Configuration Guide

VeloCloud SD-WAN Bastion Orchestrator

Version 6.0

Arista.com

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

Contents

Chapter 1

VeloCloud SD-WAN Bastion Orchestrator Configuration Guide

The Arista VeloCloud SD-WAN Bastion Orchestrator Configuration Guide provides information on how to configure a Bastion Orchestrator (Public Orchestrator) in an Internet-facing demilitarized zone (DMZ) for the purpose of staging and activation of an Edge.

Chapter 2

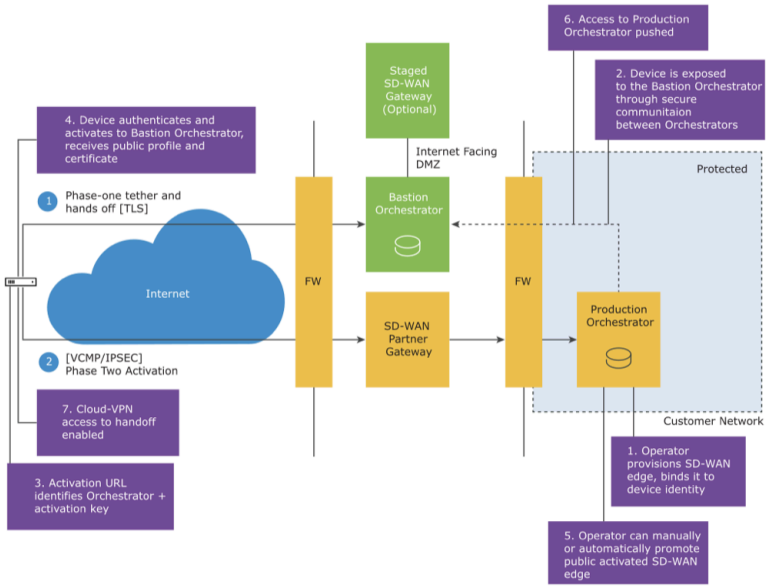
Bastion Orchestrator Overview

The VeloCloud Orchestrator stores and exports, through APIs, sensitive information about customers and their networks. To protect the on-premises customer-sensitive information from external attack and to restrict access to their APIs, VeloCloud SD-WAN supports configuration of a Bastion Orchestrator (Public Orchestrator) in an Internet-facing demilitarized zone (DMZ) for the purpose of staging and activation of a SD-WAN Edge. With the Bastion Orchestrator feature enabled, an Operator Super user can activate a provisioned Edge against the Bastion Orchestrator by using the activation key received from the Production (Private) Orchestrator. The activated Edge is then promoted from the Bastion Orchestrator to the Production Orchestrator through a secure communication.

Note: In this document, the term "Bastion Orchestrator" is used interchangeably with the term "Public Orchestrator", and the term "Production Orchestrator" is used interchangeably with the term "Private Orchestrator".

The following diagram illustrates the architecture and activation workflow of the Bastion Orchestrator.

Figure 2-1: Bastion Orchestrator Architecture and Activation Workflow



The Bastion Orchestrator architecture consists of two Orchestrator instances in communication with one another. The public-facing instance of the Bastion pair is 'Bastion Orchestrator', and the private instance is 'Production Orchestrator. The Bastion Orchestrator- Edge activation workflow includes the following steps:

1. Configure Bastion Orchestrator
2. Set up Production Orchestrator
3. Stage a Gateway to Bastion Orchestrator
4. Activate the SD-WAN Edge Against the Bastion Orchestrator

5. Promote an Activated Edge from Bastion Orchestrator to Production Orchestrator

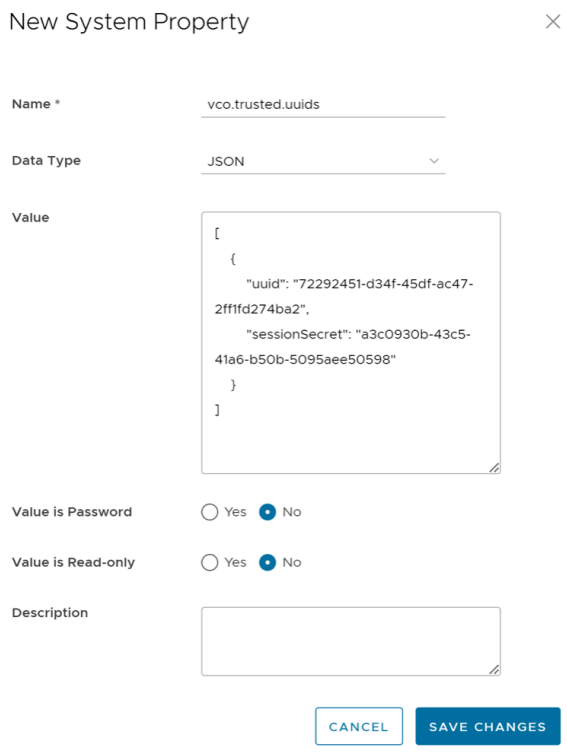
Limitations

- During the Bastion configuration, you can stage only one Operator Super user account to the Bastion Orchestrator. Once the Bastion connection is established between the Bastion and Production Orchestrators, the Operator Super user account can be used for emergency purposes to gain access to the Bastion Orchestrator. The Operator Super user who is staged will have access to only the Bastion Orchestrator configuration page.
- Unpairing of Bastion Orchestrator from the Production Orchestrator (**Return to Standalone Mode** operation) is not supported.
- For activating an Edge, the Edge must be in "Certificate Acquire" mode. While promoting the Edge, for bringing the WAN links with the gateway as UP, the Gateway must be in "Certificate Acquire" or "Certificate Required" mode.
- After the promotion of an Edge from Bastion Orchestrator to Production Orchestrator, if you want to upgrade the Edge Software image, ensure to configure the `vco.trusted.uuids` system property on the Production Orchestrator as follows:

```
[ { "uuid": "72292451-d34f-45df-ac47-2ff1fd274ba2", "sessionSecret": "a3c0930b-43c5-41a6-b50b-5
095aee50598" } ]
```

Where, *uuid* and *sessionSecret* are UUID and Session Secret values of the Bastion Orchestrator. You can get the UUID and Session Secret from the `vco.uuid` and `session.secret` system properties, respectively.

Figure 2-2: New System Property



- Once the Gateway and Edges are staged and activated in the Bastion Orchestrator, you cannot perform the Remote diagnostics tests using the Production Orchestrator for the staged Gateway and Edges in the Bastion Orchestrator; however, you can request and generate remote diagnostic bundle from the Production Orchestrator.
- The Bastion-staged profile, which is created for the purpose of staging an Enterprise customer to Bastion Orchestrator, should have minimum configuration related to Global segments. When the profile entities are updated, only the Device settings, Business policy, and Firewall under Global segment will be synchronized with the Bastion Orchestrator. The following Profile configurations will not be synchronized with the Bastion Orchestrator:
  - Segments other than Global segment
  - Network segments configurations
  - Object groups

Disaster Recovery for Bastion Orchestrator

Essentially, Disaster Recovery (DR) functionality is supported for Production (Private) Orchestrator, but for Bastion (Public) Orchestrator as it is stateless and receives its instructions from Production Orchestrator, the DR functionality for Bastion Orchestrator is currently not supported.

Newly Supported features in the 5.4.0 Release

In the 5.4.0 release, the following new features are introduced for the Bastion Orchestrator:

- Ability to view events of a Staged Edge from the Production Orchestrator through the Bastion Orchestrator.
- Ability to request diagnostic bundle from the Production Orchestrator through the Bastion Orchestrator of a Staged Edge.
- If an Edge promotion fails due to some reason, the Edge goes back to the last known good configuration i.e. connected back to Bastion.
- Ability to configure and send the Edge upgrade (Software and Firmware upgrades) related information to the Bastion Orchestrator while staging the SD-WAN Edge to Bastion Orchestrator. This allows the Edge to get upgraded immediately after the Edge is activated against the Bastion Orchestrator. For additional information, see Stage an Edge to Bastion Orchestrator.

Chapter 3

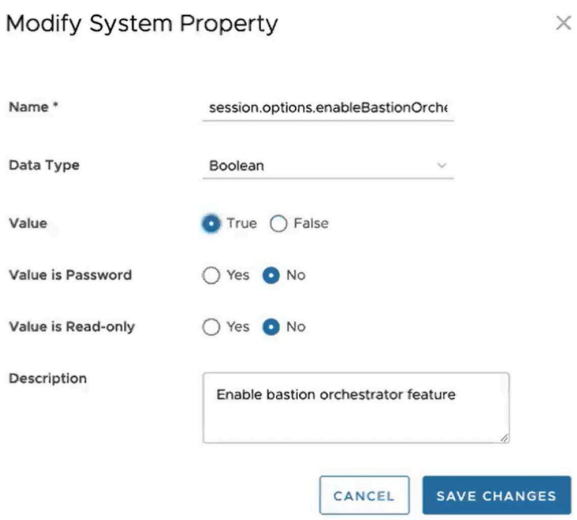
Prerequisites for Bastion Orchestrator Configuration

Discusses the Prerequisites for Bastion Orchestrator Configuration.

The following are the prerequisites to configure two Orchestrators as a Bastion pair:

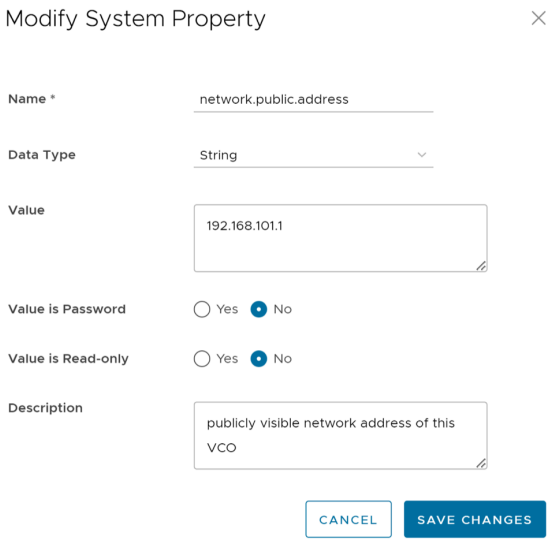
- Set the `session.options.enableBastionOrchestrator` system property to *True* in both the Orchestrators (Bastion and Production). By default, this system property is set to *False*.

  Figure 3-1: Modify System Property



- Set the `network.public.address` system property in both the Orchestrators (Bastion and Production) to its respective Orchestrator IP address.

