

ARISTA

Operator Guide

Arista VeloCloud SD-WAN

Version 6.4



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

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

Contents

About Operator Guide.....	5
What's New.....	5
Overview of	6
Supported Browsers.....	6
Operator-level UI Changes in the New.....	6
Log in to the Using SSO for Operator User.....	23
Configure Advisory Notice and Consent Warning Message for	30
Monitor Customers.....	31
Manage Customers.....	33
Create New Customer.....	35
Clone a Customer.....	41
Configure Customers.....	43
.....	51
Configure Distributed Cost Calculation.....	59
Configure Path Calculation with Multiple DSCP Labels per Flow.....	62
Activate on a	63
Activate Analytics for a New Customer.....	65
Activate Analytics for an Existing Customer.....	65
Activate Self-Healing for a New Customer.....	66
Activate Self-Healing for an Existing Customer.....	68
Manage Partners.....	69
Create New Partner.....	71
Configure Partner.....	74
Partner Settings.....	77

Manage Operators.....	79
Monitor Operator Events.....	79
Manage Operator Profiles.....	81
User Management - Operator.....	90
Users.....	91
Add New User.....	93
API Tokens.....	95
Roles.....	97
Add Role.....	99
Enterprise Security Admin Role.....	101
Service Permissions.....	106
New Permission.....	108
List of User Privileges.....	110
Authentication.....	119
Configure Azure Active Directory for Single Sign On.....	134
Configure Okta for Single Sign On.....	140
Configure OneLogin for Single Sign On.....	143
Configure PingIdentity for Single Sign On.....	145
Configure Arista CSP for Single Sign On.....	147
Orchestrator Branding - Operator.....	157
Manage User Agreements.....	163
Manage Gateway Pools and Gateways.....	168
Manage Gateway Pools.....	168
Create New Gateway Pool.....	171
Clone a Gateway Pool.....	172
Configure Gateway Pools.....	172
Manage Gateways.....	177
Create New Gateway with New Orchestrator UI.....	180
Configure Gateways.....	183
Upgrade for Dual Stack Support.....	190
Configure IPv6 Address on Gateways.....	191
Partner Gateways.....	193
Monitor Gateways.....	198
Migration.....	204
Migration - Limitations.....	205
Quiesce Gateways.....	206
Decommission Quiesced Gateways.....	208
Diagnostic Bundles for Gateways.....	208
Request Diagnostic Bundles for Gateways with New Orchestrator UI.....	209
Request Packet Capture Bundle for Gateways.....	212
Platform and Modem Firmware and Factory Images.....	214
Software Images.....	216

Edge Licensing.....	218
Manage Edge Licenses for Partners.....	220
Manage Edge Licenses for Customers.....	223
 Application Maps.....	 225
 Edge Management.....	 229
 Access SD-WAN Edges Using Key-Based Authentication.....	 232
Add SSH Key.....	233
Revoke SSH Keys.....	233
Enable Secure Edge Access for an Enterprise.....	234
Secure Edge CLI Commands.....	234
Sample Outputs.....	237
 Configure User Account details.....	 239
 Orchestrator Diagnostics.....	 246
 Orchestrator Upgrade with New Orchestrator UI.....	 252
 Replication.....	 258
 System Properties.....	 258
 External Certificate Authority.....	 260
 Appendix.....	 272
Operator-Level Orchestrator Alerts and Events.....	273
 Index.....	 283

About Operator Guide

The *(formerly known as Arista SD-WAN™)* Operator Guide provides information about, including how to configure and manage Customers and Partners who use the Orchestrator.

Intended Audience

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

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 SASE.

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

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

What's New

What's New in Version 6.4.0

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 Operator users to brand the Orchestrator User Interface (UI) by applying their company's name, logo, and colors at a global level. For more information, see Orchestrator Branding - Operator.

Release Notes

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

Overview of

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

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

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

Supported Browsers

The 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.

Operator-level UI Changes in the New

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 Operator UI for some features. It also gives the reasons for these changes.

