Partner Guide

Arista VeloCloud SD-WAN

Version 6.4

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

About Partner Guide

The*(formerly known as*VMware SD-WAN™) Partner Guide provides information about including how to add and manage Customers who use.

Intended Audience

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

Beginning with Release 4.4.0, is offered as part of. To access SASE documentation for Cloud Web Security and Secure Access, along with Release Notes for version 4.4.0 and later, see Arista VeloCloud SASE.

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 Arista Partner Gateway
4. artner 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

What's New

What's New in Version 6.4.0

Feature	Description
Custom Applications	Partner users can now create Custom Applications and use these applications in Business Policy and Firewall rules creation. For more information, see Configure Custom Applications.
Link Insights	VeloCloud introduces an **Insights** tab in the Partner portal of the Orchestrator. For more information, see Link Insights.
Multi-factor Authentication	A two factor authentication is implemented for Partners. This is similar to the existing Enterprise authentication. For more information, see Authentication.
Network Interface Stats Monitoring	Partner users can now view interface stats, real time stats, and historical interface data, on the **Monitor** > **Edges** > **System** screen of the Orchestrator. For more information, see Network Interface Statistics Monitoring.
Password Policy	Partner users can now set their own password policies directly from the Authentication screen. For more information, see Authentication.

Feature	Description
Role Customization Usability Improvements	The **Service Permissions** tab has been improved for better role customization. For more information, see Service Permissions and New Permission.
Self-Service Orchestrator Branding	VeloCloud Edge Cloud Orchestrator allows Partner users to brand the Orchestrator User Interface (UI) by applying their company's name, logo, and colors at a Partner level. For more information, see Orchestrator Branding - Partner.
User Authentication Security Policy Improvements	Partners can now set their own password policies directly from the Authentication screen. For more information, see Authentication.

Release Notes

For information on all the new/modified features for 6.4.0, see VeloCloud SD-WAN 6.4.0 Release Notes.

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 supports the following browsers:

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

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

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

Partner-level UI Changes in the New SASE Orchestrator

The (formerly known as the Arista SASE Orchestrator) has moved and redesigned some features to fit the wider scope of the product and user interface (UI). The new UI has changed from a single product portal (only for SD-

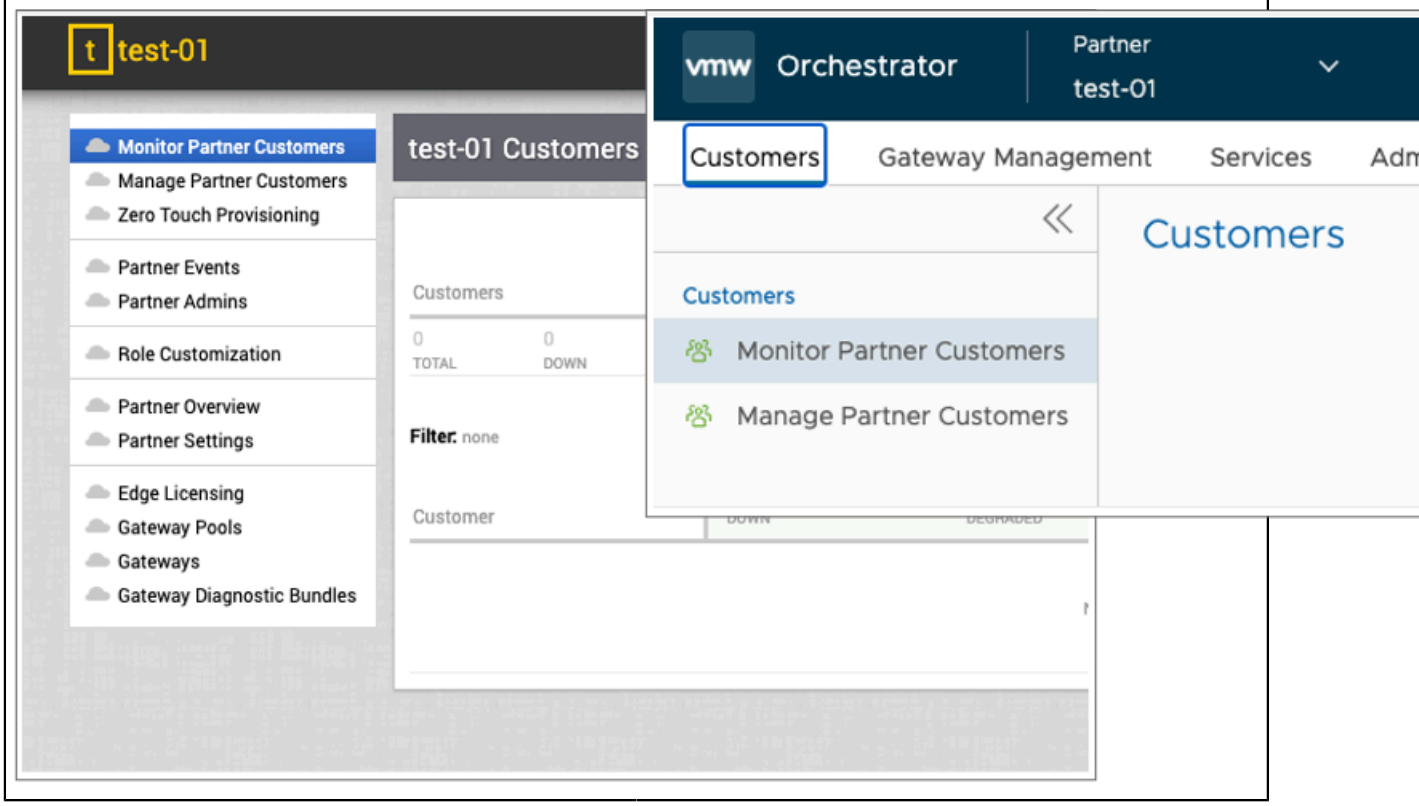
WAN) to a common management system that lets customers access multiple services in one place. These services include,, and . Future services such as Arista Private Mobile Network and Arista Edge Compute Stack will also be added. The new UI navigation has adapted to allow access to multiple services within one shared header. The primary global header now has an **Enterprise Applications** (Services) drop-down menu that lists the various supported services. You can select and navigate to each service from this menu. Enterprise **Global Settings** is now located in the **Enterprise Applications** (Services) drop-down because it has features that are shared across services. These features include User Management, Authentication, Role Customization (now Roles and Service Permissions), Customer Configuration, and more.

This document explains the changes in the Partner UI for some features. It also gives the reasons for these changes.

Monitor Partner Customers

The New UI has a **Customers** tab for Partners to easily monitor and manage their Customer views, including **Monitor Partner Customers**. This helps to organize the navigation better for Partners.

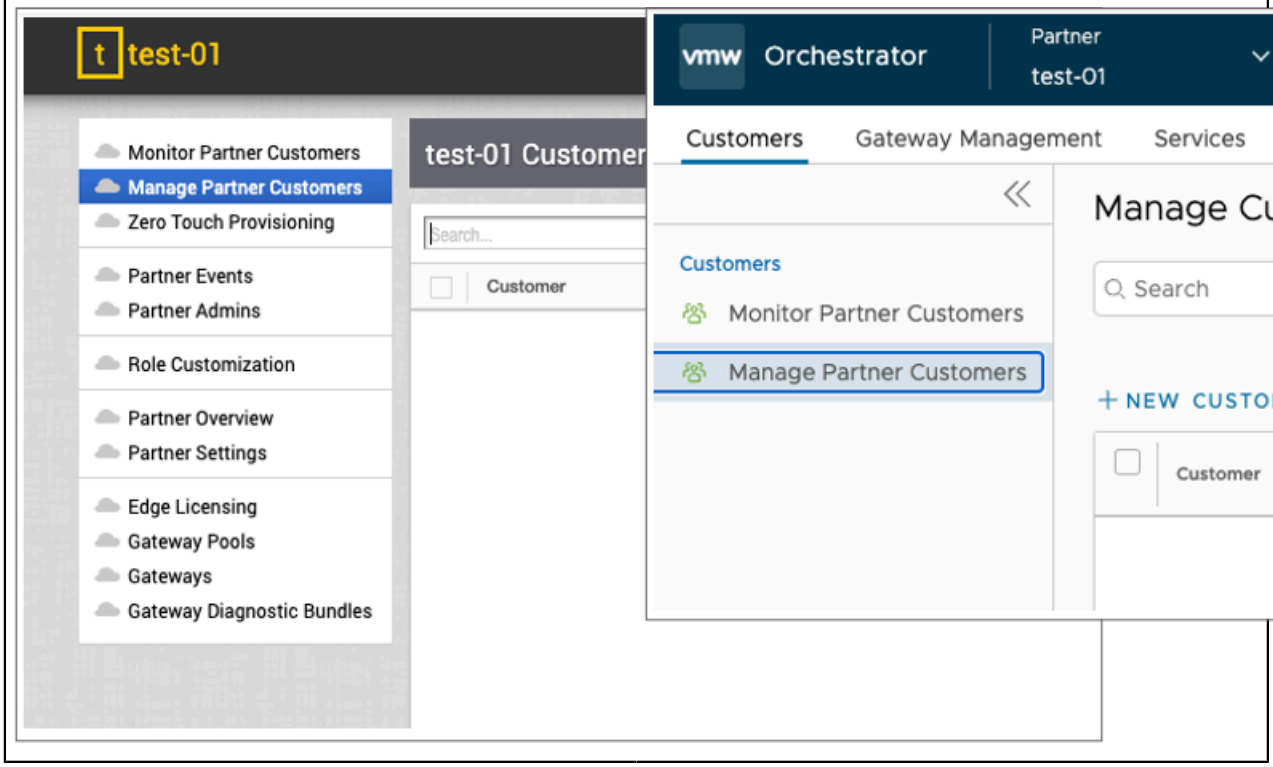
Classic Orchestrator Location	New Orchestrator Location
Partner > Monitor Partner Customers	**Partner > Customers > Monitor Partner Customers**



Manage Partner Customers

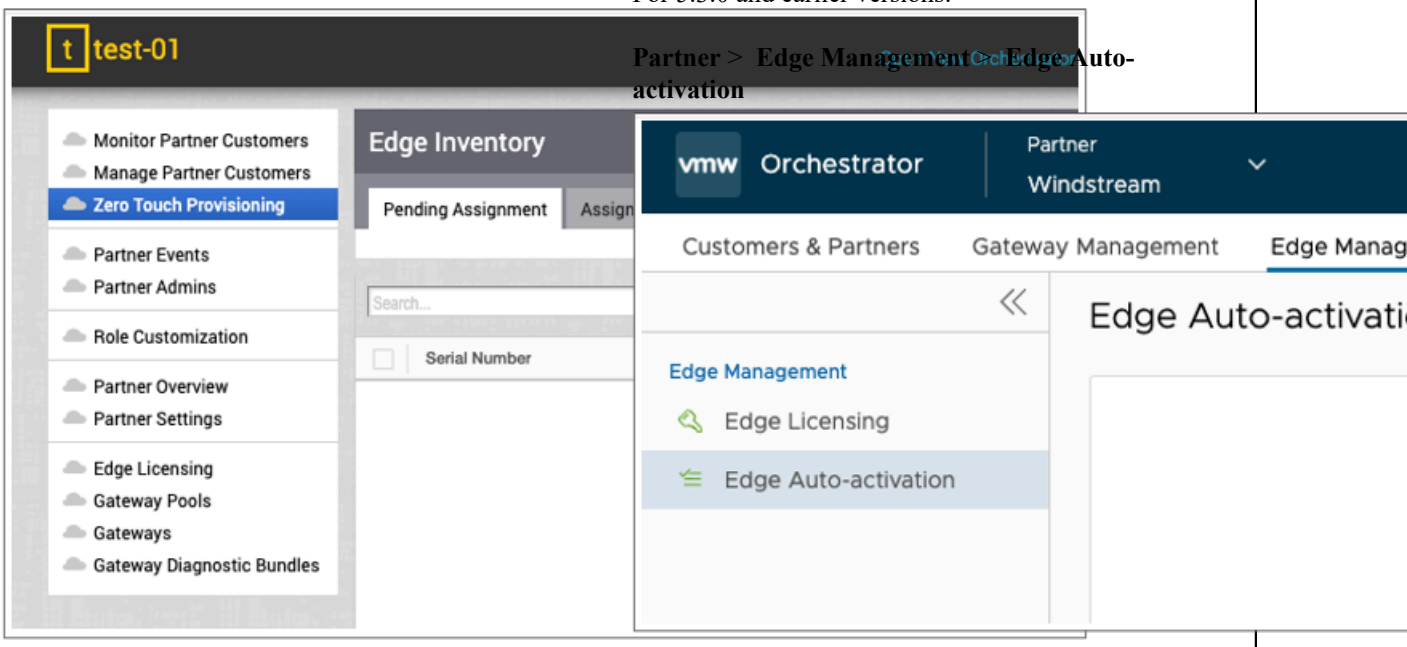
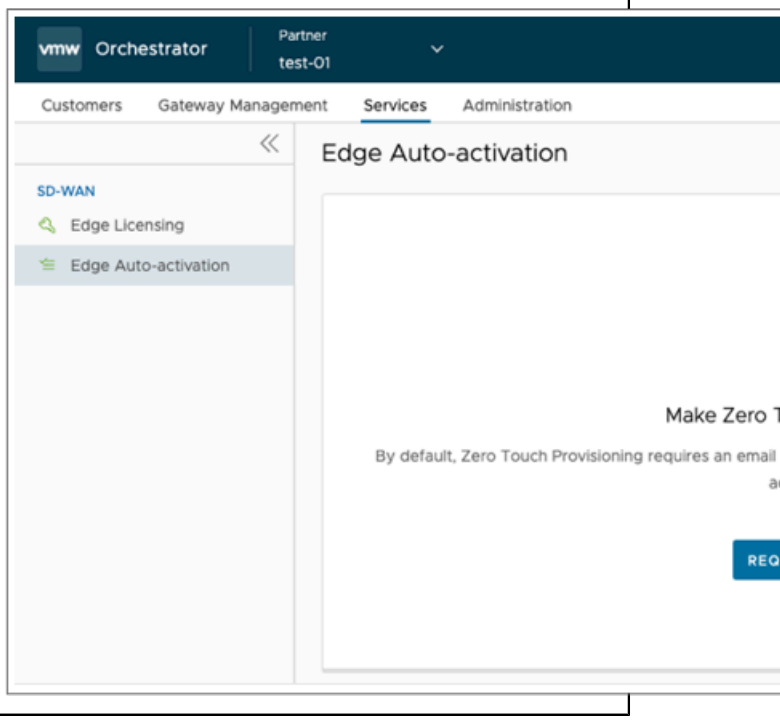
The New UI has a **Customers** tab for Partners to easily monitor and manage their Customer views, including **Manage Partner Customers**. This helps to organize the navigation better for Partners.

Classic Orchestrator Location	New Orchestrator Location
Partner > Manage Partner Customers	**Partner > Customers > Manage Partner Customers**

Classic Orchestrator Location	New Orchestrator Location
	

Zero Touch Provisioning (ZTP)

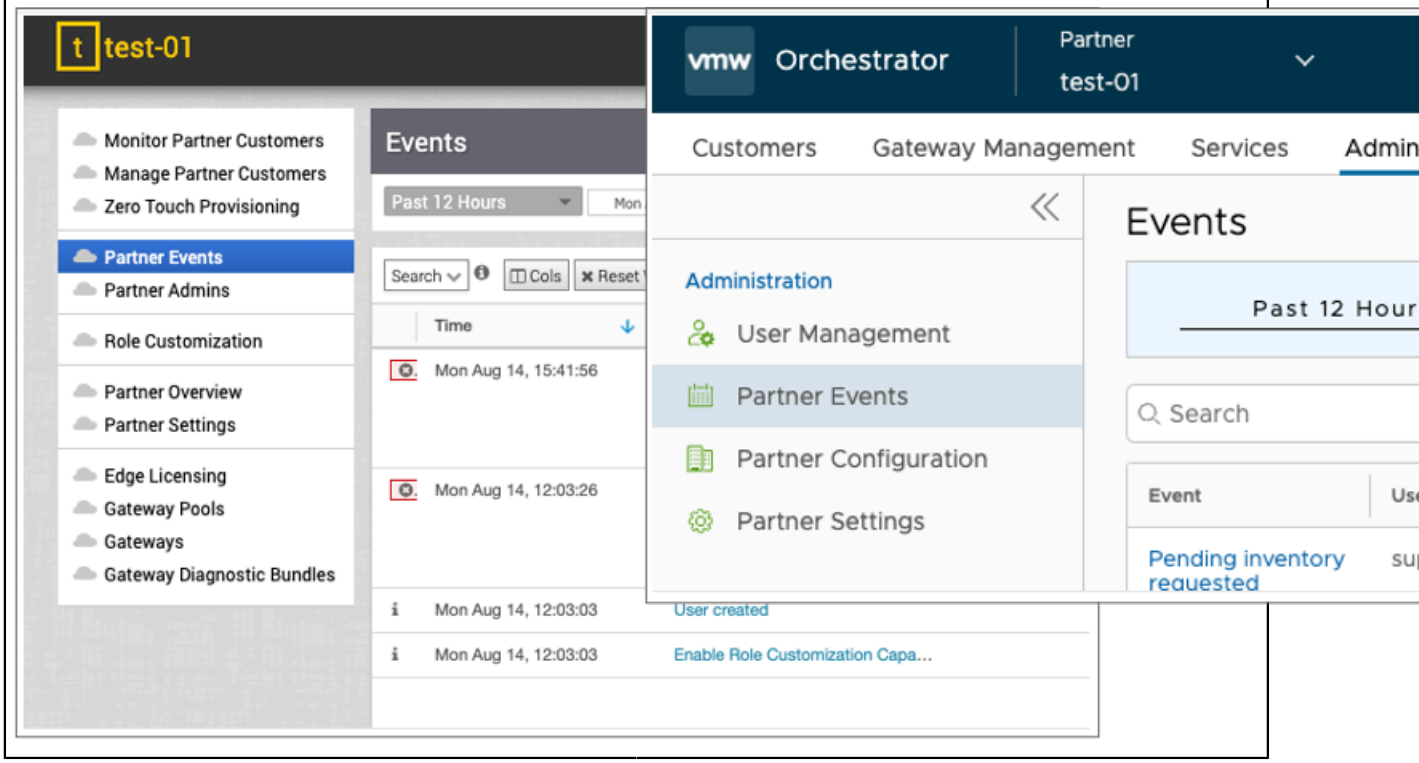
We have improved the way you activate your Edges in the New UI. You no longer need to configure **Zero Touch Provisioning** (ZTP) in the Partner Settings. You can access the ZTP feature directly from the **Edge Auto-Activation** page. We have also renamed the **Zero Touch Provisioning** feature to **Edge Auto-Activation**, because it includes both the new automatic activation method and the original email activation method. You can choose either method from the **Edge Configuration** page.

Classic Orchestrator Location	New Orchestrator Location
Partner > Zero Touch Provisioning	For 5.3.0 and earlier versions: **Partner > Edge Management > Edge Auto-activation**  For 5.4.0 and later versions: **Partner > Services > Edge Auto-activation** 

Partner Events

This feature has moved to a new location because the Classic Orchestrator UI did not have clear navigation and organization of pages. The New Orchestrator puts all the Partner administration-related features under the **Administration** tab.

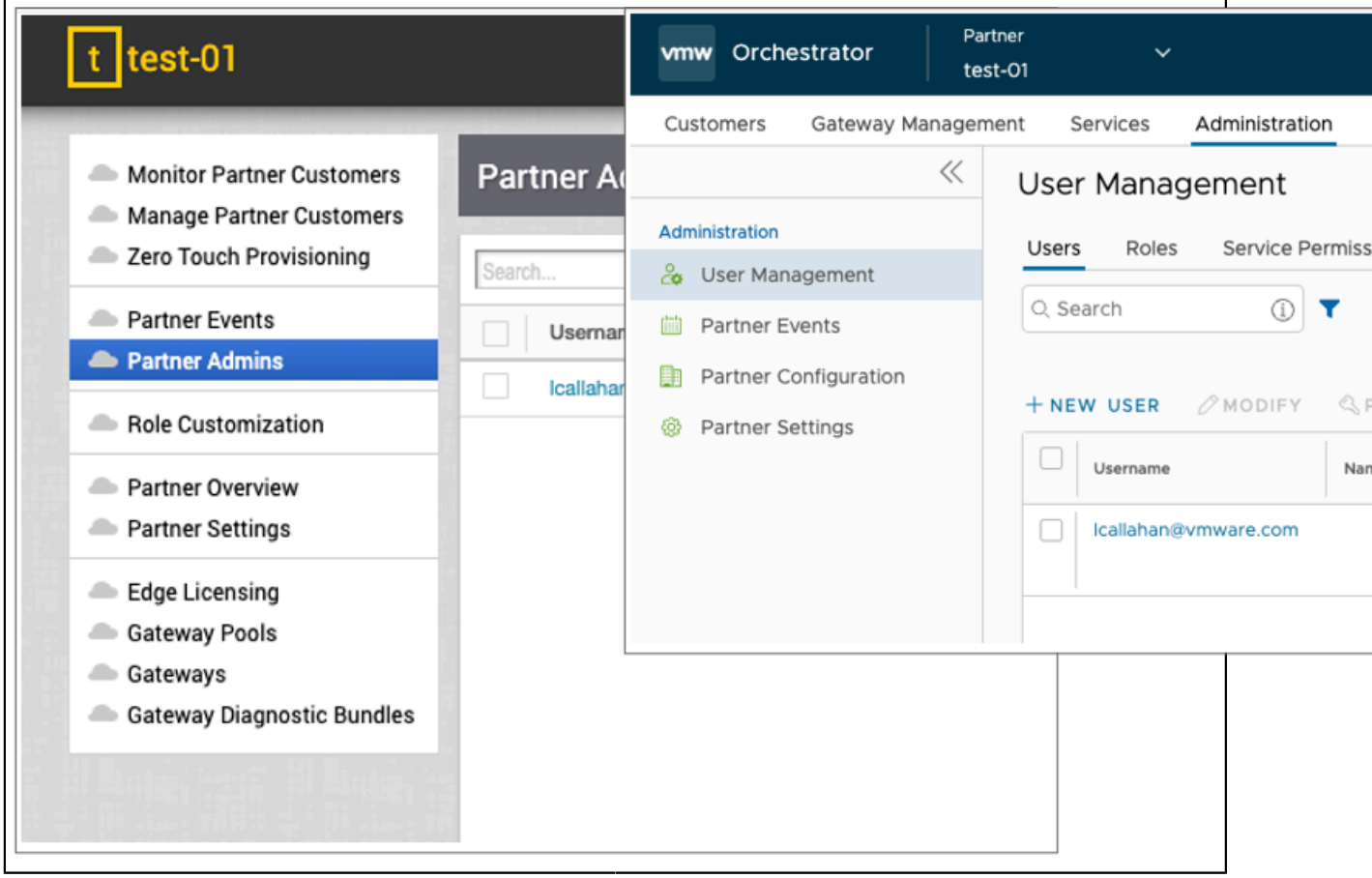
Classic Orchestrator Location	New Orchestrator Location
Partner > Partner Events	**Partner > Administration > Partner Events**



Partner Admins

This feature has moved to a new location because the Classic Orchestrator UI did not have clear navigation and organization of pages. The New Orchestrator puts all the Partner administration-related features under the **Administration** tab.

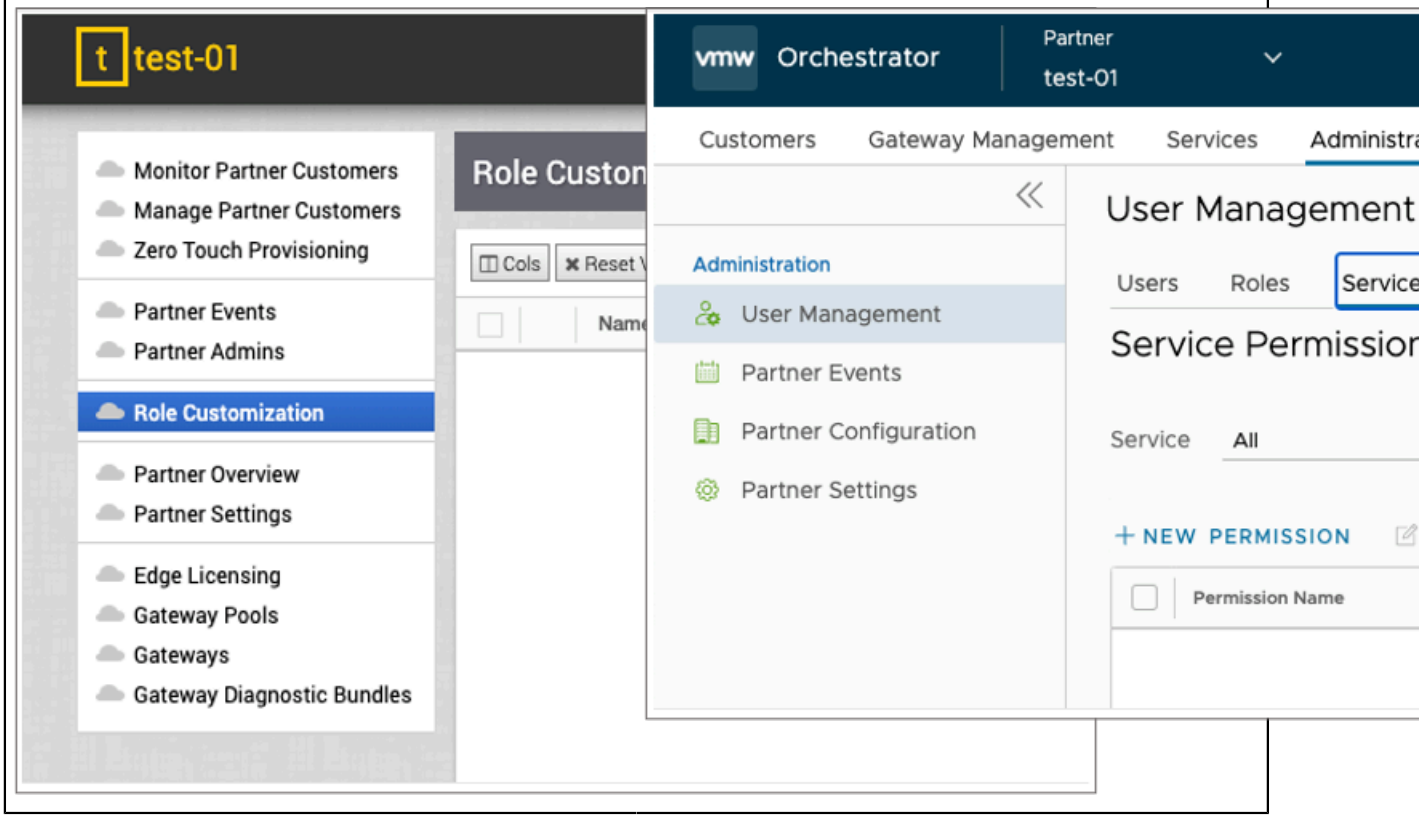
Classic Orchestrator Location	New Orchestrator Location
Partner > Partner Admins	**Partner > Administration > Partner Admins**

Classic Orchestrator Location	New Orchestrator Location
	

Role Customization (Now: Service Permissions)

We have changed the name of the "Role Customization" feature to "Service Permissions". This is to make room for the new Role Builder feature that lets you create custom roles by combining different service permissions. **Service Permissions** is a more accurate name for the feature, as it allows you to adjust the access levels for each service.

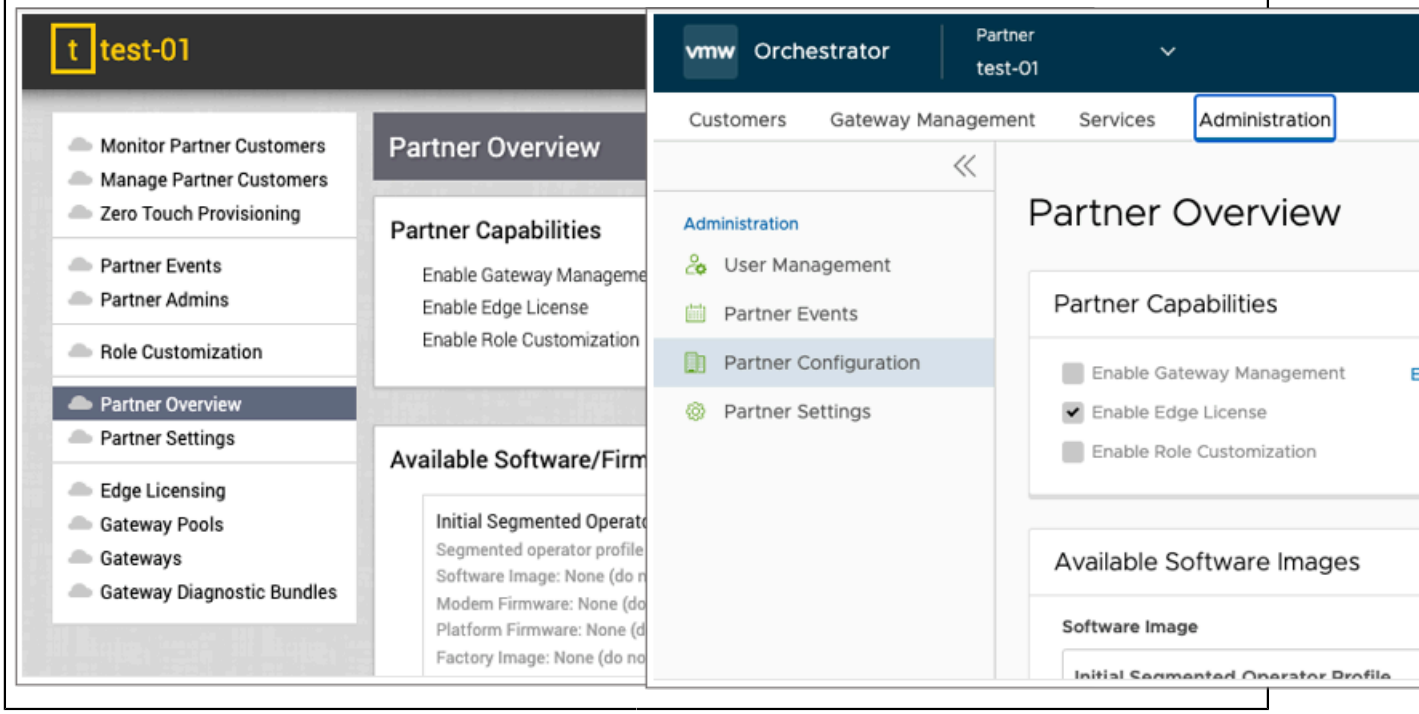
Classic Orchestrator Location	New Orchestrator Location
Partner > **Role Customization**	**Partner** > **Administration** > **User Management** > **Service Permissions**

Classic Orchestrator Location	New Orchestrator Location
	

Partner Overview (Now: Partner Configuration)

We have changed the name of the **Partner Overview** feature to **Partner Configuration**. This is to make it consistent with the **Customer Configuration** page at the Enterprise level. Both features are similar, as they allow you to manage the settings and preferences for your Partners and Customers.

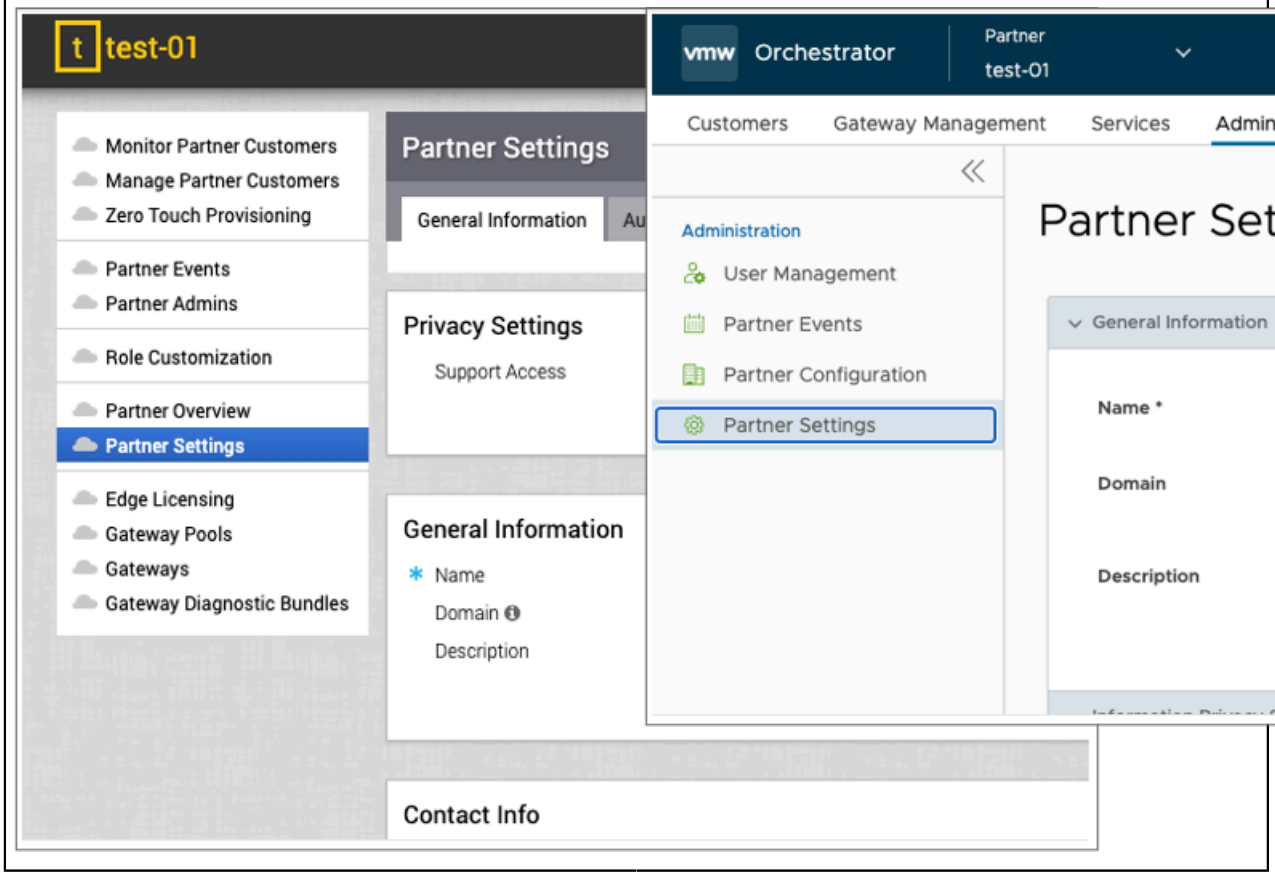
Classic Orchestrator Location	New Orchestrator Location
Partner > Partner Overview	**Partner > Administration > Partner Configuration**

Classic Orchestrator Location	New Orchestrator Location
	

Partner Settings

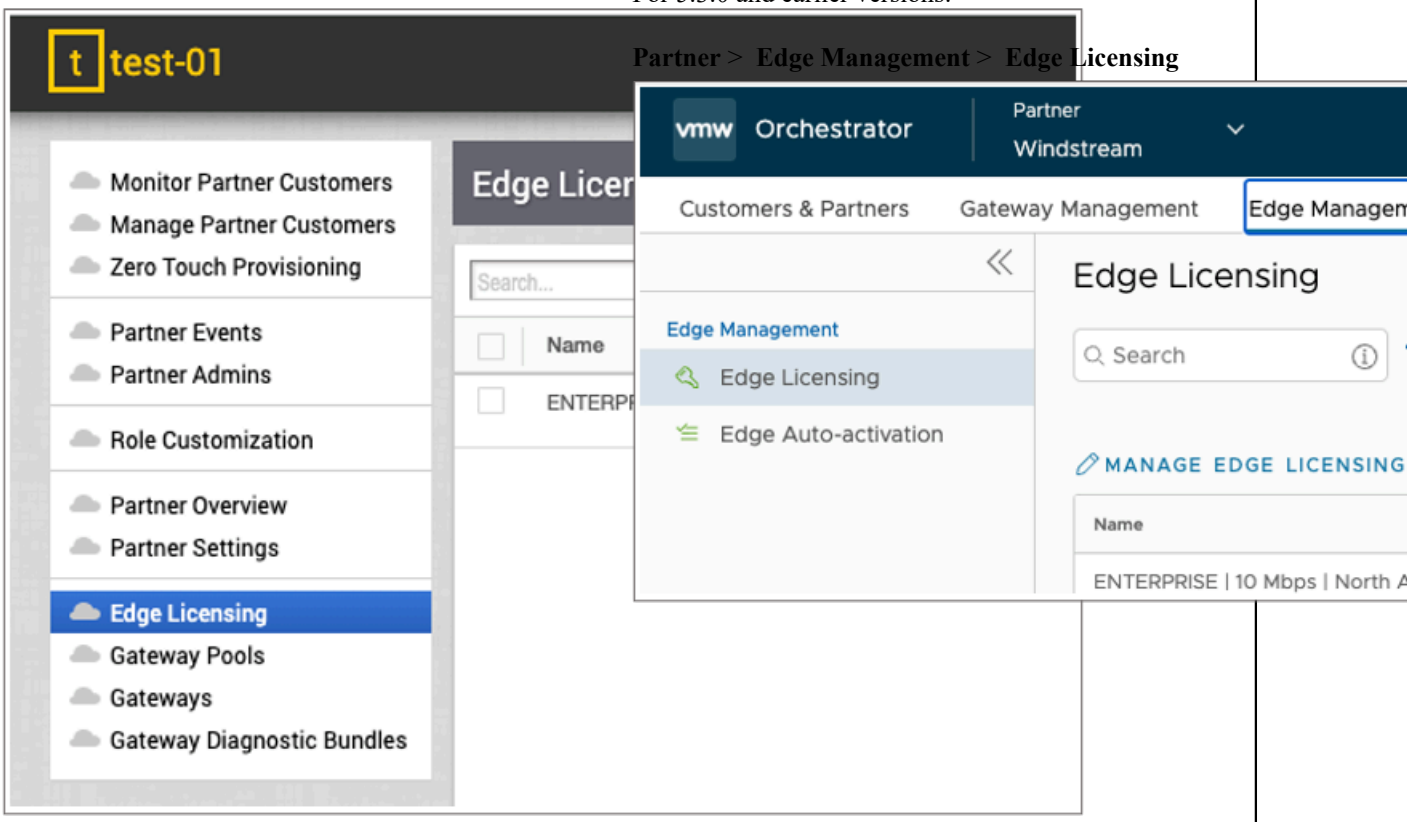
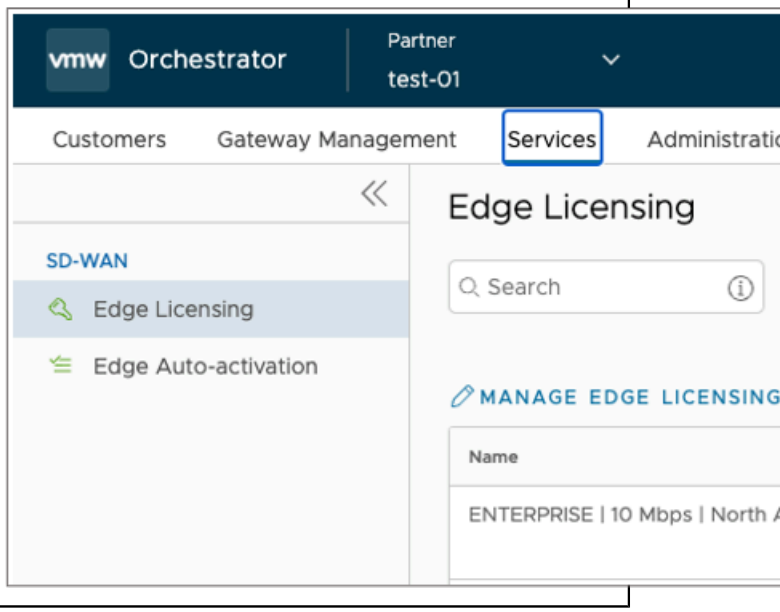
We have moved the **Partner Settings** feature from the Classic Orchestrator UI to the **Administration** tab in the New Orchestrator UI. This is because the **Partner Settings** feature is related to the other **Administration** settings like **User Management**, **Partner Events**, and **Partner Configuration**.

Classic Orchestrator Location	New Orchestrator Location
Partner > Partner Settings	**Partner > Administration > Partner Settings**

Classic Orchestrator Location	New Orchestrator Location
	

Edge Licensing

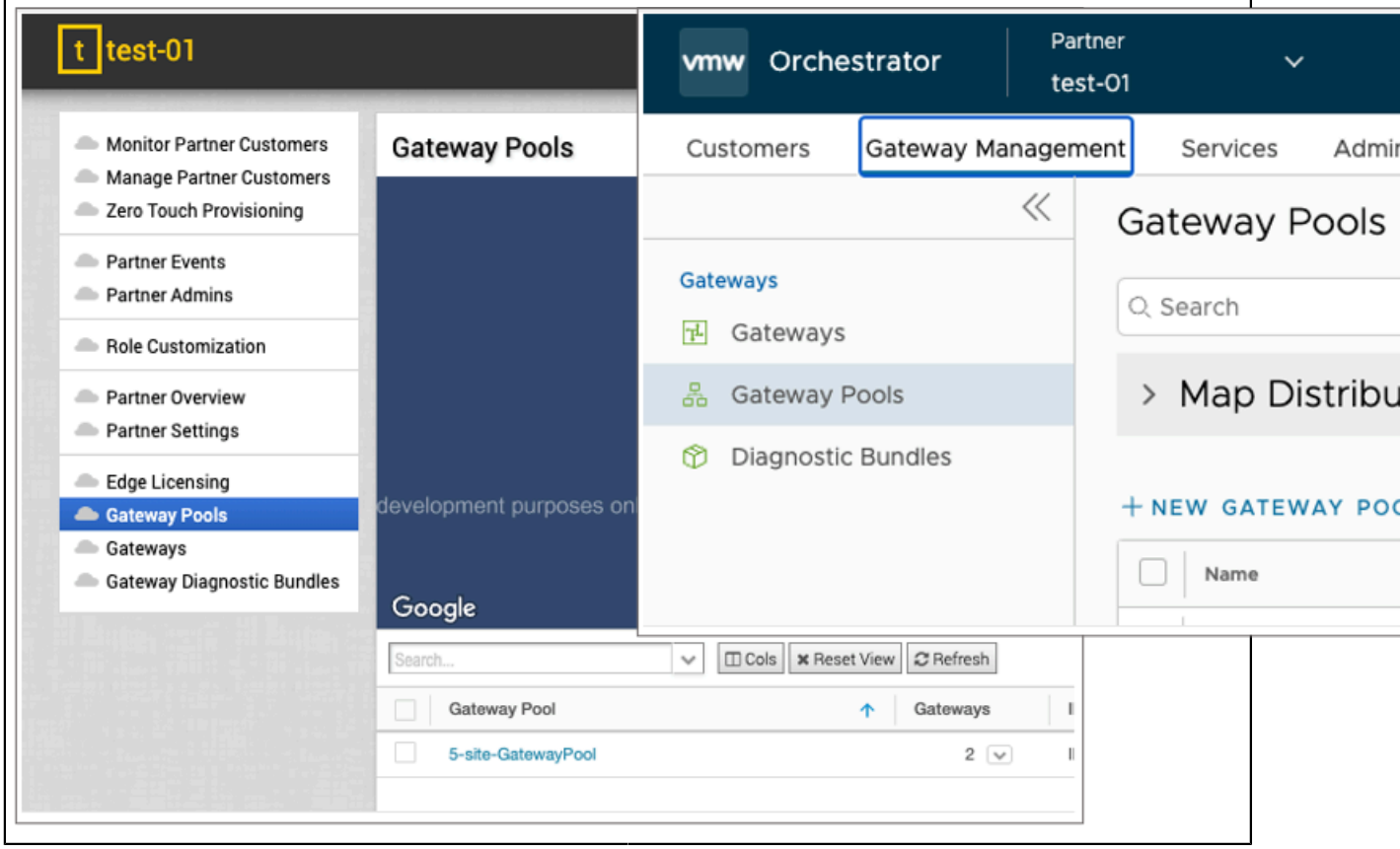
We have moved the Edge Licensing feature from the Classic Orchestrator UI to the **Edge Management** tab (for Release 5.3.0 and earlier), and the **Services** tab (for Release 5.4.0 and later) in the New Orchestrator UI. This is because the Classic Orchestrator UI could not handle multiple services that need configuration at the Partner level. The **Services** tab allows you to manage different service settings, such as SD-WAN features. **Edge Licensing** and **Edge Auto-activation** are two examples of SD-WAN features that you can find under the **Services** tab.

Classic Orchestrator Location	New Orchestrator Location
Partner > Edge Licensing	For 5.3.0 and earlier versions: **Partner > Edge Management > Edge Licensing**  For 5.4.0 and later versions: **Partner > Services > Edge Licensing** 

Gateway Pools

We have moved the **Gateway Pools** feature because the Classic Orchestrator UI had poor navigation and page layout. The New Orchestrator UI has an improved design that groups all Gateway related features under the **Gateway Management** tab.

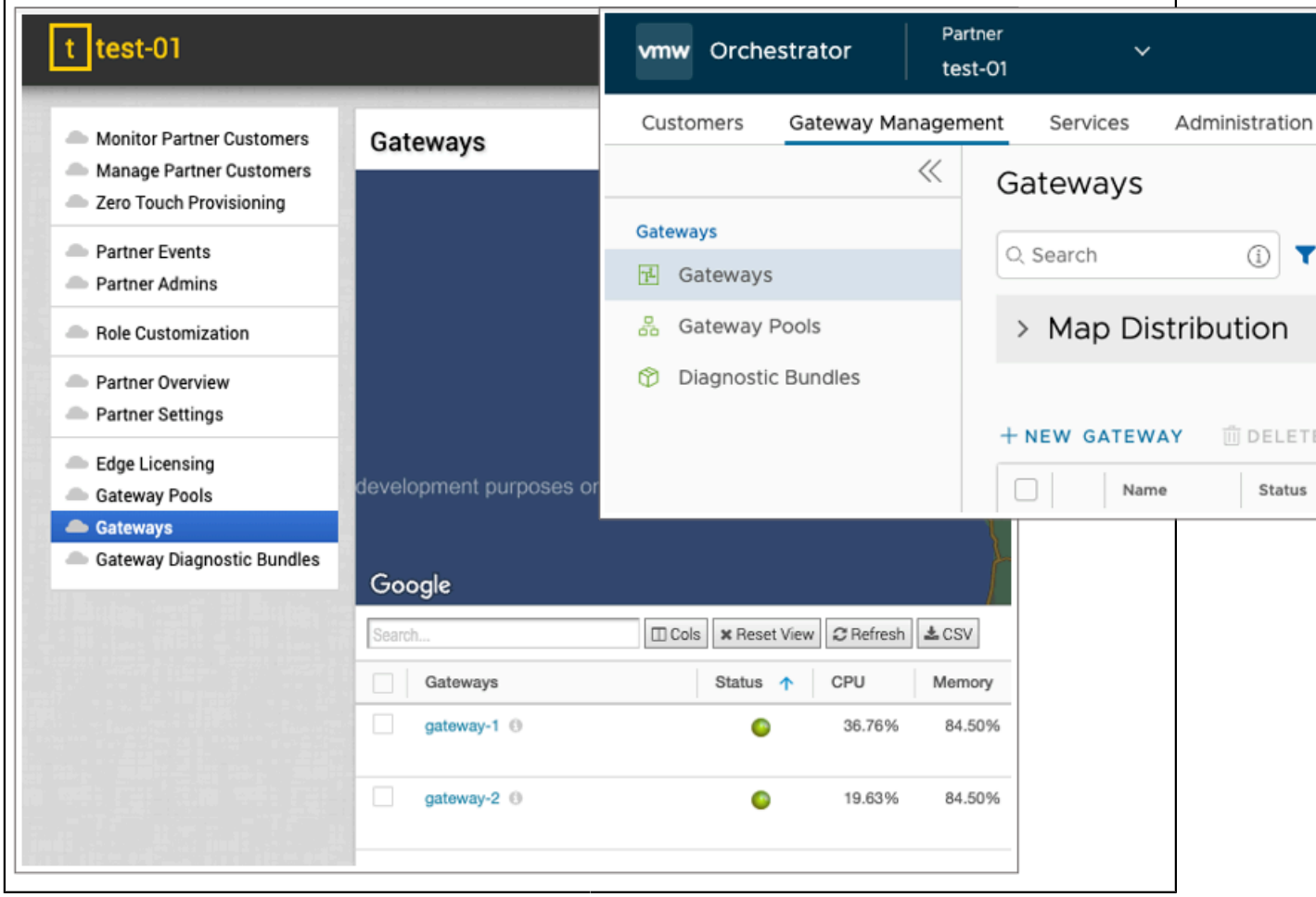
Classic Orchestrator Location	New Orchestrator Location
Partner > Gateway Pools	**Partner > Gateway Management > Gateway Pools**



Gateways

We have moved the **Gateways** feature because the Classic Orchestrator UI had poor navigation and page layout. The New Orchestrator UI has an improved design that groups all Gateway related features under the **Gateway Management** tab.

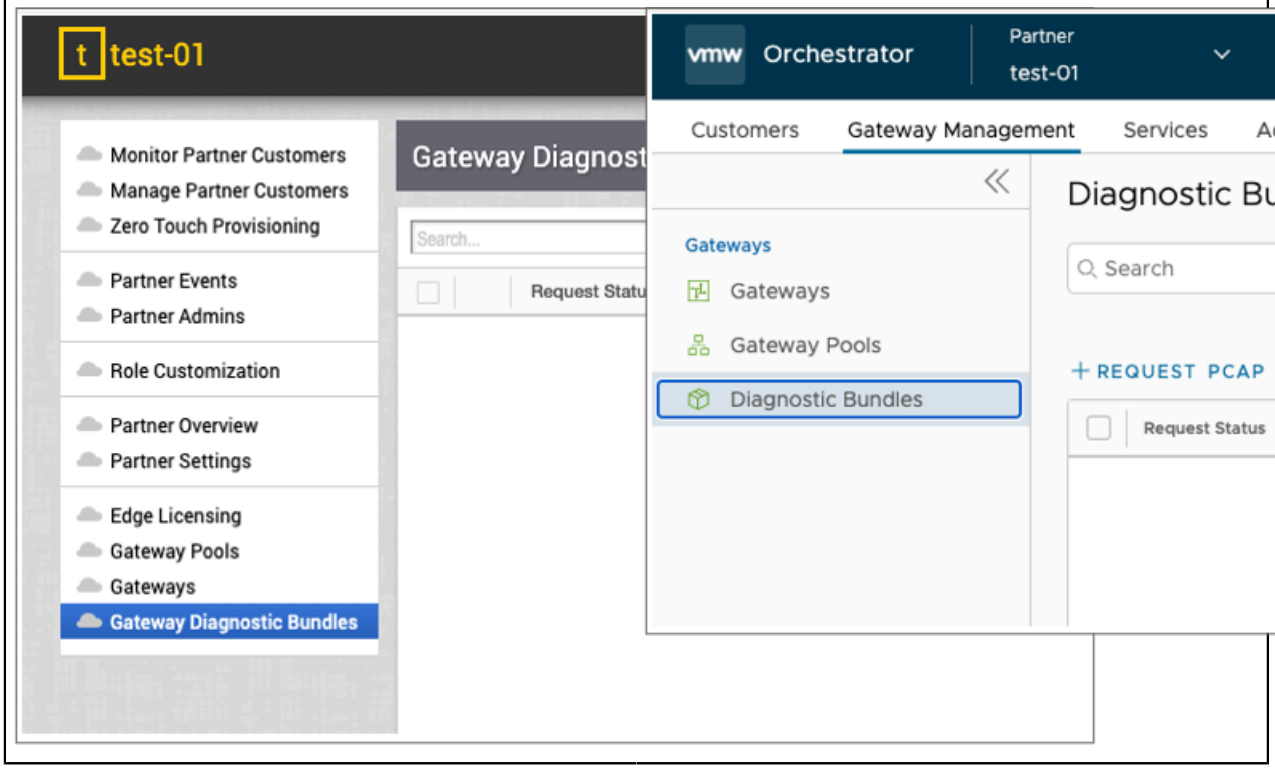
Classic Orchestrator Location	New Orchestrator Location
Partner > Gateways	**Partner > Gateway Management > Gateways**

Classic Orchestrator Location	New Orchestrator Location
	

Gateway Diagnostic Bundles

We have moved the **Gateway Diagnostic Bundles** feature because the Classic Orchestrator UI had poor navigation and page layout. The New Orchestrator UI has an improved design that groups all Gateway related features under the **Gateway Management** tab.

Classic Orchestrator Location	New Orchestrator Location
Partner > Gateway Diagnostic Bundles	**Partner > Gateway Management > Diagnostic Bundles**

Classic Orchestrator Location	New Orchestrator Location
	

Log in to using SSO for Partner User

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

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

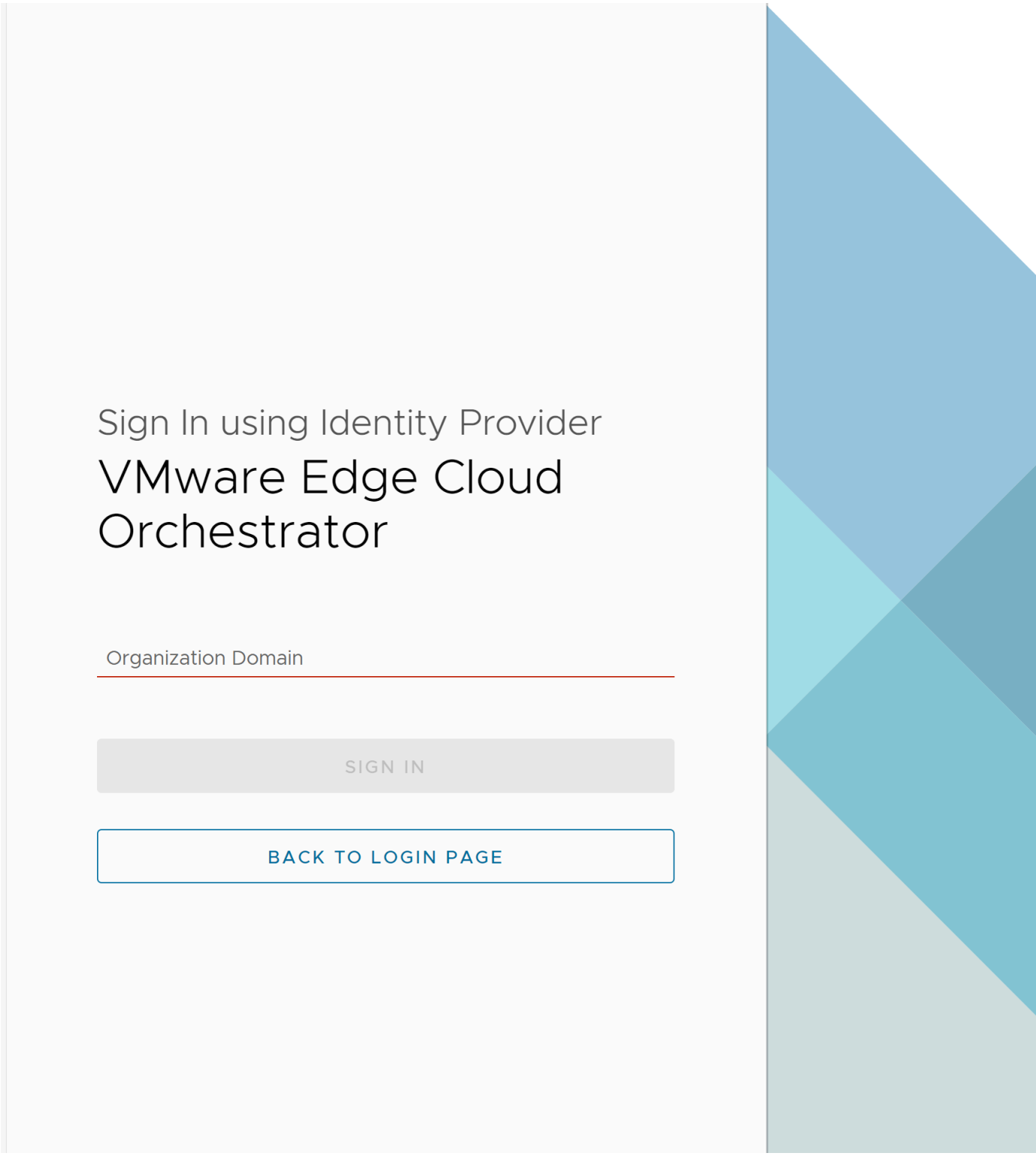
  For more information, see Authentication.

1. In a web browser, launch the application.

The screen


vmware
by Broadcom
Welcome to
VMware Edge Cloud Orchestrator
Username
Password
Forgot Password?
LOGIN

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



3. In the **Organization Domain** text box, enter the domain name used for the SSO configuration and click **Sign In**. The IDP configured for the SSO authenticates the user.

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

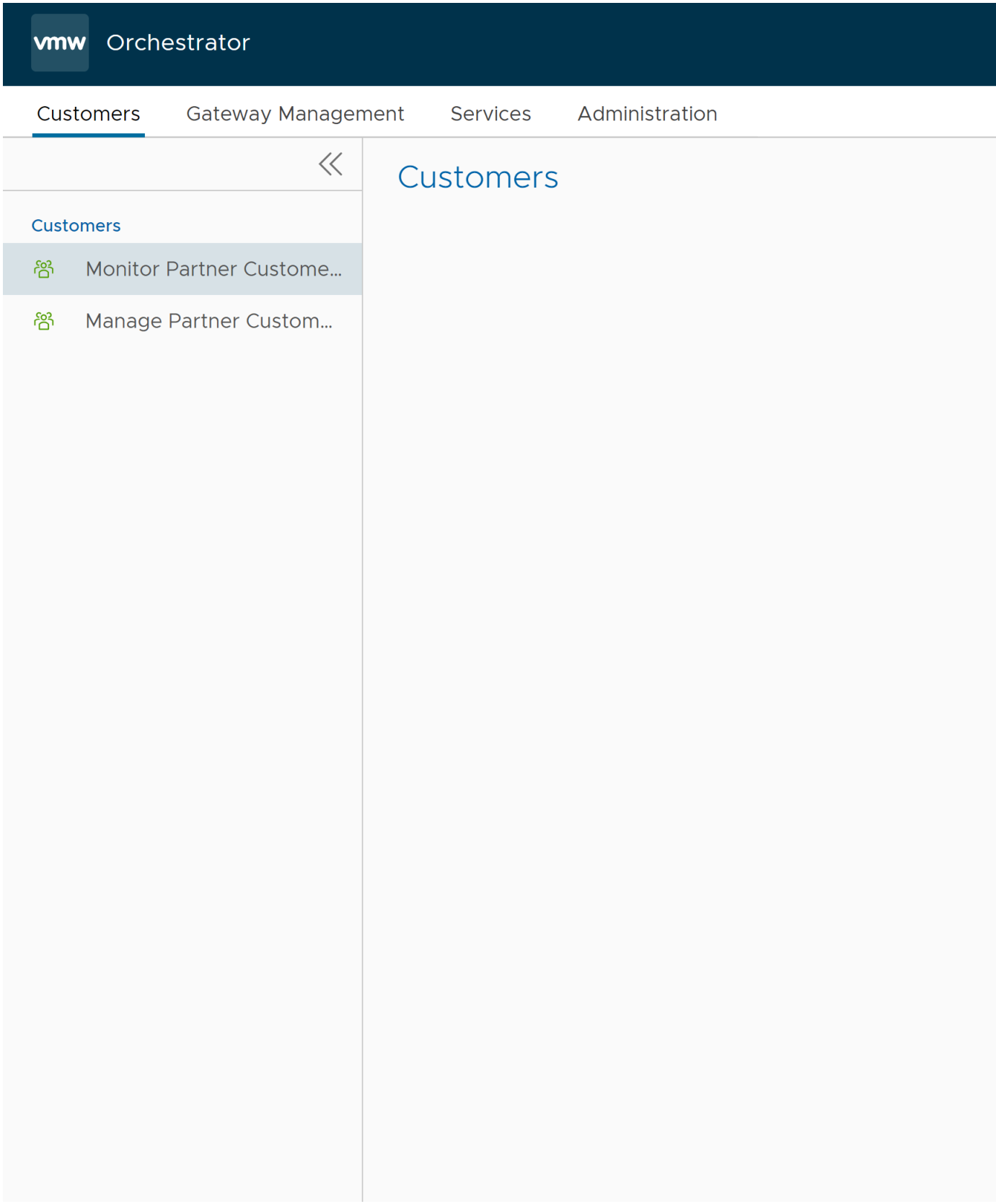
- Manage and monitor Partner customers

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

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

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

usage, and Arista trademark. For more information, see Configure User Account details.

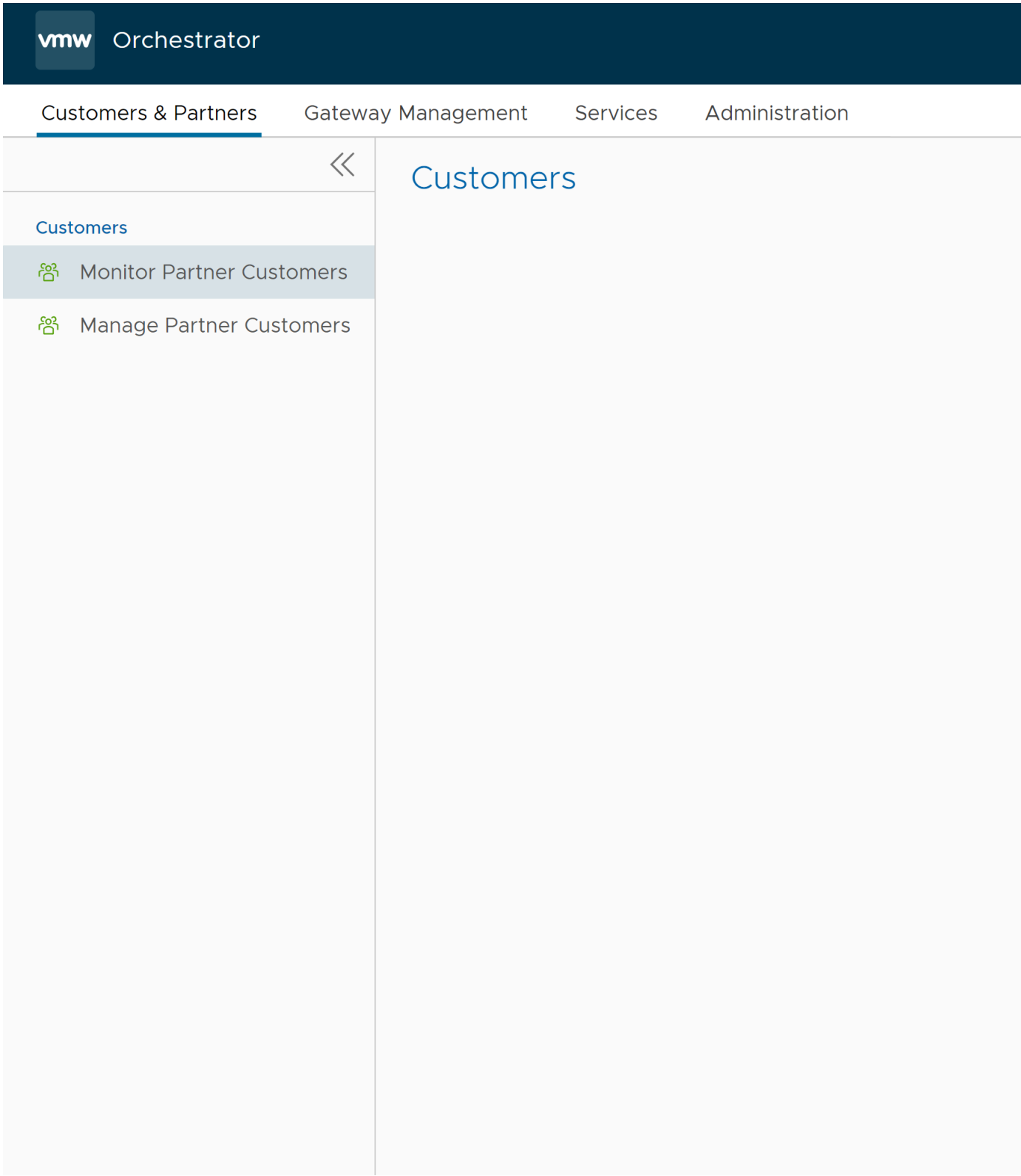


- Starting with the 5.4.0 release, the **In-product Contextual Help Panel** with context-sensitive user assistance is supported in the SD-WAN service of the Enterprise Orchestrator UI and as well as for the Operator and Partner

levels. In the Global Navigation bar, click 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.