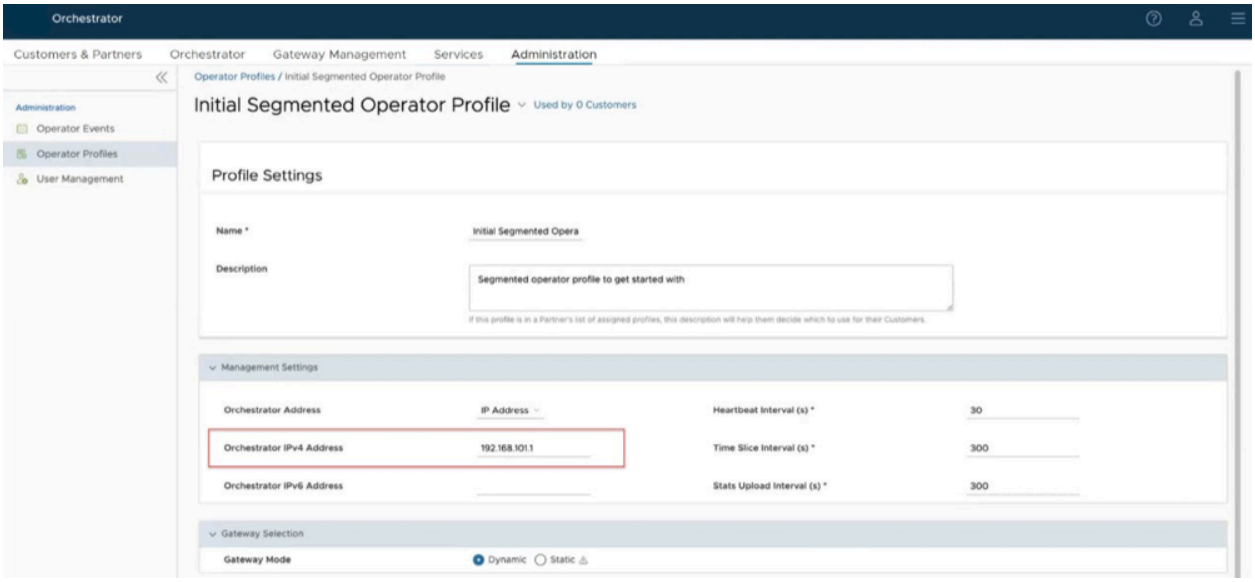
  Figure 3-2: Modify System Property



- Ensure to make a note of Universal Unique Identifier (UUID) of both the Bastion and Production Orchestrators to be used for Bastion configuration. You can get the UUID from the `vco.uuid` System Property.
- Ensure to make a note of Session Secret value of the Bastion Orchestrator from the `session.secret` System Property. The UUID and Session Secret values of the Bastion Orchestrator are required if you want to upgrade the Edge software image after Edge promotion. For additional information, see the *Limitations* section in the topic Bastion Orchestrator Overview.
- In the Production Orchestrator, ensure you have created at least one Operator Super user account that can be used for staging to the Bastion Orchestrator. For steps, see Create New Operator User. This Operator Super user account is used for emergency purposes to gain access to the Bastion Orchestrator. Under normal operating process, the account must be disabled from the Production Orchestrator to reduce the attack surface.

- In the Production Orchestrator, ensure that the Operator profile (used for Edge provisioning) have the respective Orchestrator IP address set in the **Orchestrator Address** field under **Management Settings**.

  Figure 3-3: Operator Profile Settings



- In the Production Orchestrator, create a new Enterprise profile with a minimum configuration (configuration without enterprise services, segments configuration, object groups) for the purpose of staging an Enterprise customer to a Bastion Orchestrator. for steps, see Create New Profile.

Chapter 4

Configure Bastion Orchestrator

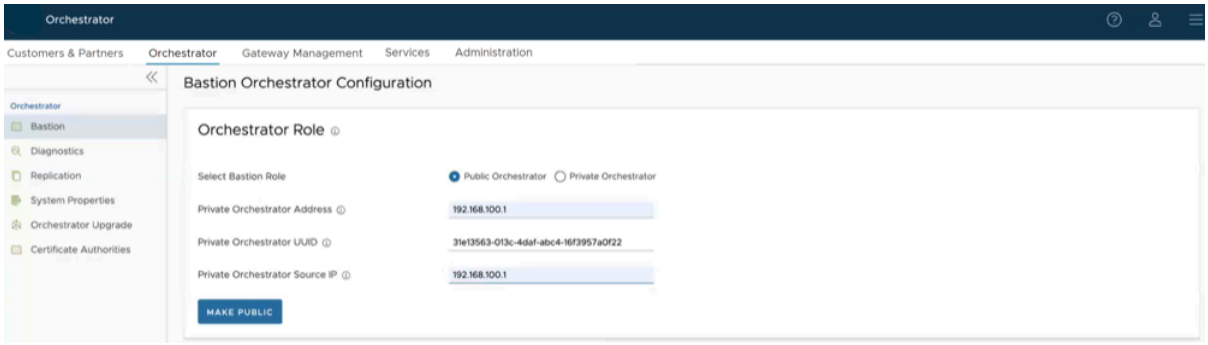
- Ensure you have two Orchestrators ready to be set up as a Bastion pair and you have set the `session.options.enableBastionOrchestrator` system property to *True* in both the Orchestrators. By default, this system property is set to *False*.
- Ensure you have at least one Operator Superuser created in the Production Orchestrator.

Only an Operator Superuser can perform Bastion Orchestrator configuration. The Bastion Orchestrator configuration involves configuring two Orchestrators as a Bastion pair.

Note: In this document, the term "Bastion Orchestrator" is used interchangeably with the term "Public Orchestrator", and the term "Production Orchestrator" is used interchangeably with the term "Private Orchestrator".

To create a Bastion pair using two Orchestrators, configure one Orchestrator as Public (Bastion) and another as Private (Production) by performing the following steps:

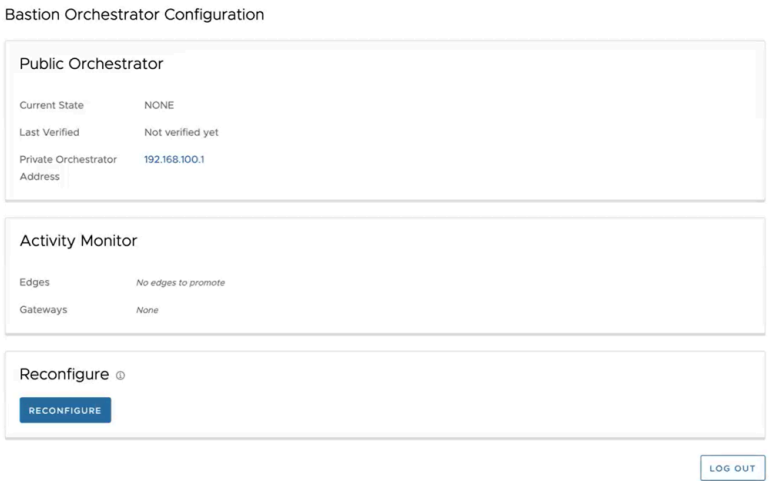
1. Configure one of the two Orchestrators as a Public Orchestrator.
   a. In a web browser, launch the Orchestrator application that needs to be configured as a Public Orchestrator, and login as an Operator user.
   b. Select the **Orchestrator** tab.
      The **Bastion Orchestrator Configuration** page appears.
      Figure 4-1: Bastion Orchestrator Configuration



   c. Under **Orchestrator Role**, select **Public Orchestrator** for the Bastion Role and enter the following configuration details:
      - **Private Orchestrator Address**- The IP address of the Production Orchestrator.
      - **Private Orchestrator UUID**- A Universal Unique Identifier value that is specified in the `vco.uuid` System Property of the Production Orchestrator.
      - **Private Orchestrator Source IP**- The NATed Source IP address of the Production Orchestrator.

d. Select **Make Public** to make the Orchestrator as a Public Orchestrator.

Figure 4-2: Public Orchestrator



e. Select **Reconfigure** if you want to make any changes to the configuration details.

f. Select **Log Out** if you want to log out of the Public Orchestrator.

2. Configure the second Orchestrator as a Private Orchestrator.

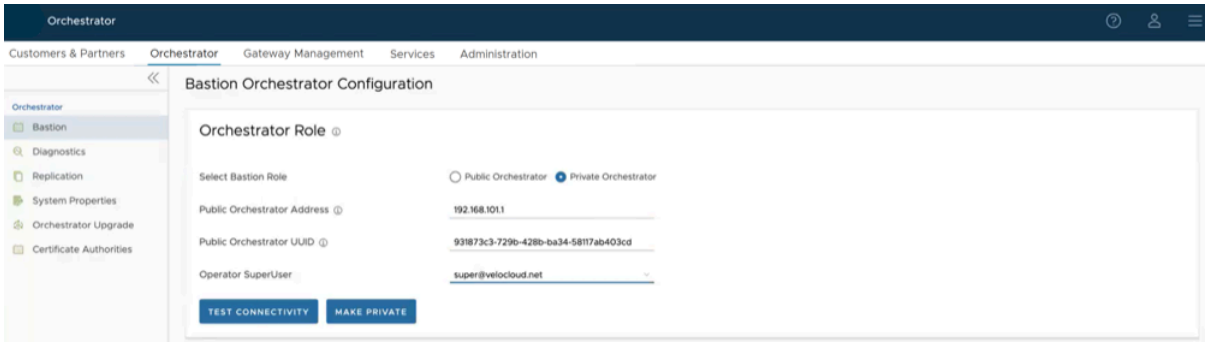
a. In a web browser, launch the Orchestrator application that needs to be configured as a Private Orchestrator, and login as an Operator user.

b. In the Orchestrator UI, select **Orchestrator**.

The **Bastion Orchestrator Configuration** page appears.

c. Under **Orchestrator Role**, select **Private Orchestrator** for the Bastion Role and enter the following configuration details:

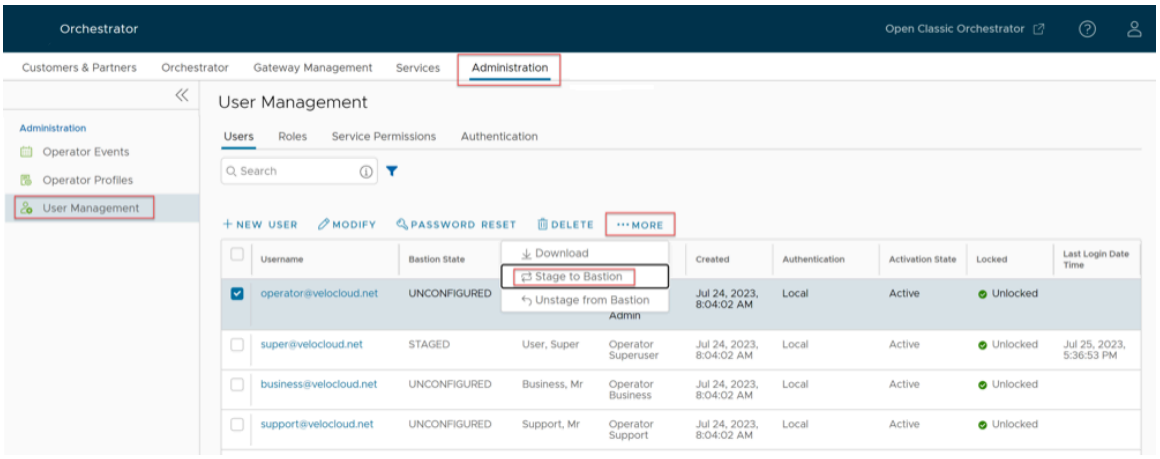
Figure 4-3: Bastion Orchestrator Configuration



- **Public Orchestrator Address**- The IP address of the Public (Bastion) Orchestrator.
- **Public Orchestrator UUID**- A Universal Unique Identifier value that is specified in the `vco.uuid` System Property of the Public Orchestrator.
- **Operator Superuser**- From the drop-down list, select an Operator Super user to be staged along with this Bastion configuration. Once the Bastion connection is established between the Public and Private Orchestrators, only the Operator Super user who is staged in this step will gain emergency access to the Public Orchestrator.