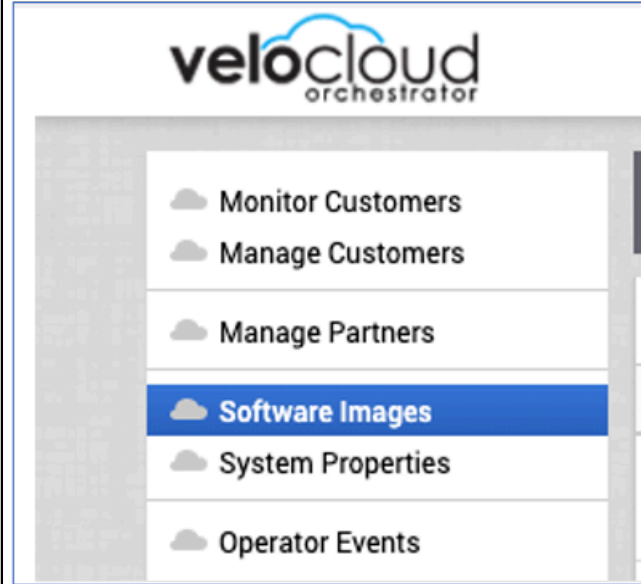
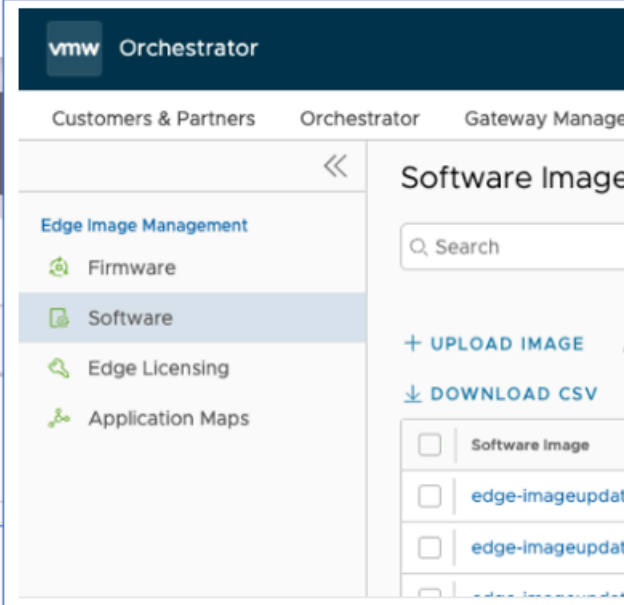
Software Images

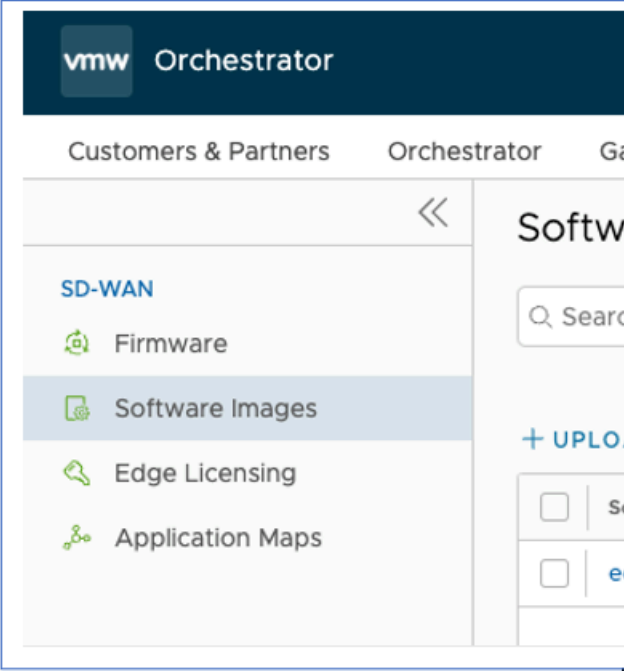
For 5.3.0 and Earlier Versions:

This feature has moved because the Edge-specific features are now under the Operator level, which can handle more than just SD-WAN features. The Operator and other levels are also adjusted to fit the new Arista Edge Cloud Orchestrator (VECO) portal, which can support multiple services.

For 5.4.0 and Later Versions:

This feature is again moved because the Classic Orchestrator UI could not fit multiple services that need configuration at the Operator level. The new **Services** tab can accommodate different service settings, including SD-WAN features such as **Software Images**, **Edge Licensing**, **Firmware**, and **Application Maps**.