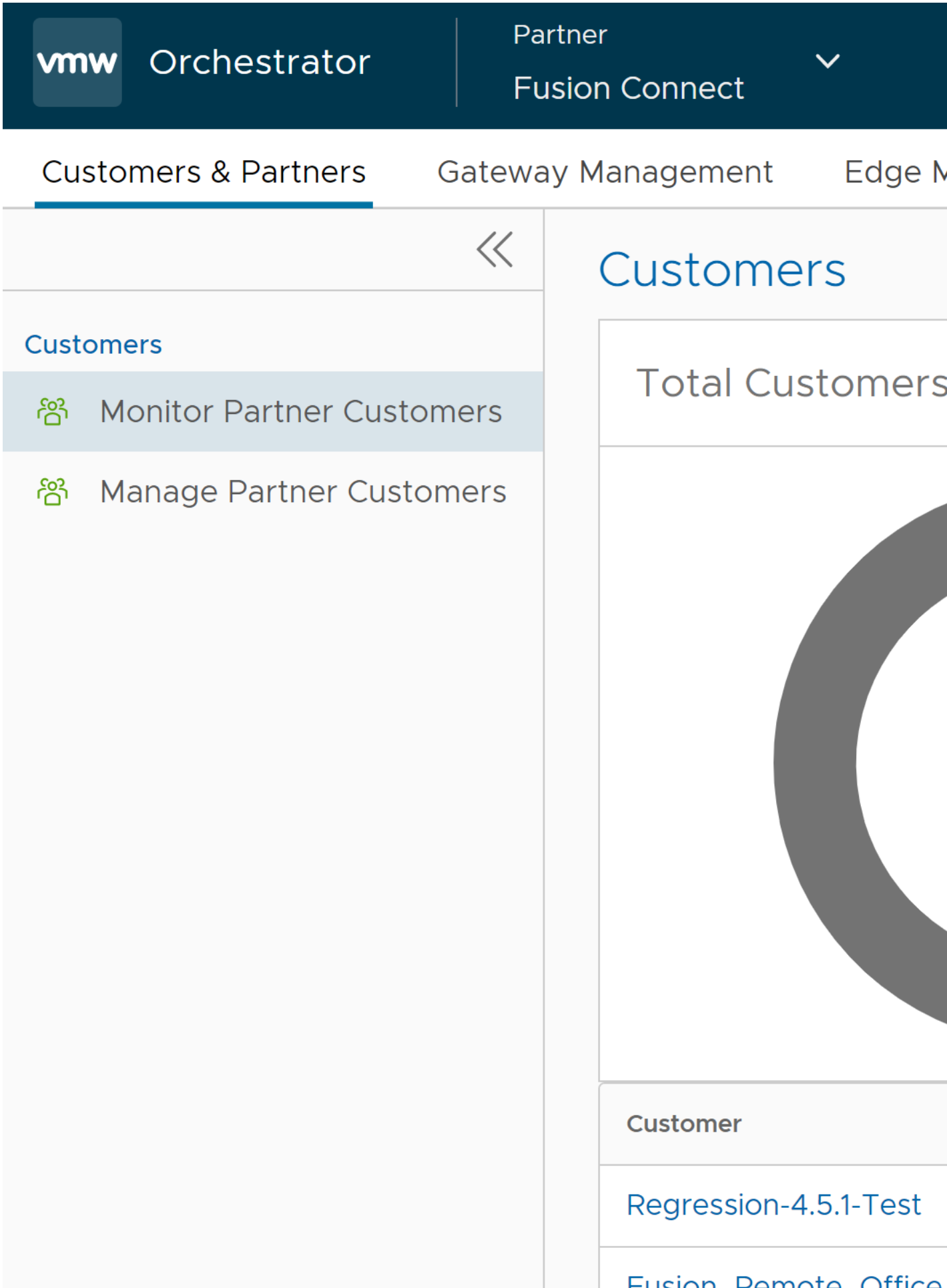
Note: By default, the Support Panel is not available to all Customers. You can activate this feature for a Customer by navigating to the **Global Settings** > **Customer Configuration** > **Additional Configuration** > **Global** > **Feature Access** page. For more information, see Configure Partner Customers.


vmw
Orchestrator
Customers & Partners
Gateway Management
Services
Administration
Customers
Customers
Monitor Partner Customers
Manage Partner Customers

Monitor Partner Customers

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

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



This screen shows the Edges for all customers managed by this Partner.

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

Total Customers:

- Customers managed by the Partner.
- Number of Edges that are DOWN, DEGRADED, CONNECTED, and UNACTIVATED. Click the number to view the corresponding Customer details in the bottom panel.
- In the bottom panel, click 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 more information see the *Administration Guide*.

Total Edges:

- Edges associated with the Customers.
- Number of Edges that are DOWN, DEGRADED, CONNECTED, and UNACTIVATED. Click the number to view the corresponding details of the Edges in the bottom panel.
- In the bottom panel, click the number of Edges link, to view the details of each Edge. Click the link to the Edge name to view more details corresponding to the selected Edge. For more information see the *Administration Guide*.

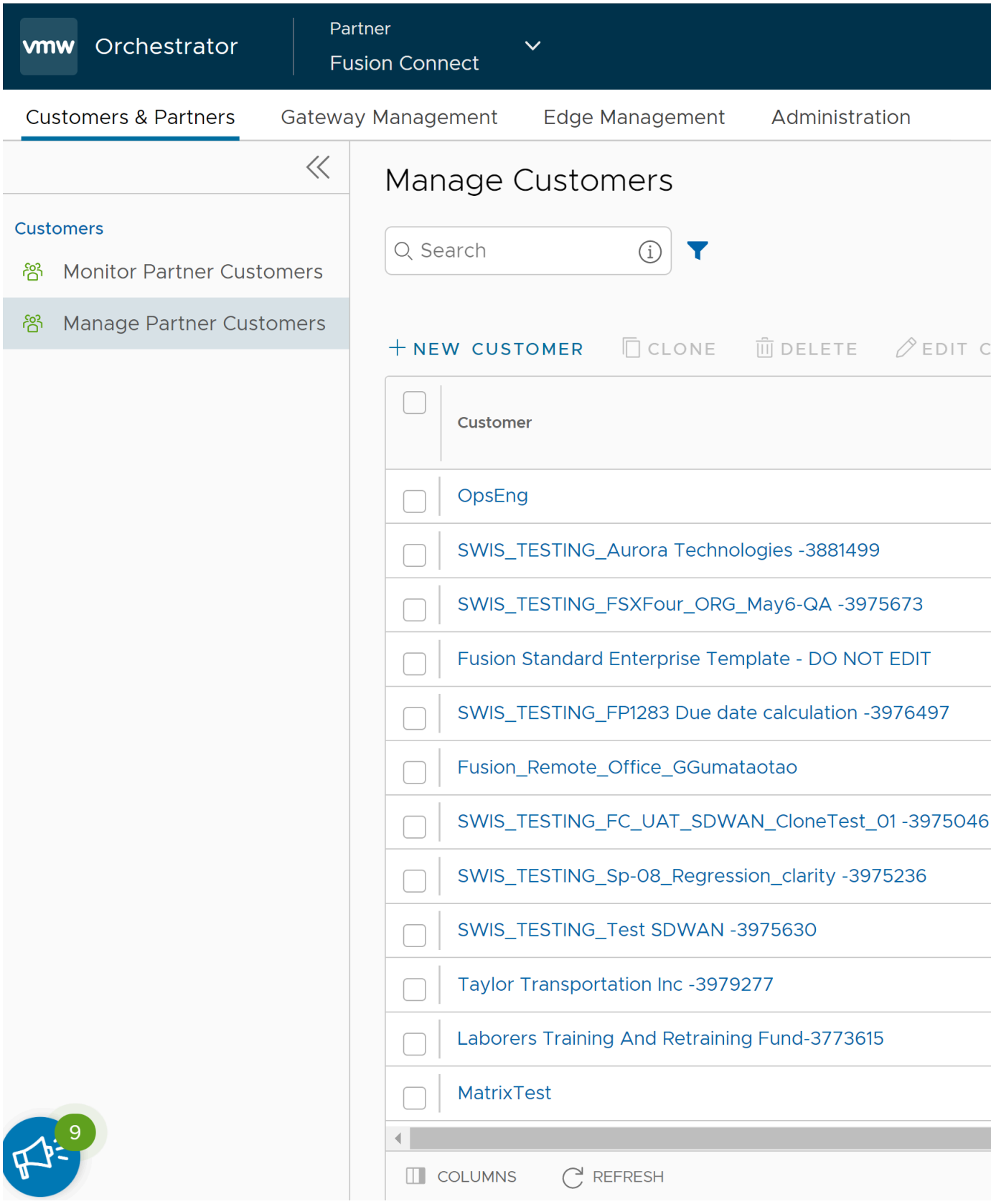
Note: The option for Auto Refresh is not available. You can refresh the Window manually to view the current data.

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 as a Partner. In the Partner portal, go to **Customers & Partners** > **Manage Partners** and from the **Manage Partners** page, click on a Partner.
2. Click **Manage Partner Customers**. The **Manage Customers** page appears.

Note: You can also navigate to this page from the Operator portal, by clicking 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.



3. You can perform the following actions:

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	Click this option to add a new Customer. For more 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 more information see, Clone Partner Customer.
Delete	Deletes the selected Customers. Enter the number of selected Customers in the pop-up window and click **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 more information, see the "*Enterprise Settings*" section in the *Administration Guide* available at www.arista.com/en/support/product-documentation.
Stage to Bastion	Click 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 more information, see *Bastion Orchestrator Configuration Guide* available at www.arista.com/en/support/product-documentation

4. Click **More** to perform the following actions:

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.

Option	Description
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 (,).

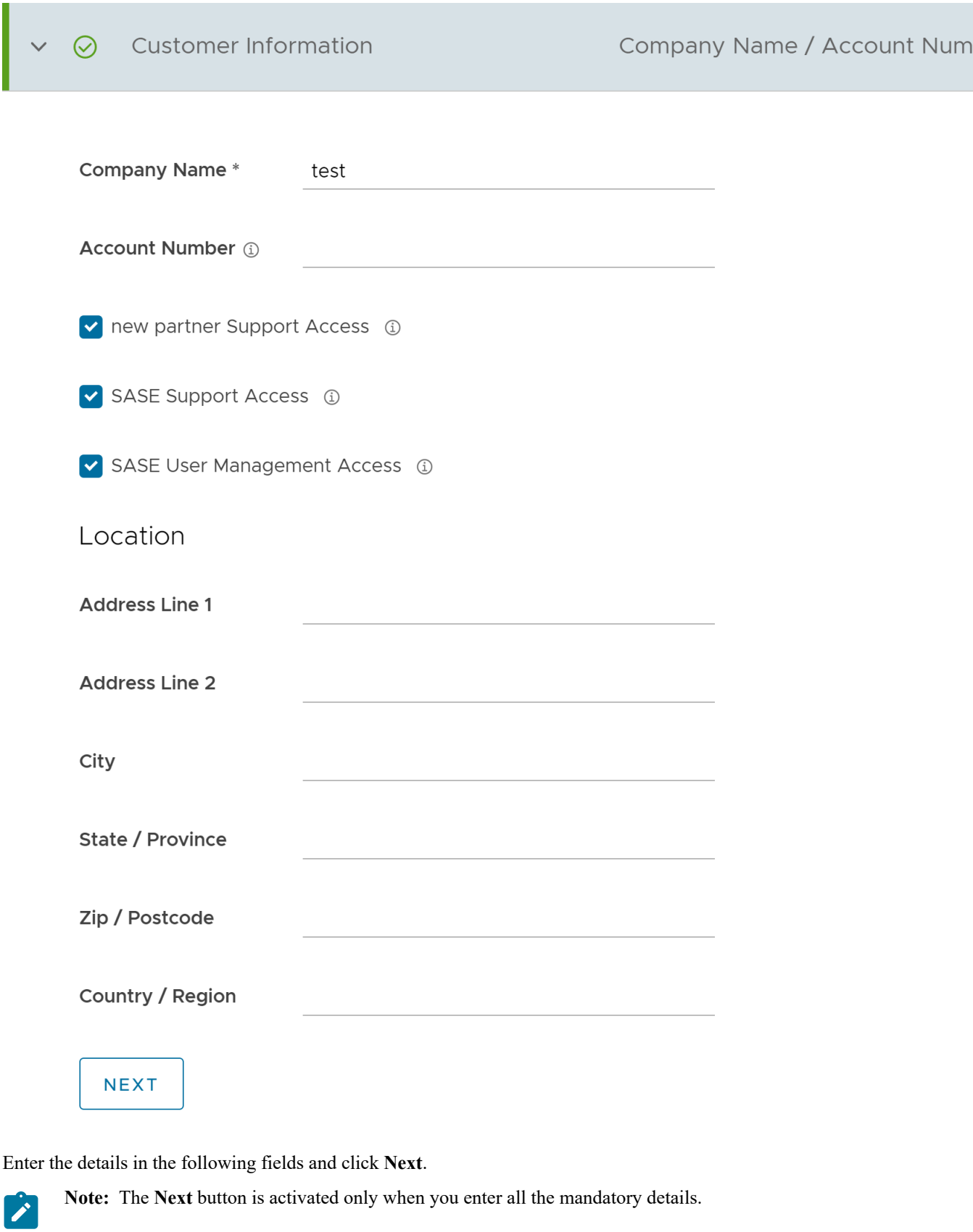
5. Following are the other options available in the **Manage Customers** area:

Option	Description
Columns	Click this option and select the checkboxes to view the required columns.
Refresh	Click this option to refresh the page.

Create New Partner Customer

In the Partner portal of the, 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 exceeds the usage capacity.

1. Login to the as a Partner.
2. In the Partner portal, go to **Customers & Partners** > **Manage Partners** and from the **Manage Partners** page, click on a Partner.
3. Click **Manage Partner Customers**. In the **Manage Customers** page appears , click **New Customer**. The **New Customer** page displays the following sections:
   a. **Customer Information:**

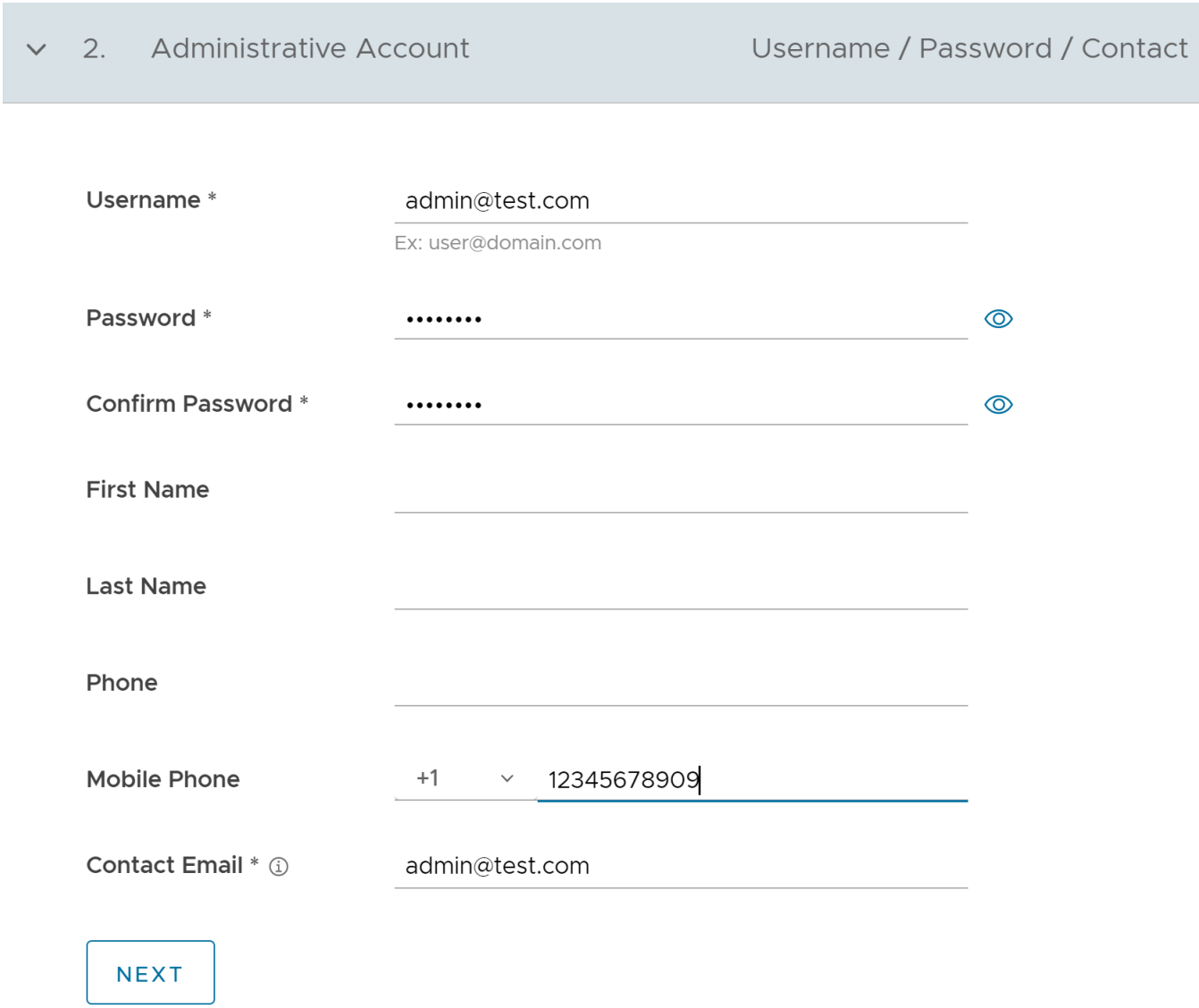


Enter the details in the following fields and click **Next**.

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

Option	Description
Company Name	Enter your company name.
Account Number	Enter a unique identifier for the Customer.
New Partner Support Access	Select the checkbox to allow the new Partner to view, configure, and troubleshoot the Customer's Edges.
SASE Support Access	This checkbox is selected by default, and grants access to the 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 checkbox to allow the 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:**



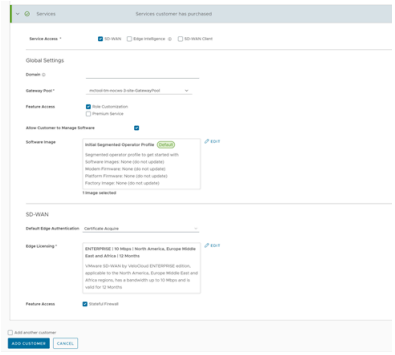
Enter the details in the following fields and click **Next**.

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

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.

Option	Description
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:**



Configure the following global settings:

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 Intelligence for the Customer.
Gateway Pool	Select an existing Gateway pool from the drop-down list. For more information, see Manage Gateway Pools.
Feature Access	You can select either **Role Customization** or **Premium Service**, or both the checkboxes.
Allow Customer to Manage Software	Select the checkbox 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. Click **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. Click **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.

Option	Description
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 more information on Operator profiles, see the "Manage Operator Profiles" section in the *Operator Guide* available at Arista VeloCloud SD-WAN Documentation.

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**.

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

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, 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 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	Click **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 more information, see Edge Licensing.

- **Edge Intelligence**: You can select this service only when **SD-WAN** is selected. When you select this service, the following options are available:

Option	Description
Nodes	Enter the maximum number of Edges that can be provisioned as Analytics Edge. By default, **Unlimited** is selected.
Feature Access	Select this check box to allow Edge Intelligence to provide recommendations to improve performance.

Note: This option is available only when the Analytics feature is activated on your. Use the following settings:

```
service.analytics.apiToken
service.analytics.analyticsEndpointDynamicIP
service.analytics.analyticsEndpointStaticIP
service.analytics.apiUrl
service.analytics.configEndpoint
```

- **SD-WAN Client**: You can select this service only when **SD-WAN** is selected.

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

Clone a Partner Customer

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

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
-
- VNF or VNF licenses
- Authentication services
- NetFlow objects like collectors or filters

Login to the as a Partner and navigate to **Manage Customers**.

1. In the **Manage Customers** page, select the customer you want to clone, and then click **Clone**.

   The **Clone Customer** page appears.

Customers / Clone SCALE Customer

Clone SCALE Customer

1. Customer Information — Company Name / Account Nur

Additional Clone Attributes

- [ ] Security Policy
- [ ] Alert Configuration
- [ ] Global Routing Pref
- [ ] Cloud Subscriptions

Company Name * Clone - SCALE

Account Number

- [x] SASE Support Access
- [x] SASE User Management Access

Location

Address Line 1

Address Line 2

City

State / Province

Zip / Postcode

Country / Region

NEXT

2. Configure the **Customer Information** and **Administrative Account** details, and **Services**. For more information, see Create New Partner Customer.
3. Click **Add Customer**.

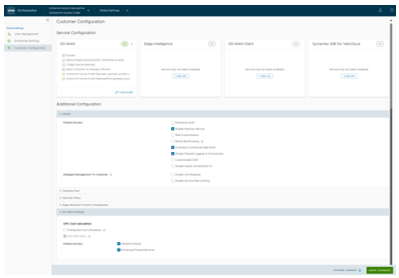
   The new customer name is displayed in the **Manage Customers** page. The customer is already configured with the cloned settings. You can click the customer name to navigate to the Enterprise portal and add or modify the configurations.

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 as a Partner.
2. In the Partner portal, select a Partner Customer, and from the top header, click **SD-WAN** > **Global Settings**.
3. From the left menu, click **Customer Configuration**. The following page is displayed:



The

Service Configuration

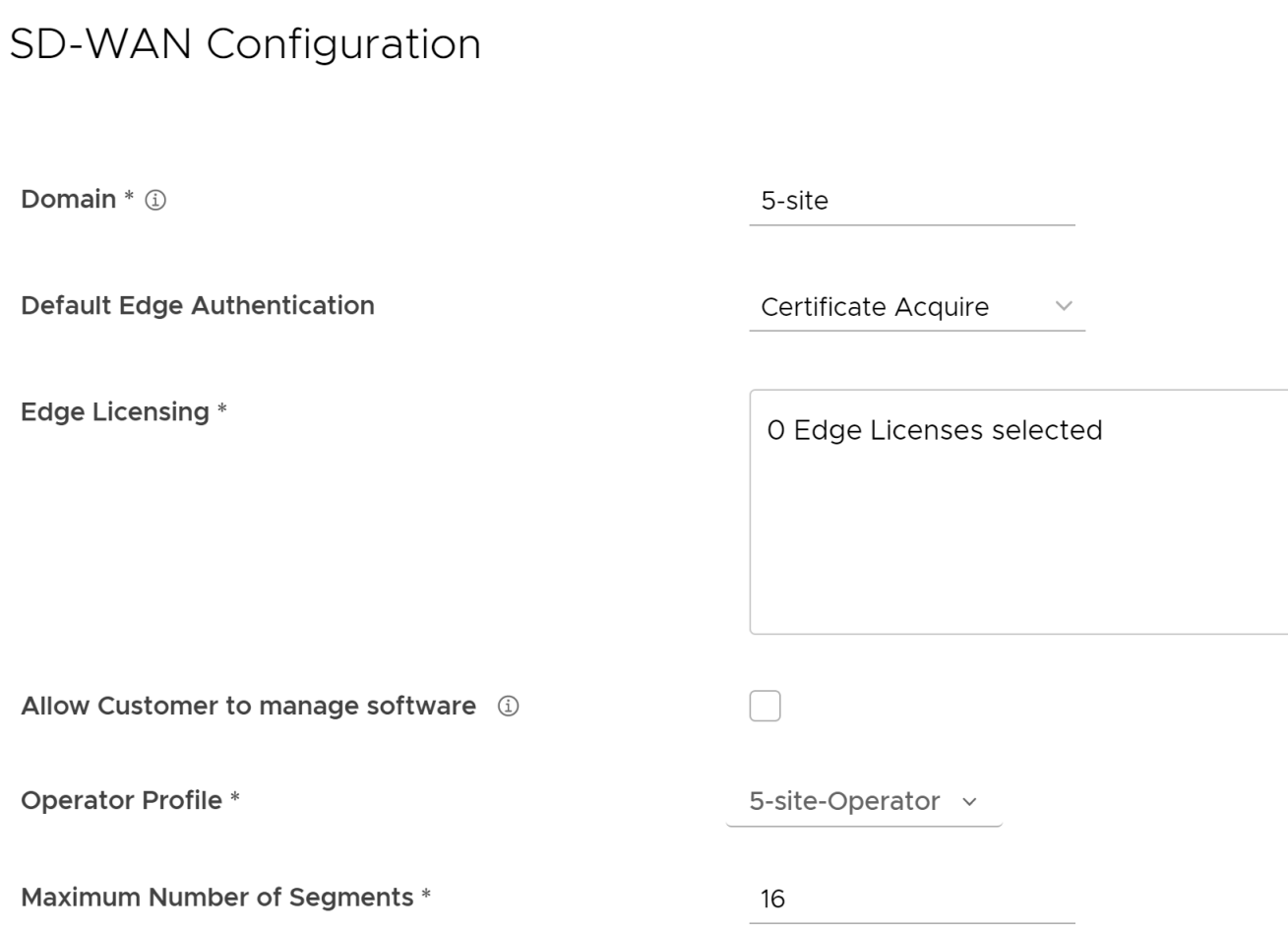
section includes the following services:

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

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

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

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

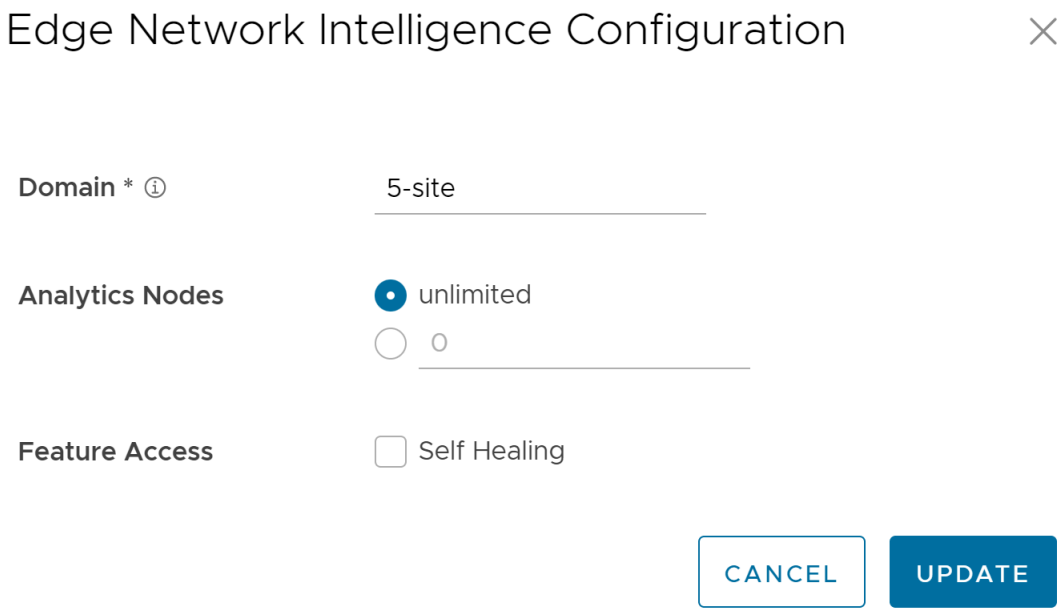


Option	Description
Domain	Enter the domain name to be used to activate Single Sign On (SSO) authentication for the Orchestrator. This is also required to activate Edge Intelligence for the Customer.

Option	Description
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, 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 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. Click **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 more 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 more information, see the topic *Edge Image Management* in the *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 more information on Operator profiles, see the "Manage Operator Profiles" section in the *Operator Guide* available at Arista VeloCloud SD-WAN Documentation.
Maximum Number of Segments	Enter the maximum number of segments that can be configured. The valid range is 1 to 16.The default value is **16**.

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

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



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

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

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

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

Option	Description
Global	

Option	Description
User Agreement Display	Select either of the following from the drop-down menu: • Inherit • Override to Hide • Override to Show **Note:** This field is available only when the system property `session.options.enableUserAgreements` is set to **True**.
Feature Access	Provides access to the selected features. Select one or more check boxes from the below list to activate these features for the 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**.

Option	Description
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.
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 Gateway Handoff to Production Orchestrator 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.

Option	Description
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.
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 Gateway Handoff to Production Orchestrator Configure Partner Handoff. For more information about configuring a Network Service for Business Policy rule, refer to the "Configure Network Service for Business Policy Rule" in the *Administration Guide* available at Arista VeloCloud SD-WAN Documentation.
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	

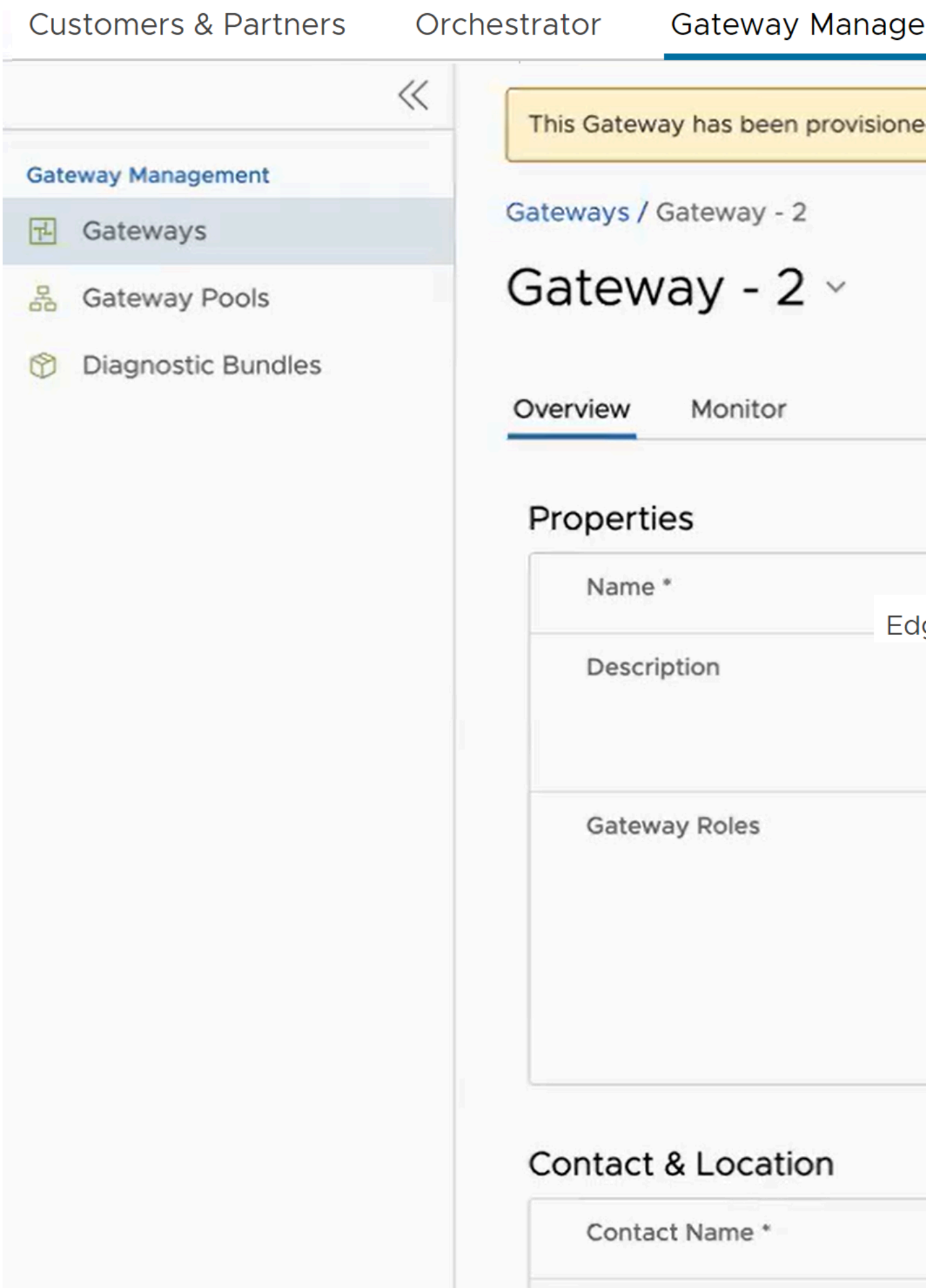
Option	Description
OFC Cost Calculation	Select the required check box: • **Distributed Cost Calculation**: Select this check box to delegate route cost calculation to Edges/ Gateways. **Note:** This option is available only for the Edges/Gateways with version 3.4.0 and later. • **Use NSD Policy**: Select 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.

5. Click **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.

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

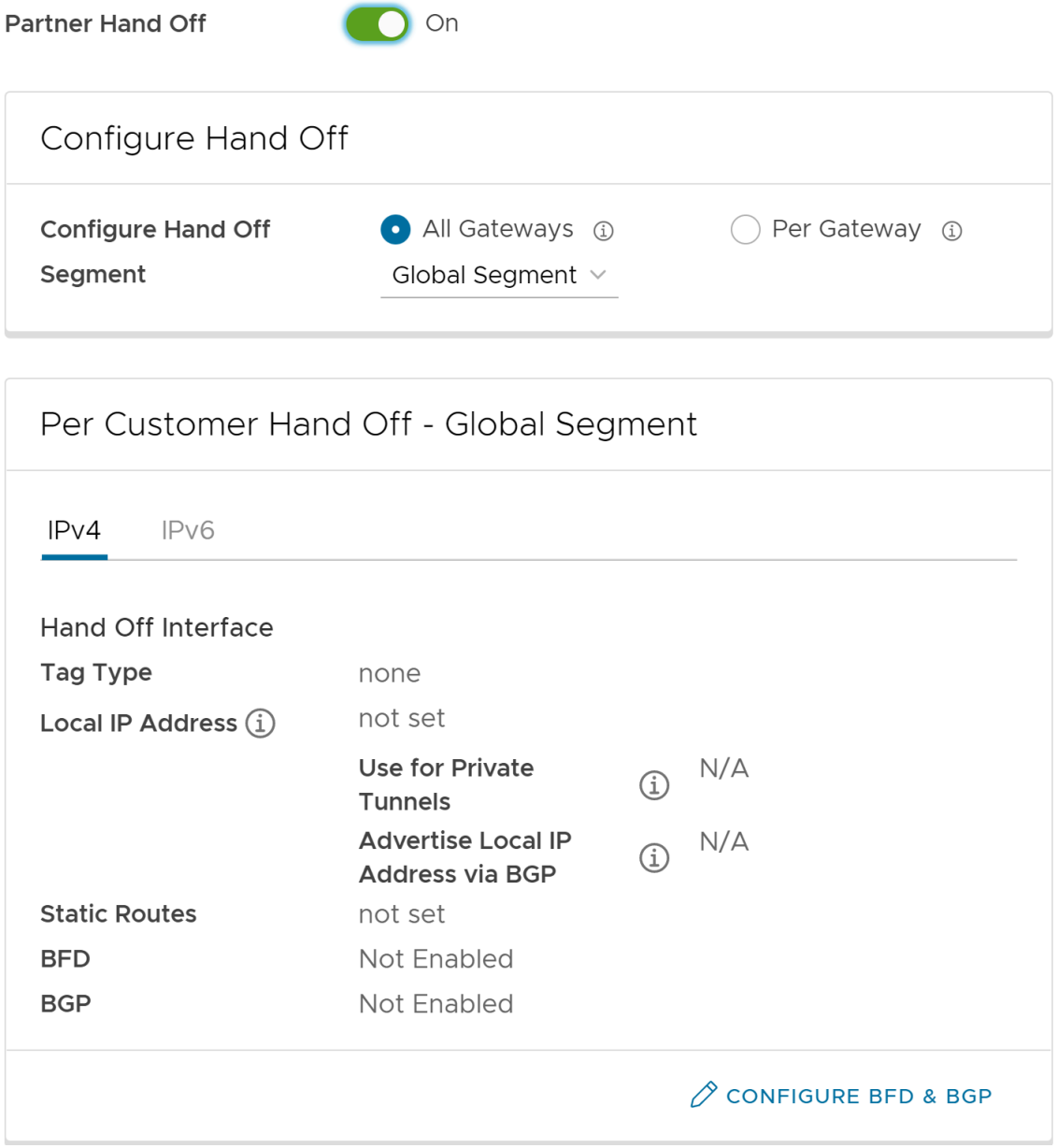
Ensure that the Gateway to be handed off is assigned with Partner Gateway Role. In the Orchestrator portal (Operator or Partner), click **Gateways** and click the link to an existing Gateway. In the **Properties** section of the selected Gateway's Overview page, you can enable the **Partner Gateway**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


Customers & Partners
Orchestrator
Gateway Manage
Gateway Management
Gateways
Gateway Pools
Diagnostic Bundles
This Gateway has been provisione
Gateways / Gateway - 2
Gateway - 2
Overview
Monitor
Properties
Name *
Description
Gateway Roles
Contact & Location
Contact Name *

Procedure:

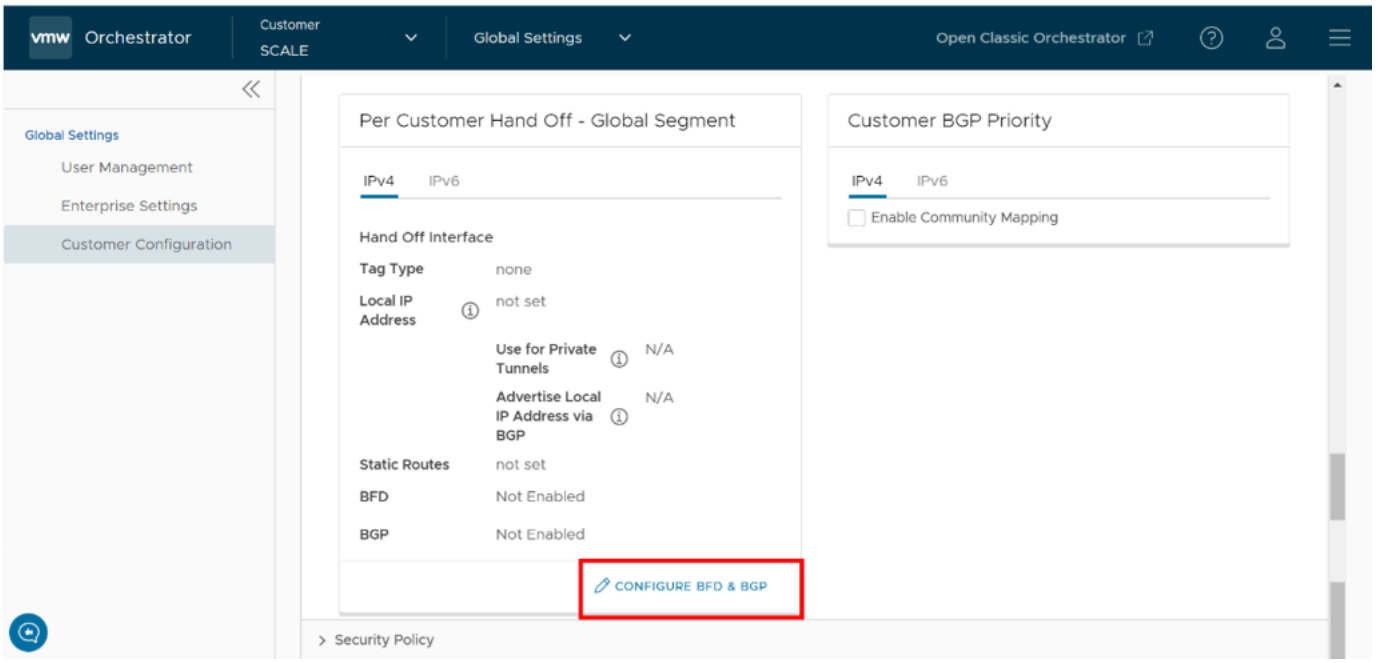
To configure the handoff settings, perform the following steps:

1. Log in to the as a Partner user.
2. Navigate to **Customers & Partners** > **Manage Customers**.
3. In the **Manage Customers** window, click the link of the desired customer.
4. Go to **Global Settings** > **Customer Configuration**.
5. In the **Customer Configuration** window, scroll down to **Additional Configuration** and expand the **Gateway Pool** area.
6. Turn on the **Partner Hand Off** toggle button.
7. In the **Configure Hand Off** area, configure the following fields in the table below:

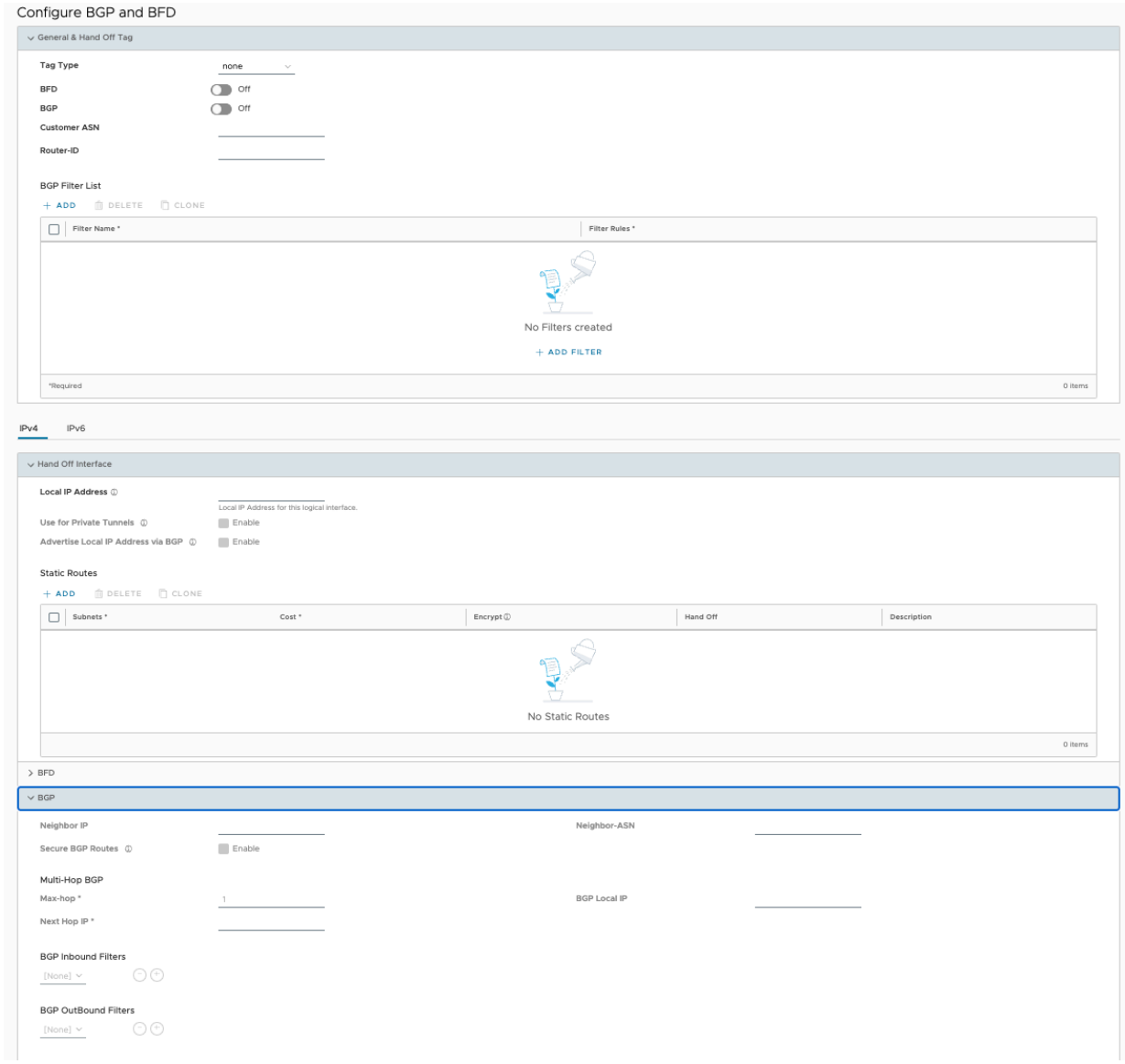


Option	Description
Configure Hand Off	By default, the hand off configuration is applied to all the Gateways. If you want to configure a specific Gateway, choose **Per Gateway**, and then select the Gateway from the drop-down list.
Segment	By default, **Global Segment** is selected, which means that the 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.

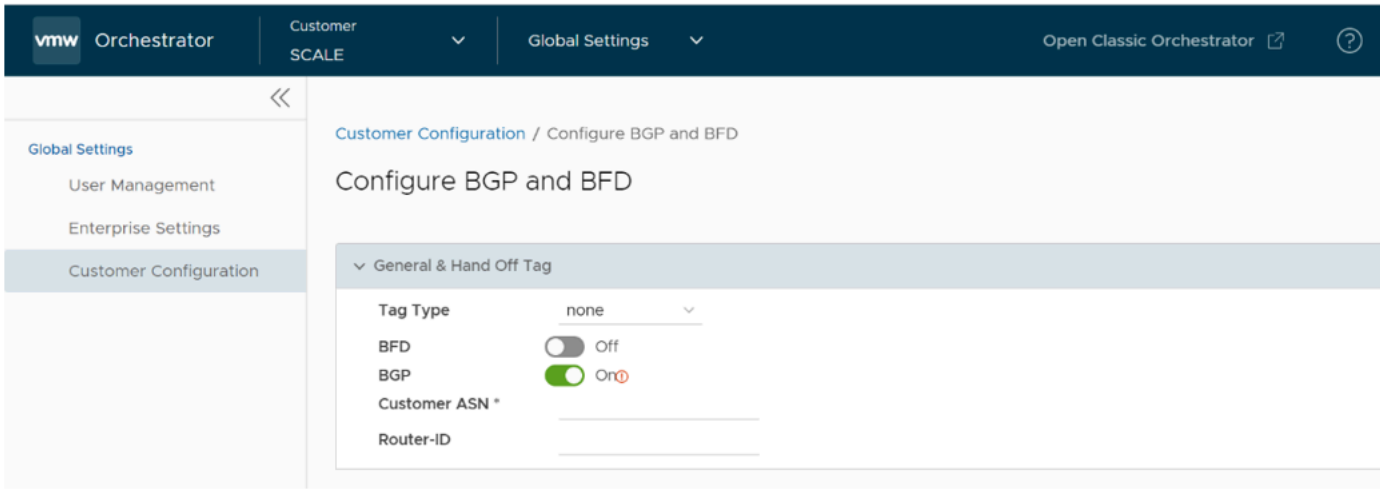
8. At the bottom of the **Per Customer Hand Off – Global Segment** area, click the **Configure BFD & BGP** link, as shown in the image below.



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


Configure BGP and BFD
General & Hand Off Tag
Tag Type
none
BFD
Off
BGP
Off
Customer ASN
Router-ID
BGP Filter List
ADD
DELETE
CLONE
Filter Name *
Filter Rules *
No Filters created
ADD FILTER
*Required
0 items
IPv4
IPv6
Hand Off Interface
Local IP Address
Local IP Address for this logical interface.
Use for Private Tunnels
Enable
Advertise Local IP Address via BGP
Enable
Static Routes
ADD
DELETE
CLONE
Subnets *
Cost *
Encrypt
Hand Off
Description
No Static Routes
0 items
BFD
BGP
Neighbor IP
Neighbor-ASN
Secure BGP Routes
Enable
Multi-Hop BGP
Max-hop *
1
BGP Local IP
Next Hop IP *
BGP Inbound Filters
[None]
BGP OutBound Filters
[None]

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



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

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.

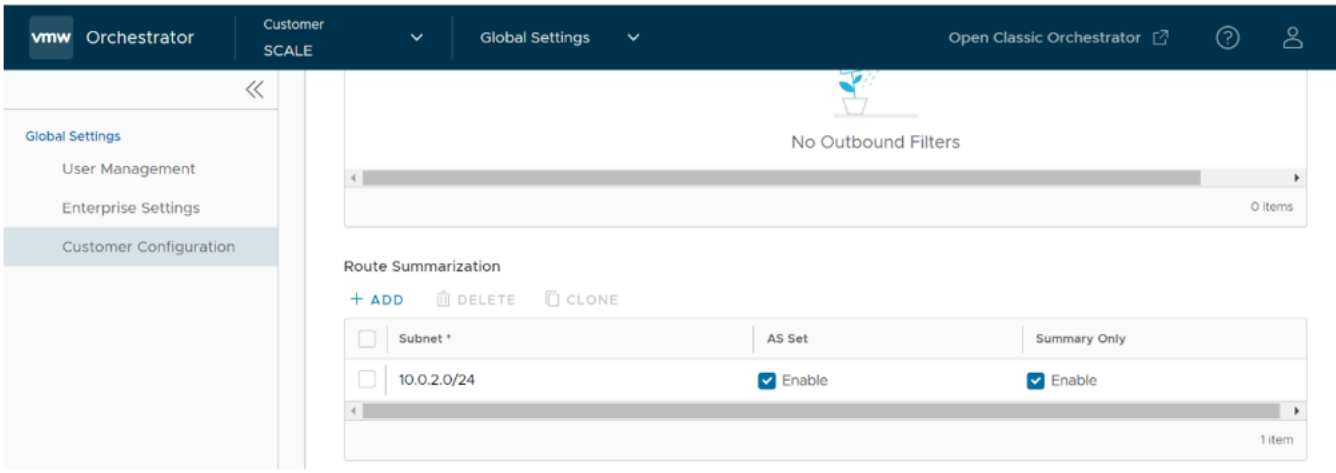
Option	Description
Encrypt	Select the check box to encrypt the traffic between Edge and Gateway.
Hand off	Select the hand off type as either **VLAN** or **NAT**.
Description	Enter a descriptive text for the static route. This field is optional.
BFD: Turn the toggle button to On to activate this section.	
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.
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.

Option	Description
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.

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 *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.



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

Option	Description
+Add	Click +Add to add a new row in the **Route Summarization** area. **Note:** To add additional rows to configure Route Summarization, click **+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, click the **Yes** check box if applicable.
Summary Only column	Under the **Summary Only** column, click the **Yes** check box to allow only the summarized route to be sent.

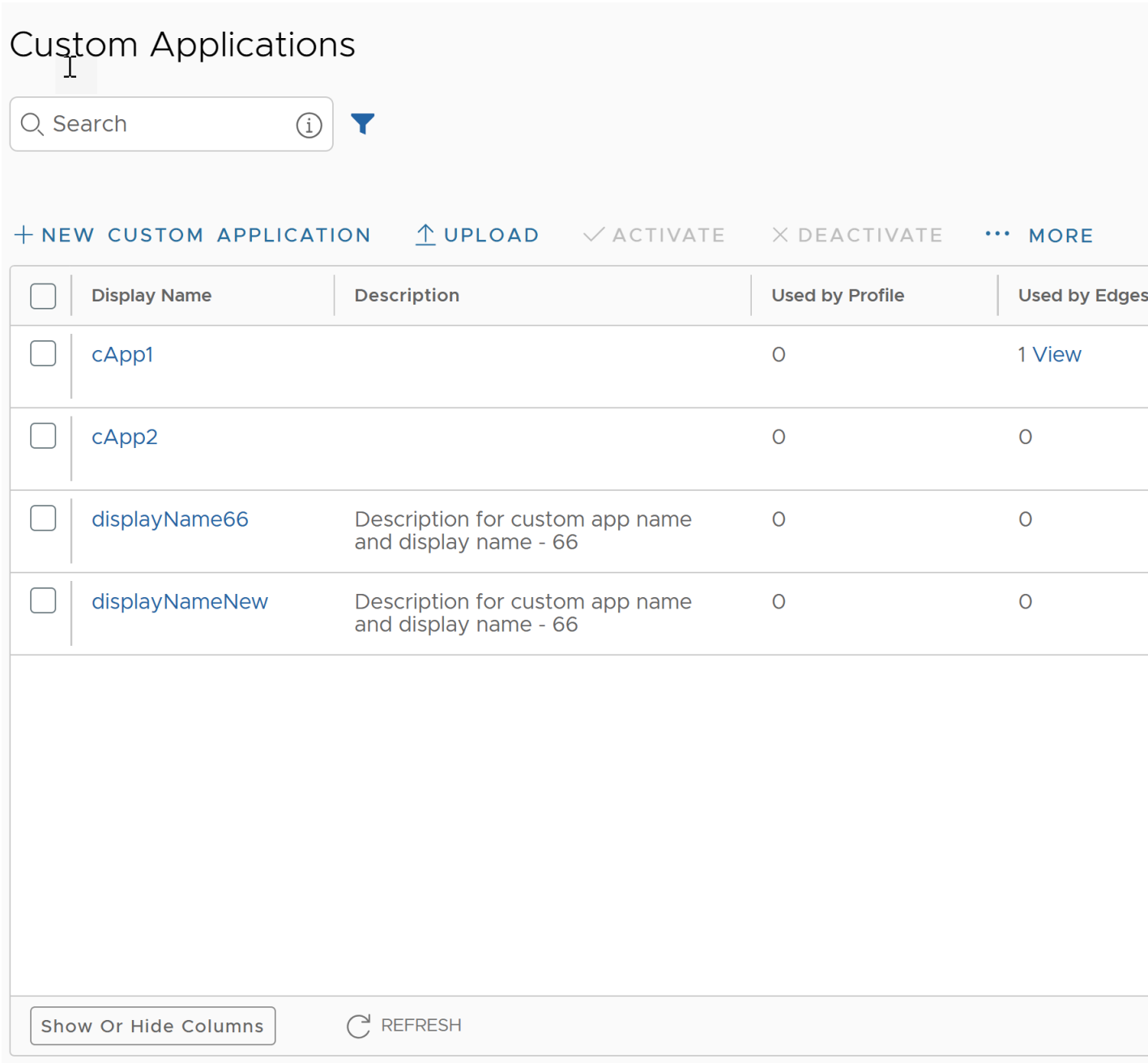
d. Click **Update** to save the settings.

Configure Custom Applications

Starting from the 6.4.0 release, Partner users can create Custom Applications and use these applications in Business Policy and Firewall rules creation. This feature is similar to the **Application Maps** feature available for the Operator users.

To access this feature, from the Partner portal, click **Configure** > **Custom Applications**.

The following screen appears:



You can configure the following options:

Note: Only a Partner Admin and a Partner Superuser can configure these options. For Partner Customer Support, this screen is read-only.

Option	Description
New Custom Application	Click to create a new Custom Application. For more information, see the topic Create New Custom Application.
Upload	Click and upload an existing Custom Application. You can either drag and drop, or browse and choose the application file to be uploaded.
Activate	Click to send the selected Custom Applications to Edges.

Option	Description
Deactivate	Click to remove the selected Custom Applications from Edges.
More	Click **More**, and then click **Download JSON**, to download and reuse the JSON file of the selected Custom Application for other Partner users. This reduces the effort of creating same Custom Applications across different Partner users.

The other options available on this screen are:

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

Click **Save Changes** to save the Custom Applications.

Note:

- The **Save Changes** button appears only after creating at least one Custom Application.
- The maximum number of Custom Applications that can be created for each Partner is **250**.
- You cannot delete a Custom Application.

Next Steps

- Use the new Custom Application to create Business Policy and Firewall rules at Edge or Profile level.

  1. For Edge level creation, go to **Configure** > **Edges**. Select an Edge and then click **Business Policy** > **Add**. In the **Application** field, select **Define**, and choose the Custom Application from the drop-down menu. Click **Save Changes**.
  2. For Edge level creation, go to **Configure** > **Edges**. Select an Edge and then click **Firewall** > **Configure Firewall**. Under **Firewall Rules**, click **New Rule**. In the **Application** field, select **Define**, and choose the Custom Application from the drop-down menu. Click **Save Changes**.

  Note:

  - The **Application** drop-down menu lists all applications created through both, **Application Maps** and **Custom Applications**. A label is displayed against all custom applications for easy identification purpose.
  - The above steps are for Edge level creation of Business Policy and Firewall rules. You can follow the same steps for creating these rules at Profile level by navigating to **Configure** > **Profiles**.

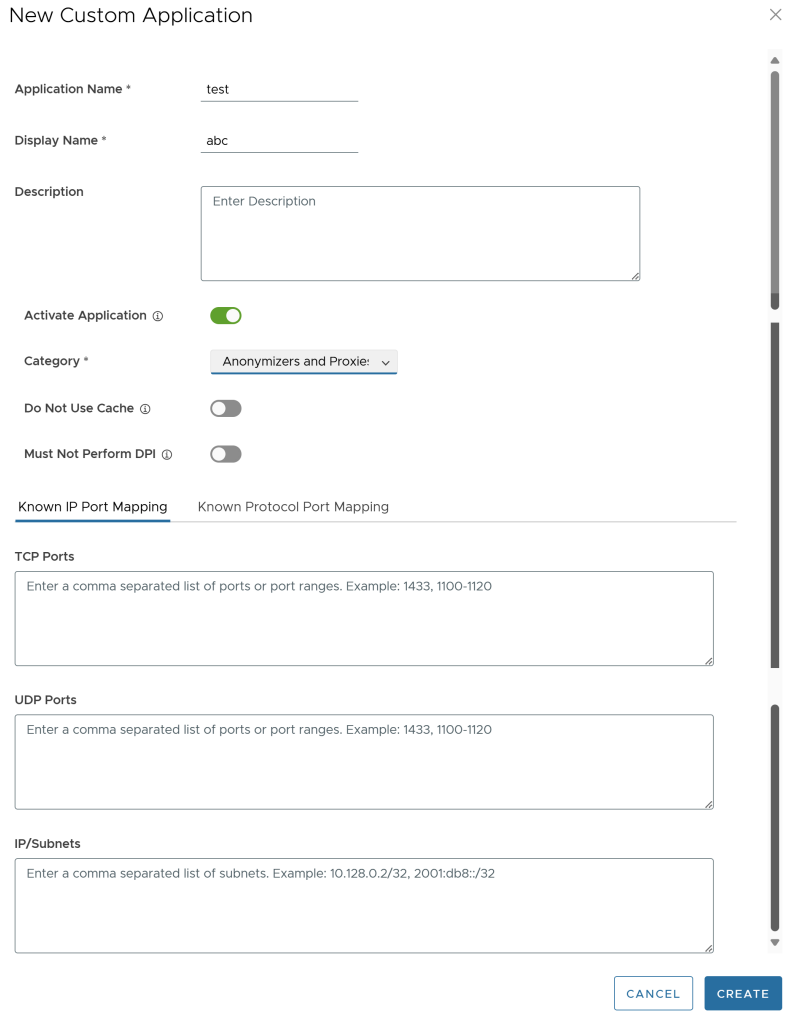
  The **Used By Profile** and **Used By Edges** columns on the **Custom Applications** main screen, display the details of the Profile and Edge(s) using the corresponding Custom Application. The Custom Applications that are associated to a Profile or an Edge cannot be deactivated.
- To monitor the Custom Applications, go to **Monitor** > **Events** > **Applications** screen.

Create New Custom Application

You can create multiple Custom Applications.

Follow the below procedure to create a new Custom Application:

1. From the Partner Portal, click **Configure** > **Custom Applications** > **New Custom Application**. The following screen appears:



2. Enter details in the following fields:

Option	Description
Application Name	Enter a unique name for the Custom Application.
Display Name	Enter a unique display name.
Description	Enter a description. This field is optional.
Activate Application	You can activate the application while creating it. An activated Custom Application is directly sent to the Edge when you save it.
Category	Select a category from the drop-down menu.
Do Not Use Cache	Slide the toggle button to activate slow-learning cache at Edge level. When activated, the Custom Applications do not use the cache, and their traffic is classified by Qosmos DPI, irrespective of IP-port or proto-port mappings.

Option	Description
Must Not Perform DPI	Slide the toggle button to deactivate DPI at Edge level. When activated, DPI is not used, even if **Do Not Use Cache** is activated, if traffic matches the known IP-port or protocol-port mapping.
Known IP Port Mapping	Enter the TCP ports, UDP ports, and IP/Subnets in a valid format.
Known Protocol Port Mapping	Enter the TCP and UDP ports in a valid format.

3. Click **Create** to save the new Custom Application. This application is then displayed on the **Custom Applications** main screen. The **State** column indicates whether the application is Active or Inactive.
4. Click **Cancel** to discard the entered details.

Activate on a

provides pre-defined system properties to configure feature in the portal. An Operator Super user can add or modify the values of the system properties to activate the Analytics service in a .

The following table describes all the -related system properties. When enabling EI for a , ensure that the following system properties are properly set in the .

System Property	Description	Value
session.options.enableEdgeAnalytics	Activate the Analytics service on a . By default, Analytics is activated for Cloud-hosted Orchestrators. **Note:** For On-prem Orchestrators, this system property is set to *false* by default. Ensure to change the value to *true* if you want to activate the Edge Intelligence feature.	*true*
service.analytics.apiURL	URL of the Analytics API	https://integration.nyansa.com/vco/api/v0/graphql
service.analytics.apiToken	API token of the Analytics API. The uses the API URL and token to contact the Cloud Analytics Engine and create new customers/ in the Analytics Engine.	For hosted Orchestrators, Arista Edge Ops can generate this token. And for on-prem Orchestrators, the Operator users should contact their SE or AE and ask them to email the EI-Activations DL to request the service.analytics.apiToken. For information on how to contact the Support Provider, see www.arista.com/en/support/product-documentation.