> **Note:** VeloCloud SD-WAN allows you to stage only one Operator Super user to the Public Orchestrator during the Bastion configuration, however; for troubleshooting purposes, you can stage multiple Operator users to Public Orchestrator after the Bastion is configured. To stage Operator users post-Bastion configuration, navigate to **Administration** > **User Management** > **Users** > **Select a User** > **More** > **Stage to Bastion** in the Production Orchestrator.

Figure 4-4: User Management



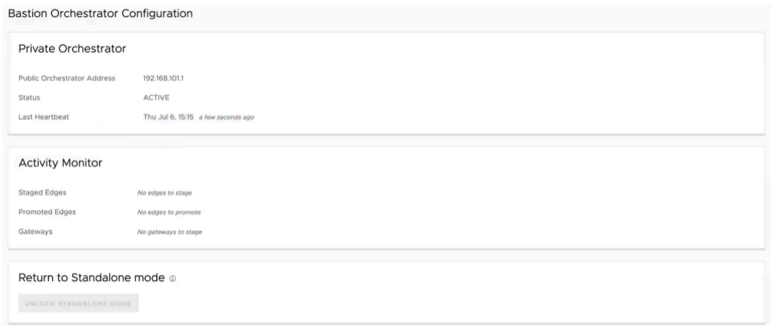
d. Select **TEST CONNECTIVITY** to test the connection between Public and Private Orchestrators.

e. Select **Make Private**.

f. The connection between Public and Private Orchestrators is tested and if the connection is successful, the Bastion pairing is established between the two Orchestrators.

> **Note:** Unpairing of Public Orchestrator from the Production Orchestrator (**Return to Standalone Mode** operation) is not supported in the 4.3.0 release.

Figure 4-5: Private Orchestrator



The Bastion Orchestrator configuration is complete, and both the Public and Private Orchestrators are configured as a Bastion pair. In the Bastion setup, only the configured Operator Super user can then access the Public Orchestrator in read-only mode.

You can stage an Enterprise customer and Edges to Bastion Orchestrator. For steps, see Stage an Edge to Bastion Orchestrator.

Chapter 5

Set up Production Orchestrator

Discusses the pre-configuration steps to be completed in the Production Orchestrator to activate a SD-WAN Edge against a Bastion Orchestrator and then promote it to the Production Orchestrator.

In the Production Orchestrator, ensure that you have completed the following minimum pre-configuration steps:

- Create New Operator User
- Create Gateways for Bastion Orchestrator Setup
- Create New Customer
- Create New Profile
- Configure Partner Hand Off
- Provision a New Edge

5.1 Create New Operator User

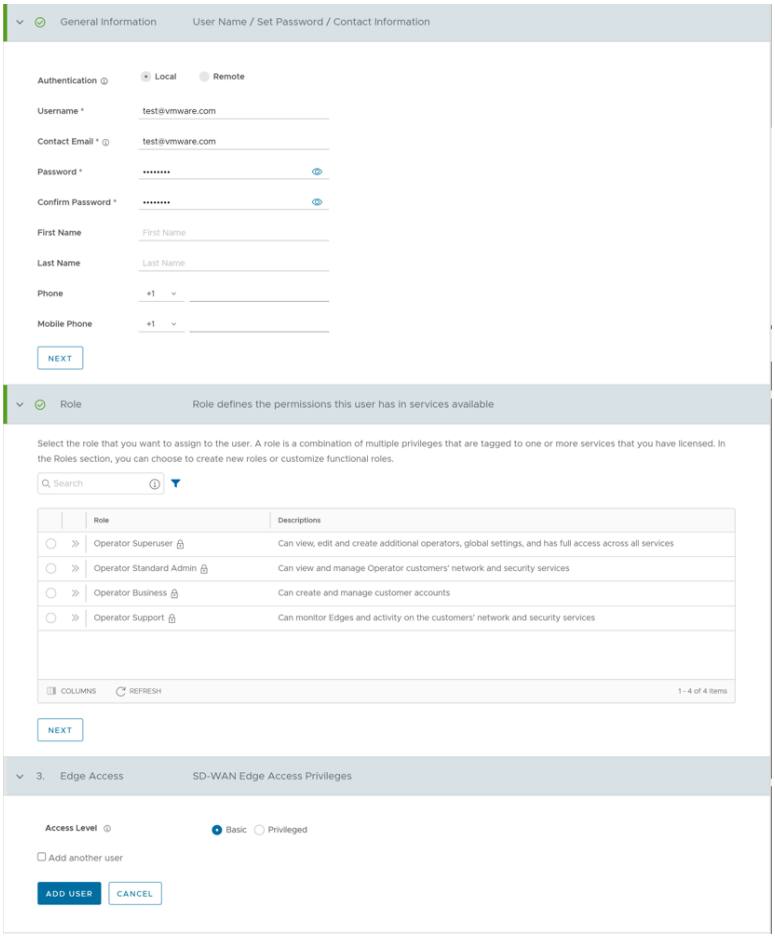
In the Operator portal, you can add new users and configure the user settings. Only Operator Superusers and Operator Standard Admins can add a new user.

To add a new user, perform the following steps:

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

The following screen appears:

Figure 5-1: New User



4. Enter the following details for the new user:

Table 1: 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 the *Roles* section in the *Arista VeloCloud SD-WAN Operator Guide*.
Edge Access	Ensure that you have Operator Super User role to modify the **Access Level** for the user. 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**. **Note:** Only Operator Super Users can modify the default value to **Privileged**.

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

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

5.2 Create Gateways for Bastion Orchestrator Setup

In the Bastion Orchestrator setup, there are two Gateways, one paired with the Bastion Orchestrator, and the other paired with Production Orchestrator and functions as a Partner Gateway.

- To create a Gateway paired with Bastion Orchestrator, see Create New Gateway.
- To create a Partner Gateway with Partner Handoff enabled, see Configure Partner Hand Off.

5.2.1 Create New Gateway

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:

Table 2: New Gateway- Options and Descriptions

Option	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**. • **Certificate Required**- Gateway uses the PKI certificate.
Contact Name	Enter the name of the Site Contact.
Contact Email	Enter the Email ID of the Site Contact.

Note:

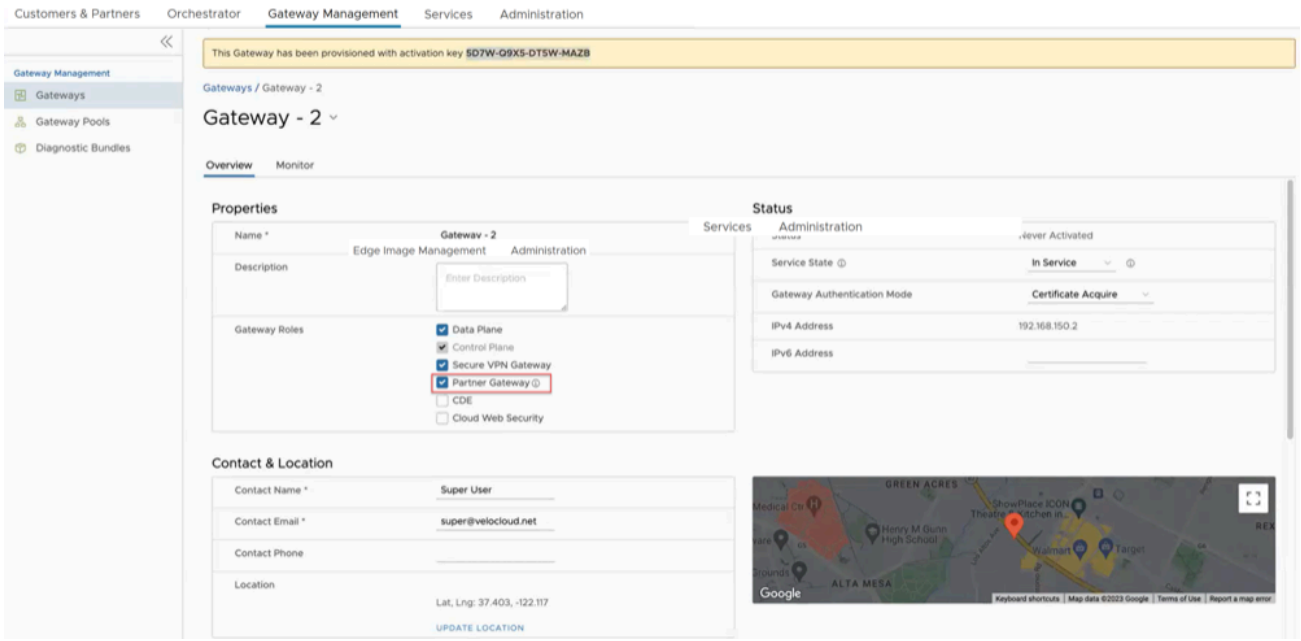
- Once you have created a Gateway, you cannot modify the IP addresses.
- Release 4.3.x and 4.4.x support Greenfield deployment of Gateways for IPv6. If you have upgraded a Gateway from a previous version earlier than 4.3.0, you cannot configure the upgraded Gateway with the IPv6 address.
- Release 4.5.0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

5.2.2 Configure Partner Hand Off

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

Figure 5-2: Gateway Properties



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.

To configure the handoff settings, perform the following steps:

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

6. In the **Configure Hand Off** area, configure the following settings:

Figure 5-3: Configure Hand Off

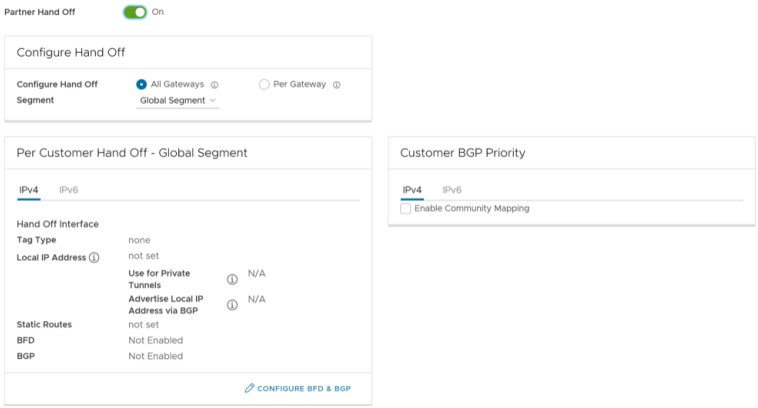
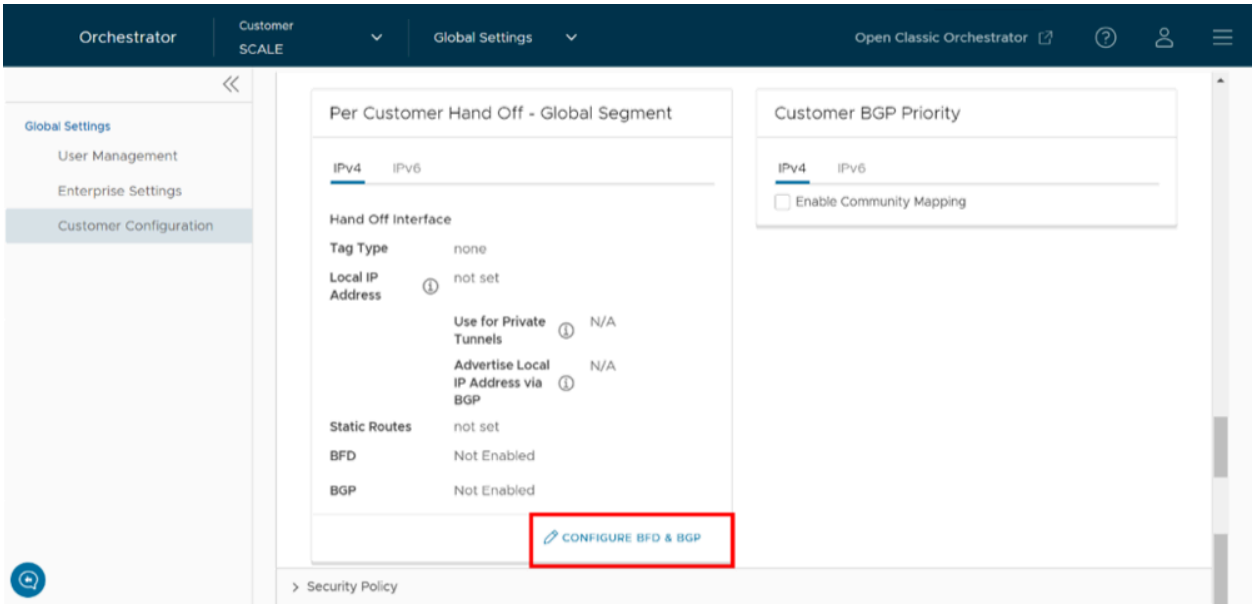


Table 3: Configure Hand Off- Options and Descriptions

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.