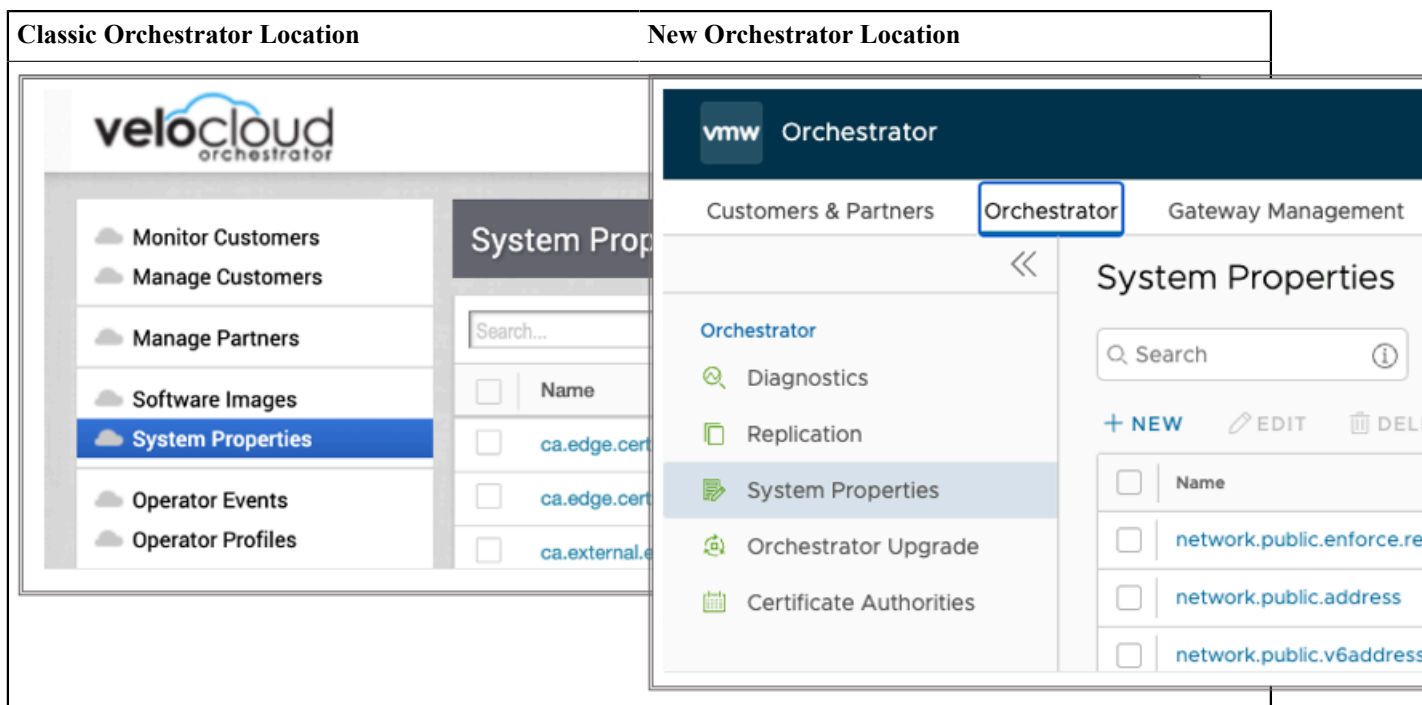
Classic Orchestrator Location	New Orchestrator Location
Operator > Software Images	For 5.3.0 and earlier versions: Operator > Edge Image Management > Software
	

Classic Orchestrator Location	New Orchestrator Location
	<div>For 5.4.0 and later versions: Operator > Services > Software Images</div> <div>A screenshot of the VMware Orchestrator web interface. The top navigation bar includes 'Customers & Partners', 'Orchestrator', and 'Gateway Management'. A left-hand sidebar menu is open, showing 'SD-WAN' as the selected category. Under 'SD-WAN', there are four items: 'Firmware', 'Software Images' (which is highlighted with a blue background), 'Edge Licensing', and 'Application Maps'. To the right of the sidebar, the main content area is titled 'Software Images' and contains a search bar and an '+ UPLOAD IMAGE' button.</div>