System Property	Description	Value
service.analytics.configEndpoint	Configuration endpoint of Analytics service	• config.nyansa.com (dynamic) or config-m2.nyansa.com (static) - For Orchestrators located in any region except for EMEA to connect to the US EI instance. • config.eu.nyansa.com (dynamic) or config-m2.eu.nyansa.com (static) - For Orchestrators located in the EMEA region to connect to the EMEA EI instance. • config.ap.nyansa.com (dynamic) or config-m2.ap.nyansa.com (static) - For Orchestrators located in the APAC region to connect to the Sydney EI instance.
service.analytics.analyticsEndpointStatic	IP analytics endpoint of Analytics service	• loupe-m.nyansa.com (dynamic) or loupe-m2.nyansa.com (static) - For Orchestrators located in any region except for EMEA to connect to the US EI instance. • loupe-m.eu.nyansa.com (dynamic) or loupe-m2.eu.nyansa.com (static) - For Orchestrators located in the EMEA region to connect to the EMEA EI instance. • loupe-m.ap.nyansa.com (dynamic) or loupe-m2.ap.nyansa.com (static) - For Orchestrators located in the APAC region to connect to the Sydney EI instance.
service.analytics.analyticsEndpointDynamic	IP analytics endpoint of Analytics service	Same values as `service.analytics.analyticsEndpoint`

Activate Analytics for a New Customer

When creating a new SD-WAN Partner customer, allows Partner Super Users and Partner Standard Admins to activate the Analytics functionality for the customer. Analytics helps to collect data from different vantage points for each application flow, which includes wireless controller, LAN switch, network services, , , , and application performance metrics. For more information, see *Arista Edge Network Intelligence Configuration Guide*.

For configuring the system properties, contact your Operator Super User.

To activate Analytics for a new customer, see Create New Partner Customer.

The new customer's name is displayed in the **Customers** screen. You can click on the customer name to navigate to the Enterprise portal and add or modify Analytics configurations for the customer. For more information, see the topic *Provision a New Edge with Analytics* in the *Administration Guide.*

Activate Analytics for an Existing Customer

allows Partner Super Users and Partner Standard Admins to activate Analytics for an existing Enterprise customer.

Ensure that your Operator has setup the required system properties to activate Analytics.

To activate Analytics for an existing customer, see the topic *Configure Analytics Settings on an Edge* in the *Administration Guide*.

Analytics is activated for the selected customer. You can click on the customer name to navigate to the Enterprise portal and add or modify Analytics configurations for the customer. For more information, see the topic *Provision a New Edge with Analytics* in the *Administration Guide*.

Activate Self-Healing for a New Customer

Self-Healing feature enables Enterprise and Managed Service Provider (MSP) users to activate and configure Self-Healing capabilities at the Customer, Profile, and Edge level.

To activate Self-Healing at the Customer level, ensure you have the following prerequisites:

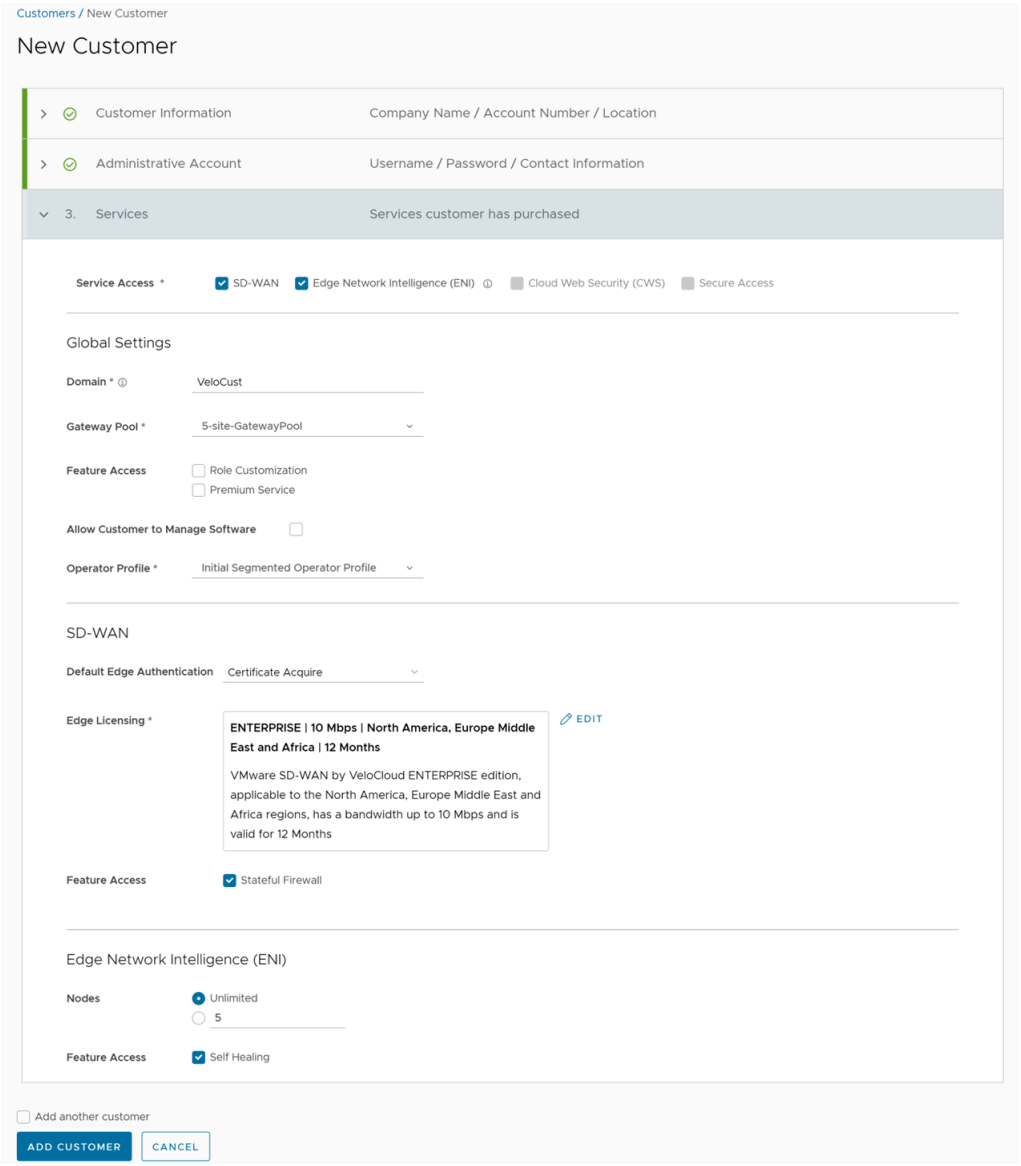
- The (Analytics) service is activated on the . For more information on how to activate the EI service on , contact your Operator Super User.
- The must be on 5.0.1.0 and the must be running a minimum of 4.3.1 code. You can review the software image installed on each edge by navigating to **Configure** > **Edges**. The table on the **Edges** page will have a column that displays Software version of Edge per customer.

When creating a new SD-WAN Partner customer, allows Partner Super Users and Partner Standard Admins to activate the Self-Healing functionality for the customer.

To activate Self-Healing for a new customer, perform the following steps:

1. Log in to the as a Partner user.
2. Navigate to **Customers & Partners** > **Manage Customers**, and then click **New Customer**.

   The **New Customer** page appears.



3. Enter all the mandatory Customer information and Administrative account details and click **Next**.
4. Under **Services** > **Service Access**, select the **SD-WAN** and **Edge Intelligence (EI)** services that the Customer can access along with the roles and permissions available for the selected service.
5. Under the **Edge Intelligence service** section, select the **Self Healing** check box to allow EI to provide remediation recommendations to improve application performance. By default, the Self-Healing feature is not activated for a customer. For more information, see the *Self-Healing Overview* section in the *Arista Edge Intelligence User Guide* published at www.arista.com/en/support/product-documentation. .

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

   Note: This option is available only when the Analytics feature is enabled on your . For more information, see the “Enable on a ” section in the *Arista Edge Intelligence Configuration Guide* available at Arista VeloCloud SD-WAN Documentation .
6. Click **Add Customer**. The new Customer name is displayed on the **Customers** page. You can click the Customer name to navigate to the Customer portal and configure Customer settings.

Once the Self-Healing feature is activated for a customer, (EI) monitors and tracks the network for systemic and application performance issues across Edges provisioned under that customer. EI then gathers data regarding Self-

Healing actions and triggers remediation recommendations to the users on the SD-WAN side directly through the incident alert email.

Note: Currently, only Manual remediation is supported by EI. Automatic remediation support is planned in future releases.

Activate Self-Healing for an Existing Customer

To activate Self-Healing for an existing customer, ensure you have the following prerequisites:

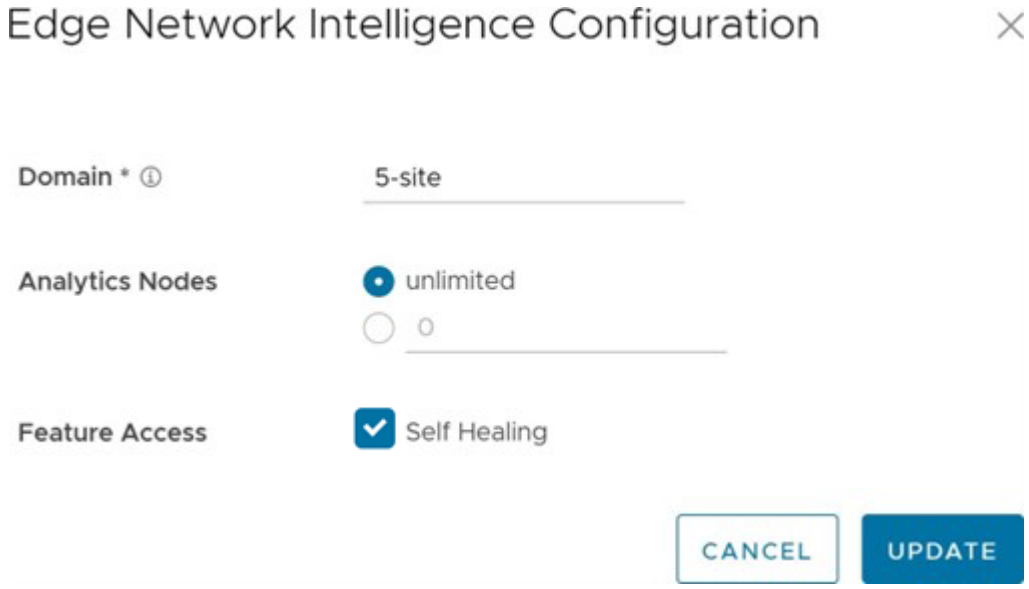
- The (Analytics) service is activated on the . For more information on how to activate the EI service on , contact your Operator Super User.
- The must be on 5.0.1.0 and the must be running a minimum of 4.3.1 code. You can review the software image installed on each Edge by navigating to **Configure** > **Edges**. The table on the **Edges** page will have a column that displays Software version of Edge per customer.

To activate Self-Healing for an existing Partner customer, perform the following steps:

1. Log in to the as a Partner user.
2. In the Partner portal, select a customer, and from the top header, click **SD-WAN** > **Global Settings**.
3. From the left menu, click **Customer Configuration**.

   The **Service Configuration** page appears.
4. In the **Edge Intelligence service** section, click the **Turn On** button to activate the EI service.

   Note: You can activate this service only when **SD-WAN** service is turned on.
5. Click the **Configure** button. The **Edge Intelligence Configuration** pop-up window appears.



6. Select the **Self Healing** checkbox to allow EI to provide remediation recommendations to improve application performance. By default, the Self-Healing feature is not activated for the customer. For more information, see the *Self-Healing Overview* section in the *Arista Edge Intelligence User Guide* published at www.arista.com/en/support/product-documentation.
7. Click the **Update** button.

Once the Self-Healing feature is activated for an existing customer, (EI) monitors and tracks the network for systemic and application performance issues across Edges provisioned under that customer. EI then gathers data regarding Self-Healing actions and triggers remediation recommendations to the users on the SD-WAN side directly through the incident alert email.

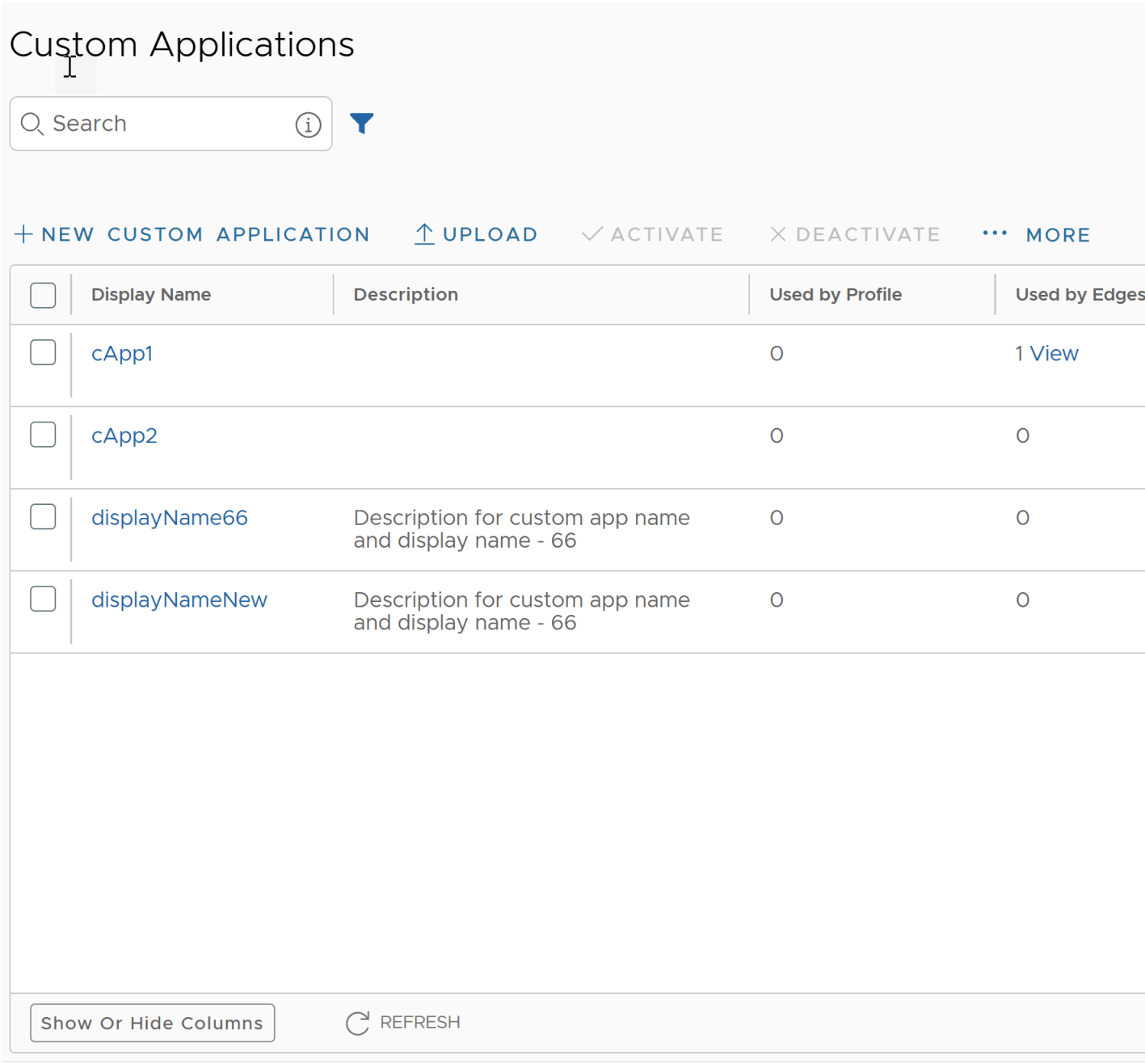
Note: Currently, only Manual remediation is supported by EI. Automatic remediation support is planned in future releases.

Configure Custom Applications

Starting from the 6.4.0 release, Partner users can create Custom Applications and use these applications in Business Policy and Firewall rules creation. This feature is similar to the **Application Maps** feature available for the Operator users.

To access this feature, from the Partner portal, click **Configure** > **Custom Applications**.

The following screen appears:



You can configure the following options:

Note: Only a Partner Admin and a Partner Superuser can configure these options. For Partner Customer Support, this screen is read-only.

Option	Description
New Custom Application	Click to create a new Custom Application. For more information, see the topic Create New Custom Application.
Upload	Click and upload an existing Custom Application. You can either drag and drop, or browse and choose the application file to be uploaded.
Activate	Click to send the selected Custom Applications to Edges.
Deactivate	Click to remove the selected Custom Applications from Edges.
More	Click **More**, and then click **Download JSON**, to download and reuse the JSON file of the selected Custom Application for other Partner users. This reduces the effort of creating same Custom Applications across different Partner users.

The other options available on this screen are:

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

Click **Save Changes** to save the Custom Applications.

Note:

- The **Save Changes** button appears only after creating at least one Custom Application.
- The maximum number of Custom Applications that can be created for each Partner is **250**.
- You cannot delete a Custom Application.

Next Steps

- Use the new Custom Application to create Business Policy and Firewall rules at Edge or Profile level.

  1. For Edge level creation, go to **Configure** > **Edges**. Select an Edge and then click **Business Policy** > **Add**. In the **Application** field, select **Define**, and choose the Custom Application from the drop-down menu. Click **Save Changes**.
  2. For Edge level creation, go to **Configure** > **Edges**. Select an Edge and then click **Firewall** > **Configure Firewall**. Under **Firewall Rules**, click **New Rule**. In the **Application** field, select **Define**, and choose the Custom Application from the drop-down menu. Click **Save Changes**.

  Note:

  - The **Application** drop-down menu lists all applications created through both, **Application Maps** and **Custom Applications**. A label is displayed against all custom applications for easy identification purpose.
  - The above steps are for Edge level creation of Business Policy and Firewall rules. You can follow the same steps for creating these rules at Profile level by navigating to **Configure** > **Profiles**.

The **Used By Profile** and **Used By Edges** columns on the **Custom Applications** main screen, display the details of the Profile and Edge(s) using the corresponding Custom Application. The Custom Applications that are associated to a Profile or an Edge cannot be deactivated.

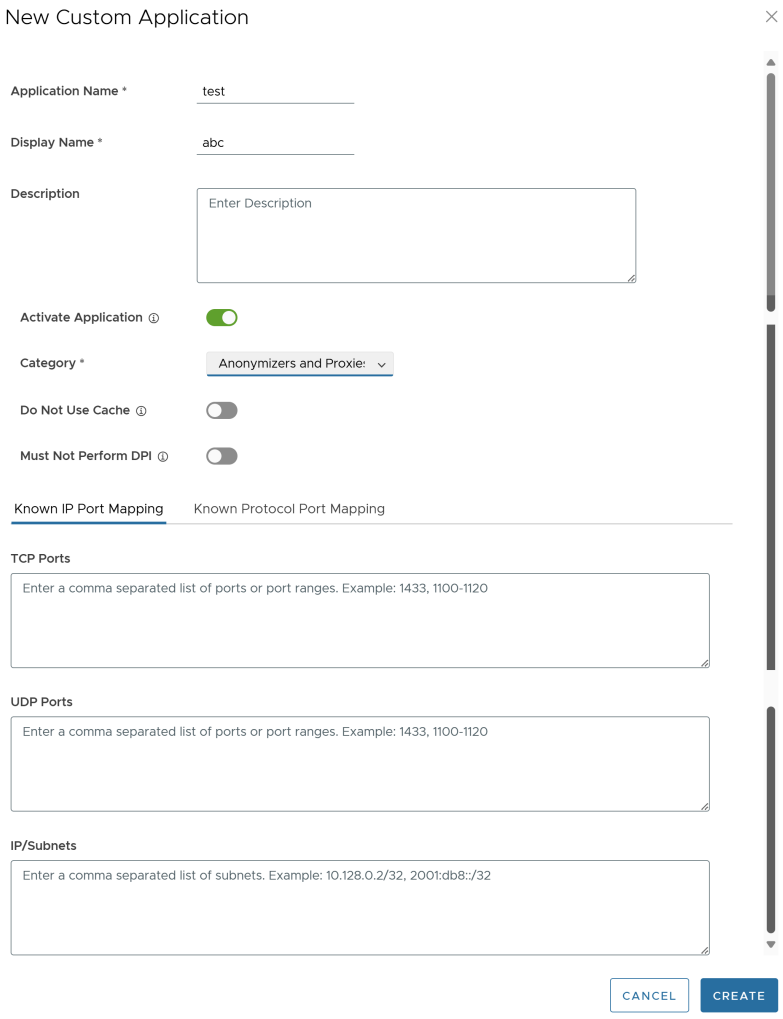
- To monitor the Custom Applications, go to **Monitor** > **Events** > **Applications** screen.

Create New Custom Application

You can create multiple Custom Applications.

Follow the below procedure to create a new Custom Application:

1. From the Partner Portal, click **Configure** > **Custom Applications** > **New Custom Application**. The following screen appears:



2. Enter details in the following fields:

Option	Description
Application Name	Enter a unique name for the Custom Application.
Display Name	Enter a unique display name.
Description	Enter a description. This field is optional.

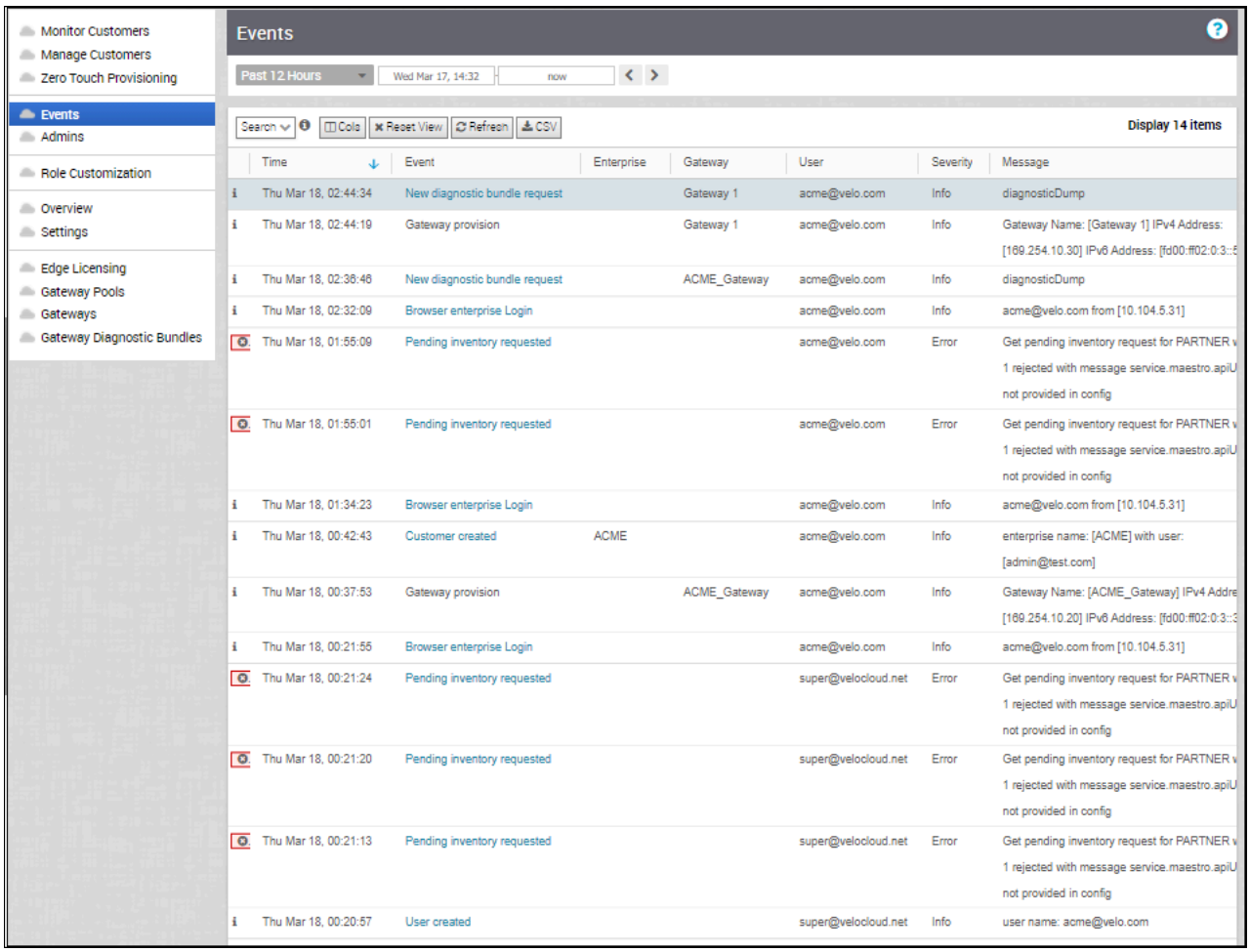
Option	Description
Activate Application	You can activate the application while creating it. An activated Custom Application is directly sent to the Edge when you save it.
Category	Select a category from the drop-down menu.
Do Not Use Cache	Slide the toggle button to activate slow-learning cache at Edge level. When activated, the Custom Applications do not use the cache, and their traffic is classified by Qosmos DPI, irrespective of IP-port or proto-port mappings.
Must Not Perform DPI	Slide the toggle button to deactivate DPI at Edge level. When activated, DPI is not used, even if **Do Not Use Cache** is activated, if traffic matches the known IP-port or protocol-port mapping.
Known IP Port Mapping	Enter the TCP ports, UDP ports, and IP/Subnets in a valid format.
Known Protocol Port Mapping	Enter the TCP and UDP ports in a valid format.

3. Click **Create** to save the new Custom Application. This application is then displayed on the **Custom Applications** main screen. The **State** column indicates whether the application is Active or Inactive.
4. Click **Cancel** to discard the entered details.

Monitor Events

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

In the Partner portal, click **Events**.



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

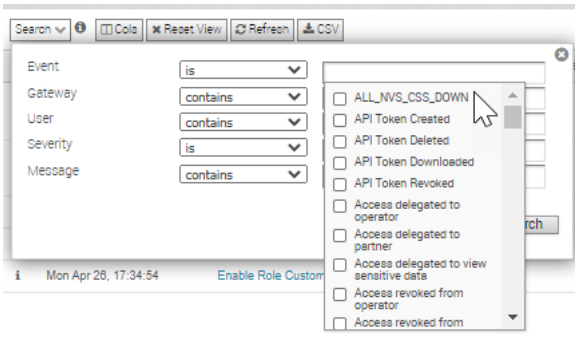
To view the older events, you can click the drop-down menu at the top of the page and choose the duration from the list. Alternatively, you can also enter the start and end dates at the top of the page to set a custom duration.

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

Once you choose or setup the duration, the page displays the events triggered during the selected period.

The page displays the following options:

- **Search** – Enter a term to search for a specific detail. Click the drop-down arrow to filter the view by specific criteria. In the Filter, click the field next to **Events** to view the list of Partner Events available and to filter by specific Events.

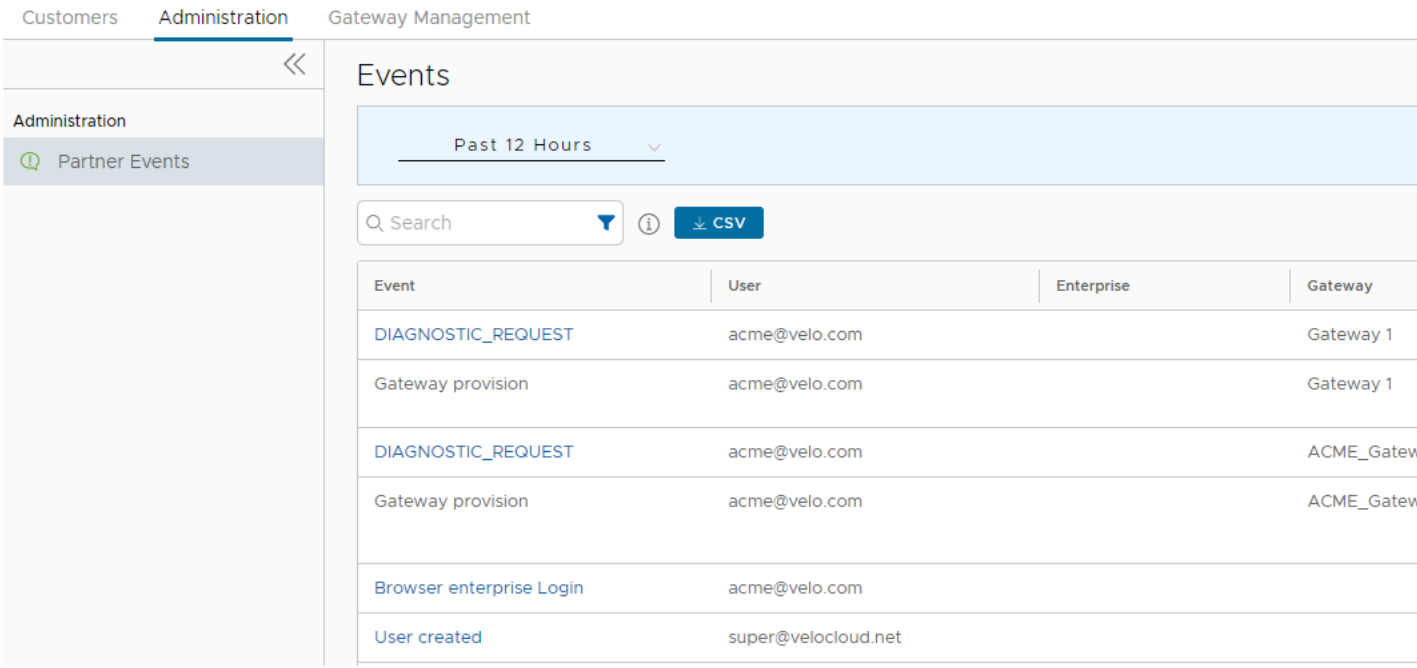


- **Cols** – Click and select the columns to be shown or hidden in the view.

- **Reset View** – Click to reset the view to default settings.
- **Refresh** – Click to refresh the details displayed with the most current data.
- **CSV** – Click to export all data to a file in CSV format.

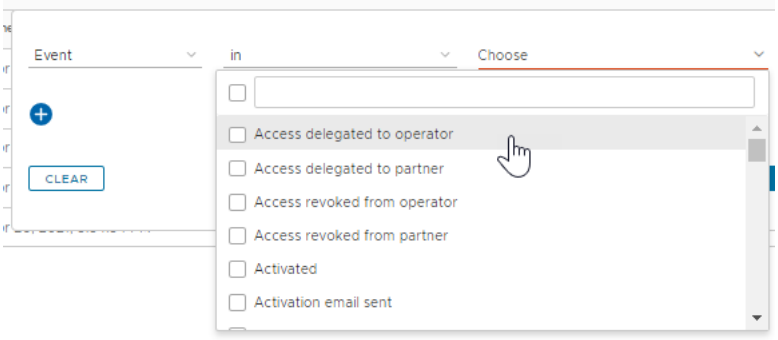
You can also view the Partner events using the new Orchestrator UI.

Click **Administration** > **Partner Events** to view the events.



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

In the **Search** field, enter a term to search for specific details. Click 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.

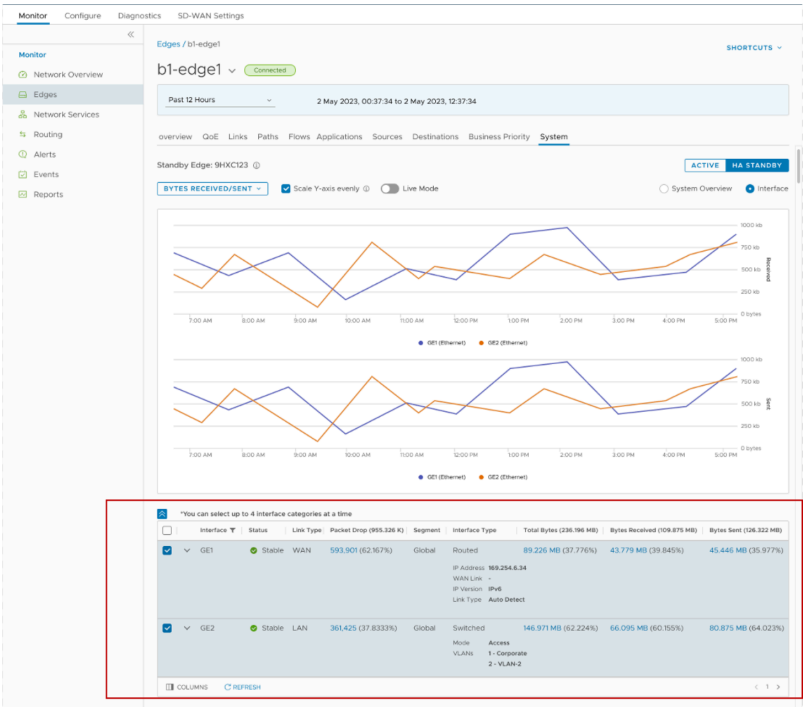


Click the **CSV** option to download a report of the events in CSV format.

Network Interface Statistics Monitoring

Starting from the 6.4.0 release, you can view both real time and historical interface statistics data, on the **Monitor** > **Edges** > **System** > **Interface** screen of the Orchestrator. This feature allows you to monitor data at the interface level.

To access the network interface stats, in the Partner portal, navigate to **Monitor** > **Edges** > **System**. On the **System** tab, the **System Overview** radio button is selected by default. Click the **Interface** radio button to view the interface statistics (stats) information.



There are two modes available:

- **Non-Live Mode**:
  - The non-live mode is activated by default.
  - It displays historical stats of an interface. Customers can view all the previously captured data.
  - This mode is supported on both **Active** and **HA Standby** Edges.
- **Live Mode**:
  - To view real time interface stats, toggle the **Live Mode** button to ON.
  - This mode is supported only on **Active** Edges.

The table below the graphs displays the following information:

Option	Description
Interface	Displays the interface name. The interfaces are GE, Loopback and SFPs.
Status	Displays the status of the interface.
Link Type	Displays the type of the link. Example: LAN, WAN, HA.
Packet Drop	Displays the packet drop details.
Segment	Displays the segment name.

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Interface Type</td><td>Displays the interface type, and the corresponding details depending on the type.
Routed: IP Address, WAN Link, IP Version, Link Type.
Switched: Mode, VLANs.
The interface mappings are listed in the table below:<table><tr><th>Interface Type</th><th>Interface is used for</th></tr><tr><td>Switched</td><td>LAN, HA</td></tr><tr><td>Loopback</td><td>N/A</td></tr><tr><td>Routed</td><td>WAN, none</td></tr></table></td></tr>
<tr><td>Total Bytes</td><td>Displays the total number of bytes.</td></tr>
<tr><td>Bytes Received</td><td>Displays the number of bytes received.</td></tr>
<tr><td>Bytes Sent</td><td>Displays the number of bytes sent.</td></tr>
</table>

Note: Click the check box against the interface to activate live mode for any selected interface. Customers can view up to four interfaces in the live mode.

Click **Columns** to hide or view the required columns. Click **Refresh** to view the latest data.

Insights

Starting from the 6.4.0 release, VeloCloud introduces an **Insights** tab in the Orchestrator. This tab is located in the top menu of the Orchestrator screen, next to the **Monitor** tab, and is activated by default. Both Enterprise and Partner users can access this tab.

The **Insights** tab displays information on various features based on Edge monitoring, configuring and troubleshooting. Currently, this tab displays information on the **Link Performance**.

The **Link Insights** feature provides insights on Edges across Enterprise. This helps in optimizing network performance, troubleshooting, managing costs, and improving user experience. This feature offers predictive insights on network links that helps Customers with opportunities for enhancements and upgrades, ensuring they can leverage the most efficient and advanced connectivity options available.

For more information, see Link Insights.

Link Insights

The **Link Insights** feature displays information on Edge incidents providing insights on link performance, reasons for failure, affected applications, traffic distribution and so on.

To access this feature, you must log into the Orchestrator as an Enterprise user. From the top menu, click **Insights**, and then from the left navigation, click **Link Insights**. The following screen is displayed:

The following information is displayed on this screen:

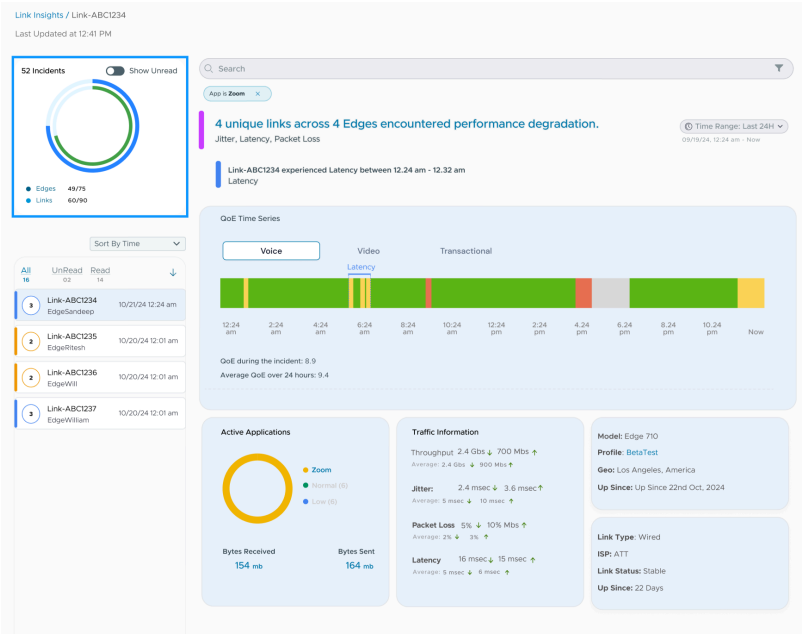
Option	Description
Incidents	Displays the summary of all the issues encountered on the links. The other sections are populated based on this summary. You can choose the data to be displayed on the screen, based on the following options in the drop-down menu: • Past 2 Hours • Past 24 Hours • Past 2 Weeks See the **Incidents** section below for more details.
Incident Geo Distribution	Turn on the **Map View On** toggle button to view the incidents by Edge locations. To hide this section, turn off the toggle button.

Option	Description
Incident Time Distribution	Turn on the **Time Distribution On** toggle button to view the exact time when the incidents have occurred with respect to Packet Loss, Latency, Jitter, and Mixed. You can select the respective check boxes to view the corresponding data. To hide this section, turn off the toggle button.
Involved ISPs	Displays information on the Internet Service Provider.
Involved Applications	Displays information on applications that were running on the network, at the time of the incident.
Incident Impact	Displays information about overall incidents based on Packet Loss, Latency, Jitter, and Mixed, on Edges and Links.
WAN Exits	Provides information on where the traffic is exiting from the current Edge.
Traffic Distribution	Displays information on the traffic distribution with respect to Voice, Video, and Transactional.

You can use the **Search** option to search for a particular section on the screen. Click the filter icon and set filters to further narrow down your search results.

Incidents

- Displays the number of Edges and Links that are affected.
- Next to the pie diagram is a statement explaining the issue along with the reason (Loss, Latency, or Jitter).
- The corresponding incident data is displayed on the left of the screen. You can sort this data by time. To view more information about a specific incident, click the tile displaying the incident. This opens a detailed view displaying the link information and the date and time when the incident occurred, along with the following details:



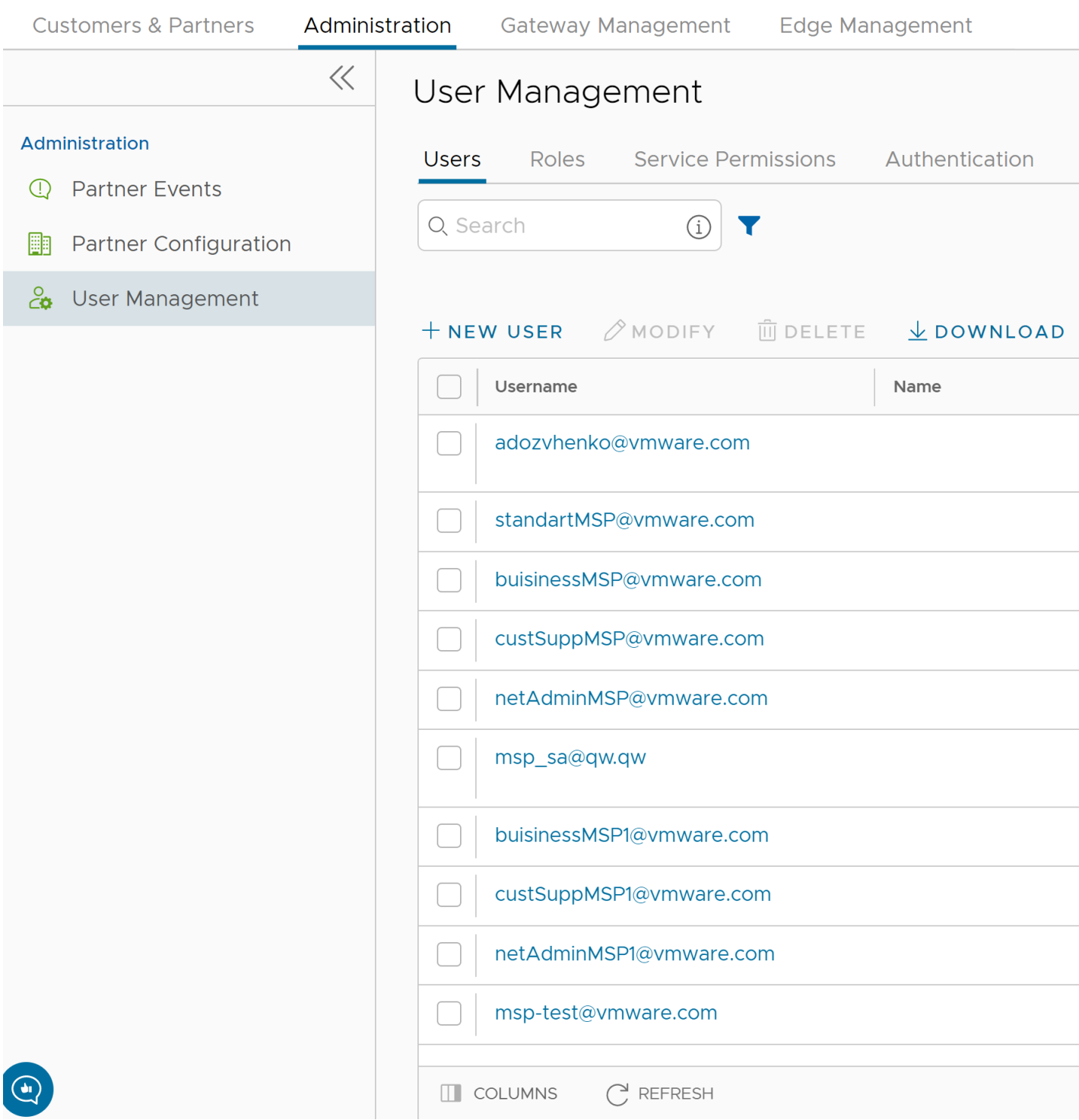
QoE Time Series	Displays the Quality of Experience information for the selected incident, with respect to Voice, Video, and Transactional. It also displays the QoE score during the incident and the average QoE score during the whole period.
Active Applications	Displays the active applications that were running at the time when the selected incident occurred.
Traffic Information	Displays the traffic that was flowing during the selected incident.

This screen also displays Edge information that includes Model, Profile, Geo, Link Type, and so on.

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:



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

For more information on each of these tabs, see:

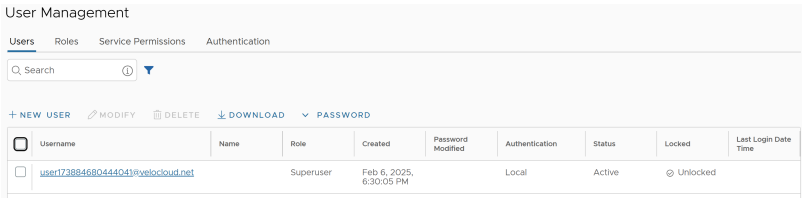
- Users
- Roles
- Service Permissions
- Authentication

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



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

Option	Description
New User	Creates a new user. For more 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 clicking the username link.
Delete	Deletes the selected user. You cannot delete the default users.
Download	Click this option to download the details of all the users into a file in a CSV format.
Password	Click this option and choose to either enforce the new password policy or reset the already enforced policy, for the selected user. You can modify the password policies by navigating to the **Authentication** tab. **Note:** Current user sessions are not terminated.

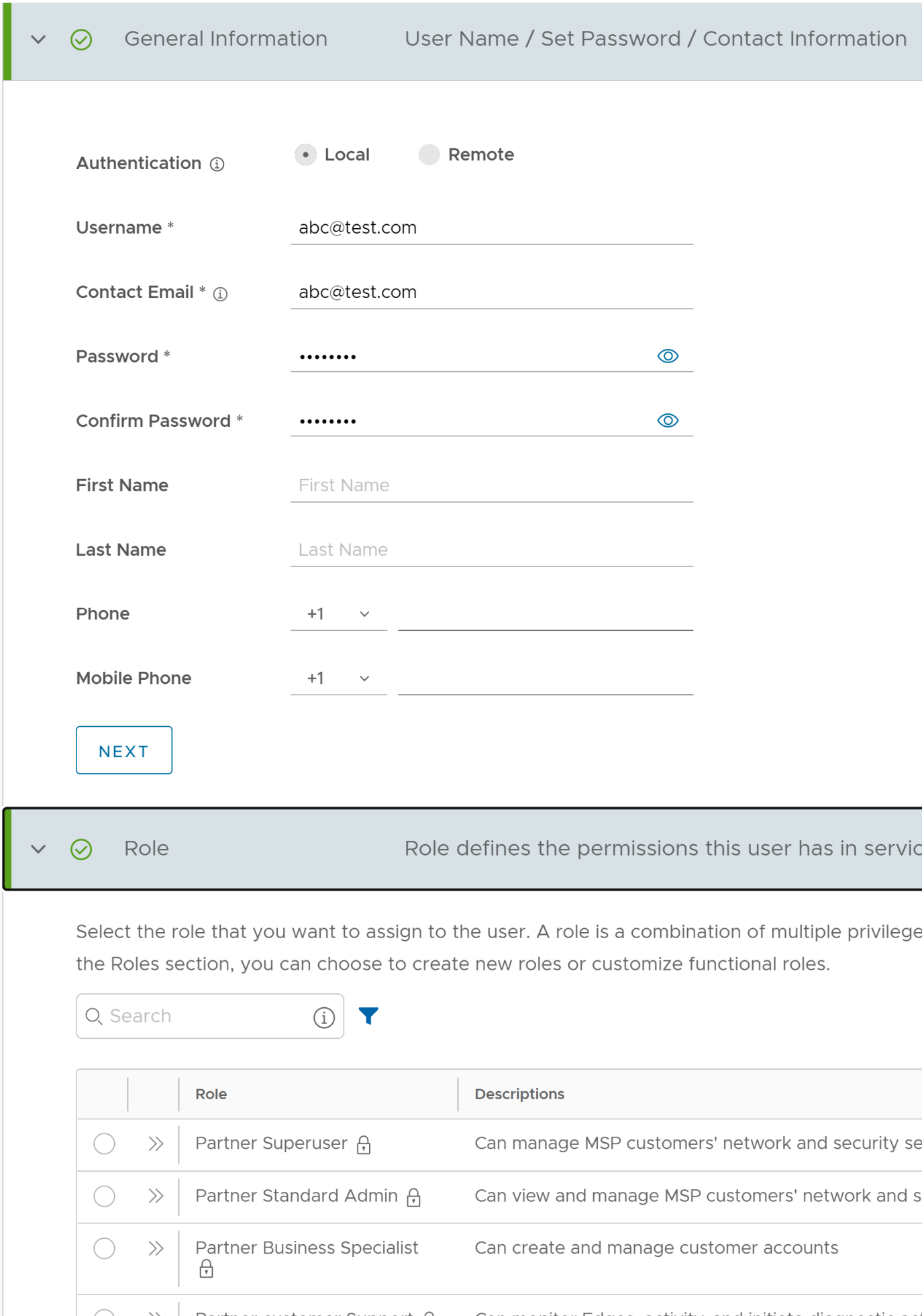
5. The following are the other options available in the **Users** tab:

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.
Show or Hide Columns	Click and select the columns to be displayed or hidden on the page.
Refresh	Click to refresh the page to display the most current data.

Add New User

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

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


General Information
User Name / Set Password / Contact Information
Authentication
Local
Remote
Username *
abc@test.com
Contact Email *
abc@test.com
Password *
Confirm Password *
First Name
First Name
Last Name
Last Name
Phone
+1
Mobile Phone
+1
NEXT
Role
Role defines the permissions this user has in servic
Select the role that you want to assign to the user. A role is a combination of multiple privilege
the Roles section, you can choose to create new roles or customize functional roles.
Search
Role
Descriptions
Partner Superuser
Can manage MSP customers' network and security se
Partner Standard Admin
Can view and manage MSP customers' network and s
Partner Business Specialist
Can create and manage customer accounts

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.

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 click **Add User**.
   The new user appears in the **User Management** > **Users** page. Click 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 more 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.

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.

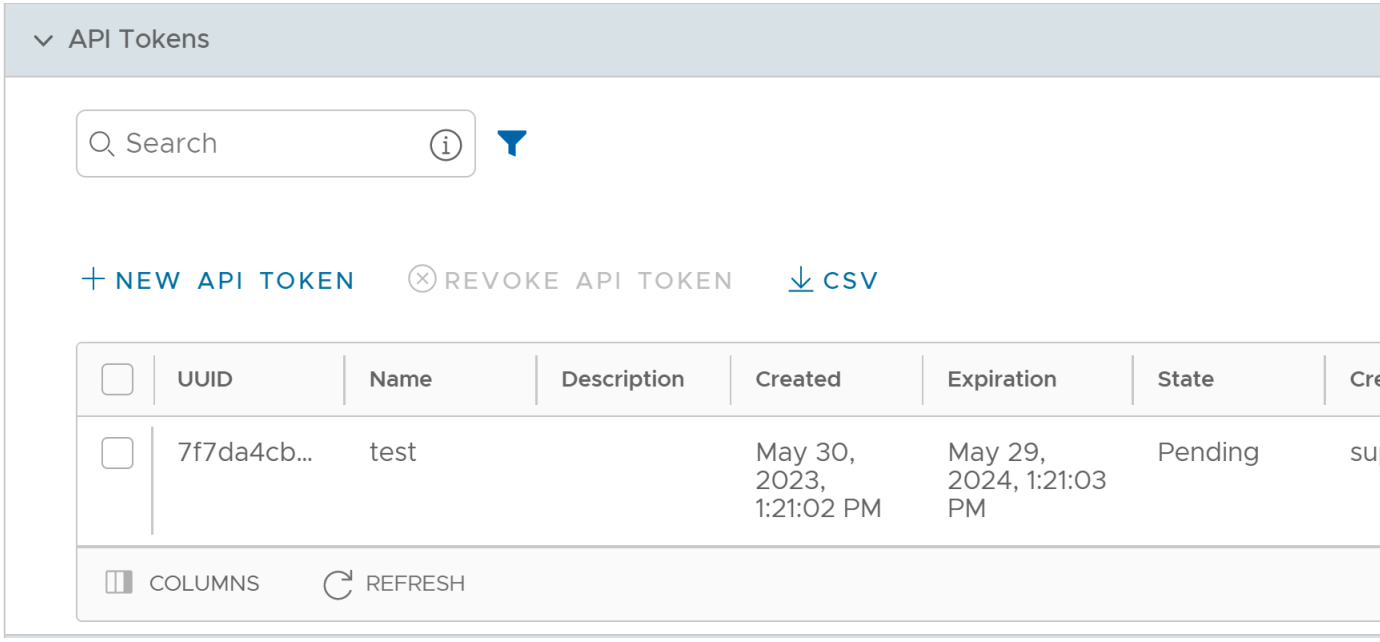
Any user can create tokens based on the privileges they have been assigned to their user roles, except the Business Specialist users.

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

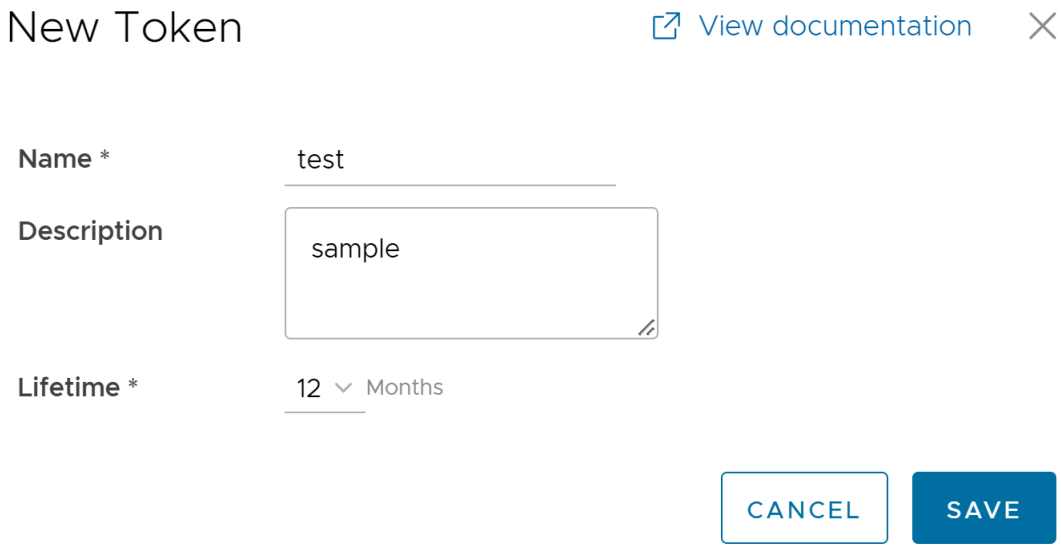
- Enterprise users can Create, Download, and Revoke tokens for them.
- Partner Super users can manage tokens of Enterprise users, if the Enterprise user has delegated user permissions to the Partner.
- Partner Super users can only create and revoke the tokens for other users.
- Users can download only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

To manage the API tokens:

1. Login to the as a Partner and navigate to **Administration** > **User Management** > **Users**.
2. Select a user and click **Modify** or click the link to the username. Go to the **API Tokens** section.



3. Click **New API 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. Click **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 click **Revoke API Token**. The status of the token is displayed as **Revoked**.
7. Click **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.

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

```
curl -k -H "Authorization: Token <Token>"
```

```
  -X POST https://vco/portal/
  -d '{ "id": 1, "jsonrpc": "2.0", "method": "enterprise/
getEnterpriseUsers", "params": { "enterpriseId": 1 }}'
```

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

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	Click and select the columns to be displayed or hidden on the page.
Refresh	Click to refresh the page to display the most current data.

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 one or more of the following services: SD-WAN, Global Settings, SD-WAN Client, Edge Compute, and Edge Intelligence (EI). 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:

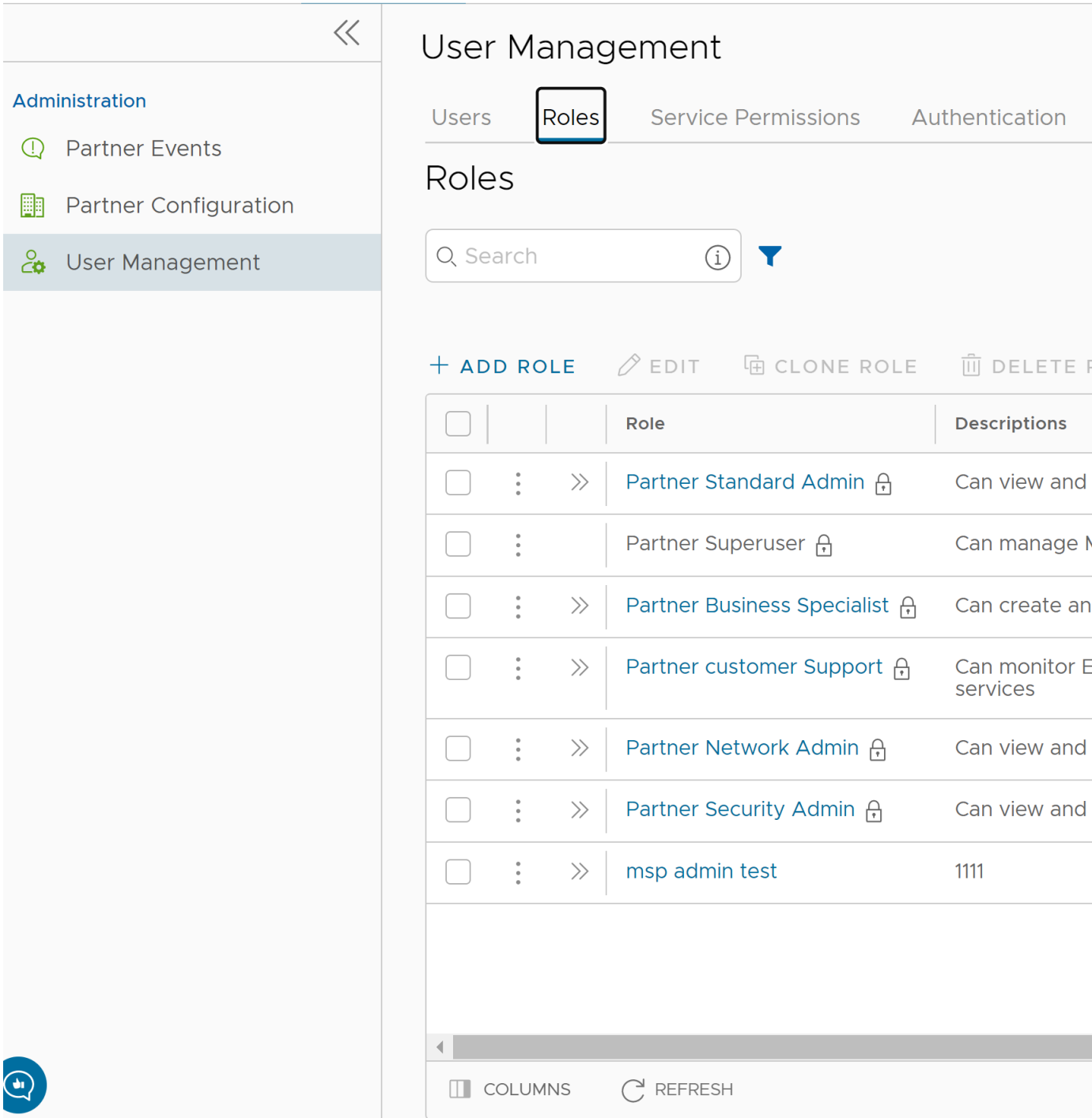
Role	SD-WAN Service	Global Settings Service
Partner Standard Admin	SD-WAN Partner Admin	Global Settings Partner Admin
Partner Security Admin	SD-WAN Security Partner Admin	Global Settings Partner Admin
Partner Network Admin	SD-WAN Partner Admin	Global Settings Partner Admin
Partner Superuser	Full Access	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 more 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 as a Partner.
2. Click **Administration** from the top menu.
3. From the left menu, click **User Management**, and then click the **Roles** tab. The following screen appears:



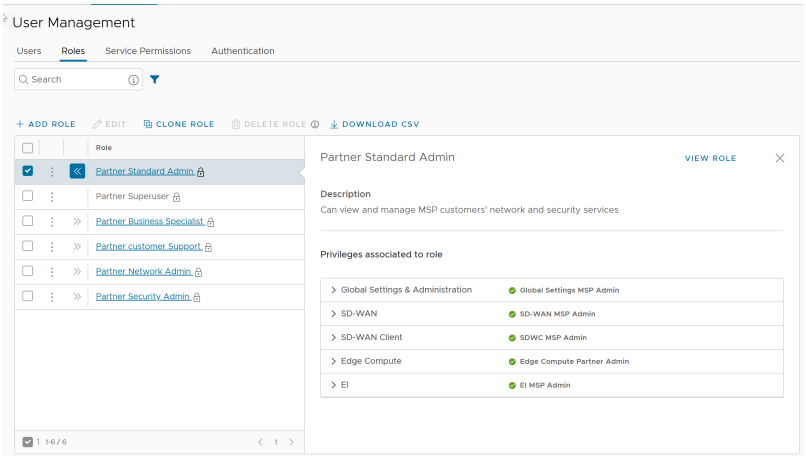
4. On the **Roles** screen, you can perform the following activities:

Option	Description
Add Role	Creates a new custom role. For more 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.

Option	Description
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. Click the Open icon ">>" displayed before the Role link, to view more details about the selected Role, as shown below:



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

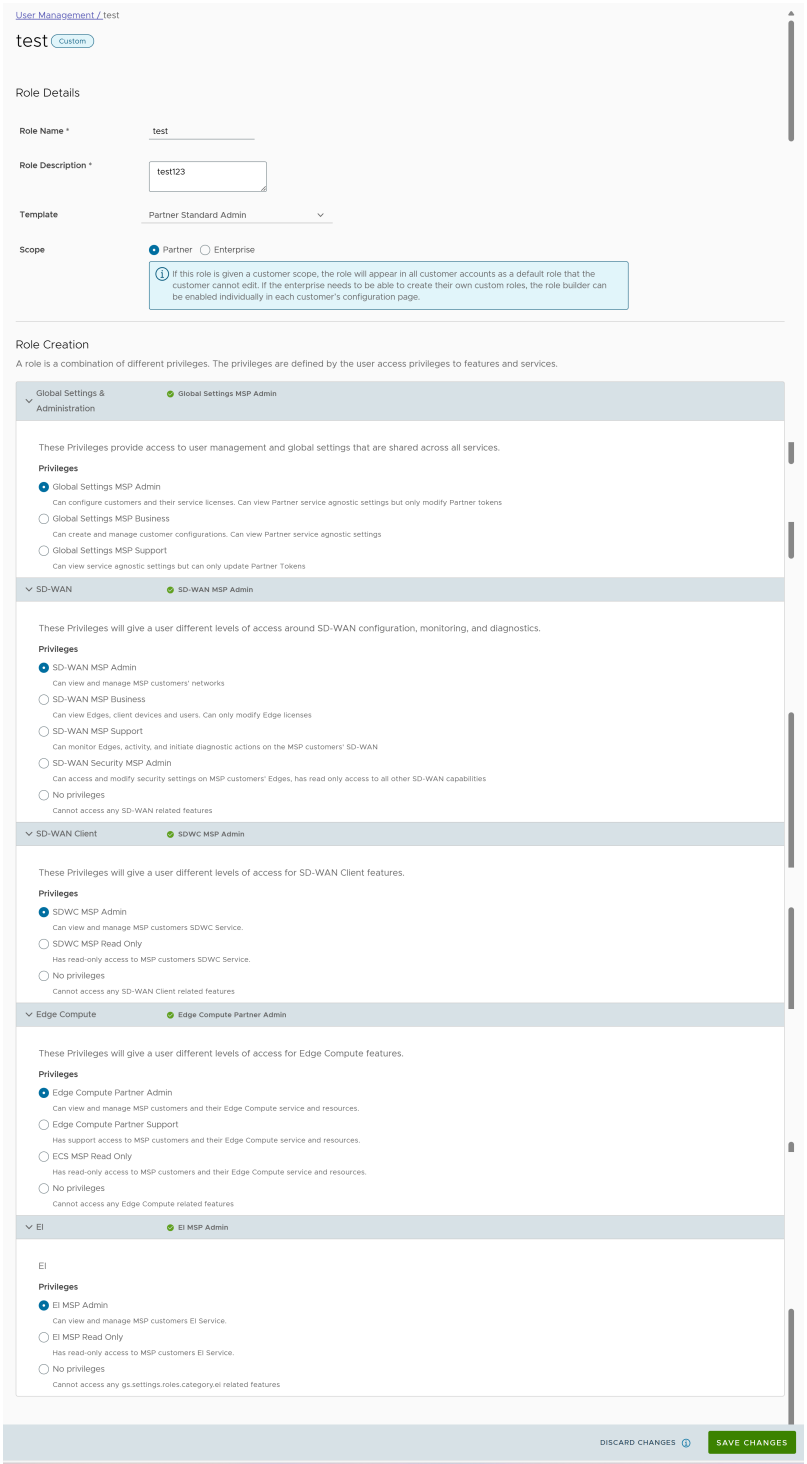
Option	Description
Search	Enter a search term to search for the matching text across the table. Use the advanced search option to narrow down the search results.
Columns	Click and select the columns to be displayed or hidden on the page.
Refresh	Click to refresh the page to display the most current data.

