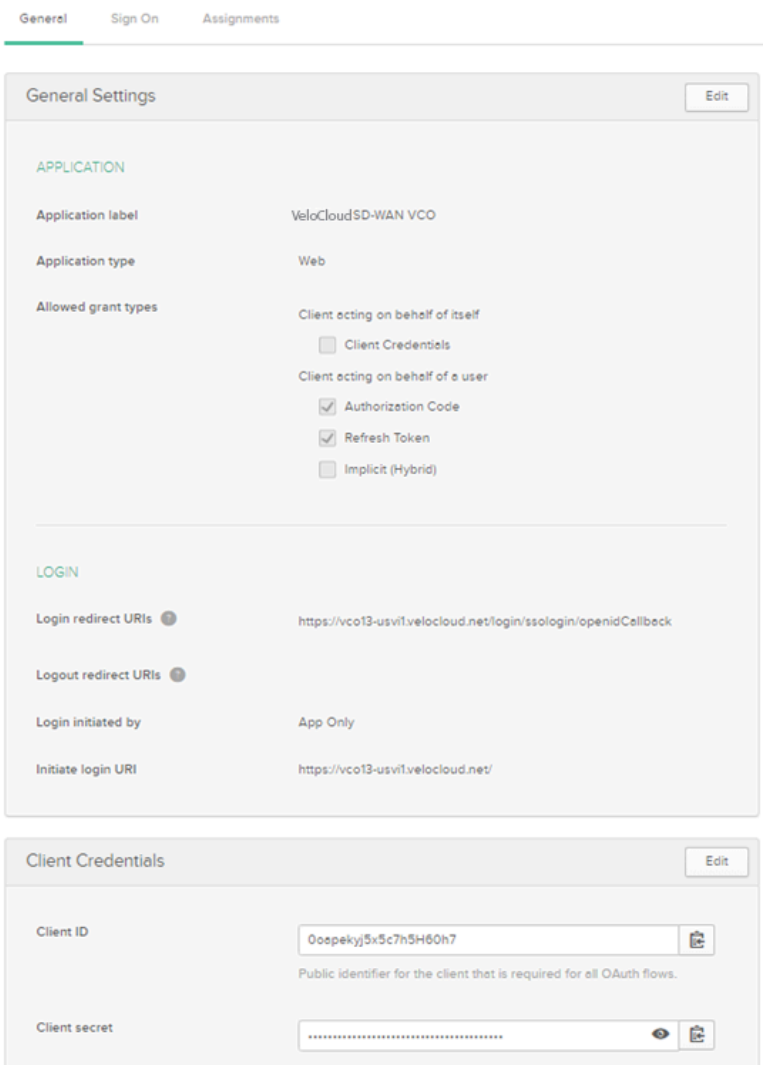
f. Under the **CONFIGURE OPENID CONNECT** area, in the **Login redirect URIs** text box, enter the redirect URL that your Orchestrator application uses as the callback endpoint.

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

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

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

Figure 9-22: Application



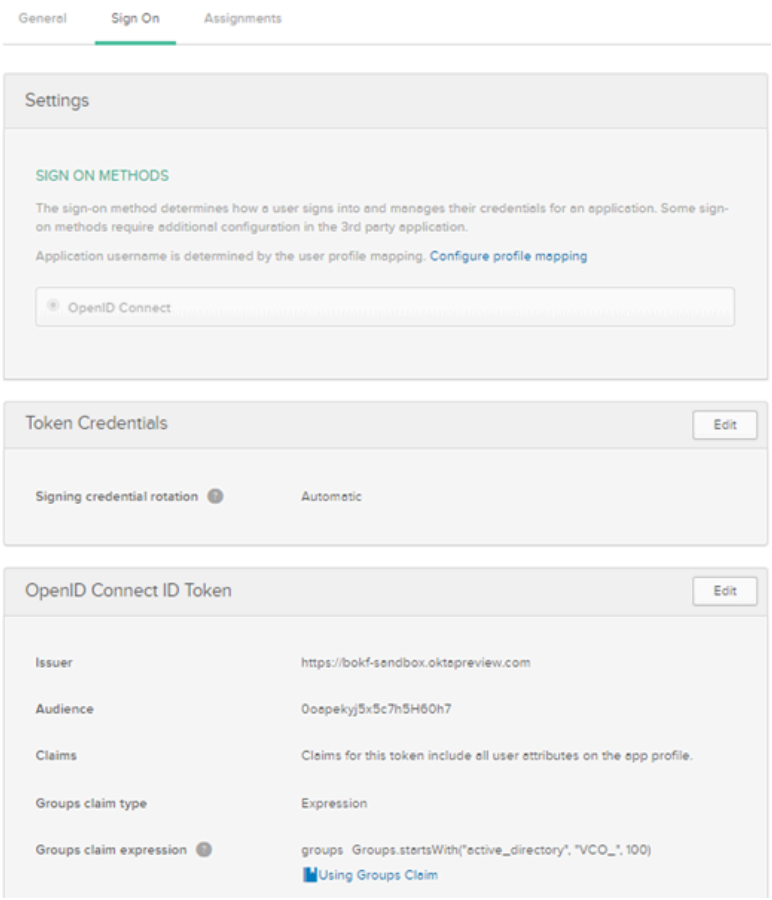
j. Select the **Sign On** tab and under the **OpenID Connect ID Token** area, select **Edit**.

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

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

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

Figure 9-23: Groups claim expression



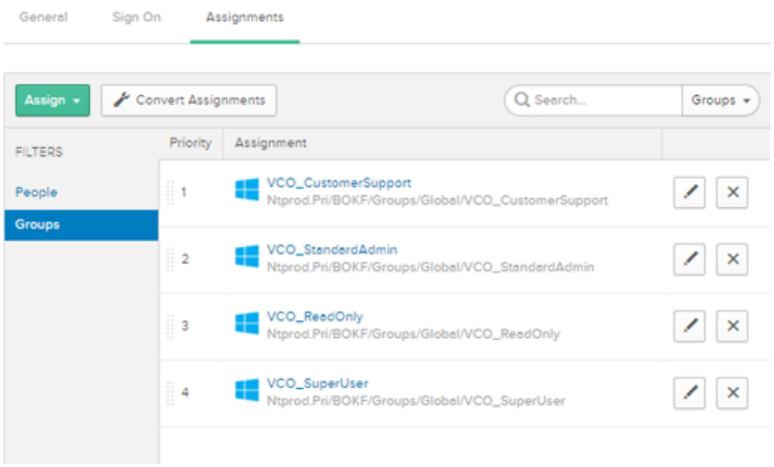
3. To assign groups and users to your Orchestrator application:

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

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

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

Figure 9-24: Groups tab



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

Configure Single Sign On in the Orchestrator.

9.4.3 Configure OneLogin for Single Sign On

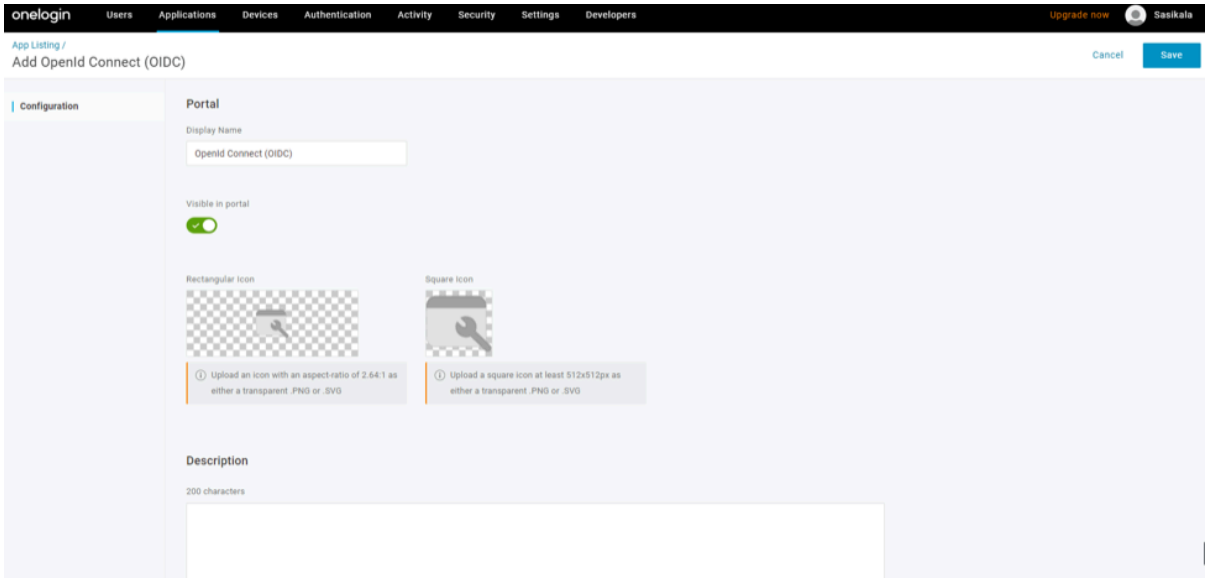
Ensure you have an OneLogin account to sign in.

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 9-25: Add OpenId Connect (OIDC)

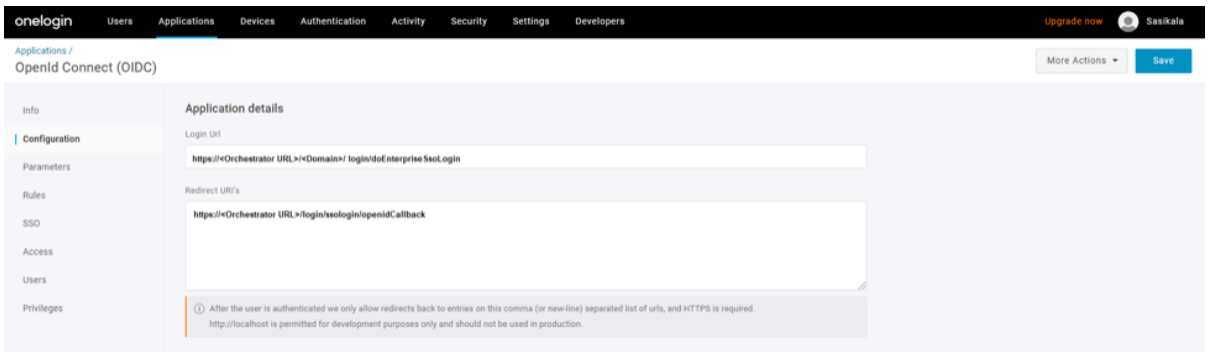


c. In the **Display Name** text box, enter the name for your application and select **Save**.

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

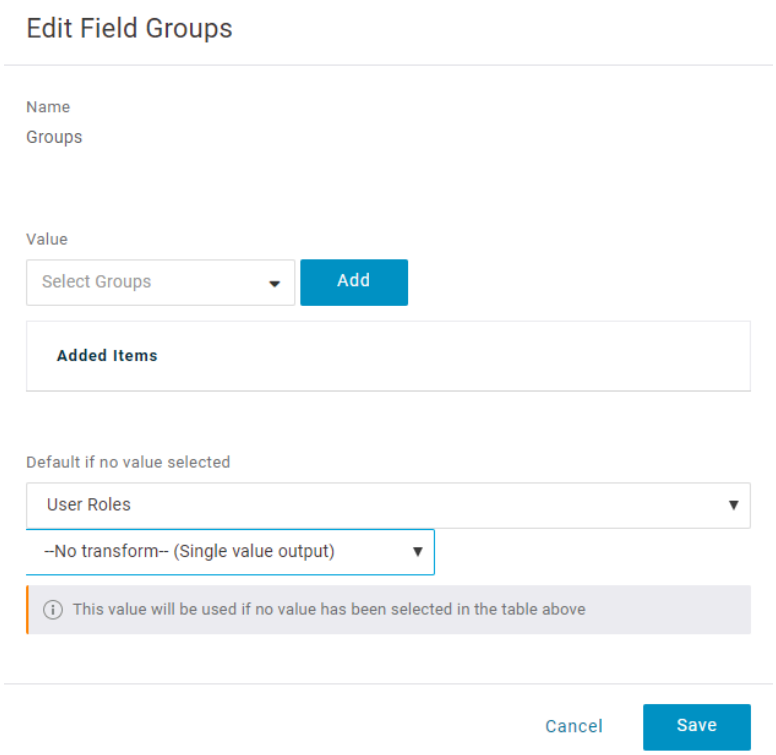
- **Login URL**- The login URL will be in this format: `https://<Orchestrator URL>/<Domain>/ login/doEnterpriseSsoLogin`. Where, <Domain> is the domain name of your Enterprise that you must have already set up to enable SSO authentication for the Orchestrator. You can get the Domain name from the Enterprise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

Figure 9-26: Application Details



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

Figure 9-27: Edit Field Groups

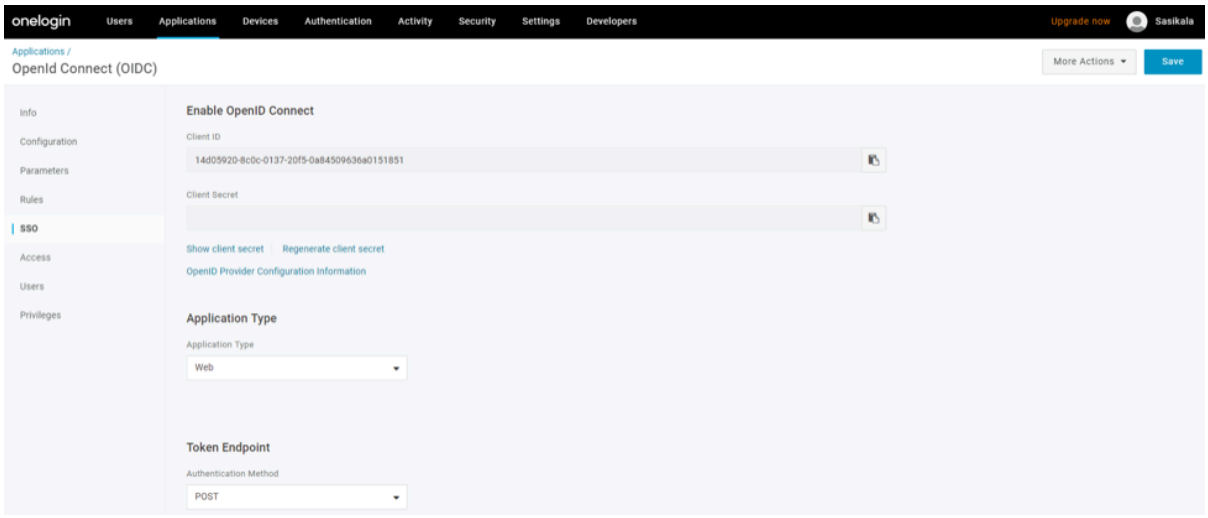


f. Configure User Roles with value “--No transform--(Single value output)” to be sent in groups attribute and select **Save**.

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

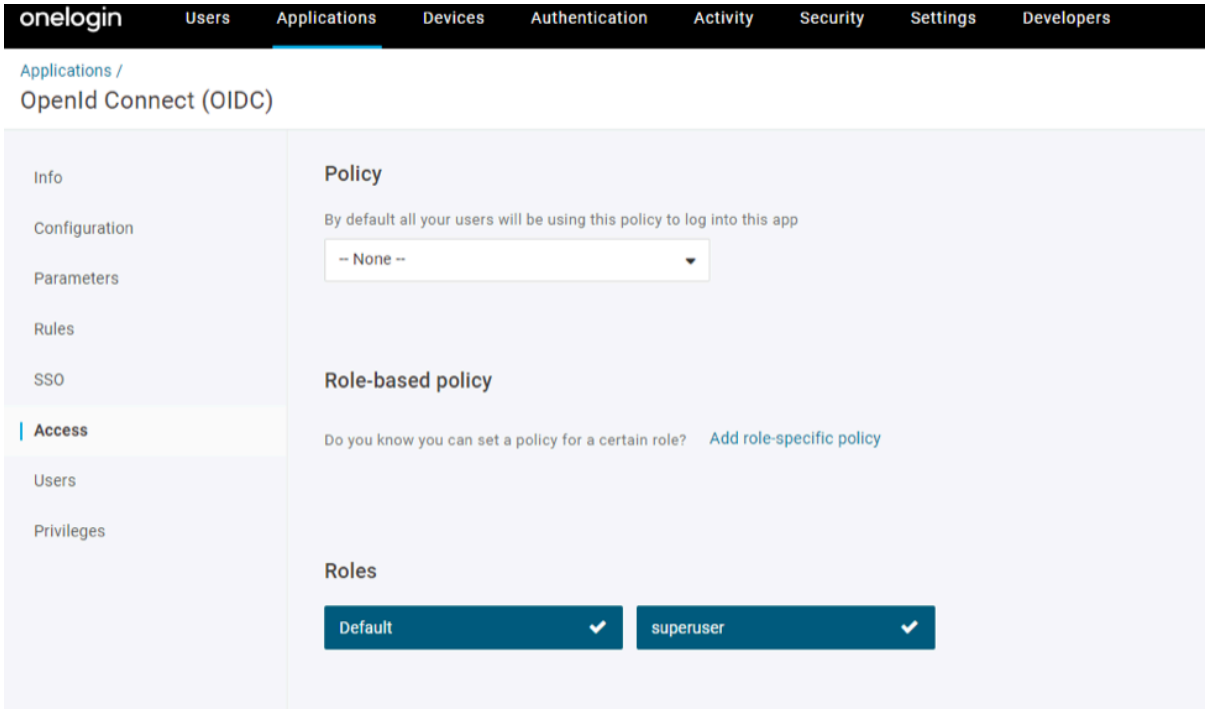
h. From the **Authentication Method** drop-down menu, select **POST** as the Token Endpoint and select **Save**. Note down the Client Credentials (Client ID and Client Secret) to be used during the SSO configuration in Orchestrator.

Figure 9-28: Application Type



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

Figure 9-29: Access tab



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

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

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

c. Select **Save Users**.

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

Configure Single Sign On in the Orchestrator.

9.4.4 Configure PingIdentity for Single Sign On

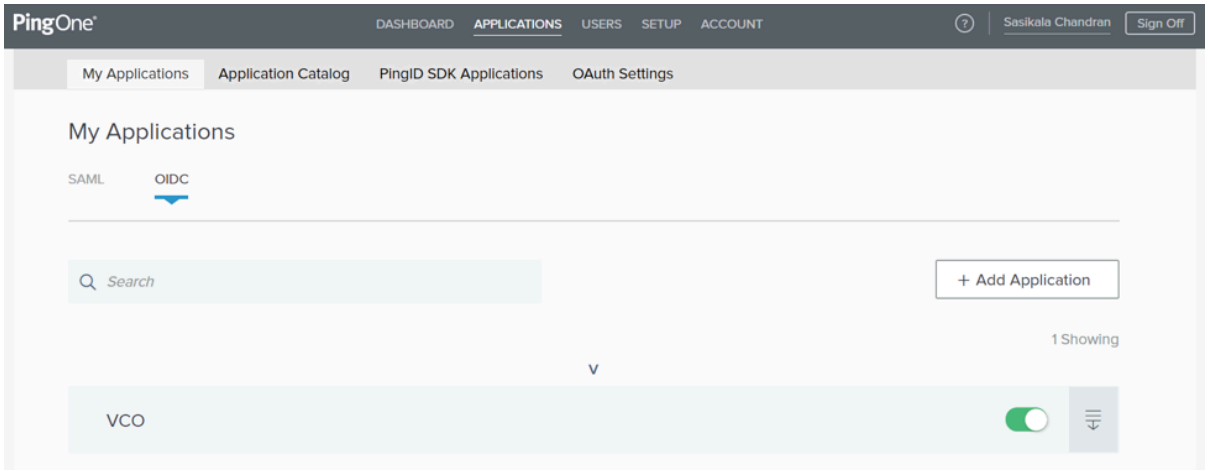
Ensure you have a PingOne account to sign in.

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.

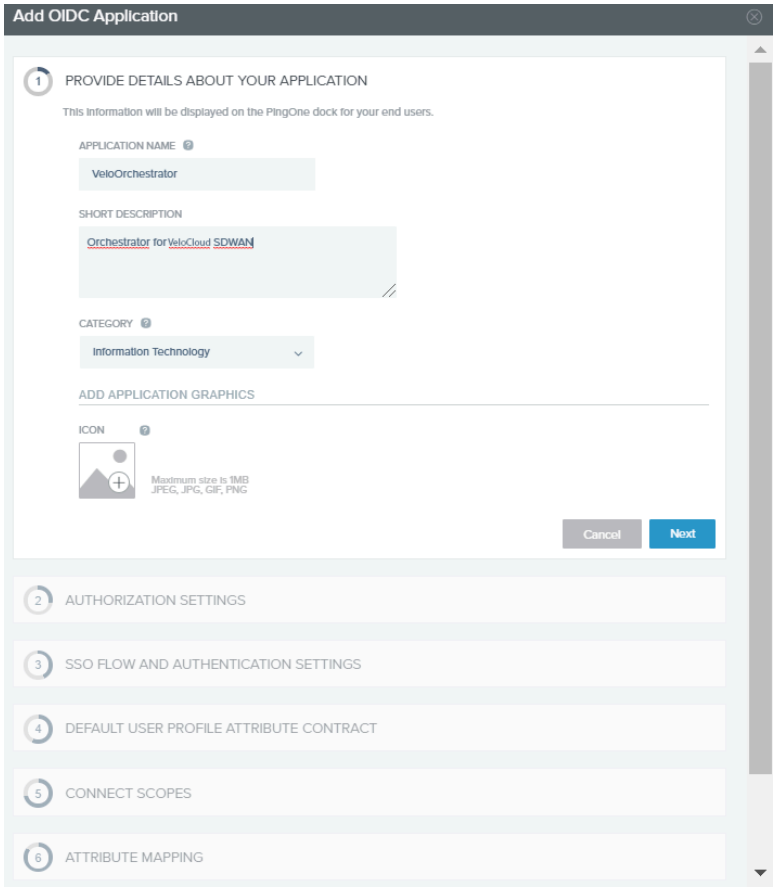
1. Log in to your PingOne account as an Admin user. The **PingOne** home screen appears.
2. To create a new application:
   a. In the upper navigation bar, select **Applications**.

Figure 9-30: My Applications



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

Figure 9-31: 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 Orchestrator.

Chapter 10

View Partner Information

As a Partner user, you can only view the Partner configuration settings. Only an Operator can edit these settings. The changes made by an Operator are applicable only to the Partner Admin and users associated with that Partner Admin. Partner Customers are not affected by this configuration.

To view the configured Partner information for a selected Partner:

1. Log in to the **Orchestrator** as a Partner user.
2. In the **Partner** portal, select the **Administration** tab, and then from the left menu, select **Partner Configuration**.

   The **Partner Overview** page with the following information appears for the selected Partner.

   Figure 10-1: Partner Overview

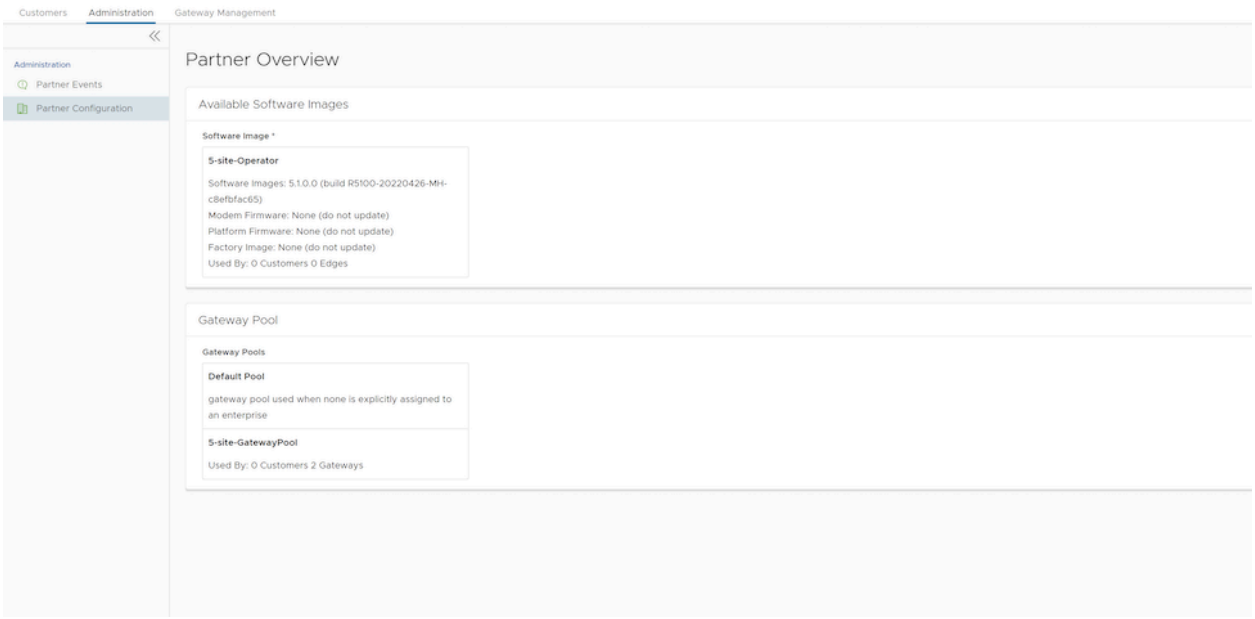


Table 30: Partner Overview Option Descriptions

Option	Description
Available Software Images	Displays all the software images assigned to the Partner by the Operator. You can assign the software images to your Enterprise customers from this list.
Gateway Pool	Displays the Gateway pools assigned to the Partner by the Operator. You can assign the Gateway pools to your Enterprise customers from this list.

To assign the software images and Gateway pools to a customer, see Create New Partner Customer and Configure Partner Customers.

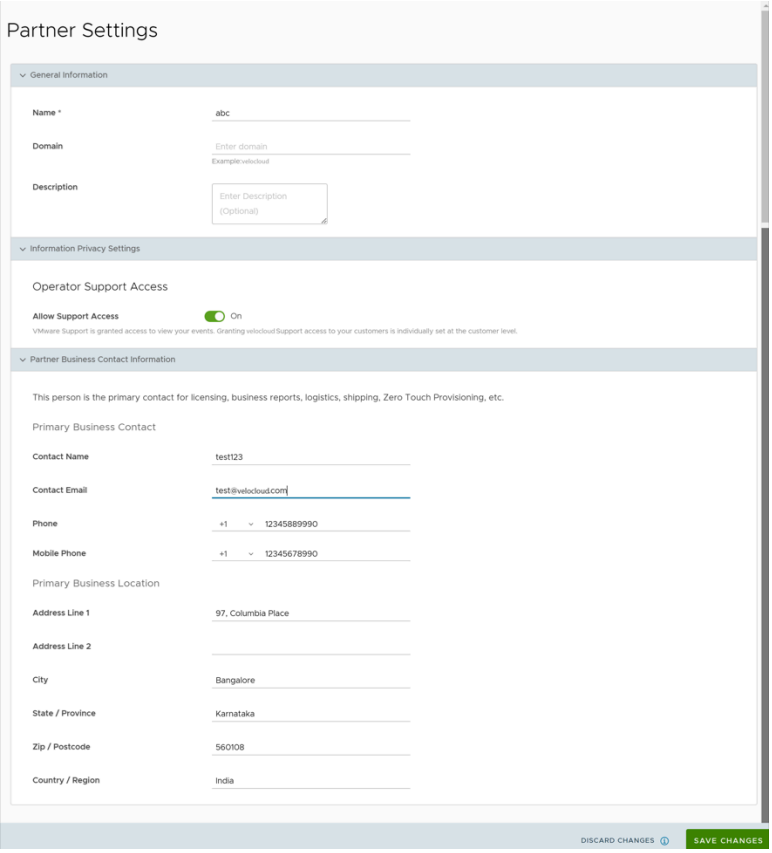
Chapter 11

Partner Settings

This feature allows you to configure Partner specific information such as name, primary location, and primary contact. You can also choose to allow or deny the Arista VeloCloud support access.

1. Log in to the Orchestrator as a Partner.
2. Select **Administration** from the top menu, and then from the left menu, select **Partner Settings**. The following screen appears:

   Figure 11-1: Displaying Partner Settings



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

Table 31: 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 Support can view Partner level events.  **Note:** You can individually allow or deny Support Access at the Enterprise level.
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**.

Chapter 12

Edge Licensing

Orchestrator provides different types of Licenses for the Edges. Partner users can manage and assign licenses to their Enterprise customers.

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

The Edge licenses are available with the following components:

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 VeloCloud offers a trial version of license with the following attributes:

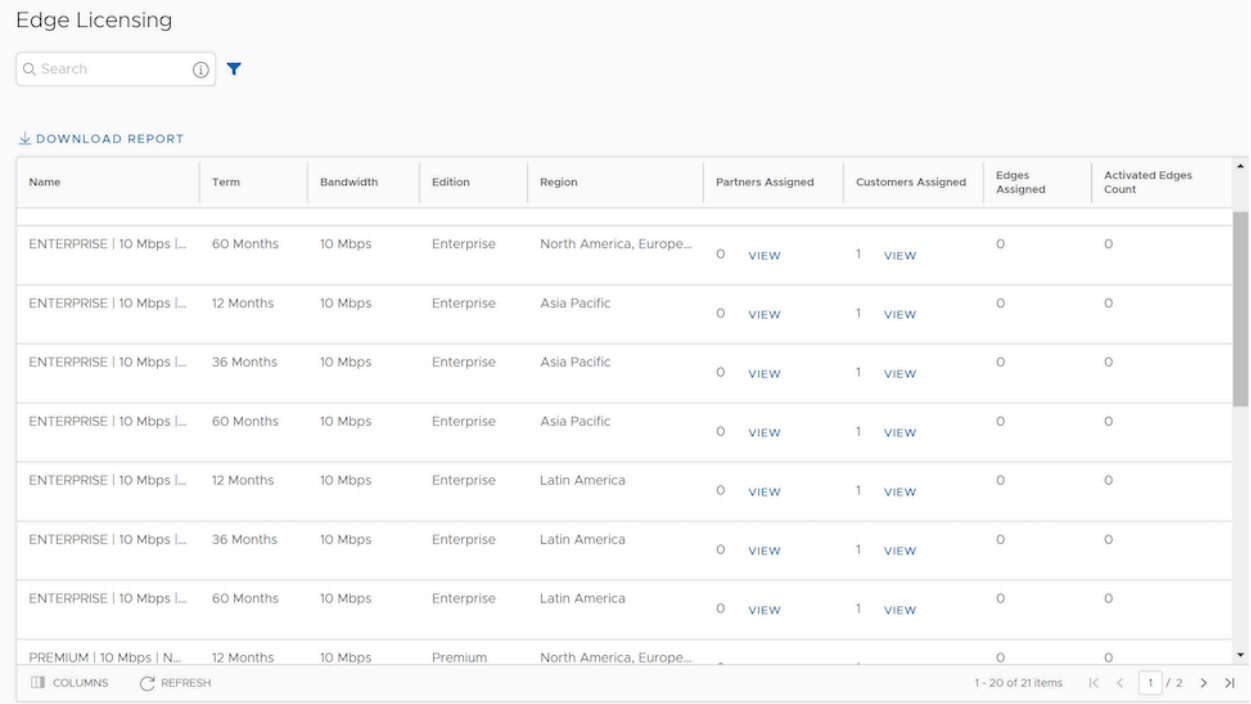
Component	Supported Attributes
Bandwidth	10 Gbps
Edition	POC
Region	North America, Europe Middle East and Africa, Asia Pacific and Latin America
Term	60 Months

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. Login to the **Orchestrator** as a Partner. In the **Partner** portal, from the top menu, select **Edge Management**, and then from the left menu, select **Edge Licensing**.

Figure 12-1: Displaying Edge Licensing



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

Table 32: 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 manage Edge licensing for Customers, see Manage Edge Licenses for Customers.

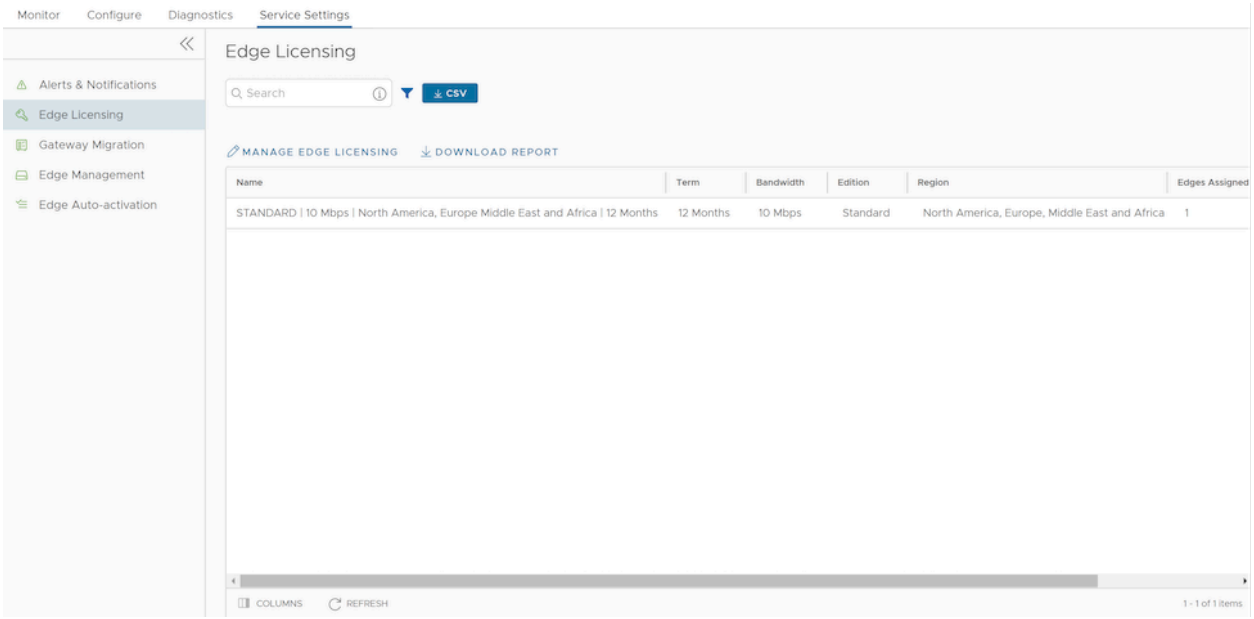
To assign the Edge licenses to Customers, see Create New Partner Customer.

12.1 Manage Edge Licenses for Customers

A Partner user can manage the Edge Licenses and assign them to Customers.