System Properties

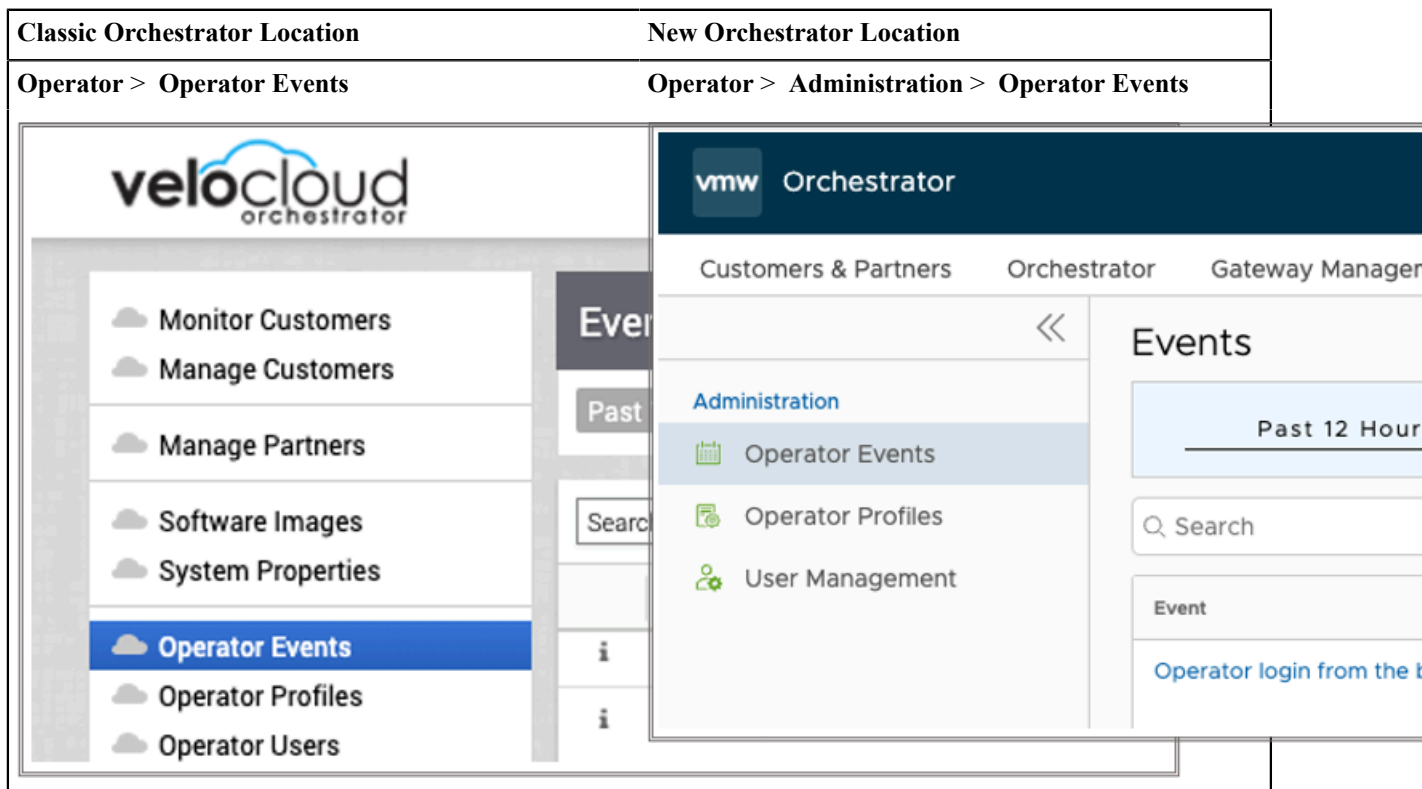
This feature has moved to a new location because the Classic Orchestrator UI did not have clear navigation and organization of pages. The New Orchestrator location has a better hierarchy and categorization of these Operator pages. It groups related features together. **System Properties** is part of Orchestrator configuration, along with **Diagnostics, Replication, Orchestrator Upgrade,** and **Certificate Authorities.**

Classic Orchestrator Location	New Orchestrator Location
Operator > System Properties	Operator > Orchestrator > System Properties