Add Role

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

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

3. From the left menu, click **User Management**, and then click the **Roles** tab.
4. Click **Add Role**.



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

Option	Description
Role Details	
Role Name	Enter a name for the new role.
Role Description	Enter a description for the role.

Option	Description
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**.
SD-WAN Client	These privileges provide the Partner or Enterprise Administrator with different levels of access around SD-WAN Client features. You can optionally choose a SD-WAN Client privilege. The default value is **No Privileges**.
Edge Compute	These privileges provide the Partner or Enterprise Administrator with different levels of read and/or write access around Edge Compute features. You can optionally choose a Edge Compute function privilege. The default value is **No Privileges**.
EI	These privileges provide the Partner or Enterprise Administrator with different levels of read and/or write access around Edge Intelligence (EI) features. You can optionally choose an EI function privilege. The default value is **No Privileges**.

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

Service Permissions

Service Permissions allow you 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.

Roles can be customized by changing the service permissions held by each role. You can customize both, default roles and new roles. Roles are created based on the selected default role. Operator, Partner, and Enterprise roles are defined separately. So, there are default roles for each level, such as Operator Superuser, Partner Standard Admin, and Enterprise Support.

When customizing a role, you must select both, the user level and the role. Typically, Operator roles have more privileges by default, than Partners or Enterprise Customers. When creating a user, you must assign a role to the user. Any change to that specific role's privileges is immediately applied to all users assigned to that role. Role customizations only apply to one role at a time. For example, changes to Operator Standard Admin roles do not get applied to Enterprise Standard Admin roles.

For more information, see the topic **Roles**.

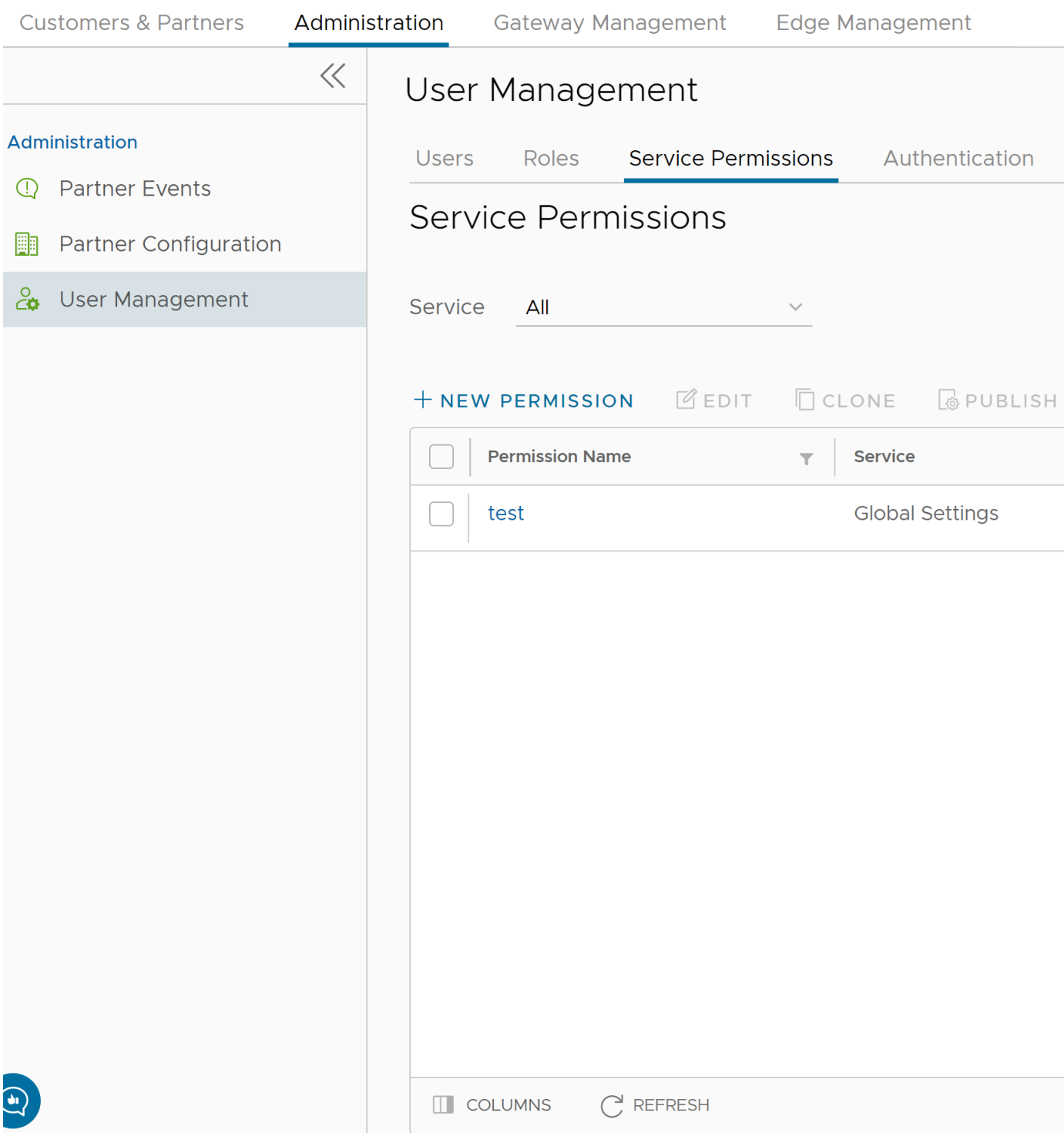
The Service Permissions are applied to the privileges as follows:

- 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 as a Partner.
2. Click **Administration** from the top menu.
3. From the left menu, click **User Management**, and then click the **Service Permissions** tab. The following screen appears:



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

Option	Description
Service	Select the service from the drop-down menu. The available services are: • **All** • **Global Settings** • **SD-WAN** • **Edge Intelligence** Each service comprises of a set of related permissions grouped together. 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 set of privileges. The newly created permission is displayed in the table. For more information, see the topic New Permission.
Edit	Allows you to edit the settings of the selected permission. You can also click 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. For example, customizations defined by an Enterprise Superuser take precedence over customizations defined by an Operator Superuser.
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. • **Unpublish Permissions**: Allows you to unpublish the selected permission changing it to a 'Draft' state. You can modify the permission and save it again, which changes it to "Published" state.

5. The table displays the following columns:

Option	Description
Permission Name	Displays the newly created permission.
Service	Displays the service of the new permission.
Scope	Displays the scope of the new permission.
Role Associated	Displays the associated roles using the same Privilege Bundle.
Last Modified	Displays the date and time when the permission was last modified.
Published	Displays either "Published" or "Draft" depending on the state of the permission.

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

Option	Description
Columns	Click and select the columns to be displayed or hidden on the page.
Refresh	Click to refresh the page to display the most current data.

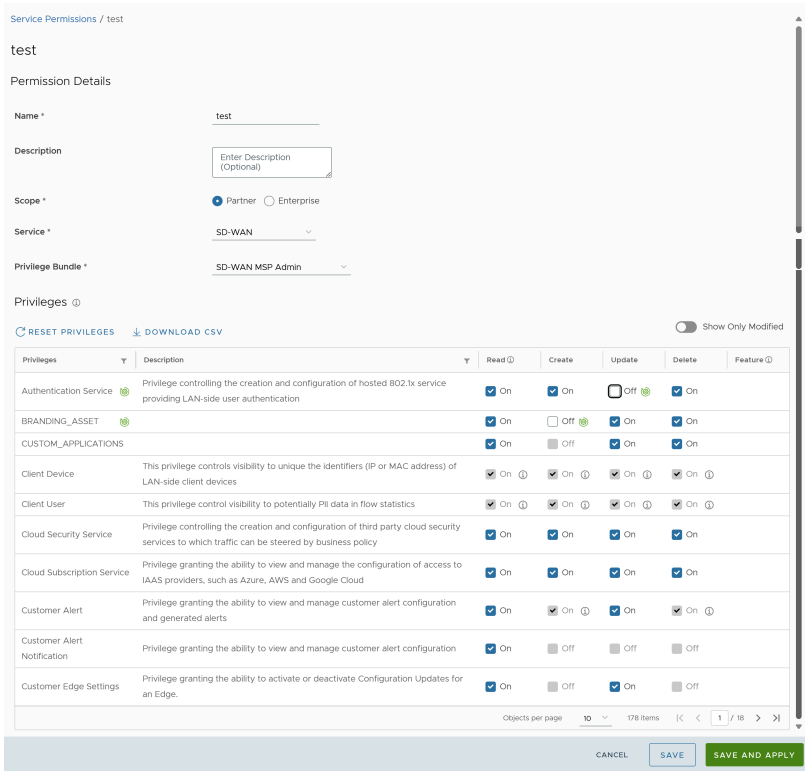
Note: Service Permissions are version dependent, and a service permission created on an Orchestrator using an earlier software release will not be compatible with an Orchestrator using a later release. For example, a service permission created on an Orchestrator that is running Release 3.4.x does not 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.

New Permission

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

To add a new permission, perform the following steps:

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



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

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** • **Edge Intelligence**
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.

To activate or deactivate a specific privilege, select or deselect the corresponding check box, in the **Privileges** table. The available check boxes are **Read**, **Create**, **Update**, and **Delete**.

Starting from the release 6.4.0, a green icon is displayed whenever a privilege is modified. This icon is displayed next to the modified check box and the privilege name.

Some privileges do not support selection of an independent action. In this case, if you select any one action check box, all the other check boxes get selected too. A tool tip is provided for such privileges. Also, the **Read** action

check box does not allow independent selection. When selected, all the other check boxes for that particular privilege also get automatically selected.

Note: You can edit only those privileges that are eligible for customization.

6. Slide the **Show Only Modified** toggle button, located at the top right of the privileges table, to view only the modified privileges.
7. Click **Reset Privileges** to reset all the changes.
8. Click **Download CSV** to download the list of all privileges, their description, and associated actions, into a file in a CSV format. You can choose from the below options:

Default Privileges	Downloads the original privileges ignoring all the current modifications.
Modified Privileges	Downloads only the privileges that were modified.
Current Privileges	Downloads all the current privileges.

Note: If you click **Reset Privileges**, and then click **Download CSV**, the **Default Privileges** and **Current Privileges** options, both display the same list.

9. Click **Save** to save the new permission. Click **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.

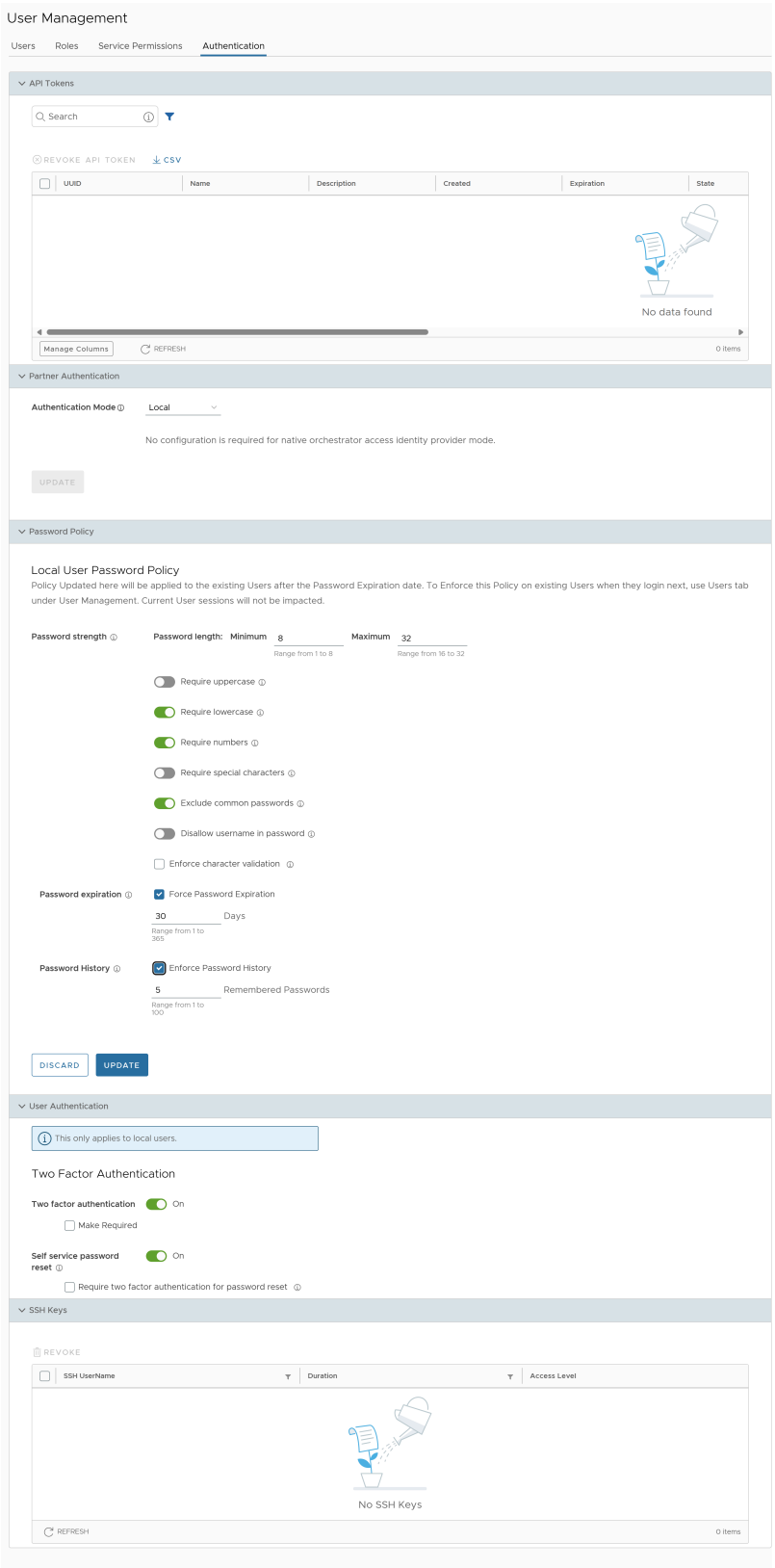
The new permission is displayed on the **Service Permissions** page. If you create another permission using the same scope and service, the privilege displays the last modified settings by default.

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



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 enables to authenticate users from OpenID Connect (OIDC)-based Identity Providers (IdPs).

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

  - AzureAD
  - Okta
  - OneLogin
  - PingIdentity
  - VMwareCSP

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

Partner Authentication

Authentication Mode ⓘ Single Sign-On

ⓘ Remember to set up https://169.254.8.2/login/ssologin/openidCallback as an allowed redirect URL

Single Sign-on Setup

Identity Provider Template ⓘ AzureAD

OIDC well-known config URL * ⓘ www.test.com

Issuer test1

Authorization Endpoint www.vmware1.com

Token Endpoint www.vmware2.com

JSON Web KeySet URI www.vmware3.com

User Information Endpoint www.vmware4.com

Client ID * ⓘ test123

Client Secret * ⓘ ••••••••••••••

Enter new value to change client secret

Scopes openid,profile,email,offline_access

Role Setup

Role Type ◯ Use default role ● Use identity provider role

Role Attribute ⓘ roles

Partner Role Map ⓘ

Orchestrator Role Name	Identity Provider Role Name
MSP Superuser	

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

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

SSH Keys

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

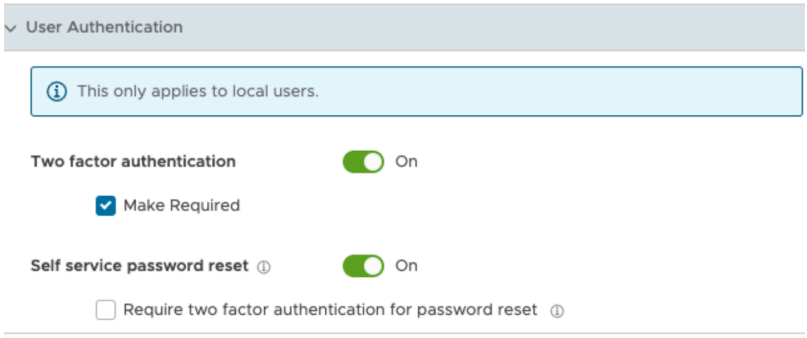
As a Partner, you can also revoke an SSH Key.

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

For more information, see Configure User Account details.

User Authentication

You can choose to activate or deactivate **Two factor authentication** feature for a Partner user.

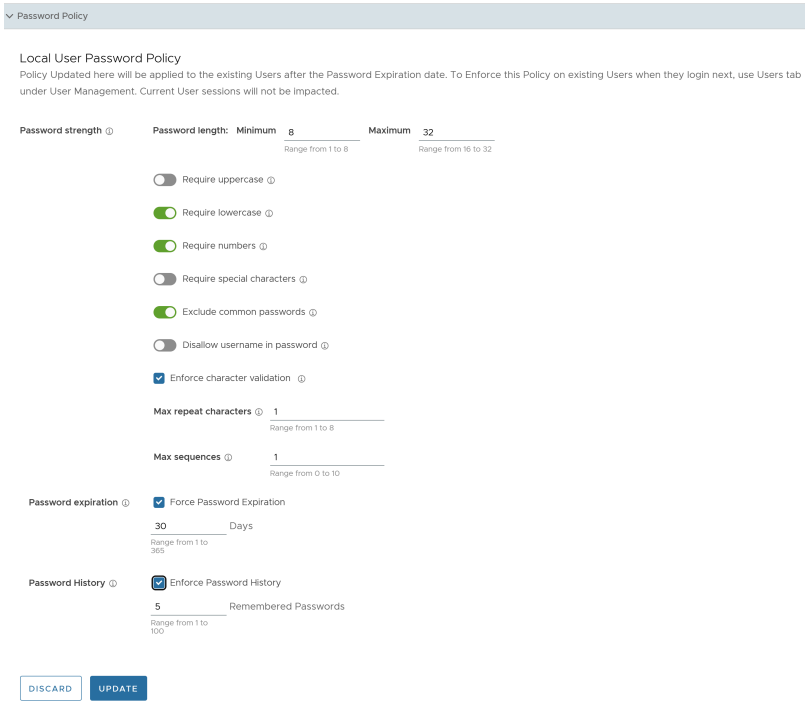


Option	Description
Two factor authentication	Slide the toggle button to activate this feature for all users. Select the **Make Required** check box to make this authentication mandatory for all users.
Self service password reset	Slide the toggle button to allow users to change their passwords using the link on the Login screen. Select the **Require two factor authentication for password reset** check box to make this authentication mandatory for all users. This makes the two factor authentication a required step before a user resets their password.

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

Password Policy

Starting from the release 6.4.0, Partner Superusers can set their own password policies directly from the Authentication screen. This section appears when the **Authentication Mode** is set to **Local**.



Option	Description
Password Strength	
Password length	Specify the minimum and maximum length of the password. The minimum length value must be in the range from **1** to **8**, whereas the maximum length value must be in the range from **16** to **32**. The default values are **8** and **32** respectively.
Require uppercase	Slide the toggle button to activate this parameter. If activated, the password must contain at least one uppercase letter.
Require lowercase	Slide the toggle button to activate this parameter. If activated, the password must contain at least one lowercase letter.
Require numbers	Slide the toggle button to activate this parameter. If activated, the password must contain at least one number.
Require special characters	Slide the toggle button to activate this parameter. If activated, the password must contain at least one special character. Hover the mouse on the information icon to view the valid special characters.
Exclude common passwords	Slide the toggle button to activate this parameter. If activated, users are not allowed to use the most commonly used passwords.
Disallow username in password	Slide the toggle button to activate this parameter. If activated, username cannot be set as the password.

Option	Description
Enforce character validation	Select this check box to ensure that the password meets the following criteria for strength and security: • **Max repeat characters**: Enter the maximum number of characters that can be repeated in the password. The accepted range is from **1** to **8**. The default value is **1**. • **Max sequences**: Enter the maximum number of consecutive characters or sequences that can be allowed in the password. The accepted range is from **0** to **10**. The default value is **1**.
Password Expiration	Select the **Force Password Expiration** check box and set the duration after which users must change their passwords. The accepted range is from **1** to **365**. The default value is **30**.
Password History	Select the **Enforce Password History** check box and enter a value that determines the number of previously created passwords that cannot be reused as the new password. This enhances the overall security. The accepted range is from **1** to **100**. The default value is **5**.

Click **Update** to save the new settings.

Click **Discard** to reset the settings.

Users who are already logged in are not affected by this update. To enforce the new password policy, an Enterprise Superuser must perform the following steps:

- Navigate to **User Management** > **Users**, and select a user.
- Click **Password** > **Enforce Policy**, and then click **Yes, Enforce**.

This forces the selected user to change their password as per the new password policy. Current user sessions are not terminated.

The **Password Modified** column on the **Users** screen, displays the date and time when the user has modified the password.

Session Limits

Note: To view this section, an Operator user must navigate to the **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:

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.

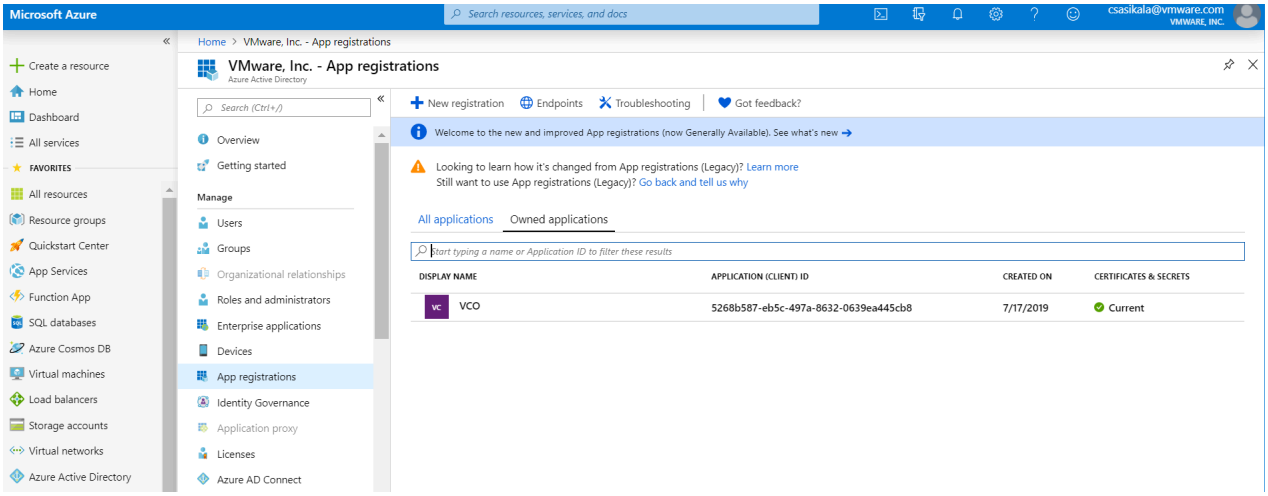
Click **Update** to save the selected values.

Configure Azure Active Directory for Single Sign On

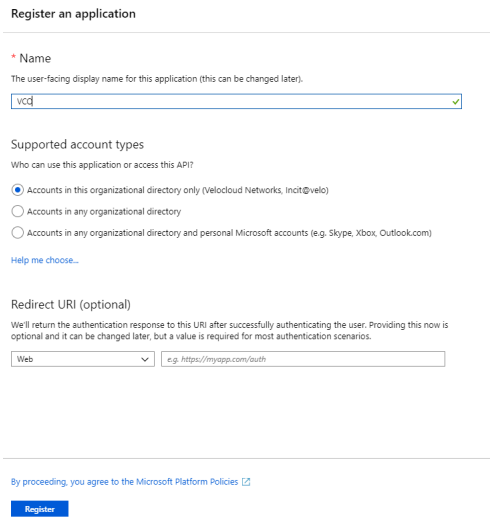
To set up an OpenID Connect (OIDC)-based application in Microsoft Azure Active Directory (AzureAD) for Single Sign On (SSO), perform the following steps.

Ensure you have an AzureAD account to sign in.

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



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



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

   In the

   application, at the bottom of the

   Configure Authentication

   screen, you can find the redirect URL link. Ideally, the

   redirect URL will be in this format: https://<Orchestrator URL>/login/ssologin/openidCallback.

e) Click **Register**.

Your

application will be registered and displayed in the

All applications

and

Owned applications

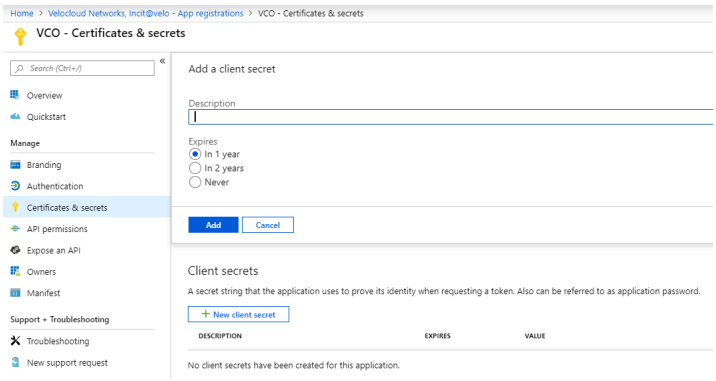
tabs. Make sure to note down the Client ID/Application ID to be used during the SSO configuration in

.

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

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

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

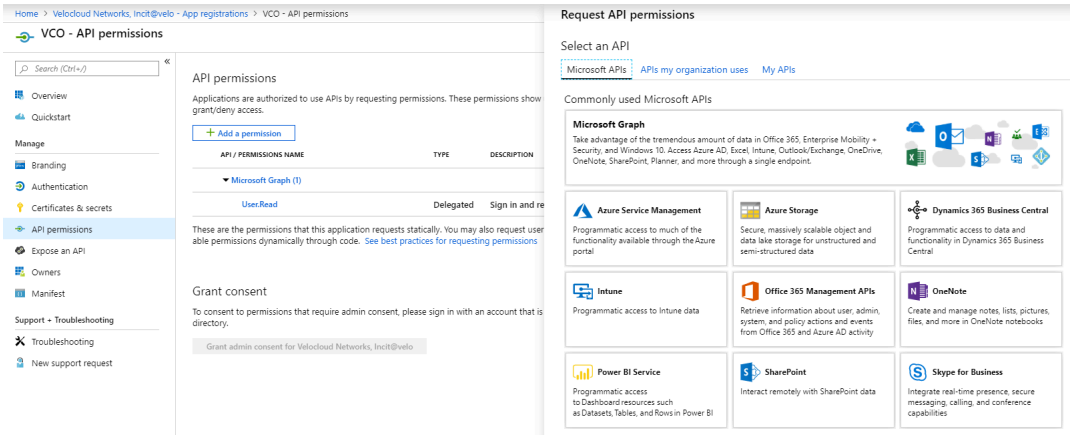


i) Provide details such as description and expiry value for the secret and click **Add**.

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

.

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

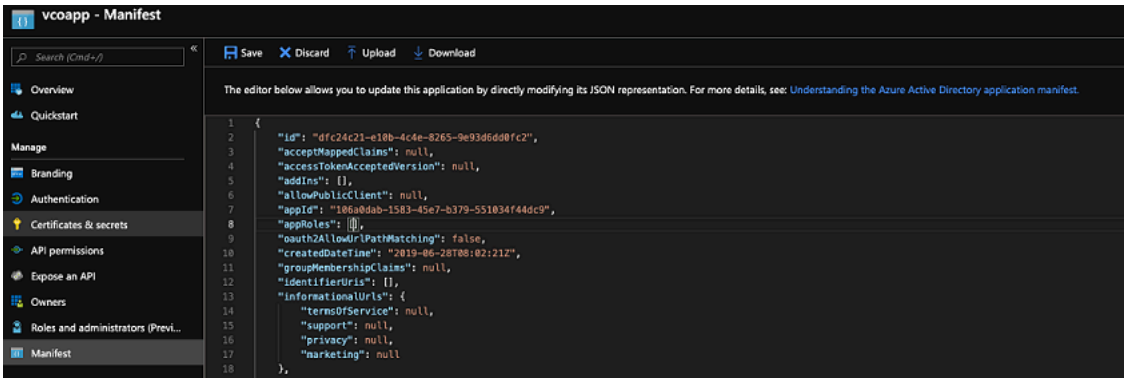


k) Click **Microsoft Graph** and select **Application permissions** as the type of permission for your application.

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

m) Click **Add permissions**.

n) To add and save roles in the manifest, click on your application and from the application **Overview** screen, click **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.



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

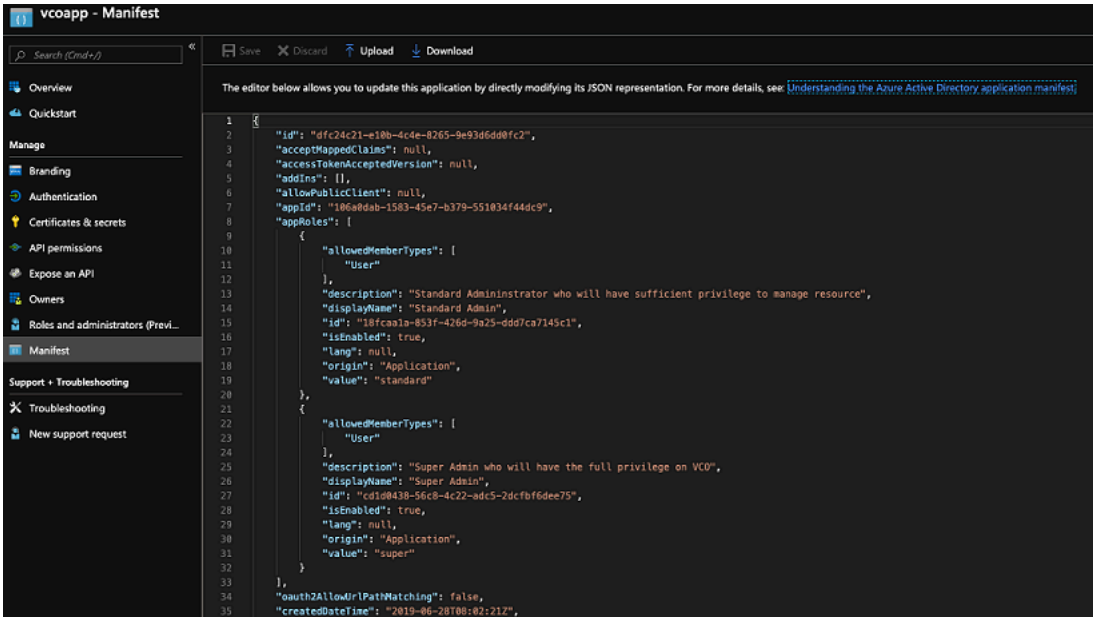
Note: The value property from `appRoles` must be added to the **Identity Provider Role Name** column of the **Role Map** table, located in the **Authentication** tab, in order to map the roles correctly.

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 ",
            "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()`

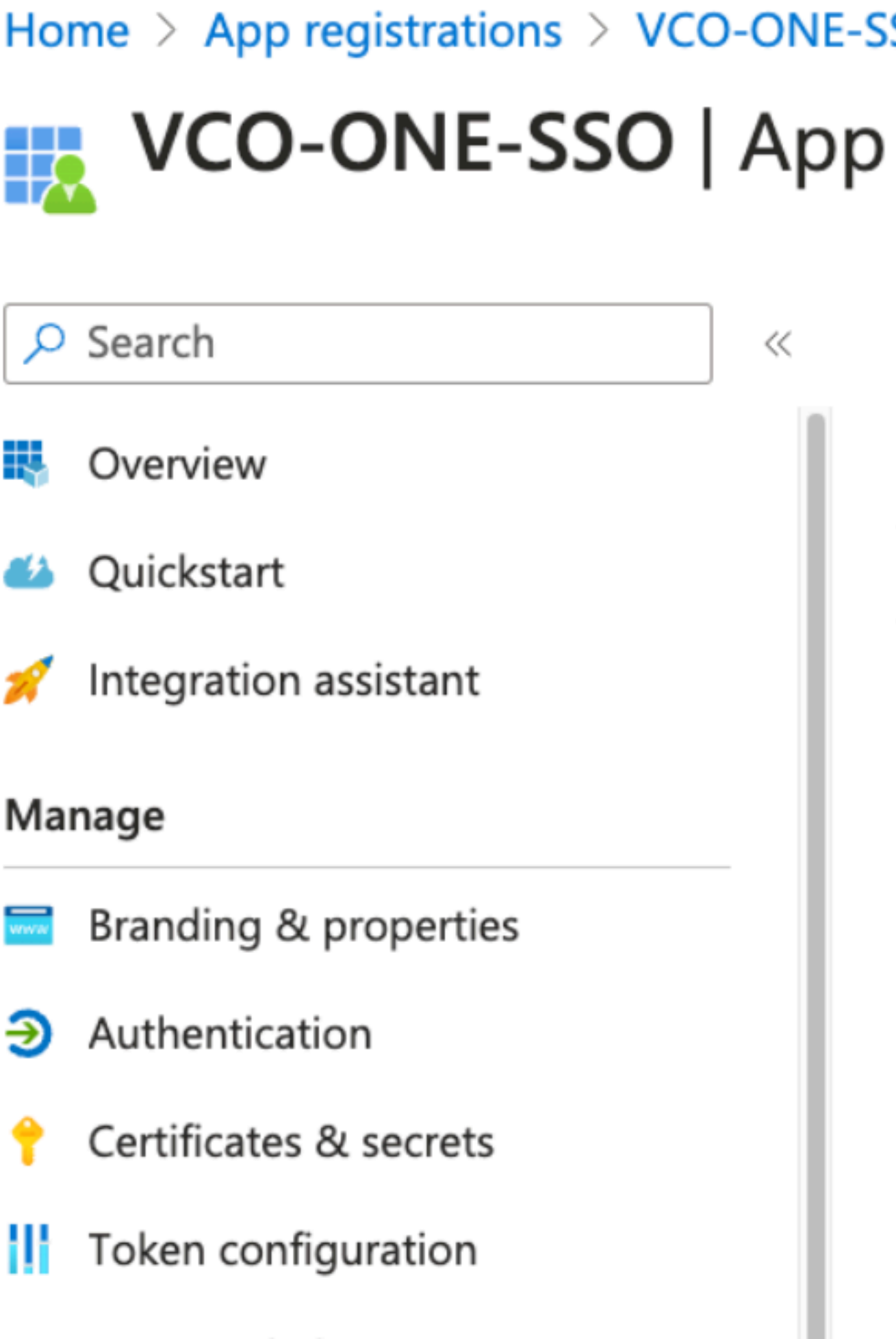


Roles are manually set up in the

, and must match the ones configured in the

Microsoft Azure

portal.


Home > App registrations > VCO-ONE-S
VCO-ONE-SSO | App
Search
Overview
Quickstart
Integration assistant
Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration

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

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

Configure Single Sign On in .

Configure Okta for Single Sign On

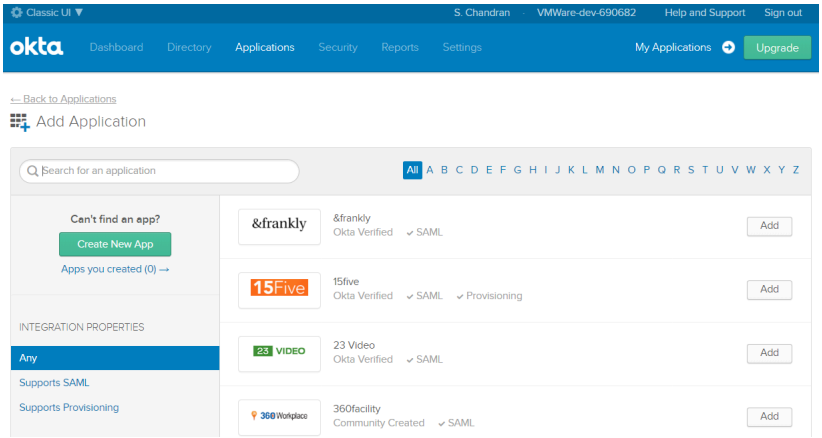
To support OpenID Connect (OIDC)-based Single Sign On (SSO) from Okta, you must first set up an application in Okta. To set up an OIDC-based application in Okta for SSO, perform the steps on this procedure.

Ensure you have an Okta account to sign in.

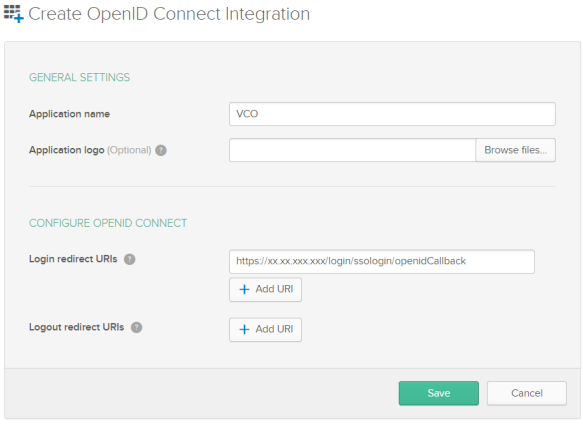
1. Log in to your Okta account as an Admin user.
   The **Okta** home screen appears.

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

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



   b) Click **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 click **Create**.
   The **Create OpenID Connect Integration** screen appears.



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 application uses as the callback endpoint.

In the

application, at the bottom of the

Configure Authentication

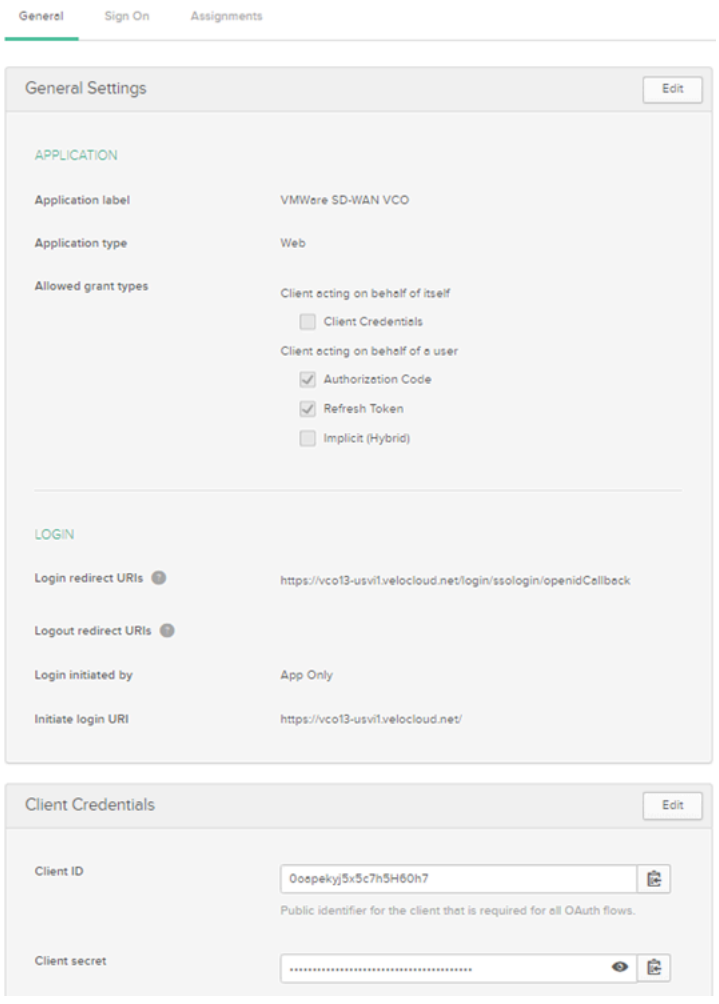
screen, you can find the redirect URL link. Ideally, the

redirect URL will be in this format: https://<Orchestrator URL>/login/ssologin/openidCallback.

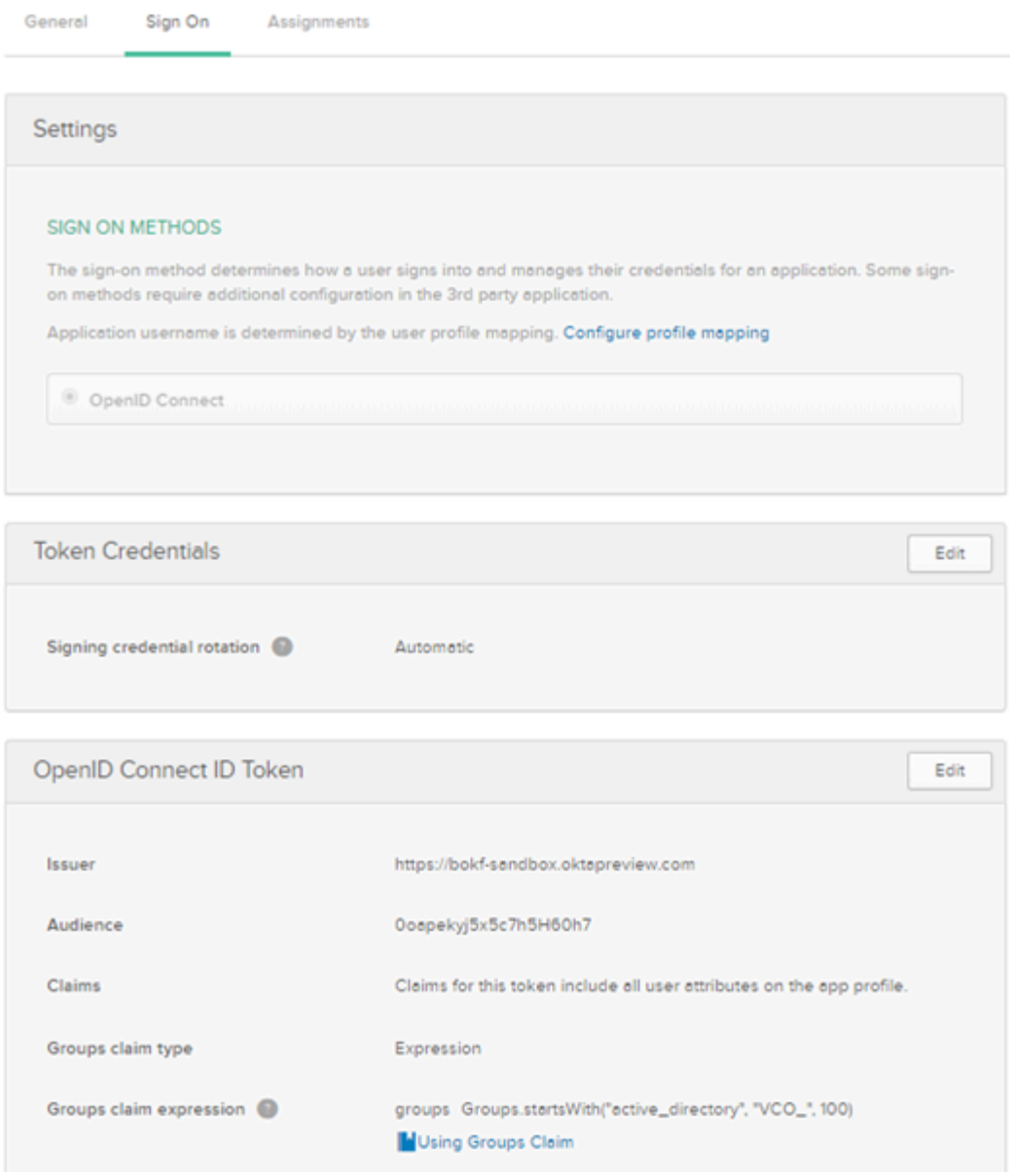
g) Click **Save**. The newly created application page appears.
h) On the **General** tab, click **Edit** and select **Refresh Token** for Allowed grant types, and click **Save**.

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

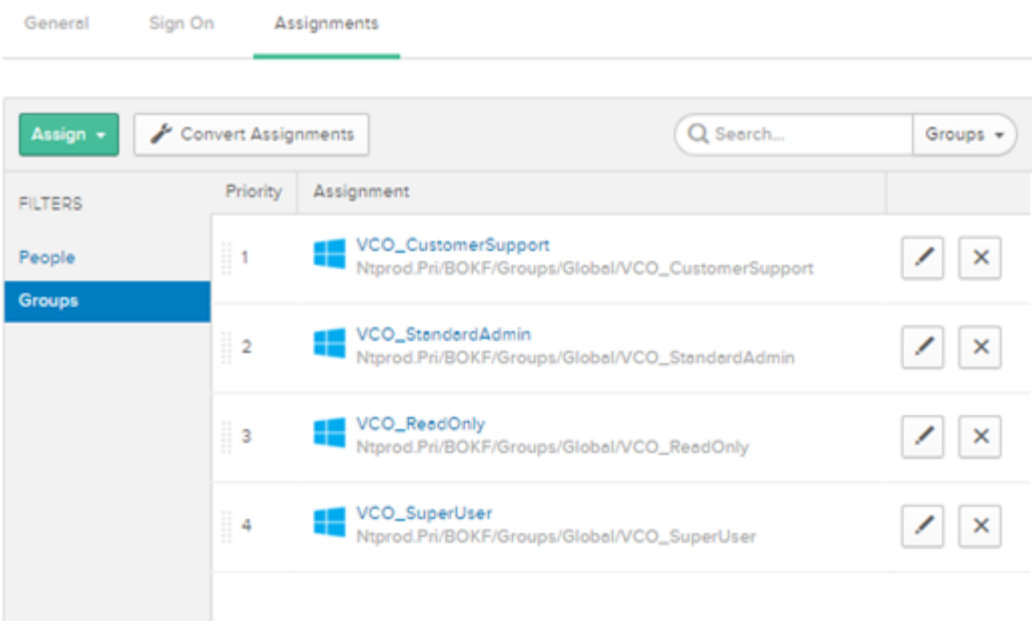
.



i) Click the **Sign On** tab and under the **OpenID Connect ID Token** area, click **Edit**.
j) From the **Groups claim type** drop-down menu, select **Expression**. By default, Groups claim type is set to **Filter**.
k) In the **Groups claim expression** textbox, enter the claim name that will be used in the token, and an Okta input expression statement that evaluates the token.
l) Click **Save**.
The application is setup in IDP. You can assign user groups and users to your application.



3. To assign groups and users to your application:
   a) Go to **Application** > **Applications** and click on your 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) Click **Assign** next to available user groups or users you want to assign the application and click **Done**. The users or user groups assigned to the application will be displayed.



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

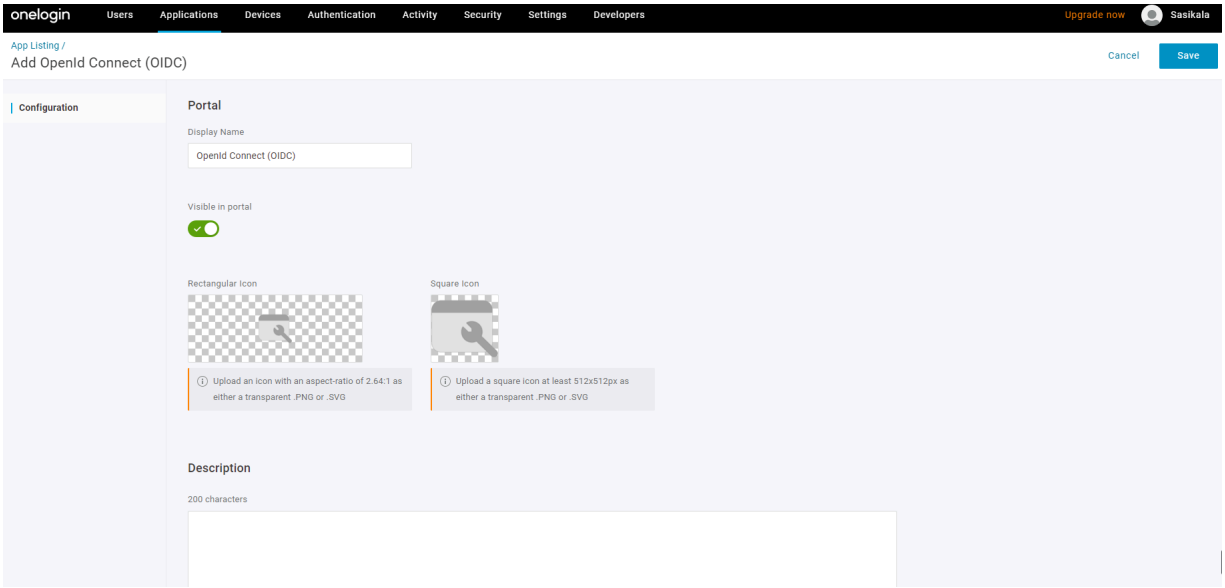
Configure Single Sign On in .

Configure OneLogin for Single Sign On

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

Ensure you have an OneLogin account to sign in.

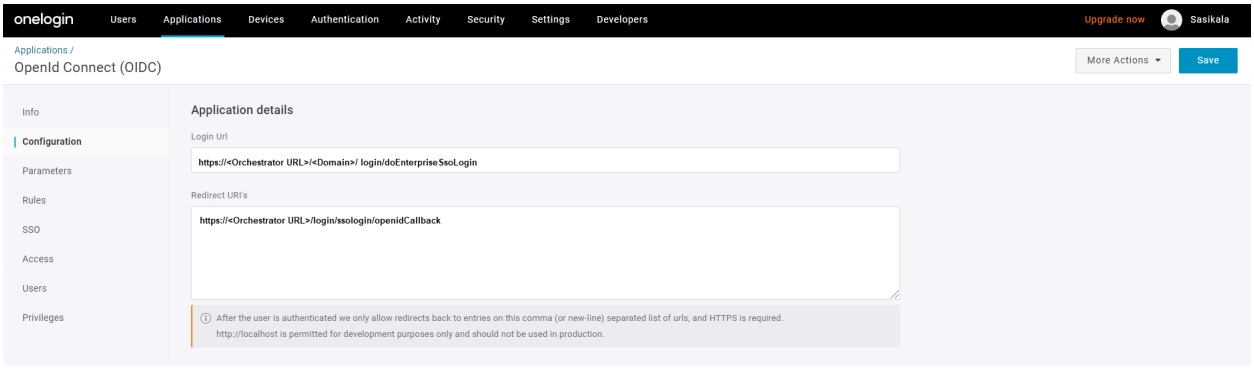
1. Log in to your OneLogin account as an Admin user.
   The **OneLogin** home screen appears.
2. To create a new application:
   a) In the upper navigation bar, click **Apps** > **Add Apps**.
   b) In the **Find Applications** text box, search for “OpenId Connect” or “oidc” and then select the **OpenId Connect (OIDC)** app.
   The **Add OpenId Connect (OIDC)** screen appears.



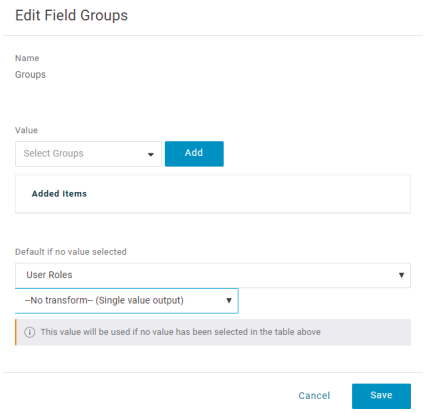
c) In the **Display Name** text box, enter the name for your application and click **Save**.

d) On the **Configuration** tab, enter the Login URL (auto-login URL for SSO) and the Redirect URI that uses as the callback endpoint, and click **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. You can get the Domain name from the Enterprise portal > **Administration** > **System Settings** > **General Information** page.
- **Redirect URI's** - The redirect URL will be in this format: https://<Orchestrator URL>/login/ssologin/ openidCallback. In the application, at the bottom of the **Authentication** screen, you can find the redirect URL link.



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



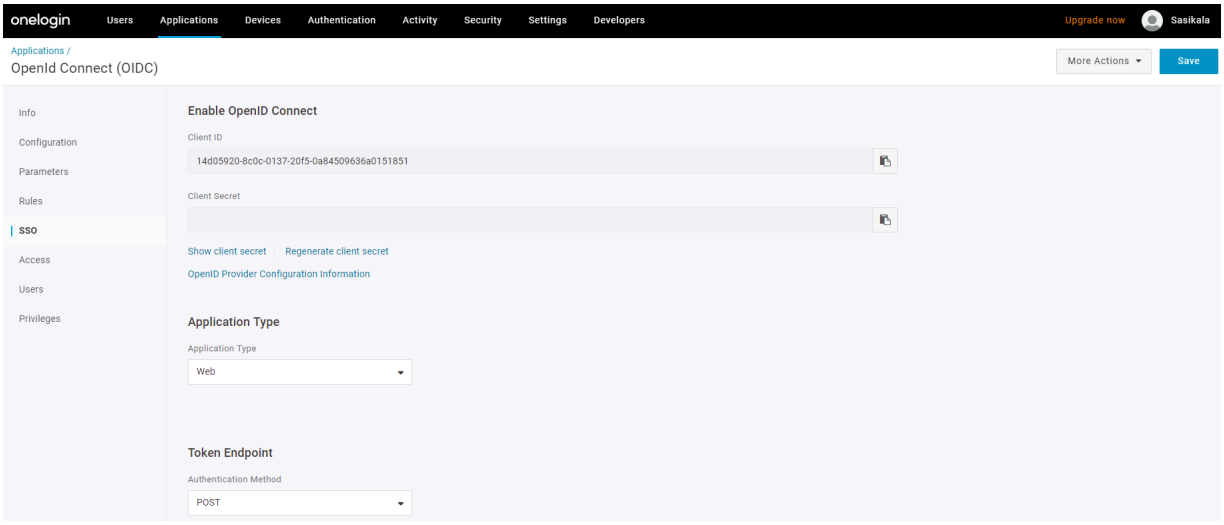
f) Configure User Roles with value "--No transform--(Single value output)" to be sent in groups attribute and click **Save**.

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

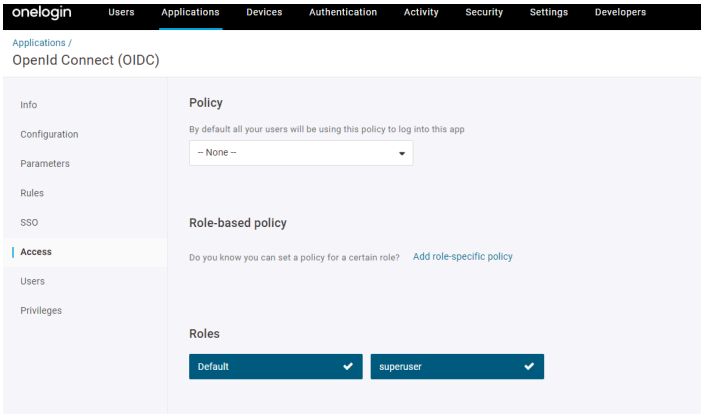
h) From the **Authentication Method** drop-down menu, select **POST** as the Token Endpoint and click **Save**.

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

.



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



3. To add roles and users to your application:
   a) Click **Users** > **Users** and select a user.
   b) On the **Application** tab, from the **Roles** drop-down menu, on the left, select a role to be mapped to the user.
   c) Click **Save Users**.

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

Configure Single Sign On in.

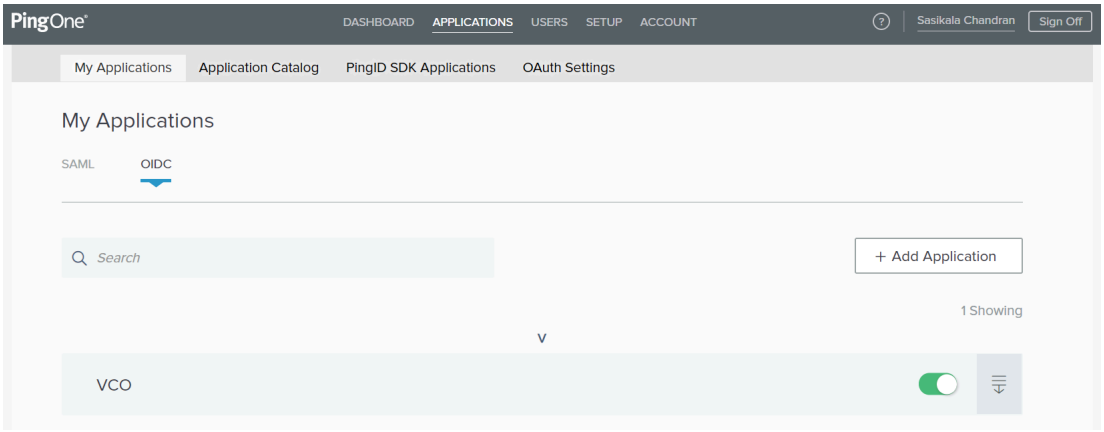
Configure PingIdentity for Single Sign On

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

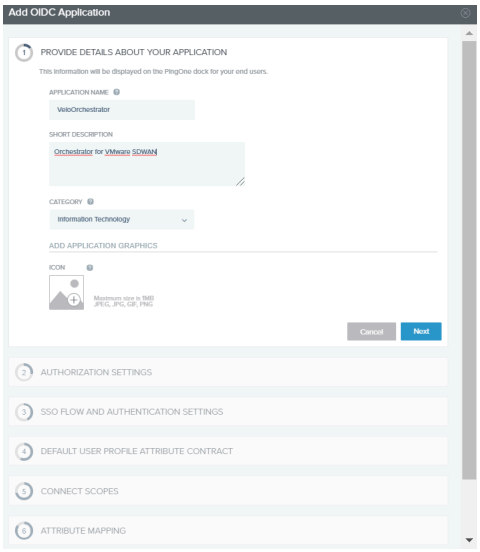
Ensure you have a PingOne account to sign in.

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

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



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



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

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

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

.

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

In the

application, at the bottom of the

Configure Authentication

screen, you can find the redirect URL link. Ideally, the

redirect URL will be in this format: https://<Orchestrator URL>/login/ssologin/openidCallback. The Start SSO URL will be in this format: https://<Orchestrator URL>/<domain name>/login/doEnterpriseSsoLogin.

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

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

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

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

i) Under **Attribute Mapping**, map your identity repository attributes to the claims available to your 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 application and click **Done**. The application will be added to your account and will be available in the **My Application** screen.

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

Configure Single Sign On in .

Configure Arista CSP for Single Sign On

To configure Arista Cloud Services Platform (CSP) for Single Sign On (SSO), perform the steps on this procedure.

Sign in to Arista CSP console (staging or production environment) with your Arista account ID. If you are new to Arista Cloud and do not have a Arista account, you can create one as you sign up. For more information, see How do I Sign up for Arista CSP section in Using Arista Cloud documentation.

1. Contact the Support Provider for receiving a Service invitation URL link to register your application to Arista CSP. For information on how to contact the Support Provider, see www.arista.com/en/support/product-documentation.
   The Support Provider will create and share:
   - a Service invitation URL that needs to be redeemed to your Customer organization
   - a Service definition uuid and Service role name to be used for Role mapping in Orchestrator
2. Redeem the Service invitation URL to your existing Customer Organization or create a new Customer Organization by following the steps in the UI screen.
   You need to be an Organization Owner to redeem the Service invitation URL to your existing Customer Organization.
3. After redeeming the Service invitation, when you sign in to Arista CSP console, you can view your application tile under **My Services** area in the **Arista Cloud Services** page.
   The Organization you are logged into is displayed under your username on the menu bar. Make a note of the Organization ID by clicking on your username, to be used during Orchestrator configuration. A shortened version of the ID is displayed under the Organization name. Click the ID to display the full Organization ID.
4. Log in to Arista CSP console and create an OAuth application. For steps, see *Use OAuth 2.0 for Web Apps* . Make sure to set Redirect URI to the URL displayed in **Configure Authentication** screen in Orchestrator. Once OAuth application is created in Arista CSP console, make a note of IDP integration details such as Client ID and Client Secret. These details will be needed for SSO configuration in Orchestrator.
5. Log in to your application as Super Admin user and configure SSO using the IDP integration details as follows.
   a) Click **Administration** > **System Settings**
   The **System Settings** screen appears.
   b) Click the **General Information** tab and in the **Domain** text box, enter the domain name for your enterprise, if it is not already set.

   Note: To enable SSO authentication for the, you must set up the domain name for your enterprise.

   c) Click the **Authentication** tab and from the **Authentication Mode** drop-down menu, select **SSO**.
   d) From the **Identity Provider template** drop-down menu, select **VMwareCSP**.
   e) In the **Organization Id** text box, enter the Organization ID (that you have noted down in Step 3) in the following format: */csp/gateway/am/api/orgs/<full organization ID>*.

f) In the **OIDC well-known config URL** text box, enter the OpenID Connect (OIDC) configuration URL (https://console.cloud.vmware.com/csp/gateway/am/api/.well-known/openid-configuration) for your IDP. The application auto-populates endpoint details such as Issuer, Authorization Endpoint, Token Endpoint, and User Information Endpoint for your IDP.

g) In the **Client Id** text box, enter the client ID that you have noted down from the OAuth application creation step.

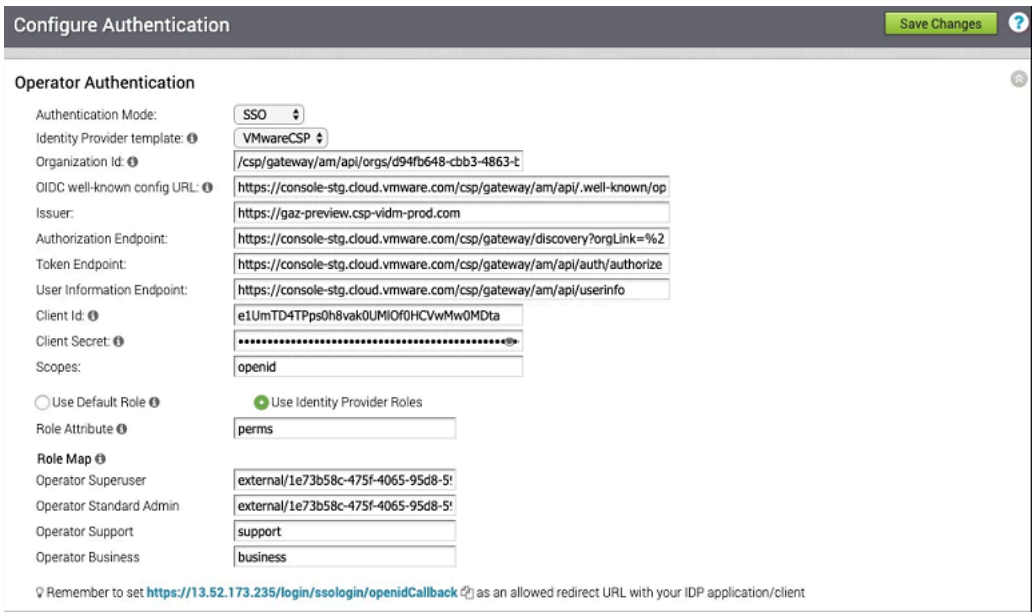
h) In the **Client Secret** text box, enter the client secret code that you have noted down from the OAuth application creation step.

i) To determine user's role in, select either **Use Default Role** or **Use Identity Provider Roles**.

j) On selecting the **Use Identity Provider Roles** option, in the **Role Attribute** text box, enter the name of the attribute set in the Arista CSP to return roles.

k) In the **Role Map** area, map the VMwareCSP-provided roles to each of the roles, separated by using commas. Roles in Arista CSP will follow this format: external/<service definition uuid>/<service role name mentioned during service template creation>. Use the same Service definition uuid and Service role name that you have received from your Support Provider.