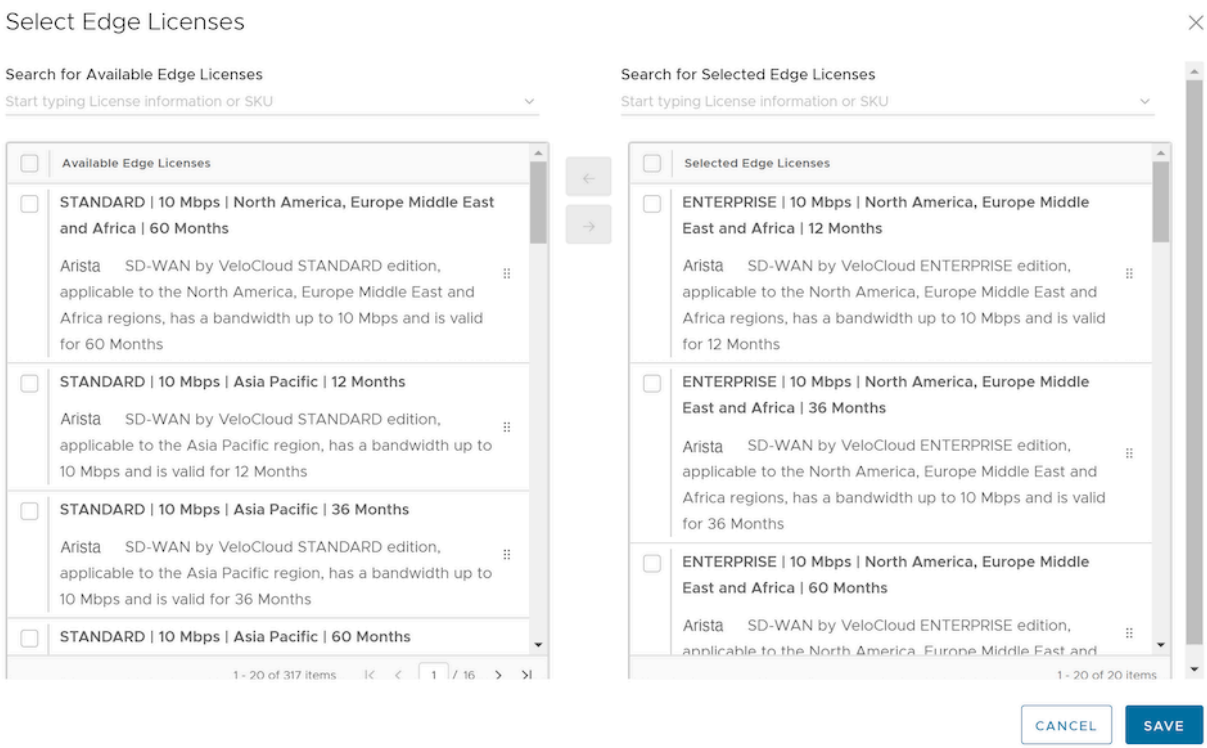
1. Login to the Orchestrator as a Partner and select **Manage Partner Customers**.
2. Select the link to a customer name to navigate to the Enterprise portal.
3. In the Enterprise portal, select **Service Settings** > **Edge Licensing**.

Figure 12-2: Edge Licensing



4. Select **Manage Edge Licensing**.

Figure 12-3: Managing Edge Licensing



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

> **Note:** Apart from the existing licenses, VeloCloud 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 **Download Report** to generate a report of the licenses and the associated Edges in CSV format.

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

You can 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 select the License under the **Properties** area in the **Edge Overview** page. You can also select the Edge and select **Assign Edge License** to assign the license.

- To assign a license to multiple Edges, select the appropriate Edges, select **Assign Edge License**, and select the license.

Chapter 13

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. Login to the **Orchestrator** as a Partner.
2. In the **Partner** portal, 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 13-1: Edge Management

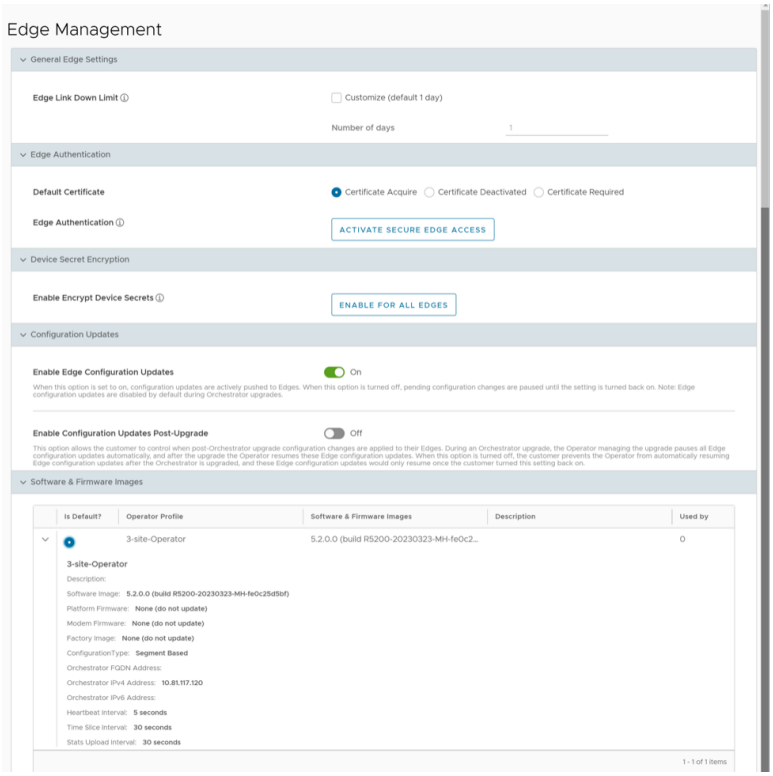


Table 33: Edge Management- Options and Descriptions

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 `edge.link.show.limit.sec`.
Number of days	Enter a value in the range **1** to **365**. The default value is **1**.
Edge Authentication	
Default Certificate	Choose the default option to authenticate the Edges associated to the Customer. • **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. **Note:** Only after acquiring the certificate, the option can be updated to **Certificate Required**. • **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. **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.
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.
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. **Note:** You can activate this option for individual Edges at the time of creating a new Edge. For additional information, see the topic *Provision a New Edge* in the *Arista VeloCloud SD-WAN Administration Guide*.
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, a Partner user must follow the below steps:
   a. Navigate to **Manage Partner Customers**, and then select **More**.
   b. Select **Update Edge Image Management** from the drop-down menu. Turn on the toggle button, and then select **Save**.

c. Select **Assign Software/Firmware Image**, and then select a Software/Firmware image from the drop-down menu. Select **Save**.

This allows the Partner user to view the details of the listed images and select the default image on the **Edge Management** screen.

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

Chapter 14

Access SD-WAN Edges Using Key-Based Authentication

This section provides 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.
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. SeeEnable Secure Edge Access for an Enterprise.

14.1 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 Superusers 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.
- Superusers can only view and revoke the SSH keys for other users.

> **Note:** Enterprise and Partner customers without SD-WAN service access cannot configure or view SSH keys related details.

To add a 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 **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 Convert Pem to Ppk File Using PuTTYgen.
   - **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.

14.2 Revoke SSH Keys

Ensure that you have a Superuser 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**.
3. To revoke the SSH keys of other Partner users:
   a. In the **Partner** portal, go to **Partner Settings** > **Authentication**.
   b. In the **SSH Keys** area, select the SSH usernames for which you want to delete the SSH keys.

c. Select **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.

14.3 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.

14.4 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 34: Secure Edge CLI 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 **`debug -h`** to view a list of available commands and options. For a sample output of one of the debug commands, see debug --dpdk_ports_dump.	Yes	Yes
`diag`	Runs the remote diagnostics commands. Run **`diag -h`** 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 **`getwanconfig GE3`** to view the configuration details of the GE3 WAN interface. Run the **`ifstatus`** 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 **`setwanconfig -h`** 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