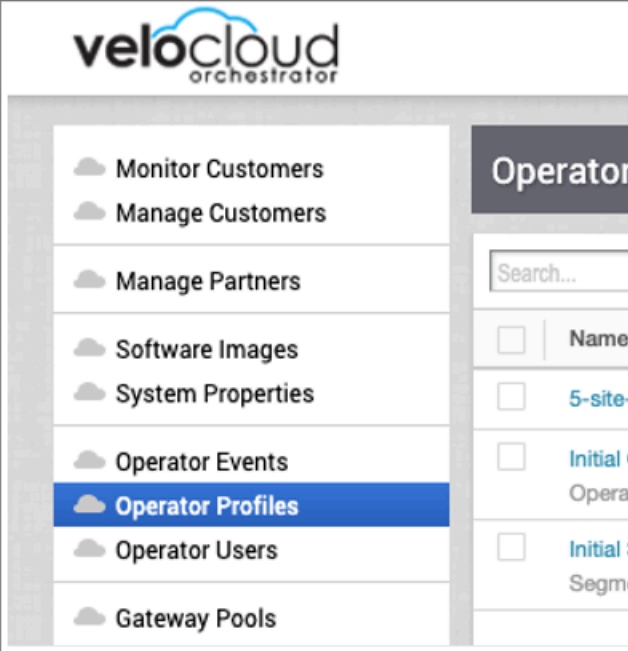
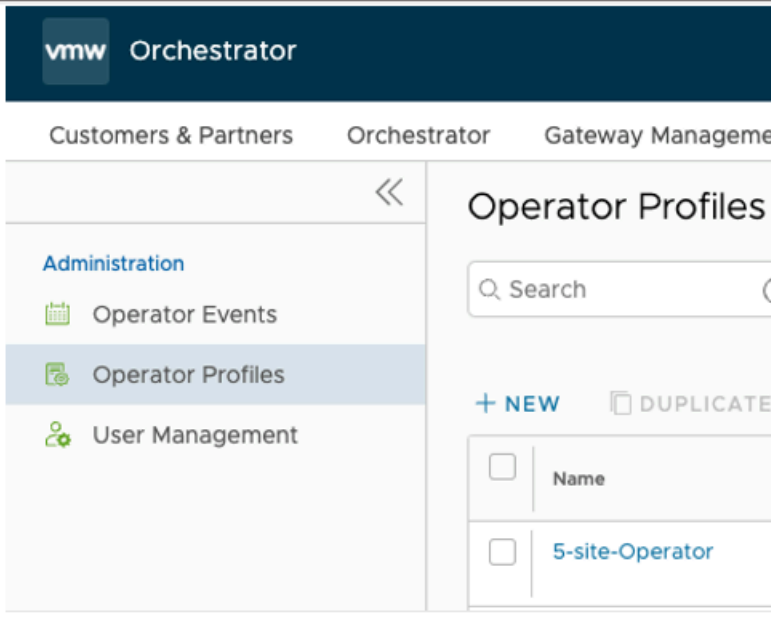
Operator Events

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 Operator administration-related features under the **Administration** tab.