6. Click **Save Changes** to save the SSO configuration.
7. Click **Test Configuration** to validate the entered OpenID Connect (OIDC) configuration.



The user is navigated to the Arista CSP website and allowed to enter the credentials. On IDP verification and successful redirect to

test call back, a successful validation message will be displayed.

You have completed integrating application in Arista CSP for SSO and can access the application logging in to the Arista CSP console.

- Within the organization, manage users by adding new users and assigning appropriate role for the users. For more information, see the *Identity & Access Management* section in Using Arista Cloud documentation.

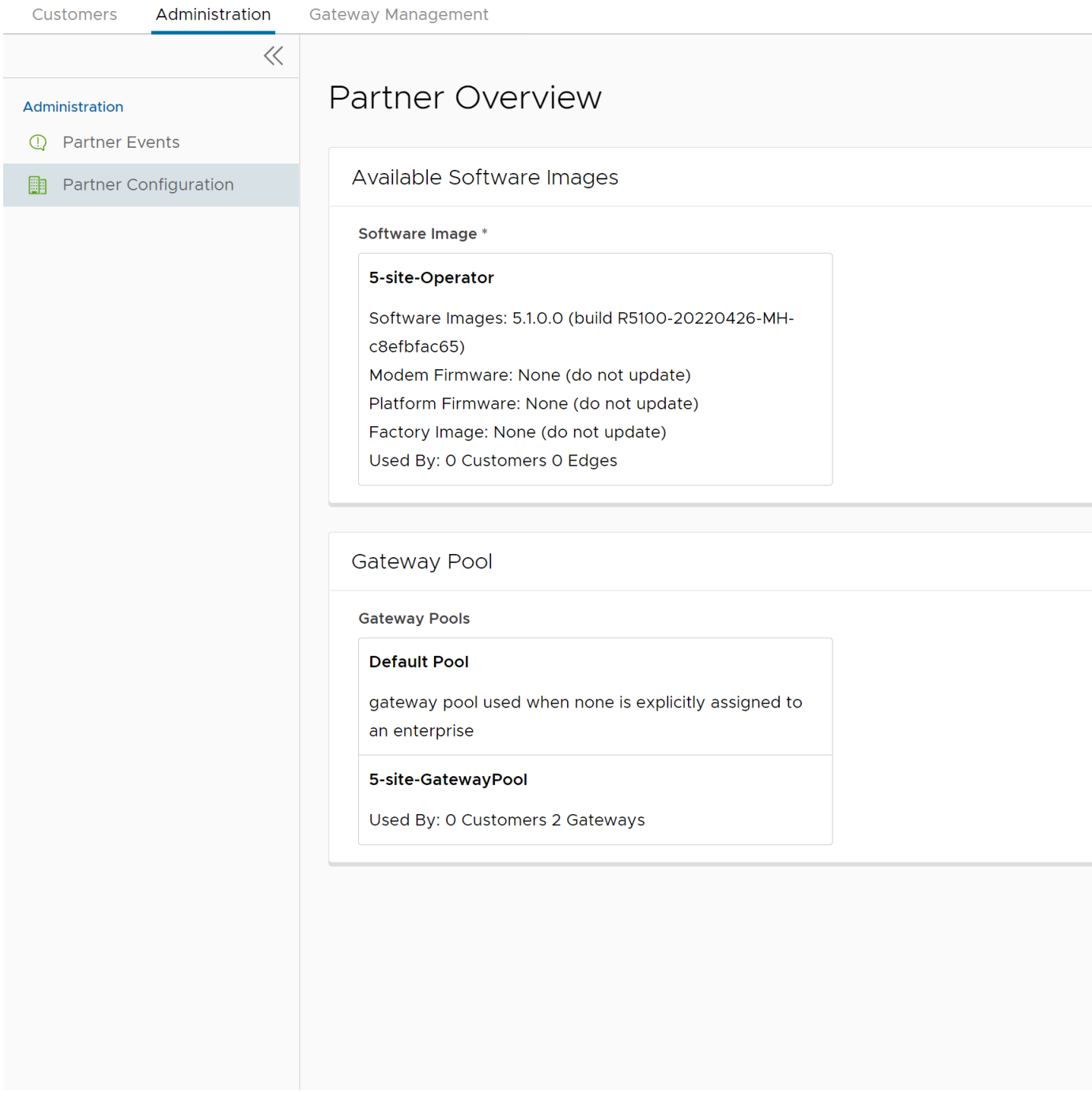
View Partner Information

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 as a Partner user.
2. In the Partner portal, click the **Administration** tab, and then from the left menu, click **Partner Configuration**.

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



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.

Option	Description
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.

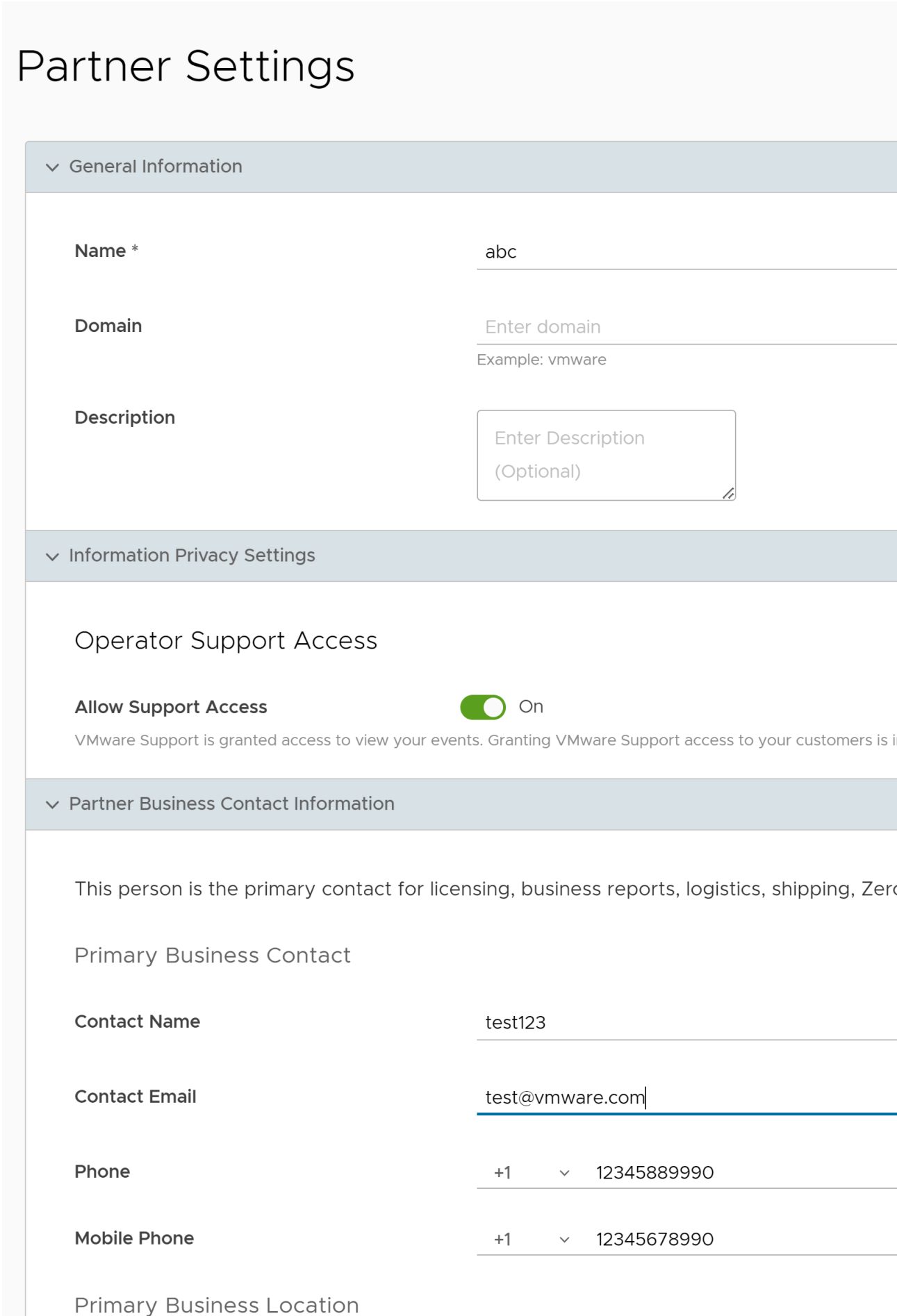
To assign the software images and Gateway pools to a customer, see Create New Partner Customer and Configure Partner Customers.

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 support access.

1. Log in to the as a Partner.

2. Click **Administration** from the top menu, and then from the left menu, click **Partner Settings**. The following screen



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

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. Click **Save Changes**.

Orchestrator Branding - Partner

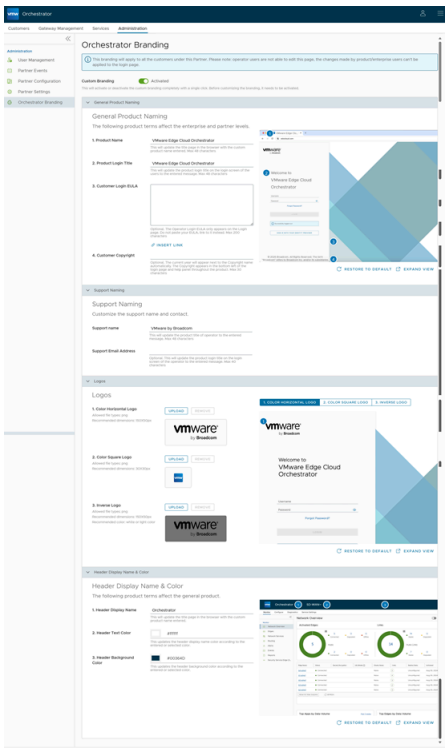
This section provides guidelines to customize the Orchestrator user interface (UI) to your company's brand. As a Partner user, you can brand the Orchestrator UI by applying your company's name, logo, and colors at a Partner level.

To enable Partner users to customize the orchestrator UI branding, the "Operator only Branding" feature must be deactivated. If this feature is turned on in your orchestrator, contact your Operator to deactivate the "Operator only Branding" feature.

Note: Deactivating the "Operator only Branding" feature will override any existing Operator branding settings.

As a Partner user, to customize the branding at Partner level, perform the following steps:

1. In the Partner portal, click **Administration** from the top menu.
2. From the left menu, click **Orchestrator Branding**. The **Orchestrator Branding** page appears.



3. To customize branding, activate the "Custom Branding" feature by turning on the **Custom Branding** toggle button.
4. You can customize the following branding aspects of the Orchestrator UI:
   a. General Product Naming
   b. Support Naming
   c. Logos
   d. Header Display Name and Color
5. As you customize the branding aspects, the changes gets applied to the Preview image on the right.

   Click **Expand View** to expand the preview image. Click **Restore to Default** to restore the branding settings to default.
6. Once you are done with branding customization, click **Save Changes** and refresh the Orchestrator to view the custom branding applied to the Partner, and customers under the Partner.

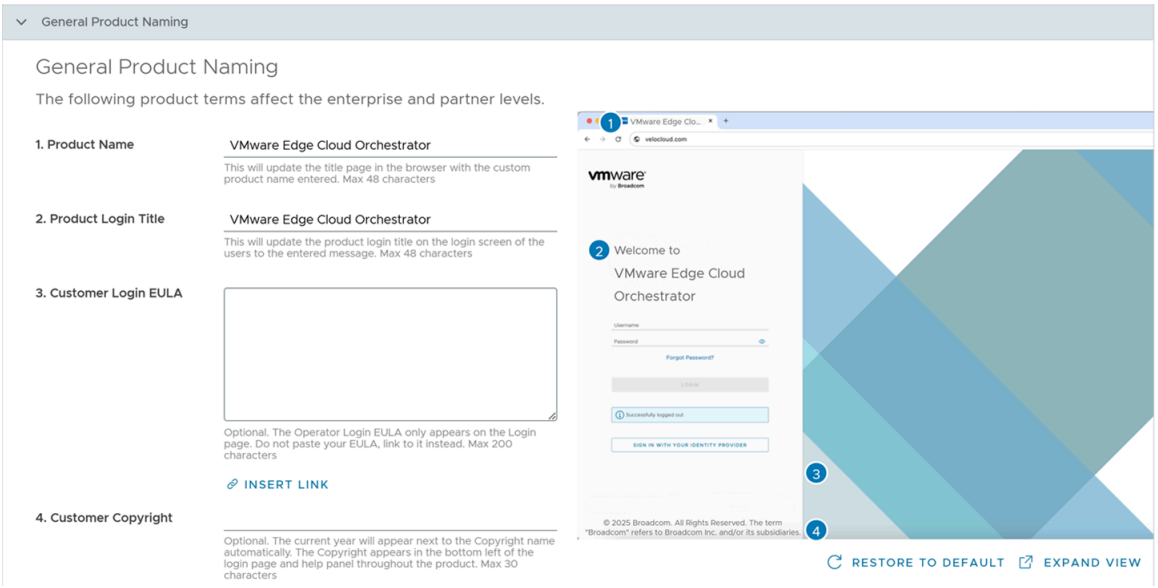
   Note: The branding changes made by Partner users will not be applied to the login page.
7. To deactivate the "Custom Branding" feature, turn off the **Custom Branding** toggle button. All the branding settings will restored back to default.

General Product Naming Branding

You can customize the following textual elements located on the Partner Login screen.

Element	Description
Product Name	Enter your product name. This updates the title page in the browser with the custom product name entered. The product name can be a maximum of 48 characters.
Product Login Title	Enter your product login title. This updates the product login title on the login screen of the users to the entered text. The product login title can be a maximum of 48 characters.

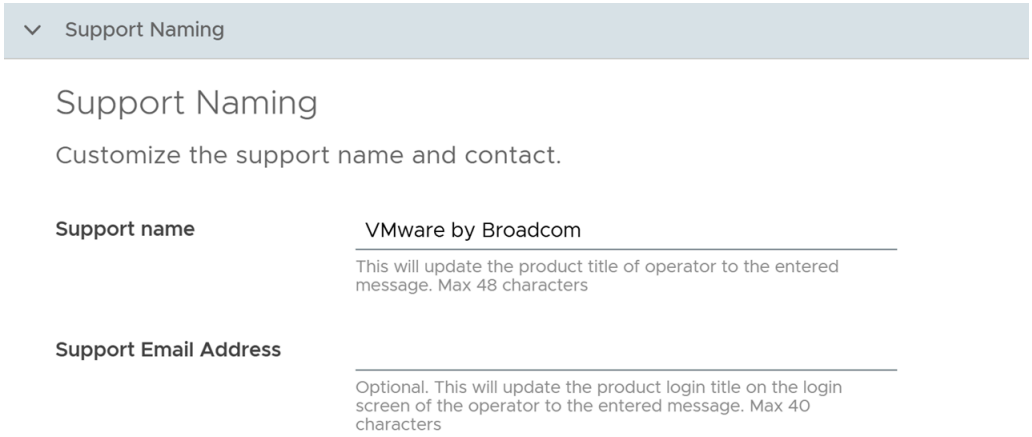
Element	Description
Customer Login EULA	This is optional. Add your Customer login EULA with a maximum of 200 characters. The Customer login EULA only appears on the login screen. You can either enter your EULA in the box and then add link by selecting the EULA, or directly add link to EULA login by clicking **Insert Link**.
Customer Copyright	This is optional. Enter your Customer copyright name and text. The current year will appear next to the copyright name automatically. The copyright appears in the bottom left of the Customer login page and help panel throughout the product. The Customer copyright text can be a maximum of 30 characters. If you have not entered any customized copyright text, the default copyright will be displayed.



Support Naming Branding

You can customize the Support name and contact details.

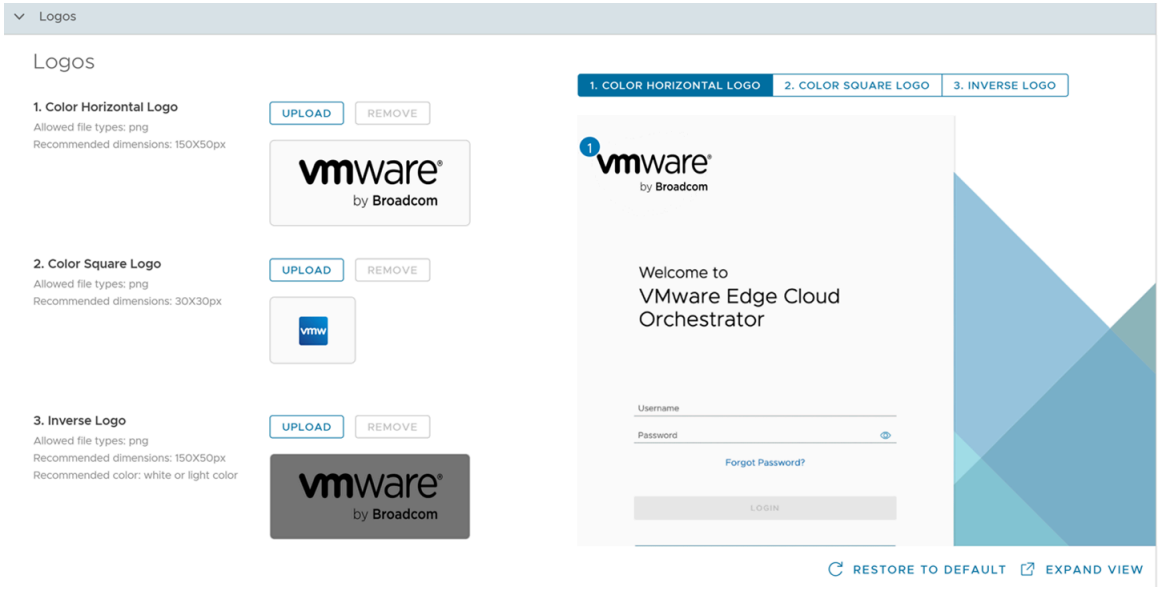
Element	Description
Support Name	Enter your custom support name. This updates the product title of Operator to the entered text. The support name can be a maximum of 48 characters.
Support Email Address	This is optional. Enter your custom support email address. This updates the product login title on the login screen of the Operator to the entered text. The support email address can be a maximum of 40 characters.



Logos Branding

Your logo will be displayed on the top, left corner of the Login page of the Orchestrator UI. You can customize the following logo elements.

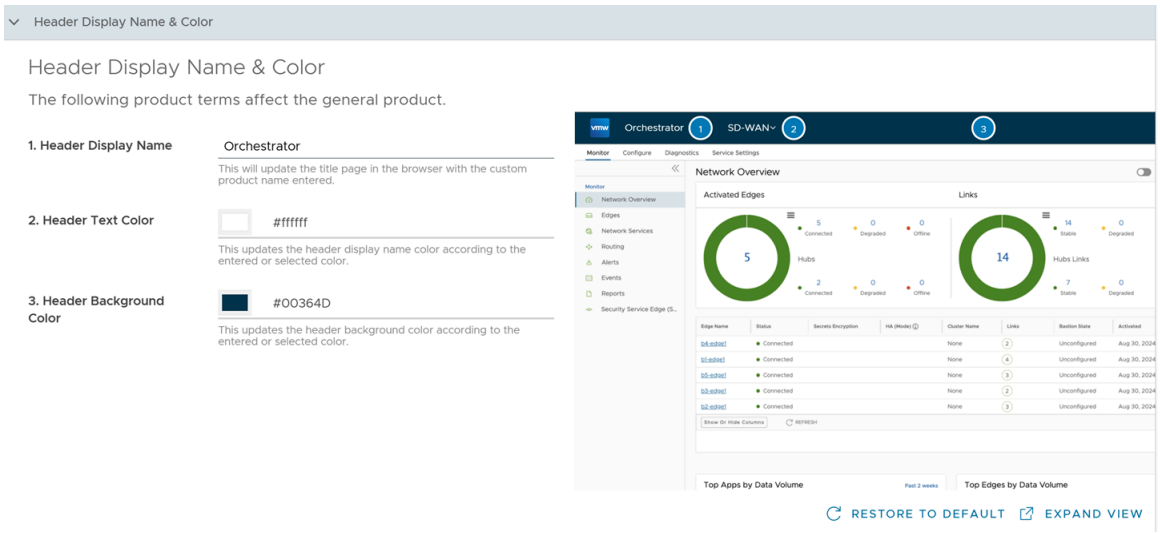
Element	Description
Color Horizontal Logo	Select and upload your custom horizontal logo by clicking **Upload**. Adhere to the following Logo requirements: • Allowed file types: png • Recommended dimensions: 150X50px
Color Square Logo	Select and upload your custom square logo by clicking **Upload**. Adhere to the following Logo requirements: • Allowed file types: png • Recommended dimensions: 30X30px
Inverse Logo	Select and upload your custom inverse logo by clicking **Upload**. Adhere to the following Logo requirements: • Allowed file types: png • Recommended dimensions: 150X50px • Recommended color: white or light color



Header Display Name and Color Branding

You can customize the following textual and visual elements located on the Orchestrator UI header.

Element	Description
Header Display Name	Enter your header display name. This updates the title page in the browser with the custom product name entered.
Header Text Color	Enter or select the header text color. This updates the header display name color according to the entered or selected color.
Header Background Color	Enter or select the header background color. This updates the header background color according to the entered or selected color.



Edge Licensing

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.

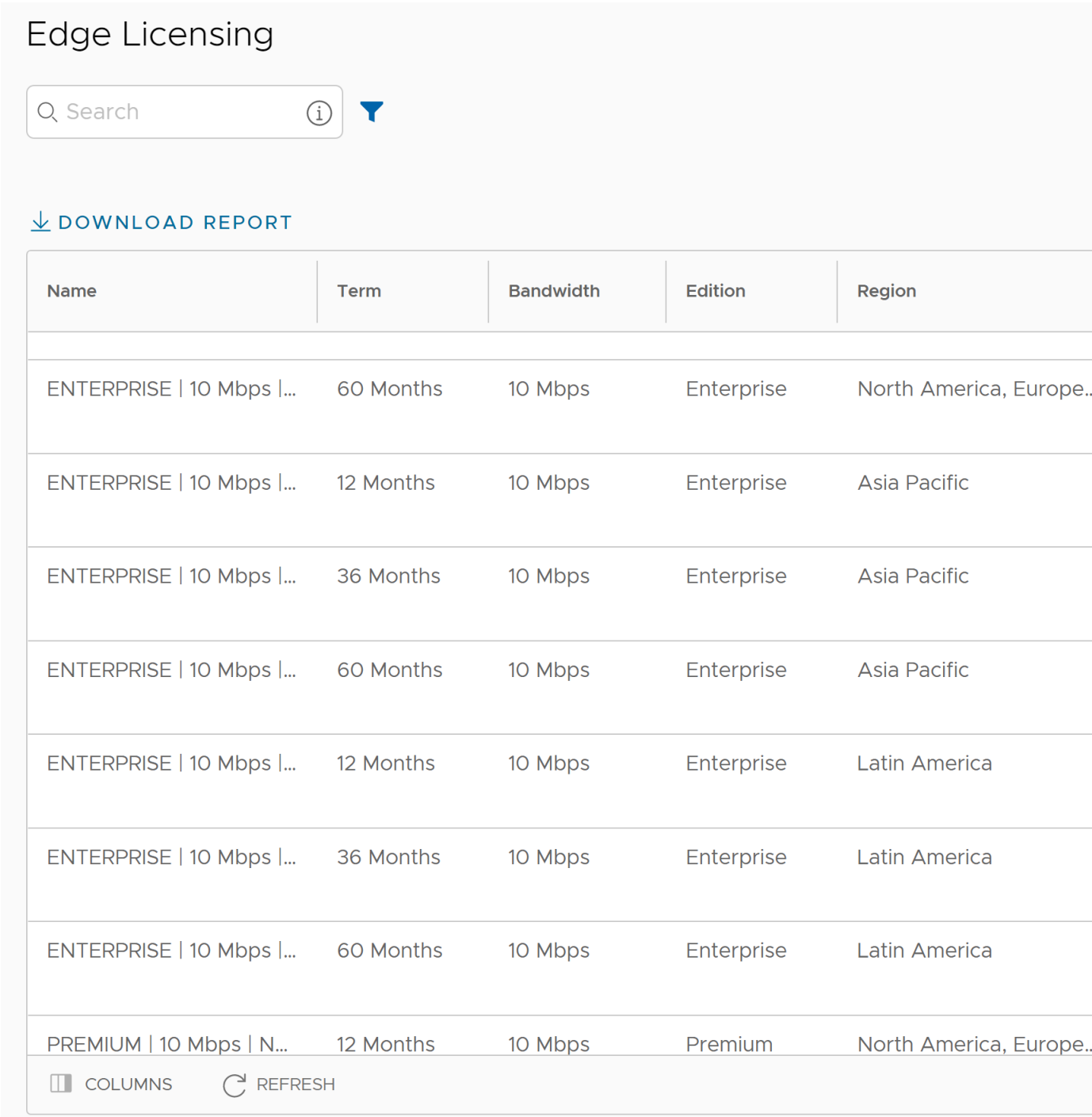
Apart from the above list, offers a trial version of license with the following attributes:

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 as a Partner. In the Partner portal, from the top menu, click **Edge Management**, and then from the left menu, click **Edge Licensing**.



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

Option	Description
Search	Enter a term to search for a matching text across the table. You can click the advanced search option to use filters to narrow down the search results.
Download Report	Click this option to download a report of the licenses, associated customers, and Edges in a CSV format.

Option	Description
Columns	Click this option and select the columns to be displayed in the table.
Refresh	Click this option to refresh the displayed list of licenses.

3. Clicking the **View** link under the **Partners assigned** column, displays the Edge license details of the selected Partner.
4. Clicking the **View** link under the **Customers assigned** column, displays the Edge license details of the selected Customer.

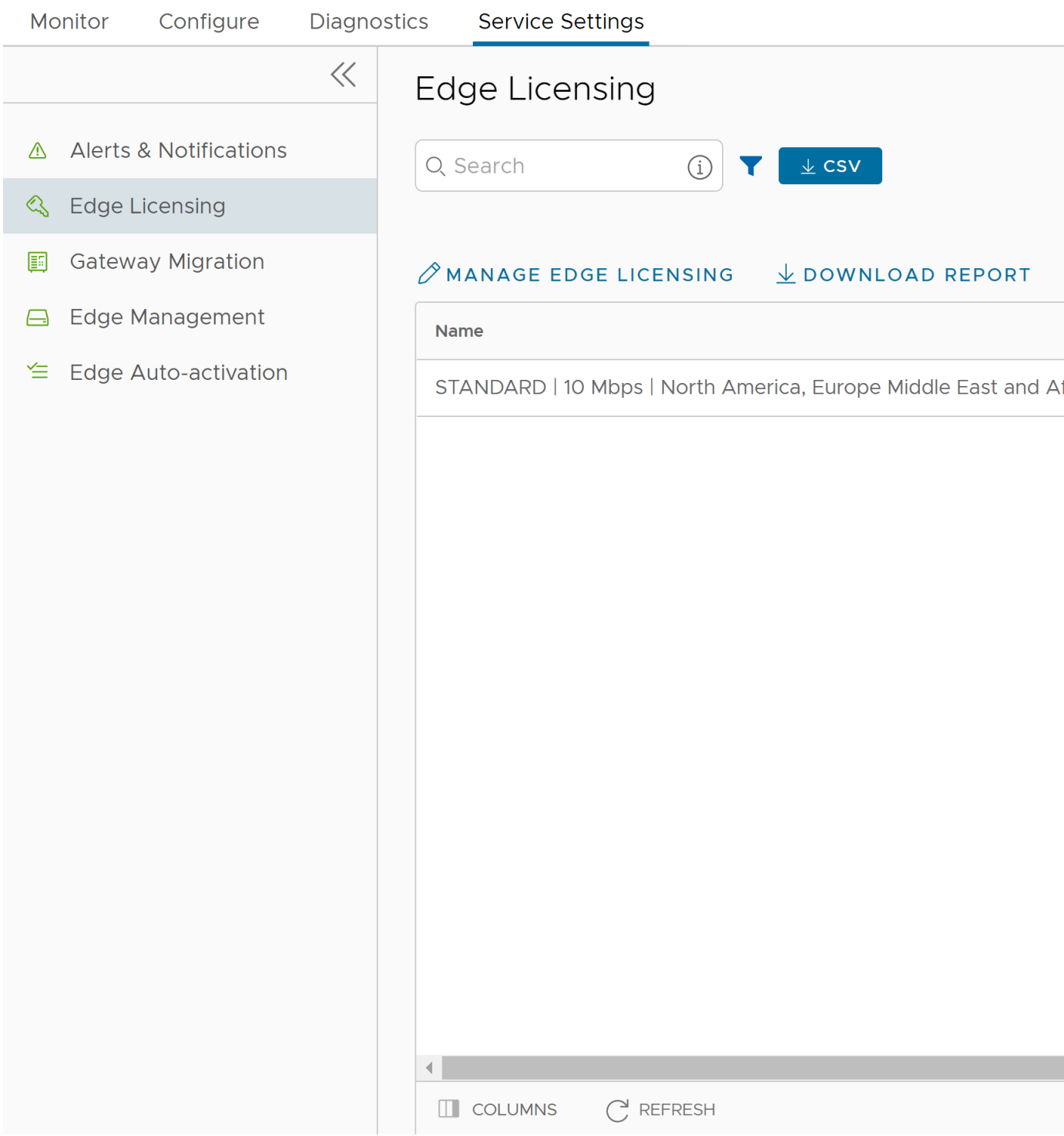
To manage Edge licensing for Customers, see Manage Edge Licenses for Customers.

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

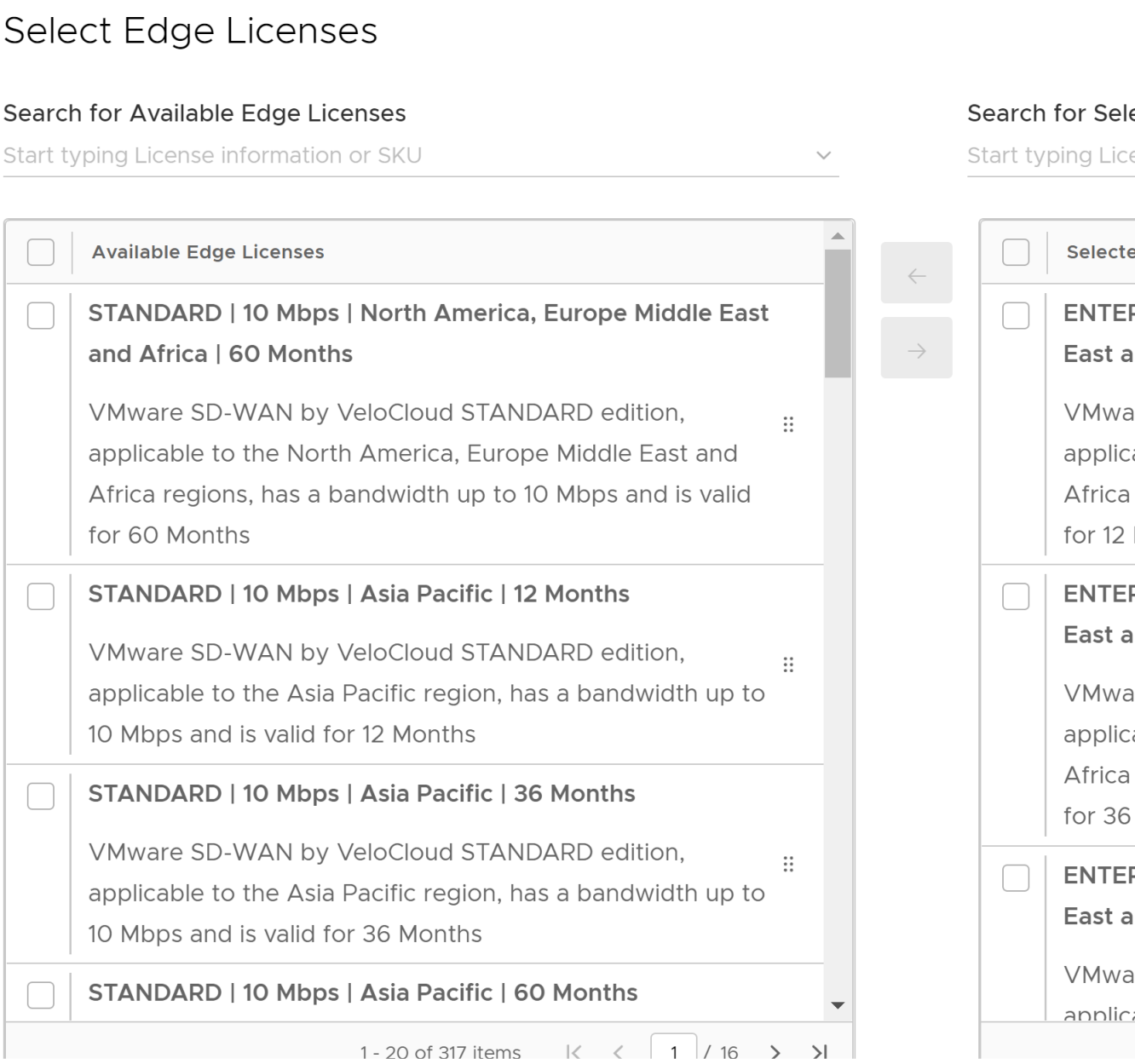
Manage Edge Licenses for Customers

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

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



4. Click **Manage 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, offers a trial version of license with the Edition as **POC**. If you select a **POC** license, you cannot choose the other licenses.

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

   Note:

   If you have selected the **POC** license, you can click **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. Click **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, click **Configure** > **Edges**.
- To assign license to each Edge, click 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 click **Assign Edge License** to assign the license.
- To assign a license to multiple Edges, select the appropriate Edges, click **Assign Edge License**, and select the license.

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 as a Partner.
2. In the Partner portal, from the top menu, click **Service Settings**, and then from the left menu, click **Edge Management**.
3. You can configure the following options and click **Save Changes**.

Edge Management

General Edge Settings

Edge Link Down Limit ⓘ

Customize (default 1 d

Number of days

Edge Authentication

Default Certificate

Certificate Acquire

Edge Authentication ⓘ

ACTIVATE SECURE E

Device Secret Encryption

Enable Encrypt Device Secrets ⓘ

ENABLE FOR ALL ED

Configuration Updates

Enable Edge Configuration Updates

On

When this option is set to on, configuration updates are actively pushed to Edges. When this option is turned off, pending configuration updates are disabled by default during Orchestrator upgrades.

Enable Configuration Updates Post-Upgrade

Off

This option allows the customer to control when post-Orchestrator upgrade configuration changes are applied to their Ed configuration updates automatically, and after the upgrade the Operator resumes these Edge configuration updates. Whe Edge configuration updates after the Orchestrator is upgraded, and these Edge configuration updates would only resume

Software & Firmware Images

Is Default?	Operator Profile	Software & Firmware Images
●	3-site-Operator	5.2.0.0 (build R5200-2023032

3-site-Operator

Description:

Software Image: **5.2.0.0 (build R5200-20230323-MH-fe0c25d5bf)**

Platform Firmware: **None (do not update)**

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 , 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 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 more information, contact your Operator. **Note:** On clicking **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	Click 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	

Option	Description
Enable Encrypt Device Secrets	Click 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 more information, see the topic *Provision a New Edge* in the *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.

Software & Firmware Images

You can view the details of the listed images and select the default image.

Note: To view this section:

- An Operator must navigate to the **Global Settings** service of the Enterprise portal, and then click **Customer Configuration** > **SD-WAN Configuration**. Select the **Allow Customer to manage software** check box. Only an Operator can add, delete, or edit an image. For more information, see the topic *Platform Firmware and Factory Images*, in the *Operator Guide*.
- A Partner user must navigate to **Manage Partner Customers**. Click **More** and perform the following:
  - Select **Update Edge Image Management**. Turn on the toggle button, and then click **Save**.
  - Select **Assign Software/Firmware Image**, and then select a Software/Firmware image from the drop-down menu. Click **Save**.

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 . 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.

Note: 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 Super User role to modify the access level for a user. See the following topics:
   - Create New Partner Admin
   - Configure Partner Admin Users
2. Generate a new pair of SSH keys or import an existing SSH key. See Add SSH Key.
3. Enable key-based authentication to access Edges. See Enable Secure Edge Access for an Enterprise.

Add SSH Key

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

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

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

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

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

To add a SSH key:

1. In the Enterprise portal, click the User icon that appears at the top-right side of the Window. The **User Information** panel appears.
2. Click **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. Click **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.

Revoke SSH Keys

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

To revoke your SSH key:

1. Login to the Orchestrator, and then click the **Open New Orchestrator UI** option available at the top of the Window.
2. Click **Launch New Orchestrator UI** in the pop-up window. The UI opens in a new tab.
3. In the new Orchestrator UI, click the User icon that appears at the top-right side of the Window. The User Information panel appears.
4. Click **Revoke SSH Key**.

To revoke the SSH keys of other Partner users:

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

The SSH keys for a user are automatically deleted when:

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

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

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. Click **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.

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.

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

Commands	Description	Access Level = Basic	Access Level = Privileged
`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
`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			

Commands	Description	Access Level = Basic	Access Level = Privileged
`shell`	Takes you into the Linux shell. Type `exit` to return to the secure Edge CLI.	No	Yes