14.4.1 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, "seauserinfo": { "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":
 "dpdk", "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" }
```

Chapter 15

Configure User Account Details

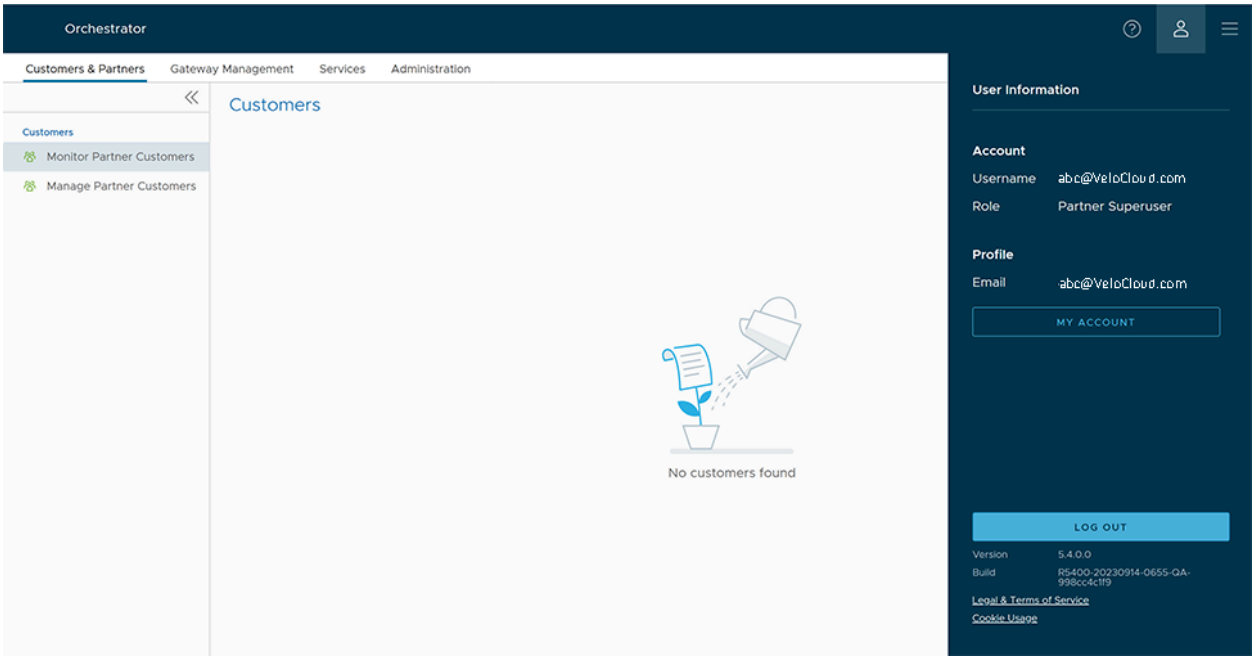
The My Account page allows you to configure basic user information, SSH keys, and API tokens. You can also view the current user's role and the associated privileges.

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:

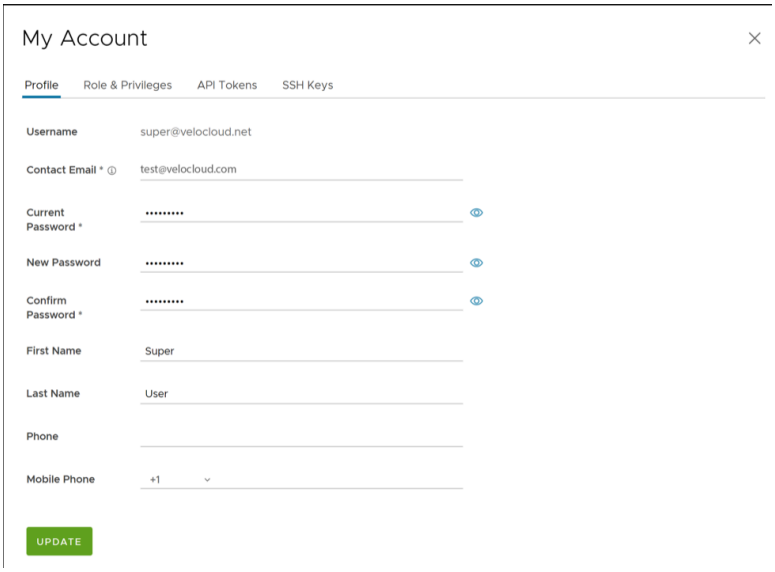
1. Select the **User** icon in the **Global Navigation** located at the top right of the screen.
   The **User Information** panel is displayed as shown below:

   Figure 15-1: User Information



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

Figure 15-2: Profile Tab



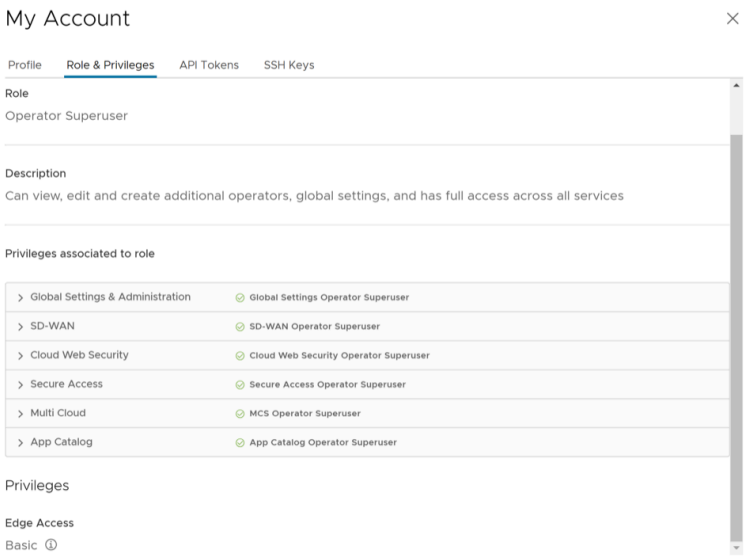
3. The **Profile** tab is displayed by default. You can update the following basic user details:

Table 35: 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. **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.
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.

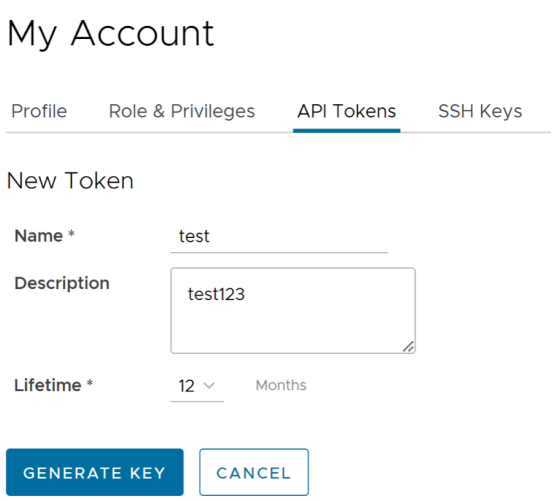
4. Select the **Role** tab to view the existing user role and description. It also displays the privileges associated with the user role.

   Figure 15-3: Role & Privileges tab



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

   Figure 15-4: API Tokens tab



6. Enter a **Name** and **Description** for the token, and then choose the **Lifetime** from the drop-down menu.
7. Select **Generate Key**.
8. 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.

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

Figure 15-5: SSH Keys tab

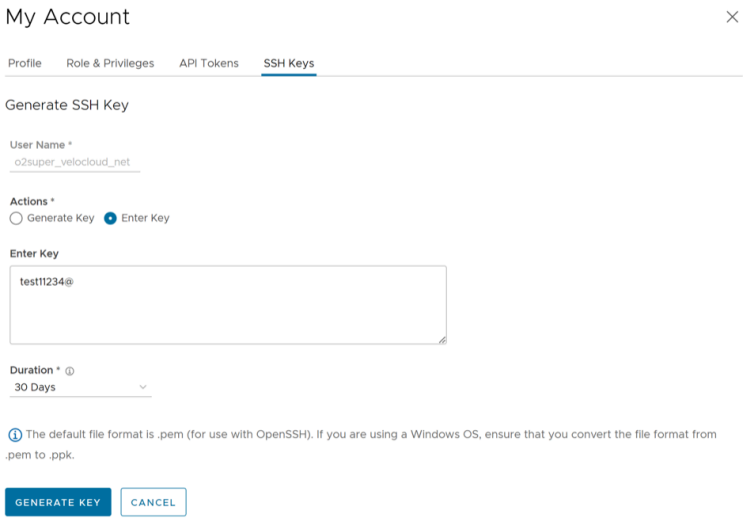


Table 36: SSH Keys Tab- Options and Descriptions

Option	Description
User Name	Displays the username and it is a read-only field.
Actions	Select either one of the following options: • **Generate key**: Use this option to generate a new pair of public and private SSH keys. **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. • **Enter key**: Use this option to paste or enter the public key if you already have a pair of SSH keys.
PassPhrase	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. **Note:** This is an optional field and is available only if you select the **Generate Key** action.
Duration	Select the number of days by when the SSH key must expire.

10. Select **Generate Key**.

Note: Only one SSH Key can be created per user.

11. 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.
12. 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.

Chapter 16

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.

16.1 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 a Partner Super user and Partner Admin user, you can create, manage, download, and delete Gateway pools created by a Partner user or a Partner Managed Gateway pools created by the Operator.

Note: The Gateway pools feature is not supported for Partner Business Specialist user and Partner IT support user.

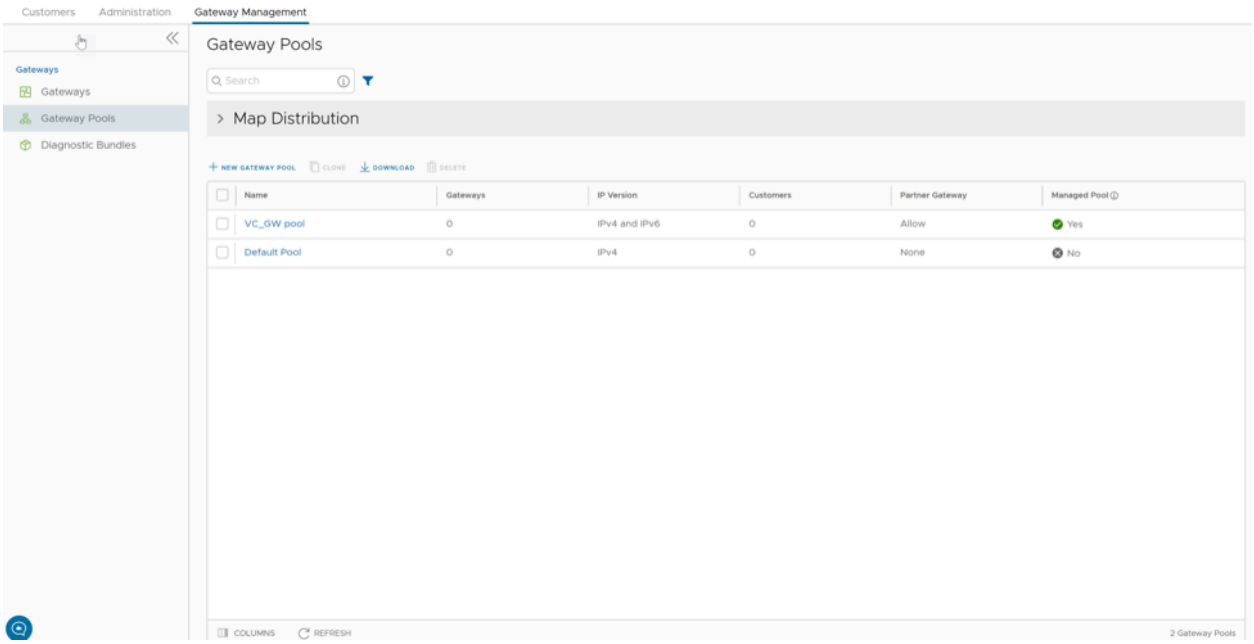
The **New Gateway Pool** and **Download** options are available only for Partners with Gateway management access activated. If the Gateway management access is deactivated for a Partner, then the Partner will have only read-only permission for the configured Gateway pools. To request Gateway Management access, Partners must contact the Operator Super user.

To manage Gateway pools, perform the following steps:

1. Log into the **Orchestrator** as a Partner 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 16-1: Manage 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 37: Manage 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. **Note:** When assigning Gateways to the Gateway pool, ensure that the IP address type of the Gateway matches the IP address type of pool.
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** > **Customer** page.
Partner Gateway	Specifies the status of the Partner Gateway. The following are the available options: • **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.

16.1.1 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 16-2: Create New Gateway Pool

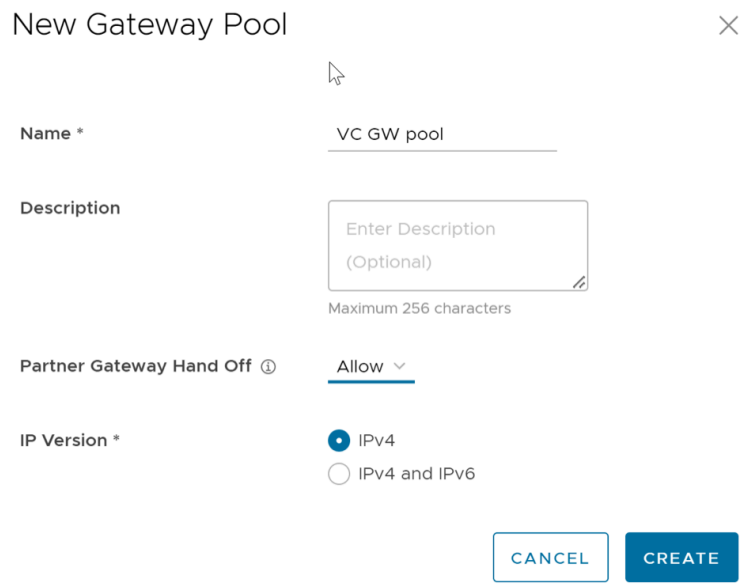


Table 38: New Gateway Pool Option Descriptions

Field	Description
Name	Enter a name for the new Gateway pool.
Description	Enter a description for the Gateway pool.
Partner Gateway Hand Off	This option determines the method to hand off the Gateways to Partners. Choose one of the following options from the drop-down list: • **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	Choose one of the following address types with which the Gateway pool should be enabled: • **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**.

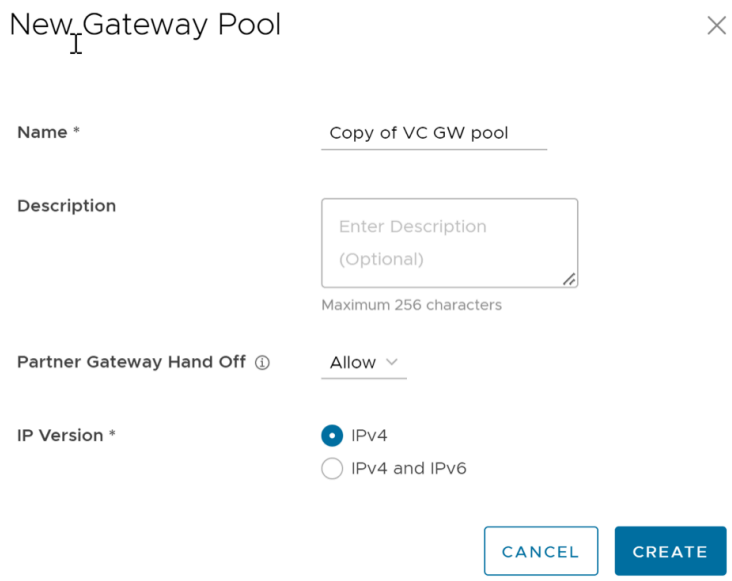
Configure the Gateway pool by adding Gateways to the pool. See Configure Gateway Pools.

16.1.2 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 16-3: Clone a Gateway Pool



   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.
3. After updating the Gateway pool details, select **Create**.

Configure the Gateway pool by adding Gateways to the pool. See Configure Gateway Pools.

16.1.3 Configure Gateway Pools

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

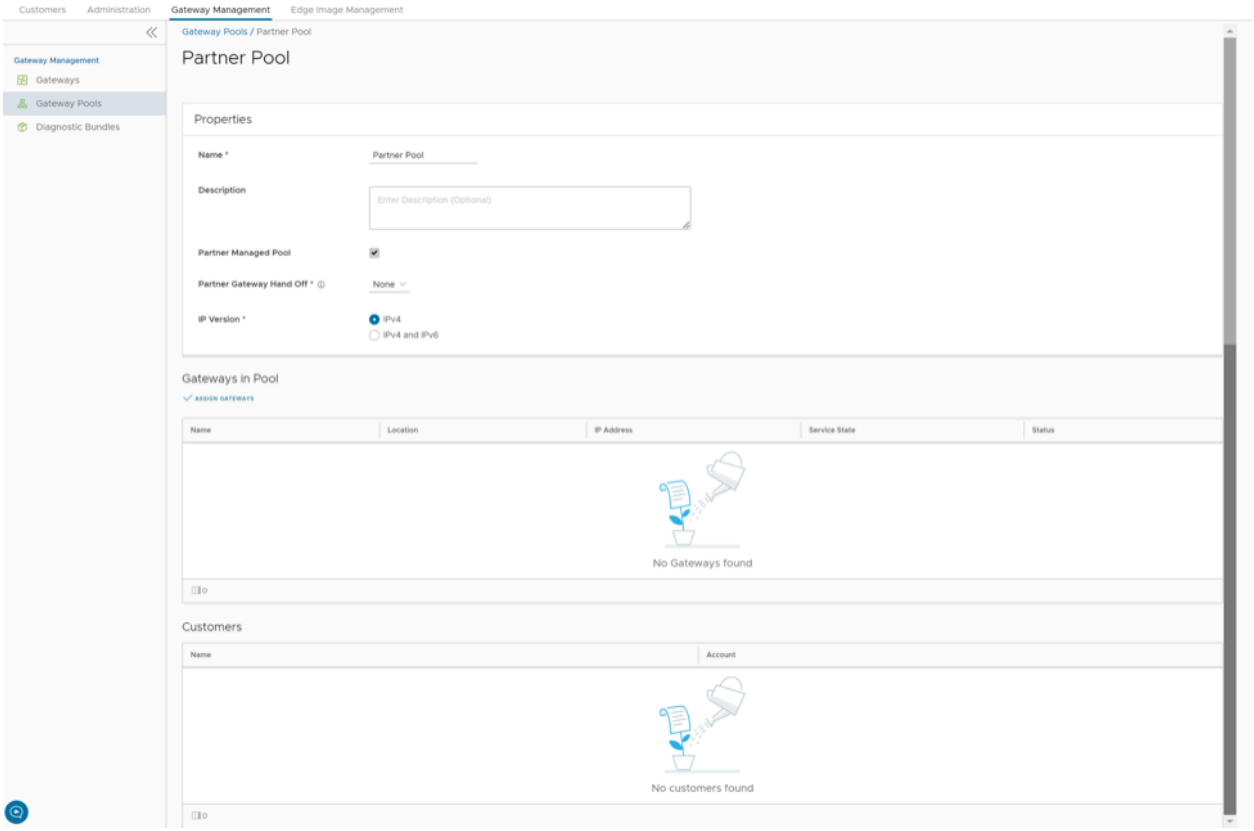
Whenever you create a new Gateway pool or clone a pool, you are redirected to the **Gateway Pool Overview** page to configure the properties of the pool.

> **Note:** You can configure only a Gateway pool created by a Partner User or a Partner Managed Gateway pool created by your Operator.

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 16-4: Configure Gateway Pools

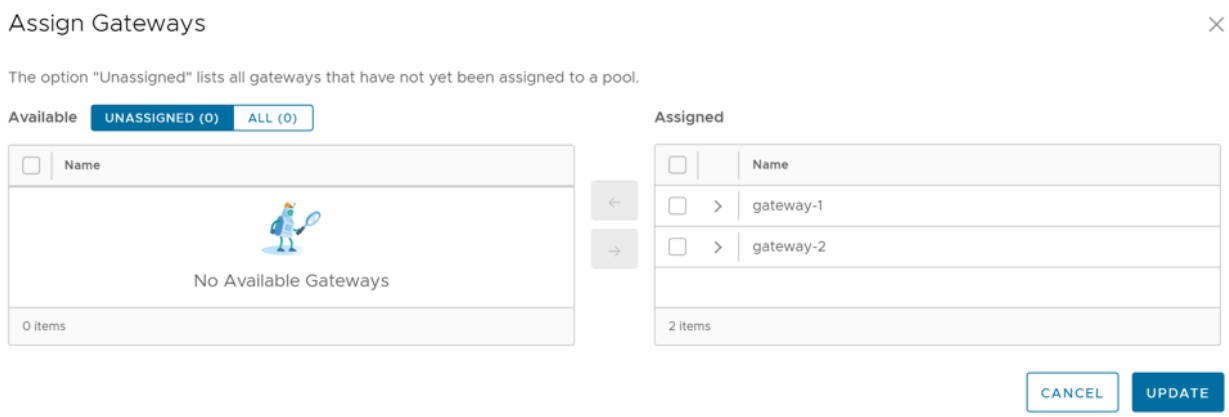


   a. In the **Properties** section, the existing Name, Description, Partner Gateway Hand Off details, and the Association Type are displayed. If required, you can modify these details.

   b. In the **Gateways in Pool** section, select **Manage** to add Gateways to the pool. The **Assign Gateways to Gateway pool** dialog appears.

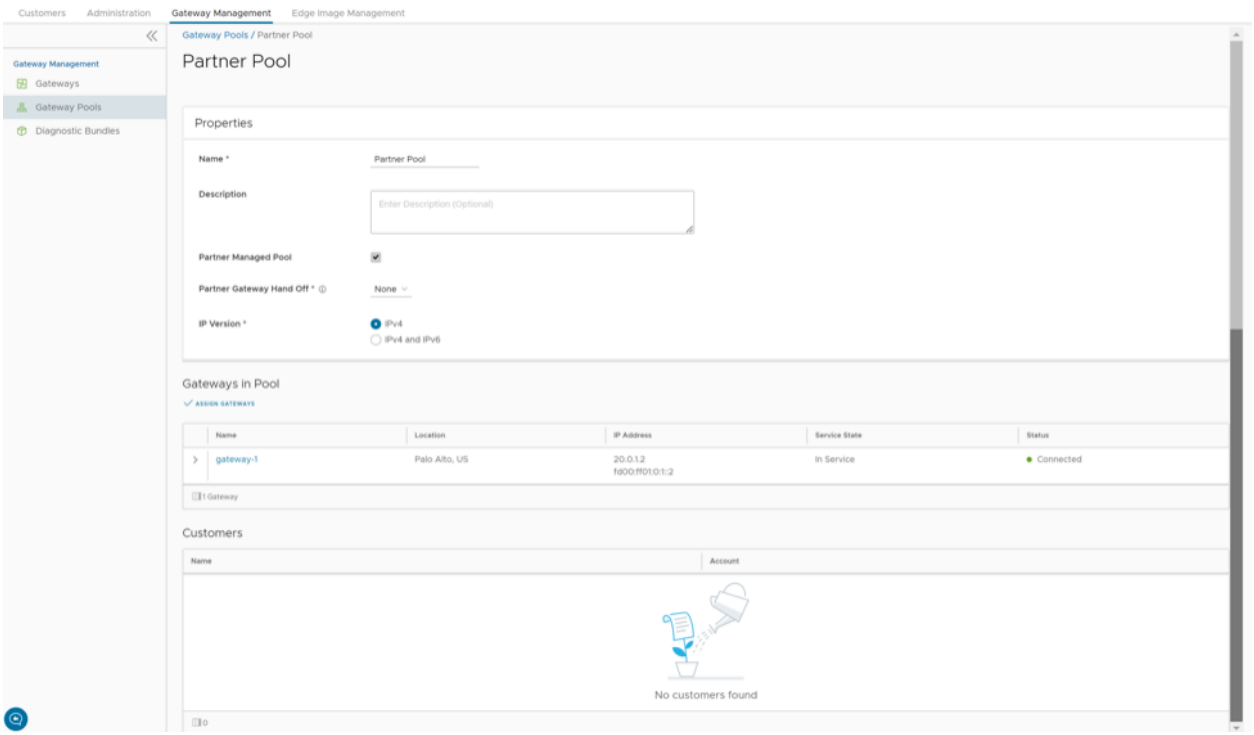
c. In the **Assign Gateways to Gateway pool** dialog, move the required Gateways from the **Available** pane to **Assigned** pane using the Arrows and select **Update**.

Figure 16-5: Assign Gateways to Gateway Pool



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

Figure 16-6: Gateways in Partner Pool



5. Select **Save Changes**.
   The configured Gateway pools are displayed in 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 Partner customer, see Create New Partner Customer.
- For an existing Partner customer, see Configure Partner Customers.
- For a new Partner, see Add New User.
- For an existing Partner, see User Management - Partner.

16.2 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.

Partner Super user and Admin with Gateway management access activated can create, manage, and delete Gateways created by a Partner or Partner managed Gateways created by an Operator. The Partner IT support users can only view the configured Gateways.

If the Gateway management access is deactivated for a Partner, then the Partner will have only read-only permission for the configured Gateways. To request Gateway Management access, Partners must contact the Operator Super user.

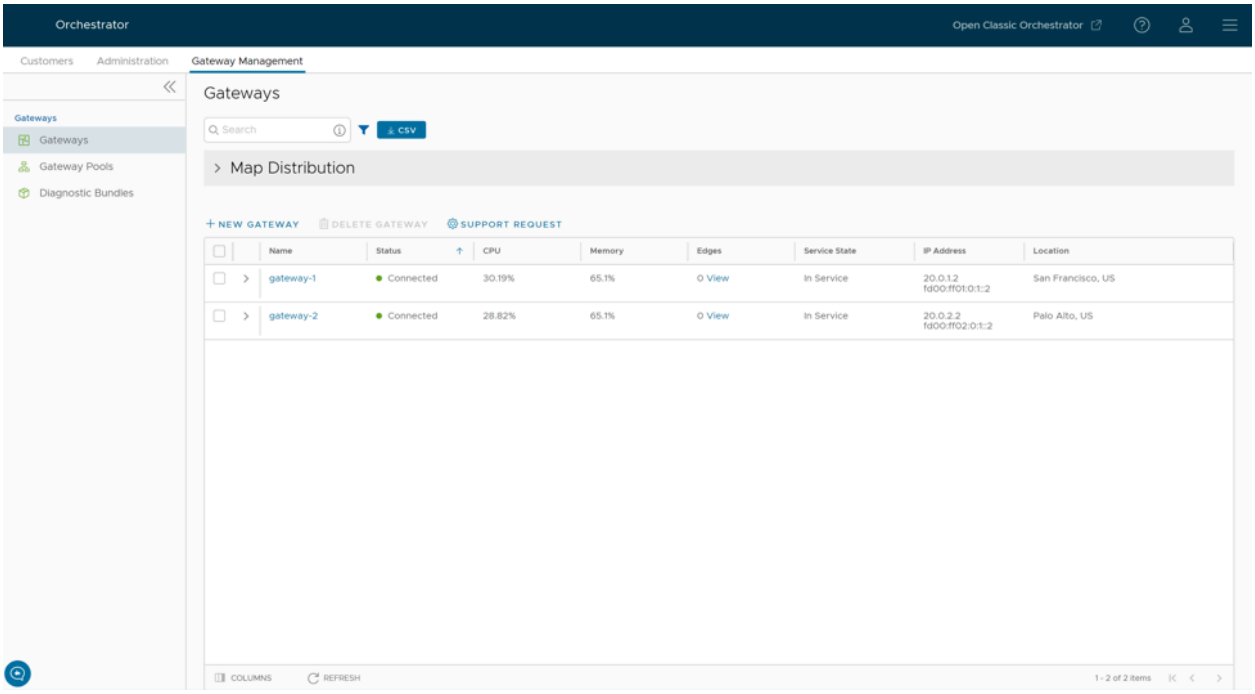
Note: The Gateways feature is not supported for the Partner Business Specialist user.

To manage Gateways, perform the following steps:

1. Log into the **Orchestrator** as a Partner 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 16-7: Manage Gateways



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 39: Existing 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: • **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 `psutil.phymem_usage` at the time of the last heartbeat. This is similar to estimating the percentage of memory usage using the **`free`** command.
Edges	Number of Edges connected to the Gateway at the time of the last heartbeat. **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.
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.

16.2.1 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 16-8: Create New Gateway

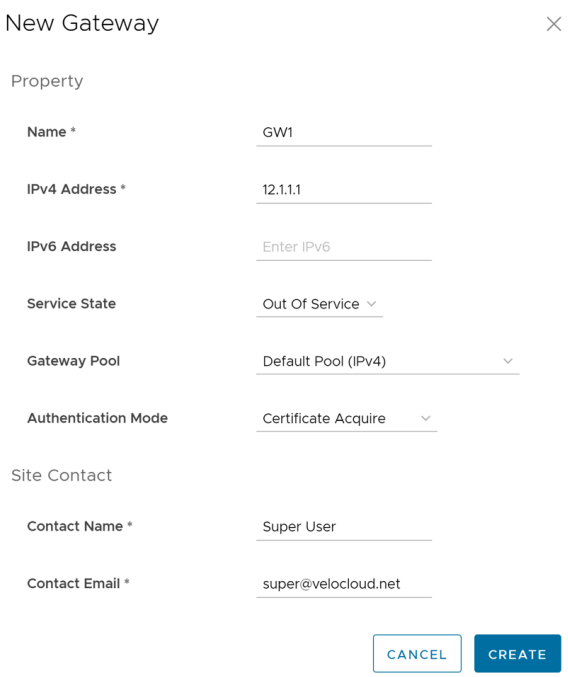


Table 40: New Gateway Field Descriptions

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	Select the service state of the Gateway from the drop-down list. The following options are available: • **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. **Note:** The **Quiesced** and **Out of Service** states are only applicable for Cloud Gateway deployment.
Gateway Pool	Select the Gateway Pool from the drop-down list, to which the Gateway would be assigned.
Authentication Mode	Select the authentication mode of the Gateway from the following available options: • **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. **Note:** After acquiring the certificate, the option can be updated to **Certificate Required**. **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. • **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.

16.2.2 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.

Note: You can configure only a Gateway created by a Partner user or a Partner managed Gateway created by your Operator.

To configure an existing Gateway:

1. In the **Partner** 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 16-9: Configure Gateways Overview Screen

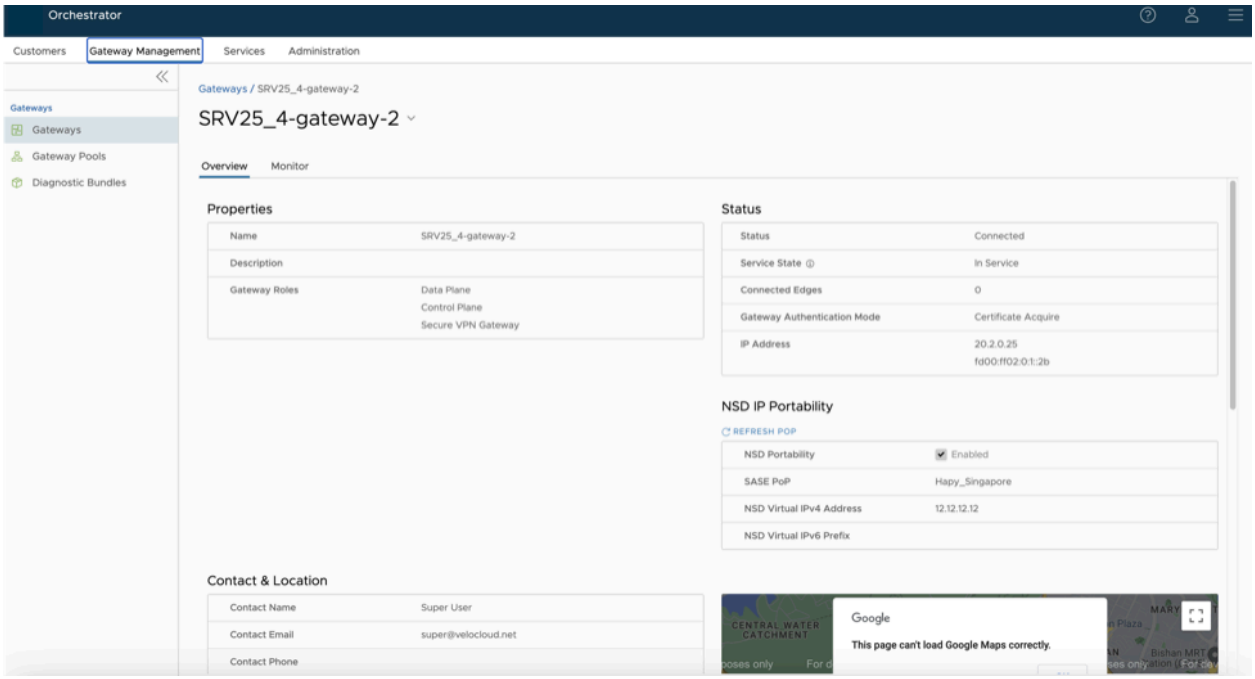


Table 41: Configure Gateways Field Descriptions

Option	Description
Properties	Displays the existing Name and Description of the selected Gateway. If required, you can modify the information. You can also configure the Gateway Roles, as required: • **Data Plane**- Enables the Gateway to operate in the Data plane and is selected by default. • **Control Plane**- Enables the Gateway to operate in the Control plane and is selected by default. • **Secure VPN Gateway**- Select the option to use the Gateway to establish an IPsec tunnel to a Non SD-WAN Destination. • **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 • **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. • **Cloud-to-Cloud Interconnect**- Select the option to enable cloud-to-cloud-interconnect (CCI) tunnels on the VeloCloud Gateways.  **Note:** This Gateway Role option is shown if the `session.options.enableZscalerCci` system property is set to True. • **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**.  **Note:** This assignment works only when the Gateway Pool's **Partner Gateway Handoff** is not set to **Only**.

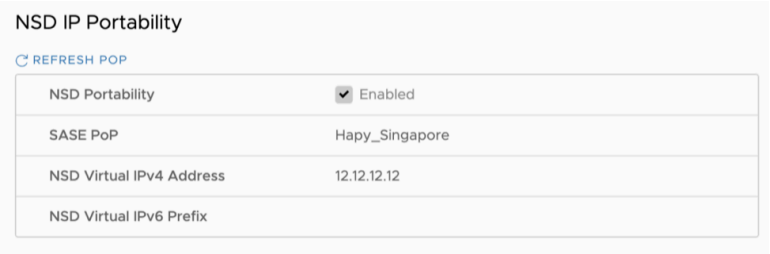
Option	Description

Status	You can configure the following details:
	• **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:
	  • **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:
	  • **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.
	  Note: The **Quiesced** and **Out of Service** states are only applicable for Cloud Gateway deployment.
	  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.
	  For additional information, see Migrate Quiesced Gateways.
	  Note: Self-service migration is not supported on Partner Gateways.

Connected Edges	Displays the number of Edges connected to the Gateway. This option is displayed only when the Gateway is activated.

Option	Description

Gateway Authentication Mode	Select the authentication mode of the Gateway from the drop-down menu:
	• **Certificate Deactivated**- Gateway uses a pre-shared key mode of authentication. If you change the mode from **Certificate Deactivated** to:
	  • **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:
	  • **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.
	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.
	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	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. **Note:** Adding IPv6 address is a one-time activity and once you save the changes, you cannot modify the IP addresses. **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.
Contact & Location	Displays the existing contact details. If required, you can modify the information.
NSD IP Portability	Beginning with the 6.0 Orchestrator release, the NSD IP Portability for the Gateway is supported. Portable NSD IPs allow an Operators to move NSD configurations to different Gateways in the POP without requiring the customer to reconfigure their tunnels. **Note:** For a Partner user, the NSD Portability functionality is read-only and cannot be edited. **Figure 16-10: NSD IP Portability** 
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. For additional information, see the *Configure NAT Entry Syslog for Gateways* section in the *VeloCloud SD-WAN Operator Guide*.
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 *Partner Gateway (Advanced Handoff) Details* 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 42: 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: • **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: • **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 Partner Handoff.

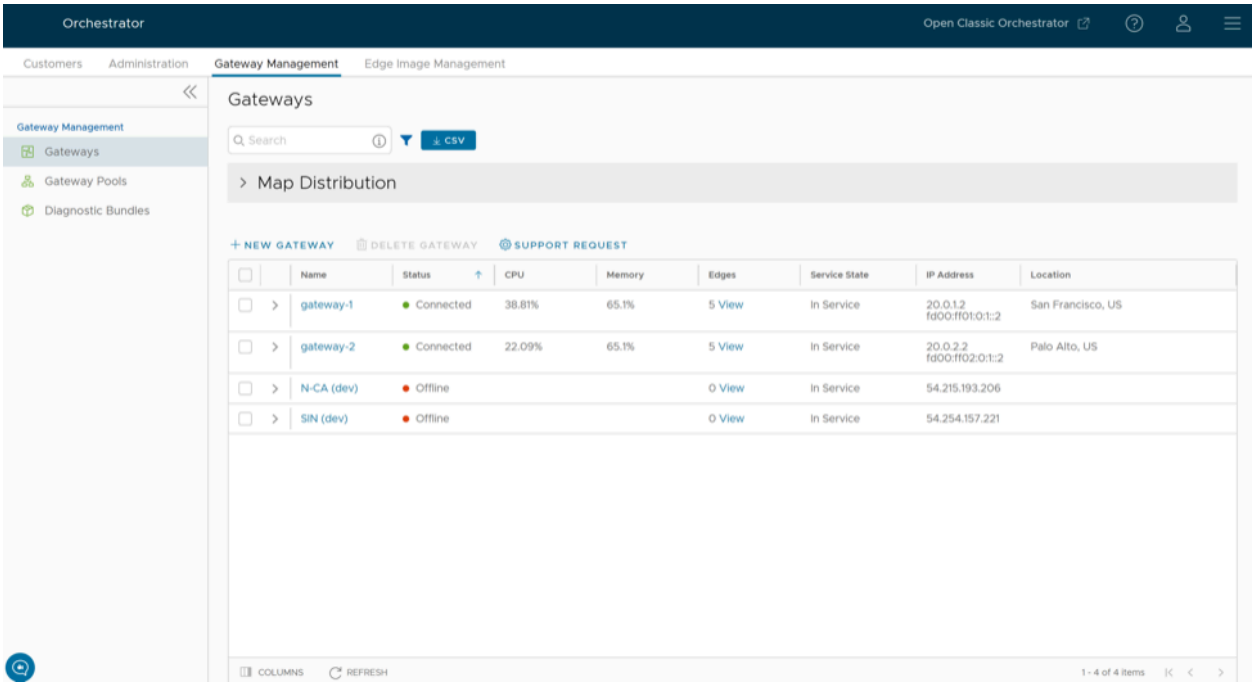
16.2.3 Monitor Gateways

You can monitor the status and network usage data of Gateways available in the Partner portal of the Orchestrator.

To monitor the Gateways:

1. Login to the **Orchestrator** as a Partner and in the **Partner** portal, select **Gateway Management** > **Gateways**.
2. The **Gateways** page displays the list of available Gateways.

   Figure 16-11: Monitor Gateways Screen



3. Select **Map Distribution** to expand and view the locations of the Gateways in the Map. By default, this view is collapsed.
4. You can also select the arrows prior to each Gateways name to view additional details.

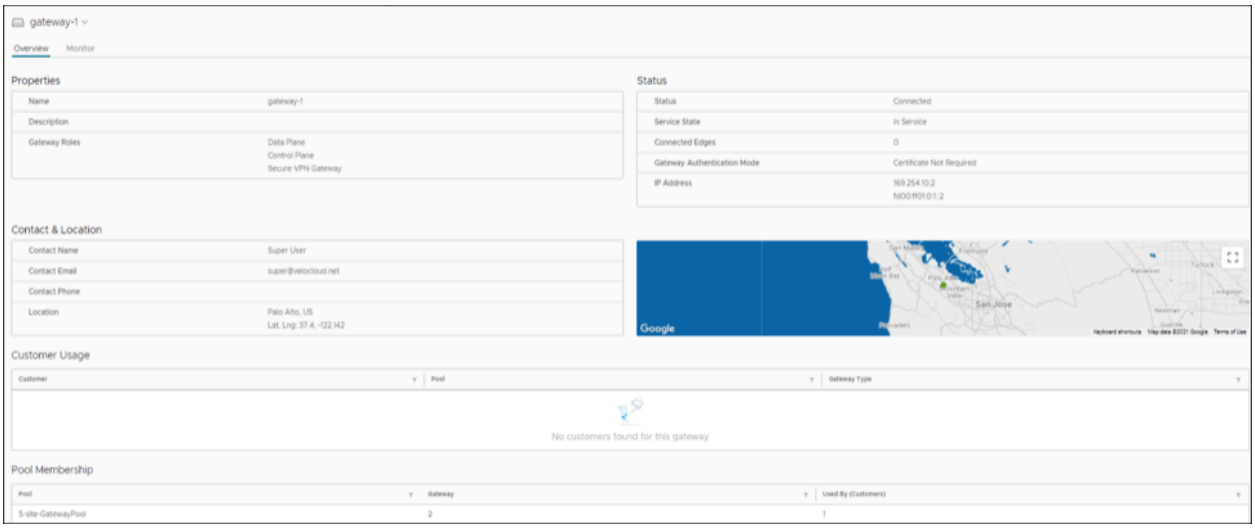
   The page displays the following details:

   - **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.

5. In the Search field, enter a term to search for specific details. Select the **Filter** icon to filter the view by a specific criterion.
6. 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 16-12: Monitor Gateway Overview Screen

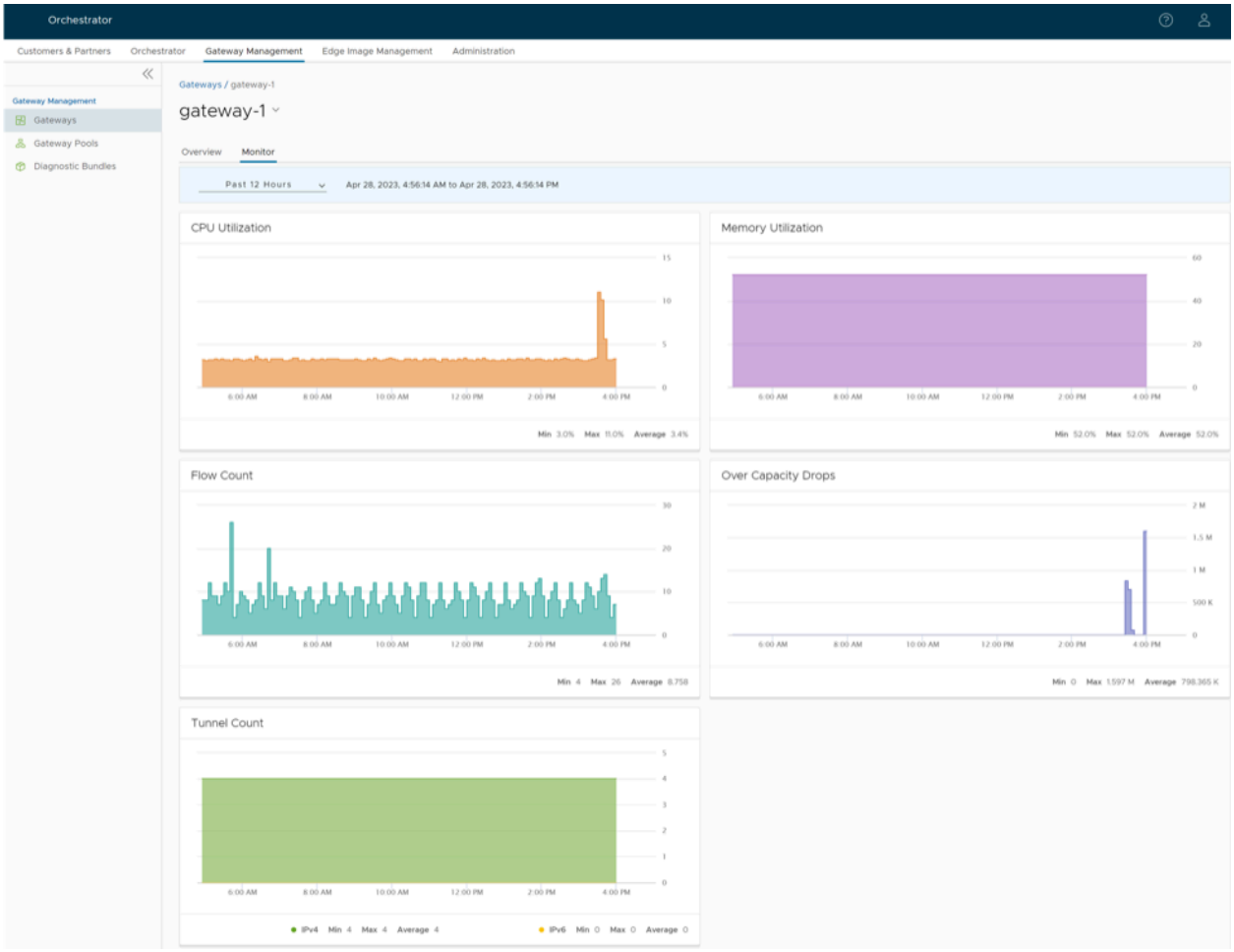


The **Overview** tab displays the properties, status, location, customer usage, and Gateway Pool of the selected Gateway.

Note: You can only view the details of the selected Gateway, using this tab. To configure the options, navigate to the **Gateways** page in the Partner portal of the Orchestrator.

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

Figure 16-13: Monitor Gateway Usage Screen



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.

Note: If you are a Partner user, follow the above instructions in the Partner portal to view the details of the Partner Gateways.

16.3 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.

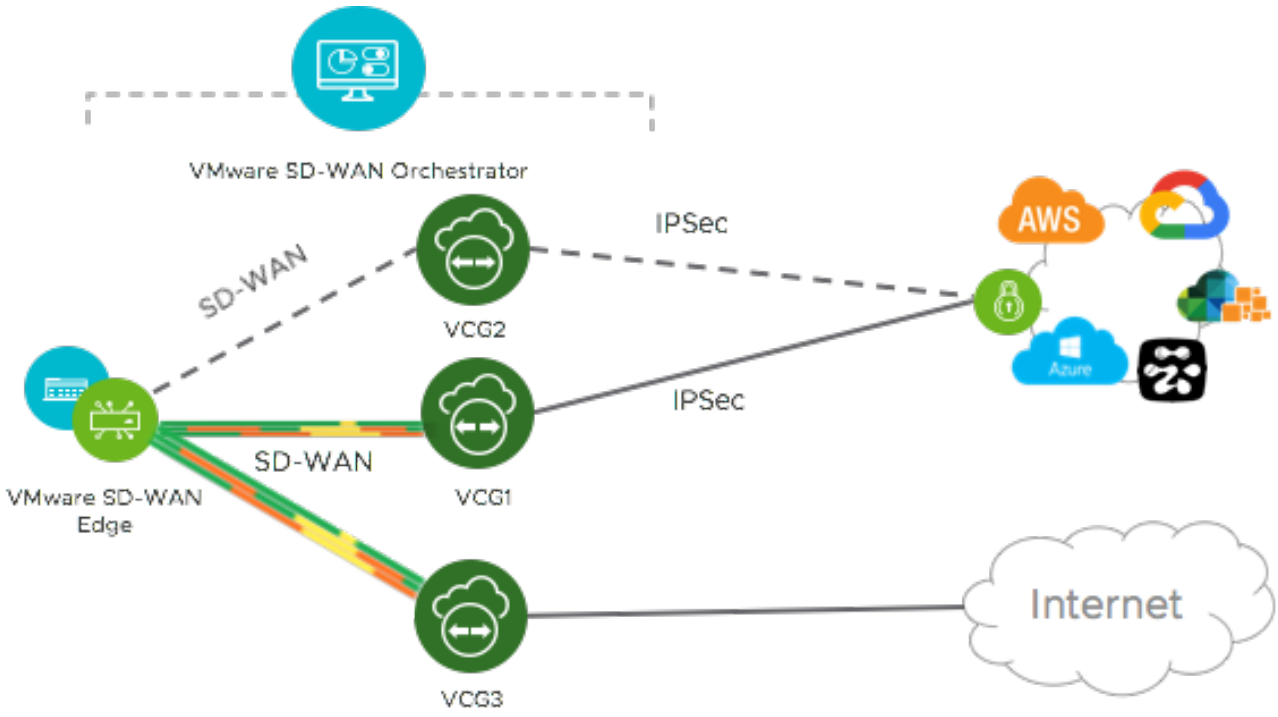
Gateway migration may be required in the following scenarios:

- 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:

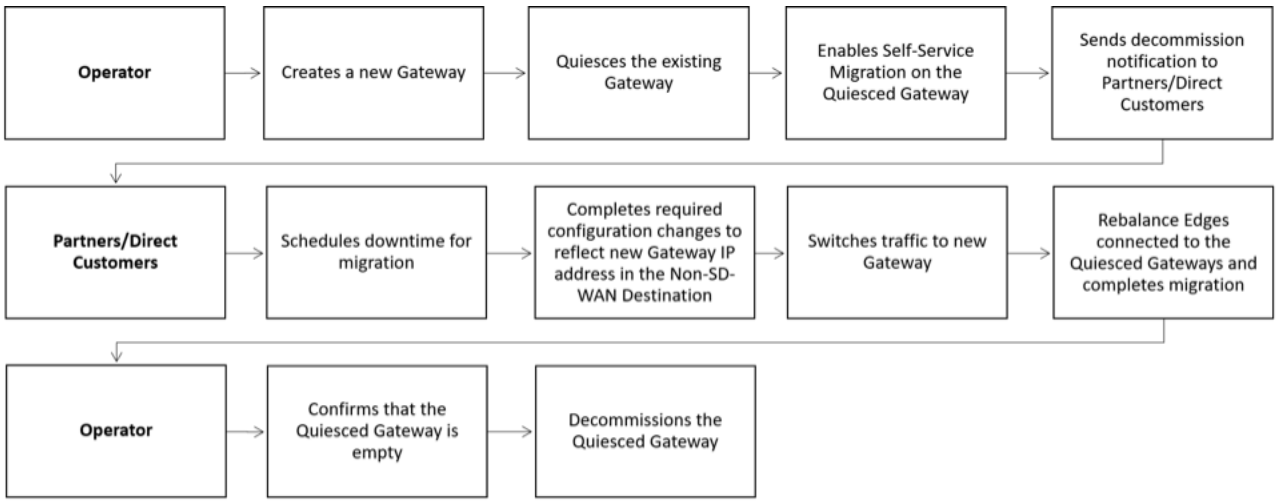
Figure 16-14: Secure VPN Gateway Migration Process



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 16-15: Secure VPN Gateway Migration Workflow



16.3.1 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.

16.3.2 Migrate Quiesced Gateways

Operators send notification emails about Gateway migration to Administrators with Super User privileges. Plan your migration based on the notification email that you receive from your Operator.

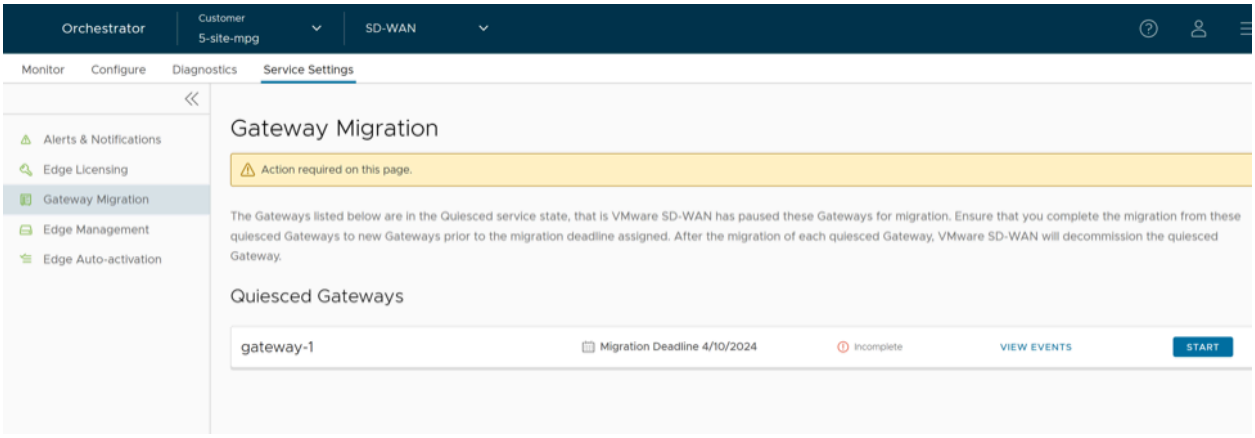
Before you migrate the Edges and NSDs (if configured) from the quiesced Gateway to the new Gateway, ensure that you schedule a maintenance window as traffic may be disrupted during migration.

To avoid any service disruption, ensure that you migrate to the new Gateway within the Migration Deadline mentioned in the notification email.

To migrate from a quiesced Gateway to a new Gateway, perform the following steps:

1. In the **SD-WAN** service of the **Enterprise** portal, go to **Service Settings** > **Gateway Migration**. The list of quiesced Gateways appears.

   Figure 16-16: Quiesced Gateways List

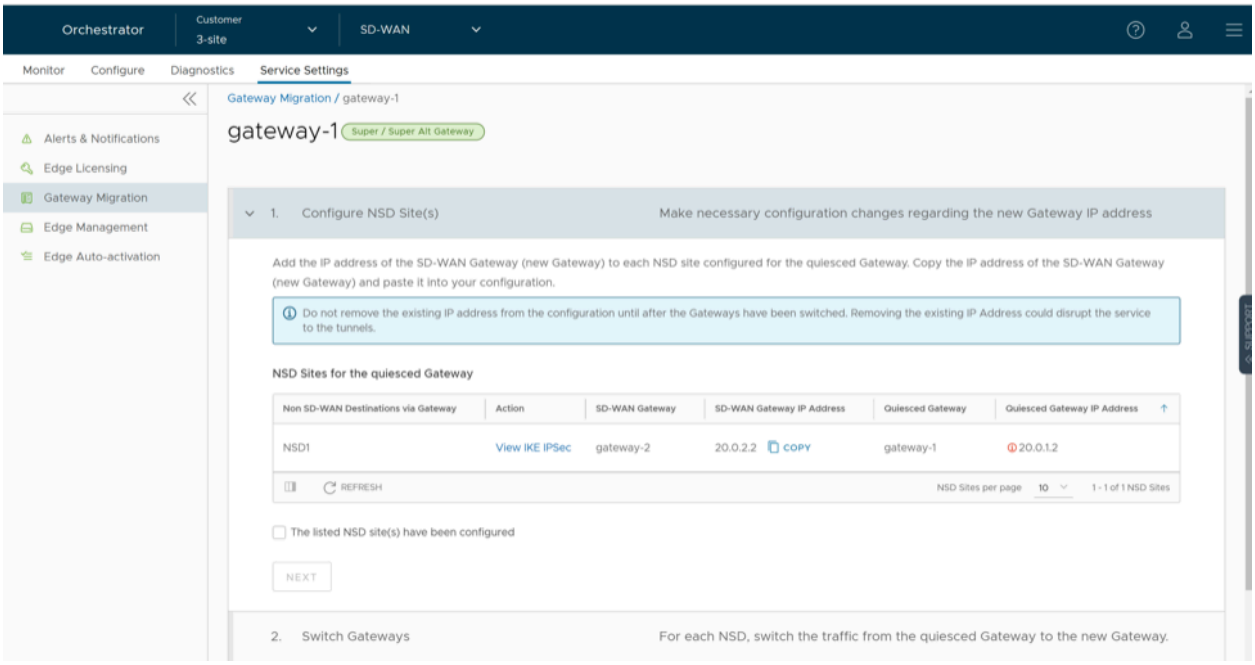


2. Select **Start** for the quiesced Gateway from which you want to migrate to the new Gateway.

> **Note: Step 3** and **Step 4** are only applicable if you have the NSDs configured from the quiesced Gateway. If there are no NSDs configured, go to **Step 5** to rebalance cloud Gateways and Edges that are connected to the quiesced Gateway.

3. Make the required configuration to all the NSDs that are configured through the quiesced Gateway.

Figure 16-17: Configure NSDs



a. Select the **View IKE IPSec** link to view a sample configuration for the NSD. Copy the template and customize it to suit your deployment.

b. Add the IP address of the SD-WAN Gateway (new Gateway IP) to each NSD configured for the quiesced Gateway.

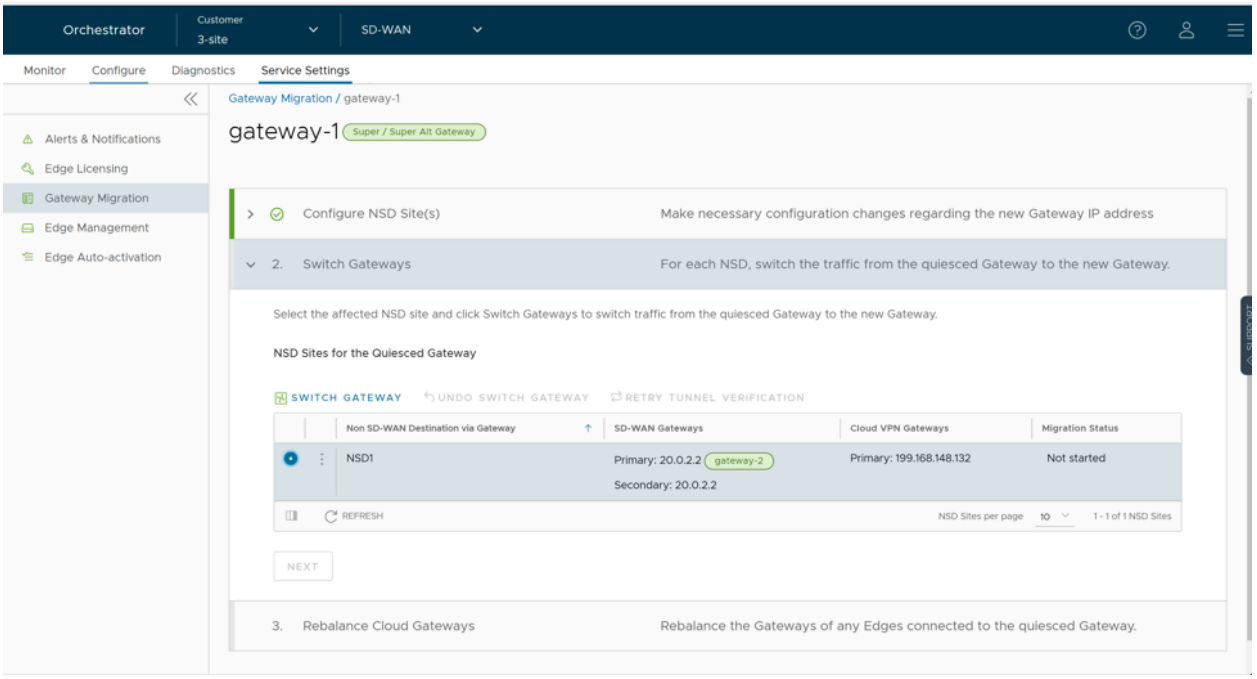
   For example, if you have configured an NSD for AWS, you must add the IP address of the new Gateway in the NSD configuration in the AWS instance.

c. After making the configuration changes to all the NSDs, select the **The listed NSD site(s) have been configured** check box, and then select **Next**.

Note: The Configure NSD Site(s) option is not available for NSDs configured automatically as well as for Gateways with Data Plane role that are not attached to any NSDs.

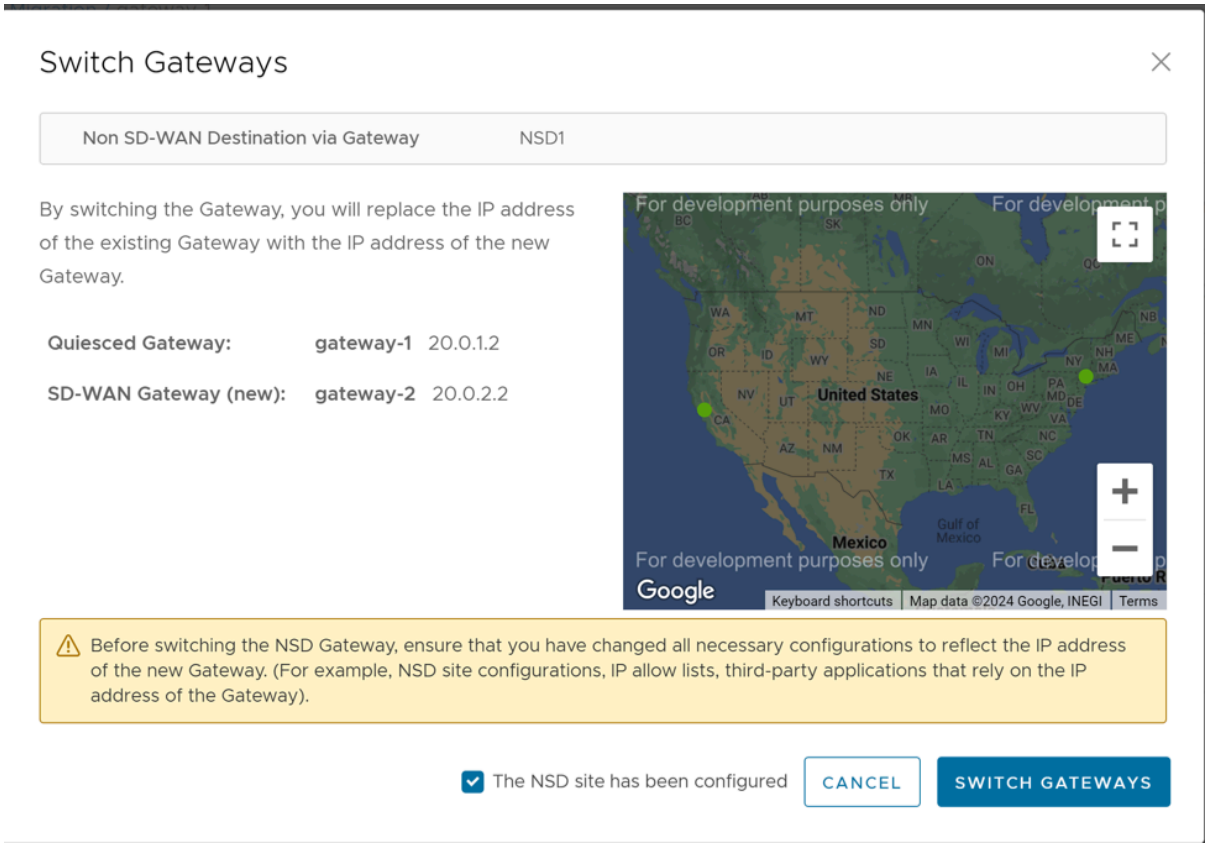
4. Select each NSD and select **Switch Gateway** to switch the traffic from the quiesced Gateway to the new Gateway.

Figure 16-18: Switch to New Gateway



a. In the **Switch Gateway** pop-up window, select the **The NSD site has been configured** check box to confirm that you have made the required changes to the remote-end NSD configuration.

Figure 16-19: Non-SD-WAN configuration



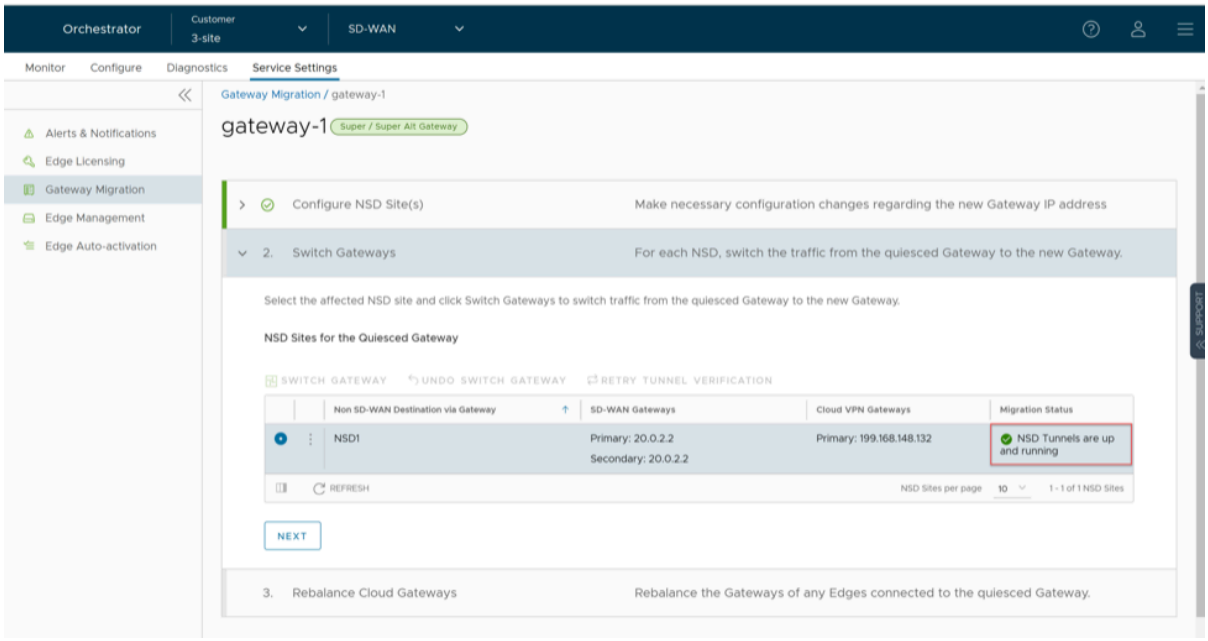
Note: This confirmation is not applicable for NSDs configured automatically.

b. Select **Switch Gateway**.

It may take few minutes to verify the tunnel status. The IP address of the quiesced Gateway is replaced with the IP address of the new Gateway so that the traffic switches to the new Gateway. The **Migration**

Status changes to "NSD Tunnels are up and running" as shown in the following screen shot. If the Switch Gateway action fails, see What to do When Switch Gateway Action Fails.

Figure 16-20: Gateway Migration- Service Setting

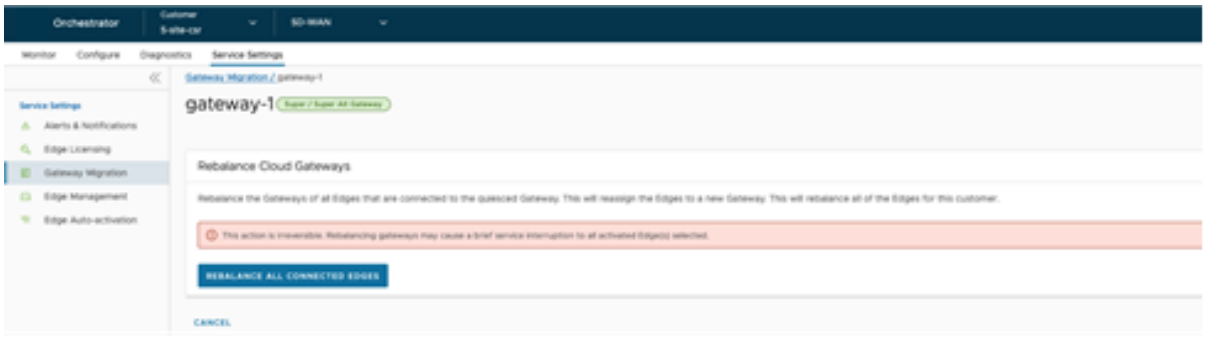


c. Select **Next**.

> **Note:** The Switch Gateway option is not available for Gateways with Data Plane role that are not attached to any NSDs.

d. Rebalance Cloud Gateways (Primary or Secondary or Super Gateways) of all Edges or the required Edges that are connected to the quiesced Gateway so that the Edges get reassigned to the new Gateway. You can rebalance Gateways from the **Configure** > **Edges** page as well.

Figure 16-21: Rebalance All Connected Edges- Super Gateway



When rebalancing Super Gateways, all the Edges connected to the quiesced Gateway will be rebalanced. Rebalancing of selected Edges is not allowed.

Figure 16-22: Rebalance All Connected Edges- Primary or Secondary Gateway

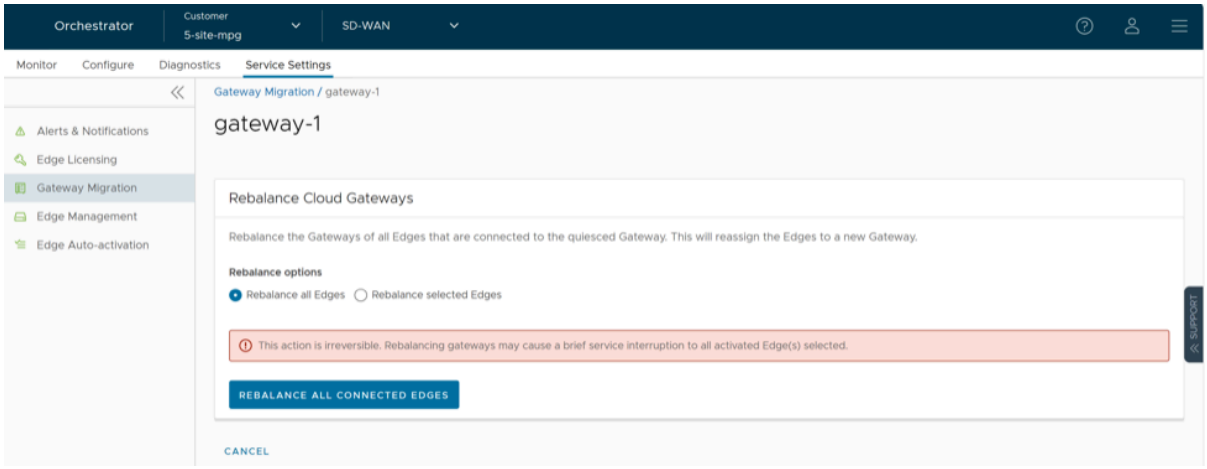
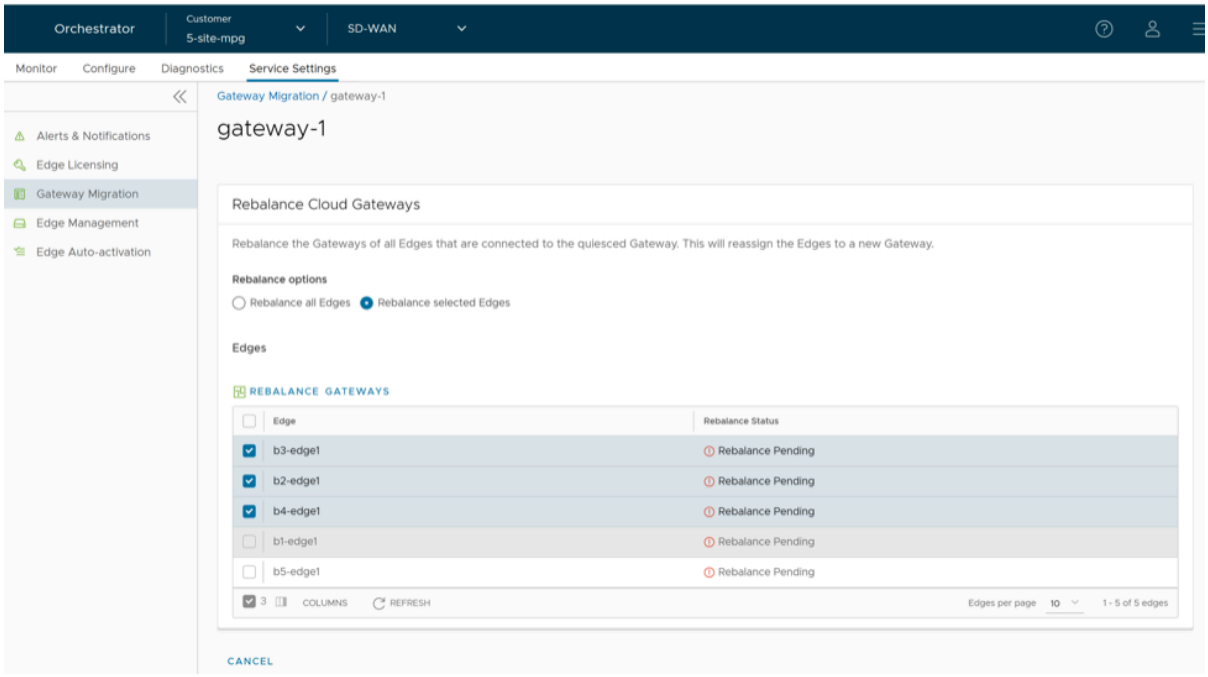
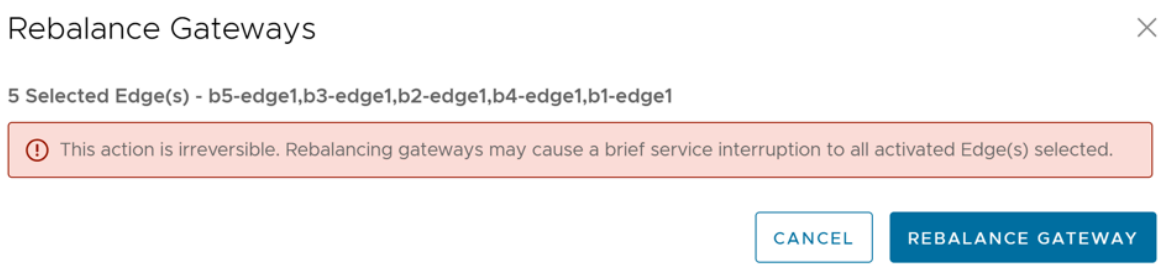


Figure 16-23: Rebalance Selected Edges- Primary or Secondary Gateway



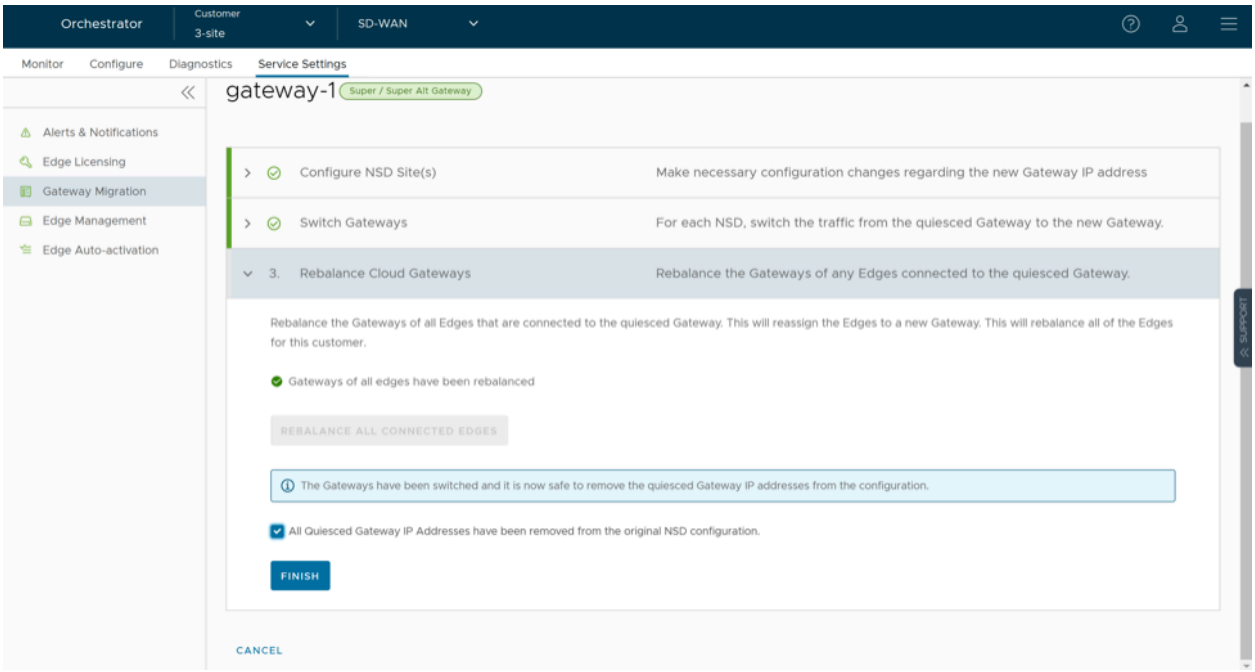
Select the Edges that are connected to the quiesced Gateway and select **Rebalance Gateways** to reassign Edges to the new Gateway.

Figure 16-24: Re-assign Edges to the New Gateway



5. Select **Rebalance Gateway** to complete the Gateway migration. The Edges connected to the quiesced Gateway are migrated to the new Gateway.

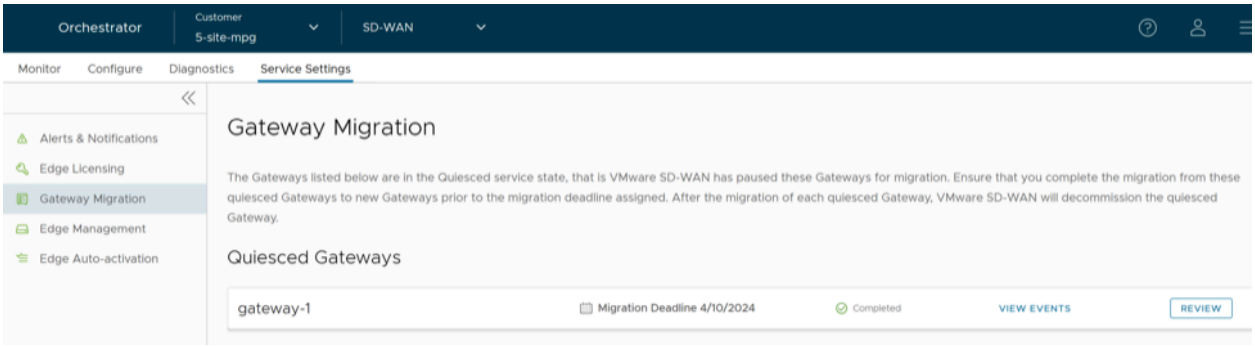
Figure 16-25: Rebalance Gateway



6. Select **Finish**.

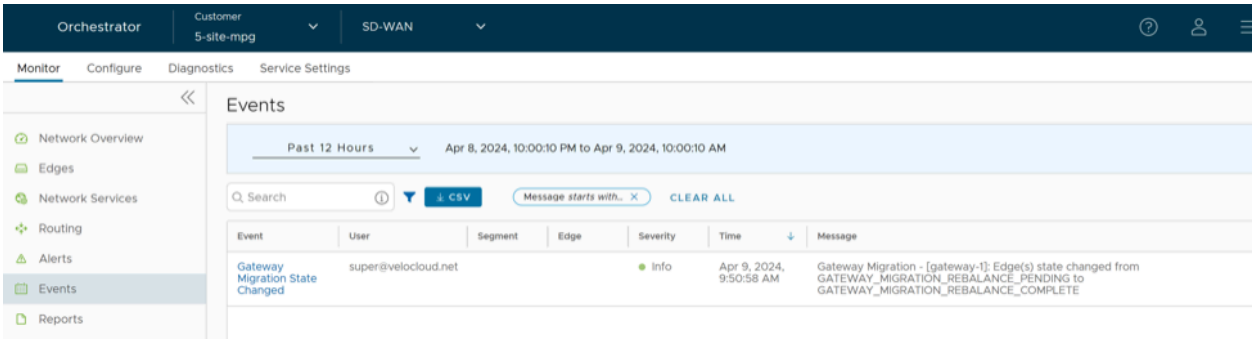
Go to the **Gateway Migration** page and select **Review** to review the migration steps, if required.

Figure 16-26: Review Gateway Migration



The Gateways that have been migrated remain in this page until the Migration Deadline assigned for the quiesced Gateway. After the Migration Deadline, you can view the history of migration events in the **Monitor** > **Events** page.

Figure 16-27: Monitor Events



16.3.3 What to do When Switch Gateway Action Fails

During the Gateway migration, when the Switch Gateway action for an Non SD-WAN Destination (NSD) fails, perform the following steps to troubleshoot the issue:

1. In the **SD-WAN** service of the **Enterprise** portal, go to the **Gateway Migration** page. For instruction to navigate to this page, see Migrate Quiesced Gateways.
2. Under the **Switch Gateways** step of the Migration Wizard, select the NSD for which the Switch Gateway action failed, and then select **Retry Tunnel Verification**.

   The tunnel status is verified again to see if the **Migration Status** changes to "**NSD Tunnels are up and running**".

   If the **Migration Status** does not change and the Switch Gateway action fails again for the NSD, select the NSD, and then select **Undo Switch Gateway**.

   All configuration changes to the NSD are reverted to the original settings.
3. Select **Switch Gateway** again to replace the IP address of the quiesced Gateway with that of the new Gateway and thereby switch the traffic to the new Gateway.

4. Rebalance the Gateway and complete the migration.

Select **View Events** on the **Gateway Migration** page to view the history of migration events in the **Monitor** > **Events** page.

16.4 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

16.4.1 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.