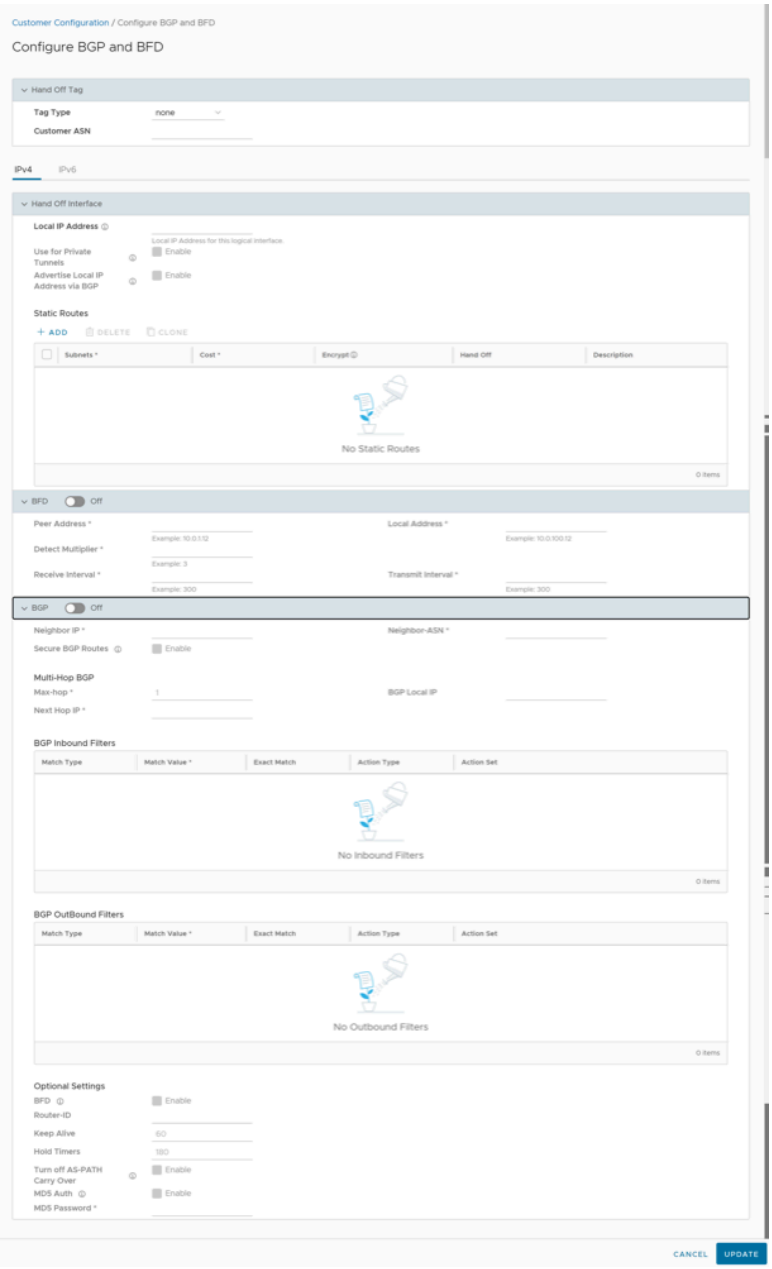
7. At the bottom of the **Per Customer Hand Off – Global Segment** area, select the **Configure BFD & BGP** link, as shown in the image below.

Figure 5-4: Select "Configure BFD & BGP" Link



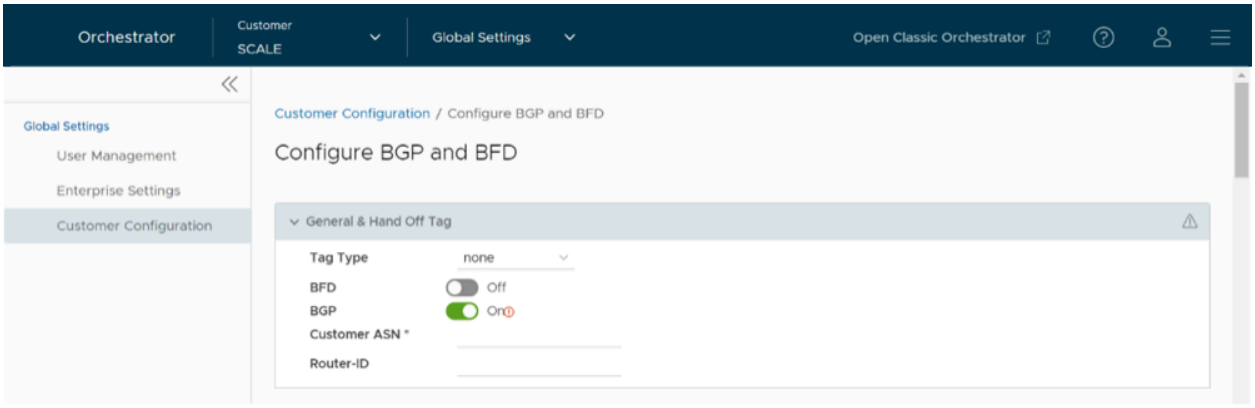
The **Configure BGP and BFD** screen appears.

Figure 5-5: Configure BGP and BFD



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

Figure 5-6: General & Hand Off Tag



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

Table 4: Configure BGP and BFD- Options and 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.
Max-hop	Enter the number of maximum hops to allow multi-hop for the BGP peers. The range for Max-hop is from 1 to 255, and the default value is 1.  **Note:** This field is available only for eBGP neighbors, when the local ASN and the neighboring ASN are different.

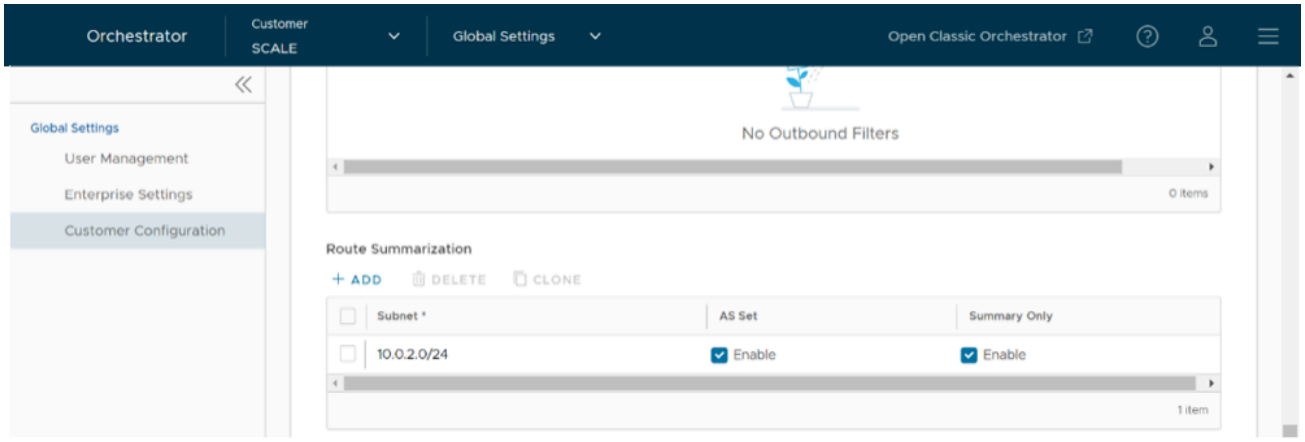
Option	Description
Next Hop IP	Enter the next-hop IP address to be used by BGP to reach the multi-hop BGP peer. **Note:** This option is available only for multi-hop eBGP with Max-hop count greater than 1.
Neighbor-ASN	Enter the Autonomous System Number of the Neighbor network.
BGP Local IP	Local IP address is the equivalent of a loopback IP address. Enter an IP address that the BGP neighborships can use as the source IP address for the outgoing BGP packets. **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 Inbound Filters	Displays the BGP inbound filters.
BGP Outbound Filters	Displays the BGP outbound filters.
BGP Optional Settings	
BFD	Select the check box to subscribe to the BFD session.
Router-ID	Enter the Router ID to identify the BGP Router.
Keep Alive	Enter the BGP Keep Alive time in seconds. The default timer is 60 seconds.
Hold Timers	Enter the BGP Hold time in seconds. The default timer is 180 seconds.
Turn off AS-PATH Carry Over	Select the check box to turn off AS-PATH carry over, which influences the outbound AS-PATH to make the L3-routers prefer a path towards a PE. If you select this option, ensure to tune your network to avoid routing loops. It is recommended not to select this check box.
MD5 Auth	Select the check box to activate BGP MD5 authentication. This option is used in a legacy network or federal network, and is used as a security guard for BGP peering.
MD5 Password	Enter a password for MD5 authentication. **Note:** Starting from the 4.5 release, the use of the special character "<" in the password is no longer supported. In cases where users have already used "<" in their passwords in previous releases, they must remove it to save any changes on the page.

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

a. If applicable, configure for Route Summarization.