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:      Arista
Serial:     Arista-420efa0d2a6ccb35-9b9bee2f04f74b32
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_velocloud_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": {
      "autonegotiation": 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"
}
```

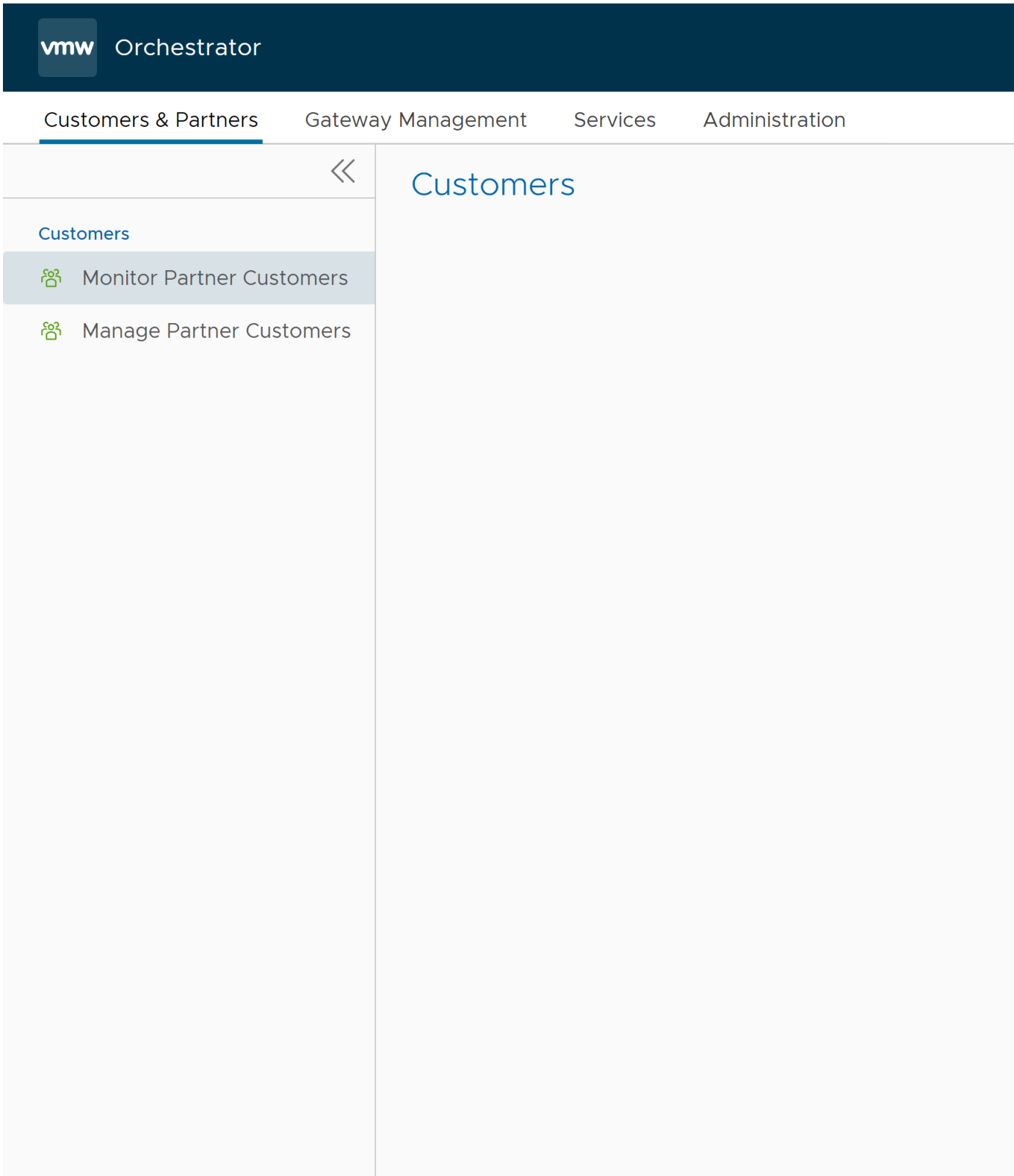

Configure User Account details

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.

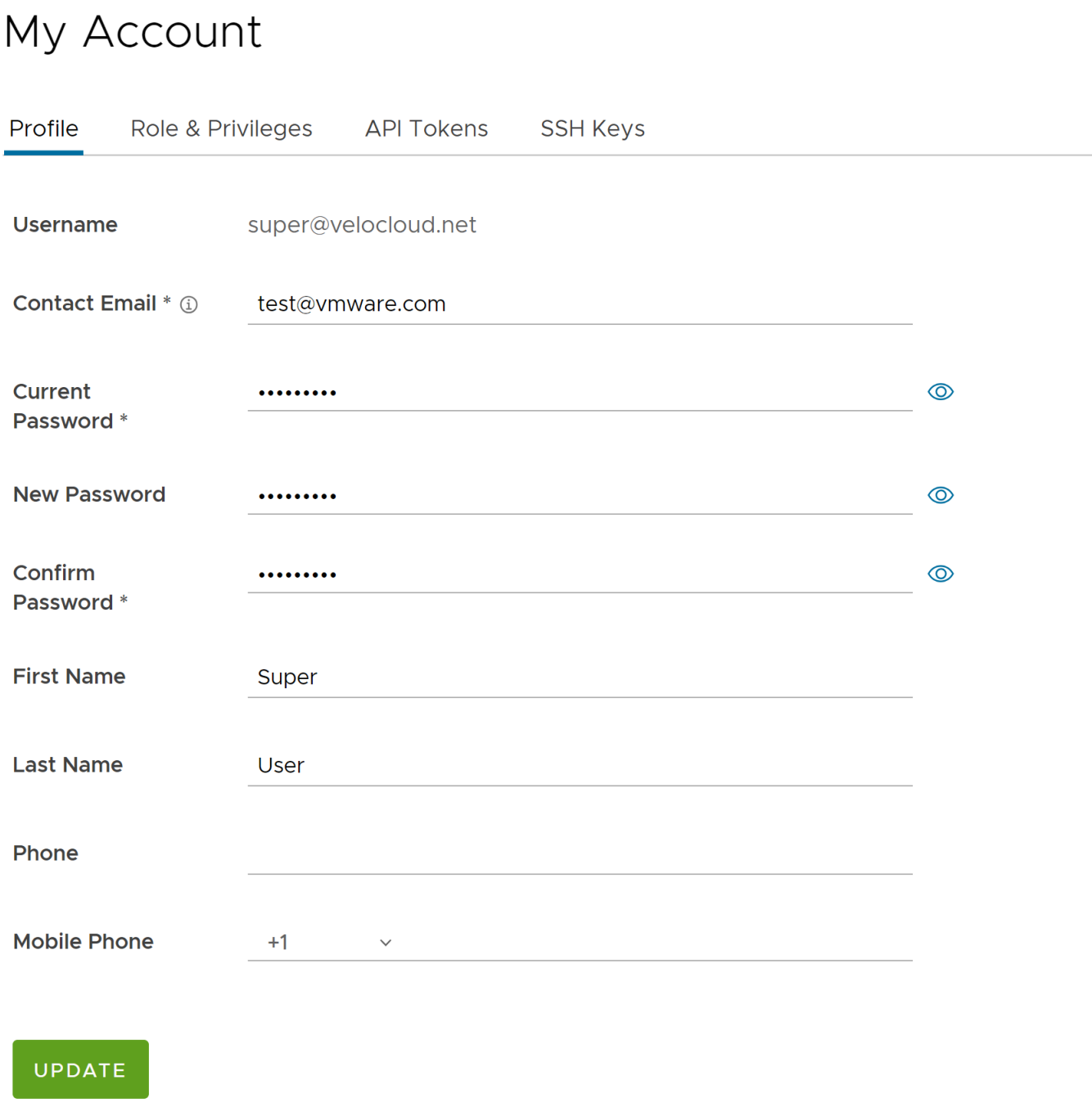
Ensure to configure privileges for a user to access Edges in a secure manner. You must choose **Basic** access level for the user. You can configure the access level when you create a new user (under User Management), and choose to modify it at a later point in time. Ensure that you have Superuser role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

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

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



3. Click the **My Account** button. The following screen appears:

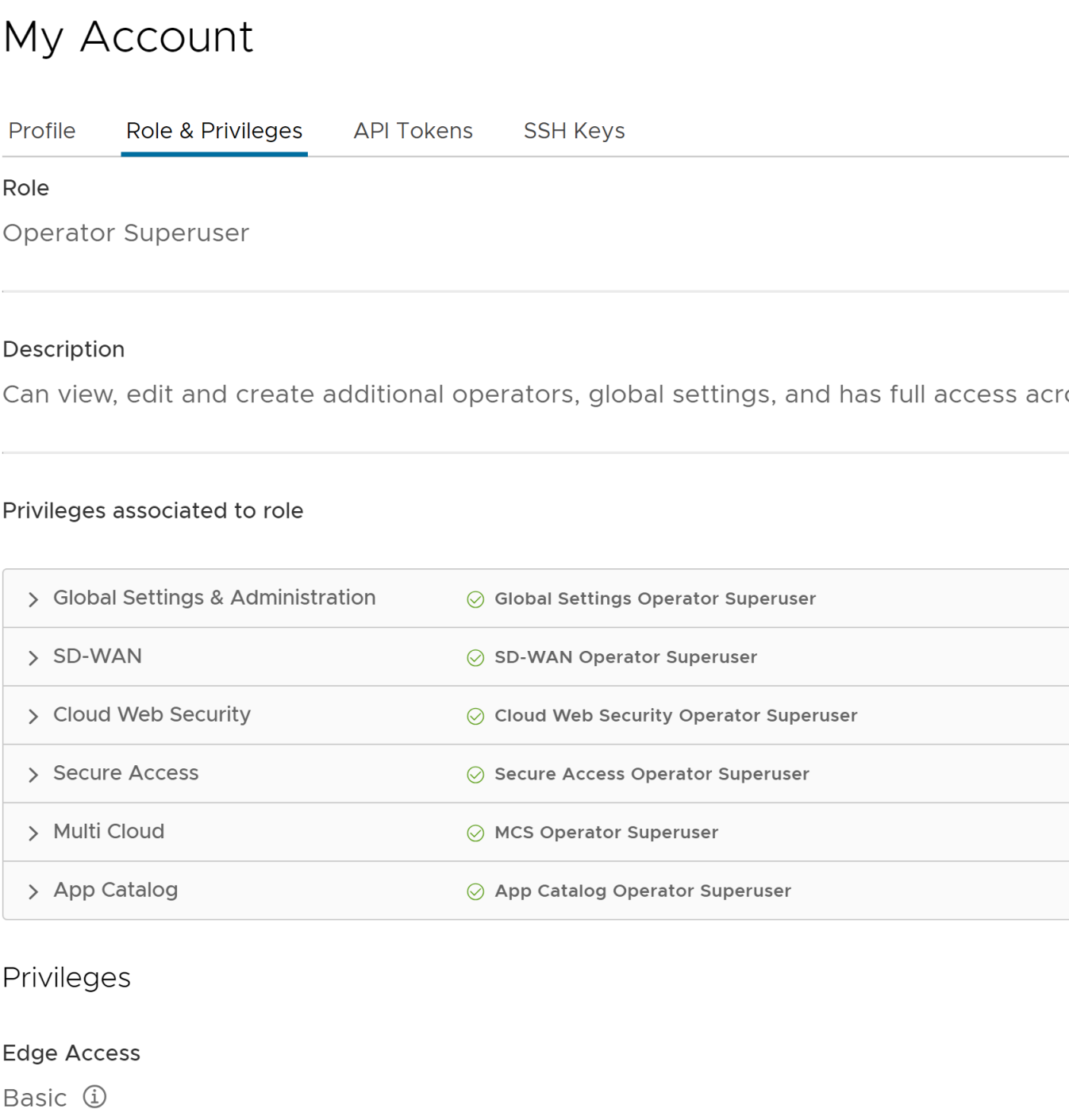


4. The **Profile** tab is displayed by default. You can update the following basic user details:

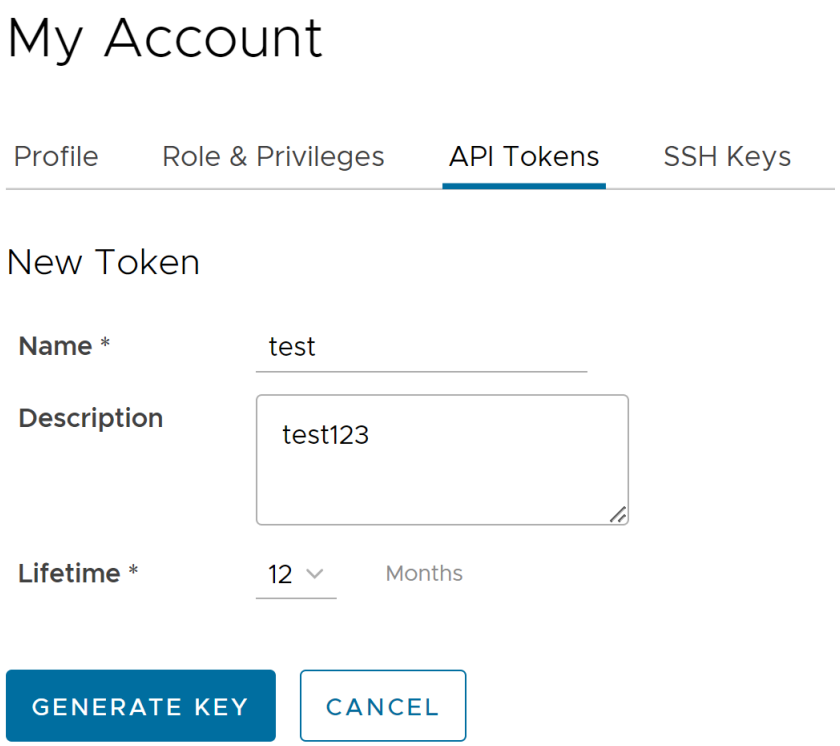
Option	Description
Username	Displays the username and it is a read-only field.
Contact Email	Enter the primary contact email address of the user.
Current Password	Enter the current password.

Option	Description
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.

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



6. Click the **API Tokens** tab. The following screen is displayed.



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

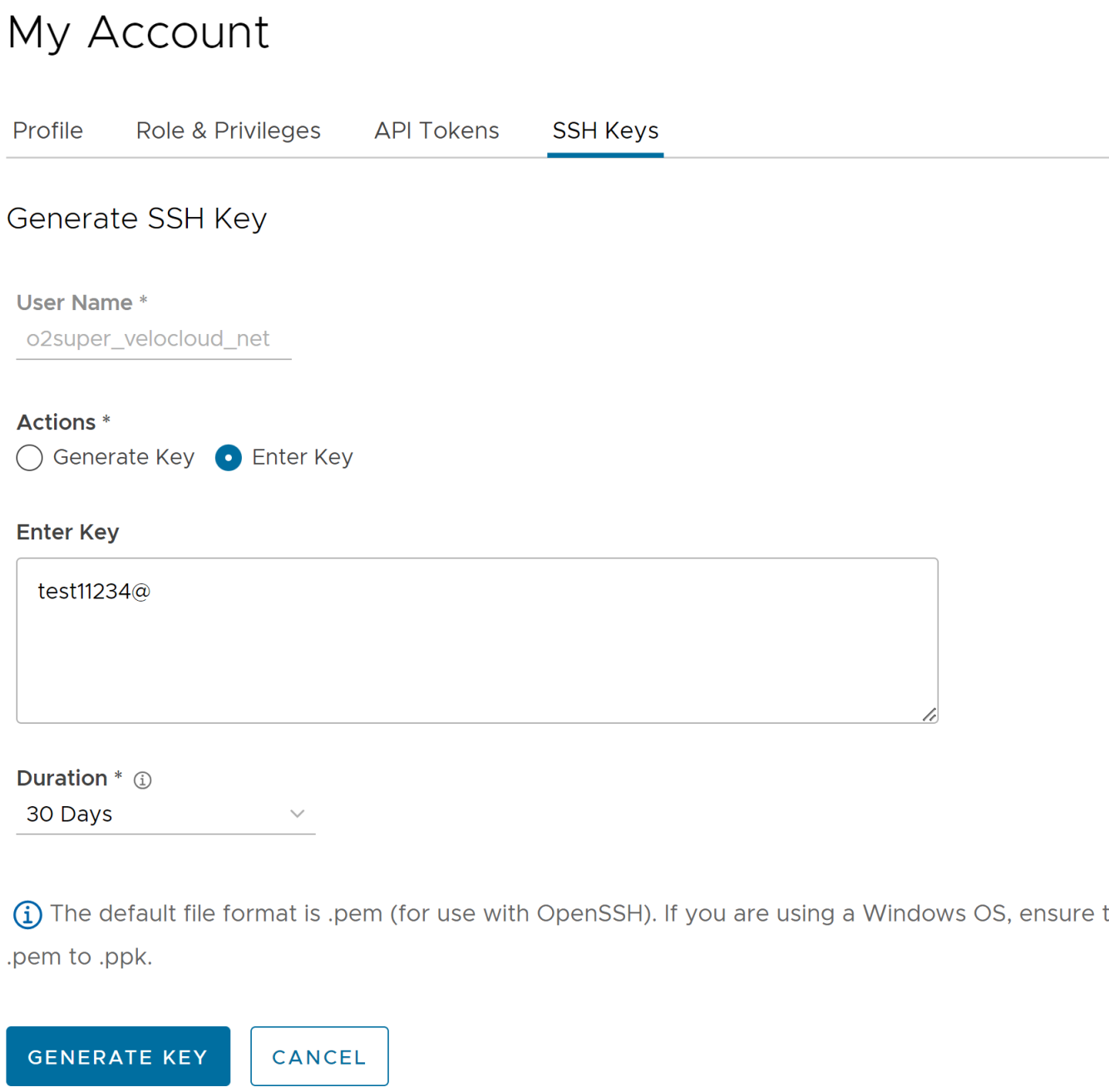
   Based on their roles, users can perform the following actions:

   - 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.

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



Option	Description
User Name	Displays the username and it is a read-only field.

Option	Description
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 **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. Click **Generate Key**.

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

11. To deactivate an SSH token, click the **Revoke** button. A pop-up window appears, to confirm the revoke operation. Select the check box, and then click **Revoke** to permanently revoke the key.

    The SSH keys for a user are automatically deleted when:

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

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

    What to do next:

    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.

Manage Gateway Pools and Gateways

network consists of multiple service Gateways deployed at top tier network and cloud data centers. The 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.

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 . 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.

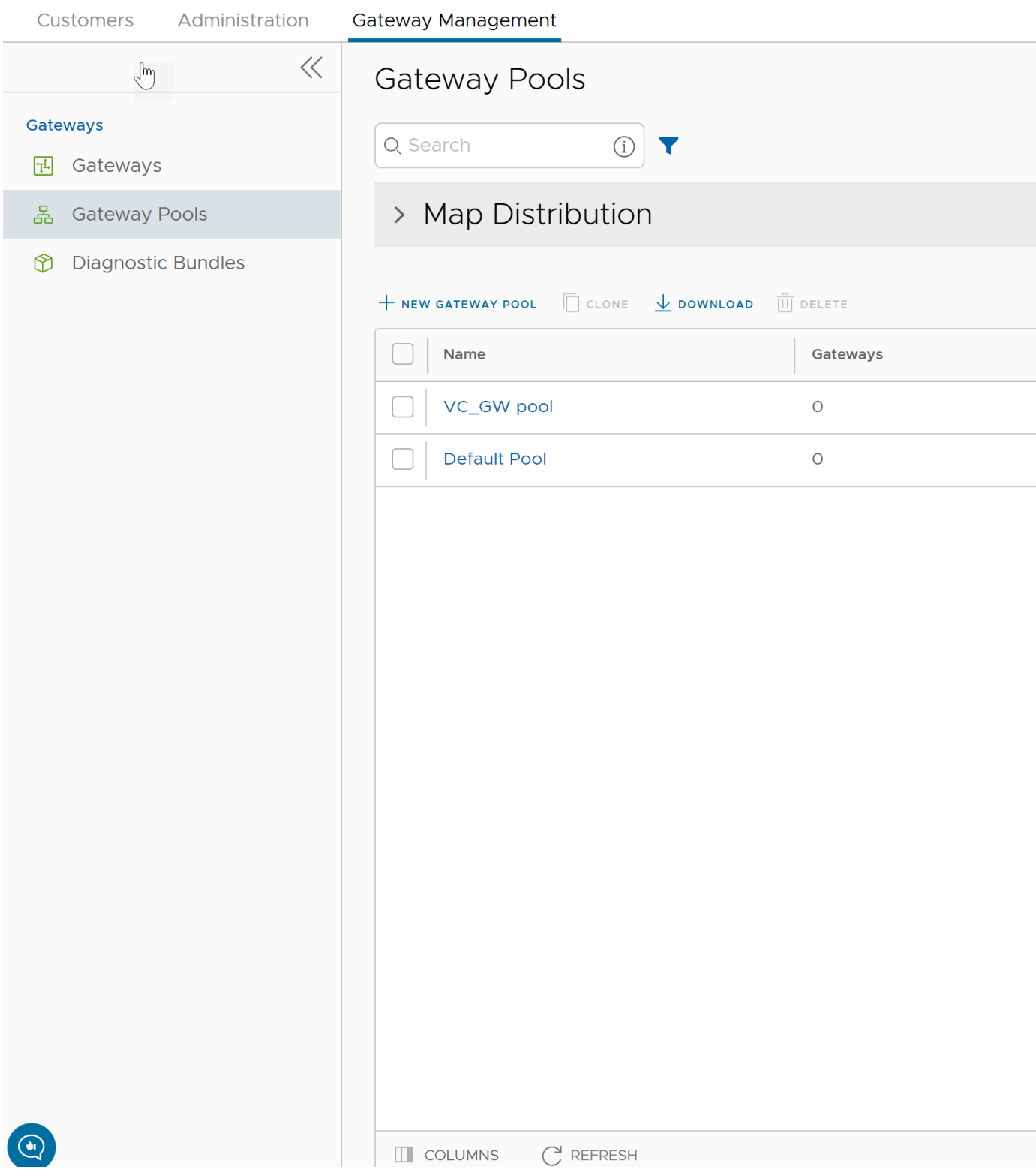
Note: The Gateway pools feature is not supported for Partner Business Specialist user and Partner IT support user.

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, click the **Gateway Management** tab and go to **Gateway Pools** in the left navigation pane.

   The **Gateway Pools** page appears.



3. To search a specific Gateway pool, enter a relevant search text in the **Search** box. For advanced search, click 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 click 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.

Field	Description
Name	Specifies the name of the Gateway pool. When clicking on 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 clicking on 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 clicking on a Customer link in the **Customers** column, a dialog opens with listed customers. If a user clicks on 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.

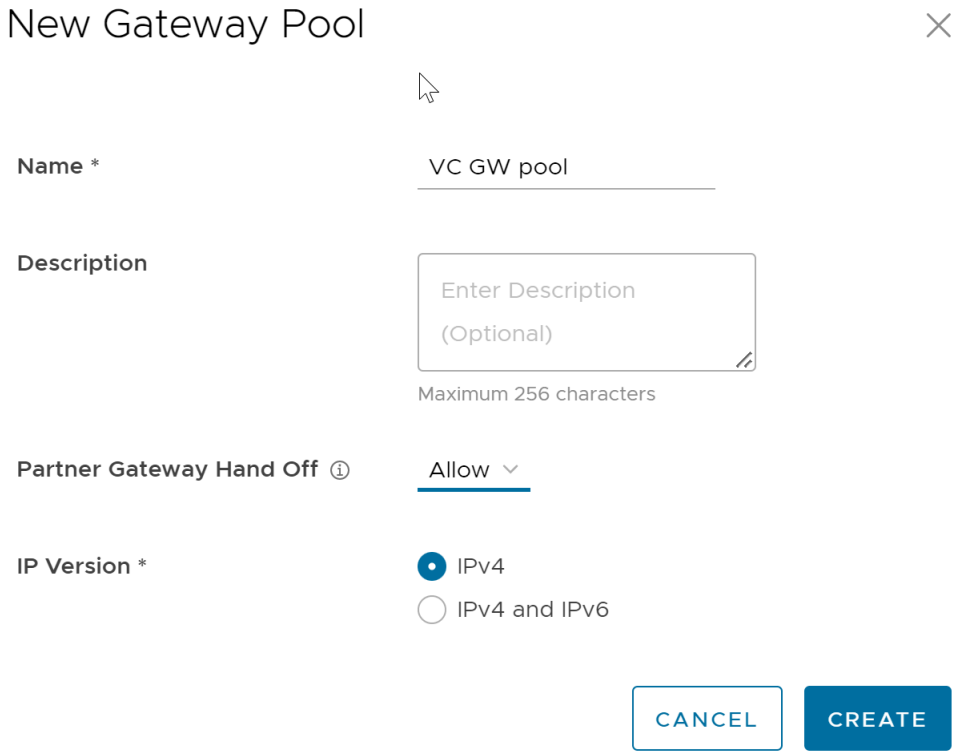
On the **Gateway Pools** page, you can perform the following activities:

- **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 an Enterprise Customer.
- You can also configure the existing Gateway pools by clicking the name link of the Gateway pool. See Configure Gateway Pools.

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



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.

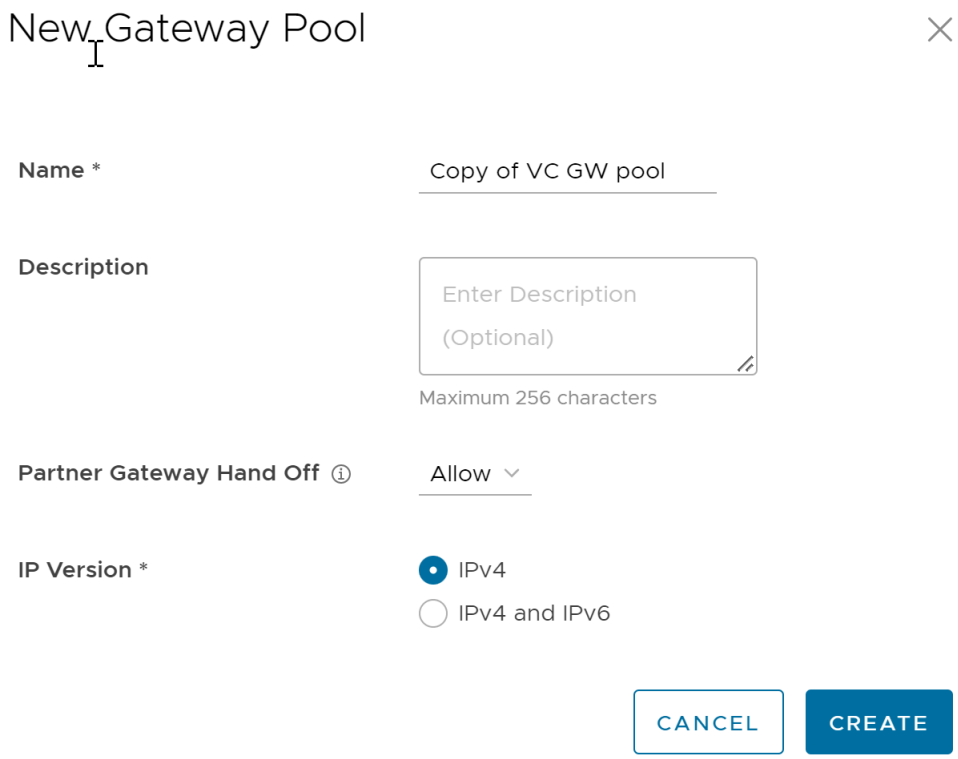
Field	Description
IP Version	Choose one of the following address types with which the Gateway pool should be enabled: • **IPv4** – Allows to add IPv4 only Gateways. • **IPv4 and IPv6** – Allows to add Gateways with IPv4 and IPv6 addresses. **Note:** If you want to use Edges with IPv6 support, then choose **IPv4 and IPv6**.

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

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, click 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 click **Clone**. The **New Gateway Pool** dialog with the cloned settings appears.



   The Gateway pool clones the existing configuration from the selected Gateway pool. If required, you can modify the details. For more information on the options, see Create New Gateway Pool.
3. After updating the Gateway pool details, click **Create**.

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

Configure Gateway Pools

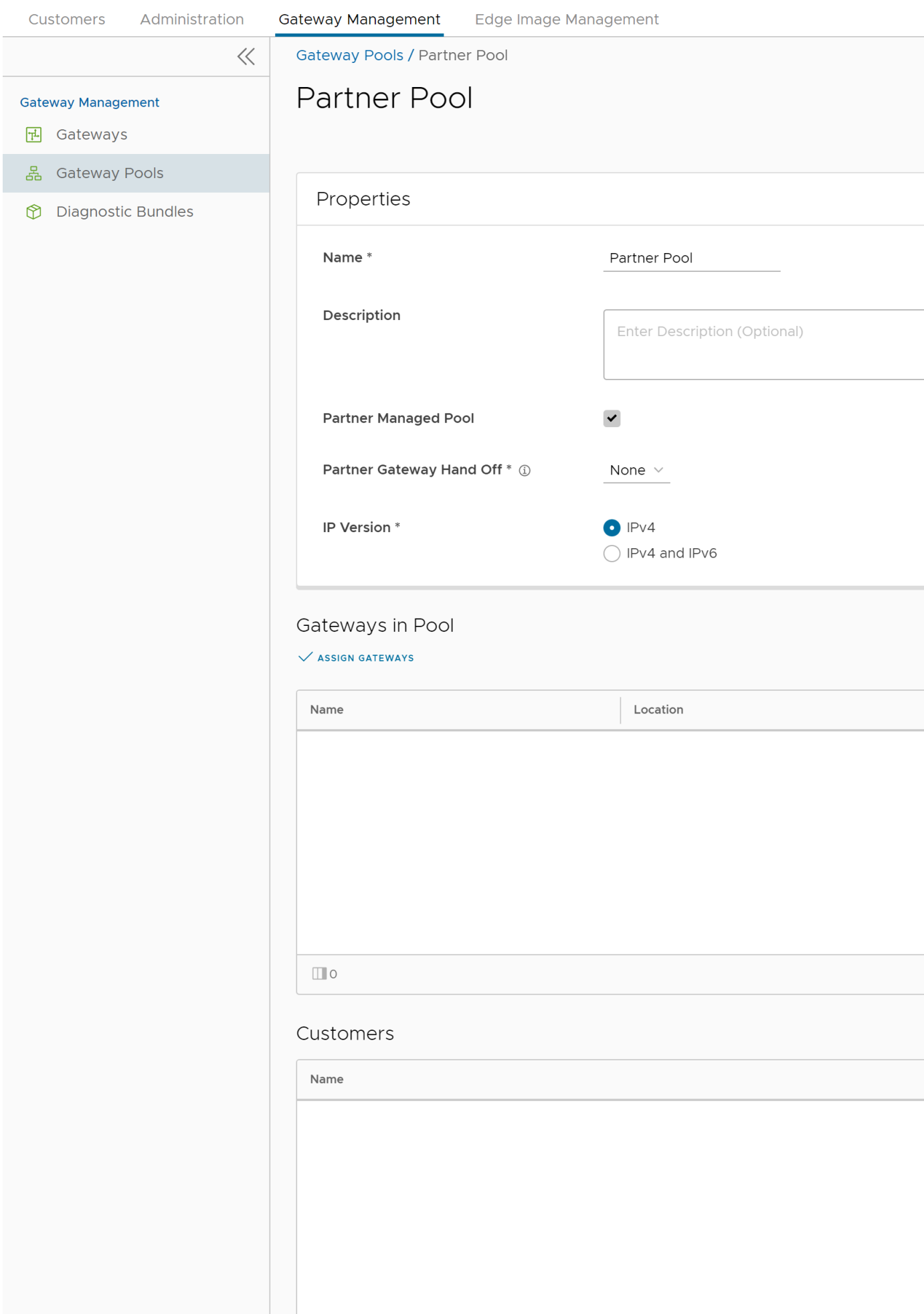
After creating a Gateway pool, you can add Gateways to the pool and associate the pool to an Enterprise Customer.

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.

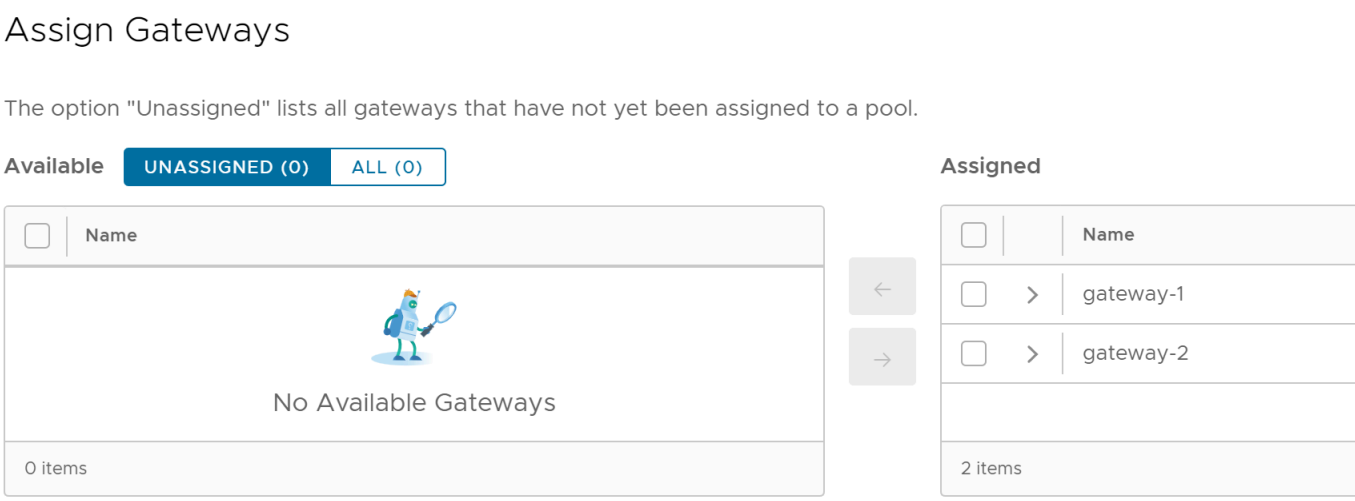
Note: You can configure only a Gateway pool created by a Partner User or a Partner Managed Gateway pool created by your Operator.

To configure an existing Gateway pool:

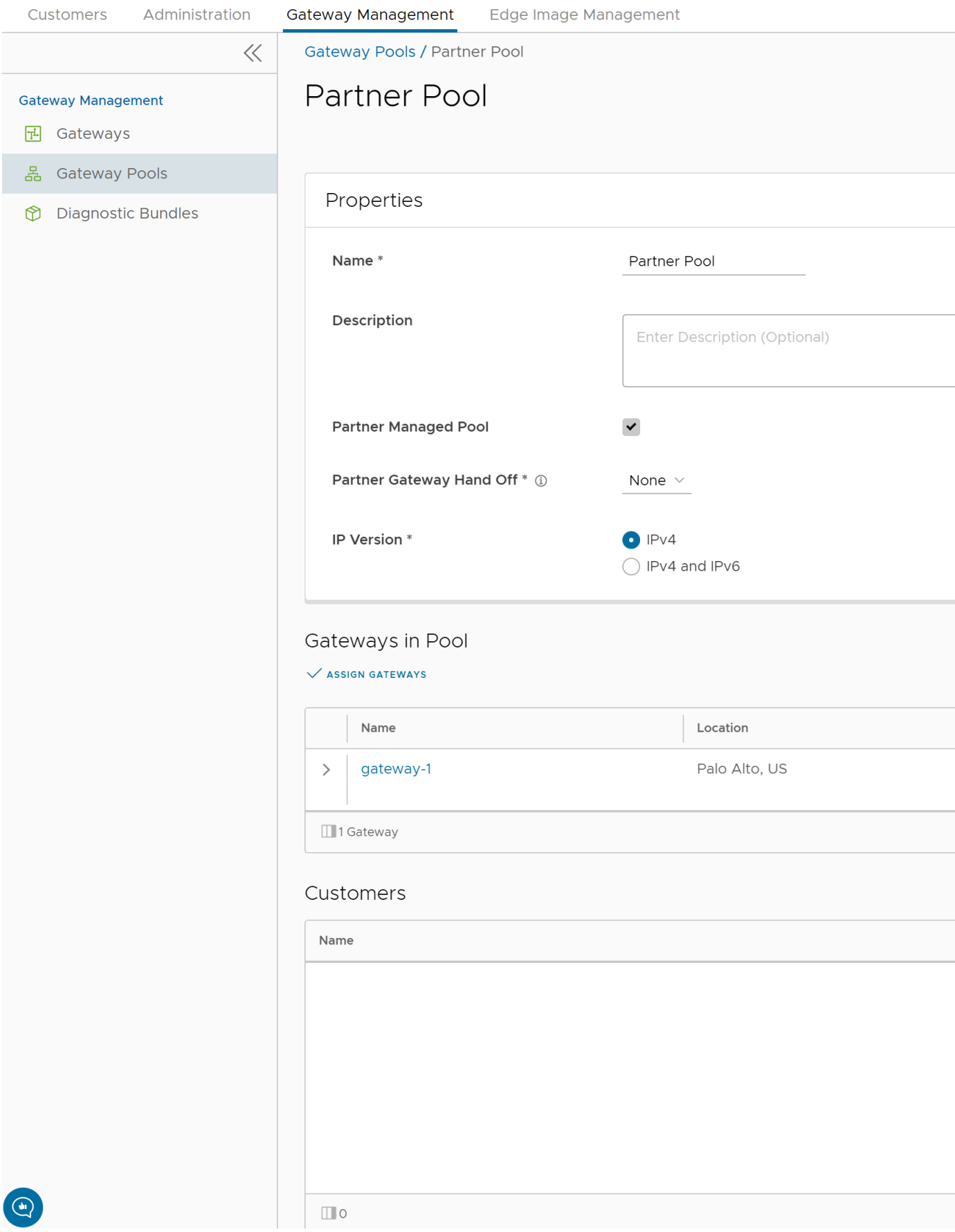
1. In the Orchestrator UI, click the **Gateway Management** tab and go to **Gateway Pools** in the left navigation pane. The **Gateway Pools** page appears.
2. Click the name link to a Gateway pool that you want to configure.
3. Configure the following details for the Gateway pool:


Customers
Administration
Gateway Management
Edge Image Management
Gateway Management
Gateways
Gateway Pools
Diagnostic Bundles
Gateway Pools / Partner Pool
Partner Pool
Properties
Name *
Partner Pool
Description
Enter Description (Optional)
Partner Managed Pool
Partner Gateway Hand Off *
None
IP Version *
IPv4
IPv4 and IPv6
Gateways in Pool
ASSIGN GATEWAYS
Name
Location
0
Customers
Name

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, click **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 click **Update**.



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


Customers
Administration
Gateway Management
Edge Image Management
Gateway Management
Gateways
Gateway Pools
Diagnostic Bundles
Gateway Pools / Partner Pool
Partner Pool
Properties
Name *
Partner Pool
Description
Enter Description (Optional)
Partner Managed Pool
Partner Gateway Hand Off *
None
IP Version *
IPv4
IPv4 and IPv6
Gateways in Pool
ASSIGN GATEWAYS
Name
Location
gateway-1
Palo Alto, US
1 Gateway
Customers
Name
0

5. Click **Save Changes**.

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

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

Refer to the following links to associate the Gateway pool:

- For a new customer, see Create New Partner Customer.
- For an existing customer, see Configure Partner Customers.

Manage 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 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 . If required, you can create additional 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.

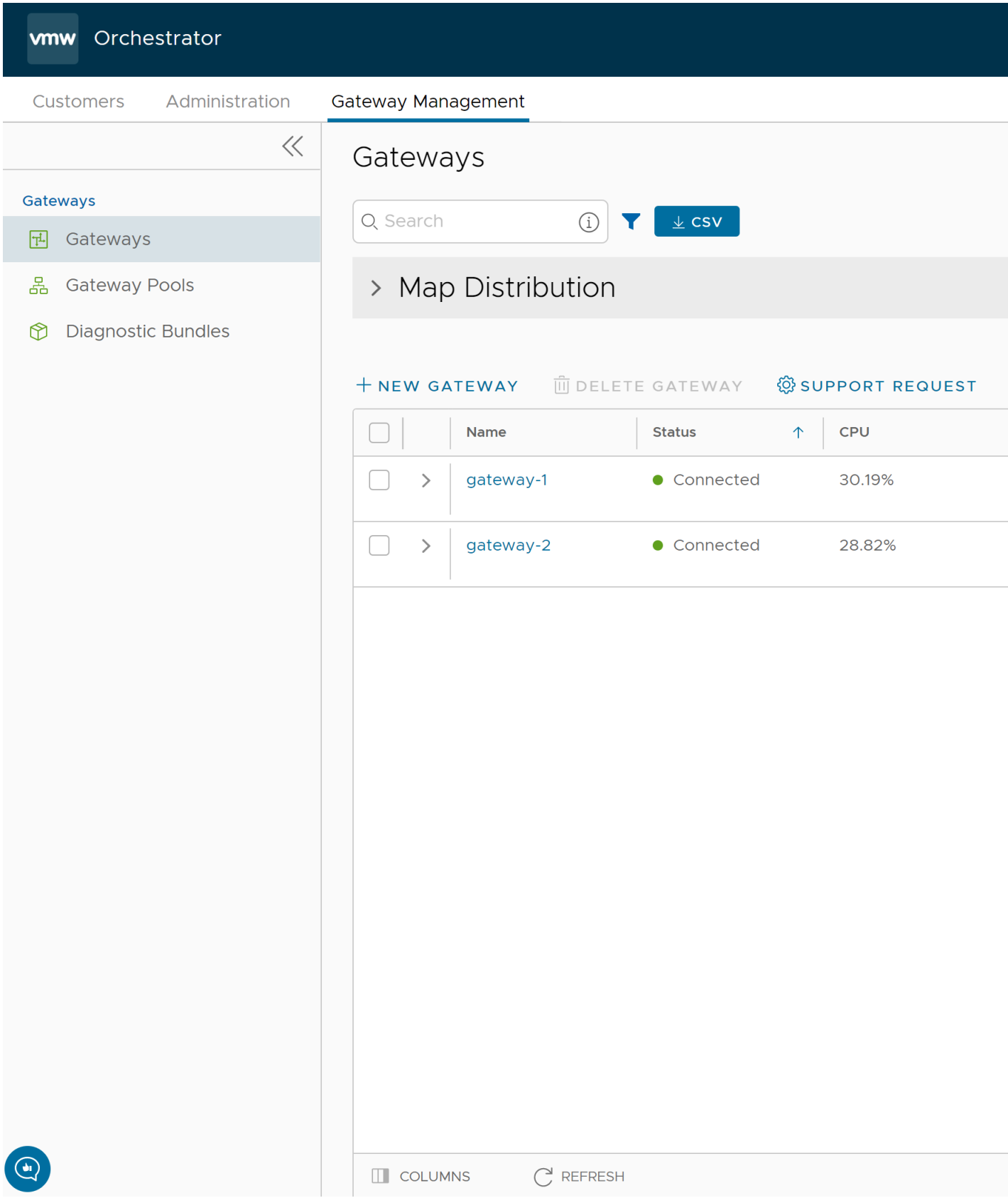
If the Gateway management access is deactivated for a Partner, then the Partner will have only read-only permission for the configured Gateways. To request Gateway Management access, Partners must contact the Operator Super user.

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, click the **Gateway Management** tab and go to **Gateways** in the left navigation pane.

   The **Gateways** page appears.



To search a specific Gateway, enter a relevant search text in the **Search** box. For advanced search, click 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 click the **+** and **-** buttons to zoom in and zoom out the map, respectively.

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

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:** Click **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.

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

- **New Gateway** – Creates a new Gateway. See Create New Gateway to Pair with Bastion Orchestrator Create New Gateway with New Orchestrator UI.
- **Delete Gateway** – Deletes the selected Gateway. You cannot delete a Gateway that is already being used by an Enterprise Customer.

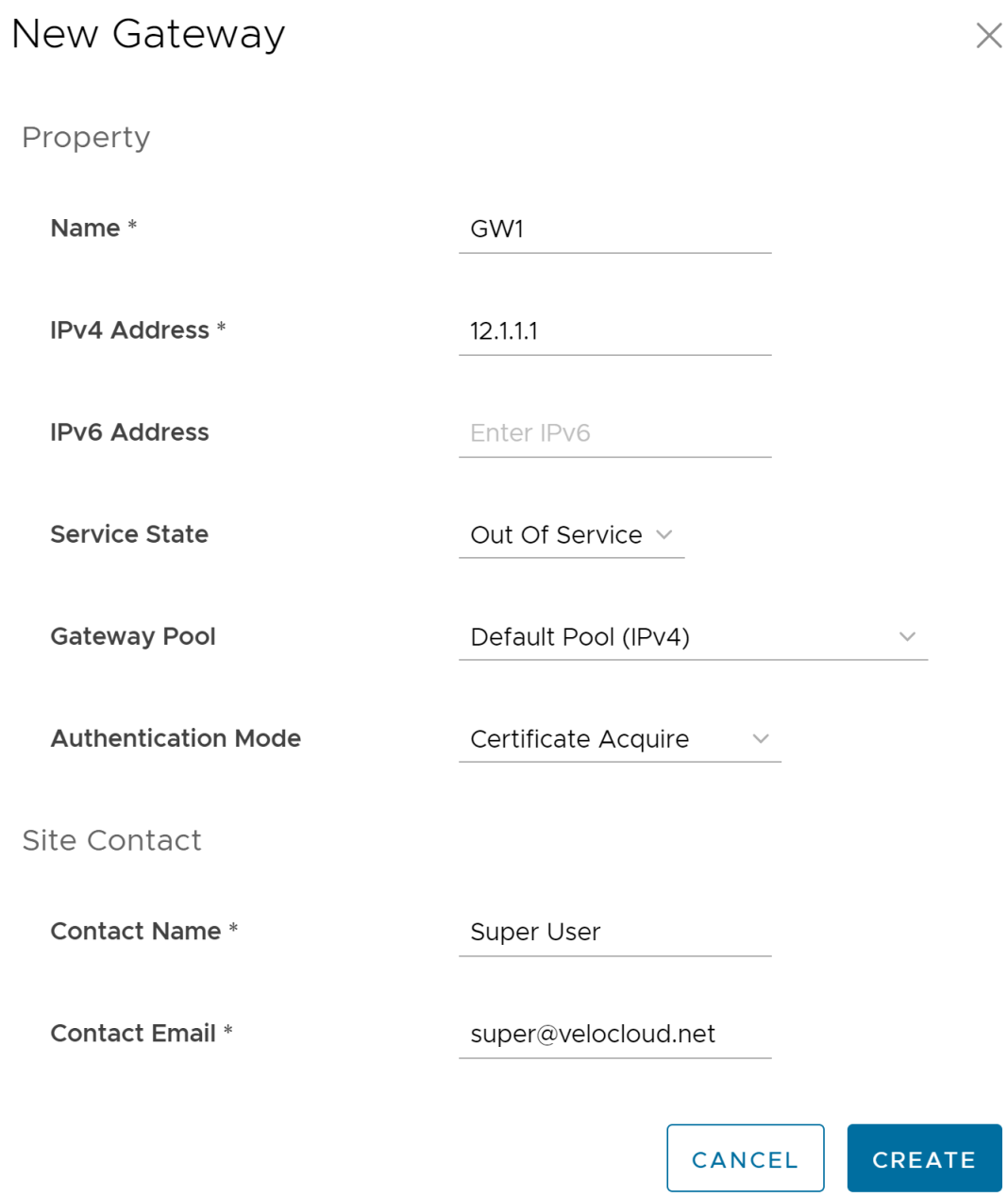
- **Support Request** – Redirects to a Knowledge Base article that has instructions on how to file a support request.

Create New Gateway with New Orchestrator UI

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



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 , 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 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.

To configure additional settings for the Gateway, see Configure Gateways.

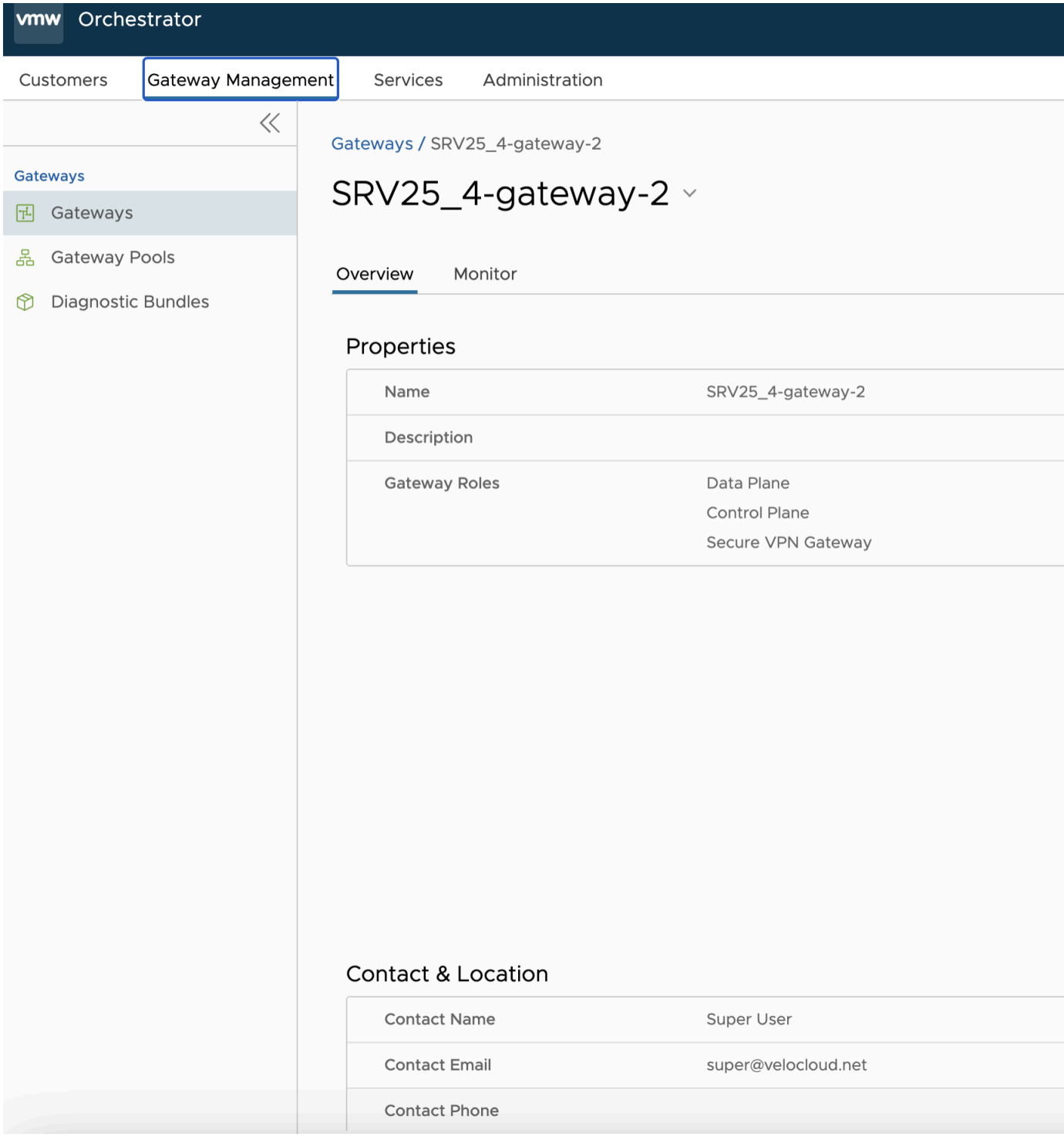
Configure Gateways

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, click the **Gateway Management** tab and go to **Gateways** in the left navigation pane. The **Gateways** page displays the list of available Gateways.
2. Click 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:


vmw Orchestrator
Customers
Gateway Management
Services
Administration
Gateways
Gateways
Gateway Pools
Diagnostic Bundles
Gateways / SRV25_4-gateway-2
SRV25_4-gateway-2
Overview
Monitor
Properties
Name
SRV25_4-gateway-2
Description
Gateway Roles
Data Plane
Control Plane
Secure VPN Gateway
Contact & Location
Contact Name
Super User
Contact Email
super@velocloud.net
Contact Phone

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. • **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.  **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**.

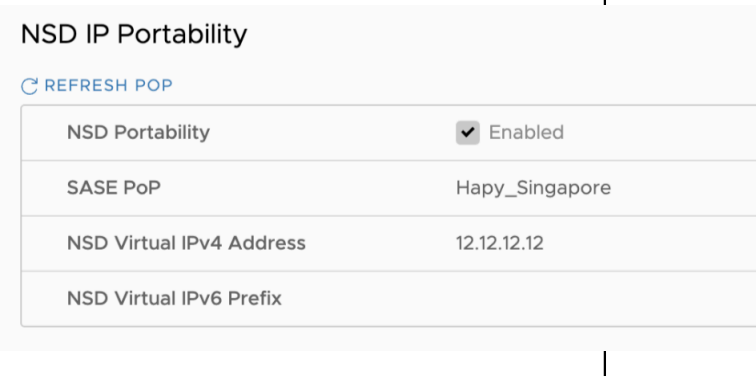
Option	Description

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 more 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 , 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 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:

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. 

Option	Description
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 more information, see the *Configure NAT Entry Syslog for Gateways* section in the *Operator Guide* published at www.arista.com/en/support/product-documentation
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 more information, see the *Partner Gateway (Advanced Handoff) Details* section below.

Partner Gateway (Advanced Handoff) Details

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

Option	Description
Static Routes | Subnets – Specify the subnets or routes that the should advertise to the. This is global per 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 and have the handoff of type NAT. You can click 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 uses ICMP probe to check for the reachability of a particular IP address and notifies the to failover to the secondary Gateway if the IP address is not reachable. This option supports only IPv4 addresses.	

Option	Description
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 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** – responds to the ICMP request only when the service is up and when at least one tunnel is up. • **Always** – 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. With BGP support on the Partner Gateway, using ICMP probe for failover and route convergence is no longer required. For more information on configuring BGP support and handoff settings for a Partner Gateway, see Configure Partner Gateway Handoff to Production Orchestrator Configure Partner Handoff.

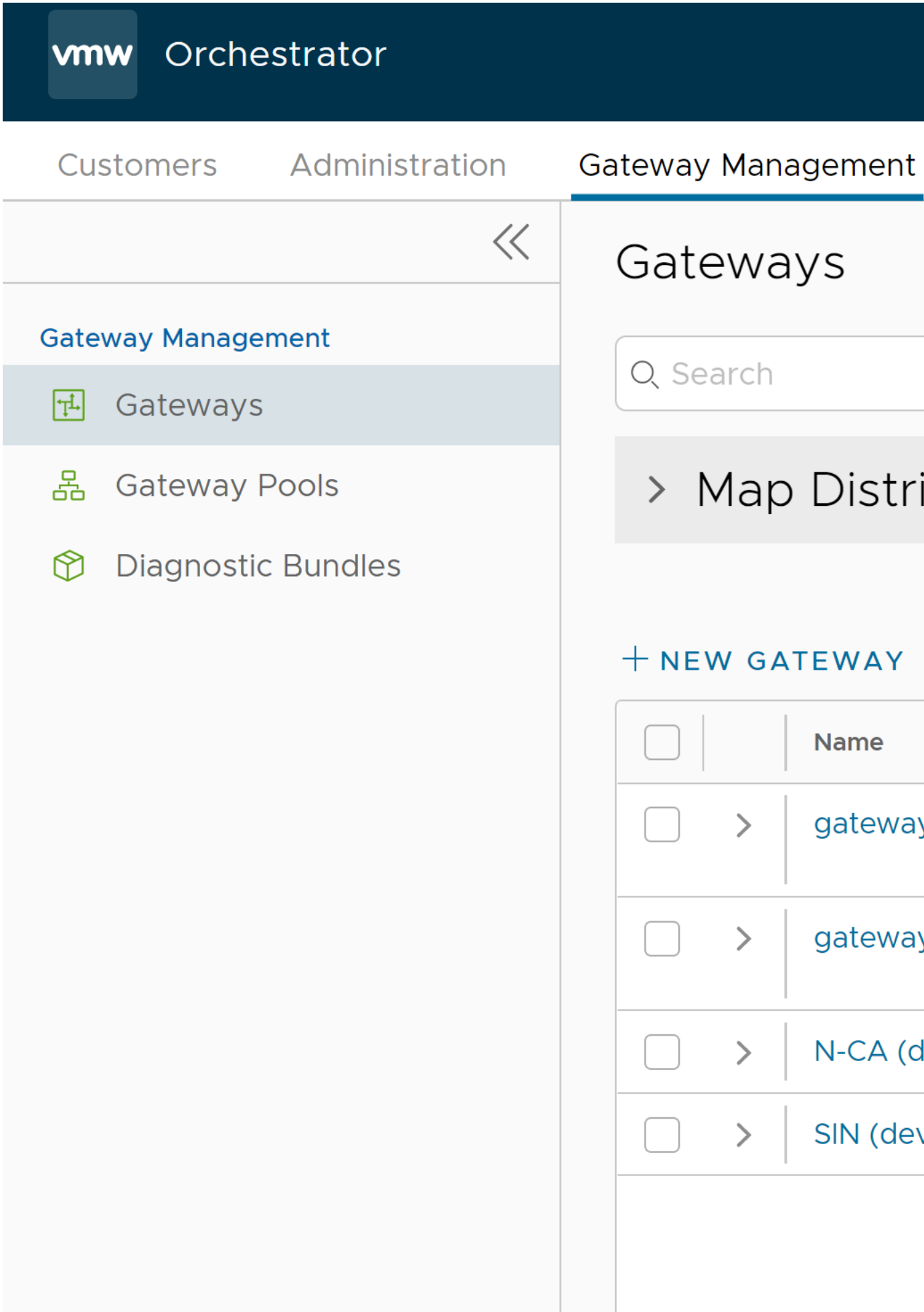
4. After configuring the required details, click **Save Changes**.

Monitor Gateways

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

To monitor the :

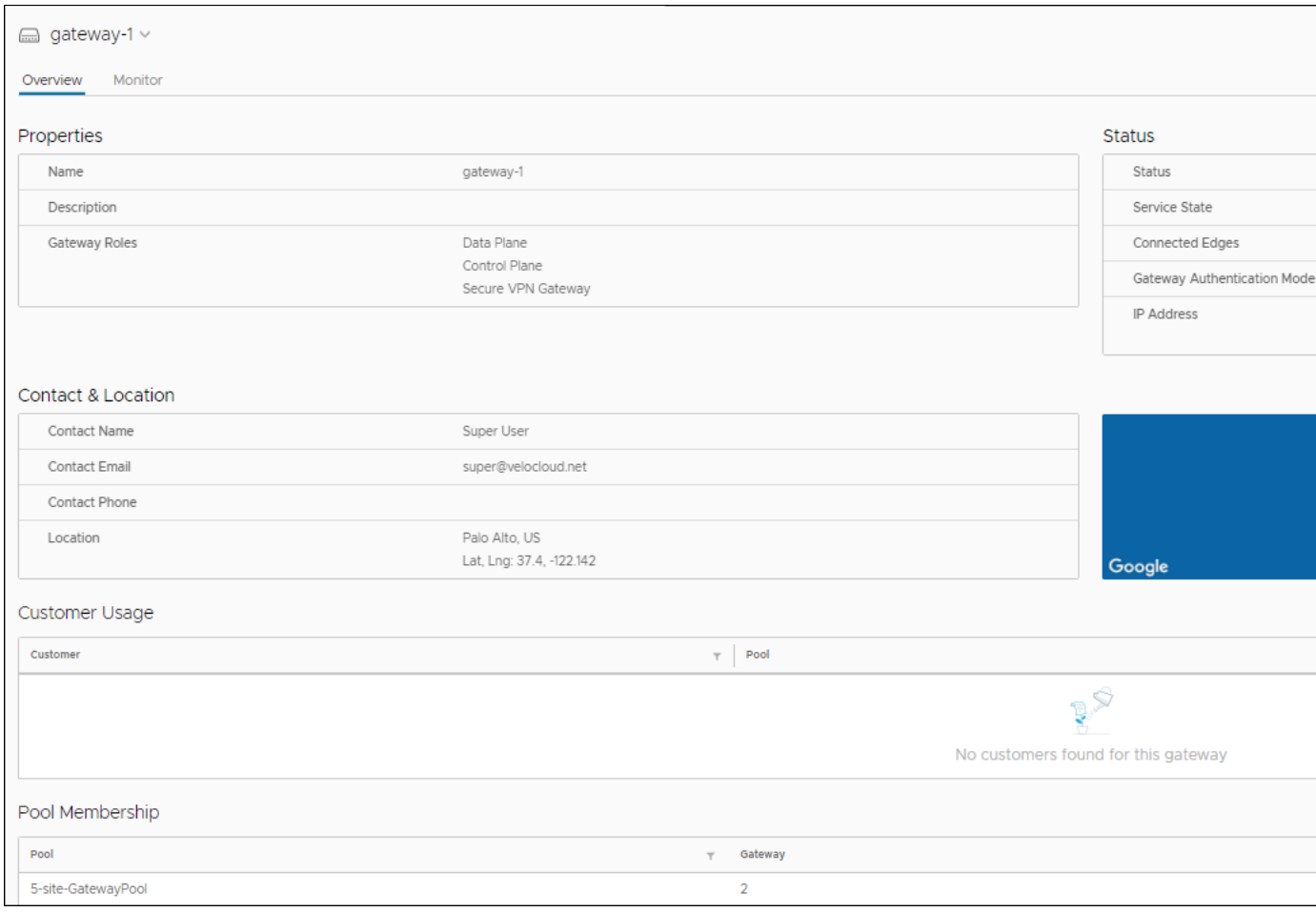
1. Login to the as a Partner and in the Partner portal, Click **Gateway Management** > **Gateways**.
2. The **Gateways** page displays the list of available Gateways.


vmw Orchestrator
Customers
Administration
Gateway Management
Gateway Management
Gateways
Gateway Pools
Diagnostic Bundles
Gateways
Search
Map Distri
+ NEW GATEWAY
Name
gateway
gateway
N-CA (d
SIN (dev

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

   The page displays the following details:

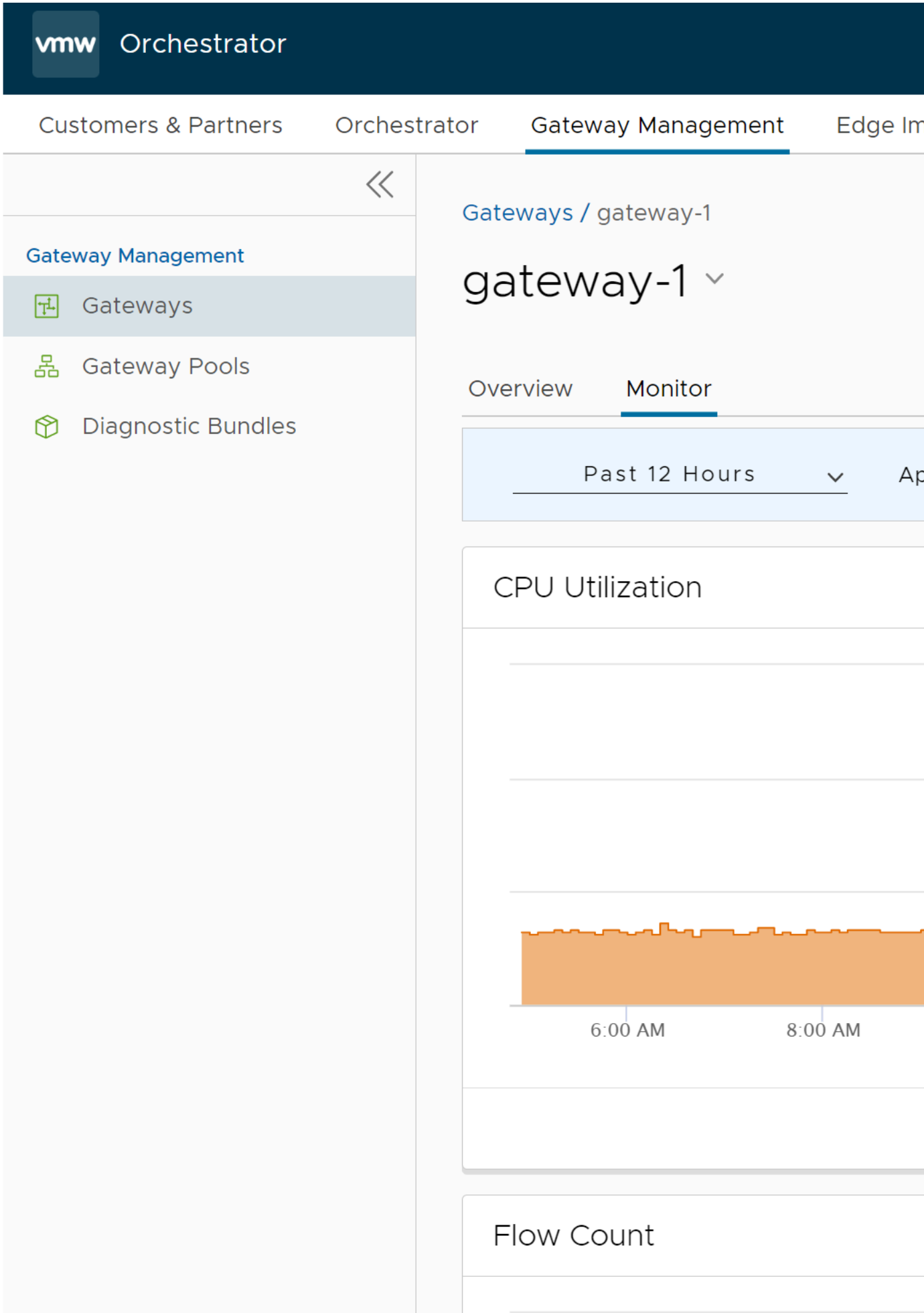
   - **Name** – Name of the .
   - **Status** – Current status of the . The status may be one of the following: Connected, Degraded, Never Activated, Not in Use, Offline, Out of Service, or Quiesced.
   - **CPU** – Percentage of CPU utilization by the .
   - **Memory** – Percentage of memory utilization by the .
   - **Edges** – Number of connected to the .
   - **Service State** – Service state of the . 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 .
   - **Location** – Location of the .
5. In the Search field, enter a term to search for specific details. Click the Filter icon to filter the view by a specific criterion.
6. Click the **CSV** option to download a report of the in the CSV format.
7. Click the link to a to view the details of the selected .



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

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 .

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


vmw
Orchestrator
Customers & Partners
Orchestrator
Gateway Management
Edge Im
Gateway Management
Gateways
Gateway Pools
Diagnostic Bundles
Gateways / gateway-1
gateway-1
Overview
Monitor
Past 12 Hours
Ap
CPU Utilization
6:00 AM
8:00 AM
Flow Count

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 more details.

Migration

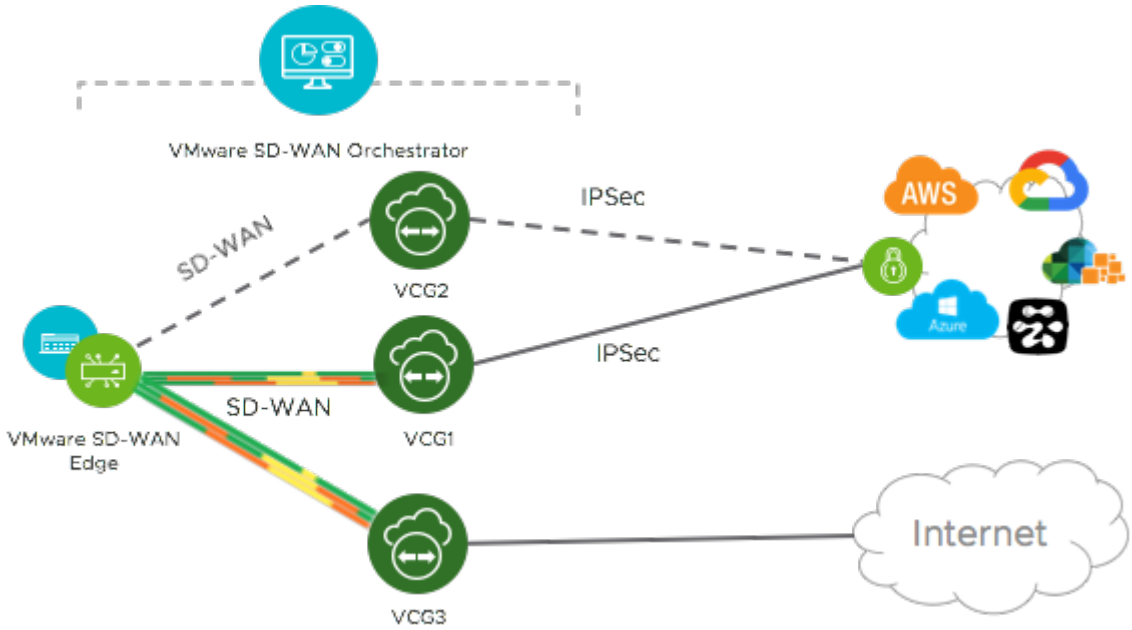
provides a self-service migration functionality that allows you to migrate from your existing Gateway to a new Gateway without your Operator's support.

Gateway migration may be required in the following scenarios:

- Achieve operational efficiency.
- Decommission old Gateways.

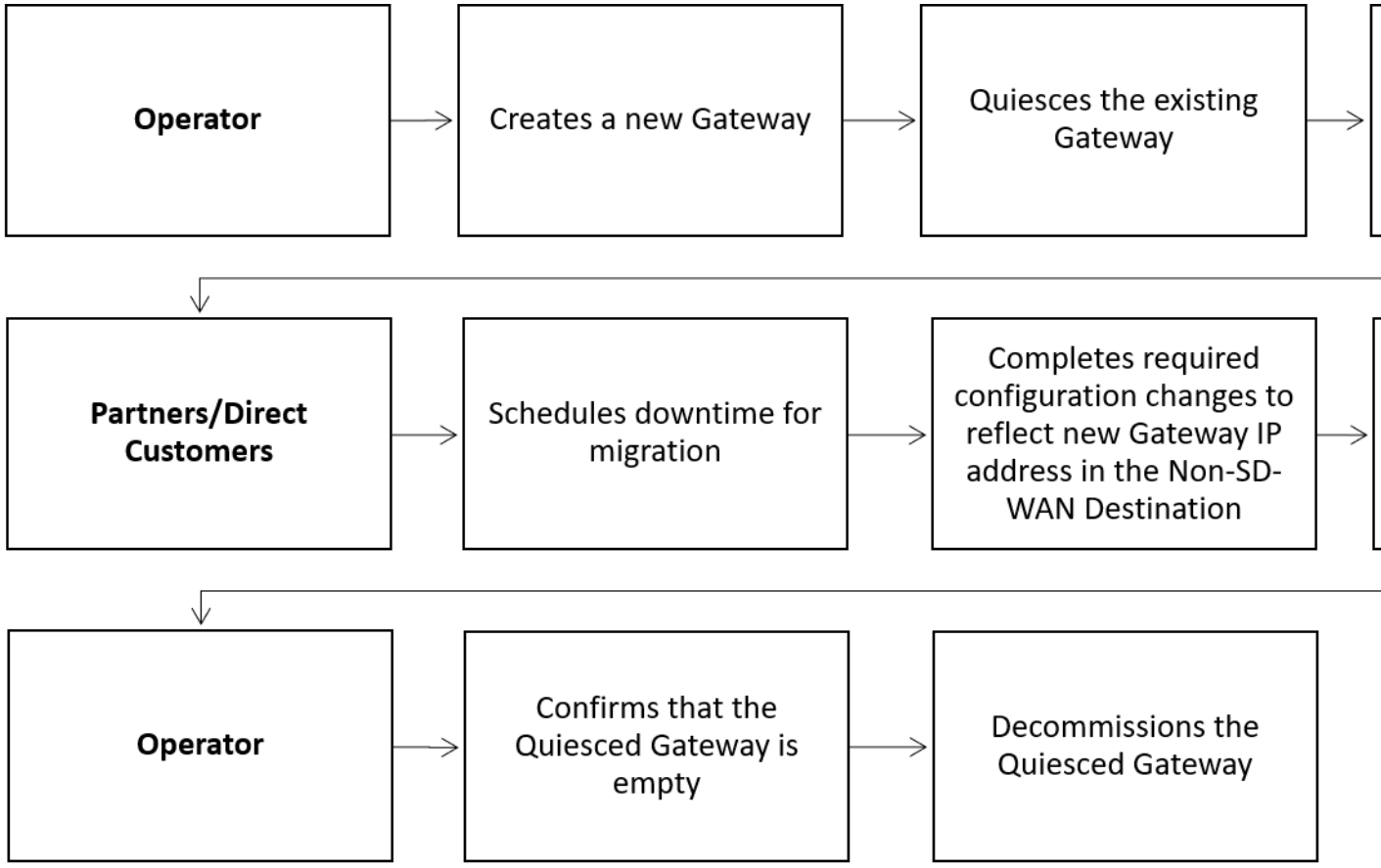
Gateways are configured with specific roles. For example, a Gateway with data plane role is used to forward data plane traffic from source to destination. Similarly, a Gateway with Control Plane role is called a Super Gateway and is assigned to an Enterprise. Edges within the Enterprise are connected 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 more information about the Gateway roles, see the "Configure Gateways" section in the *Operator Guide* available at https://www.arista.com/en/support/product-documentation.

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



In this example, a 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:



Migration - Limitations

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.

Migrate Quiesced Gateways

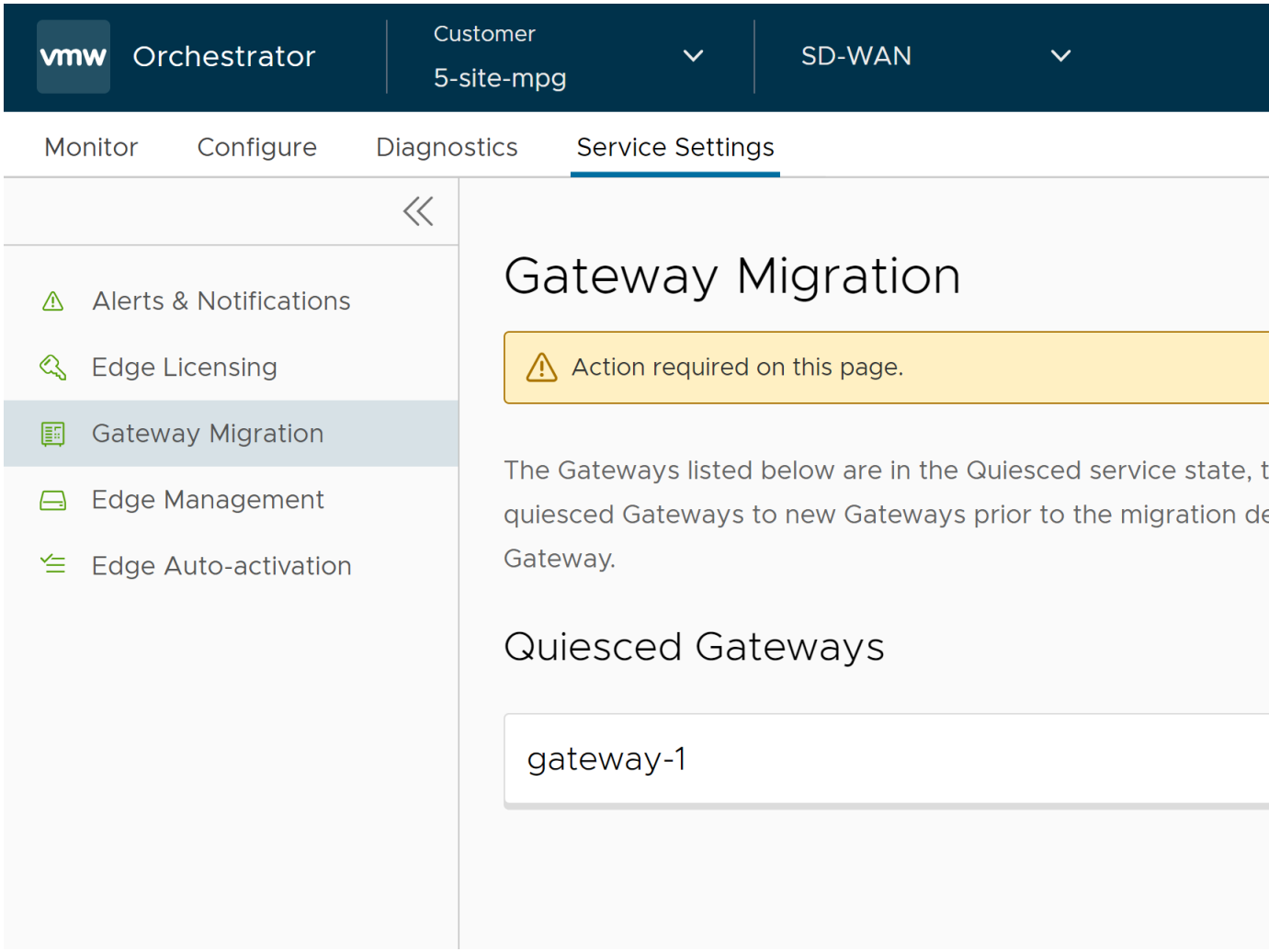
Operators send notification emails about Gateway migration to Administrators with Super User privileges. Plan your migration based on the notification email that you receive from your Operator.

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.

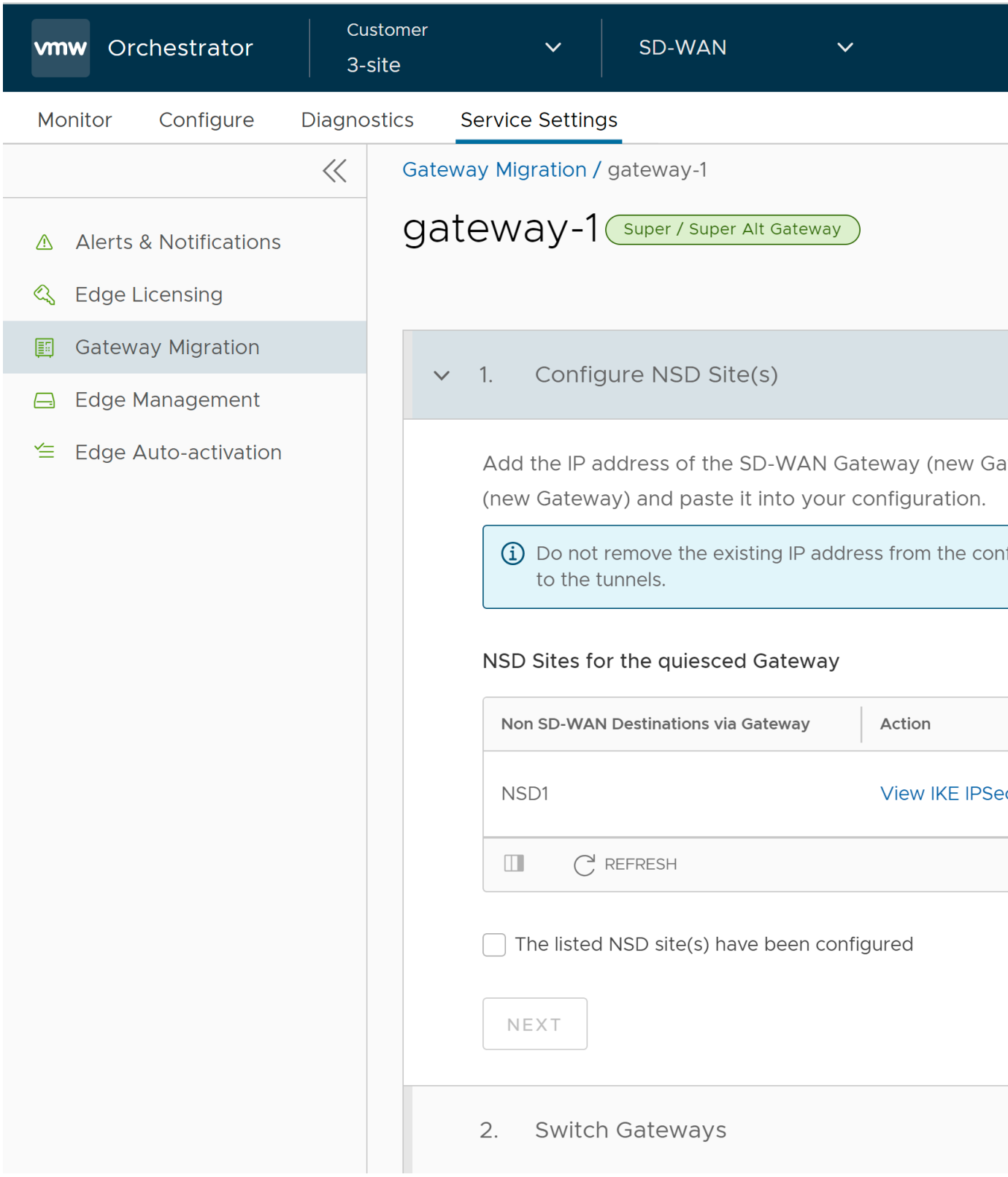


2. Click **Start** for the quiesced Gateway from which you want to migrate to the new Gateway.

Note:

Note: Step 3 and 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.



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

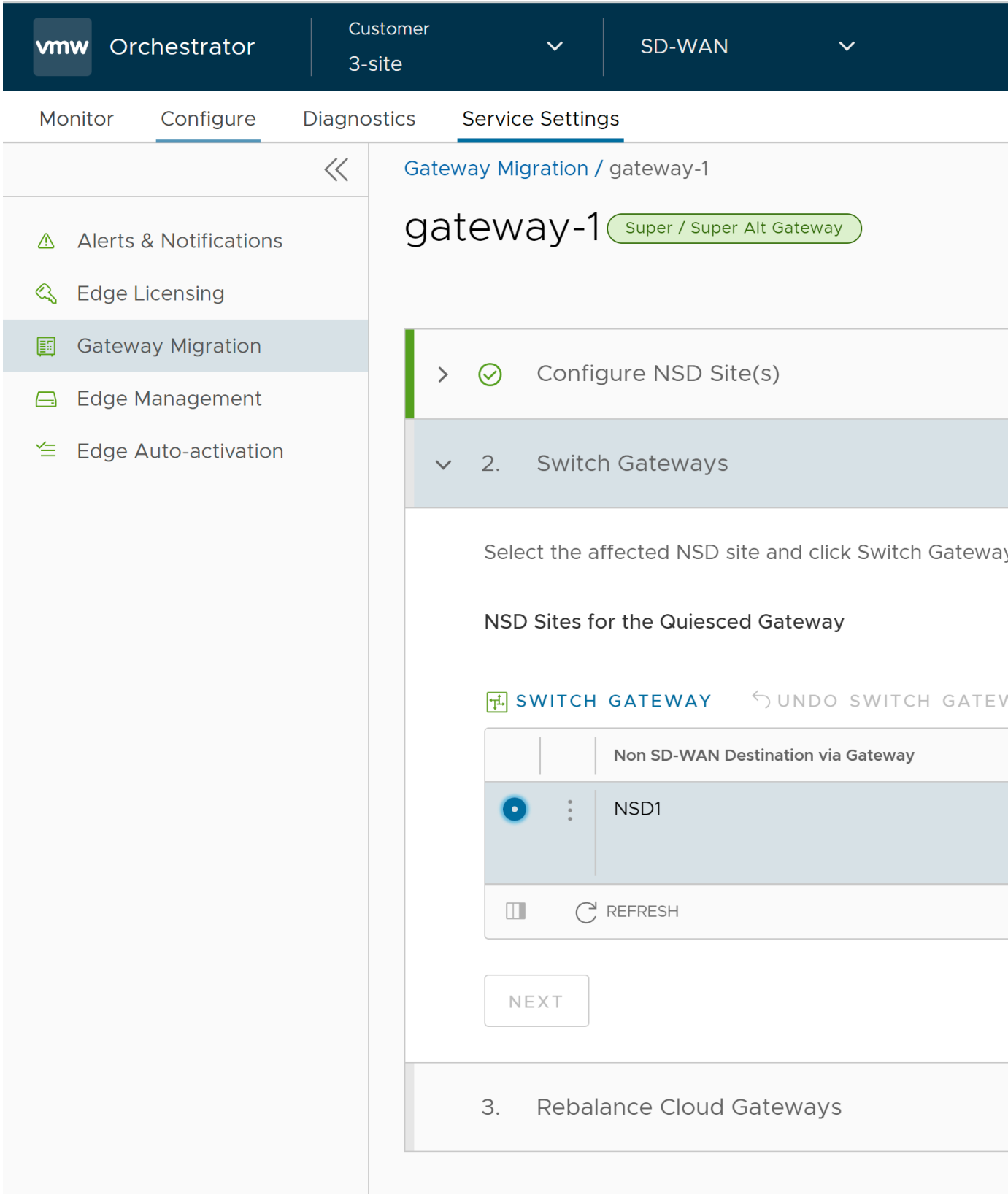
b) Add the IP address of the SD-WAN Gateway (new Gateway IP) to each NSD configured for the quiesced Gateway.

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.

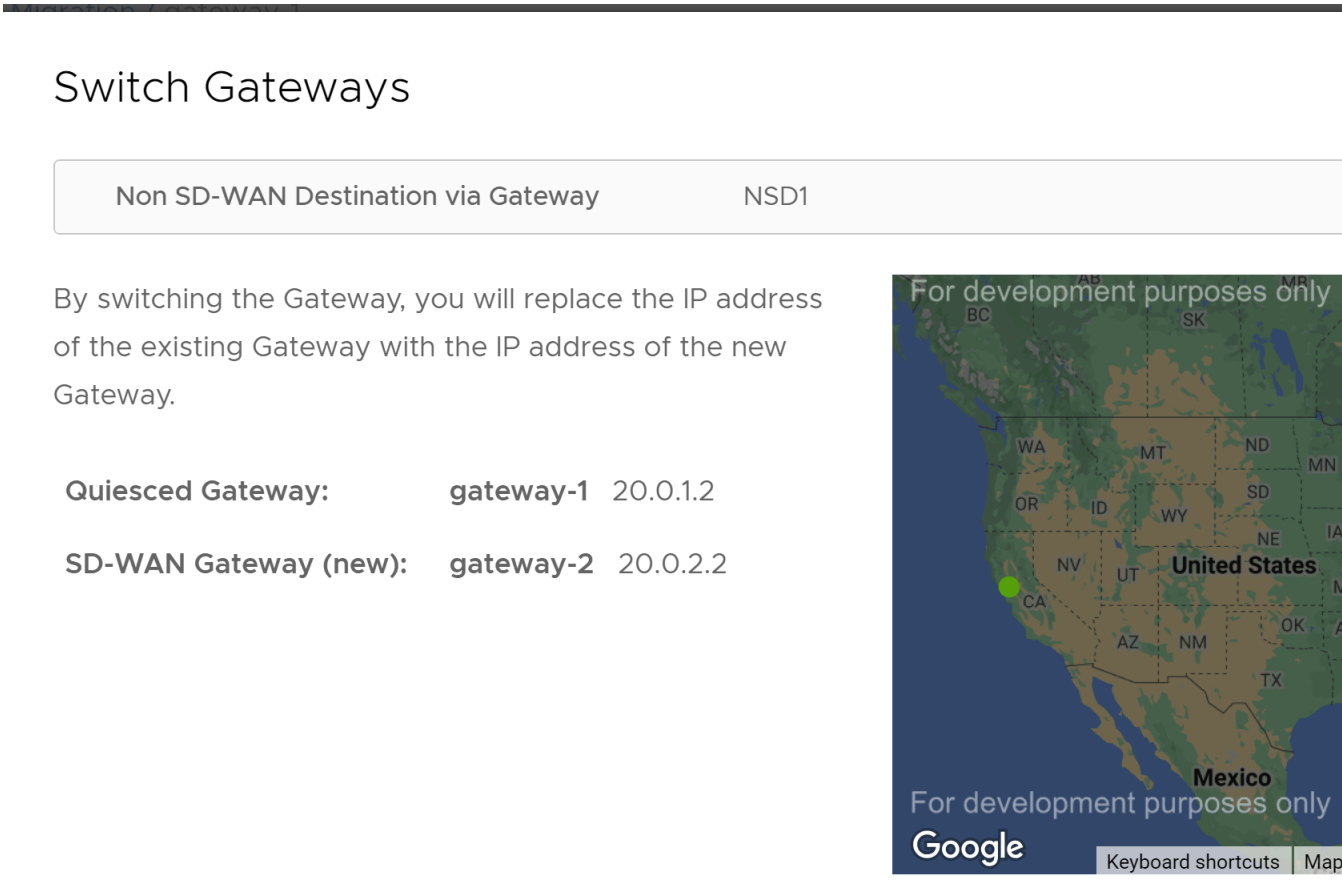
c) After making the configuration changes to all the NSDs, select the **The listed NSD site(s) have been configured** check box, and then click **Next**.

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 click **Switch Gateway** to switch the traffic from the quiesced Gateway to the 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.



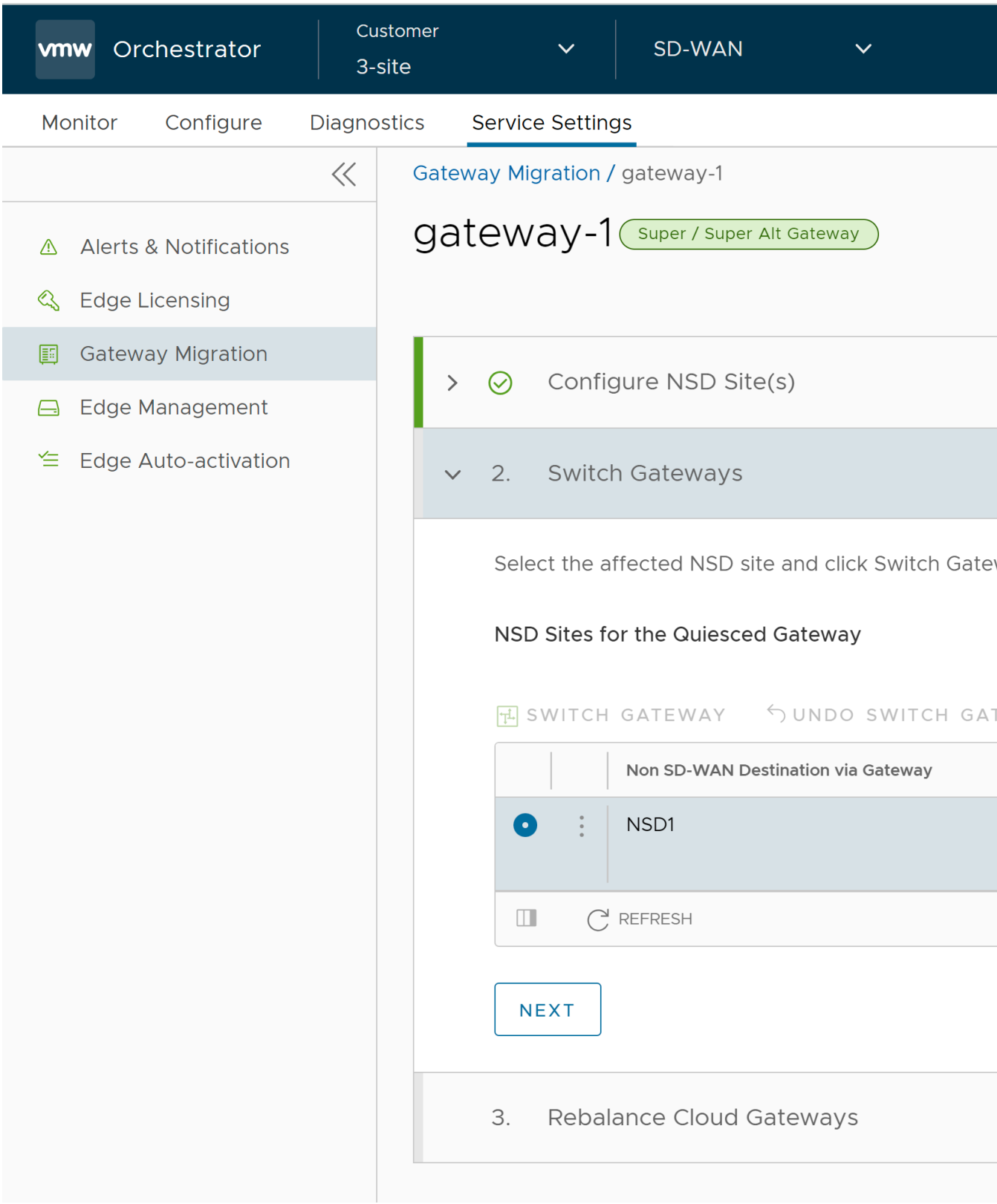
Note: This confirmation is not applicable for NSDs configured automatically.

b) Click **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 screenshot. If the Switch Gateway action fails, see

What to do When Switch Gateway Action Fails

.



c) Click **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.

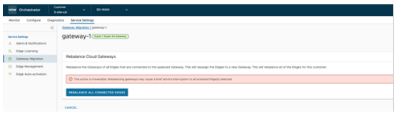


Figure 1: Rebalance All Connected Edges - Super Gateway

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

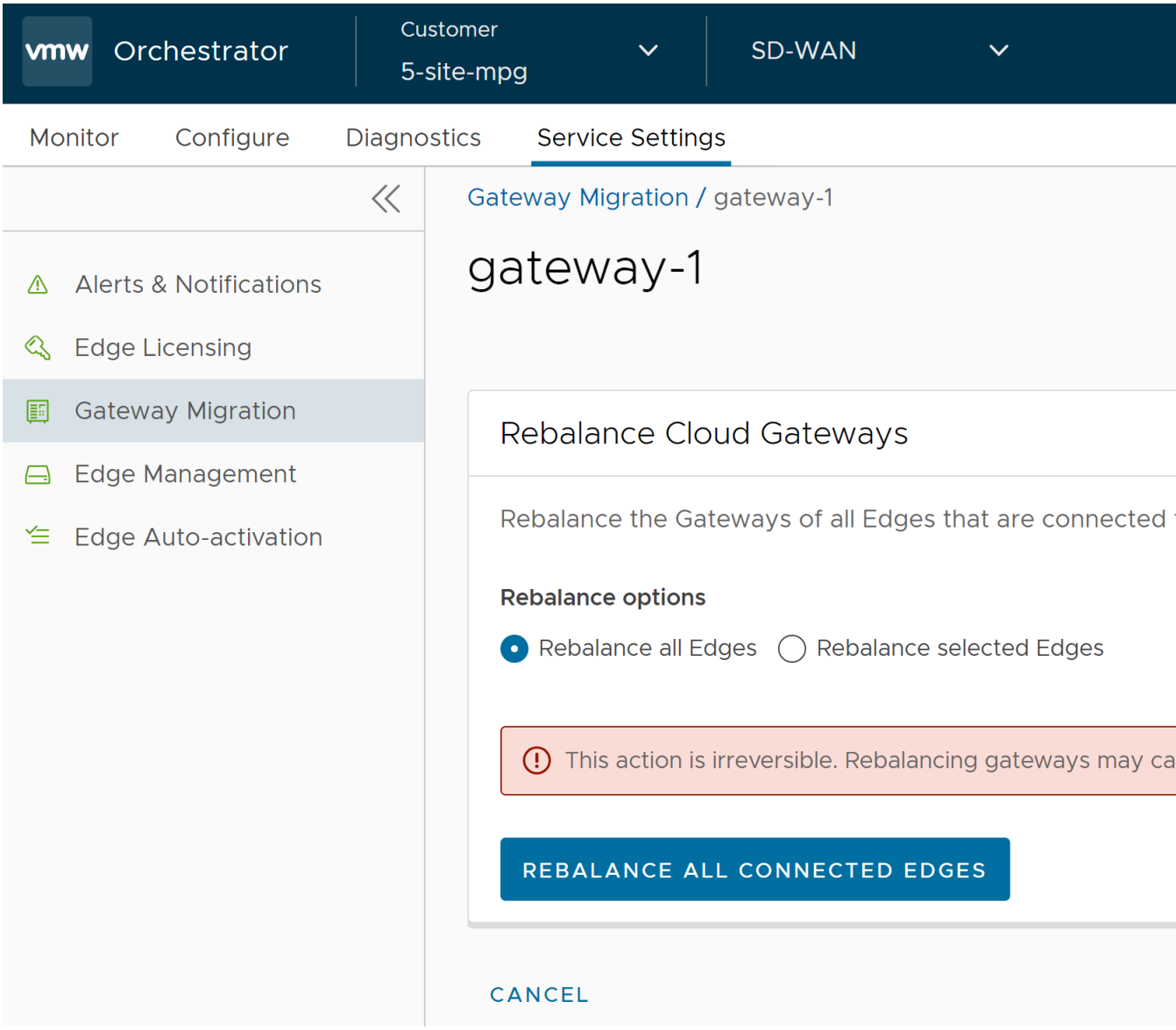


Figure 2: Rebalance All Connected Edges - Primary or Secondary Gateway

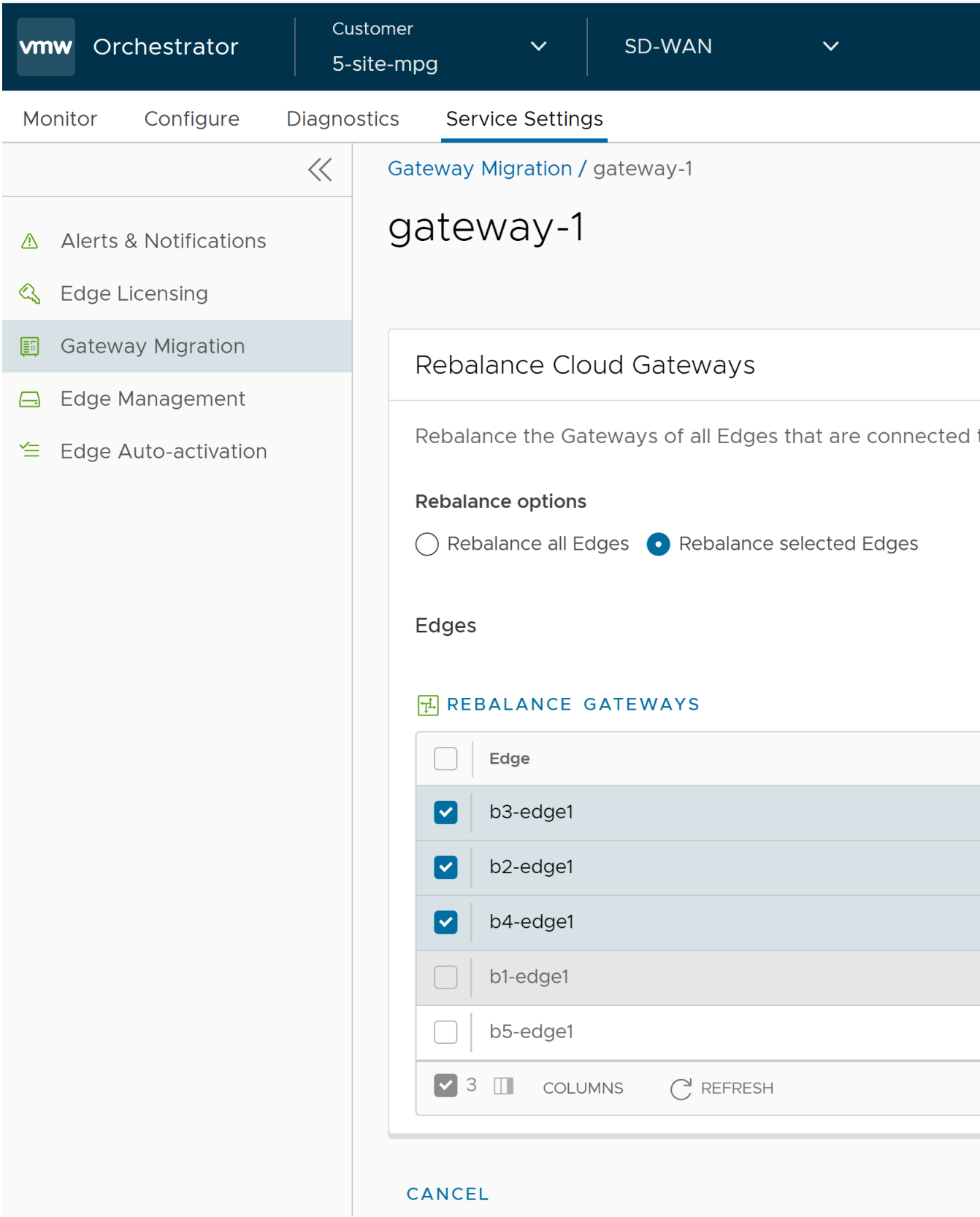
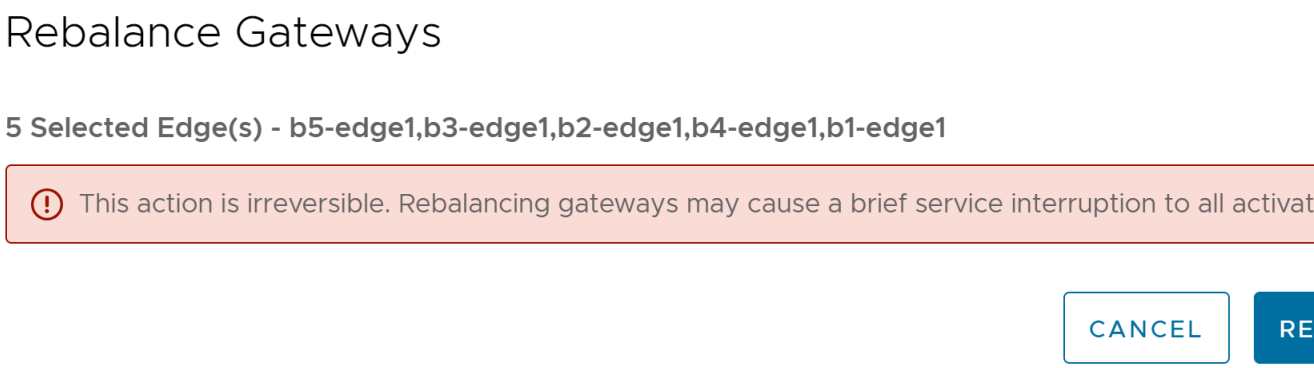
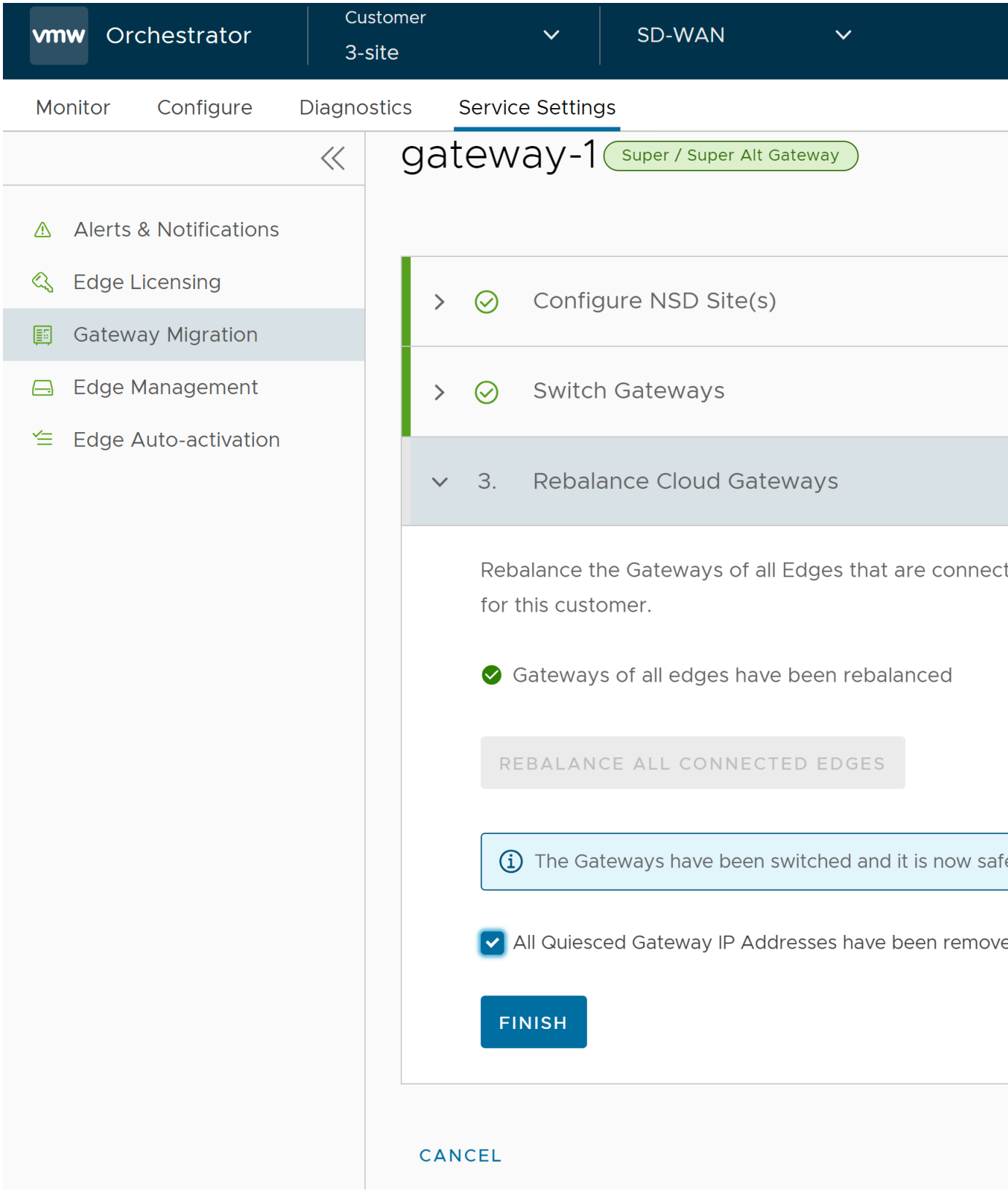


Figure 3: Rebalance Selected Edges - Primary or Secondary Gateway

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

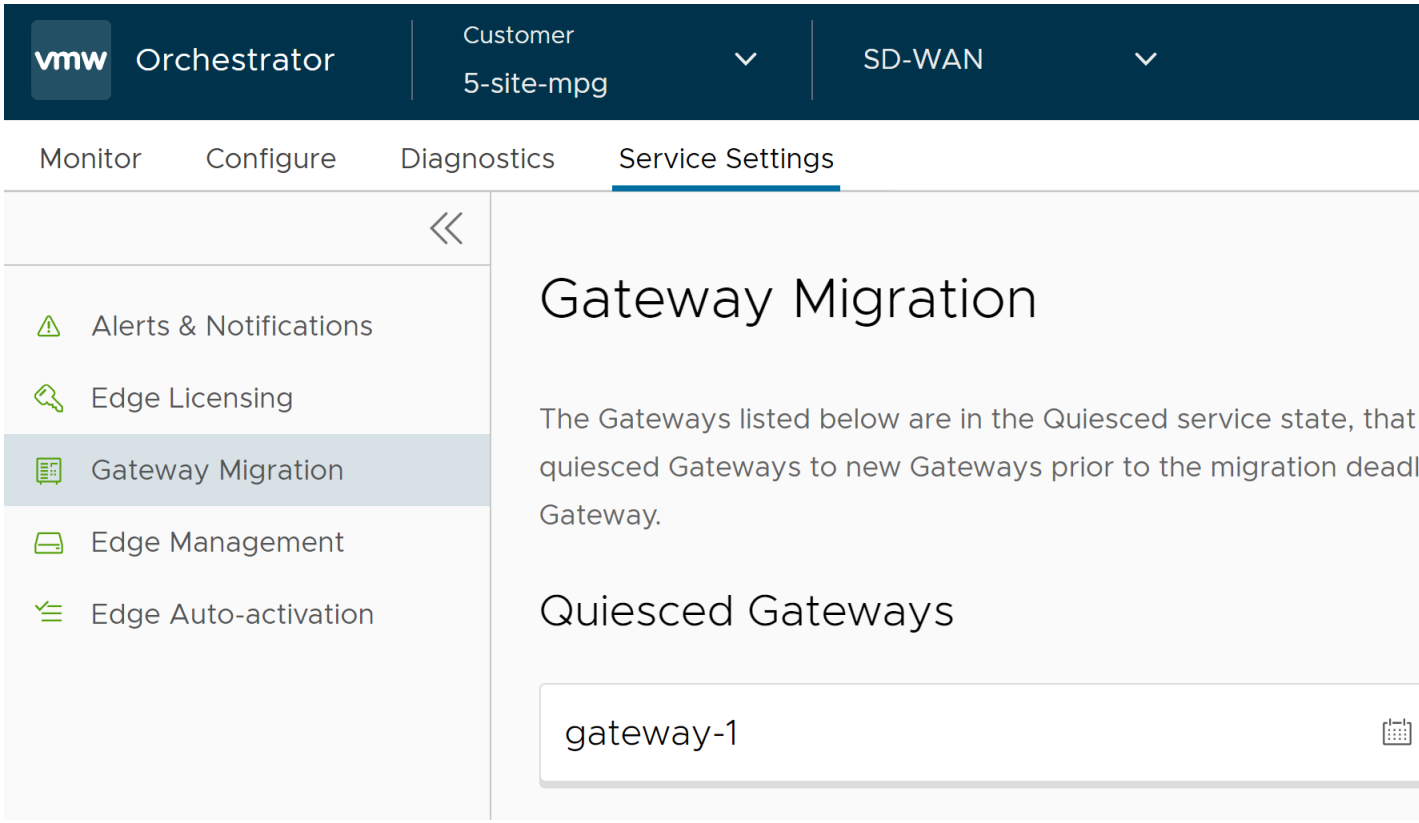


5. Click **Rebalance Gateway** to complete the Gateway migration. The Edges connected to the quiesced Gateway are migrated to the new Gateway.