Partner Super user and Admin with Gateway management access activated can create, manage, and delete diagnostic bundles only for Gateway created by a Partner or a Partner managed Gateway created by your Operator. The Partner IT support users can only view the generated Diagnostic bundles and download the CSV file.

Note: The Diagnostic bundles feature is not supported for Partner Business Specialist user.

Note: The **Request Diagnostic Bundle** and **Download Bundle** options are available only for Partners with Gateway management access activated. If the Gateway management access is deactivated for a Partner, then the Partner can only view the generated Diagnostic bundles and download only the CSV file but cannot request a new Diagnostic bundle or download the generated bundle. To request Gateway Management access, Partners should contact the Operator Super user.

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 16-28: Request Diagnostic Bundle

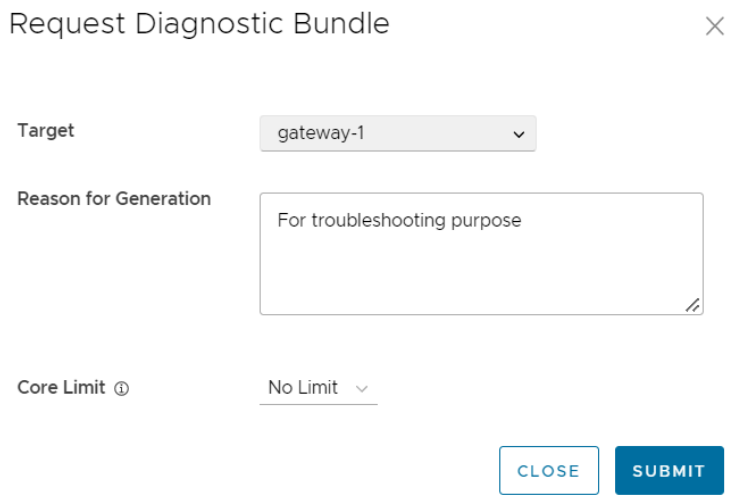


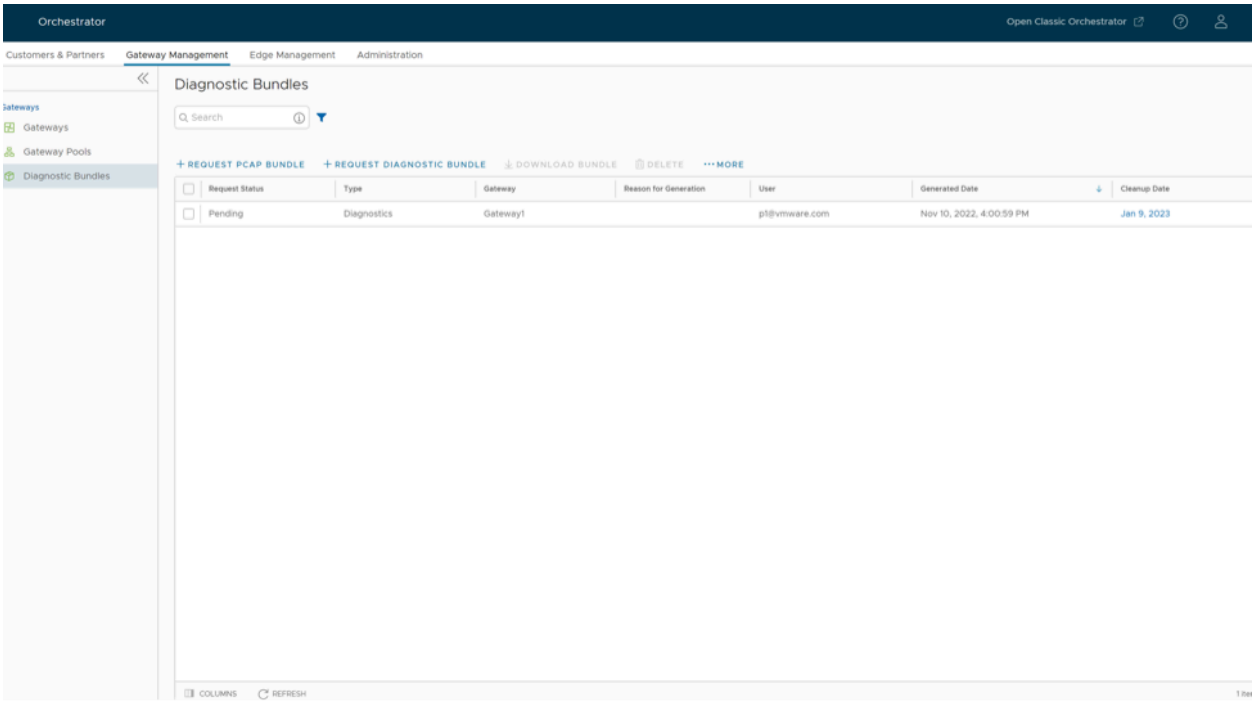
Table 43: Diagnostic Bundle Field Descriptions

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.

Note: The **Request Diagnostic Bundle** and **Download Bundle** options are available only for Partners with Gateway management access activated. If the Gateway management access is deactivated for a Partner, then the Partner can only view the generated Diagnostic bundles and download only the CSV file, but cannot request a new Diagnostic bundle or download the generated bundle. To request Gateway Management access, Partners should contact the Operator Super user.

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

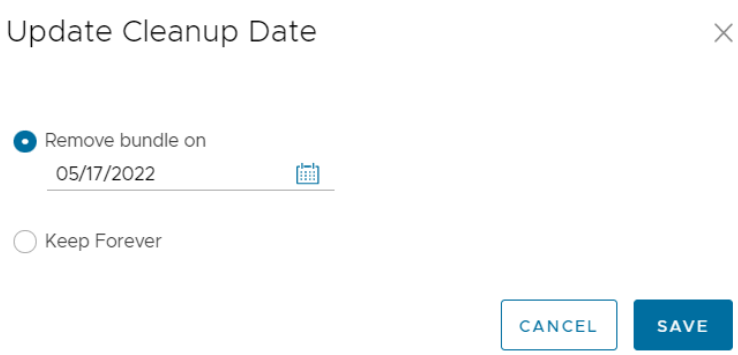
Figure 16-29: Diagnostic Bundles List



4. 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.

- **Download Diagnostic Bundle**- You can download the generated Diagnostic bundles to troubleshoot an Edge. 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.
- **Delete Diagnostic Bundle**- 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 16-30: Delete Diagnostic Bundle



In the **Update Cleanup Date** dialog, choose the date on which the selected Bundle would be deleted.

If you want to retain the Bundle, select the **Keep Forever** check box, so that the Bundle does not get deleted automatically.

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

16.4.2 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.

Partner Super user and Admin with Gateway management access activated can create, manage, and delete Packet Capture (PCAP) bundles only for Gateway created by a Partner or a Partner managed Gateway created by your Operator. The Partner IT support users can only view the generated PCAP bundles and download the CSV file.

Note: The Diagnostic bundles feature is not supported for Partner Business Specialist user.

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 16-31: Request PCAP Bundle

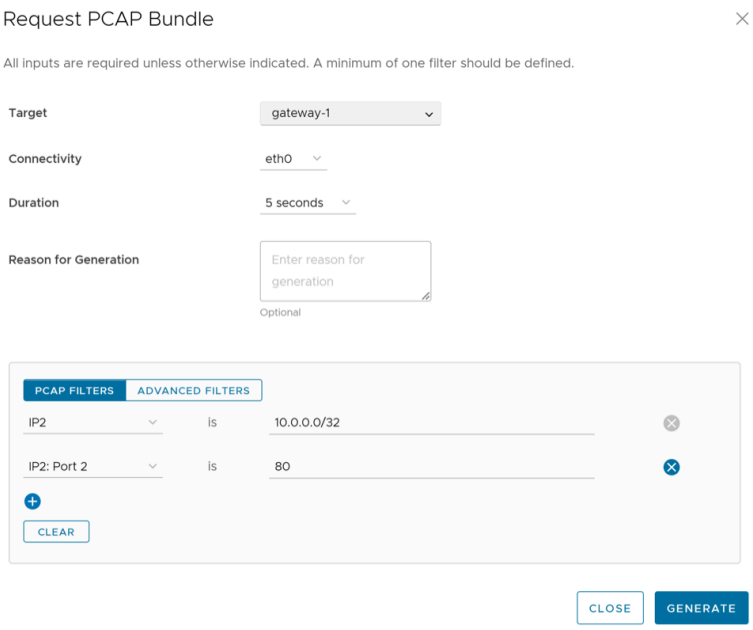


Table 44: PCAP Bundle Field Descriptions

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	You can define PCAP filters by which you want to control the PCAP data to be generated by choosing the following options: • **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. **Note:** If you choose to use the PCAP filtering capability then you must define at least one filter.
Advanced Filters	You can define free form filters by which you want to control the PCAP data to be generated.

Note: The **Request Diagnostic Bundle** and **Request PCAP Bundle** options are available only for Partners with Gateway management access activated. If the Gateway management access is deactivated for a Partner, then the Partner can only view the generated Diagnostic bundles and download only the CSV file, but cannot request a new Diagnostic or PCAP bundle or download the generated bundle. To request Gateway Management access, Partners should contact the Operator Super user.

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**.

Chapter 17

Activate SD-WAN Edges using Edge Auto-activation

Edge Auto-activation allows you to activate Edges by powering on the Edges and connecting them to the Internet.

Note: Starting from the 5.1.0 release, **Zero Touch Provisioning** is renamed as **Edge Auto-activation**.

This method eliminates the need of an activation link. Using this feature, the Service Provider can preconfigure the Edges and have them shipped to the Customers. The Customers just need to power-on the Edges and connect the cables to the internet to activate the Edges.

This method of Edge activation is also useful when the person at the remote site is unable to connect a laptop/tablet/phone to the Edge, and therefore cannot use an email or cannot click an activation code/URL.

Note:

- Edge Auto-activation supports Edge models: 510, 510 LTE, 6x0, 7x0 and 3xx0.
- For Edge Auto-activation to work, use the Orchestrator software version 4.3.0 or later.

As a Partner user, complete the following tasks to activate Edges using Edge Auto-activation:

- Sign-Up for Edge Auto-activation
- Assign Edges to Customers

17.1 Sign-Up for Edge Auto-activation

- As a Partner user, ensure that you have a valid Partner Relationship Management Identifier (PRM ID), received at the time of registering with Arista. If you do not have a valid PRM ID, contact Arista Partner Connect.
- Outbound internet connectivity via DHCP is required to complete the push activation successfully.

To sign-up for Edge Auto-activation:

1. Log in to **Orchestrator**, and then go to **Edge Management** > **Edge Auto-activation**.
2. On the **Edge Auto-activation** page, enter the **PRM ID**.
3. Select **Submit**.

Note: You are required to enter the **PRM ID** only when you login for the first time. You can view the Edge inventory in the **Available Inventory** tab only after the successful validation of PRM ID.

The validation process may take up to 3 to 5 days. If you enter an incorrect PRM ID, you must contact the Customer Support team to get it changed.

Only the Edges that were shipped to you after the successful completion of the sign-up process appear in the **Available Inventory** tab. Ensure that the PRM ID assigned to you is used in all your future orders so that the inventory is reflected correctly. You must assign the Edges to Customers, and then assign profile and license to Edges. For instructions, see Assign Edges to Customers.

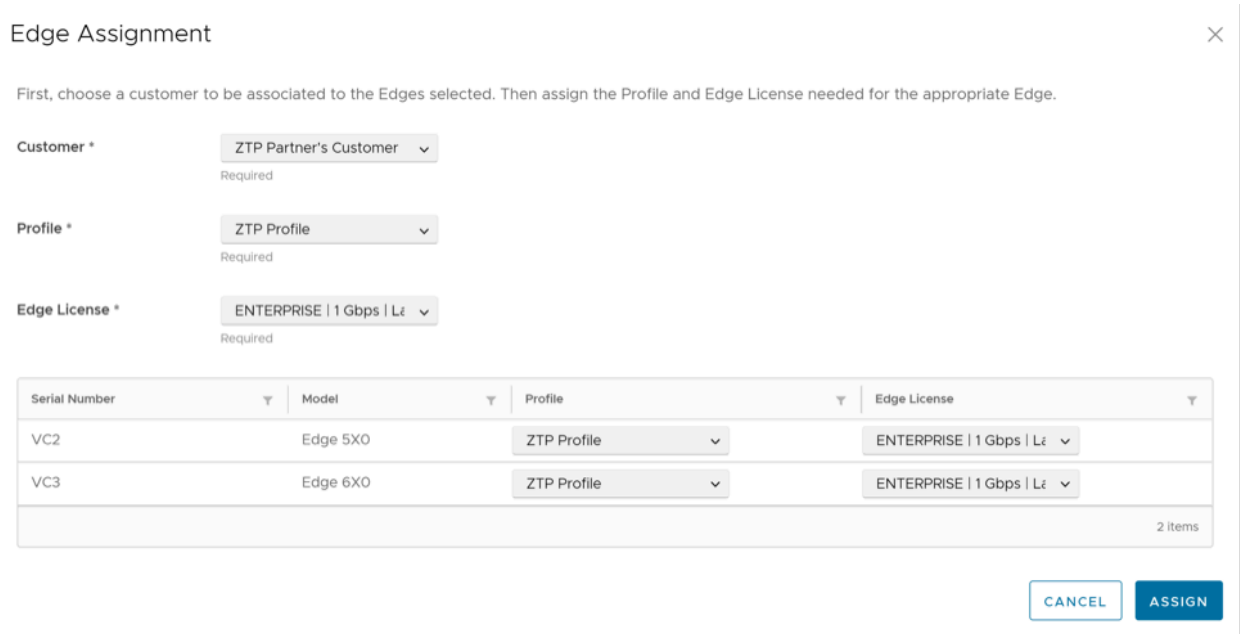
17.2 Assign Edges to Customers

Ensure that you have signed-up for Edge Auto-activation so that you can view the list of Edges in the **Available Inventory** page. For instructions, refer to Sign-Up for Edge Auto-activation.

To assign Edges to Customers:

1. Log in to **Orchestrator**, and then go to **Edge Management** > **Edge Auto-activation**.
   A list of Edge inventory with Serial number and Model appears.
2. Select all the Edges that you want to assign to Customers, and then select **Assign To Customer**. The **Edge Assignment** window appears.

   Figure 17-1: Edge Assignment



3. From the **Customer** drop-down list, select the Customer to whom you want to assign the Edges.
4. From the **Profile** and **Edge License** drop-down lists, select the required profile and license that you want to assign to all Edges in the inventory.

Note: You can choose to override these settings for a specific Edge by selecting the appropriate profile and license in the table.

5. Select **Assign**. The Edges for which you have assigned a Customer, a profile and a license, appear in the **Assigned Inventory** tab. The **Inventory State** for the assigned Edges is displayed as **Assigned to Customer** and the **Edge State** is displayed as **Pending**.
6. Following are the additional options available on the **Edge Auto-activation** page:

Table 45: Edge Auto-activation- Additional Settings

Option	Description
Search	Enter a search term to be searched across the items in the table. Use the advanced search option for more filters.
Download CSV	Select to download the list of Edges in an excel format.
Columns	Select the checkboxes to view the required columns.
Refresh	Select this option to refresh the table properties.

When your Customer powers-on the assigned physical Edges and connects them to the internet, the Edges are redirected to the Orchestrator, where they are automatically activated. After an Edge is activated, the **Edge State** in the **Assigned Inventory** tab changes from **Pending** to **Activated**.

17.2.1 Reassign an Edge to Another Customer

You can reassign an Edge to another Customer before the Edge is activated.

If you choose to reassign an Edge that is already activated, you must deactivate the Edge, and then reassign the Edge to another Customer. For instructions about how to deactivate an Edge, refer to the topic *Remote Actions* in the *Arista SD-WAN Troubleshooting Guide*. Once you deactivate the Edge, the Edge state changes to Offline. You can now reassign the Edge to another Customer.

To reassign an Edge to another Customer:

1. Log in to **Orchestrator**, and then go to **Edge Management** > **Edge Auto-activation**. Select **Assigned Inventory** tab.
2. Select the Edge that you want to reassign, and then select **Reassign**. The **Edge Reassignment** window appears.
3. From the **Customer** drop-down list, select the Customer to whom you want to reassign the Edge.
4. From the **Profile** and **Edge License** drop-down lists, select the required profile and license that you want to assign to the Edge.
5. Select **Reassign**.

Though the Edge is reassigned to the new Customer, a corresponding entry would still be available in the **Configure** > **Edges** page of the Customer to whom the Edge was originally assigned. Select the logical Edge entry, and then select **Delete** to manually delete the entry.

17.3 Activate Edges Using Email

In this method, the Edge is shipped to the Customer site with a factory-default configuration. Prior to activation, the Edge contains no configuration or credentials to connect to the Enterprise network.

Complete the following steps to activate Edges using the Email method:

1. Send an Activation Email. The administrator initiates the activation process by sending an activation procedure email to the person that will install the Edge, typically a Site Contact. For additional information, see Send Edge Activation Email.

2. Activate the Edge Device. The instructions in the activation procedure email activates the Edge device. For additional information, see Activate an Edge Device.

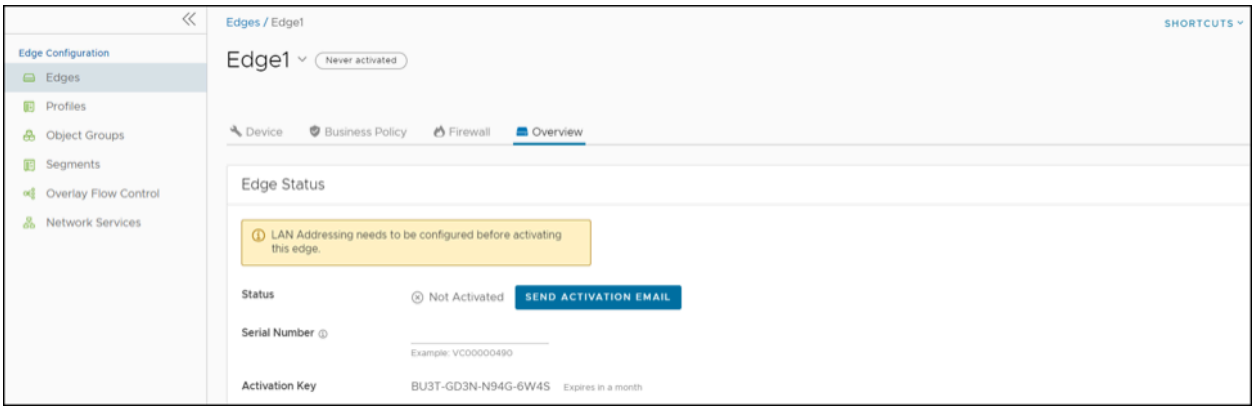
17.3.1 Send Edge Activation Email

The administrator initiates the activation process of an Edge by sending an activation procedure Email to the person installing the Edge, typically a Site Contact.

To send the Edge Activation Email:

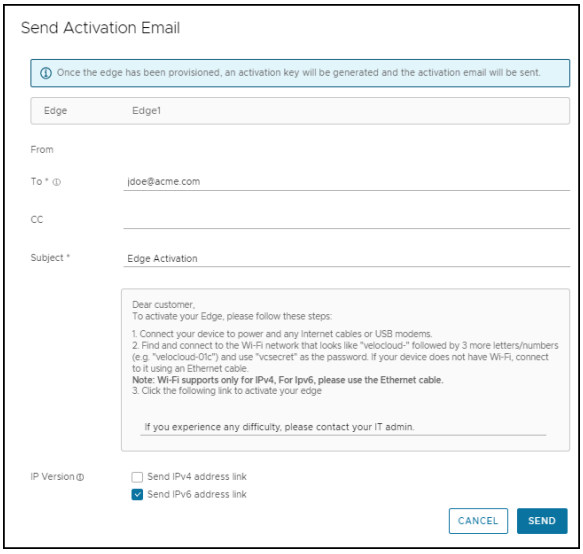
1. In the **SD-WAN** service of the **Enterprise** portal, go to **Configure** > **Edges**.
2. The **Edges** page displays the existing Profiles.
3. Select the link to the Edge to be activated or select the **View** link in the **Device** column of the Edge.
4. Select the **Overview** tab. For an Edge that is not activated, the **Edge Status** section displays the option to send an activation Email:

Figure 17-2: Edge Status



5. Select **Send Activation Email**.

Figure 17-3: Send Activation Email



6. Enter the details like Email address of the recipient, the Site contact, and Subject line. A default Email message is available. If required, you can add the contact details of IT admin in the message. Select the IP version of the activation link to be sent. You can select the link to contain either IPv4 address or IPv6 address, or both.
7. Select **Send** and the activation Email is sent to the Site contact.

   Once the Site contact receives the activation Email, you can activate the Edge. For additional information, see Activate an Edge Device.

Note:

- For the Edge 510 LTE device, the Activation Email consists of Cellular Settings like SIM PIN, Network, APN, and Username. A supported factory default image is required.
- For the 610, 620, 640, 680, and 610 LTE devices with SFP that are configured with ADSL2/ VDSL2, the activation email consists of configuration settings like Profile, PVC, VPC, and so on. A supported factory default image is required.

Remote Diagnostics for 510 LTE and 6X0 Devices:

- If you configure the SD-WAN Edge 510 LTE device, you can run the “LTE Modem Information” diagnostic test for troubleshooting purposes. The **LTE Modem Information** diagnostic test will retrieve diagnostic information, such as signal strength, connection information, etc.
- The **DSL Status** diagnostic test is available only for the 610, 620, 640, and 680 devices. Running this test will show the DSL status, which includes information such as Mode (Standard or DSL), Profile, xDSL Mode, and so on.

For information on how to run a diagnostic test, see the *Arista SD-WAN Troubleshooting Guide*.

17.3.2 Activate an Edge Device

The Site Contact performs the steps outlined in the Edge activation procedure email.

In general, the Site Contact completes the following steps:

1. Connect the Edge to a power source and insert any WAN link cables or USB modems for Internet connectivity.
2. Connect a personal computer or mobile device (with access to the activation email) to your Edge by one of two methods:

   Note: The connected personal computer or mobile device cannot directly access the public internet through the Edge device until it is activated.

   a. Find and connect to the Wi-Fi network that looks like velocloud- followed by three more letters/numbers (for example, velocloud-01c) with the password vcsecret.

      Note: Refer to the Wi-Fi SSID from the Edge device. The default Wi-Fi is vc-wifi. The Edge activation email provides instructions for using one or more Wi-Fi connections.

   b. If the Edge is not Wi-Fi capable (for example, a 6x0N model or a 3x00 model), use an Ethernet cable to connect to either an Ethernet-equipped computer or a mobile device with an Ethernet adapter to one of the Edge's LAN ports.

      Note: For additional information about using either an iOS or Android mobile device with an Ethernet adapter to activate an Edge, refer to the below sections:

      - Edge Activation using an iOS Device and an Ethernet Cable
      - Edge Activation using an Android Device and an Ethernet Cable

3. Select the hyperlink in the email to activate the Edge.

   During the Edge activation, the activation status screen appears on your connected device.

   The Edge downloads the configuration and software from the Orchestrator and reboots multiple times to apply the software update (If the Edge has a front LED status light, that light would blink and change colors multiple times during the activation process).

   Once the Edge activation process successfully completes, the Edge is ready for service (if the Edge has a front LED status light, the light would show as solid green). Once an Edge is activated, it is "useable" for routing network traffic. In addition, more advanced functions such as monitoring, testing, and troubleshooting are also available.

17.3.2.1 Edge Activation using an iOS Device and an Ethernet Cable

There are multiple ways to activate a VeloCloud SD-WAN Edge. It is recommended to use the Edge Auto-activation push activation whenever possible. Alternatively, you can use the email activation (pull activation) method using an iOS device and an Ethernet cable.

The components required for this procedure are:

- iPhone/iPad with email access
- Ethernet adapter suitable for phone or tablet

Note: The example used here is an Edge 540 and an iPhone 12 Pro Max. You can use other Edge and iPhone/iPad models too.

1. Complete the Edge configuration on the Orchestrator software. For details, refer to the *Configure Edge Device* section in the *Arista VeloCloud SD-WAN Administration Guide*.
2. Navigate to **Configure** > **Edges** > **Edge Overview tab**, and then select the **Send Activation Email** button.
3. Enter the email address of the person activating the Edge, and then select **Send**.
4. Power up the Edge, and then connect it to an available internet connection using an Ethernet cable.

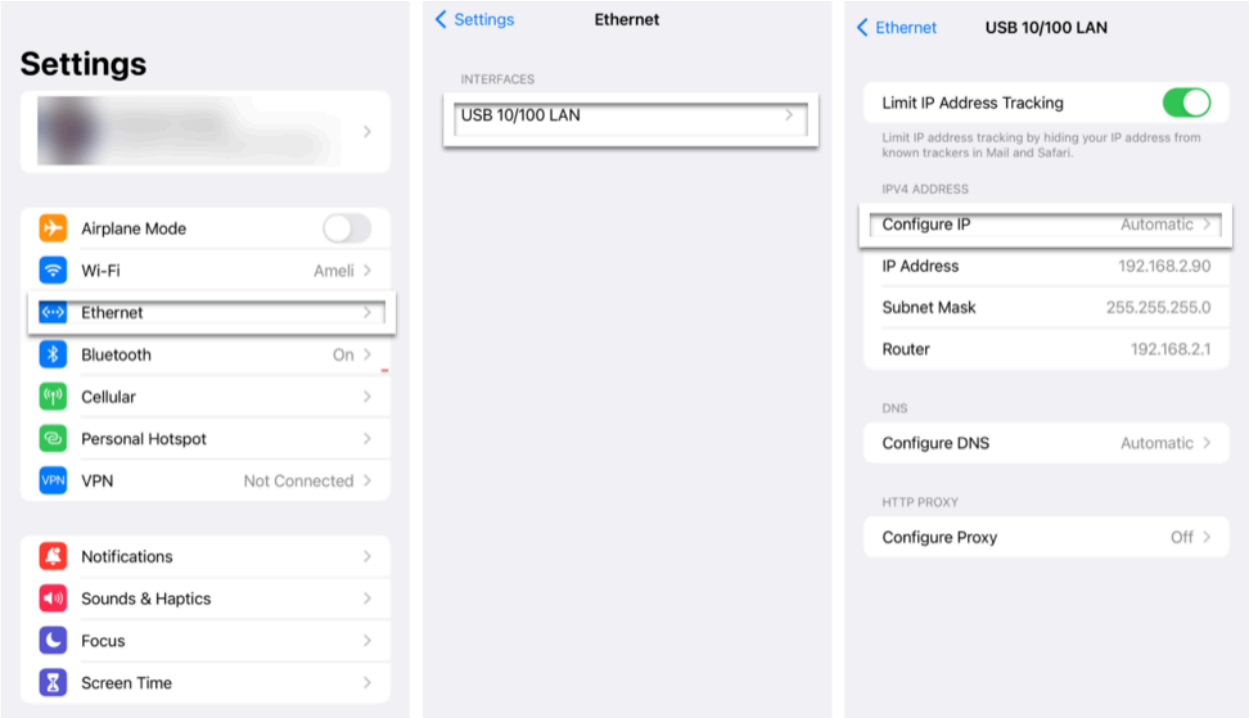
   Note: Refer to *Edge Activation Guides* to check details of the model you are installing to determine the correct port.

5. Connect an Ethernet adapter to your phone, and then connect the Edge's LAN port to the Ethernet adapter.

   Note: The Edge is configured by default to acquire a DHCP IP address from the ISP on the WAN (uplink). The Edge also assigns a DHCP address to the phone connected to the LAN port. When the WAN connection is fully operational, the cloud LED on the front of the Edge turns green.

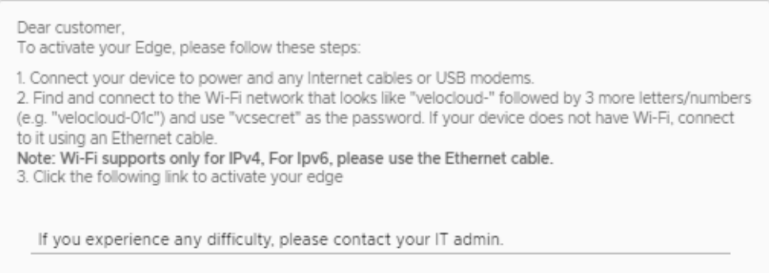
6. In your iOS device, go to **Settings** > **Ethernet**. Select the appropriate interface. Under the IPv4 Address, select **Configure IP** as **Automatic**.

Figure 17-4: Settings



7. Open the activation email from your phone, and then select the activation link displayed at the bottom of the screen to activate your Edge. The following screenshot is an example.

Figure 17-5: Sample Email



You can see the activation progress on your phone screen. Once complete, **Activation successful** message is displayed. Your Edge device is now activated.

17.3.2.2 Edge Activation using an Android Device and an Ethernet Cable

The procedure below discusses the Edge email activation (pull activation) using an Android device and an Ethernet cable.

The components required for this procedure are:

- Android phone with email access
- Ethernet adapter suitable for the phone

> **Note:** The example used here is an Edge 610 and a Samsung Galaxy S10+ Smartphone. You can use other Edge and Android phone models too.

1. Complete the Edge configuration on the Orchestrator software. For details, refer to the *Configure Edge Device* section in the *Arista VeloCloud SD-WAN Administration Guide*.
2. Navigate to **Configure** > **Edges** > **Edge Overview tab**, and then select the **Send Activation Email** button.
3. Enter the email address of the person activating the Edge, and then select **Send**.
4. Power up the Edge, and then connect it to an available internet connection using an Ethernet cable.

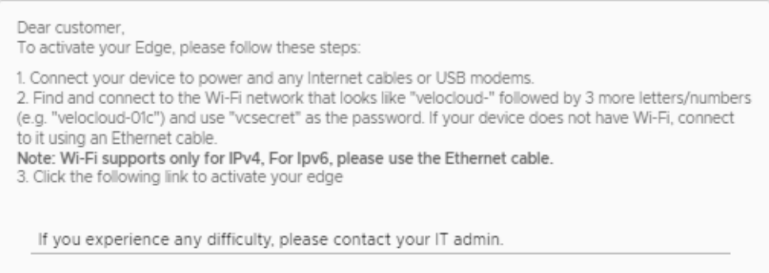
> **Note:** Refer to *Edge Activation Guides* to check details of the model you are installing to determine the correct port.

5. Connect an Ethernet adapter to your phone, and then connect the Edge's LAN port to the Ethernet adapter.

> **Note:** The Edge is configured by default to acquire a DHCP IP address from the ISP on the WAN (uplink). The Edge also assigns a DHCP address to the phone connected to the LAN port. When the WAN connection is fully operational, the cloud LED on the front of the Edge turns green.

6. Open the activation email from your phone, and then select the activation link displayed at the bottom of the screen to activate your Edge. The following screenshot is an example.

   Figure 17-6: Sample Email



   You can see the activation progress on your phone screen. Once complete, **Activation successful** message is displayed. Your Edge device is now activated.

17.4 Request RMA Reactivation

Initiate a Return Merchandise Authorization (RMA) request either to return the existing Edge or to replace an Edge.

There are several scenarios that require an Edge RMA reactivation. Following are the two most common scenarios:

- Replace an Edge due to a malfunction—A typical scenario that requires an Edge RMA reactivation occurs when a malfunctioned Edge of the same model needs replacement. For example, a customer needs to replace a 520 Edge model with another 520 Edge model.
- Upgrade an Edge hardware model—Another common scenario that requires an Edge RMA reactivation is when you want to replace an Edge with a different model. Usually this is due to a scaling issue in which you have outgrown the capacity of the current Edge.

> **Note:** RMA reactivation request is allowed only for activated Edges.

You can initiate the RMA reactivation request using one of the following methods:

- Request RMA Reactivation Using Edge Auto-activation
- Request RMA Reactivation Using Email

17.4.1 Request RMA Reactivation Using Edge Auto-activation

To request RMA reactivation using Zero Touch Provisioning:

1. Log in to **Orchestrator**, and in the **SD-WAN** service of the **Enterprise** portal go to **Configure** > **Edges**.
2. Select the Edge that you want to replace.
   The **Edge Overview** page appears.
3. Scroll down to the **RMA Reactivation** area, and then select **Request Reactivation** to generate a new activation key. The status of the Edge changes to **Reactivation Pending** mode.

> **Note:** The reactivation key is valid for one month only. When the key expires, a warning message is displayed. To generate a new key, select **Generate New Activation Key**. For details, refer to *RMA Reactivation* section in the *View Edge Information* topic in the *Arista VeloCloud SD-WAN Administration Guide*.

4. In the **RMA Serial Number** field, enter the serial number of the new Edge that is to be activated.
5. From the **RMA Model** drop-down list, select the hardware model of the new Edge that is to be activated.

> **Note:** If the Serial Number and the hardware model do not match the new Edge that is to be activated, the activation fails.

6. Select **Update**. The status of the new Edge changes to **Reactivation Pending** and the status of the old Edge changes to **RMA Requested**. To view the Edge State, go to **Service Settings** > **Edge Auto-activation**.
7. Complete the following tasks to activate the new Edge:
   a. Disconnect the old Edge from the power and network.
   b. Connect the new Edge to the power and network. Ensure that the Edge is connected to the Internet.