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

Figure 5-7: Route Summarization



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

Table 5: Route Summarization- Options and Descriptions

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

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

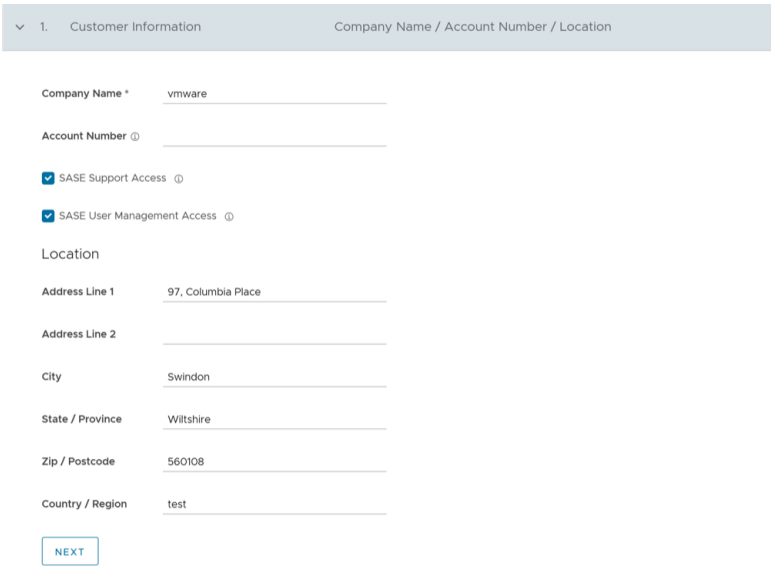
5.3 Create New Customer

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

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

a. Customer Information:

Figure 5-8: Customer Information



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

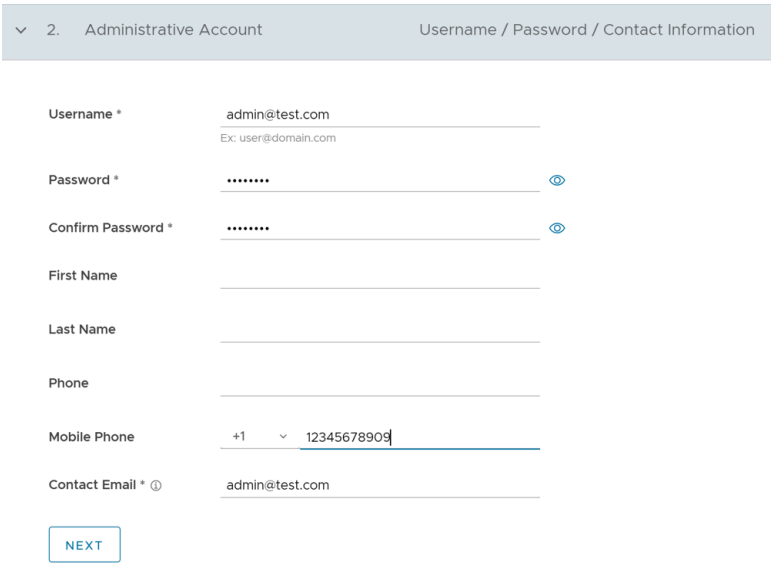
Note: The **Next** button is activated only when you enter all the mandatory details.

Table 6: Customer Information- Options and Descriptions

Option	Description
Company Name	Enter your company name.
Account Number	Enter a unique identifier for the Customer.
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.
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. Administrative Account:

Figure 5-9: Administrative Account



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

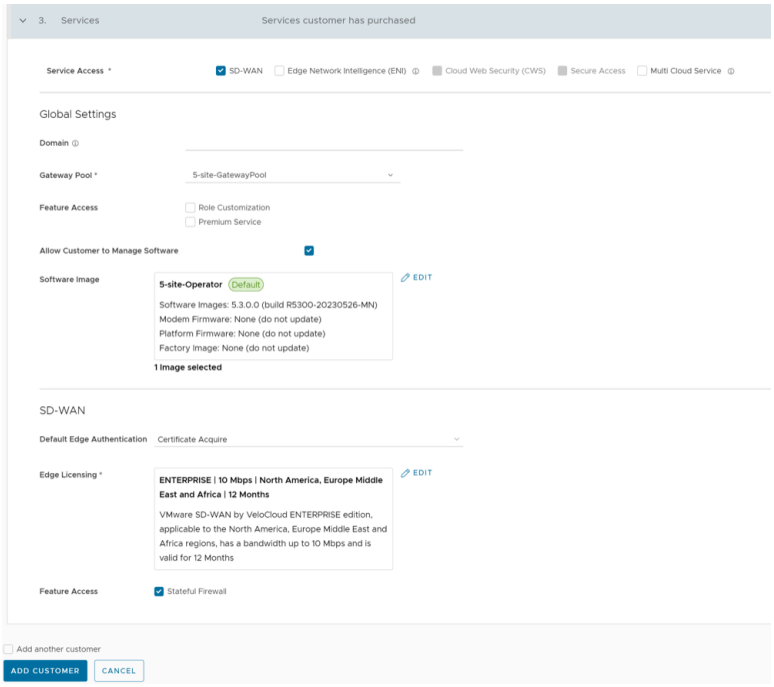
Note: The **Next** button is activated only when you enter all the mandatory details.

Table 7: Administrative Account- Options and 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. Services:

Figure 5-10: Services



Configure the following global settings:

Table 8: Services- Options and Descriptions

Option	Description
Domain	Enter the domain name to be used to activate Single Sign On (SSO) authentication for the Orchestrator. This field is required when Edge Intelligence is activated for the Customer.
Gateway Pool	Select an existing Gateway pool from the drop-down list.
Feature Access	You can select either **Role Customization** or **Premium Service**, or both the check boxes.
Allow Customer to Manage Software	Select the check box if you want to allow an Enterprise Super User to manage the software images available for the Enterprise. Once selected, the **Software Image** field is displayed. Select **Add** and in the **Select Software/Firmware Images** pop-up window, select and assign the software/firmware images from the available list for the Enterprise. Select **Done** to add the selected images to the **Software Image** list. **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.

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

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

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

Table 9: SD-WAN Service- Options and 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.
Feature Access	Select the **Stateful Firewall** check box to override the Stateful Firewall settings activated on the Enterprise Edge.

3. 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.

5.4 Create New Profile

One of the prerequisites for Bastion configuration is to create a new Enterprise profile with a minimum configuration for the purpose of staging an Enterprise customer to a Bastion Orchestrator.

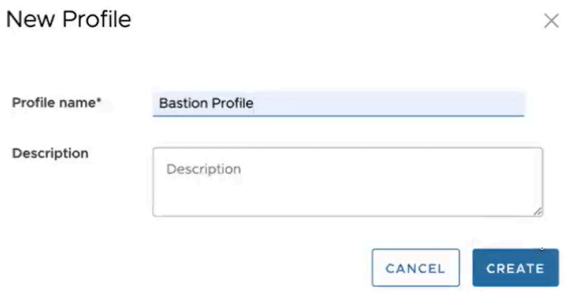
To create a Profile, perform the following steps:

1. In the **SD-WAN** service of the **Enterprise** portal, select the **Configure** tab.
2. From the left menu, select **Profiles**.

   The **Profiles** page appears.

3. In the **Profiles** page, select **New Profile**.

Figure 5-11: New Profile



4. Enter a name and description for the new Profile and select **Create**.
   The new profile with minimum configuration is created and it appears in the **Profiles** page.

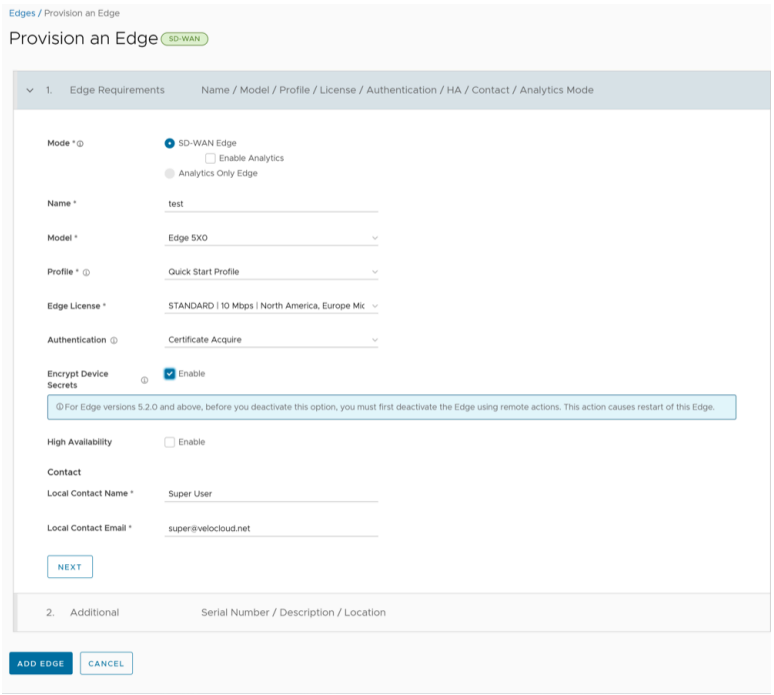
5.5 Provision a New Edge

Enterprise Administrators can provision a single Edge or multiple Edges for Enterprise Customers.

To create a new Edge, perform the following steps:

1. In the **SD-WAN** service of the **Enterprise** portal, select **Configure** > **Edges**.
2. In the **Edges** screen, select **Add Edge**.
   The **Provision an Edge** screen appears.

Figure 5-12: Provision an Edge



3. You can configure the following options:

Table 10: Provision an Edge- Options and Descriptions

Option	Description
Mode	By default, **SD-WAN Edge** mode is selected.
Name	Enter a unique name for the Edge.
Model	Select an Edge model from the drop-down menu.
Profile	Select a Profile to be assigned to the Edge, from the drop-down menu.  **Note:** If an **Edge Staging Profile** is displayed as an option due to Edge Auto-activation, it indicates that this Profile is used by a newly assigned Edge, but has not been configured with a production Profile.
Edge License	Select an Edge license from the drop-down menu. The list displays the licenses assigned to the Enterprise, by the Operator.

Option	Description
Authentication	Choose the mode of authentication from the drop-down menu: • **Certificate Deactivated**: Edge uses a pre-shared key mode of authentication. **Warning:** This mode is not recommended for any customer deployments. • **Certificate Acquire**: This mode is selected by default and is recommended for all customer deployments. With **Certificate Acquire** mode, certificates are issued at the time of Edge activation and renewed automatically. The Orchestrator 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**, if needed. • **Certificate Required**: This mode is only appropriate for customer enterprises that are "static". A static enterprise is defined as one where no more than a few new Edges are likely to be deployed and no new PKI oriented changes are anticipated. **Important: Certificate Required** has no security advantages over **Certificate Acquire**. Both modes are equally secure and a customer using **Certificate Required** should do so only for the reasons outlined in this section. **Certificate Required** mode means that no Edge heartbeats are accepted without a valid certificate. **CAUTION:** Using this mode can cause Edge failures in cases where a customer is unaware of this strict enforcement. With this mode, the Edge uses the PKI certificate. Operators can change the certificate renewal time window for Edges by editing the Orchestrator's System Properties. For additional information, contact your Operator. **Note:** • With the Bastion Orchestrator feature enabled, the Edges that are to be staged to Bastion Orchestrator should have the authentication mode set to either **Certificate Acquire** or **Certificate Required**. • When an Edge certificate is revoked, the Edge is deactivated and needs to go through the activation process. The current QuickSec design checks certificate revocation list (CRL) time validity. The CRL time validity must match the current time of Edges for the CRL to have impact on new established connection. To implement this, ensure the Orchestrator time is updated properly to match with the date and time of the Edges.
Encrypt Device Secrets	Select the **Enable** check box to allow the Edge to encrypt the sensitive data across all platforms. This option is also available on the Edge **Overview** page. **Note:** For Edge versions 5.2.0 and above, before you deactivate this option, you must first deactivate the Edge using remote actions. This causes restart of the Edge.
High Availability	Select the **Enable** check box to apply High Availability (HA). Edges can be installed as a single standalone device or paired with another Edge to provide High Availability (HA) support.
Local Contact Name	Enter the name of the site contact for the Edge.

Option	Description
Local Contact Email	Enter the email address of the site contact for the Edge.