Operator Profiles

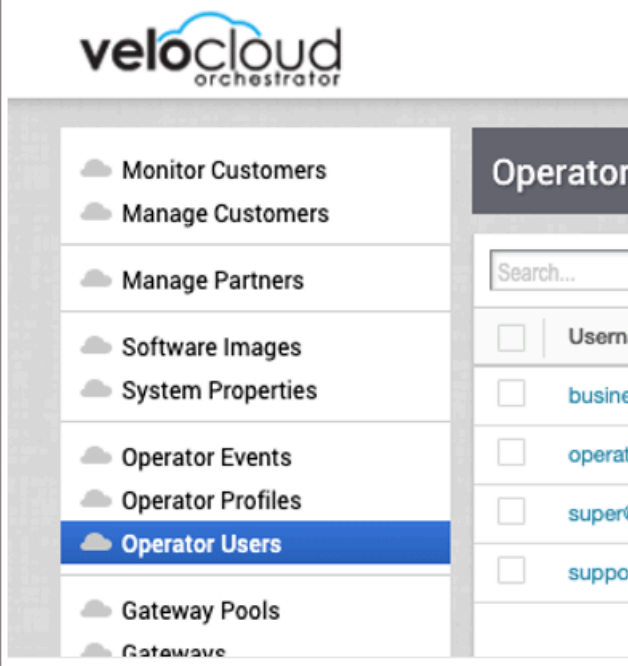
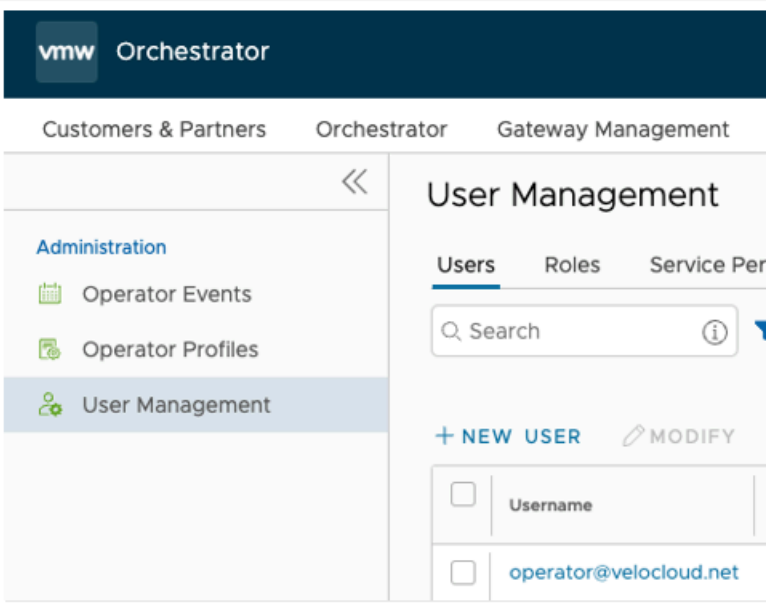
This feature has moved to a new location because the Classic Orchestrator UI did not have clear navigation and organization of pages. The New Orchestrator puts all the Operator administration-related features under the **Administration** tab.

Classic Orchestrator Location	New Orchestrator Location
Operator > Operator Profiles	Operator > Administration > Operator Profiles
	

Operator Users

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 Operator administration-related features under the **Administration** tab.

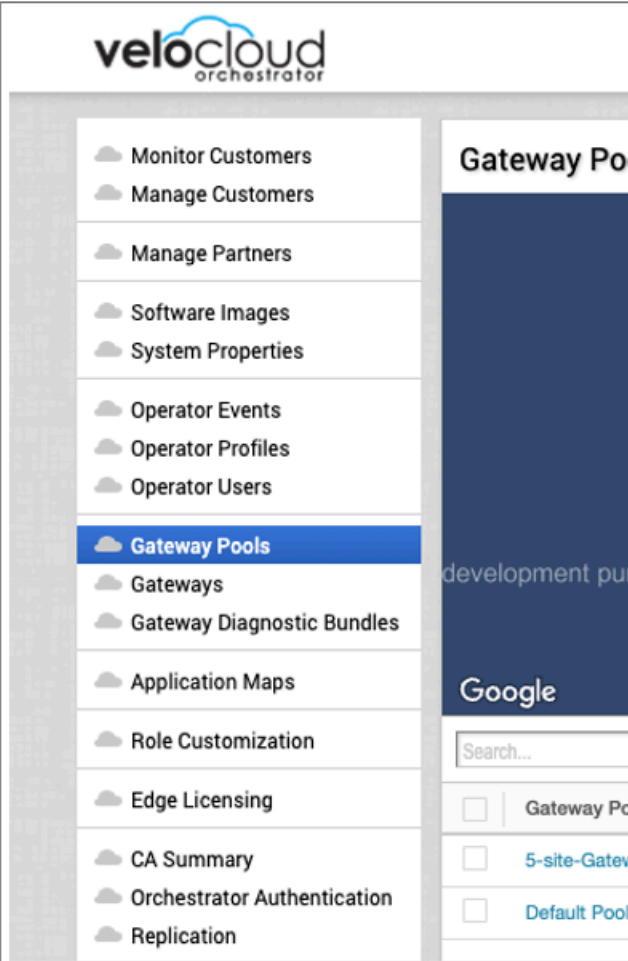
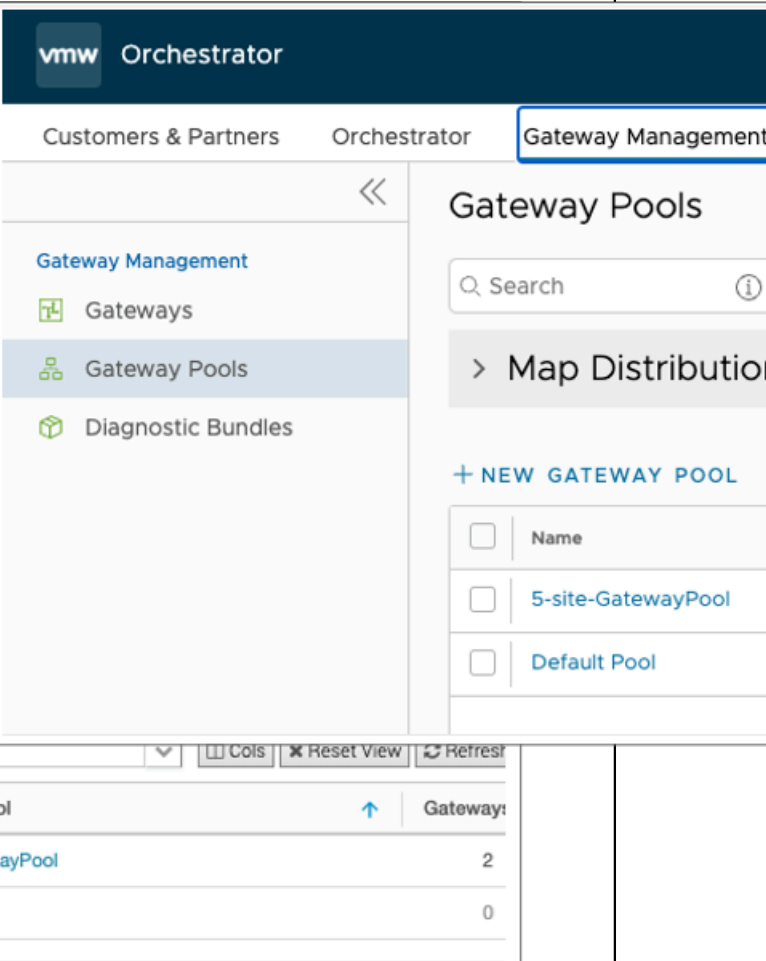
Classic Orchestrator Location	New Orchestrator Location
Operator > Operator Users	Operator > Administration > Operator Users