The new Edge is redirected to the Orchestrator where it is automatically activated. The status of the new Edge changes to **Activated**.

Return the old Edge to Arista so that the logical entry for the old Edge with the state **RMA Requested** gets removed from the **Service Settings** > **Edge Auto-activation** page.

17.4.2 Request RMA Reactivation Using Email

To request RMA reactivation using email:

1. Log in to **Orchestrator**, and then go to **Configure** > **Edges**.
2. Select the Edge that you want to replace.
   The **Edge Overview** page appears.
3. Scroll down to the **RMA Reactivation** area, and then select **Request Reactivation** to generate a new activation key. The status of the Edge changes to **Reactivation Pending** mode.

> **Note:** The reactivation key is valid for one month only. When the key expires, a warning message is displayed. To generate a new key, select **Generate New Activation Key**. For details, refer to *RMA Reactivation* section in the *View Edge Information* topic in the *Arista VeloCloud SD-WAN Administration Guide*.

4. Select **Send Activation Email** to initiate the Edge activation Email with instructions. The Email consists of the instructions along with the activation URL. The URL displays the Activation key and the IP address of the Orchestrator.
5. Complete the following tasks to activate the new Edge:
   a. Disconnect the old Edge from the power and network.
   b. Connect the new Edge to the power and network. Ensure that the Edge is connected to the Internet.
   c. Follow the activation instructions in the email. Select the activation link in the email to activate the Edge.

The Edge downloads the configuration and software from the Orchestrator and gets activated.

Chapter 18

Install Partner Gateway

This document discusses the steps needed to install and deploy VeloCloud Gateway as a Partner Gateway. It also covers how to configure the VRF/VLAN and BGP configuration necessary on the Orchestrator on the Partner Gateway.

18.1 Installation Overview

This section provides an overview of Partner Gateway installation.

About Partner Gateways

Partner Gateways are Gateways tailored to an on-premise operation in which the Gateway is installed and deployed with two interfaces.

- One interface is facing the private and/or public WAN network and is dedicated to receiving VCMP encapsulated traffic from the remote edges, as well as standard IPsec traffic from Non SD-WAN Destinations.
- Another interface is facing the datacenter and provides access to resources or networks attached to a PE router, which the Partner Gateway is connected to. The PE router typically affords access to shared managed services that are extended to the branches, or access to a private (MPLS / IP-VPN) core network in which individual customers are separated.

The following distributions are provided:

Table 46: Distributions

Provided	Description	Example
Arista	Gateway OVA package.	velocloud-vcg-X.X.X-GA.ova
KVM	Gateway qcow2 disk image.	velocloud-vcg-X.X.X-GA.qcow2

18.2 Minimum Hypervisor Hardware Requirements

The Gateway runs on a standard hypervisor (KVM or VMware ESXi).

Note: Starting from the 6.0.0 release, Intel E810 NIC is supported on a Gateway using SR-IOV on KVM 22.04, for high performance Data Plane throughput.

Minimum Server Requirements

To run the hypervisor:

- CPU: Intel XEON (10 cores minimum to run a single 8-core gateway VM) with minimum clock speed of 2.0 Ghz is required to achieve maximum performance.
  - ESXi vmxnet3 network scheduling functions must have 2 cores reserved per Gateway virtual machine (VM), regardless of the number of cores assigned to the Gateway.
    - Example: Assume there is a 24-core server running ESXi+vmxnet3. You can deploy 2 - (8 core) Gateways. i.e. 2 gateways multiplied by 8 cores requires 16 cores reserved for gateway application and leaves 8 free cores. By using the formula above, in order to support these two Gateways running at peak performance scale the ESXi/vmxnet3 system requires an additional 4 cores (two cores for each of the two Gateways deployed). That is a total of 20 cores required to run 2 gateways on a 24 core system.

      Note: When using SR-IOV, the network scheduling function is offloaded to the pNIC to achieve higher performance. However, the hypervisor must still perform other scheduling functions like CPU, memory, NUMA allocation management. It is required to always keep two free cores for hypervisor usage.

- The CPU must support and activate the following instruction sets: AES-NI, SSSE3, SSE4, RDTSC, RDSEED, RDRAND, AVX/AVX2/AVX512.
- A minimum of 4GB free RAM must be available to the server system aside from the memory assigned to the PGW VMs. One Gateway VM requires 16GB RAM, or 32GB RAM if certificate-based authentication is activated.
- Minimum of 150GB magnetic or SSD based, persistent disk volume (One Gateway VM requires 64GB or 96GB Disk Volume, if certificate-based authentication is activated).
- Minimum required IOPS performance: 200 IOPS.
- Minimum 1x10Ge network interface ports and 2 ports is preferred when enabling the Gateway partner hand-off interface (1Ge NICs are supported, but will bottleneck performance). The physical NIC cards supporting SR-IOV are Intel 82599/82599ES and Intel X710/XL710 chipsets. (See the ‘Enable SR-IOV’ guide).

  Note: SR-IOV does not support NIC bonding. For redundant uplinks, use ESXi vSwitch.

- VeloCloud Gateway is a data-plane intensive workload that requires dedicated CPU cycles to ensure optimal performance and reliability. Meeting these defined settings are required to ensure the Gateway VM is not oversubscribing the underlying hardware and causing actions that can destabilize the Gateway service (e.g. NUMA boundary crossing, memory, and/or vCPU oversubscription).
- Ensure that the SD-WAN Partner Gateway VM and the resources such as network interfaces, memory, physical CPUs used to support it fit within a single NUMA node.
- 

  Note: Configure the host BIOS settings as follows:
  - Hyper-threading- Turned off
  - Power Savings- Turned off
  - CPU Turbo- Enabled
  - AES-NI- Enabled
  - NUMA Node Interleaving- Turned off

- Use ESXi host version: ESXi-6.7.0-14320388-standard or above
- Upgrade VM compatibility should be set before starting the Gateway SD-WAN Gateway instance

Table 47: Example Server Specifications

NIC Chipset	Hardware	Specification
Intel 82599/82599ES	HP DL380G9	http://www.hp.com/hpinfo/newsroom/press_kits/2014/ComputeEra/HP_ProLiantDL380_DataSheet.pdf
Intel X710/XL710	Dell PowerEdge R640	https://www.dell.com/en-us/work/shop/povw/poweredge-r640 • CPU Model and Cores- Dual Socket Intel(R) Xeon(R) Gold 5218 CPU @ 2.30GHz with 16 cores each • Memory- 384 GB RAM
Intel X710/XL710	Supermicro SYS-6018U-TRTP+	https://www.supermicro.com/en/products/system/1U/6018/SYS-6018U-TRTP_.cfm • CPU Model and Cores- Dual Socket Intel(R) Xeon(R) CPU E5-2630 v4 @ 2.20GHz with 10 Cores each • Memory- 256 GB RAM
Intel E810-CQDA2	Dell PowerEdge R640	https://www.dell.com/en-us/work/shop/povw/poweredge-r640 • • CPU Model and Cores- Dual Socket Intel(R) Xeon(R) Gold 5218 CPU @ 2.30GHz with 16 cores each • Memory- 384 GB RAM

Table 48: Required NIC Specifications for SR-IOV Support

Hardware Manufacturer	Firmware Version	Host Driver for Ubuntu 20.04.6	Host Driver for Ubuntu 22.04.2	Host Driver for ESXi 7.0U3	Host Driver for ESXi 8.0U1a
Dual Port Intel Corporation Ethernet Controller XL710 for 40GbE QSFP+	7.10	2.20.12	2.20.12	1.11.2.5 and 1.11.3.5	1.11.2.5 and 1.11.3.5
Dual Port Intel Corporation Ethernet Controller X710 for 10GbE SFP+	7.10	2.20.12	2.20.12	1.11.2.5 and 1.11.3.5	1.11.2.5 and 1.11.3.5
Quad Port Intel Corporation Ethernet Controller X710 for 10GbE SFP+	7.10	2.20.12	2.20.12	1.11.2.5 and 1.11.3.5	1.11.2.5 and 1.11.3.5
Dell rNDC X710/350 card	nvm 7.10 and FW 19.0.12	2.20.12	2.20.12	1.11.2.5 and 1.11.3.5	1.11.2.5 and 1.11.3.5
Dual Port Intel Corporation Ethernet Controller E810-CQDA2 for 100GbE QSFP	4.20	ICE 1.11.14	ICE 1.11.14	Not supported yet	Not supported yet

Table 49: Supported Hypervisor Versions

Hypervisor	Supported Versions
Arista	• Intel 82599/82599ES- ESXi 6.7 U3, ESXi 7.0U3, ESXi 8.0U1a. To use SR-IOV, the vCenter and the vSphere Enterprise Plus license are required. • Intel X710/XL710- ESXi 6.7 U3 with Arista vSphere Web Client 6.7.0 up to ESXi 8.0 U1a with Arista vSphere Web Client 8.0.
KVM	• Intel 82599/82599ES- Ubuntu 20.04.6 LTS, Ubuntu 22.04.2 • Intel X710/XL710- Ubuntu 20.04.6 LTS, Ubuntu 22.04.2 • Intel E810-CQDA2- Ubuntu 22.04.2

Gateway Virtual Machine (VM) Specification

For Arista, the OVA already specifies the minimum virtual hardware specification. For KVM, an example XML file is provided. The minimum virtual hardware specifications are:

- If using VMware ESXi:
  - Latency Sensitivity must be set to 'High'.
    - Procedure (Adjust Latency Sensitivity)
      1. Browse to the virtual machine in the vSphere Client.
         a. To find a virtual machine, select a data center, folder, cluster, resource pool, or host.
         b. Select the **VMs** tab.
      2. Right-click the virtual machine, and then select **Edit Settings**.

3. Select **VM Options** and select **Advanced**.
4. Select a setting from the **Latency Sensitivity** drop-down menu.
5. Select **OK**.

- CPU reservation set to 100%.
- CPU shares set to **high**.
- CPU Limit must be set to **Unlimited**.
- 8 vCPUs (4vCPUs are supported but expect lower performance).

> **Important:** All vCPU cores should be mapped to the same socket with the Cores per Socket parameter set to either 8 with 8 vCPUs, or 4 where 4 vCPUs are used.

> **Note:** Hyper-threading must be deactivated to achieve maximum performance.

- Procedure for Allocate CPU Resources:
  1. Select **Virtual Machines** in the Arista Host Client inventory.
  2. Right-click a virtual machine from the list and select **Edit** settings from the pop-up menu.
  3. On the **Virtual Hardware** tab, expand CPU, and allocate CPU capacity for the virtual machine.

Table 50: Gateway Virtual Machine (VM) Specification

Option	Description
Reservation	Guaranteed CPU allocation for this virtual machine.
Limit	Upper limit for this virtual machine's CPU allocation. Select Unlimited to specify no upper limit.
Shares	CPU shares for this virtual machine in relation to the parent's total. Sibling virtual machines share resources according to their relative share values bounded by the reservation and limit. Select Low, Normal, or High, which specify share values respectively in a 1:2:4 ratio. Select Custom to give each virtual machine a specific number of shares, which express a proportional weight.

- CPU affinity must be activated. Follow the steps below:
  1. In the vSphere Web Client go to the **VM Settings** tab.
  2. Choose the **Options** tab and select **Advanced General** > **Configuration Parameters**.
  3. Add entries for numa.nodeAffinity=0, 1, ..., where 0 and 1 are the processor socket numbers.
- vNIC must be of type 'vmxnet3' (or SR-IOV, see SR-IOV section for support details).
- Minimum of any one of the following vNICs:
  - The First vNIC is the public (outside) interface, which must be an untagged interface.
  - The Second vNIC is optional and acts as the private (inside) interface that can support VLAN tagging dot1q and Q-in-Q. This interface typically faces the PE router or L3 switch.

- Optional vNIC (if a separate management/OAM interface is required).
- Memory reservation is set to ‘maximum.’
  - 16GB of memory (32GB RAM is required when enabling certificate-based authentication).
- 64 GB of virtual disk (96GB disk is required when enabling certificate- based authentication).

> **Note:** Arista uses the above defined settings to obtain scale and performance numbers. Settings that do not align with the above requirements are not tested by Arista and can yield unpredictable performance and scale results.

- If using KVM:
  - vNIC must be of 'Linux Bridge' type. (SR-IOV is required for high performance, see SR-IOV section for support details).
  - 8 vCPUs (4vCPUs are supported but expect lower performance).

> **Important:** All vCPU cores should be mapped to the same socket with the Cores per Socket parameter set to either 8 with 8 vCPUs, or 4 where 4 vCPUs are used.

> **Note:** Hyper-threading must be deactivated to achieve maximum performance.

  - 16GB of memory (32GB RAM is required when enabling certificate- based authentication)
  - Minimum of any one of the following vNICs:
    - The First vNIC is the public (outside) interface, which must be an untagged interface.
    - The Second vNIC is optional and acts as the private (inside) interface that can support VLAN tagging dot1q and Q-in-Q. This interface typically faces the PE router or L3 switch.
  - Optional vNIC (if a separate management/OAM interface is required).
  - 64 GB of virtual disk (96GB disk is required when enabling certificate- based authentication).

Firewall/NAT Requirements

> **Note:** These requirements apply if the Gateway is deployed behind a Firewall and/or NAT device.

- The firewall needs to allow outbound traffic from the Gateway to TCP/443 (for communication with Orchestrator).
- The firewall needs to allow inbound traffic from the Internet to UDP/2426 (VCMP), UDP/4500, and UDP/500. If NAT is not used, then the firewall needs to also allow IP/50 (ESP).
- If NAT is used, the above ports must be translated to an externally reachable IP address. Both the 1:1 NAT and port translations are supported.

Use of DPDK on Gateways

To improve packet throughput performance, Gateways take advantage of Data Plane Development Kit (DPDK) technology. DPDK is a set of data plane libraries and drivers provided by Intel for offloading TCP

packet processing from the operating system kernel to processes running in user space and results in higher packet throughput. For additional details, see https://www.dpdk.org/.

On Arista hosted Gateways and Partner Gateways, DPDK is used on interfaces that manage data plane traffic and is not used on interfaces reserved for management plane traffic. For example, on a typical Arista hosted Gateway, eth0 is used for management plane traffic and would not use DPDK. In contrast, eth1, eth2, and eth3 are used for data plane traffic and use DPDK.

18.3 Gateway Installation Procedure

This section describes the Gateway installation procedures.

To install the Gateway, perform the following steps:

1. Create Gateway on **Orchestrator** and make a note of the activation key.
2. Configure Gateway on **Orchestrator**.
3. Create the cloud-init file.
4. Create the VM in ESXi or KVM.
5. Boot the Gateway VM and ensure the Gateway cloud-init initializes properly. At this stage, the Gateway should already activate itself against the Orchestrator.
6. Verify connectivity and deactivate cloud-init.

Important: Gateway supports both the virtual switch and SR-IOV. This guide specifies the SR-IOV as an optional configuration step.

18.3.1 Pre-Installation Considerations

The Arista Partner Gateway provides different configuration options. A worksheet should be prepared before the installation of the Gateway.

Worksheet

Table 51: Worksheet Table

Gateway	• Version • OVA/QCOW2 file location • Activation Key • Orchestrator (IP ADDRESS/vco-fqdn-hostname) • Hostname
Hypervisor	Address/Cluster name
Storage	Root volume datastore (>40GB recommended)
CPU Allocation	CPU Allocation for KVM/Arista.
Installation Selections	DPDK—This is optional and enabled by default for higher throughput. If you choose to deactivate DPDK, contact Arista Customer Support.
OAM Network	• DHCP • OAM IPv4 Address • OAM IPv4 Netmask • DNS server- primary • DNS server- secondary • Static Routes
ETH0 – Internet Facing Network	• IPv4 Address • IPv4 Netmask • IPv4 Default gateway • DNS server- primary • DNS server- secondary
Handoff (ETH1)- Network	• MGMT VRF IPv4 Address • MGMT VRF IPv4 Netmask • MGMT VRF IPv4 Default gateway • DNS server- primary • DNS server- secondary • Handoff (QinQ (0x8100), QinQ (0x9100), none, 802.1Q, 802.1ad) • C-TAG • S-TAG

Console access	• Console_Password
	• SSH:
	  • Enabled (yes/no)
	  • SSH public key

NTP	• Public NTP:
	  • server 0.ubuntu.pool.ntp.org
	  • server 1.ubuntu.pool.ntp.org
	  • server 2.ubuntu.pool.ntp.org
	  • server 3.ubuntu.pool.ntp.org
	• Internal NTP server- 1
	• Internal NTP server- 2

Gateway Section

Most of the Gateway section is self-explanatory.

Table 52: Gateway

Gateway	• Version- Should be same or lower than Orchestrator • OVA/QCOW2 file location- Plan ahead the file location and disk allocation • Activation Key • Orchestrator (IP ADDRESS/vco-fqdn-hostname) • Hostname- Valid Linux Hostname “RFC 1123”

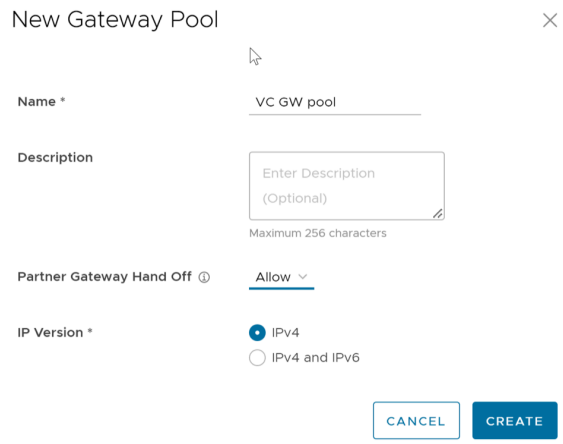
Creating a Gateway and Getting the Activation Key

To create a Gateway and get the activation key, perform the following steps:

1. In the **Operator** portal, select the **Gateway Management** tab and go to **Gateway Pools** in the left navigation pane. The **Gateway Pools** page appears. Create a new Gateway pool. For running Gateway in

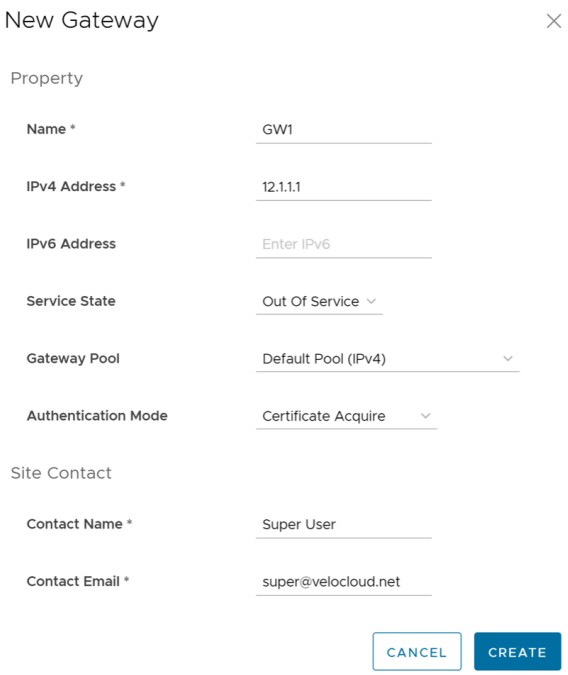
the Service Provider network, check the **Allow Partner Gateway** checkbox. This will enable the option to include the partner gateway in this gateway pool.

Figure 18-1: New Gateway Pool



2. In the **Operator** portal, select **Gateway Management** > **Gateways** and create a new gateway and assign it to the pool. The IP address of the gateway entered here must match the **public IP address** of the gateway. If unsure, you can run curl ipinfo.io/ip from the Gateway which will return the public IP of the Gateway.

Figure 18-2: New Gateway



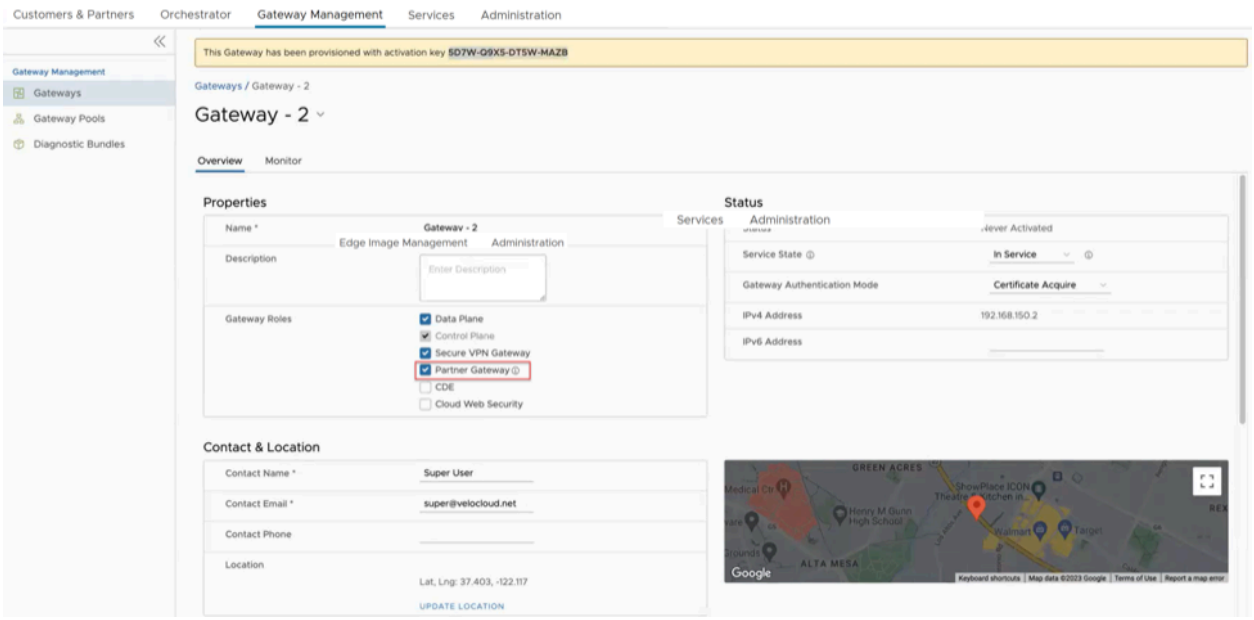
3. Make a note of the activation key and add it to the worksheet.

Activate Partner Gateway Mode

To activate partner Gateway mode, perform the following steps:

In the **Operator** portal, select **Gateway Management** > **Gateways** and select the Gateway. Check the **Partner Gateway** check box to activate the Partner Gateway.

Figure 18-3: Gateway 2



There are additional parameters that can be configured. The most common are the following:

a. Advertise `0.0.0.0/0` with no encrypt – This option will enable the Partner Gateway to advertise a path to Cloud traffic for the SAAS Application. Since the Encrypt Flag is off, it will be up to the customer configuration on the business policy to use this path or not.

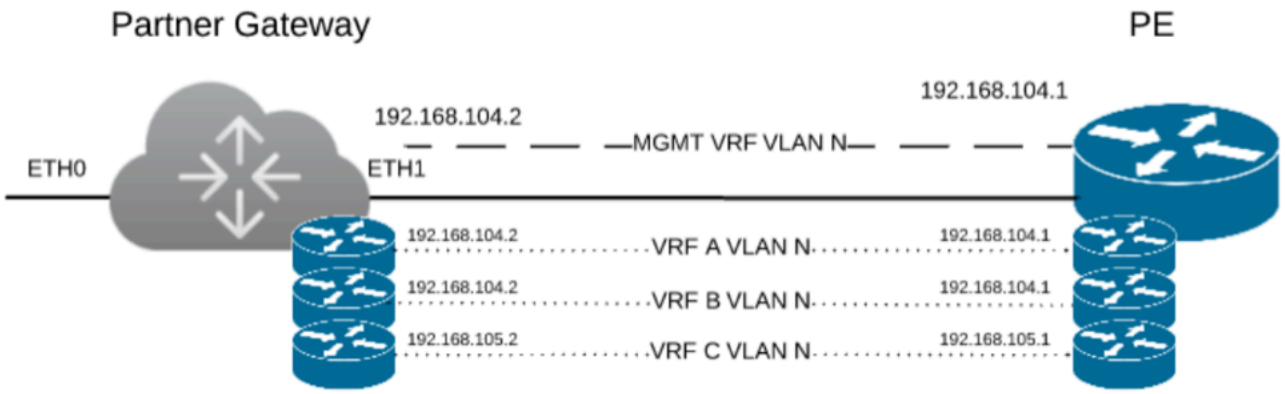
b. The second recommend option is to advertise the Orchestrator IP as a `/32` with encrypt.

c. This will force the traffic that is sent from the Edge to the Orchestrator to take the Gateway Path. This is recommended since it introduces predictability to the behavior that the Edge takes to reach the Orchestrator.

Networking

Important: The following procedure and screenshots focus on the most common deployment, which is the 2-ARM installation for the Gateway. The addition of an OAM network is considered in the section titled, OAM Interface and Static Routes.

Figure 18-4: Partner Gateway



The diagram above is a representation of the Gateway in a 2-ARM deployment. In this example, we assume eth0 is the interface facing the public network (Internet) and eth1 is the interface facing the internal network (handoff or VRF interface).

Note: A Management VRF is created on the Gateway and is used to send a periodic ARP refresh to the default gateway IP to check that the handoff interface is physically up and speed ups the failover time. It is recommended that a dedicated VRF is set up on the PE router for this purpose. Optionally, the same management VRF can also be used by the PE router to send an IP SLA probe to the Gateway to check for Gateway status (Gateway has a stateful ICMP responder that will respond to ping only when its service is up).If a dedicated Management VRF is not set up, then you can use one of the customer VRFs as a Management VRF, although this is not recommended.

For the Internet Facing network, you only need the basic network configuration.

Table 53: Internet Facing Network

ETH0 – Internet Facing Network	• IPv4_Address • IPv4_Netmask • IPv4_Default_gateway • DNS_server_primary • DNS_server_secondary

For the Handoff interface, you must know which type of handoff you want to configure and the Handoff configuration for the Management VRF.

Table 54: Handoff Configuration

ETH1 – HANDOFF Network	• MGMT_IPv4_Address • MGMT_IPv4_Netmask • MGMT_IPv4_Default gateway • DNS_Server_Primary • DNS_Server_Secondary • Handoff (QinQ (0x8100), QinQ (0x9100), none, 802.1Q, 802.1ad) • C_TAG_FOR_MGMT_VRF • S_TAG_FOR_MGMT_VRF

Console Access

Table 55: Console Access

Console access	• Console_Password
	• SSH:
	  • Enabled (yes/no)
	  • SSH public key

In order to access the Gateway, a console password and/or an SSH public key must be created.

Cloud-Init Creation

The configuration options for the gateway that we defined in the worksheet are used in the cloud-init configuration. The cloud-init config is composed of two main configuration files, the metadata file and the user-data file. The meta-data contains the network configuration for the Gateway, and the user-data contains the Gateway Software configuration. This file provides information that identifies the instance of the Gateway being installed.

Below are the templates for both meta_data and user_data files. Network-config can be omitted and network interfaces will be configured via DHCP by default.

Fill the templates with the information in the worksheet. All #_VARIABLE_# must be replaced, and check any #ACTION#

Important: The template assumes you are using static configuration for the interfaces. It also assumes that you are either using SR-IOV for all interfaces or none. For additional information, see OAM - SR-IOV with vmxnet3 or SR-IOV with VIRTIO.

meta-data file:

```
instance-id: #_Hostname_# local-hostname: #_Hostname_#
```

network-config file (leading spaces are important!)

Note: The network-config examples below describe configuring the virtual machine with two network interfaces, eth0 and eth1, with static IP addresses. eth0 is the primary interface with a default route and a metric of 1. eth1 is the secondary interface with a default route and a metric of 13. The system will be configured with password authentication for the default user (vcadmin). In addition, the SSH authorized key will be added for the vcadmin user. The SD-WAN Gateway will be automatically activated to the Orchestrator with the provided activation_code.

```
version: 2 ethernets: eth0: addresses: - #_IPv4_Address_/mask# gateway4: #_IPv4_Gateway_#
 nameservers: addresses: - #_DNS_server_primary_# - #_DNS_server_secondary_# search: [] routes:
 - to: 0.0.0.0/0 via: #_IPv4_Gateway_# metric: 1 eth1: addresses: - #_MGMT_IPv4_Address_/Mask#
 gateway4: 192.168.152.1 nameservers: addresses: - #_DNS_server_primary_# - #_DNS_server_
secondary_# search: [] routes: - to: 0.0.0.0/0 via: #_MGMT_IPv4_Gateway_# metric: 13
```

user-data file:

```
#cloud-config hostname: #_Hostname_# password: #_Console_Password_# chpasswd: {expire: False}
 ssh_pwauth: True ssh_authorized_keys: - #_SSH_public_Key_# velocloud: vcg: vco: #_VCO_#
 activation_code: #_Activation_Key# vco_ignore_cert_errors: false
```

The default username for the password that is configured in the user-data file is 'vcadmin'. Use this default username to login to the Gateway for the first time.

Important: Always validate user-data and metadata, using http://www.yamllint.com/ network-config should also be a valid network configuration (https://cloudinit.readthedocs.io/en/19.4/topics/network-config.html). Sometimes when working with the Windows/Mac copy paste feature, there is an issue of introducing Smart Quotes which can corrupt the files. Run the following command to make sure you are smart quote free.

```
sed s/[”“]/'"'/g /tmp/user-data > /tmp/user-data_new
```

Create ISO File

Once you have completed your files, they need to be packaged into an ISO image. This ISO image is used as a virtual configuration CD with the virtual machine. This ISO image, called vcg01-cidata.iso, is created with the following command on a Linux system:

```
genisoimage -output vcg01-cidata.iso -volid cidata -joliet -rock user-data meta-data network-confi
g
```

If you are on a MAC OSX, use the command below instead:

```
mkisofs -output vcg01-cidata.iso -volid cidata -joliet -rock {user-data,meta-data,network-config}
```

This ISO file which we will call #CLOUD_INIT_ISO_FILE# is going to be used in both OVA and Arista installations.

18.3.2 Install Gateway

You can install Gateway on Arista and KVM.

KVM provides multiple ways to provide networking to virtual machines. Arista recommends the following options:

- SR-IOV
- Linux Bridge
- OpenVSwitch Bridge

If you decide to use SR-IOV mode, enable SR-IOV on KVM and Arista. For steps, see:

- Activate SR-IOV on KVM
- Enable SR-IOV on Arista

To install Gateway:

- On KVM, see Install Gateway on KVM
- Install Gateway on Arista

18.3.2.1 Enable SR-IOV on Arista

Enabling SR-IOV on Arista is an optional configuration.

Prerequisites

This requires a specific NIC card. The following chipsets are certified by Arista to work with the Gateway.

- Intel 82599/82599ES
- Intel X710/XL710

Note: Before using the Intel X710/XL710 cards in SR-IOV mode on Arista, make sure the supported Firmware and Driver versions described in the *Deployment Prerequisites* section are installed correctly.

To enable SR-IOV on Arista, perform the following steps:

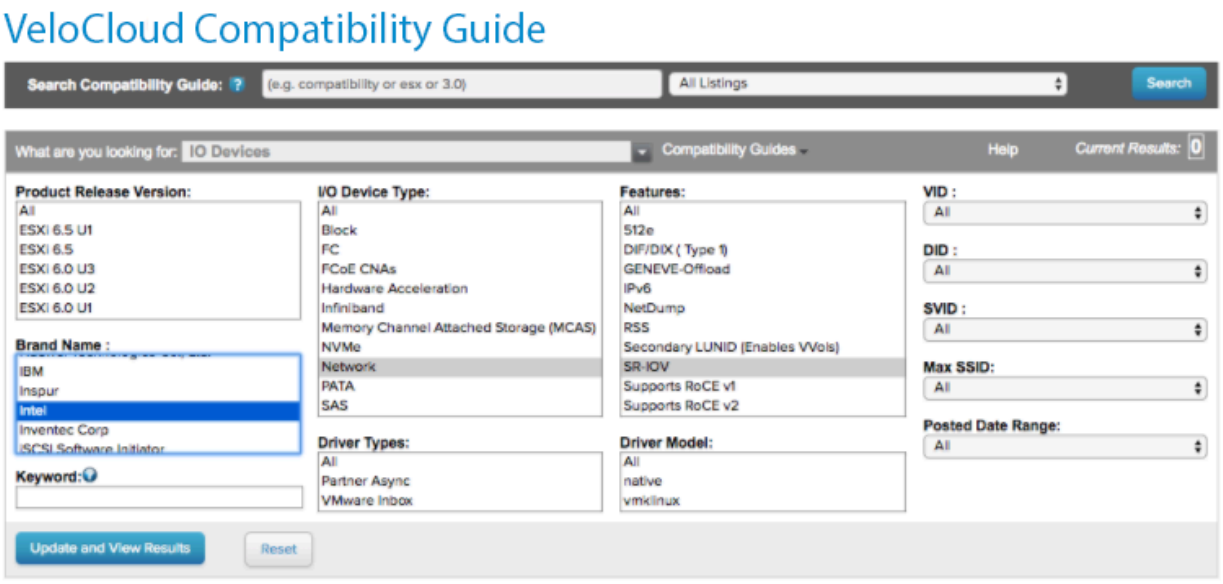
1. Make sure that your NIC card supports SR-IOV. Check the Arista Hardware Compatibility List (HCL)

   Brand Name: Intel

   I/O Device Type: Network

Features: SR-IOV

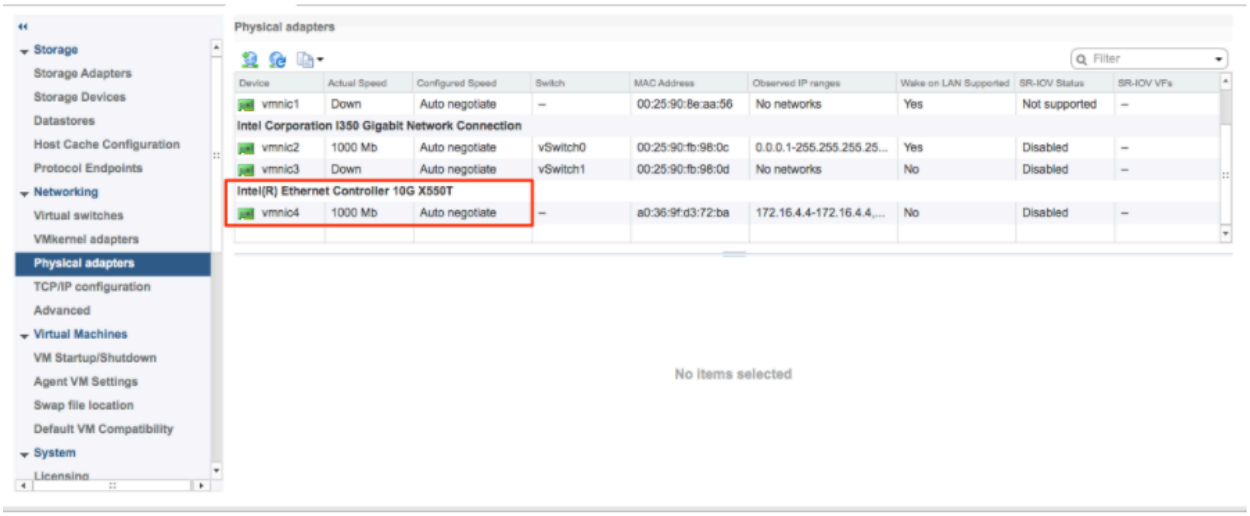
Figure 18-5: Arista Compatibility



Refer Arista KB article on details of how to enable SR-IOV on the supported NIC.

2. Once you have a support NIC card, go to the specific Arista host, select the **Configure** tab, and then choose **Physical adapters**

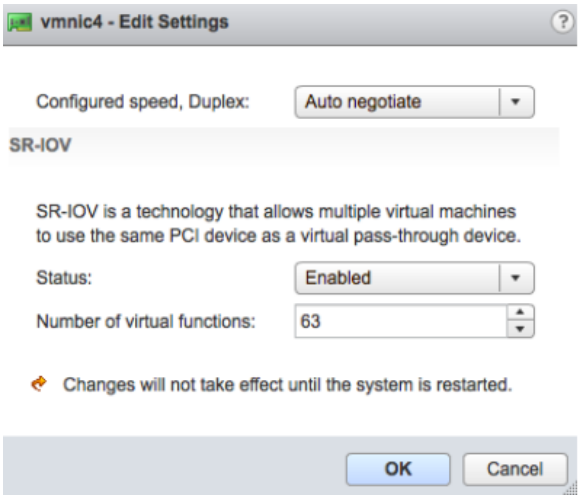
Figure 18-6: Physical Adapters



3. Select **Edit Settings**. Change **Status** to **Enabled** and specify the number of virtual functions required. This number varies by the type of NIC card.

4. Reboot the hypervisor.

Figure 18-7: Edit Settings



5. If SR-IOV is successfully enabled, the number of Virtual Functions (VFs) will show under the particular NIC after ESXi reboots.

Figure 18-8: Adapters

Note: To support VLAN tagging on SR-IOV interfaces, user must configure VLAN ID 4095 (Allow All) on the Port Group connected to the SR-IOV interface. For additional information, see *VLAN Configuration*.

18.3.2.2 Install Gateway on Arista

Describes how to install the Gateway OVA on Arista.

Note: This deployment is tested on ESXi versions 6.7, 6.7U3, 7.0, 7.0U3 and 8.0.1.

Important: When you are done with the OVA installation, do not start the VM until you have the cloud-init iso file and mount as CD-ROM to the Gateway VM. Otherwise, you will need to re-deploy the VM again.

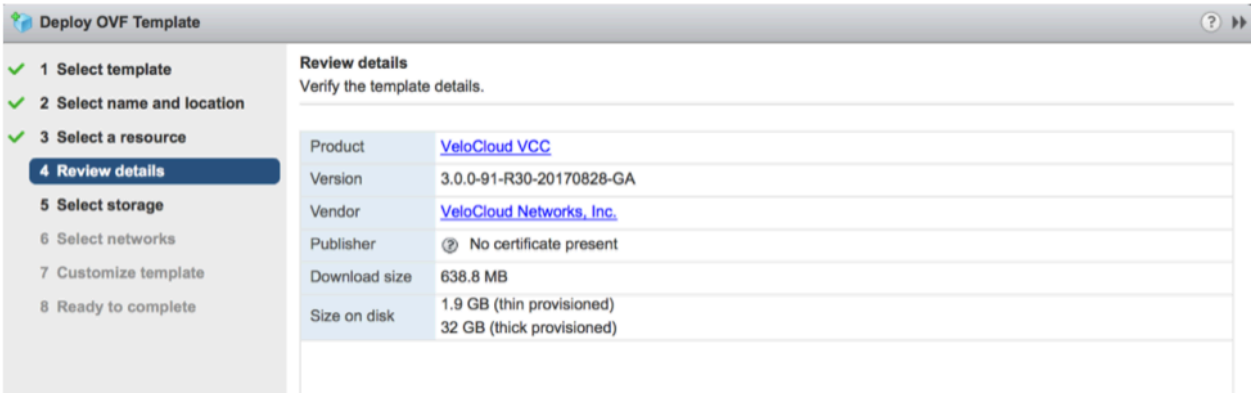
If you decide to use SR-IOV mode, then you can optionally enable SR-IOV on Arista. To enable the SR-IOV on Arista, see Enable SR-IOV on Arista.

To install the Gateway OVA, perform the following steps:

1. Select the **ESXi host**, go to **Actions**, and then **Deploy OVF Template**. Select the Gateway OVA file provided by Arista and select **Next**.

   Review the template details in **Step 4** (**Review details**) of the **Deploy OVA/OVF Template** wizard as shown in the following image.

Figure 18-9: Deploy OVF Template

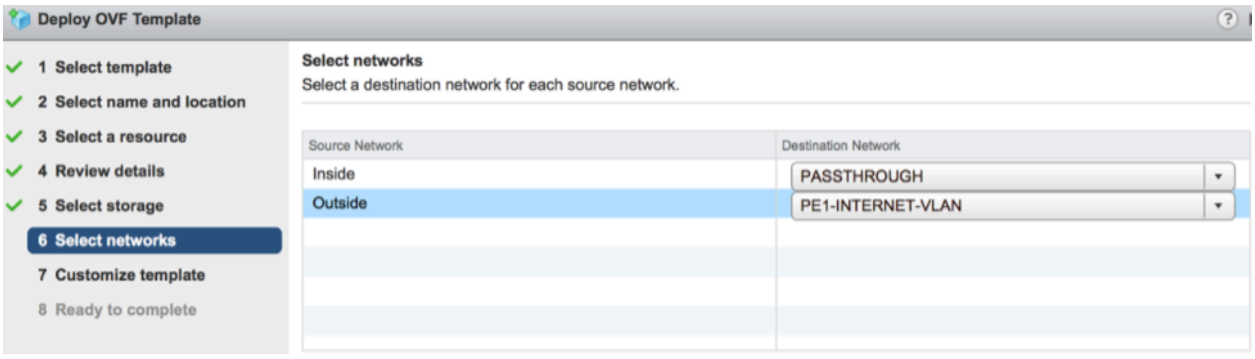


2. For the Select networks step, the OVA comes with two pre-defined networks (vNICs).

Table 56: Networks

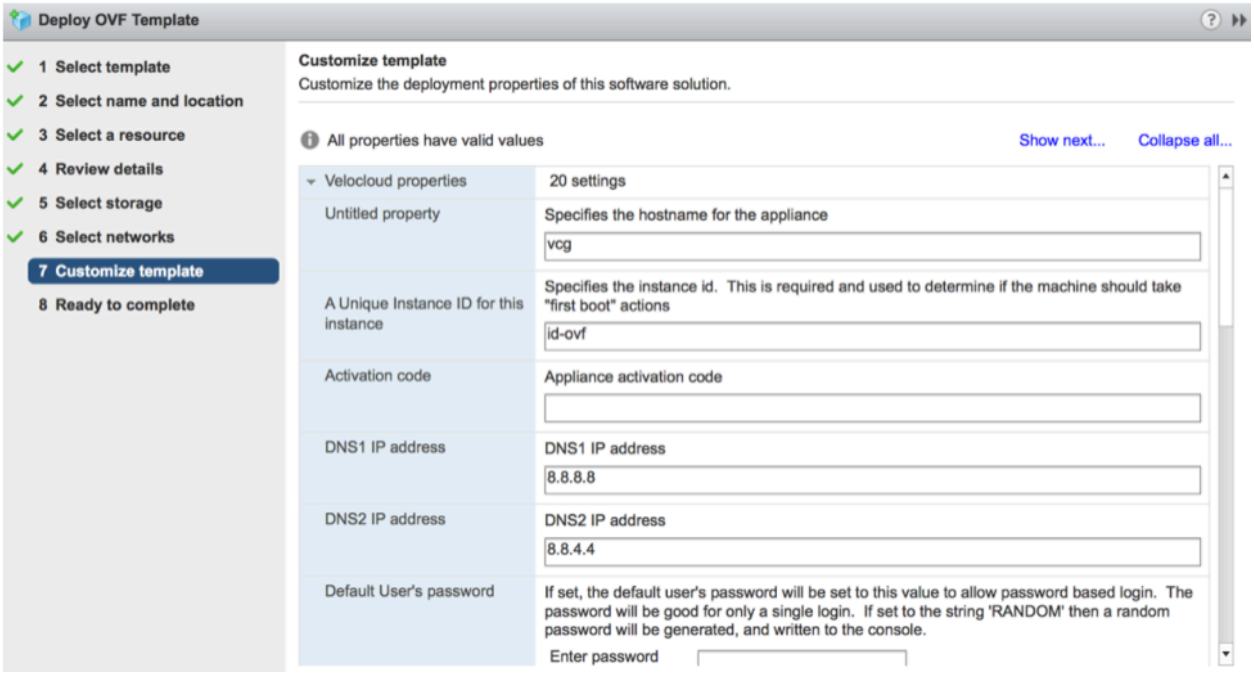
vNIC	Description
Inside	This is the vNIC facing the PE router and is used for handoff traffic to the MPLS PE or L3 switch. This vNIC is normally bound to a port group that does a VLAN pass-through (VLAN=4095 in vswitch configuration).
Outside	This is the vNIC facing the Internet. This vNIC expects a non-tagged L2 frame and is normally bound to a different port group from the Inside vNIC.

Figure 18-10: Deploy OVF Template



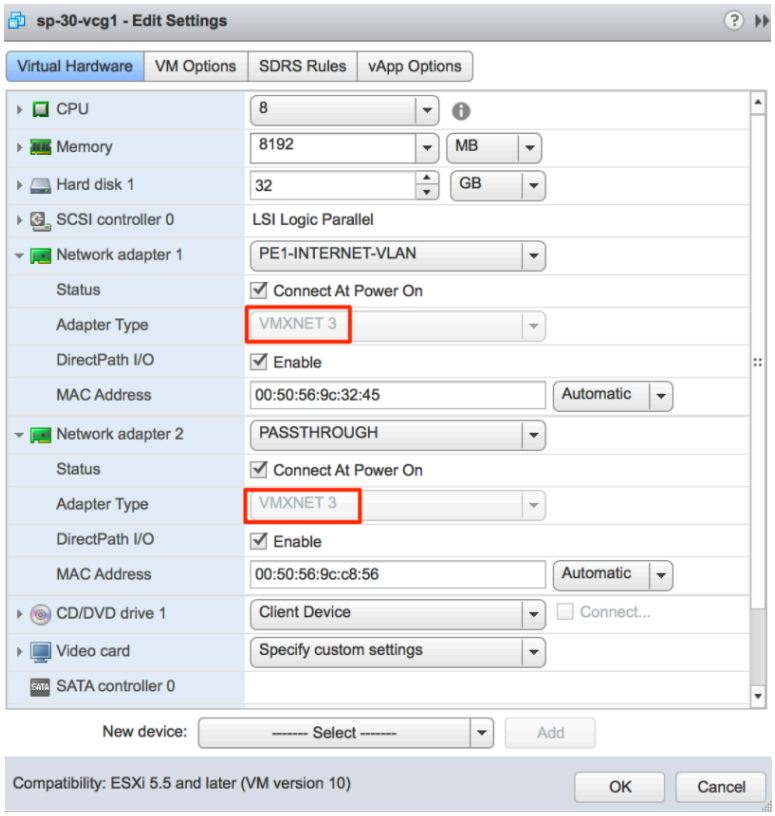
3. For the Customize template step, do not change anything. This is when you use vApp to configure the VM. We will not use vApp in this example. Select **Next** to continue with deploying the OVA.

Figure 18-11: Customize Templates



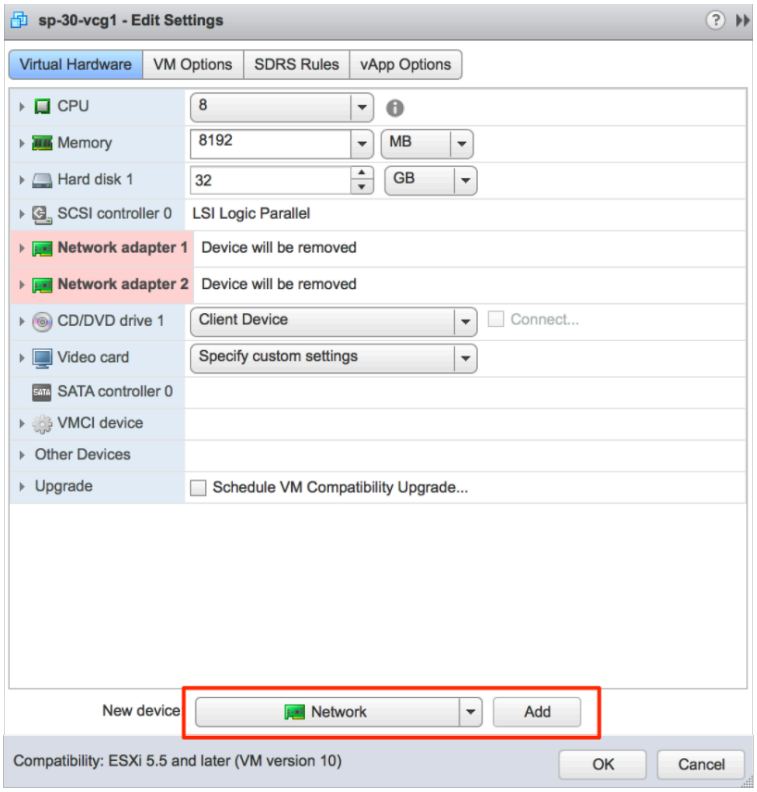
4. Once the VM is successfully deployed, return to the VM and select **Edit Settings**. Two vNICs are created with adapter type = vmxnet3.

Figure 18-12: Edit Settings



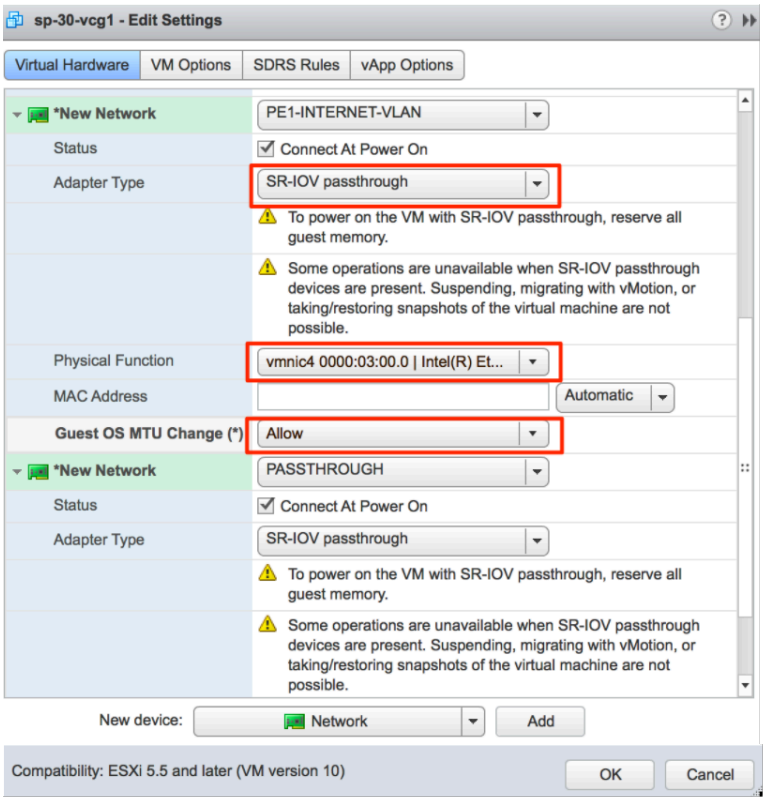
5. (Optional for SR-IOV) This step is required only if you plan to use SR-IOV. Because the OVA by default creates the two vNICs as ***vmxnet3***, we will need to remove the two vNICs and re-add them as SR-IOV.

Figure 18-13: SR-IOV



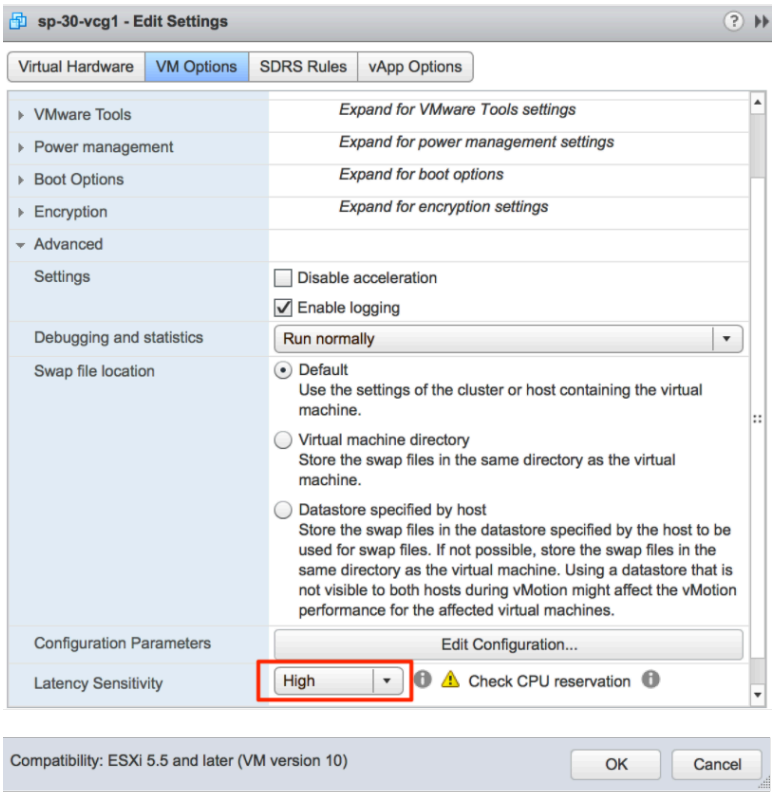
When adding the two new SR-IOV vNICs, use the same port group as the original two ***vmxnet3*** vNICs. Make sure the Adapter Type is SR-IOV passthrough. Select the correct physical port to use and set the **Guest OS MTU Change** to **Allow**. After you add the two vNICs, select **OK**.

Figure 18-14: Adapter and Port



6. As Gateway is a real-time application, you need to configure the **Latency Sensitivity** to **High**

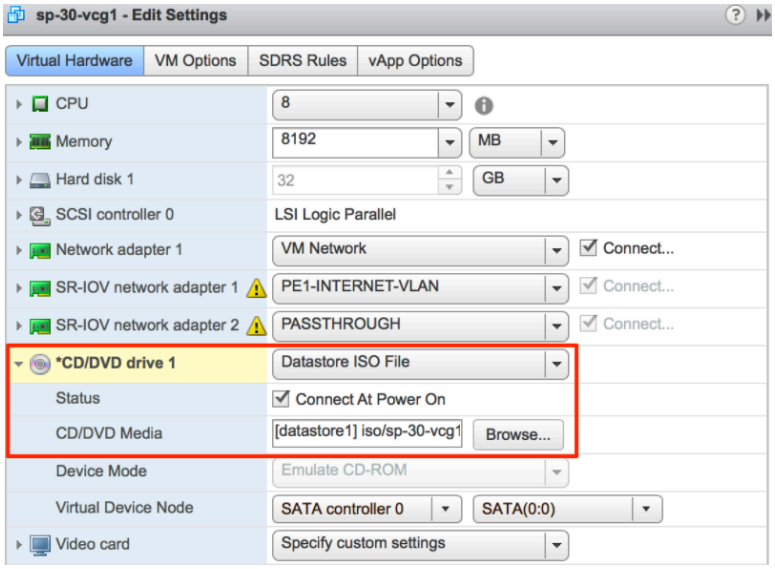
Figure 18-15: Latency Sensitivity



7. Refer to *Cloud-init Creation*. The Cloud-init file is packaged as a CD-ROM (iso) file. You need to mount this file as a CD-ROM.

> **Note:** You must upload this file to the datastore.

Figure 18-16: CD/DVD Status



8. Start the VM.

18.3.2.3 Activate SR-IOV on KVM

To enable the SR-IOV mode on KVM, perform the following steps.

Prerequisites

This requires a specific NIC card. The following chipsets are certified by Arista to work with the Gateway and Edge.

- Intel 82599/82599ES
- Intel X710/XL710

Note:

- Before using the Intel X710/XL710 cards in SR-IOV mode on KVM, make sure the supported Firmware and Driver versions specified in the *Deployment Prerequisites* section are installed correctly.
- SR-IOV mode is not supported if the KVM Virtual Edge is deployed with a High-Availability topology. For High-Availability deployments, ensure that SR-IOV is not enabled for that KVM Edge pair.

To enable SR-IOV on KVM, perform the following steps:

1. Enable SR-IOV in BIOS. This will be dependent on your BIOS. Login to the BIOS console and look for SR-IOV Support/DMA. You can verify support on the prompt by checking that Intel has the correct CPU flag.

```
cat /proc/cpuinfo | grep vmx
```

2. Add the options on Bboot (in /etc/default/grub).

```
GRUB_CMDLINE_LINUX="intel_iommu=on"
```

   a. Run the following commands: **`update-grub`** and **`update-initramfs -u`**.

   b. Reboot

   c. Make sure iommu is enabled.