4. Enter all the required details and select **Next** to configure the following additional options:

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

Table 11: Additional Options

Option	Description
Serial Number	Enter the serial number of the Edge. If specified, the Edge must display this serial number on activation. **Note:** When deploying virtual VeloCloud Edges on AWS Edges, make sure to use the instance ID as the serial number for the Edge.
Description	Enter an appropriate description.
Location	Select the **Set Location** link to set the location of the Edge. If not specified, the location is auto-detected from the IP address when the Edge is activated.

5. Select **Add Edge**.
   The Edge gets provisioned with an activation key.

> **Note:** The activation key expires in one month if the Edge device is not activated against it.

After you have provisioned an Edge, the Edge appears in the **Edges** screen.

Chapter 6

Stage an Edge to Bastion Orchestrator

- Ensure you have configured two Orchestrators as a Bastion pair. For steps, see Configure Bastion Orchestrator.
- Ensure you have set up the Production Orchestrator to support Bastion configurations. For steps, see Set up Production Orchestrator.
- Ensure you have created a Bastion profile with a minimum configuration in the Production Orchestrator, for the purpose of staging an Enterprise customer to Bastion Orchestrator.
- Ensure you have uploaded the Software and Firmware images related to the provisioned Edge from your local repository to the Orchestrator portal. For steps to upload Firmware and Software images, see the *Firmware Images* and *Software Images* sections in the *Arista VeloCloud SD-WAN Operator Guide*.

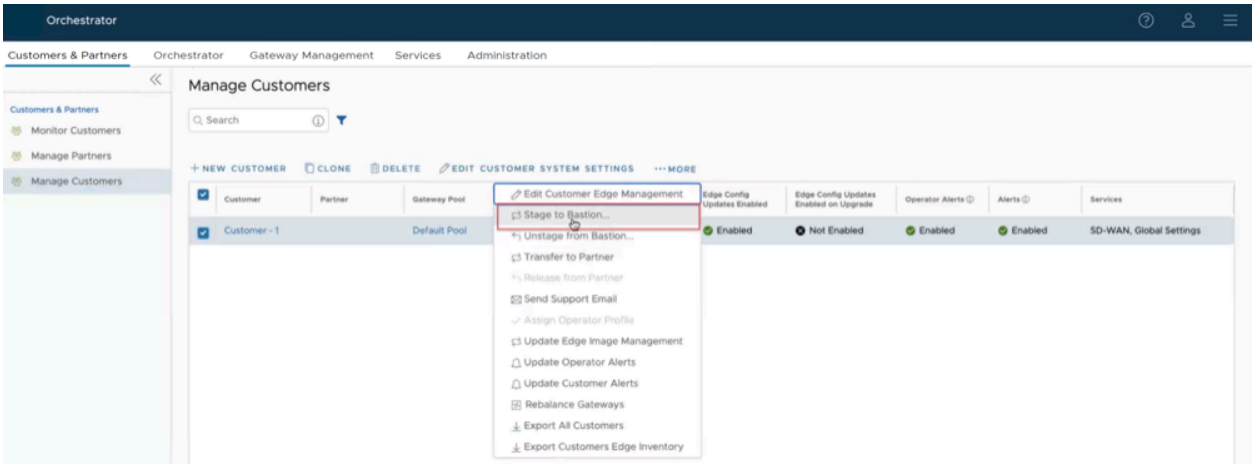
Starting with the 5.4 release, while you stage the SD-WAN Edge to Bastion Orchestrator, you now have an option in the UI to configure and send the Edge upgrade related information to the Bastion Orchestrator. This allows the Edge to get upgraded immediately after the Edge is activated against the Bastion Orchestrator.

Note: Only SD-WAN Edge that are not activated can be staged to the Bastion Orchestrator.

To stage a SD-WAN Edge to Bastion Orchestrator along with Edge upgrade settings, perform the following steps.

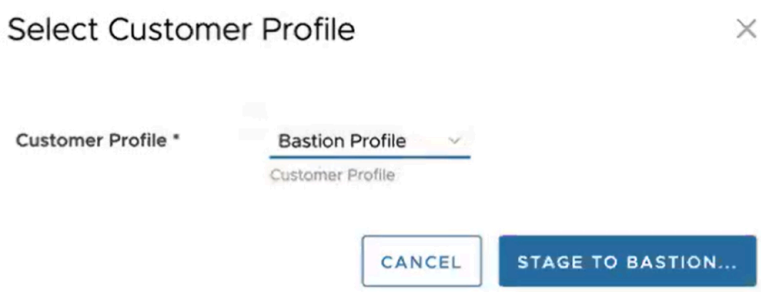
1. In a web browser, launch the Production Orchestrator and login as an Operator user.
2. Before you stage a SD-WAN Edge to Bastion Orchestrator, you must first stage an Enterprise associated with the Edge to the Bastion Orchestrator. In the Operator portal, select **Customers & Partners** > **Manage Customers**.

   Figure 6-1: Staging an Enterprise to Bastion Orchestrator



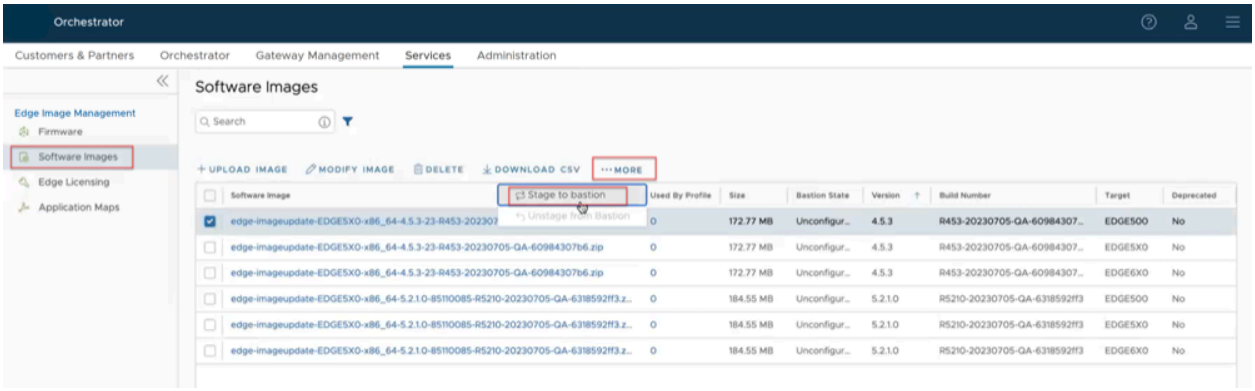
3. Select an Enterprise customer to stage to Bastion Orchestrator and select **More** > **Stage to Bastion**. The **Select Customer Profile** pop-up window appears.

   Figure 6-2: Selecting a Customer Profile



4. From the **Customer Profile** drop-down menu, select a Bastion profile (minimum configuration profile created for staging purpose) to stage along with the customer and select **Stage to Bastion**. The selected Enterprise customer is staged along with the Bastion profile to the Bastion Orchestrator. Now, you can stage software images related to the provisioned Edge to the Bastion Orchestrator.
5. To stage the software images related to the provisioned Edge to the Bastion Orchestrator, select **Services** > **Software Images**. The **Software Images** page appears.

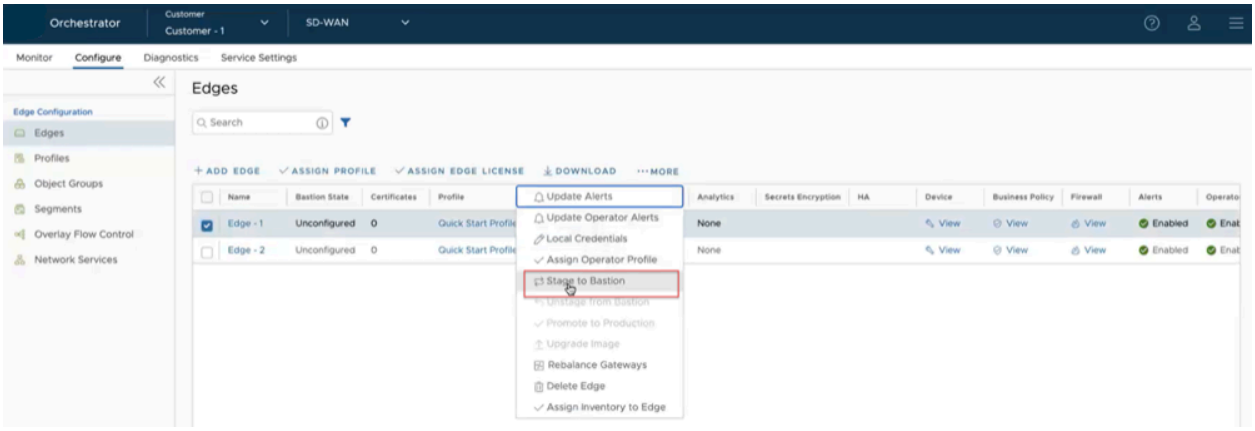
   Figure 6-3: Selecting a Software Image to Stage to Bastion Orchestrator



6. Select a software image to stage to Bastion Orchestrator and select **More** > **Stage to Bastion**. All the associated software images are staged to the Bastion Orchestrator.

7. To stage a SD-WAN Edge to the Bastion Orchestrator with Edge upgrade information, select the Edge and select **More** > **Stage to Bastion**.

   Figure 6-4: Selecting an Edge to Stage to Bastion Orchestrator



8. In the **Stage to Bastion** pop-up window, select the **Upgrade edge after activation** check box and select the image type and version to upgrade the Edge after activation, and select **Submit**.

   Figure 6-5: Stage to Bastion Window

9. The selected Edge along with the Edge upgrade information is staged to the Bastion Orchestrator and it is ready to be activated and upgraded.

   You can view the Bastion state and status of the Edge from the **Monitor** > **Network Overview** page. For additional information, see Monitor Bastion Orchestrator Configuration and Events.

   The selected Edge is staged to the Bastion Orchestrator. You can view the staged Edges under **Activity Monitor** in the **Bastion Orchestrator Configuration** screen.

10. To remove a staged Edge from the Bastion Orchestrator, select **More** > **Unstage from Bastion**.

- Activate the SD-WAN Edge Against the Bastion Orchestrator

Stage a Gateway to Bastion Orchestrator

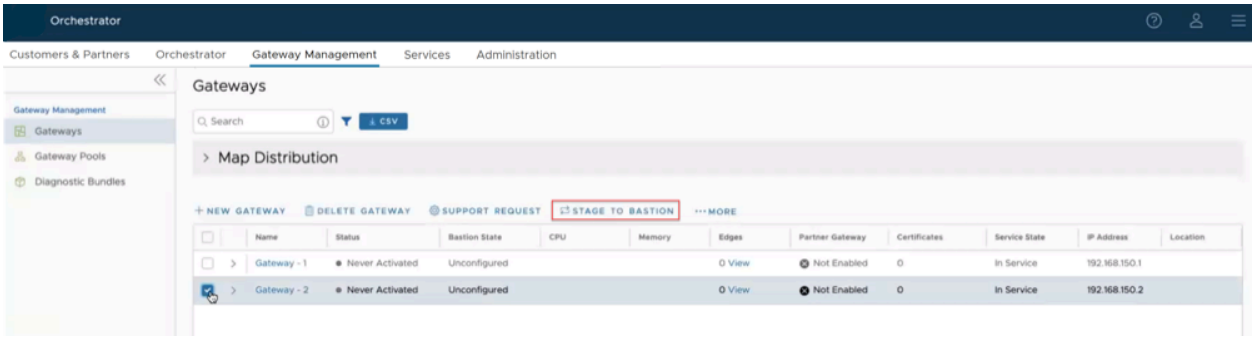
Optionally, an Operator user can stage a SD-WAN Gateway to Bastion Orchestrator.