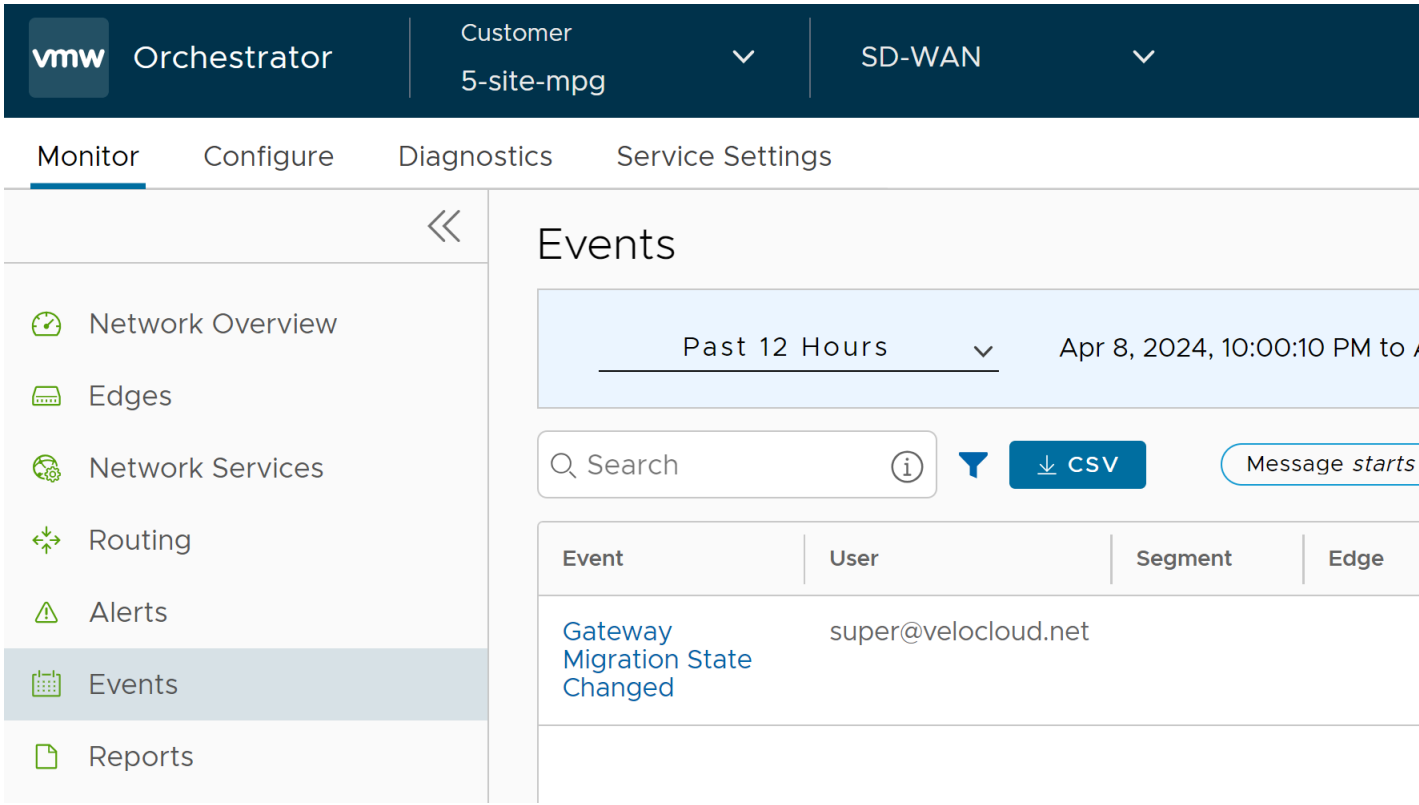


6. Click **Finish**.

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



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.



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 click **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 click **Undo Switch Gateway**.

   All configuration changes to the NSD are reverted to the original settings.
3. Click **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.

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

Diagnostic Bundles for Gateways

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

- Request Diagnostic Bundles for Gateways with New Orchestrator UI
- Request Packet Capture Bundle for Gateways

Request Diagnostic Bundles for Gateways with New Orchestrator UI

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

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.

Request Diagnostic Bundle

To generate a new Diagnostic bundle:

1. In the new UI, click 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, click **Request Diagnostic Bundle**.
3. In the **Request Diagnostic Bundle** dialog, configure the following details and click **Submit**.

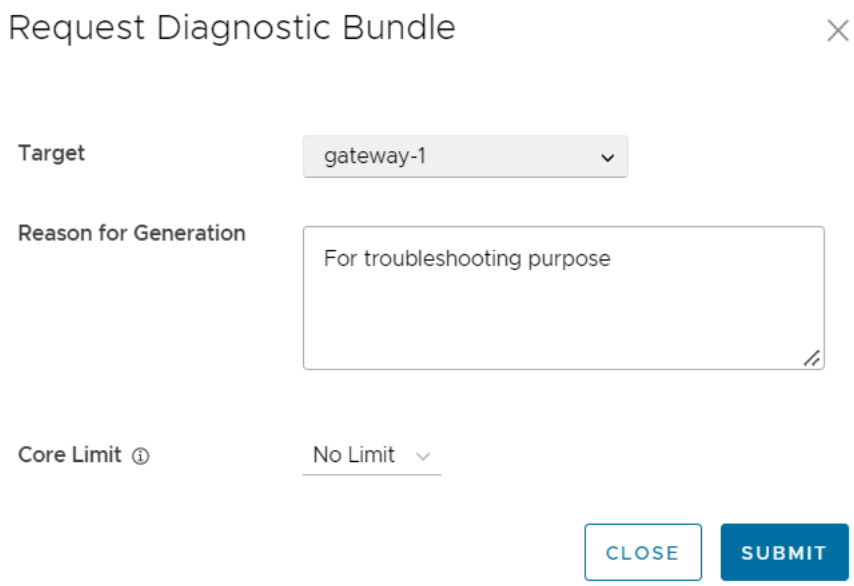


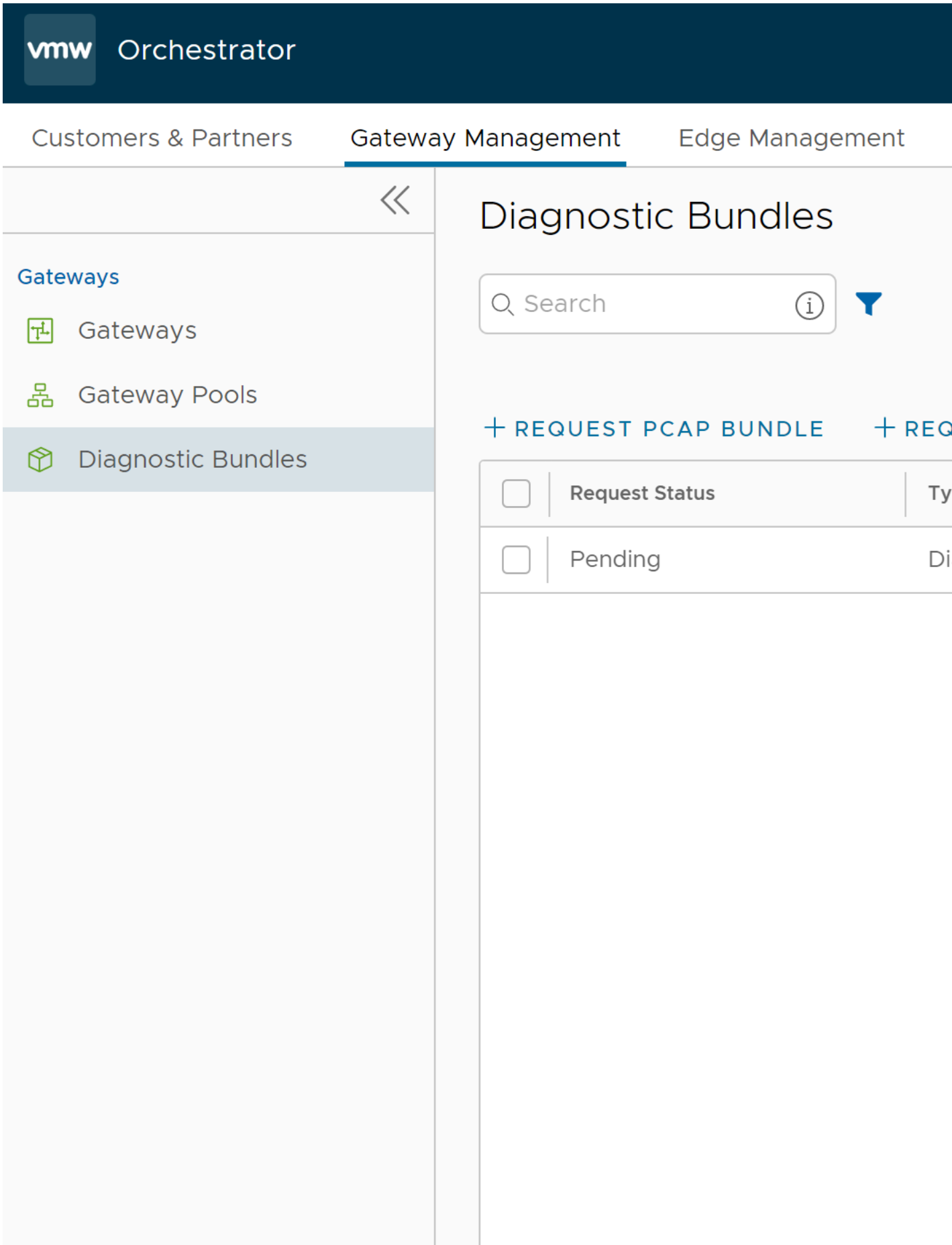
Table 1:

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.

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


vmw
Orchestrator
Customers & Partners
Gateway Management
Edge Management
Gateways
Gateways
Gateway Pools
Diagnostic Bundles
Diagnostic Bundles
Search
+ REQUEST PCAP BUNDLE
+ REQ
Request Status
Ty
Pending
Di

Download Diagnostic Bundle

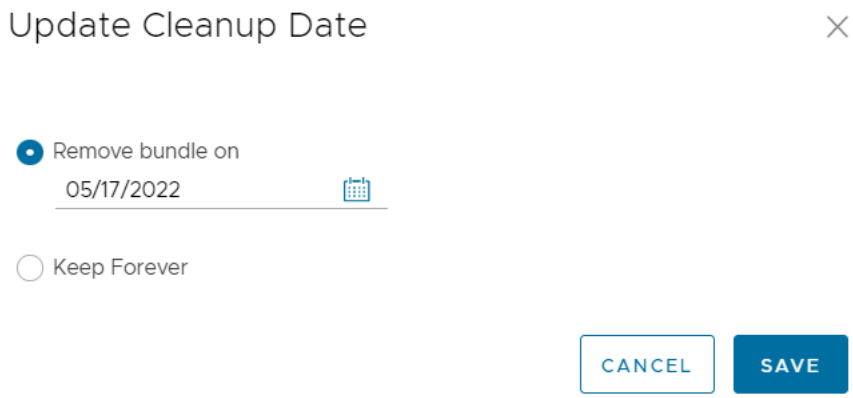
You can download the generated Diagnostic bundles to troubleshoot an Edge.

To download a generated bundle, click the link next to **Complete** in the **Request Status** column or select the bundle and click **Download Bundle**. The bundle is downloaded as a ZIP file.

You can send the downloaded bundle to a 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 click the link to the **Cleanup Date** or choose the bundle and click **More** > **Update Cleanup Date** to modify the Date.



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** checkbox, so that the Bundle does not get deleted automatically.

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

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.

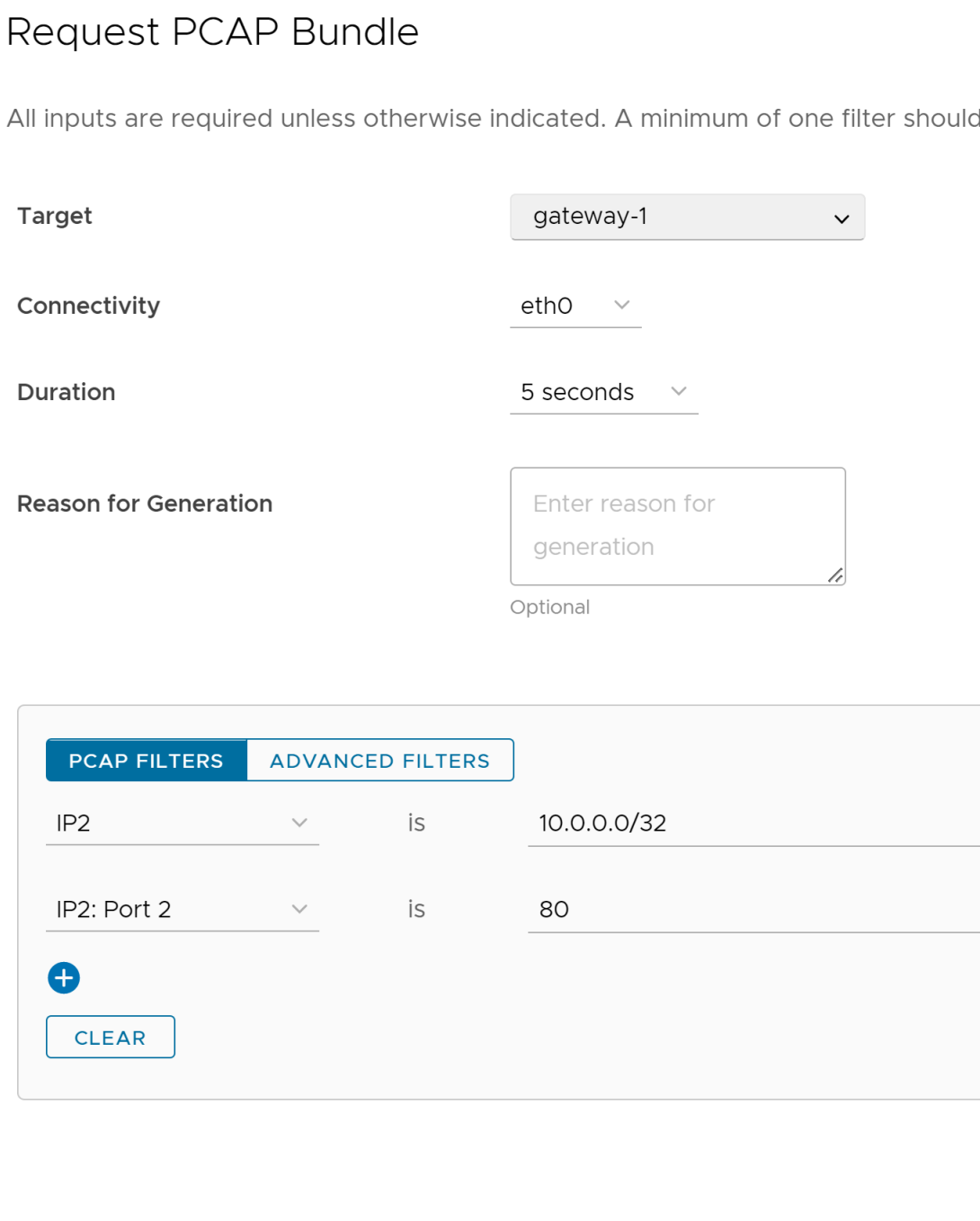
Partner Super user and Admin with Gateway management access activated can create, manage, and delete Packet Capture (PCAP) bundles only for Gateway created by a Partner or a Partner managed Gateway created by your Operator. The Partner IT support users can only view the generated PCAP bundles and download 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, click 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, click **Request PCAP Bundle**.
3. In the **Request PCAP Bundle** dialog, configure the following details and click **Generate**.



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.

Field	Description
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, click the link next to **Complete** in the **Request Status** column or select the bundle and click **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 click the link to the **Cleanup Date** or choose the bundle and click **More** > **Update Cleanup Date** to modify the Date.
6. To delete a bundle manually, select the bundle and click **Delete**.

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, 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

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 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 , and then go to **Edge Management** > **Edge Auto-activation**.
2. On the **Edge Auto-activation** page, enter the **PRM ID**.
3. Click **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.

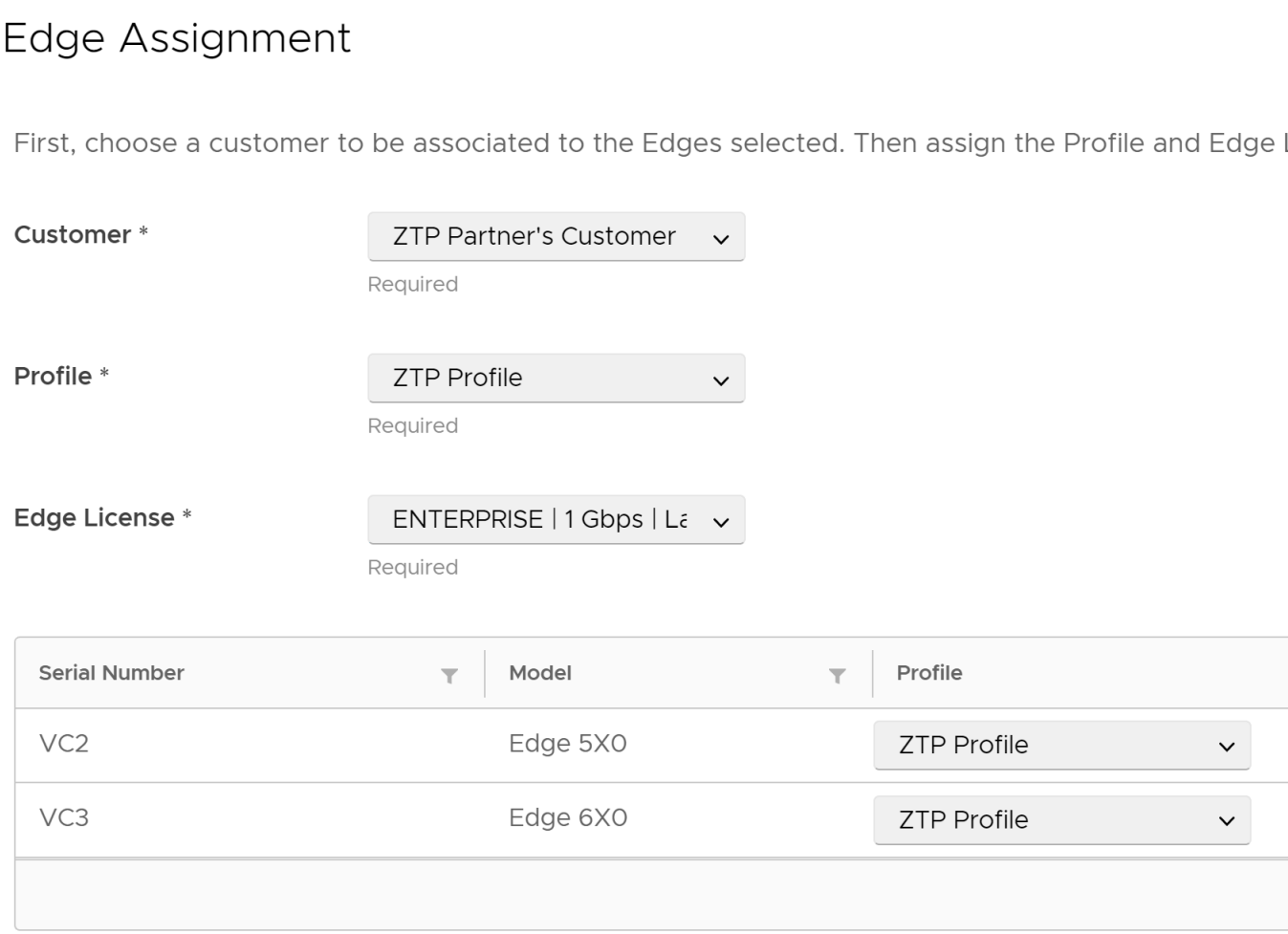
Only the Edges that were shipped to you after the successful completion of the sign-up process appear in the **Available Inventory** tab. Ensure that the PRM ID assigned to you is used in all your future orders so that the inventory is reflected correctly. You must assign the Edges to Customers, and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

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 , 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 click **Assign To Customer**. The **Edge Assignment** window appears.



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. Click **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:

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	Click to download the list of Edges in an excel format.

Option	Description
Columns	Click this option and select the checkboxes to view the required columns.
Refresh	Click 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 , where they are automatically activated. After an Edge is activated, the **Edge State** in the **Assigned Inventory** tab changes from **Pending** to **Activated**.

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*. 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, and then go to **Edge Management** > **Edge Auto-activation**. Click **Assigned Inventory** tab.
2. Select the Edge that you want to reassign, and then click **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. Click **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 click **Delete** to manually delete the entry.

Activate Using Email

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

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

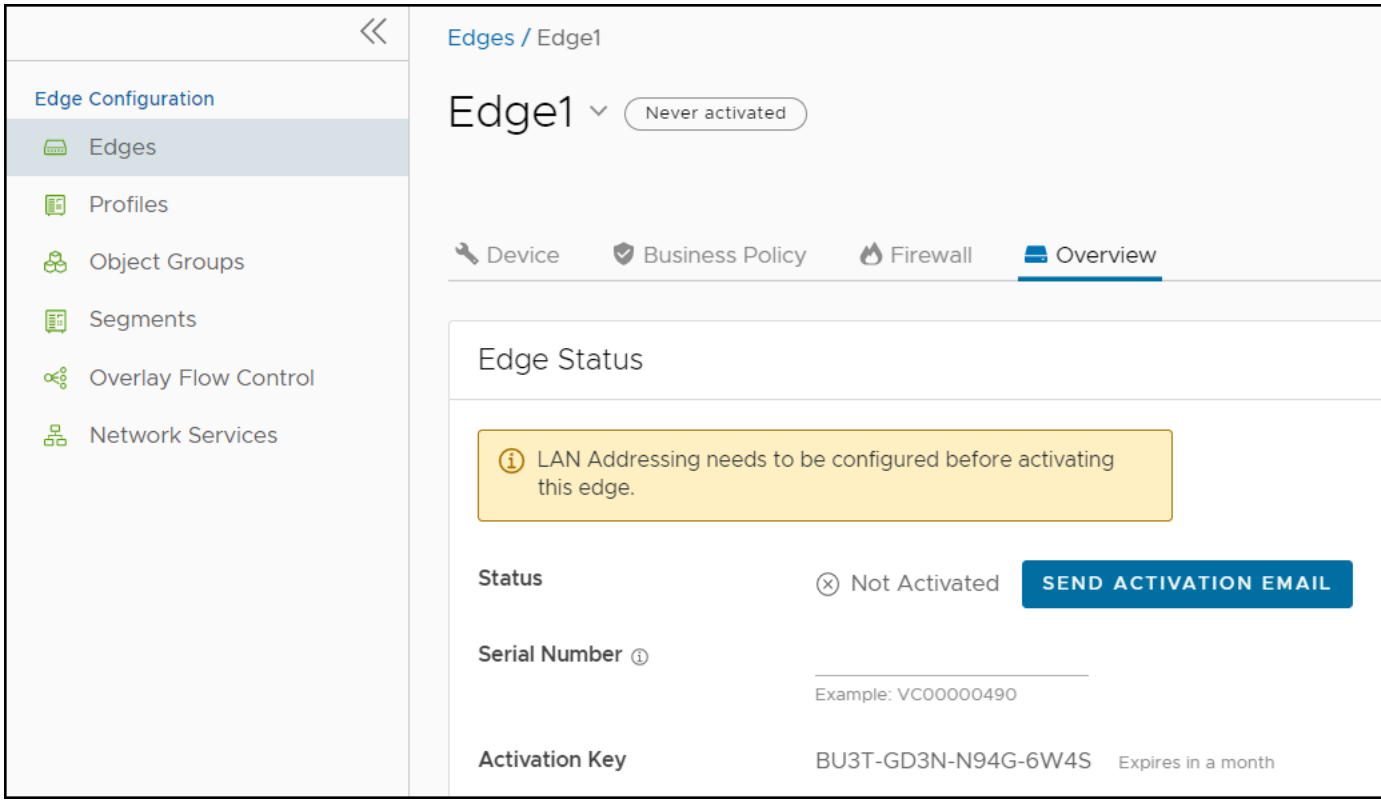
1. Send an Activation Email. The administrator initiates the activation process by sending an activation procedure email to the person that will install the Edge, typically a Site Contact. For more information, see Send Edge Activation Email.
2. Activate the Edge Device. The instructions in the activation procedure email activates the Edge device. For more information, refer to Activate an Edge Device.

Send Edge Activation Email

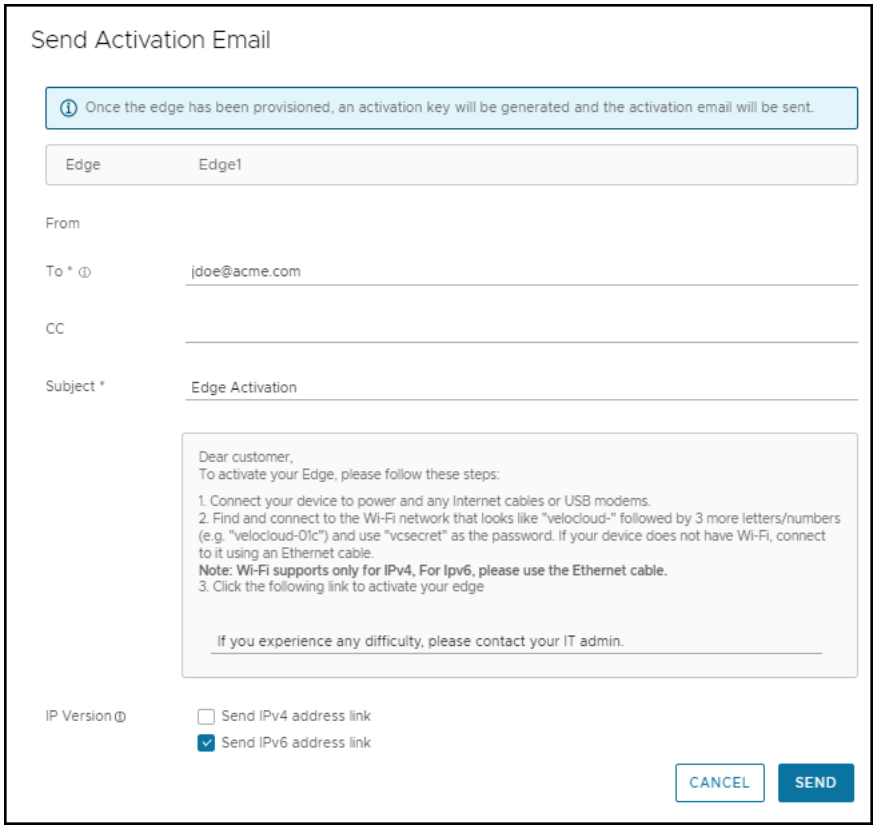
The administrator initiates the activation process of an Edge by sending an activation procedure Email to the person installing the Edge, typically a Site Contact.

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. Click the link to the Edge to be activated or click the **View** link in the **Device** column of the Edge.
4. Click the **Overview** tab. For an Edge that is not activated, the **Edge Status** section displays the option to send an activation Email:



5. Click **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. Click **Send** and the activation Email is sent to the Site contact.

Once the Site contact receives the activation Email, the person can activate the Edge. For more 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, 6x0, and 7x0 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 *Troubleshooting Guide* published at www.arista.com/en/support/product-documentation.

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 more 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. Click 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 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.

Edge Activation using an iOS Device and an Ethernet Cable

There are multiple ways to activate a 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:

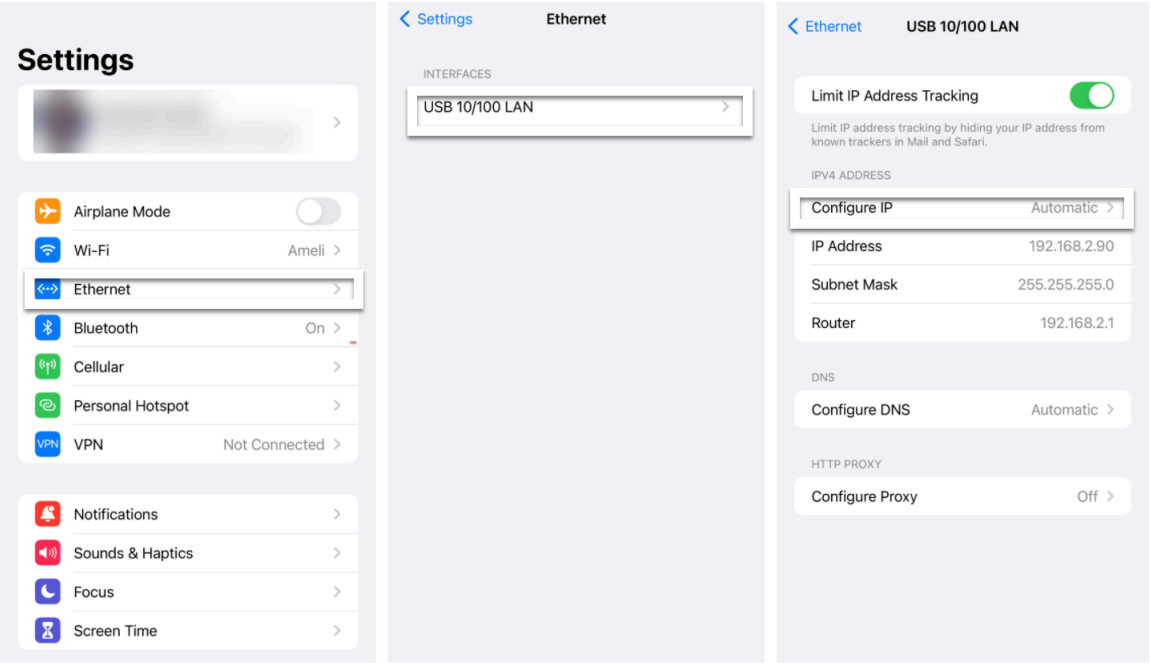
- iPhone/iPad with email access
- Ethernet adapter suitable for phone or tablet

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.

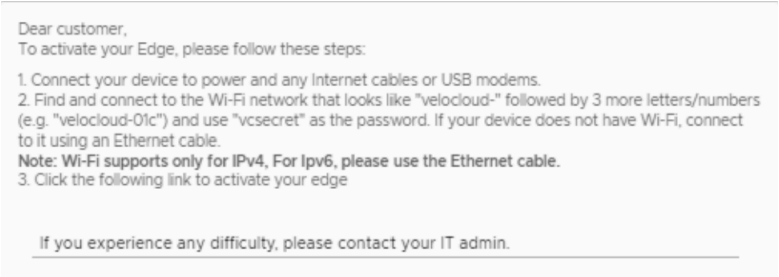
1. Complete the Edge configuration on the Orchestrator software. For details, refer to the *Configure Edge Device* section in the *Administration Guide*.
2. Navigate to **Configure** > **Edges** > **Edge Overview tab**, and then click the **Send Activation Email** button.
3. Enter the email address of the person activating the Edge, and then click **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**.



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



8. You can see the activation progress on your phone screen. Once complete, **Activation successful** message is displayed.

Your Edge device is now activated.

Edge Activation using an Android Device and an Ethernet Cable

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

The components required for this procedure are:

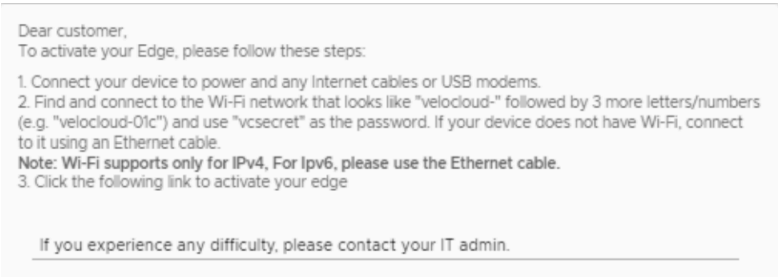
- Android phone with email access
- Ethernet adapter suitable for the phone

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 *Administration Guide*.
2. Navigate to **Configure** > **Edges** > **Edge Overview tab**, and then click the **Send Activation Email** button.
3. Enter the email address of the person activating the Edge, and then click **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 click the activation link displayed at the bottom of the screen to activate your Edge. The following screenshot is an example.



7. You can see the activation progress on your phone screen. Once complete, **Activation successful** message is displayed.

Your Edge device is now activated.

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

Request RMA Reactivation Using Edge Auto-activation

To request RMA reactivation using Zero Touch Provisioning:

1. Log in to , and in the **SD-WAN** service of the Enterprise portal go to **Configure > Edges**.
2. Click the Edge that you want to replace. The **Edge Overview** page appears.
3. Scroll down to the **RMA Reactivation** area, and then click **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, click **Generate New Activation Key**.
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. Click **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 where it is automatically activated. The status of the new Edge changes to **Activated**.

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

Request RMA Reactivation Using Email

To request RMA reactivation using email:

1. Log in to , and then go to **Configure > Edges**.
2. Click the Edge that you want to replace. The **Edge Overview** page appears.
3. Scroll down to the **RMA Reactivation** area, and then click **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, click **Generate New Activation Key**.
4. Click **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 .
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. Click the activation link in the email to activate the Edge.

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

Install Partner Gateway

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

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 .
- 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:

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`

Hypervisor Minimum Hardware Requirements

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

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. The CPU must support and enable the following instruction sets: AES-NI, SSSE3, SSE4, RDTSC, RDSEED, RDRAND, AVX/AVX2/AVX512.
- Minimum of 36GB RAM (One gateway VM requires 32GB RAM)
- Minimum of 150GB magnetic or SSD based, persistent disk volume (One gateway VM requires 96GB)
- Minimum 1x10Ge network interface ports and 2 is preferred when enabling 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.
- 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

Examples of 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

Required NIC Specifications for SR-IOV support

Hardware Manufacturer	Firmware Version	Host Driver for Ubuntu 18.04	Host Driver for ESXi 6.7
Dual Port Intel Corporation Ethernet Controller XL710 for 40GbE QSFP+	7.0	2.10.19.30	1.8.6 and 1.10.9.0
Dual Port Intel Corporation Ethernet Controller X710 for 10GbE SFP+	7.0	2.10.19.30	1.8.6 and 1.10.9.0

Hardware Manufacturer	Firmware Version	Host Driver for Ubuntu 18.04	Host Driver for ESXi 6.7
Quad Port Intel Corporation Ethernet Controller X710 for 10GbE SFP+	7.0	2.10.19.30	1.8.6 and 1.10.9.0
Dell rNDC X710/350 card	nvm 7.10 and FW 19.0.12	2.10.19.30	1.8.6 and 1.10.9.0

Supported Hypervisor Versions

Hypervisor	Supported Versions
Arista	• Intel 82599/82599ES - ESXi 6.7 U3 up to ESXi 7.0. To use SR-IOV, the vCenter and the vSphere Enterprise Plus license are required. • Intel X710/XL710 - ESXi 6.7 with Arista vSphere Web Client 6.7.0 up to ESXi 7.0 with Arista vSphere Web Client 7.0
KVM	• Intel 82599/82599ES - Ubuntu 16.04 LTS and Ubuntu 18.04 LTS • Intel X710/XL710 - Ubuntu 16.04 LTS and Ubuntu 18.04 LTS

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 Arista ESXi:
  - Latency Sensitivity must be set to 'High'.
  - vNIC must be of 'vmxnet3' type (or SR-IOV, see SR-IIOV 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.
  - 32 GB of memory
  - 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).
  - 96 GB of virtual disk.
- If using KVM:
  - vNIC must be of 'Linux Bridge' type. (SR-IOV is required for high performance, see SR-IIOV 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.

- 32 GB of memory
- 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).
- 96 GB of virtual disk.

Firewall/NAT Requirements

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

- The firewall needs to allow outbound traffic from the to TCP/443 (for communication with).
- 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

To improve packet throughput performance, 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 more 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.

Installation Procedures

This section describes the installation procedures.

In general, installing the involves the following steps:

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

Important:

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

Pre-Installation Considerations

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

Worksheet

	• Version • OVA/QCOW2 file location • Activation Key • (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

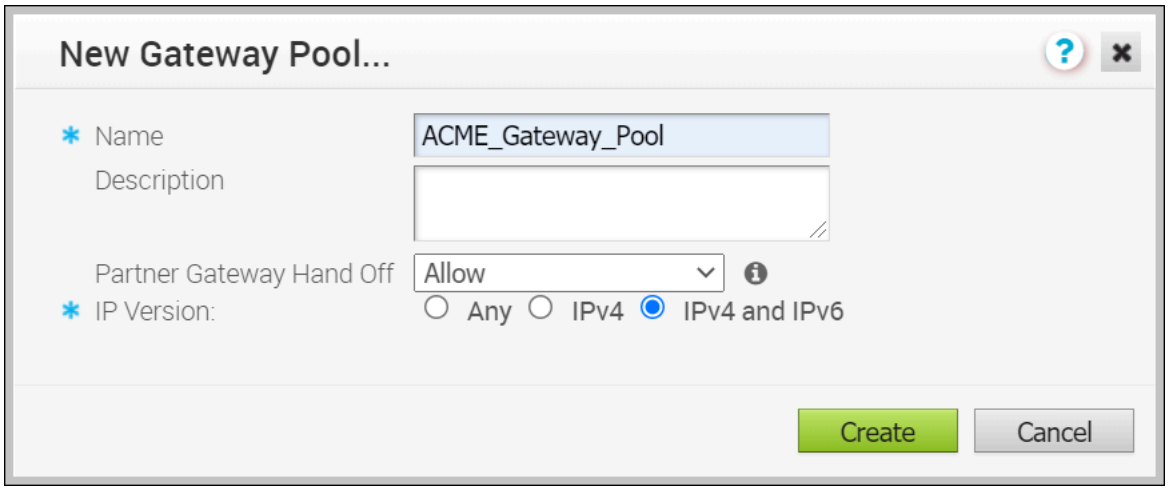
Section

Most of the section is self-explanatory.

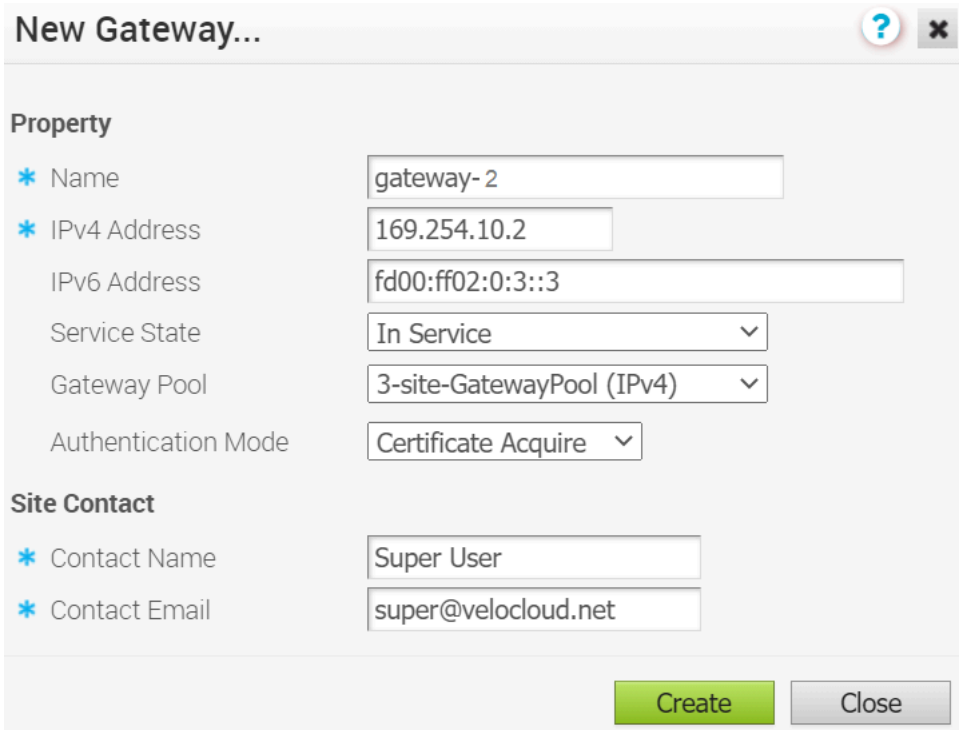
	• Version - Should be same or lower than • OVA/QCOW2 file location - Plan ahead the file location and disk allocation • Activation Key • (IP ADDRESS/vco-fqdn-hostname) • Hostname - Valid Linux Hostname “RFC 1123”

Creating a Gateway and Getting the Activation Key

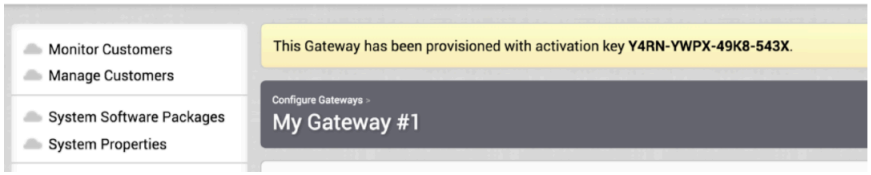
1. Go to **Operator > Gateway Pool** and create a new pool. For running in the Service Provider network, check the **Allow Partner Gateway** checkbox. This will enable the option to include the partner gateway in this gateway pool.



2. Go to **Operator > Gateway** 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 which will return the public IP of the .

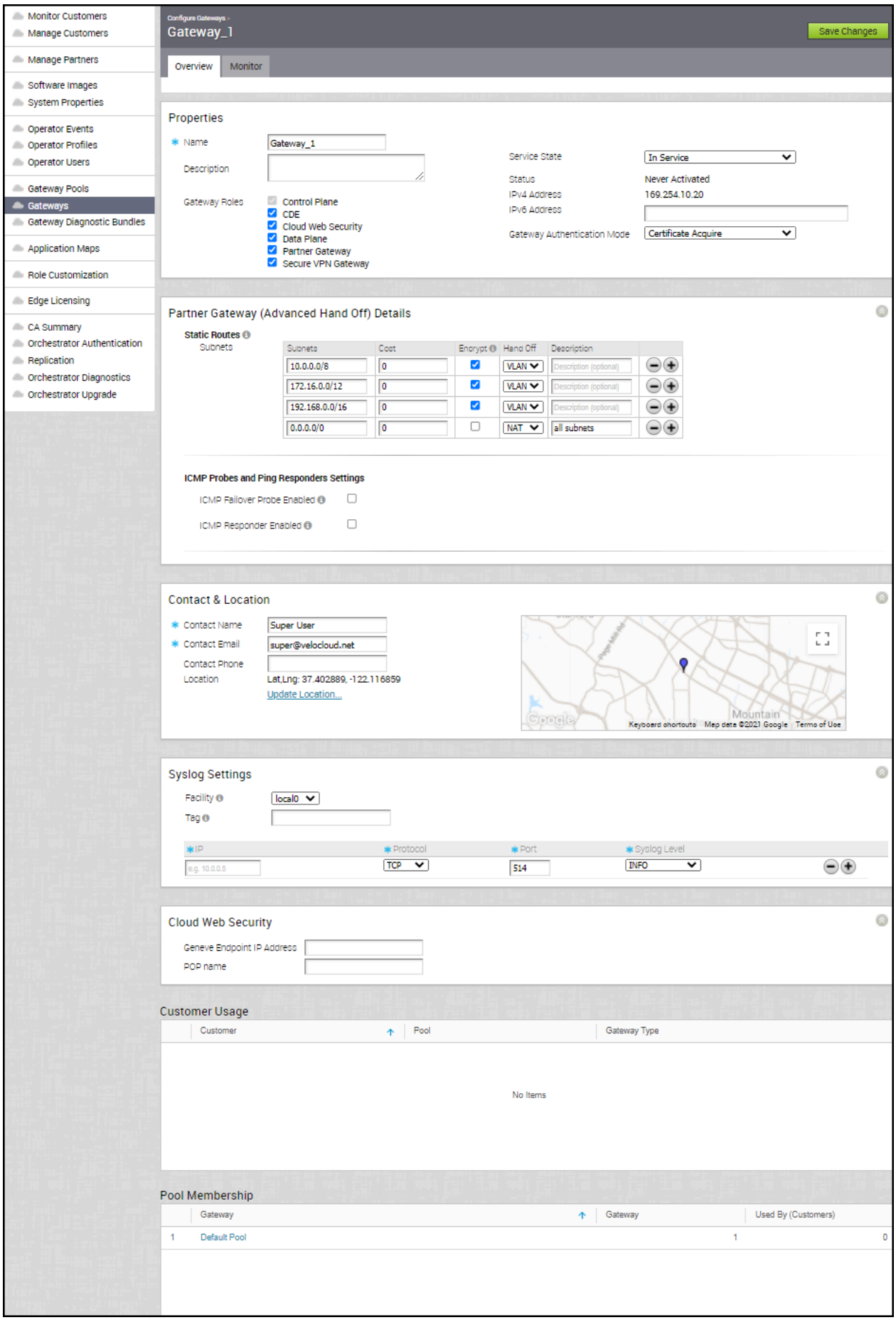


3. Make a note of the activation key and add it to the worksheet.



Enable Partner Gateway Mode

1. Go to **Operator > Gateways** and select the . Check the **Partner Gateway** checkbox to enable the Partner Gateway.


Monitor Customers
Manage Customers
Manage Partners
Software Images
System Properties
Operator Events
Operator Profiles
Operator Users
Gateway Pools
Gateways
Gateway Diagnostic Bundles
Application Maps
Role Customization
Edge Licensing
CA Summary
Orchestrator Authentication
Replication
Orchestrator Diagnostics
Orchestrator Upgrade
Configure Gateways
Gateway_1
Save Changes
Overview
Monitor
Properties
Name
Gateway_1
Description
Gateway Roles
Control Plane
CDE
Cloud Web Security
Data Plane
Partner Gateway
Secure VPN Gateway
Service State
In Service
Status
Never Activated
IPv4 Address
169.254.10.20
IPv6 Address
Gateway Authentication Mode
Certificate Acquire
Partner Gateway (Advanced Hand Off) Details
Static Routes
Subnets
Subnets
Cost
Encrypt
Hand Off
Description
10.0.0.0/8
172.16.0.0/12
192.168.0.0/16
0.0.0.0/0
VLAN
NAT
all subnets
ICMP Probes and Ping Responders Settings
ICMP Failover Probe Enabled
ICMP Responder Enabled
Contact & Location
Contact Name
Super User
Contact Email
super@velocloud.net
Contact Phone
Location
Lat,Lng: 37.402889, -122.116859
Update Location...
Google
Mountain
Keyboard shortcuts
Map data ©2021 Google
Terms of Use
Syslog Settings
Facility
local0
Tag
IP
Protocol
Port
Syslog Level
TCP
514
INFO
Cloud Web Security
Geneve Endpoint IP Address
POP name
Customer Usage
Customer
Pool
Gateway Type
No Items
Pool Membership
Gateway
Gateway
Used By (Customers)
1
Default Pool
1
0

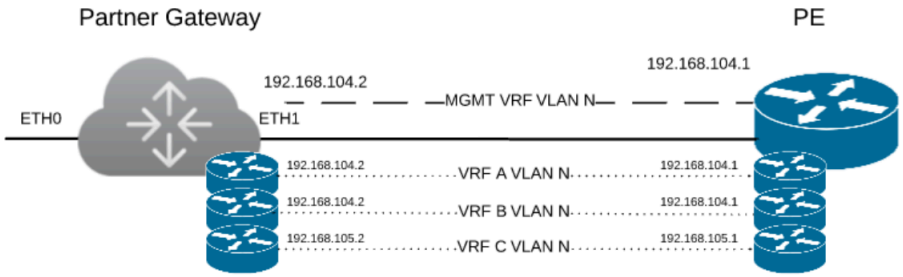
There are additional parameters that can be configured. The most common are the following:

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

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

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.



The diagram above is a representation of the 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 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 to check for status (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.

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.

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

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 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 more 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 SD-WAN 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 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-config
```