```
velocloud@KVMperf3:~$ dmesg | grep -i IOMMU [ 0.000000] Command line: BOOT_IMAGE=/v
mlinuz-3.13.0-107-generic root=/dev/mapper/qa--multiboot--002--vg-root ro intel_iommu=o
n splash quiet vt.handoff=7 [ 0.000000] Kernel command line: BOOT_IMAGE=/vmlinuz-3.13.0
-107-generic root=/dev/mapper/qa--multiboot--002--vg-root ro intel_iommu=on splash quiet
 vt.handoff=7 [ 0.000000] Intel-IOMMU: enabled …. velocloud@KVMperf3:~$
```

3. Based on the NIC chipset used, add a driver as follows:
   For the Intel 82599/82599ES cards in SR-IOV mode:

   a. Download and install **ixgbe** driver from the Intel website.

   b. Configure ixgbe config (tar and sudo make install).

```
velocloud@KVMperf1:~$ cat /etc/modprobe.d/ixgbe.conf
```

c. If the ixgbe config file does not exist, you must create the file as follows.

```
options ixgbe max_vfs=32,32 options ixgbe allow_unsupported_sfp=1 options ixgbe MDD=0,0
 blacklist ixgbevf
```

d. Run the **`update-initramfs -u`** command and reboot the Server.

e. Use the **`modinfo`** command to verify if the installation is successful.

```
velocloud@KVMperf1:~$ modinfo ixgbe and ip link filename: /lib/modules/4.4.0-62-generic/
updates/drivers/net/ethernet/intel/ixgbe/ixgbe.ko version: 5.0.4 license: GPL description:
 Intel(R) 10GbE PCI Express Linux Network Driver author: Intel Corporation, <linux.nics@i
ntel.com> srcversion: BA7E024DFE57A92C4F1DC93
```

For the Intel X710/XL710 cards in SR-IOV mode:

f. Download and install the i40e driver from the Intel website.

g. Create the Virtual Functions (VFs).

```
echo 4 > /sys/class/net/device name/device/sriov_numvfs
```

h. To make the VFs persistent after a reboot, add the command from the previous step to the "`/etc/rc.d/rc.local`" file.

i. To make the VFs persistent after a reboot, add the command from the previous step to the "`/etc/rc.d/rc.local`" file.

j. Deactivate the VF driver.

```
echo “blacklist i40evf” >> /etc/modprobe.d/blacklist.conf
```

k. Run the **`update-initramfs -u`** command and reboot the Server.

Validating SR-IOV (Optional)

You can quickly verify if your host machine has SR-IOV enabled by using the following command:

```
lspci | grep -i Ethernet
```

Verify if you have Virtual Functions:

```
01:10.0 Ethernet controller: Intel Corporation 82599 Ethernet Controller Virtual Function(rev 01)
```

18.3.2.4 Install Gateway on KVM

Describes how to install the Gateway qcow on KVM.

> **Note:** This deployment is tested on KVM Ubuntu 16.04 and 18.04.

Pre-Installation Considerations

KVM provides multiple ways to provide networking to virtual machines. The networking in libvirt should be provisioned before the VM configuration. There are multiple ways to configure networking in KVM. For a full configuration of options on how to configure Networks on libvirt, see the following link:

https://libvirt.org/formatnetwork.html

From the full list of options, VMware recommends the following modes:

- SR-IOV (This mode is required for the Gateway to deliver the maximum throughput specified by VMware)
- OpenVSwitch Bridge

If you decide to use SR-IOV mode, enable SR-IOV on KVM. To enable the SR-IOV on KVM, see Activate SR-IOV on KVM.

To install the Gateway on KVM, perform the following steps:

1. Copy the QCOW and the Cloud-init files created in the **Cloud-Init Creation** section to a new empty directory.
2. Create the Network interfaces that you are going to use for the device.

   Using SR-IOV: The following is a sample network interface template specific to Intel X710/XL710 NIC cards using SR-IOV.

```
<interface type='hostdev' managed='yes'> <mac address='52:54:00:79:19:3d'/> <driver
 name='vfio'/> <source> <address type='pci' domain='0x0000' bus='0x83' slot='0x0a'
 function='0x0'/> </source> <model type='virtio'/> </interface>
```

   Using OpenVSwitch: The following are the sample templates of a network interface using OpenVSwitch.

```
git ./vcg/templates/KVM_NETWORKING_SAMPLES/template_outside_openvswitch.xml
```

```
<?xml version="1.0" encoding="UTF-8"?> <network> <name>public_interface</name> <!--This is
 the network name--> <model type="virtio" /> <forward mode="bridge" /> <bridge name="publici
nterface" /> <virtualport type="openvswitch" /> <vlan trunk="yes"> <tag id="50" /> <!--Define
 all the VLANS for this Bridge --> <tag id="51" /> <!--Define all the VLANS for this Bridge -->
 </vlan> </network>
```

   Create a network for inside_interface:

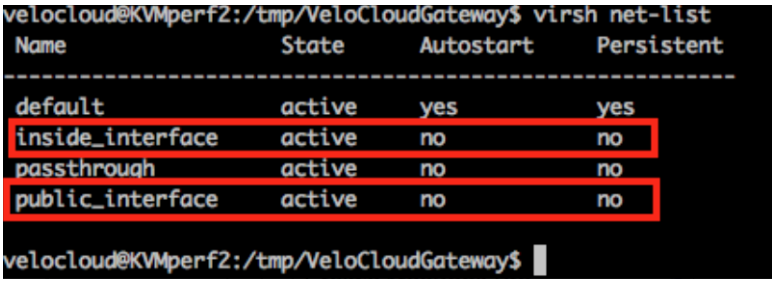
```
git ./vcg/templates/KVM_NETWORKING_SAMPLES/template_inside_openvswitch.xml
```

```
<network> <name>inside_interface</name> <!--This is the network name--> <model type='virtio'/>
 <forward mode="bridge"/> <bridge name="insideinterface"/> <virtualport type='openvswitch'></
virtualport> <vlan trunk='yes'></vlan> <tag id='200'/> <!—Define all the VLANS for this Bridge
 --> <tag id='201'/> <!—Define all the VLANS for this Bridge --> <tag id='202'/> <!—Define all
 the VLANS for this Bridge --> </network>
```

   If you are using OpenVSwitch mode, then you have to verify if the basic networks are created and active before launching the VM.

Note: This validation step is not applicable for SR-IOV mode as you do not create any network before the VM is launched.

Figure 18-17: Status



3. Edit the VM XML file. There are multiple ways to create a Virtual Machine in KVM. You can define the VM in an XML file and create it using libvirt, using the sample VM XML template specific to OpenVSwitch mode and SR-IOV mode.

```
vi my_vm.xml
```

The following is a sample template of a VM which uses OpenVSwitch interfaces. Use this template by making edits, wherever applicable.

```
<?xml version="1.0" encoding="UTF-8"?> <domain type="kvm"> <name>#domain_name#</name> <memory
 unit="KiB">8388608</memory> <currentMemory unit="KiB">8388608</currentMemory> <vcpu>8</
vcpu> <cputune> <vcpupin vcpu="0" cpuset="0" /> <vcpupin vcpu="1" cpuset="1" /> <vcpupin
 vcpu="2" cpuset="2" /> <vcpupin vcpu="3" cpuset="3" /> <vcpupin vcpu="4" cpuset="4" /
> <vcpupin vcpu="5" cpuset="5" /> <vcpupin vcpu="6" cpuset="6" /> <vcpupin vcpu="7"
 cpuset="7" /> </cputune> <resource> <partition>/machine</partition> </resource> <os>
 <type>hvm</type> </os> <features> <acpi /> <apic /> <pae /> </features> <cpu mode="host-
passthrough" /> <clock offset="utc" /> <on_poweroff>destroy</on_poweroff> <on_reboot>re
start</on_reboot> <on_crash>restart</on_crash> <devices> <emulator>/usr/bin/kvm-spice</
emulator> <disk type="file" device="disk"> <driver name="qemu" type="qcow2" /> <source
 file="#folder#/#qcow_root#" /> <target dev="hda" bus="ide" /> <alias name="ide0-0-0" />
 <address type="drive" controller="0" bus="0" target="0" unit="0" /> </disk> <disk type="file"
 device="cdrom"> <driver name="qemu" type="raw" /> <source file="#folder#/#Cloud_ INIT_
 ISO#" /> <target dev="sdb" bus="sata" /> <readonly /> <alias name="sata1-0-0" /> <address
 type="drive" controller="1" bus="0" target="0" unit="0" /> </disk> <controller type="usb"
 index="0"> <alias name="usb0" /> <address type="pci" domain="0x0000" bus="0x00" slot="0x01"
 function="0x2" /> </controller> <controller type="pci" index="0" model="pci-root"> <alias
 name="pci.0" /> </controller> <controller type="ide" index="0"> <alias name="ide0" />
 <address type="pci" domain="0x0000" bus="0x00" slot="0x01" function="0x1" /> </controller>
 <interface type="network"> <source network="public_interface" /> <vlan> <tag id="#public_v
lan#" /> </vlan> <alias name="hostdev1" /> <address type="pci" domain="0x0000" bus="0x00"
 slot="0x11" function="0x0" /> </interface> <interface type="network"> <source network="insi
de_interface" /> <alias name="hostdev2" /> <address type="pci" domain="0x0000" bus="0x00"
 slot="0x12" function="0x0" /> </interface> <serial type="pty"> <source path="/dev/pts/3" />
 <target port="0" /> <alias name="serial0" /> </serial> <console type="pty" tty="/dev/pts/3">
 <source path="/dev/pts/3" /> <target type="serial" port="0" /> <alias name="serial0" /> </
console> <memballoon model="none" /> </devices> <seclabel type="none" /> </domain>
```

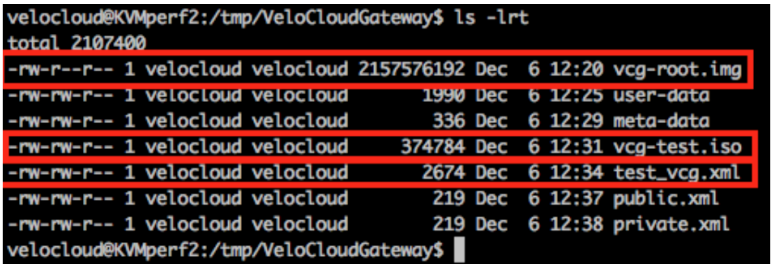
The following is a sample template of a VM which uses SR-IOV interfaces. Use this template by making edits, wherever applicable.

```
<?xml version="1.0" encoding="UTF-8"?> <domain type="kvm"> <name>#domain_name#</name> <memory
 unit="KiB">8388608</memory> <currentMemory unit="KiB">8388608</currentMemory> <vcpu>8</
vcpu> <cputune> <vcpupin vcpu="0" cpuset="0" /> <vcpupin vcpu="1" cpuset="1" /> <vcpupin
 vcpu="2" cpuset="2" /> <vcpupin vcpu="3" cpuset="3" /> <vcpupin vcpu="4" cpuset="4" /
> <vcpupin vcpu="5" cpuset="5" /> <vcpupin vcpu="6" cpuset="6" /> <vcpupin vcpu="7"
 cpuset="7" /> </cputune> <resource> <partition>/machine</partition> </resource> <os>
 <type>hvm</type> </os> <features> <acpi /> <apic /> <pae /> </features> <cpu mode="host-
passthrough" /> <clock offset="utc" /> <on_poweroff>destroy</on_poweroff> <on_reboot>re
start</on_reboot> <on_crash>restart</on_crash> <devices> <emulator>/usr/bin/kvm-spice</
emulator> <disk type="file" device="disk"> <driver name="qemu" type="qcow2" /> <source
```

```
 file="#folder#/#qcow_root#" /> <target dev="hda" bus="ide" /> <alias name="ide0-0-0" />
 <address type="drive" controller="0" bus="0" target="0" unit="0" /> </disk> <disk type="file"
 device="cdrom"> <driver name="qemu" type="raw" /> <source file="#folder#/#Cloud_ INIT_
 ISO#" /> <target dev="sdb" bus="sata" /> <readonly /> <alias name="sata1-0-0" /> <address
 type="drive" controller="1" bus="0" target="0" unit="0" /> </disk> <controller type="usb"
 index="0"> <alias name="usb0" /> <address type="pci" domain="0x0000" bus="0x00" slot="0x01"
 function="0x2" /> </controller> <controller type="pci" index="0" model="pci-root"> <alias
 name="pci.0" /> </controller> <controller type="ide" index="0"> <alias name="ide0" /> <address
 type="pci" domain="0x0000" bus="0x00" slot="0x01" function="0x1" /> </controller> <interface
 type='hostdev' managed='yes'> <mac address='52:54:00:79:19:3d'/> <driver name='vfio'/>
 <source> <address type='pci' domain='0x0000' bus='0x83' slot='0x0a' function='0x0'/> </
source> <model type='virtio'/> </interface> <interface type='hostdev' managed='yes'> <mac
 address='52:54:00:74:69:4d'/> <driver name='vfio'/> <source> <address type='pci' domain='0x000
0' bus='0x83' slot='0x0a' function='0x1'/> </source> <model type='virtio'/> </interface>
 <serial type="pty"> <source path="/dev/pts/3" /> <target port="0" /> <alias name="serial0
" /> </serial> <console type="pty" tty="/dev/pts/3"> <source path="/dev/pts/3" /> <target
 type="serial" port="0" /> <alias name="serial0" /> </console> <memballoon model="none" /> </
devices> <seclabel type="none" /> </domain>
```

4. Launch the VM by performing the following steps:
   a. Ensure you have the following three files in your directory as shown in the following sample screenshot:
      - qcow file - vcg-root
      - cloud-init - vcg-test.iso
      - Domain XML file that defines the VM - test_vcg.xml, where test_vcg is the domain name.)

      Figure 18-18: List of Files



   b. Define VM.

```
velocloud@KVMperf2:/tmp/VeloCloudGateway$ virsh define test_vcg.xml Domain test_vcg defined
 from test_vcg.xml
```

   c. Set VM to autostart.

```
velocloud@KVMperf2:/tmp/VeloCloudGateway$ virsh autostart test_vcg
```

   d. Start VM.

```
velocloud@KVMperf2:/tmp/VeloCloudGateway$ virsh start test_vcg
```

5. If you are using SR-IOV mode, after launching the VM, set the following on the Virtual Functions (VFs) used:
   a. Set the spoofcheck off.

```
ip link set eth1 vf 0 spoofchk off
```

   b. Set the Trusted mode on.

```
ip link set dev eth1 vf 0 trust on
```

c. Set the VLAN, if required.

```
ip link set eth1 vf 0 vlan 3500
```

Note: The Virtual Functions configuration step is not applicable for OpenVSwitch (OVS) mode.

6. Console into the VM.

```
virsh list Id Name State ---------------------------------------------------- 25 test_vcg
 running velocloud@KVMperf2$ virsh console 25 Connected to domain test_vcg Escape character is
 ^]
```

Special Consideration for KVM Host

- Deactivate GRO (Generic Receive Offload) on physical interfaces (to avoid unnecessary re-fragmentation in Gateway).

```
ethtool -K <interface> gro off tx off
```

- Deactivate CPU C-states (power states affect real-time performance). Typically, this can be done as part of kernel boot options by appending processor.max_cstate=1 or just deactivate in the BIOS.
- For production deployment, vCPUs must be pinned to the instance. No oversubscription on the cores should be allowed to take place.

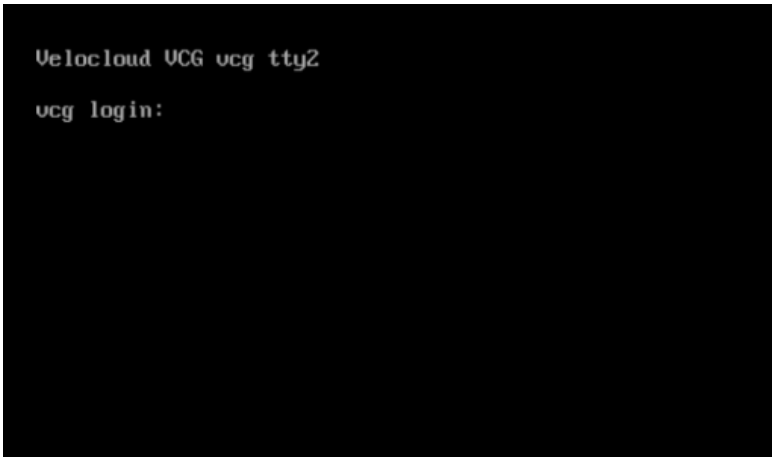
18.4 Post-Installation Tasks

This section discusses post-installation and installation verification steps.

If everything worked as expected in the installation, you can now login to the VM.

1. If everything works as expected, you should see the login prompt on the console. You should see the prompt name as specified in cloud-init.

   Figure 18-19: Login Prompt

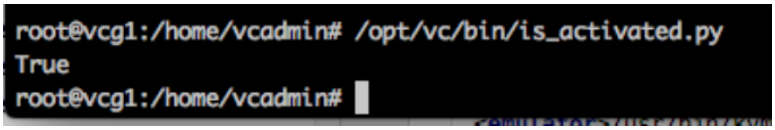


2. You can also refer to `/run/cloud-init/result.json`. If you see the message below, it is likely that the cloud init runs successfully.

   Figure 18-20: cloud init Successful Message

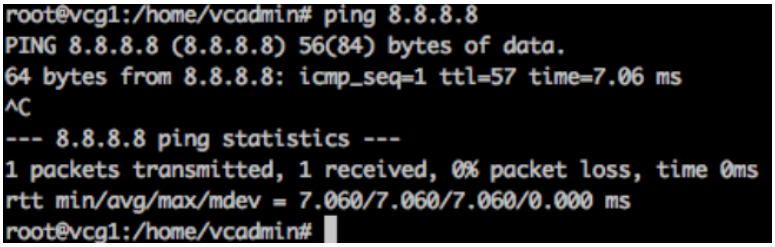
3. Verify that the Gateway is registered with Orchestrator.

   Figure 18-21: Verify Registered Gateway



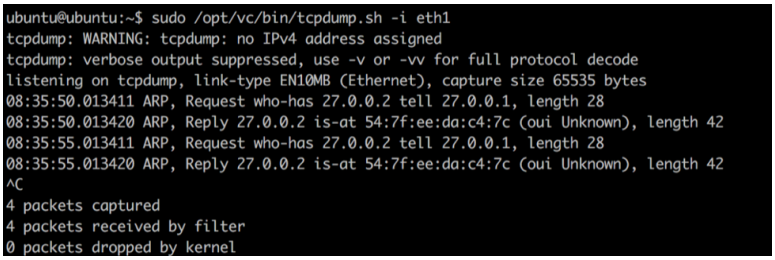
4. Verify Outside Connectivity.

Figure 18-22: Verify Outside Connectivity



5. Verify that the MGMT VRF is responding to ARPs.

Figure 18-23: Verify MGMT VRF



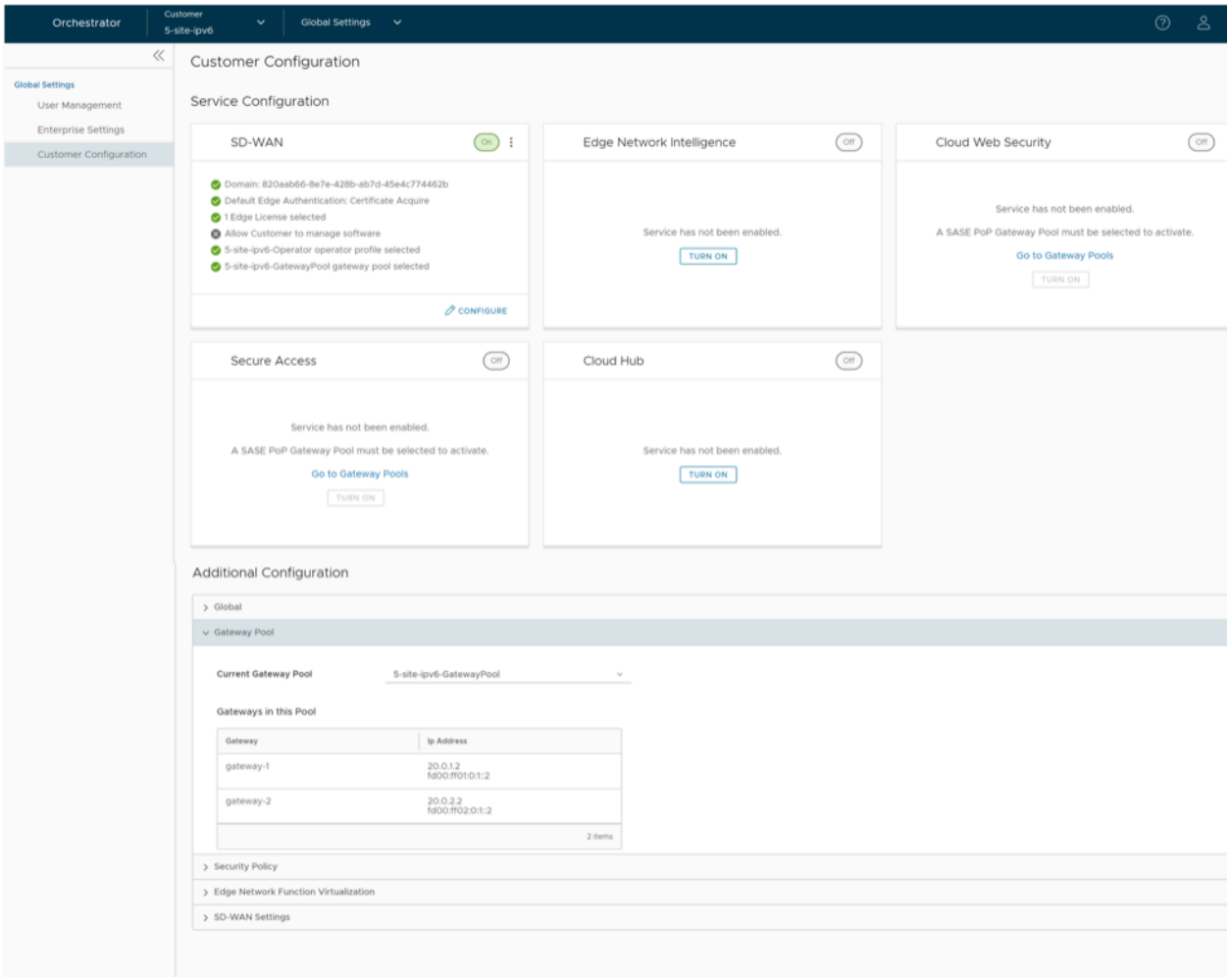
6. **Optional:** Deactivate cloud-init so it does not run on every boot.

> **Note:** If you have deployed OVA on VMware vSphere with vAPP properties, you must deactivate cloud-init prior to upgrading to versions 4.0.1 or 4.1.0. This is to ensure that the customization settings such as network configuration or password are not lost during the upgrade.

```
touch /etc/cloud/cloud-init.disabled
```

7. Associate the new gateway pool with the customer.

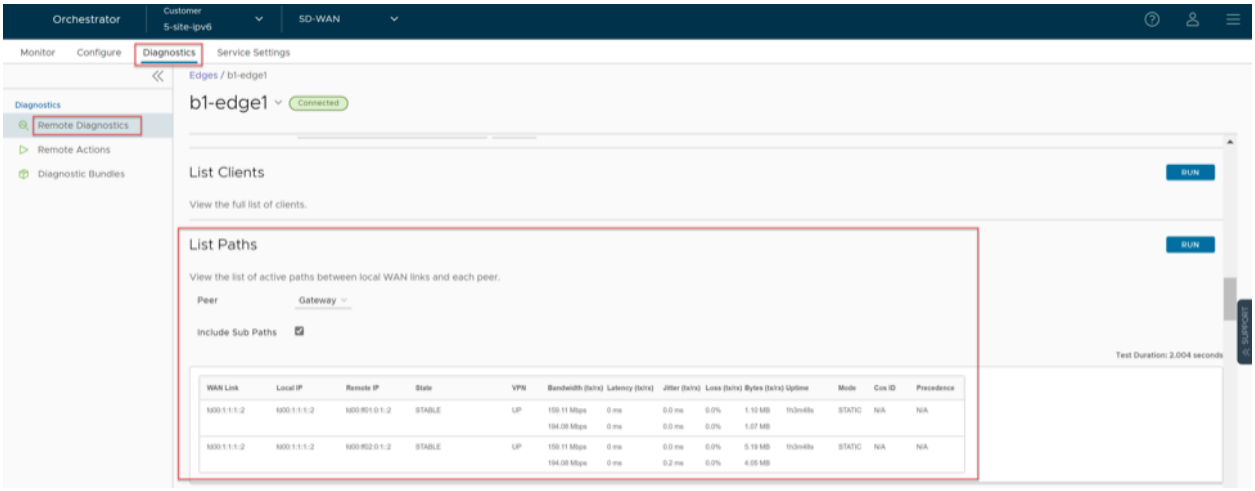
Figure 18-24: Associate Gateway Pool



8. Associate the Gateway with an Edge. For additional information, see the "Assign Partner Gateway Handoff " section in the *VeloCloud SD-WAN Administration Guide*.
9. Verify that the Edge is able to establish a tunnel with the Gateway on the Internet side. From the **Orchestrator**, go to **Monitor** > **Edges** > **[Edge]** > **Overview**.

From the **Orchestrator**, go to **Diagnostics** > **Remote Diagnostics** > **[Edge]** > **List Paths**, and select **Run** to view the list of active paths.

Figure 18-25: List of Active Paths



10. Configure the Handoff interface. See Configure Partner Handoff.
11. Verify that the BGP session is up.
12. Change the network configuration.

    Network configuration files are located under /etc/netplan.

    Example network configuration (whitespace is important!) - `/etc/netplan/50-cloud-init.yaml`:

```
network: version: 2 ethernets: eth0: addresses: - 192.168.151.253/24 gateway4: 192.168.151.1
 nameservers: addresses: - 8.8.8.8 - 8.8.4.4 search: [] routes: - to: 192.168.0.0/16 via:
 192.168.151.254 metric: 100 eth1: addresses: - 192.168.152.251/24 gateway4: 192.168.152.1
 nameservers: addresses: - 8.8.8.8 search: []
```

Important: When cloud-init is enabled, network configuration is regenerated on every boot. In order to make changes to location configuration, deactivate cloud-init or deactivate cloud-init network configuration component:

```
echo 'network: {config: disabled}' > /etc/cloud/cloud.cfg.d/99-disable-network-
config.cfg
```

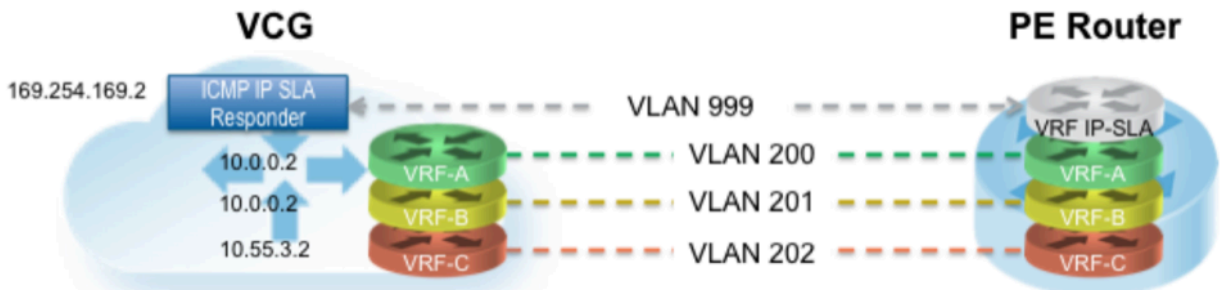
Configure Handoff Interface in Data Plane

VeloCloud Gateway Network Configuration

In the example featuring figure below (VRF/VLAN Hand Off to PE), we assume eth0 is the interface facing the public network (Internet) and eth1 is the interface facing the internal network (customer VRF through the PE).BGP peering configuration is managed on the VCO on a per customer/VRF basis under “Configure

> Customer". Note that the IP address of each VRF is configurable per customer. The IP address of the management VRF inherits the IP address configured on the SD-WAN Gateway interface in Linux.

Figure 18-26: VRF/VLAN Hand Off to PE Router



A management VRF is created on the SD-WAN Gateway and is used to send periodic ARP refresh to the default Gateway IP to determine the next-hop MAC. It is recommended that a dedicated VRF is set up on the PE router for this purpose. The same management VRF can also be used by the PE router to send IP SLA probe to the SD-WAN Gateway to check for SD-WAN Gateway status (SD-WAN Gateway has stateful ICMP responder that will respond to ping only when its service is up). BGP Peering is not required on the Management VRF. If a Management VRF is not set up, then you can use one of the customer VRFs as Management VRF, although this is not recommended.

1. Edit the `/etc/config/gatewayd` and specify the correct VCMP and WAN interface. VCMP interface is the public interface that terminates the overlay tunnels. The WAN interface in this context is the handoff interface facing the PE.

```
"vcmp.interfaces":[ "eth0" ], (..snip..) "wan": [ "eth1" ],
```

2. Configure the Management VRF. This VRF is used by the SD-WAN Gateway to ARP for next-hop MAC (PE router). The same next-hop MAC will be used by all the VRFs created by the SD-WAN Gateway. You need to configure the Management VRF parameter in `/etc/config/gatewayd`.

   The Management VRF is the same VRF used by the PE router to send IP SLA probe to. The SD-WAN Gateway only responds to the ICMP probe if the service is up and if there are edges connected to it. Below table explains each parameter that needs to be defined. This example has Management VRF on the 802.1q VLAN ID of 1000.

   Table 57: Management VRF Parameters to be Defined

mode	QinQ (0x8100), QinQ (0x9100), none, 802.1Q, 802.1ad
c_tag	C-Tag value for QinQ encapsulation or 802.1Q VLAN ID for802.1Q encapsulation
s_tag	S-Tag value for QinQ encapsulation
interface	Handoff interface, typically eth1

```
"vrf_vlan": { "tag_info": [ { "resp_mode": 0, "proxy_arp": 0, "c_tag": 1000, "mode": "802.1Q",
 "interface": "eth1", "s_tag": 0 } ] },
```

3. Edit the `/etc/config/gatewayd-tunnel` to include both interfaces in the wan parameter. Save the change.

   `wan="eth0 eth1"`

Remove Blocked Subnets

By default, the SD-WAN Gateway blocks traffic to 10.0.0.0/8 and 172.16.0.0/14. We will need to remove them before using this SD-WAN Gateway because we expect SD-WAN Gateway to be sending traffic to private subnets as well. If you do not edit this file, when you try to send traffic to blocked subnets, you will find the following messages in `/var/log/gwd.log`

```
2015-12-18T12:49:55.639 ERR [NET] proto_ip_recv_handler:494 Dropping packet destined for
 10.10.150.254, which is a blocked subnet. 2015-12-18T12:52:27.764 ERR [NET] proto_ip_recv
_handler:494 Dropping packet destined for 10.10.150.254, which is a blocked subnet. [message
 repeated 48 times] 2015-12-18T12:52:27.764 ERR [NET] proto_ip_recv_handler:494 Dropping packet
 destined for 10.10.150.10, which is a blocked subnet.
```

o

1. On SD-WAN Gateway, `edit /opt/vc/etc/vc_blocked_subnets.jsonfile`. You will find that this file first has the following.

   ```
   [ { "network_addr": "10.0.0.0", "subnet_mask": "255.0.0.0" }, { "network_addr": "172.16.0.0",
    "subnet_mask": "255.255.0.0" } ]
   ```

2. Remove the two networks. The file should look like below after editing. Save the change.

   ```
   [ ]
   ```

3. Restart the SD-WAN Gateway process by `sudo /opt/vc/bin/vc_procmon restart`.

18.5 Upgrade Gateway

This section describes how to upgrade a Gateway installation.

Important: This procedure will not work for upgrading a Gateway image version from 3.x to 4.x due to a significant platform changes. Upgrading from a 3.x to 4.x image will require a new Gateway deployment and reactivation. See Partner Gateway Upgrade and Migration for upgrade information.

Note: Currently, Arista does not support downgrading for the VeloCloud Orchestrator and VeloCloud Gateway. So before upgrading the Orchestrator or Gateway, Arista recommends you to back up the system prior to upgrade for easy recovery in the event the upgrade is not successfully completed.

Authenticate Software Update Package Via Digital Signature

The software installer in the Orchestrator version 4.3.0 and higher now has the ability to authenticate the software update package using a digital signature.

Prior to upgrading to a newer version of the software, make sure the public key exists to verify the package. The known public key location to verify signature is as follows, `/var/lib/velocloud/software_update/keys/software.key`. Alternatively, the key can be provided on the command line using--pubkey parameter.

The current release public key is:

```
-----BEGIN PUBLIC KEY----- MHYwEAYHKoZIzj0CAQYFK4EEACIDYgAEbjZ08w3RNJvuOICBp8fysU/3opLejsrP
 pArA1IyKeUzU0U31MU4kPcLdggojobNfs3i1kvyvGvprEmfGYWzc3dXUyT9Tv73C lVgYPLNd/nOxJsXomROKogfvJdYFuy4/
 -----END PUBLIC KEY----
```

If the key is missing or the signature cannot be verified, the Operator will be notified that the package is untrusted with an option to proceed or not proceed.

To skip verification, use "--untrusted" parameter.

If running in batch mode or not on the terminal, the installation is aborted unless the "--untrusted" option is specified on the command line.

By default, the installer will run in interactive mode and may issue prompts. For automated scripts, use --batch parameter to suppress prompts.

Upgrade Procedures

To upgrade a Gateway installation:

1. Download the Gateway update package.
2. Upload the image to the Gateway system (using, for example, the **`scp`** command). Copy the image to the following location on the system:

   `/var/lib/velocloud/software_update/vcg_update.tar`
3. Connect to the Gateway console and run:

```
sudo /opt/vc/bin/vcg_software_update
```

18.6 Activate Replacement Partner Gateway

Before you can use this Gateway replacement method, you must adjust the System Property **gateway.activation.validate.deviceID** and set the value to **false**. To do this you or another Operator with a Superuser role must go to **Orchestrator** > **System Properties** and search for **gateway.activation** and inspect **gateway.activation.validate.deviceID**. If the **Value** is already **false** as in the screenshot below, then you are ready for the next steps. If the **Value** is **true**, then a Gateway reactivation will not work, and you need to modify this System Property by selecting it.

Figure 18-27: System Properties

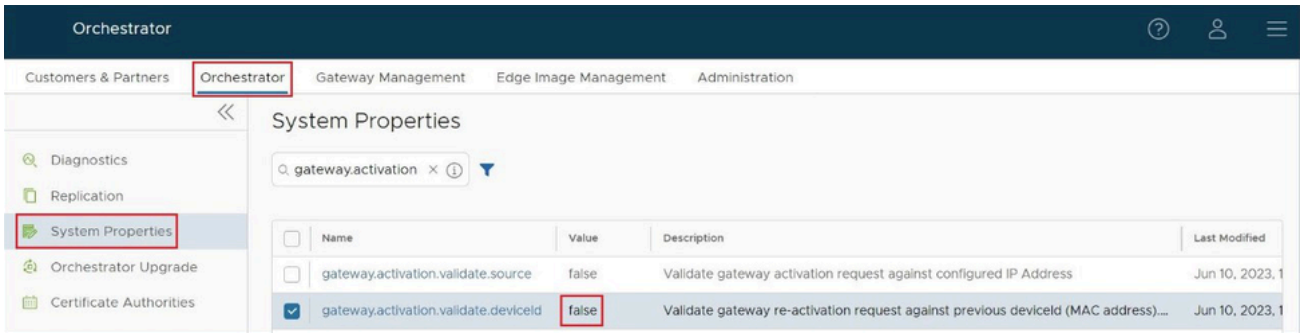
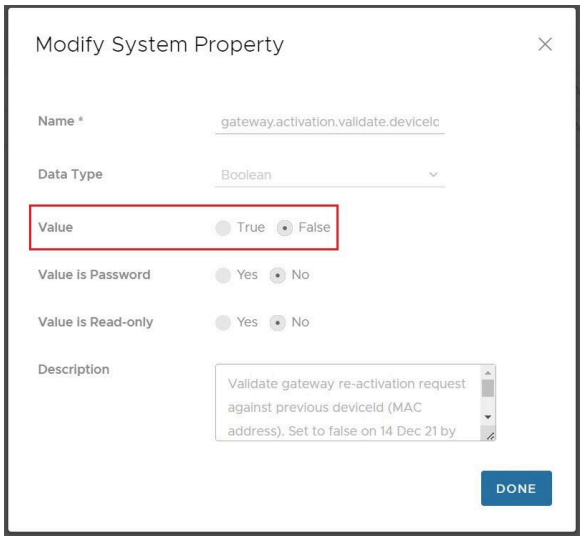


Figure 18-28: Modify System Property



You must be an Operator with a Superuser role to make this change. By default, the Orchestrator performs a **deviceID** verification, and with this System Property set to **true**, activating a replacement Gateway would fail because the **deviceID** would not be the same as the original Gateway. Setting this property to **false** disables the verification process on the Orchestrator.

Note: There are no adverse effects to changing this value. You may leave it as **false** since the Gateway authentication keys are indefinitely valid.

Important: If you are on a Hosted Shared Orchestrator and do not know whether the **gateway.activation.validate.deviceID** System Property is set to False and find that you cannot reactivate your Partner Gateway, you can reach out to VeloCloud SD-WAN Support and they will assist you in changing that System Property on your Orchestrator.

This section covers activating a replacement Partner Gateway.

Gateway activation keys do not have the same default 30 day lifetime as Edges. In fact, a Gateway activation key has an infinite lifespan. If an on-premises Gateway fails and you wish to replace it with a newly built Gateway using the same name and IP address, you can use the same activation key that was used on the original Gateway.

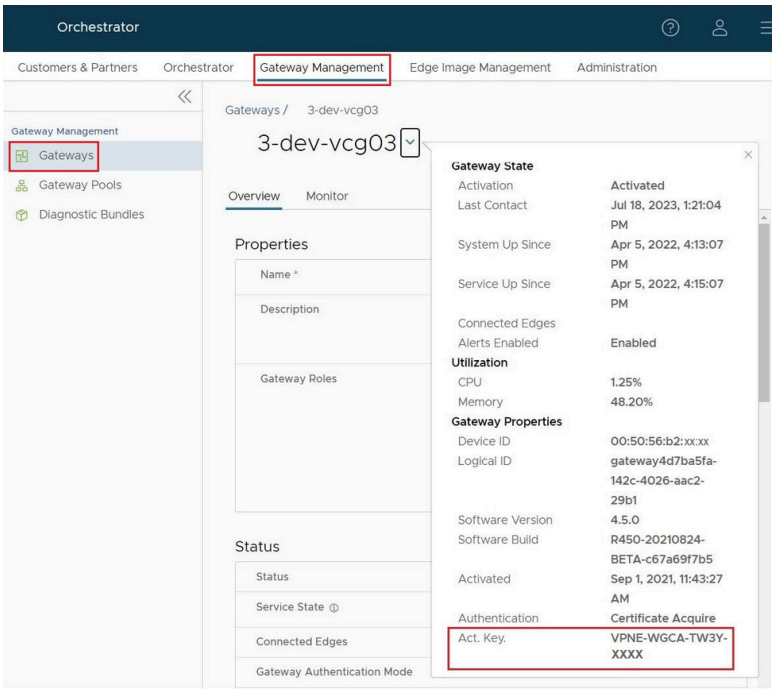
As a result, for most Gateway issues, the quickest method of recovery is to spin up a new VM and register it to the Orchestrator using the failed Gateway's activation key. This saves you a lot of time as the Orchestrator will push the existing configuration onto this new instance. Most Partners prefer this approach over configuring a new Gateway from scratch.

Replacement Partner Gateway Workflow

These are the steps to activate a replacement Partner Gateway:

1. Locate the original activation key. This key is found by going to **Gateway Management** > **Gateways** and selecting the name of the Gateway you are replacing. Select the down arrow beside the name and note the activation key.

   Figure 18-29: Gateway Management



2. Use the activation key to activate the replacement Gateway on your newly spun up VM: `/opt/vc/bin/activate.py -s vco_name_or_ip activation_key`.

18.7 Custom Configurations

This section describes custom configurations.

18.7.1 NTP Configuration

NTP configuration involves editing the `/etc/ntpd.conf` file.

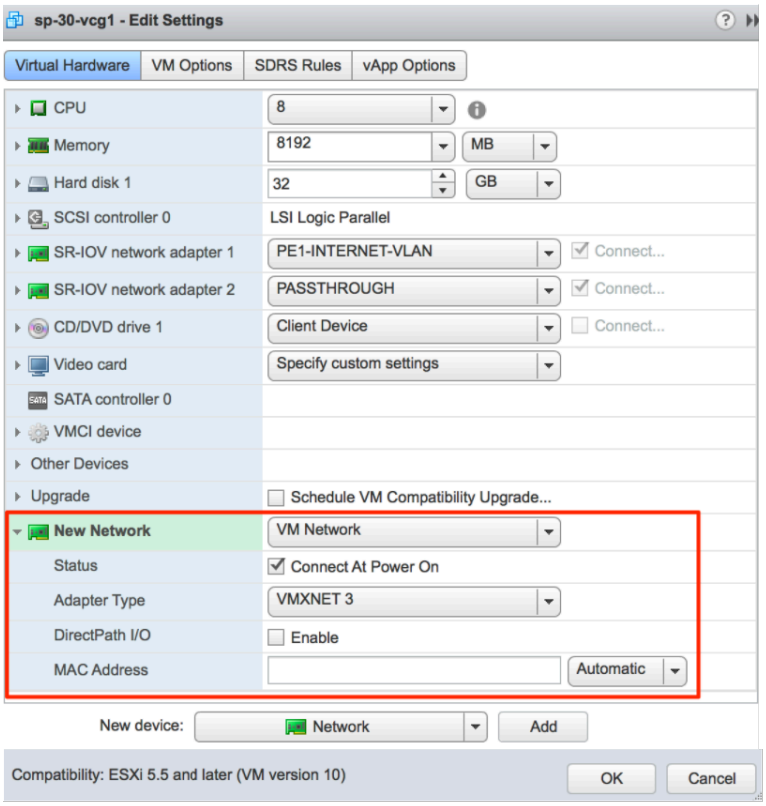
18.7.2 OAM Interface and Static Routes

If Gateways are to be deployed with an OAM interface, complete the following steps.

1. Add an additional interface to the VM (ETH2).

Arista: If a dedicated VNIC for Management/OAM is desired, add another vNIC of type ***vmxnet3***. You must repeat the previous step, which is to select **OK** and then **Edit Settings** again so you can make a note of the vNIC MAC address.

Figure 18-30: Edit Settings



KVM: If a dedicated VNIC for Management/OAM is desired, make sure you have a libvirt network named ***oam-network***. Then add the following lines to your XML VM structure:

```
….. </controller> <interface type='network'> <source network='public_interface'/> <vlan><tag
 id='#public_vlan#'/></vlan> <alias name='hostdev1'/> <address type='pci' domain='0x0000'
 bus='0x00' slot='0x11' function='0x0'/> </interface> <interface type='network'> <source
 network='inside_interface'/> <alias name='hostdev2'/> <address type='pci' domain='0x000
0' bus='0x00' slot='0x12' function='0x0'/> </interface> <interface type='network'> <source
 network='oam_interface'/> <vlan><tag id='#oam_vlan#'/></vlan> <alias name='hostdev2'/>
 <address type='pci' domain='0x0000' bus='0x00' slot='0x13' function='0x0'/> </interface>
 <serial type='pty'> <source path='/dev/pts/3'/> <target port='0'/> <alias name='serial0'/> </
serial>
```

2. Configure the network-config file with the additional interface.

```
version: 2 ethernets: eth0: addresses: - #_IPv4_Address_/mask# mac_address: #_mac_Address_#
 gateway4: #_IPv4_Gateway_# nameservers: addresses: - #_DNS_server_primary_# - #_DNS_server_
secondary_# search: [] routes: - to: 0.0.0.0/0 via: #_IPv4_Gateway_# metric: 1 eth1: addresses:
 - #_MGMT_IPv4_Address_/Mask# mac_address: #_MGMT_mac_Address_# nameservers: addresses: -
 #_DNS_server_primary_# - #_DNS_server_secondary_# search: [] routes: - to: 0.0.0.0/0 via:
 #_MGMT_IPv4_Gateway_# metric: 13 eth2: addresses: - #_OAM_IPv4_Address_/Mask# nameservers:
 addresses: - #_DNS_server_primary_# - #_DNS_server_secondary_# search: [] routes: - to:
 10.0.0.0/8 via: #_OAM_IPv4_Gateway_# - to: 192.168.0.0/16 via: #_OAM_IPv4_Gateway_#
```

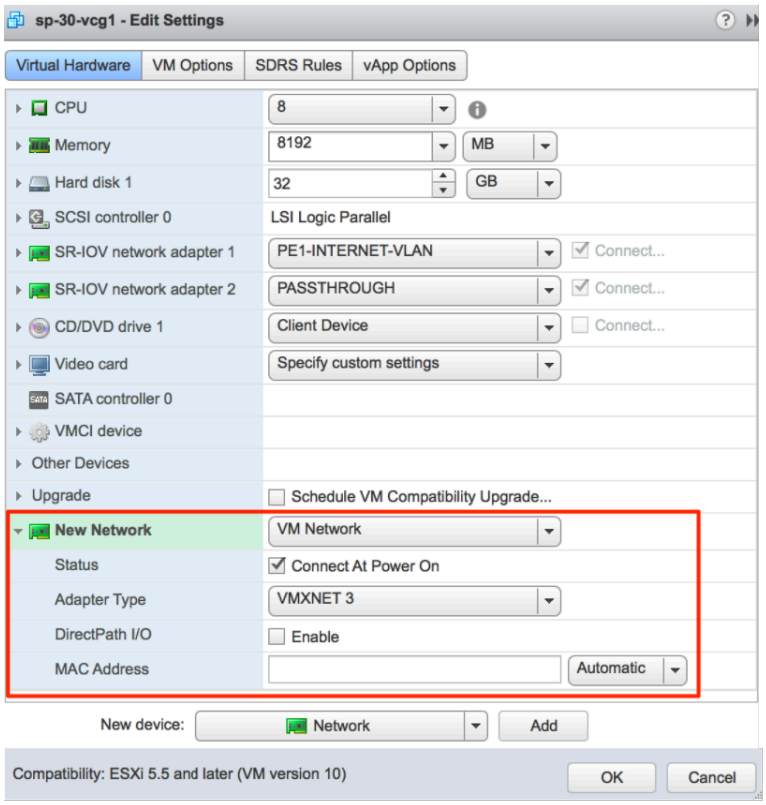
18.7.3 OAM - SR-IOV with vmxnet3 or SR-IOV with VIRTIO

It is possible in some installations to mix and match and provide different interface types for the Gateway. This generally happens if you have an OAM without SR-IOV. This custom configuration requires additional steps since this causes the interfaces to come up out of order.

Record the MAC address of each interface.

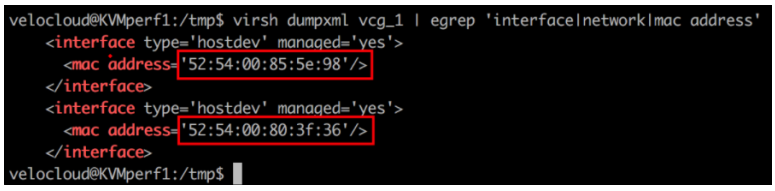
Arista: After creating the machine, go to **Edit Settings** and copy the Mac address.

Figure 18-31: Edit Settings



KVM: After defining the VM, run the following command:

Figure 18-32: Run the Command



18.7.4 Special Consideration When Using 802.1ad Encapsulation

It seems certain that 802.1ad devices do not populate the outer tag EtherType with 0x88A8. Special change is required in user data to interoperate with these devices.

Assuming a Management VRF is configured with S-Tag: 20 and C-Tag: 100, edit the vrf_vlan section in `/etc/ config/ gatewayd` as follows. Also, **define resp_mode** to 1 so that the Gateway will relax its check to allow Ethernet frames that have incorrect EtherType of 0x8100 in the outer header.

18.8 SNMP Integration

This section discusses how to configure SNMP integration.

For additional information on SNMP configuration, see Net-SNMP documentation. To configure SNMP integration:

1. Edit `/etc/snmp/snmpd.conf`.
2. Add the following lines to the config file with source IP address of the systems that will be connecting to SNMP service. You can configure using either SNMPv2c or SNMPv3.
   - The following example will configure access to all counters from localhost via community string vc-vcg and from 10.0.0.0/8 with community string `myentprisecommunity` using SNMPv2c version.

```
agentAddress udp:161 # com2sec sec.name source community com2sec local localhost vc-vcg
 com2sec myenterprise 10.0.0.0/8 myentprisecommunity# group access.name sec.model sec.name
 group rogroup v2c local group rogroup v2c myenterpriseview all included .1 80 # access
 access.name context sec.model sec.level match read write notif access rogroup "" any noauth
 exact all none none#sysLocation Sitting on the Dock of the Bay #sysContact Me <me@example.o
rg>sysServices 72master agentx# # Process Monitoring ## At least one 'gwd' process proc
 gwd # At least one 'mgd' process proc mgd# # Disk Monitoring # # 100MBs required on root
 disk, 5% free on /var, 10% free on all other disks disk / 100000 disk /var 5% includeAllDis
ks 10%# # System Load # # Unacceptable 1-, 5-, and 15-minute load averages load 12 10
 5 # "Pass-through" MIB extension command pass_persist .1.3.6.1.4.1.45346 /opt/vc/bin/s
nmpagent.py veloGateway
```

Note: In the above example, the process gwd comprises entire Data and Control Plane of the Gateway. The Management Plane Daemon (mgd) is responsible for communication with the Orchestrator. This process is kept isolated from gwd so that in the incident of a total failure of the gwd process, the Orchestrator is still reachable for configuration changes or software updates required to resolve the failure.

   - The following example shows configuration using SNMPv3 version.

```
vcadmin:~$ cat /etc/snmp/snmpd.conf ##################################################
########################### # # EXAMPLE.conf: # An example configuration file for
 configuring the Net-SNMP agent ('snmpd') # See the 'snmpd.conf(5)' man page for details
 # # Some entries are deliberately commented out, and will need to be explicitly activated
 # ################################################################################ # #
 AGENT BEHAVIOUR # # Listen for connections from the local system only # agentAddress
 udp:127.0.0.1:161 # Listen for connections on all interfaces (both IPv4 *and* IPv6)
 agentAddress udp:161 ###################################################################
############## # # SNMPv3 AUTHENTICATION # # Note that these particular settings don't
 actually belong here. # They should be copied to the file /var/lib/snmp/snmpd.conf #
 and the passwords changed, before being uncommented in that file *only*. # Then restart
 the agent # createUser authOnlyUser MD5 "remember to change this password" # createUser
 authPrivUser SHA "remember to change this one too" DES # createUser internalUser MD5 "this
 is only ever used internally, but still change the password" # If you also change the
 usernames (which might be sensible), # then remember to update the other occurances in
 this example config file to match. ######################################################
########################### # # ACCESS CONTROL # # system + hrSystem groups only view
 systemonly included .1.3.6.1.4.1.45346 # Full access from the local host # rocommunity
 public localhost # Default access to basic system info rocommunity public default -V
 systemonly # Full access from an example network # Adjust this network address to match
 your local settings, change the community string, # and check the 'agentAddress' setting
 above rocommunity secret 10.0.0.0/16 # Full read-only access for SNMPv3 rouser authOnlyUser
 # Full write access for encrypted requests # Remember to activate the 'createUser' lines
```

```
 above rwuser authPrivUser priv # It's no longer typically necessary to use the full
 'com2sec/group/access' configuration # r[ow]user and r[ow]community, together with suitable
 views, should cover most requirements ##################################################
############################ # # SYSTEM INFORMATION # # Note that setting these values
 here, results in the corresponding MIB objects being 'read-only' # See snmpd.conf(5) for
 more details sysLocation Bay sysContact super@velocloud.net # Application + End-to-End
 layers sysServices 72 # # Process Monitoring # # At least one 'mountd' process proc mountd
 # No more than 4 'ntalkd' processes - 0 is OK proc ntalkd 4 # At least one 'sendmail'
 process, but no more than 10 proc sendmail 10 1 # Walk the UCD-SNMP-MIB::prTable to see
 the resulting output # Note that this table will be empty if there are no "proc" entries
 in the snmpd.conf file # # Disk Monitoring # # 10MBs required on root disk, 5% free on /
var, 10% free on all other disks disk / 10000 disk /var 5% includeAllDisks 10% # Walk the
 UCD-SNMP-MIB::dskTable to see the resulting output # Note that this table will be empty
 if there are no "disk" entries in the snmpd.conf file # # System Load # # Unacceptable
 1-, 5-, and 15-minute load averages load 12 10 5 # Walk the UCD-SNMP-MIB::laTable to
 see the resulting output # Note that this table *will* be populated, even without a
 "load" entry in the snmpd.conf file ####################################################
############################ # # ACTIVE MONITORING # # send SNMPv1 traps trapsink localhost
 public # send SNMPv2c traps trap2sink localhost public # send SNMPv2c INFORMs informsink
 localhost public # Note that you typically only want *one* of these three lines #
 Uncommenting two (or all three) will result in multiple copies of each notification. #
 # Event MIB - automatically generate alerts # # Remember to activate the 'createUser'
 lines above iquerySecName internalUser rouser internalUser # generate traps on UCD error
 conditions defaultMonitors yes # generate traps on linkUp/Down linkUpDownNotifications
 yes ############################################################################## # #
 EXTENDING THE AGENT # # Arbitrary extension commands # extend test1 /bin/echo Hello, world!
 extend-sh test2 echo Hello, world! ; echo Hi there ; exit 35 #extend-sh test3 /bin/sh /tmp/
shtest # Note that this last entry requires the script '/tmp/shtest' to be created first,
 # containing the same three shell commands, before the line is uncommented # Walk the
 NET-SNMP-EXTEND-MIB tables (nsExtendConfigTable, nsExtendOutput1Table # and nsExtendOutpu
t2Table) to see the resulting output # Note that the "extend" directive supercedes the
 previous "exec" and "sh" directives # However, walking the UCD-SNMP-MIB::extTable should
 still returns the same output, # as well as the fuller results in the above tables. # #
 "Pass-through" MIB extension command # #pass .1.3.6.1.4.1.8072.2.255 /bin/sh PREFIX/local/
passtest #pass .1.3.6.1.4.1.8072.2.255 /usr/bin/perl PREFIX/local/passtest.pl rocommunity
 velocloud localhost #pass .1.3.6.1.4.1.45346 /opt/vc/bin/snmpagent.py veloGateway
 pass_persist .1.3.6.1.4.1.45346 /opt/vc/bin/snmpagent.py veloGateway # Note that this
 requires one of the two 'passtest' scripts to be installed first, # before the appropriate
 line is uncommented. # These scripts can be found in the 'local' directory of the source
 distribution, # and are not installed automatically. # Walk the NET-SNMP-PASS-MIB::netSnmp
PassExamples subtree to see the resulting output # # AgentX Sub-agents # # Run as an AgentX
 master agent master agentx # Listen for network connections (from localhost) # rather than
 the default named socket /var/agentx/master
```

3. Edit `/etc/iptables/rules.v4`. Add the following lines to the config with the source IP of the systems that will be connecting to SNMP service:

```
# WARNING: only add targeted rules for addresses and ports # do not add blanket drop or accept
 rules since Gateway will append its own rules # and that may prevent it from functioning
 properly *filter :INPUT ACCEPT [0:0] -A INPUT -p udp -m udp --source 127.0.0.1 --dport 161 -
m comment --comment "allow SNMP port" -j ACCEPT -A INPUT -p udp -m udp --source 10.0.0.0/8 --
dport 161 -m comment --comment "allow SNMP port" -j ACCEPT :FORWARD ACCEPT [0:0] :OUTPUT ACCEPT
 [0:0] COMMIT
```

4. Restart snmp and iptables services:

```
/etc/init.d/snmpd restart /etc/init.d/firewall restart service vc_process_monitor restart
```

18.9 Custom Firewall Rules

This section describes how to modify custom firewall rules.

To modify local firewall rules, edit the following file: /etc/iptables/rules.v4

Important: Add only targeted rules for addresses and ports. Do not add blanket drop or accept rules. Gateway will append its own rules to the table and, because the rules are evaluated in order, that may prevent Gateway software from functioning properly.

```
*filter :INPUT ACCEPT [0:0] -A INPUT -p udp -m udp --source 127.0.0.1 --dport 161 -m comment --
comment "allow SNMP port" -j ACCEPT :FORWARD ACCEPT [0:0] :OUTPUT ACCEPT [0:0] COMMIT
```

Restart netfilter service:

```
service netfilter-persistent restart service vc_process_monitor restart
```

Chapter 19

Partner Gateway Upgrade and Migration

This document provides instructions on how to upgrade the Partner Gateway from the 3.3.2 or 3.4 release to the 4.0 release.

The Gateway appliance includes the following changes in the 4.0 release:

- A new system disk layout based on LVM to allow more flexibility in volume management
- A new kernel version
- New and upgraded base OS packages
- Improved security hardening based on Center for Internet Security benchmarks

The Gateway appliance includes the following system changes in the 4.0 release:

- **`ifupdown`** has been deprecated in favor of https://netplan.io/
  - **`ifup`** and **`ifdown`** are no longer available
  - Network configuration is now in `/etc/netplan vs /etc/network/`
  - `etc/network/ifup.d` and `/etc/network/ifdown.d` no longer work. Network-dispatcher locations should be used `/usr/lib/networkd-dispatcher` (**`dormant.d`**, **`no-carrier.d`**, **`off.d`**, **`routable.d`**)
- Substantial changes to cloud-init. Cloud-init deployment scripts must be reviewed and tested for compatibility
- net-tools (**`ifconfig`**, **`netstat`**, etc) are considered “deprecated” and may be removed in the future versions

Network Configuration

`ifupdown` has been deprecated in favor of https://netplan.io/. Network configuration has moved from `/etc/network to /etc/netplan`.

Example network configuration (whitespace is important!)- `/etc/netplan/50-cloud-init.yaml`:

```
network: version: 2 ethernets: eth0: addresses: - 192.168.151.253/24 gateway4: 192.168.151.1
 nameservers: addresses: - 8.8.8.8 - 8.8.4.4 search: [] routes: - to: 192.168.0.0/16 via:
 192.168.151.254 metric: 100 eth1: addresses: - 192.168.152.251/24 gateway4: 192.168.152.1
 nameservers: addresses: - 8.8.8.8 search: []
```

Network configuration is regenerated on every boot. To make changes to the location configuration, deactivate the Cloud-init network configuration.

```
echo 'network: {config: disabled}' > /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg
```

Cloud-init

Cloud-init was upgraded to version 20.2. additional information on Cloud-init can be found here: https://cloudinit.readthedocs.io/en/stable/index.html

Example 1: Simple

meta-data:

instance-id: vcg1

local-hostname: vcg1

user-data:

```
#cloud-config hostname: vcg1 password: Velocloud123 chpasswd: {expire: False} ssh_pwauth: True
```

Example 2: New-style network configuration (network-config file)

meta-data:

```
instance-id: vcg1 local-hostname: vcg1
```

user-data:

```
#cloud-config hostname: vcg1 password: Velocloud123 chpasswd: {expire: False} ssh_pwauth: True
 ssh_authorized_keys: - ssh-rsa … rsa-key velocloud: vcg: vco: demo.velocloud.net activation_code:
 F54F-GG4S-XGFI vco_ignore_cert_errors: false runcmd: - 'echo “Welcome to VeloCloud”'
```

network-config Example 1:

```
version: 2 ethernets: eth0: addresses: - 192.168.152.55/24 gateway4: 192.168.152.1 nameservers:
 addresses: - 192.168.152.1 eth1: addresses: - 192.168.151.55/24 gateway4: 192.168.151.1
 nameservers: addresses: - 192.168.151.1
```

network-config Example 2:

Note: If multiple interfaces are present on the Gateway and need an interface to be selected as a preferred interface for the default gateway, the below configuration (with the metric value) can be used to select the correct interface.

```
version: 2 ethernets: eth0: addresses: [192.168.82.1/24] eth1: addresses: [70.150.1.1/24]
 routes: - {metric: 1, to: 0.0.0.0/0, via: 70.150.1.254} eth2: addresses: [70.155.1.1/24]
 routes: - {metric: 2, to: 0.0.0.0/0, via: 70.155.1.254}
```

Net-tools

Net-tools utilities like ifconfig, netstat, route, etc. are considered “deprecated.” Net-tools suggested replacements are shown in the table below. These commands only display information for the Linux Host and not for the SD-WAN Overlay Network.

Note: For additional information, type: **man ip**.

Table 58: Net-tools Utilities

Old Net-tool Utilities	New Corresponding Net-tool Utilities
arp	ip n (ip neighbor)
ifconfig	ip a (ip addr), ip link, ip -s (ip -stats)
nameif	ip link, ifrename
netstat	ss, ip route (for netstat-r), ip -s link (for netstat -i), ip maddr (for netstat-g)
route	ip r (ip route)

Sample Command Output for Net-tool Utilities

The sample output is confirmation that the command is successful. Sample command outputs for **ip n** (ip neighbor), **ip a (ipaddr**), and **ip link** are shown below.

ip n (**ip neighbor**):

```
root@SS-gateway-1:~# ip n 192.168.0.100 dev eth2 lladdr 00:50:56:84:85:d4 REACHABLE 192.168.0.250
 dev eth2 lladdr 00:50:56:84:97:66 REACHABLE 13.1.1.2 dev eth0 lladdr 00:50:56:84:e7:fa REACHABLE
 root@SS-gateway-1:~#
```

ip a (**ipaddr**):

```
root@SS-gateway-1:~# ip a 1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
 group default qlen 1000 link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00 inet 127.0.0.1/8
 scope host lo valid_lft forever preferred_lft forever inet6 ::1/128 scope host valid_lft forever
 preferred_lft forever 2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP
 group default qlen 4096 link/ether 00:50:56:84:a0:09 brd ff:ff:ff:ff:ff:ff inet 13.1.1.1/24
 brd 13.1.1.255 scope global eth0 valid_lft forever preferred_lft forever inet6 fe80::250:56f
f:fe84:a009/64 scope link valid_lft forever preferred_lft forever 3: eth1: <BROADCAST,MU
LTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000 link/ether 00:50:56:84:a
6:ab brd ff:ff:ff:ff:ff:ff inet 101.101.101.1/24 brd 101.101.101.255 scope global eth1 valid_lft
 forever preferred_lft forever inet6 fe80::250:56ff:fe84:a6ab/64 scope link valid_lft forever
 preferred_lft forever 4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP
 group default qlen 1000 link/ether 00:50:56:84:bc:75 brd ff:ff:ff:ff:ff:ff inet 192.168.0.201/24
 brd 192.168.0.255 scope global eth2 valid_lft forever preferred_lft forever inet6 fe80::250:56f
f:fe84:bc75/64 scope link valid_lft forever preferred_lft forever 6: gwd1: <POINTOPOINT,
MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 4096
 link/none inet 169.254.129.1/32 scope global gwd1 valid_lft forever preferred_lft forever inet6
 fe80::27d5:9e46:e7f7:7198/64 scope link stable-privacy valid_lft forever preferred_lft forever
 root@SS-gateway-1:~#
```

ip link

```
root@SS-gateway-1:~# ip link 1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
 mode DEFAULT group default qlen 1000 link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00 2:
 eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP mode DEFAULT group default
 qlen 4096 link/ether 00:50:56:84:a0:09 brd ff:ff:ff:ff:ff:ff 3: eth1: <BROADCAST,MULTICAST,UP,LO
WER_UP> mtu 1500 qdisc mq state UP mode DEFAULT group default qlen 1000 link/ether 00:50:56:84:a
6:ab brd ff:ff:ff:ff:ff:ff 4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP
 mode DEFAULT group default qlen 1000 link/ether 00:50:56:84:bc:75 brd ff:ff:ff:ff:ff:ff 6: gwd1:
 <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN mode DEFAULT
 group default qlen 4096 link/none root@SS-gateway-1:~#
```

Upgrade Considerations

> **Note:** The below steps are based on the assumption that you want to keep the same IP address and Gateway name for the new Gateway deployed in the 4.0 release. However, if you want to create a new Gateway with a different IP address and, you can follow the new Gateway procedures.

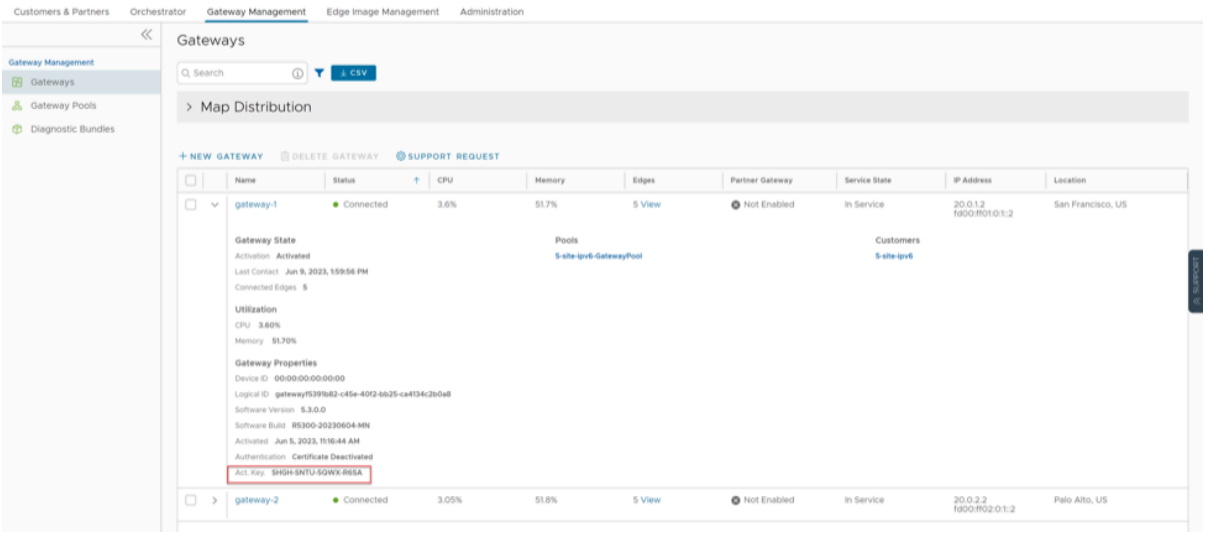
Due to substantial changes to the disk layout and system files, an in-place upgrade is not possible from older releases to the 4.0 release. The migration will require deploying new 4.0 Gateway systems and decommissioning systems running older code.

For VPN Gateways or NAT Gateways with well-known public IP addresses, adhere to the following procedure below if the public IP of the Gateway must be preserved.

Procedure: (VNP or NAT Gateways with Well-Known Public IP Addresses)

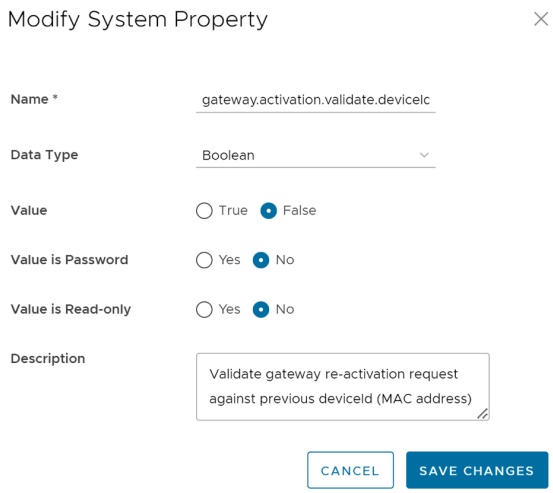
1. Launch the new Gateway system based on the 4.0 release image. Refer to the deployment guide for your platform for additional information (Gateway Installation Procedures).
2. Shutdown the old Gateway system. (Bring down the old Gateway VM (either by running the **`sudo poweroff`** command on the CLI console, or by powering off from the available Hypervisor options).
3. Migrate the public IP to the new system: update the NAT record to point to the new Gateway system, or configure the public IP on the new Gateway network interface. Deploy the new Gateway with the Cloud-int examples given above using the same IP address as the previous Gateway.
4. Obtain the activation key from the existing Gateway record in the Orchestrator (as described in the steps below).
   a. From the **Orchestrator**, go to **Gateway Management** > **Gateways**.
   b. In the **Gateways** screen, select the Gateway for which you to obtain the activation key and select the right arrow before the Gateway name.
   c. An information box expands and you can find the activation key at the bottom, as shown in the image below.

Figure 19-1: Gateway Management



5. Set the following system property **gateway.activation.validate.deviceId** to **False**, as shown in the image below. Refer to the *System Properties* section in the *Arista VeloCloud SD-WAN Operator Guide*, if necessary for additional information.

   Figure 19-2: Modify System Property



6. Re-activate the new Gateway system: from the CLI console run: `sudo /opt/vc/bin/activate.py -s <vco_address> <activation_code>`

7. Restore the following system property **gateway.activation.validate.deviceId** to the original value (if necessary).

   The Gateway is now registered and ready to receive a connection from the Edges.

Note: The Gateway reactivation can be performed via Cloud-int, as described in the User Data section in this document.

Activation Example Output

```
root@gateway/opt/vc# /opt/vc/bin/activate.py FLM6-CSV6-REJS-XFR5 -i -s
169.254.8.2
```

Activation successful, VCO overridden back to `169.254.8.2 root@SS1-gateway-2:/opt/vc#`

Gateways Without Well-known Public IPs

This section is only for Gateways without a well-known public IP, such as, VPN Gateways. If this scenario applies, follow the procedure below.

Procedure: (Gateways Without Well-known Public IPs)

1. Launch a new Gateway system. Refer to the deployment guide for your platform if necessary (Gateway Installation Procedures).

2. Activate a new Gateway system.

3. Add new Gateway to the Orchestrator Gateway pool. Refer to the "Gateway Management" section in the VeloCloud SD-WAN Operator Guide for additional details.

- The Gateway is now registered and ready to receive a connection from the Edges.

4. Remove the old Gateway from Orchestrator Gateway pool. Refer to the "Gateway Management" section in VeloCloud SD-WAN Operator Guide for additional information.
5. Decommission the old Gateway VM. (Remove the Gateway record from the Orchestrator and decommission the VM instance).

Obtaining Gateway Activation Key Via API

To deploy using the API Method, use the following: `network/getNetworkGateways`

Sample response:

```
{"jsonrpc":"2.0","result":[{"id":1, "activationKey":"69PX-YHY2-N5PZ-G3UW …
```

Configure Handoff Interface in Data Plane

To configure Handoff Interface in Data Plane, see the topic *Post-Installation Tasks*.

Appendix A

References

A.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 Global Settings Guide*
- *Arista VeloCloud SD-WAN Operator 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*