- Ensure you have configured two Orchestrators as a Bastion pair. For steps, see Configure Bastion Orchestrator.
- Ensure you have set up the Production Orchestrator to support Bastion configurations. For steps, see Set up Production Orchestrator.

To stage a SD-WAN Gateway to Bastion Orchestrator, perform the following steps.

1. In a web browser, launch the Production Orchestrator and login as an Operator user.
2. In the **Operator** portal, select the **Gateway Management** tab from the top menu and then select **Gateways** from the left navigation menu.
3. Select a SD-WAN Gateway to stage to the Bastion Orchestrator and select **Stage to Bastion**.

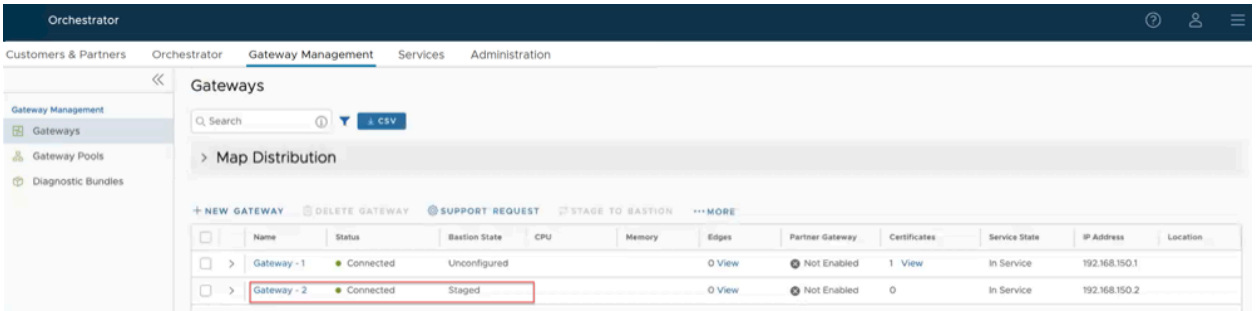
Figure 7-1: Selecting a Gateway to Stage to Bastion



Note: You can stage only a SD-WAN Gateway that is used by a non-activated Edge to the Bastion Orchestrator.

The selected Gateway is staged to the Bastion Orchestrator as shown in the following screenshot.

Figure 7-2: Staging a Gateway to Bastion Orchestrator



4. To remove a staged Gateway from the Bastion Orchestrator, select **More** > **Unstage from Bastion**.

Chapter 8

Activate the SD-WAN Edge Against the Bastion Orchestrator

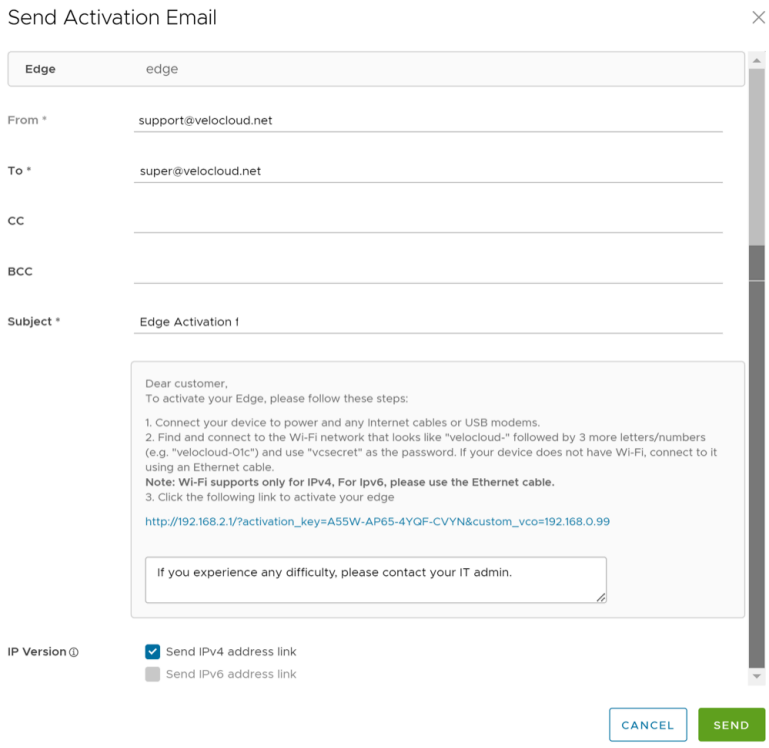
Once a SD-WAN Edge is staged to Bastion Orchestrator, an Operator user can activate the Edge against the Bastion Orchestrator. The process of activating the Edge begins with the initiation of an Edge activation procedure e-mail that is sent to the Site Contact by the IT Admin.

Ensure that the SD-WAN Edge to be activated is in Staged Bastion state.

To send the activation procedure email:

1. In the **Enterprise** portal of the Production Orchestrator, go to **Configure** > **Edges**.
2. Select on a Staged Edge you want to activate. The **Edge Overview** page appears.
3. Select the **Overview** tab and in the **Edge Status** area, select **Send Activation Email**. A **Send Activation Email** dialog box appears with a suggested email to be sent to a Site Contact. Simple instructions are provided for the Site Contact to connect and activate the Edge.

   Figure 8-1: Activating an SD-WAN Edge



4. Select **Send** to send the Edge activation procedure email to the Site Contact. On receiving the Edge activation email, the Site Contact performs the steps outlined in the activation email to connect and activate the Staged Edge to Bastion Orchestrator.

   During the Edge activation process, the Staged Edge will download the configurations from the Production Orchestrator via a secure channel and will activate the Edge against the Bastion Orchestrator. You can view the activation status of the Edge from the **Monitor** > **Network Overview** page. The Edges that are

activated against the Bastion Orchestrator will have **Status** as `Connected` in Green color and **Bastion State** as `Staged`.

For additional information, see Monitor Bastion Orchestrator Configuration and Events.

Note: If an Edge activated against the Bastion Orchestrator is unstaged, users will not be able to stage it again. The workaround is to delete the already activated Edge, add a new Edge and then stage it to the Bastion Orchestrator.

- Promote an Activated Edge from Bastion Orchestrator to Production Orchestrator

Chapter 9

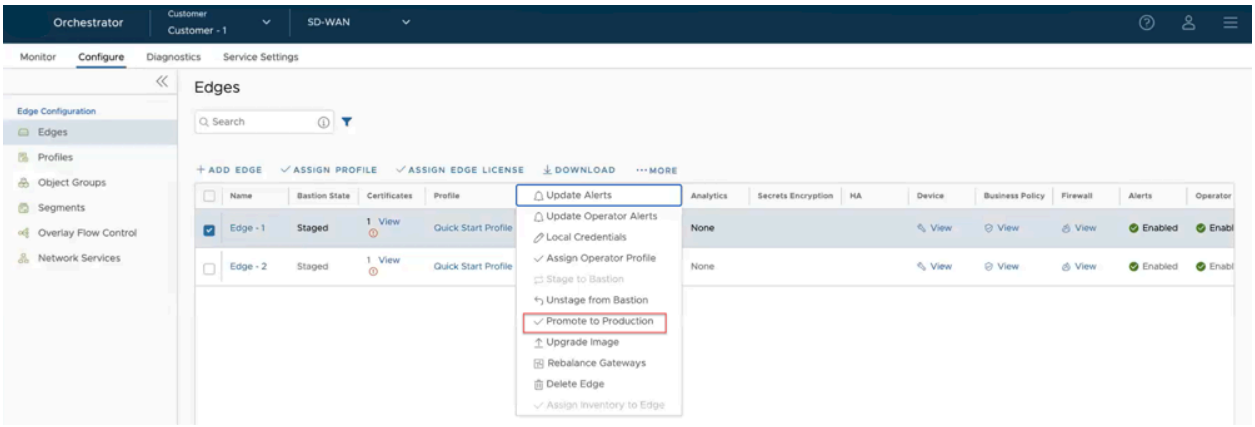
Promote an Activated Edge from Bastion Orchestrator to Production Orchestrator

Once a SD-WAN Edge is activated successfully and it is ready for routing network traffic, you can promote the activated Edge from the Bastion Orchestrator to the Production Orchestrator through a secure channel.

To promote the activated SD-WAN Edge from the Bastion Orchestrator to the Production Orchestrator:

1. In the **Enterprise** portal of the **Production Orchestrator**, go to **Configure** > **Edges**.
2. Select a SD-WAN Edge to be promoted and select **More** > **Promote to Production**.

   Figure 9-1: Selecting an Edge to Promote to Production



   The selected Edge is promoted to the Production Orchestrator and will be assigned with the Production profile that is used during Edge provisioning. You can view the Bastion state and status of the Edge from the **Monitor** > **Network Overview** page. For additional information, see Monitor Bastion Orchestrator Configuration and Events.

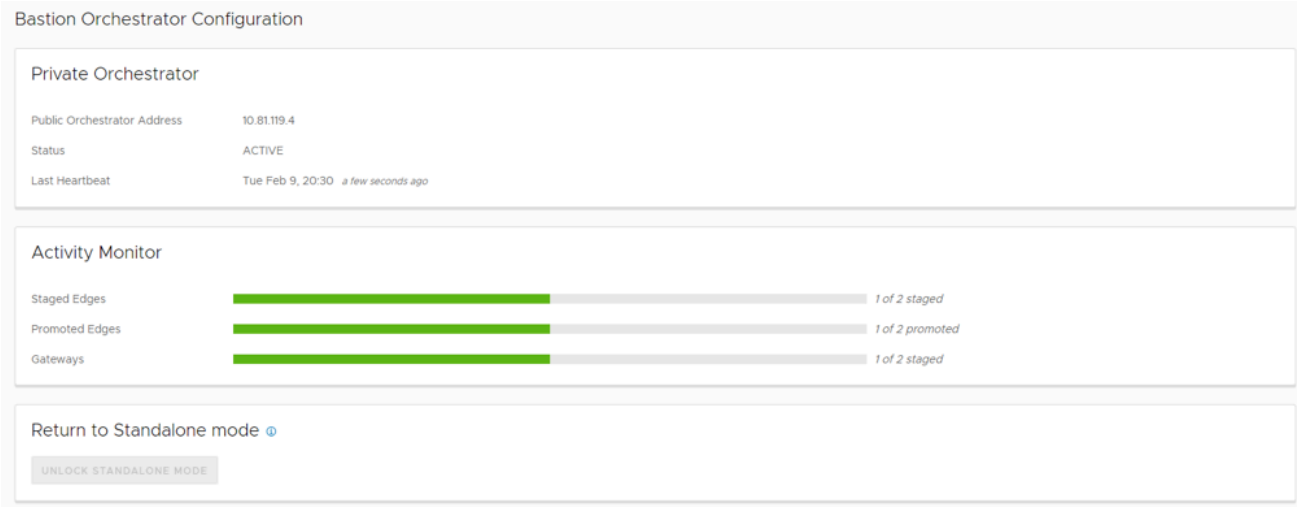
Once the SD-WAN Edge is promoted to Production Orchestrator, all the information such as Enterprise customer details, Edge details, Bastion profile, and Operator users (other than the single Super user indicated on the Private configuration page) will be removed from the Bastion Orchestrator.