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.

Install

You can install on Arista and KVM.

KVM provides multiple ways to provide networking to virtual machines. 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 :

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

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 to work with the.

- 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.

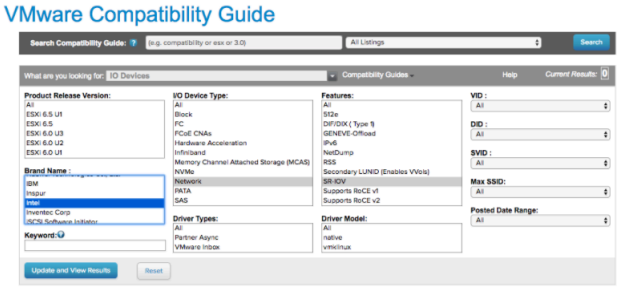
To enable SR-IOV on Arista:

1. Make sure that your NIC card supports SR-IOV. Check the Arista Hardware Compatibility List (HCL) at https://www.vmware.com/resources/compatibility/search.php?deviceCategory=io

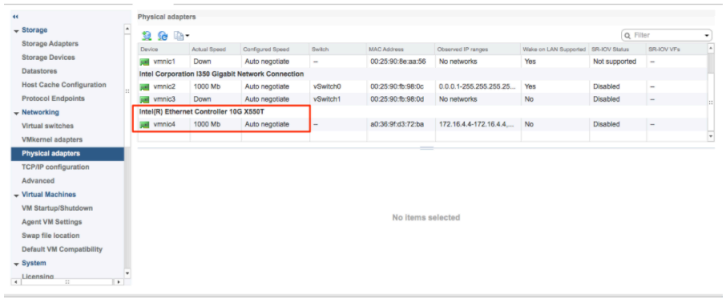
   Brand Name: Intel

   I/O Device Type: Network

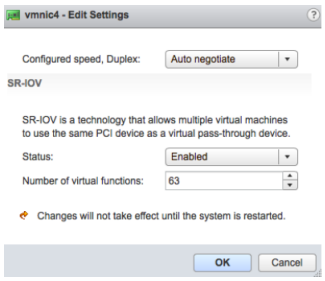
   Features: SR-IOV

   The following Arista KB article provides details of how to enable SR-IOV on the supported NIC: www.arista.com/en/support/product-documentation. .
2. Once you have a support NIC card, go to the specific Arista host, select the **Configure** tab, and then choose **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.



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

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 more information, see *VLAN Configuration*.

Install on Arista

Describes how to install the OVA on Arista.

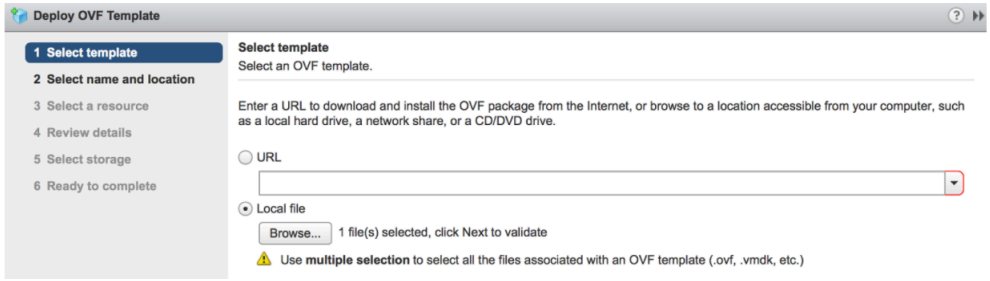
Note: This deployment is tested on ESXi versions 6.7, 6.7U3, 7.0, 7.0U3 and 8.0.1.

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 VM. Otherwise, you will need to re-deploy the VM again.

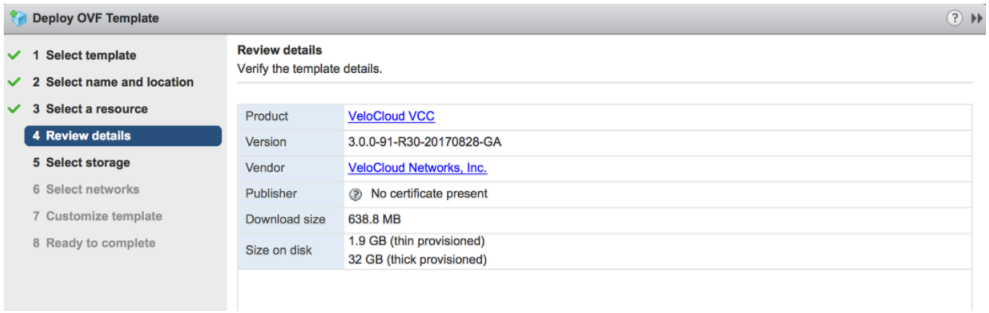
If you decide to use SR-IOV mode, then you can optionally enable SR-IOV on Arista. To enable the SR-IOV on Arista, see Enable SR-IOV on Arista

To install the OVA on Arista:

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

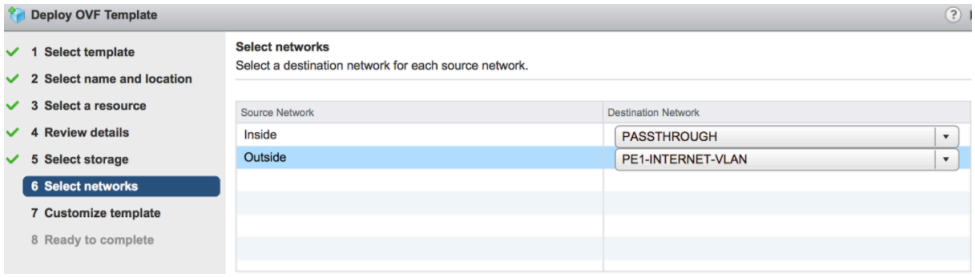


Review the template details in Step 4 (**Review details**) of the **Deploy OVA/OVF Template** wizard as shown in the image below.

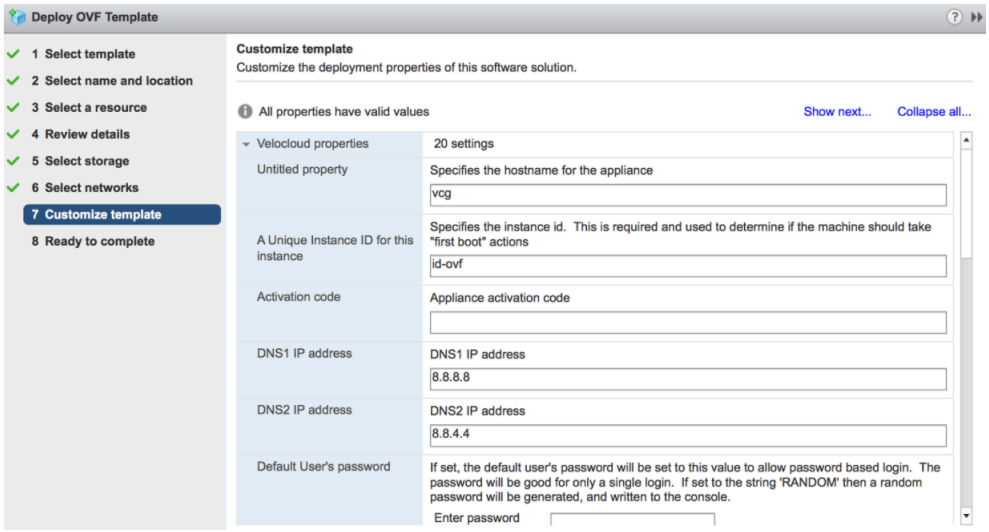


2. For the **Select networks** step, the OVA comes with two pre-defined networks (vNICs).

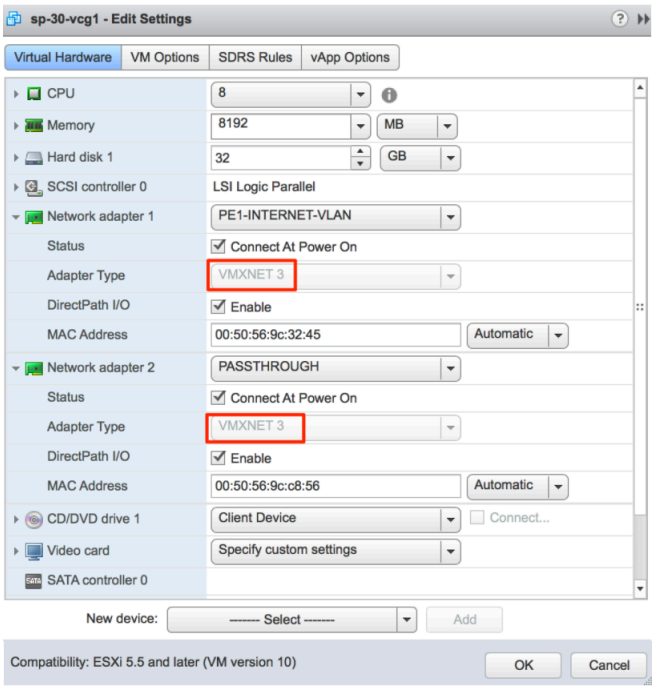
vNIC	Description
Inside	This is the vNIC facing the PE router and is used for handoff traffic to the MPLS PE or L3 switch. This vNIC is normally bound to a port group that does a VLAN pass-through (VLAN=4095 in vswitch configuration).
Outside	This is the vNIC facing the Internet. This vNIC expects a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



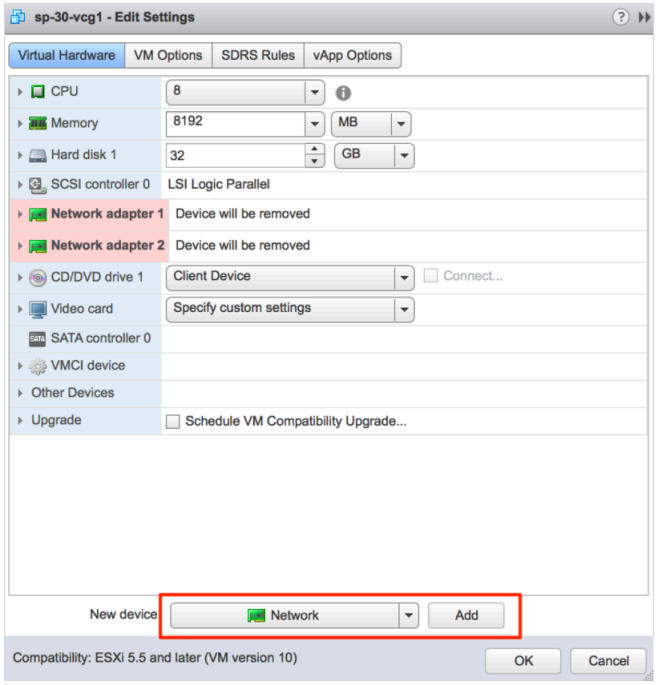
3. For the Customize template step, do not change anything. This is when you use vApp to configure the VM. We will not use vApp in this example. Click **Next** to continue with deploying the OVA.



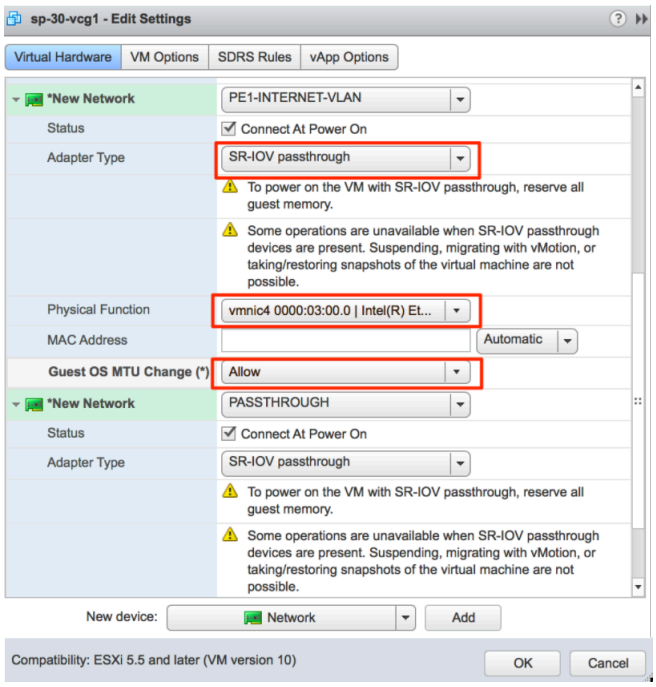
4. Once the VM is successfully deployed, return to the VM and click **Edit Settings** . Two vNICs are created with adapter type = vmxnet3.



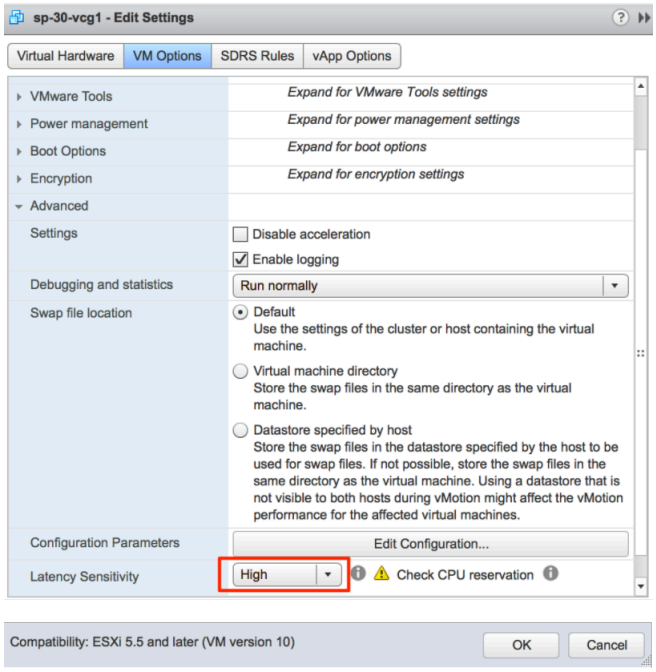
5. (Optional for SR-IOV) This step is required only if you plan to use SR-IOV. Because the OVA by default creates the two vNICs as vmxnet3, we will need to remove the two vNICs and re-add them as SR-IOV.



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, click **OK**.

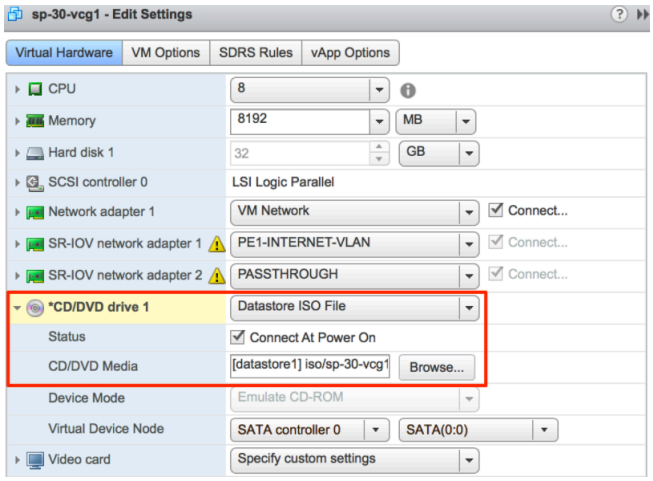


6. As is a real-time application, you need to configure the **Latency Sensitivity** to **High**. For more information about how to configure the VM for real-time application, see https://www.arista.com/en/support/product-documentation
.



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.



8. Start the VM.

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 to work with the and .

- 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.

Note: 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:

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=/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] 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@intel.com>
 srcversion: BA7E024DFE57A92C4F1DC93
```

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

     a. Download and install **i40e** driver from the Intel website.

b. Create the Virtual Functions (VFs).

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

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

d. Deactivate the VF driver.

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

e. 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)
```

Install on KVM

Describes how to install the qcow on KVM.

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, recommends the following modes:

- SR-IOV (This mode is required for the to deliver the maximum throughput specified by)
- 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.

Installation Steps on KVM

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="publicinterface" />
   <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>
```

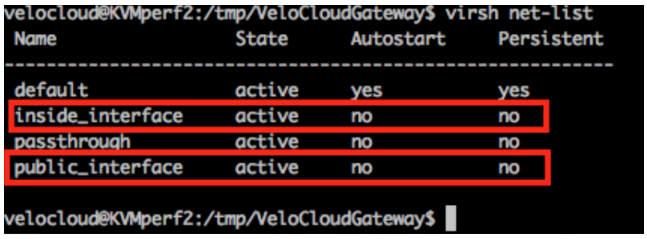
Create a network for `inside_interface`:

```
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.



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>restart</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_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="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 />
```

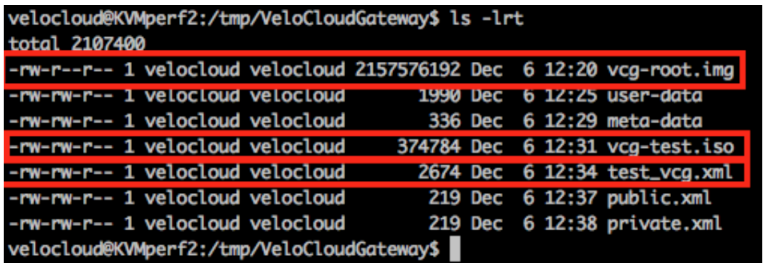
```
  </features>
  <cpu mode="host-passthrough" />
  <clock offset="utc" />
  <on_poweroff>destroy</on_poweroff>
  <on_reboot>restart</on_reboot>
  <on_crash>restart</on_crash>
  <devices>
     <emulator>/usr/bin/kvm-spice</emulator>
     <disk type="file" device="disk">
        <driver name="qemu" 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='0x0000' 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.)



   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).

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

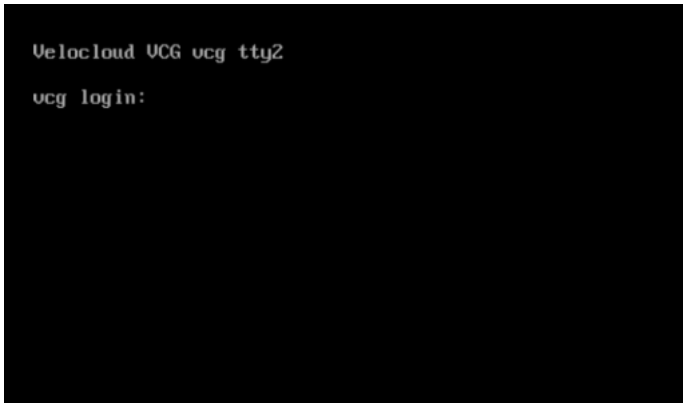
- Deactivate CPU C-states (power states affect real-time performance). Typically, this can be done as part of kernel boot options by appending `processor.max_cstate=1` or just deactivate in the BIOS.
- For production deployment, vCPUs must be pinned to the instance. No oversubscription on the cores should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

Post-Installation Tasks

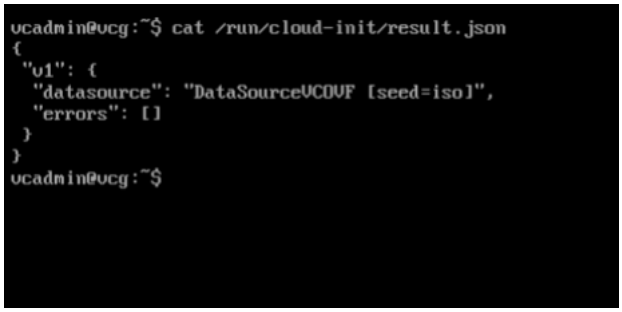
This section describes post-installation and installation verification steps.

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.

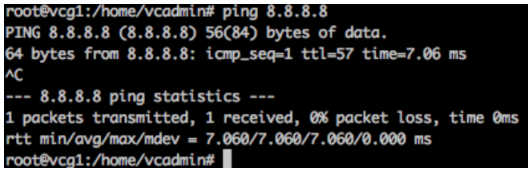


2. You can also refer to `/run/cloud-init/result.json`. If you see the message below, it is likely that the cloud init runs successfully.



3. Verify that the is registered with .

4. Verify Outside Connectivity.



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

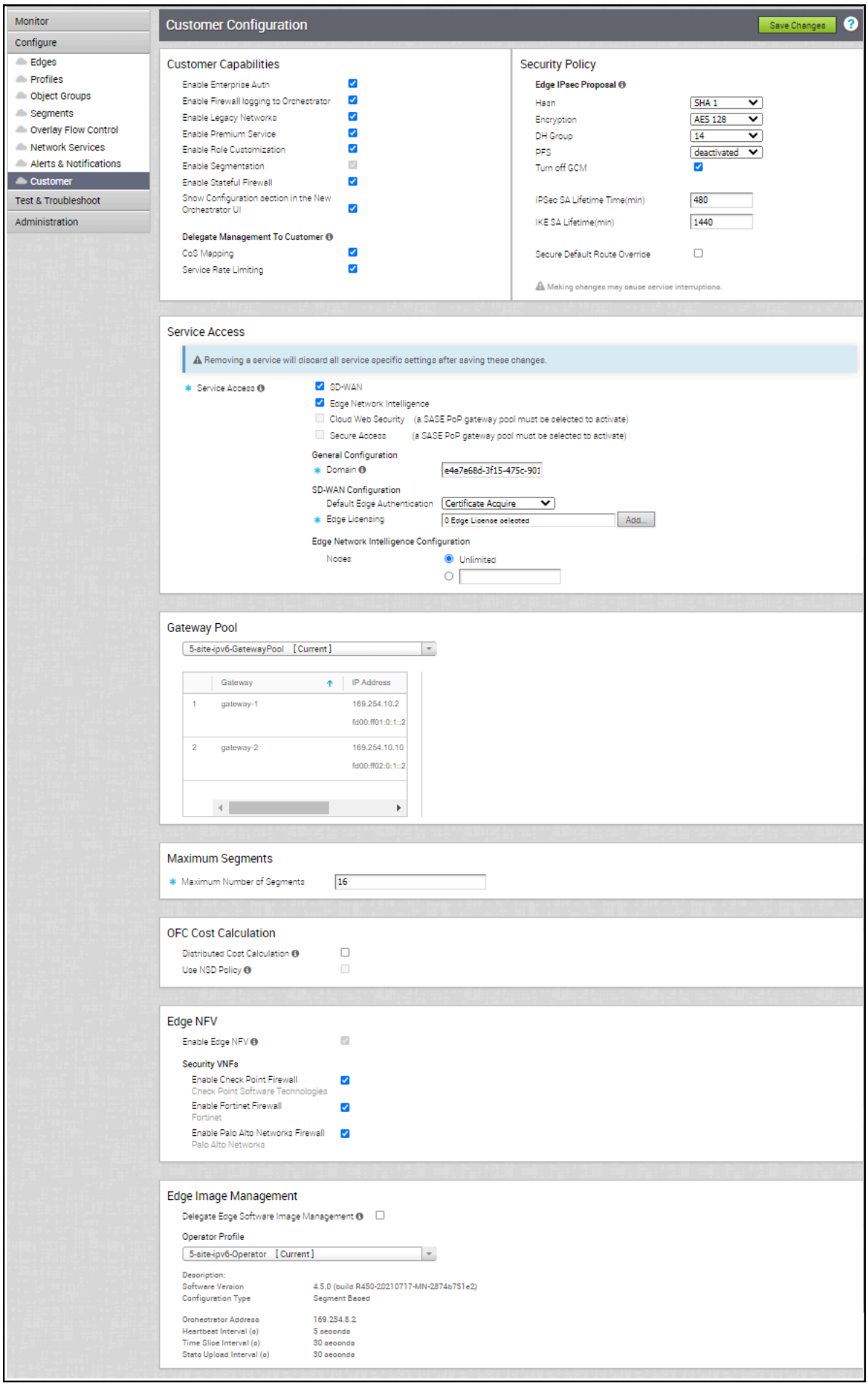
```
ubuntu@ubuntu:~$ sudo /opt/vc/bin/tcpdump.sh -i eth1
tcpdump: WARNING: tcpdump: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on tcpdump, link-type EN10MB (Ethernet), capture size 65535 bytes
08:35:50.013411 ARP, Request who-has 27.0.0.2 tell 27.0.0.1, length 28
08:35:50.013420 ARP, Reply 27.0.0.2 is-at 54:7f:ee:da:c4:7c (oui Unknown), length 42
08:35:55.013411 ARP, Request who-has 27.0.0.2 tell 27.0.0.1, length 28
08:35:55.013420 ARP, Reply 27.0.0.2 is-at 54:7f:ee:da:c4:7c (oui Unknown), length 42
^C
4 packets captured
4 packets received by filter
0 packets dropped by kernel
```

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

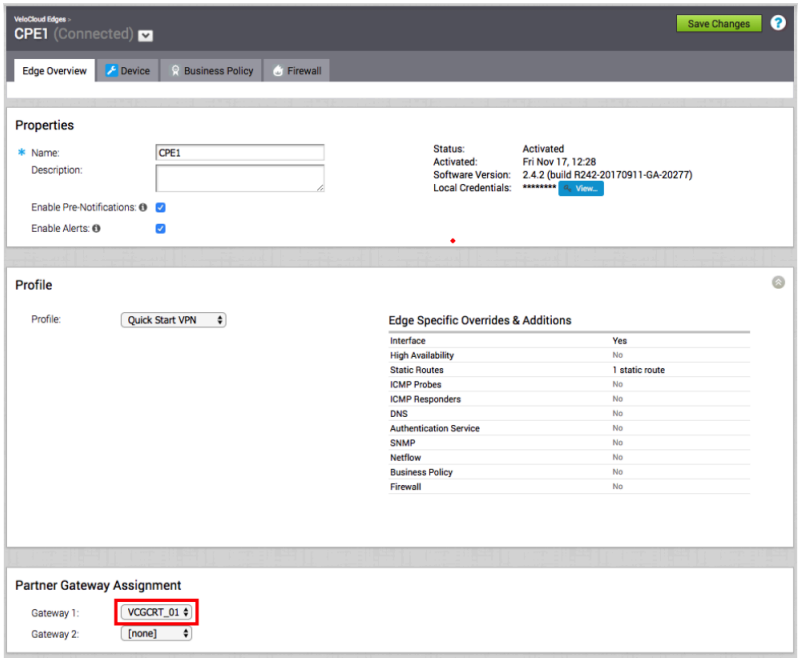
Note: If you have deployed OVA on vSphere with vAPP properties, you must deactivate cloud-init prior to upgrading to versions 4.0.1 or 4.1.0. This is to ensure that the customization settings such as network configuration or password are not lost during the upgrade.

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

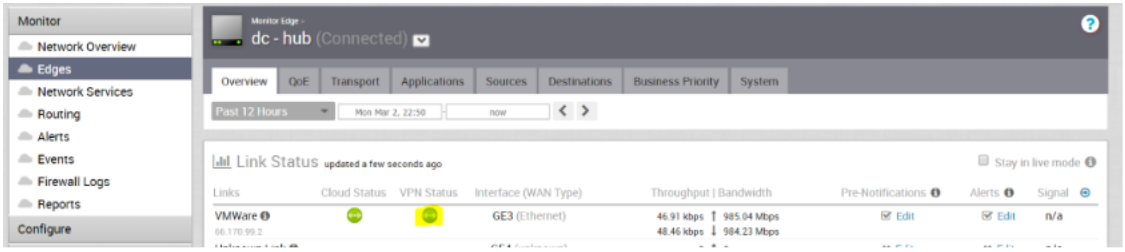
7. Associate the new gateway pool with the customer.


Monitor
Configure
Edges
Profiles
Object Groups
Segments
Overlay Flow Control
Network Services
Alerts & Notifications
Customer
Test & Troubleshoot
Administration
Customer Configuration
Save Changes
Customer Capabilities
Enable Enterprise Auth
Enable Firewall logging to Orchestrator
Enable Legacy Networks
Enable Premium Service
Enable Role Customization
Enable Segmentation
Enable Stateful Firewall
Show Configuration section in the New Orchestrator UI
Delegate Management To Customer
CoS Mapping
Service Rate Limiting
Security Policy
Edge IPsec Proposal
Hash
SHA 1
Encryption
AES 128
DH Group
14
PFS
deactivated
Turn off GCM
IPSec SA Lifetime Time(min)
480
IKE SA Lifetime(min)
1440
Secure Default Route Override
Making changes may cause service interruptions.
Service Access
Removing a service will discard all service specific settings after saving these changes.
Service Access
SD-WAN
Edge Network Intelligence
Cloud Web Security (a SASE PoP gateway pool must be selected to activate)
Secure Access (a SASE PoP gateway pool must be selected to activate)
General Configuration
Domain
e4e7e68d-3f15-475c-901
SD-WAN Configuration
Default Edge Authentication
Certificate Acquire
Edge Licensing
0 Edge License selected
Add...
Edge Network Intelligence Configuration
Nodes
Unlimited
Gateway Pool
5-site-ipv6-GatewayPool [Current]
Gateway
IP Address
1
gateway-1
169.254.10.2
fd00:ff01:0:1::2
2
gateway-2
169.254.10.10
fd00:ff02:0:1::2
Maximum Segments
Maximum Number of Segments
16
OFC Cost Calculation
Distributed Cost Calculation
Use NSD Policy
Edge NFV
Enable Edge NFV
Security VNFs
Enable Check Point Firewall
Check Point Software Technologies
Enable Fortinet Firewall
Fortinet
Enable Palo Alto Networks Firewall
Palo Alto Networks
Edge Image Management
Delegate Edge Software Image Management
Operator Profile
5-site-ipv6-Operator [Current]
Description:
Software Version
4.5.0 (build R450-20210717-MN-2874b751e2)
Configuration Type
Segment Based
Orchestrator Address
169.254.8.2
Heartbeat Interval (s)
5 seconds
Time Slice Interval (s)
30 seconds
Stats Upload Interval (s)
30 seconds

8. Associate the Gateway with an Edge.

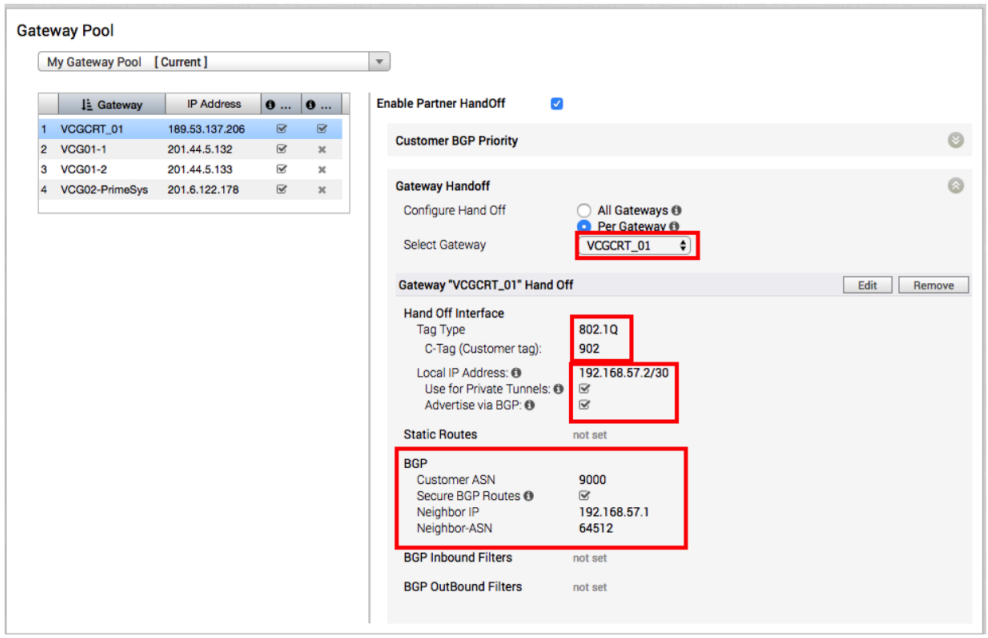


9. Verify that the Edge is able to establish a tunnel with the Gateway on the Internet side. From the Arista SD-WAN Orchestrator, go to **Monitor** > **Edges** > **Overview**.



From the Arista SD-WAN Orchestrator, go to **Test & Troubleshoot** > **Remote Diagnostics** > **[Edge]** > **List Paths**, and click **Run** to view the list of active paths.

10. Configure the Handoff interface.



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: []
```

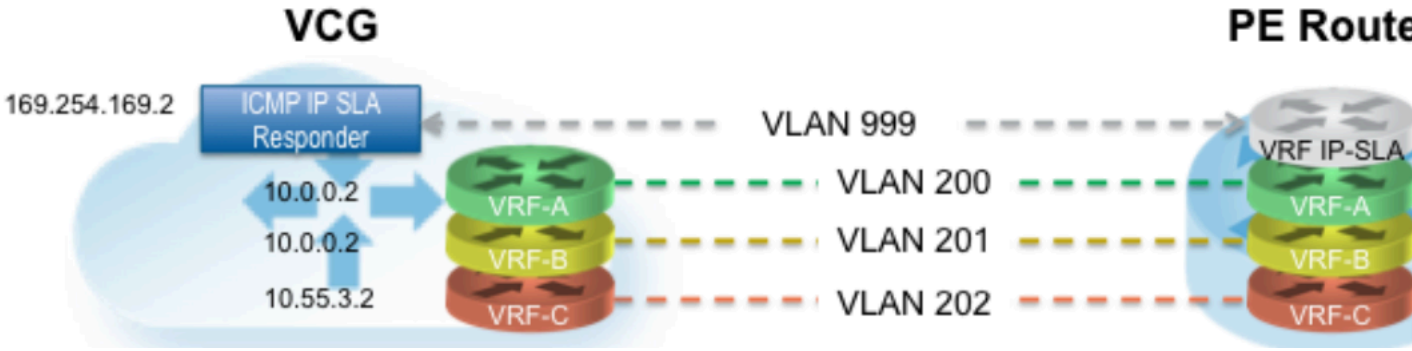
Important: when cloud-init is enabled, network configuration is regenerated on every boot. In order to make changes to location configuration, deactivate cloud-init or deactivate cloud-init network configuration component:

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

Configure Handoff Interface in Dataplane

Arista SD-WAN 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.



A management VRFis 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.

Step 1: Edit the /etc/config/gatewaydand 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.

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

            "wan": [
                "eth1"
            ],
```

Step 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 VRFparameter 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.

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
             }
          ]
      },
```

Step 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.
```

Step 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"
            }
]
```

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

```
[
]
```

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

Upgrade

This section describes how to upgrade a 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. Please refer to Partner Gateway Upgrade and Migration 3.4 to 4.0 for upgrade information.

Note: Currently, does not support downgrading for the and . So before upgrading the or , 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 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 installation:

1. Download the update package.
2. Upload the image to the 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 console and run:

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

Activate Replacement Partner Gateway

This section covers activating a replacement Partner Gateway.

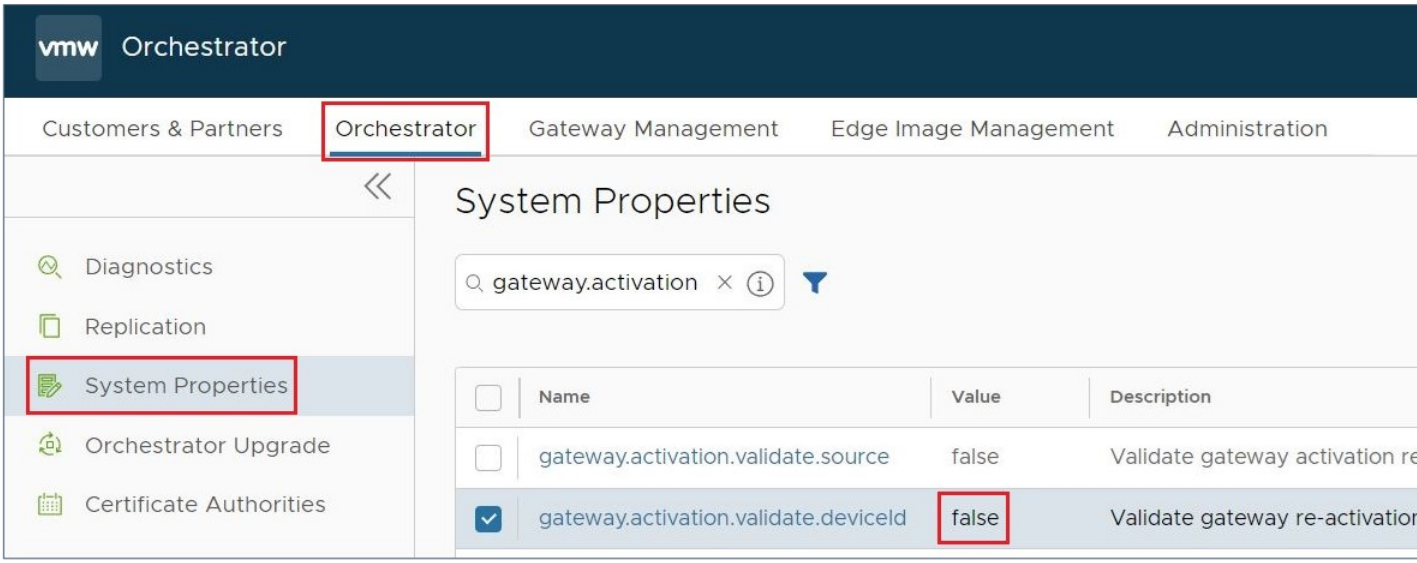
Overview

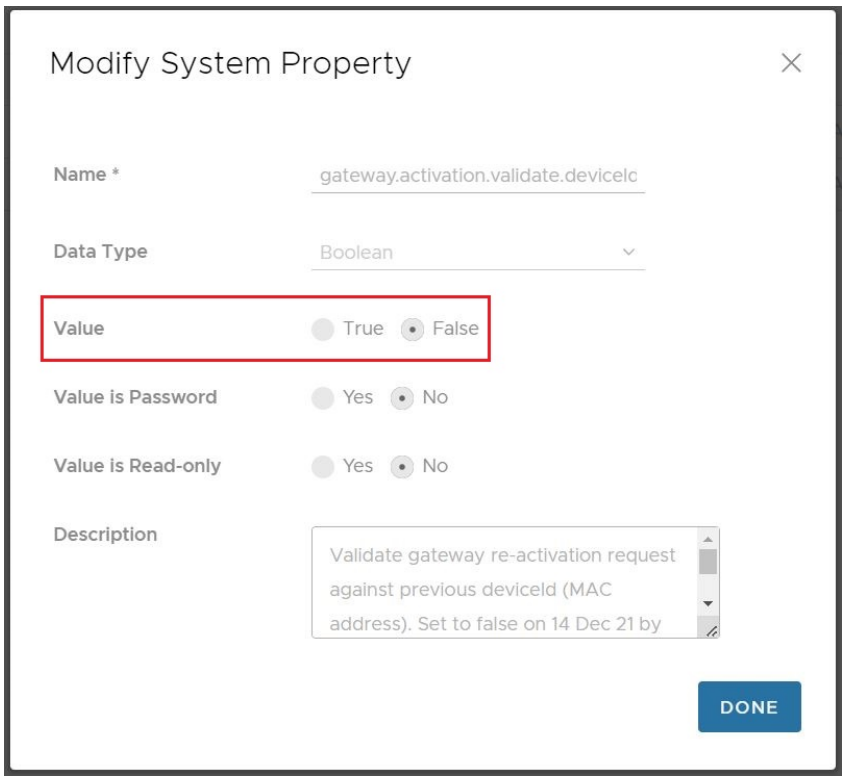
Gateway activation keys do not have the same default 30 day lifetime as Edges. In fact, a Gateway activation key has an infinite lifespan. If an on-premises Gateway fails and you wish to replace it with a newly built Gateway using the same name and IP address, you can use the same activation key that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

Prerequisites

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 clicking on it.





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.

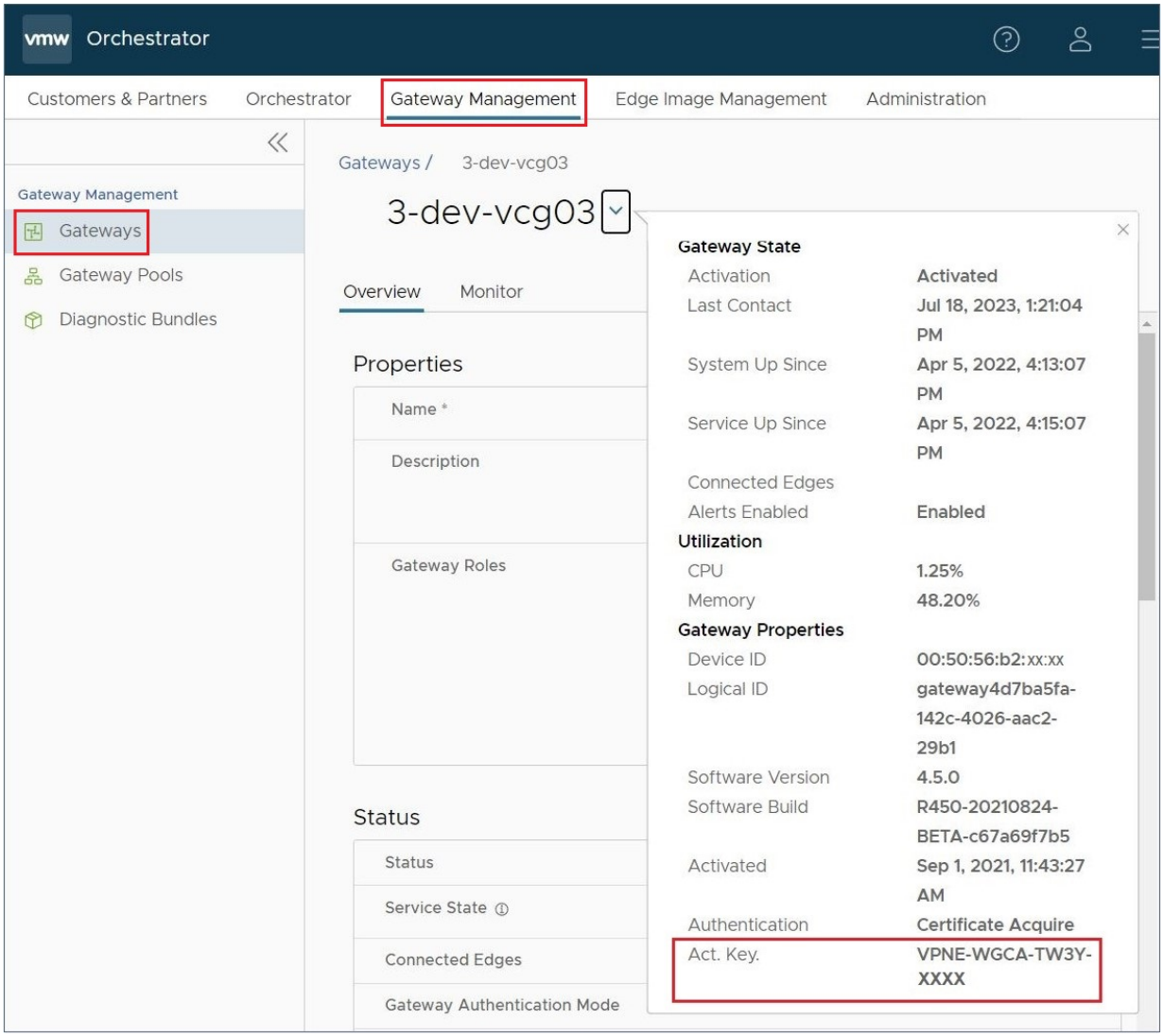
Note: There are no adverse effects to changing this value. You may leave it as **false** since the Gateway authentication keys are indefinitely valid.

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 toArista VeloCloud SD-WAN Support and they will assist you in changing that System Property on your Orchestrator.

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 clicking on the name of the Gateway you are replacing. Click the down arrow beside the name and note the activation key.



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**.

Custom Configurations

This section describes custom configurations.

NTP Configuration

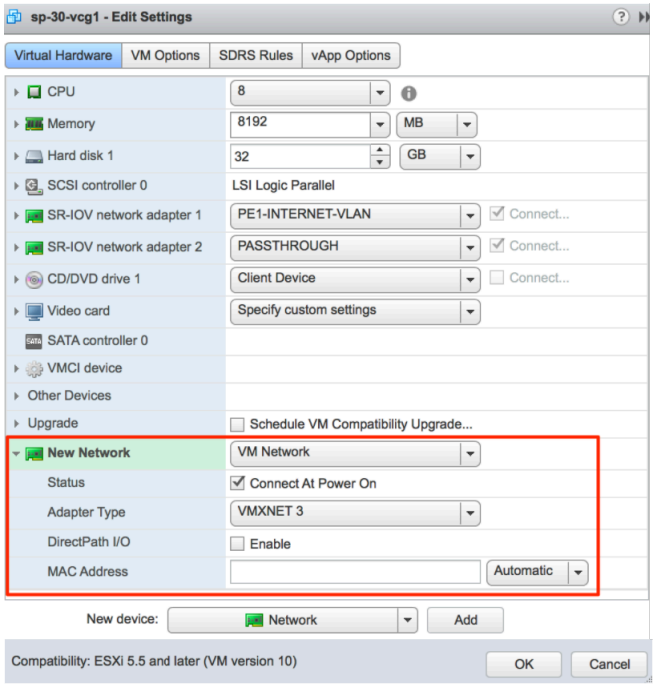
NTP configuration involves editing the `/etc/ntpd.conf` file.

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 click **OK** and then **Edit Settings** again so you can make a note of the vNIC MAC address.



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='0x0000' 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:
```

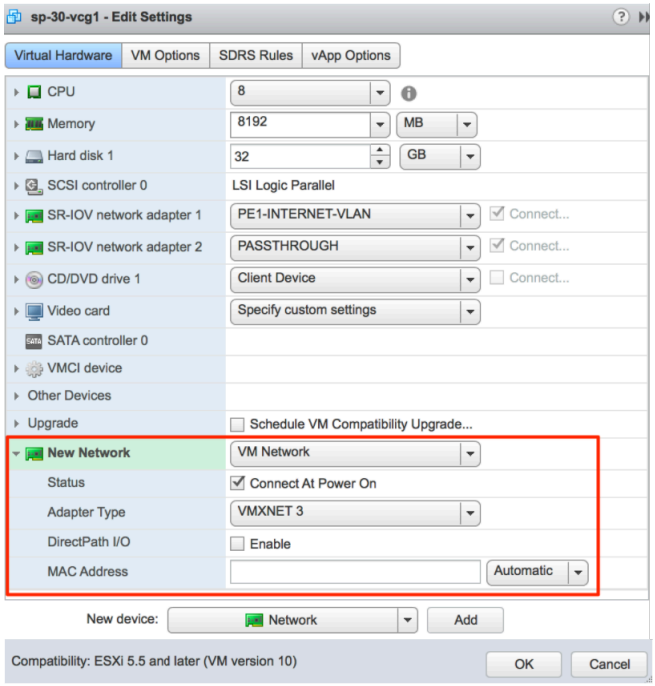
```
      - #_IPv4_Address_/mask#
  mac_address: #_mac_Address_#
    gateway4: #_IPv4_Gateway_#
    nameservers:
      addresses:
        - #_DNS_server_primary_#
        - #_DNS_server_secondary_#
      search: []
    routes:
      - to: 0.0.0.0/0
        via: #_IPv4_Gateway_#
        metric: 1

  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_#
```

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.



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

```
velocloud@KVMperf1:/tmp$ virsh dumpxml vcg_1 | egrep 'interface|network|mac address'
    <interface type='hostdev' managed='yes'>
      <mac address='52:54:00:85:5e:98'/>
    </interface>
    <interface type='hostdev' managed='yes'>
      <mac address='52:54:00:80:3f:36'/>
    </interface>
velocloud@KVMperf1:/tmp$
```

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 will relax its check to allow Ethernet frames that have incorrect EtherType of 0x8100 in the outer header.

SNMP Integration

This section describes how to configure SNMP integration.

For more 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.org>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%
includeAllDisks 10%#
# System Load
#
# Unacceptable 1-, 5-, and 15-minute load averages
load 12 10 5
```

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 nsExtendOutput2Table) 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::netSnmpPassExamples 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
```

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. 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
```

Partner Gateway Upgrade and Migration 3.3.2 or 3.4 to 4.0

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 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 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. More 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 more information, type: man ip.

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::250:56ff:fe84:a009/64 scope link
    valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group
 default qlen 1000
 link/ether 00:50:56:84:a6: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::250:56ff: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,LOWER_UP> mtu 1500 qdisc mq state UP mode
 DEFAULT group default qlen 1000
 link/ether 00:50:56:84:a6: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

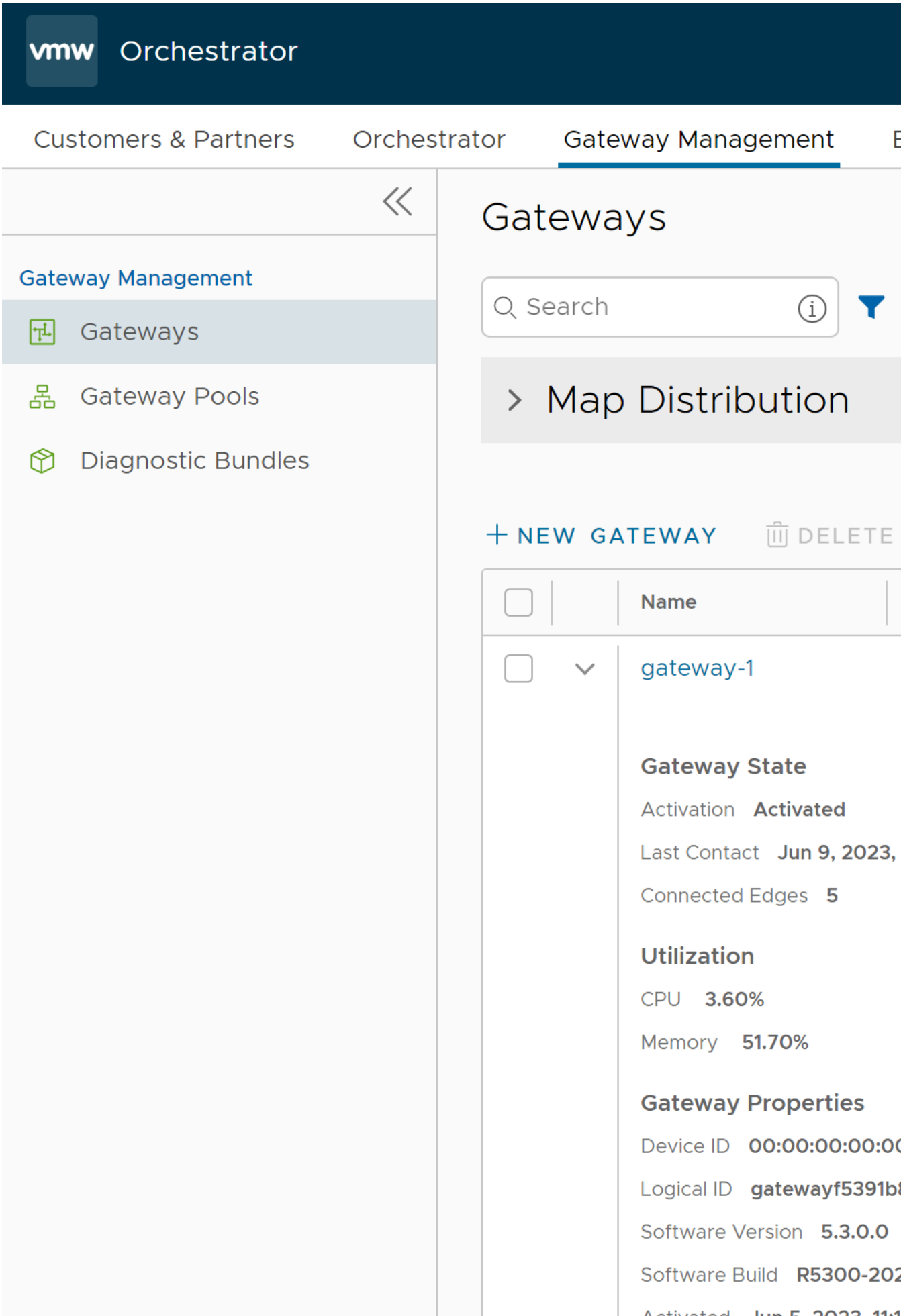
Note: The below steps are based on the assumption that you want to keep the same IP address and name for the new deployed in the 4.0 release. However, if you want to create a new with a different IP address and, you can follow the new procedures.

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 systems and decommissioning systems running older code.

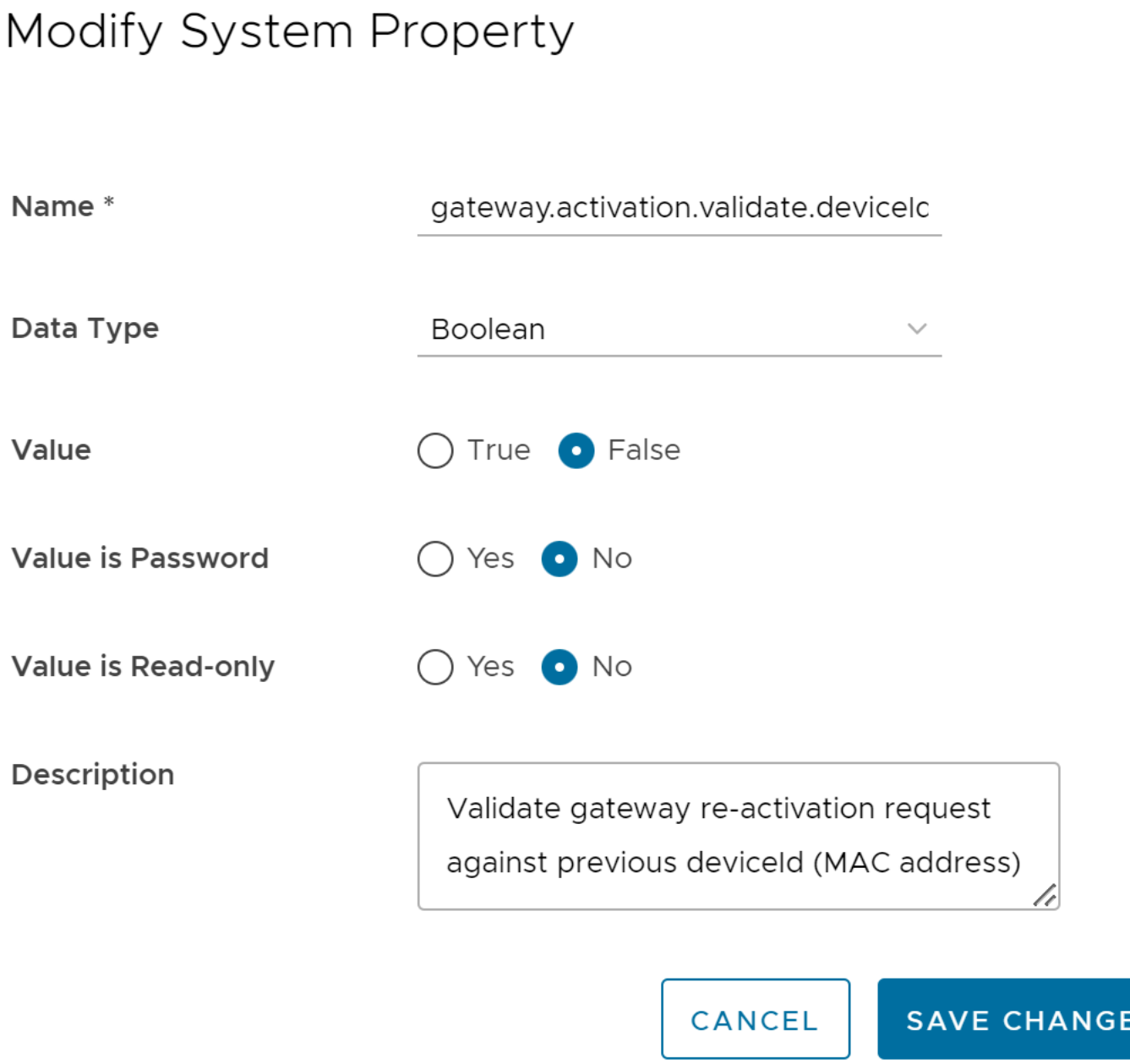
For VPN or NAT with well-known public IP addresses, adhere to the following procedure below if the public IP of the must be preserved.

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

1. Launch the new system based on the 4.0 release image. Refer to the deployment guide for your platform for more information (Gateway Installation Procedures).
2. Shutdown the old system. (Bring down the old 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 system, or configure the public IP on the new network interface. Deploy the new Gateway with the Cloud-int examples given above using the same IP address as the previous.
4. Obtain the activation key from the existing record in the (as described in the steps below).
   a. From the, go to **Gateway Management** > **Gateways**.
   b. In the **Gateways** screen, select the for which you to obtain the activation key and click 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.


vmw
Orchestrator
Customers & Partners
Orchestrator
Gateway Management
Gateway Management
Gateways
Gateway Pools
Diagnostic Bundles
Gateways
Search
Map Distribution
+ NEW GATEWAY
DELETE
Name
gateway-1
Gateway State
Activation Activated
Last Contact Jun 9, 2023,
Connected Edges 5
Utilization
CPU 3.60%
Memory 51.70%
Gateway Properties
Device ID 00:00:00:00:0
Logical ID gatewayf5391b
Software Version 5.3.0.0
Software Build R5300-202

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 Operator Guide, if necessary for more information.



6. Re-activate the new 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 is now registered and ready to receive a connection from the Edges.

Note: The 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#

Without Well-known Public IPs

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

Procedure: (Without Well-known Public IPs)

1. Launch a new system. Refer to the deployment guide for your platform if necessary (Gateway Installation Procedures).
2. Activate a new system.
3. Add new to the pool. Refer to the "Gateway Management" section in the Operator Guide for more details.
   a. The is now registered and ready to receive a connection from the Edges.
4. Remove the old from pool. Refer to the "Gateway Management" section in Operator Guide for more information.
5. Decommission the old VM. (Remove the record from the 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*.

Index

V