In the Production Orchestrator UI, under the **Activity Monitor** area in the **Bastion Orchestrator Configuration** page, you can find the following details:

- Count of Staged Edges out of the total number of Edges configured for an Enterprise.
- Count of Promoted Edges out of the total number of Edges configured for the Enterprise.

- Count of Staged Gateways out of the total number of Gateways configured for the Enterprise.

Figure 9-2: Displaying the Activity Monitor of Edges



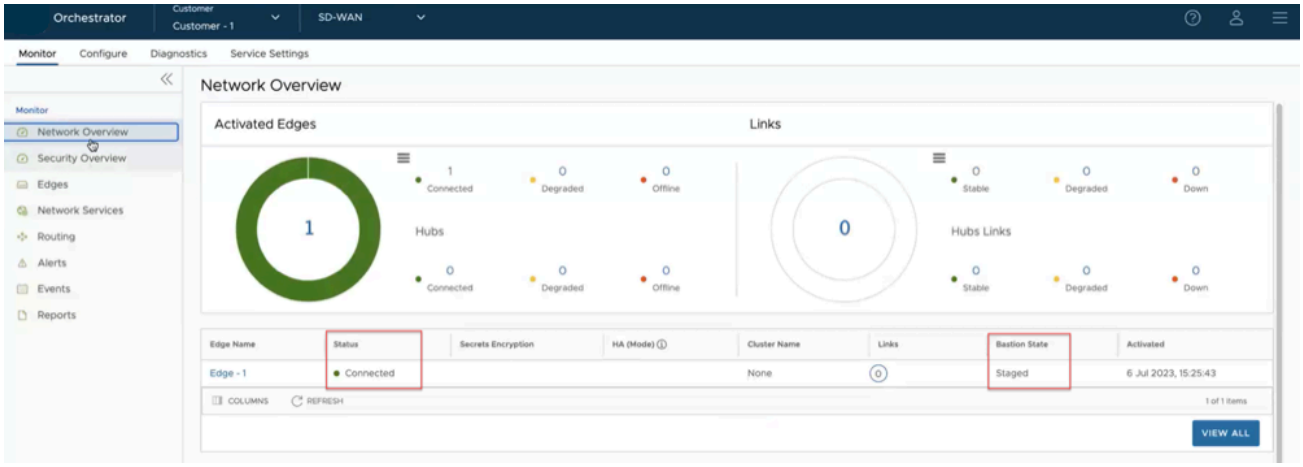
Chapter 10

Monitor Bastion Orchestrator Configuration and Events

VeloCloud Orchestrator allows an Enterprise user to monitor the status of SD-WAN Edges and their Bastion states from the **Monitor** > **Network Overview** page.

Selecting **Monitor** > **Network Overview** in the navigation panel opens the **Network Overview** screen. In the Summary dashboard table, a new column **Bastion State** is added to display Bastion state for the SD-WAN Edges.

Figure 10-1: Displaying Activated Edges



Based on the Edge status and Bastion state, you can infer if a SD-WAN Edge is activated against a Bastion or Production Orchestrator:

- When a SD-WAN Edge is activated against a Bastion Orchestrator then the Edge status appears as `Connected` in Green color and the Bastion state transitions to `Staged`.
- When a SD-WAN Edge is activated against a Production Orchestrator then the Edge status appears as `Connected` in Green color and the Bastion state transitions to `Unconfigured`.

SD-WAN Edge Bastion States and Transitions

Transitions are driven by Edge heartbeats (which occur under normal circumstances every 15 seconds).

The following table describes the Bastion state types and transitions for a SD-WAN Edge.

Table 12: Bastion State Type Descriptions

Bastion State	Description
UNCONFIGURED	The initial state of a SD-WAN Edge before it is staged. The SD-WAN Edge is available only in Production Orchestrator.
STAGE_REQUESTED	An intermediate state before the SD-WAN Edge is staged to Bastion Orchestrator.
STAGED	The SD-WAN Edge is staged to Bastion Orchestrator.
UNSTAGE_REQUESTED	An intermediate state before the SD-WAN Edge is removed from Bastion Orchestrator.
UNSTAGED	The SD-WAN Edge is removed from Bastion Orchestrator and available only in Production Orchestrator.
PROMOTION_REQUESTED	An intermediate state when a user has requested promotion of the SD-WAN Edge from Bastion Orchestrator to Production Orchestrator.
PROMOTION_PENDING	Configuration for the SD-WAN Edge to be promoted has been pushed to the Bastion Orchestrator and is waiting for the Edge to send heartbeat back to the Production Orchestrator.
PROMOTED	The SD-WAN Edge has been successfully promoted and currently heartbeats to the Production Orchestrator.

Orchestrator Events

The following table describes all the Enterprise and Operator events generated in a Bastion Orchestrator configuration setup.

Table 13: Enterprise and Operator Events

Event Type	Event	Displayed on Orchestrator UI As	Severity	Generated By	Generated When
Operator Event	BASTION_ STATE_UPDATED	${*entity*} ${*name*} bastion state changed from {*from state*} to {*to state*}. Where,{*entity*} could be a Gateway or Enterprise and {*from state*} and {*to state*} could be one of the following: • STAGE_REQUESTED • STAGED • UNSTAGE_REQUESTED • UNSTAGED	INFO/ERROR	Orchestrator	The Bastion state transitions from one state to another.
Operator Event	MANAGED_ VCO_ACTIVATED	Activated the managed VCO {*IP*}	INFO	Orchestrator	The activation of an Orchestrator is successful.
Operator Event	MANAGED_VCO_ ACTIVATION_FAILED	Failed to activate the managed VCO {*IP*}	ERROR	Orchestrator	The activation of an Orchestrator fails.
Operator Event	VCO_ACTION_ RESPONSE_ PROCESSING_FAILED	Failed to execute the response of action {*action*}. Where, {*action*} could be one of the following: • STAGE_ENTERPRISE • STAGE_EDGE • STAGE_GATEWAY • STAGE_OPERATOR_USER • UNSTAGE_GATEWAY • UNSTAGE_EDGE • UNSTAGE_ENTERPRISE • UNSTAGE_OPERATOR_USER • PROMOTE_EDGE • PROMOTE_EDGE_COMPLETE • STAGED_GATEWAY_UPDATE • STAGED_EDGE_UPDATE • STAGED_ENTERPRISE_UPDATE • STAGED_CONFIGURATION_UPDATE • STAGED_OPERATOR_USER_UPDATE • STAGED_EDGE_ACTIVATED • STAGED_GATEWAY_ACTIVATED	ERROR	Orchestrator	After an action has been executed in the Bastion Orchestrator, the respective response action execution in Production Orchestrator fails.

Event Type	Event	Displayed on Orchestrator UI As	Severity	Generated By	Generated When
Enterprise Event	BASTION_STATE_ UPDATED	${*entity*} ${*name*} bastion state changed from {*from state*} to {*to state*}. Where, {*entity*} could be an Edge or Profile and {*from state*} and {*to state*} could be one of the following: • STAGE_REQUESTED • STAGED • UNSTAGE_REQUESTED • UNSTAGED • PROMOTION_REQUESTED • PROMOTION_PENDING • PROMOTED	INFO/ERROR	Orchestrator	The Bastion state transitions from one state to another.

Chapter 11

RMA Reactivation for Bastion Orchestrator Topology

In a Bastion Orchestrator topology setup, VeloCloud SD-WAN allows RMA reactivation only for activated and promoted SD-WAN Edges to the Production Orchestrator.

You can initiate an RMA reactivation request to:

- Replace a SD-WAN Edge due to a malfunction
- Upgrade a SD-WAN Edge hardware model

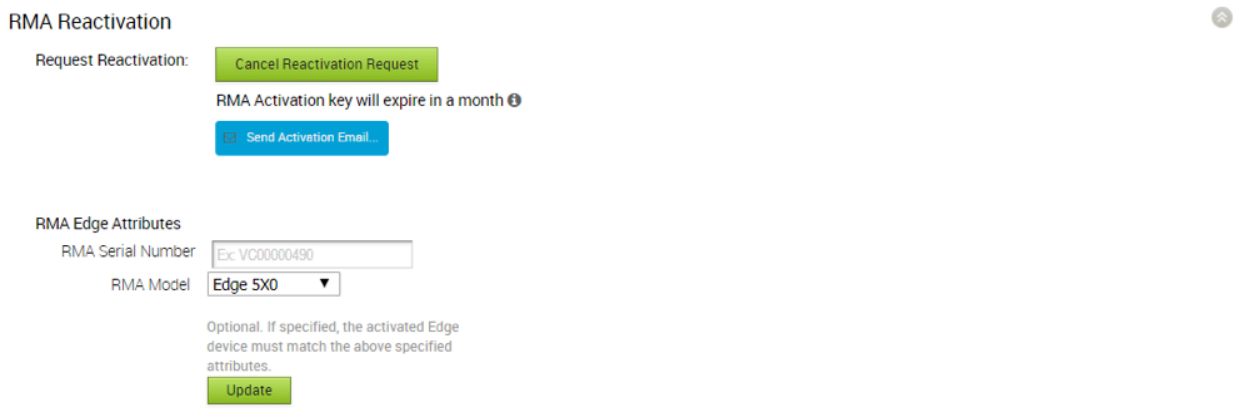
To request Edge RMA reactivation, perform the following steps.

1. Login to the **Orchestrator** and in the **SD-WAN** service of the **Enterprise** portal, go to **Configure** > **Edges**.
2. Select the Edge you want to reactivate.
3. Select the **Overview** tab, go to the **RMA Reactivation** area.
4. Select **Request Reactivation** to generate a new activation key. The status of the SD-WAN Edge changes to **Reactivation Pending** mode. The Bastion state changes to **Staged** and the Edge is pushed back to the Bastion (Public) Orchestrator.

   Note: The reactivation key is only valid for one month.

   When the key expires, a warning message is displayed. To generate a new key, select **Generate New Activation Key** and specify the number of days for the key to be active, and select **Submit**. A new key is generated, and you can reactivate the Edge with the new key

Figure 11-1: Requesting RMA Reactivation



5. Select **Cancel Reactivation Request** to cancel the request. When you cancel the request, the status of the Edge changes to **Activated** mode and the Bastion state changes to **Promoted**.
6. Optionally, in the **RMA Edge Attributes**, you can enter the Serial Number of the Edge. If you are reactivating a different Edge model, choose the model from the RMA model list and select **Update**.

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

7. 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 Bastion Orchestrator.
8. To activate the 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.

   > **Note:** Select the activation link in the email to activate the Edge.

   > **Note:** The Edge downloads the configuration and software from the Bastion Orchestrator and gets activated against it.
9. Select **Save Changes**.

- Promote an Activated Edge from Bastion Orchestrator to Production Orchestrator

Chapter 12

References

12.1 Related Documents

The following documentation is available for ***Arista VeloCloud SD-WAN***:

- *Arista VeloCloud SD-WAN Operator Guide*
- *Arista VeloCloud SD-WAN Administration Guide*
- *Arista VeloCloud SD-WAN Orchestrator Deployment and Monitoring Guide*
- *Arista VeloCloud SD-WAN Gateway Monitoring Guide*
- *Arista VeloCloud SD-WAN Partner Guide*
- *Arista VeloCloud SASE Global Settings 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*