Classic Orchestrator Location	New Orchestrator Location
	

Gateway Pools

We have moved the **Gateway Pools** feature to the New Orchestrator UI for enhanced user experience. The New Orchestrator UI has a better design that groups all Gateway related features under the **Gateway Management** tab.

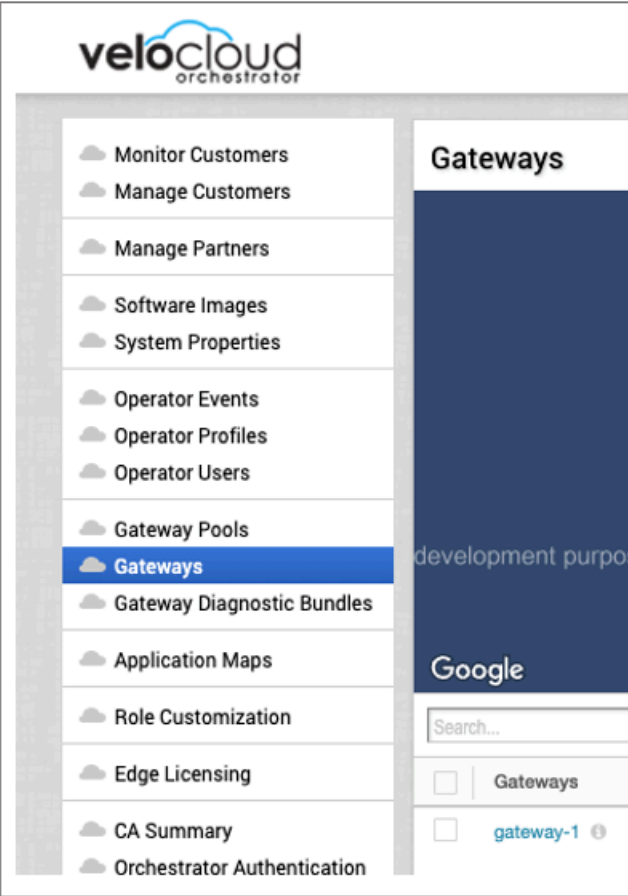
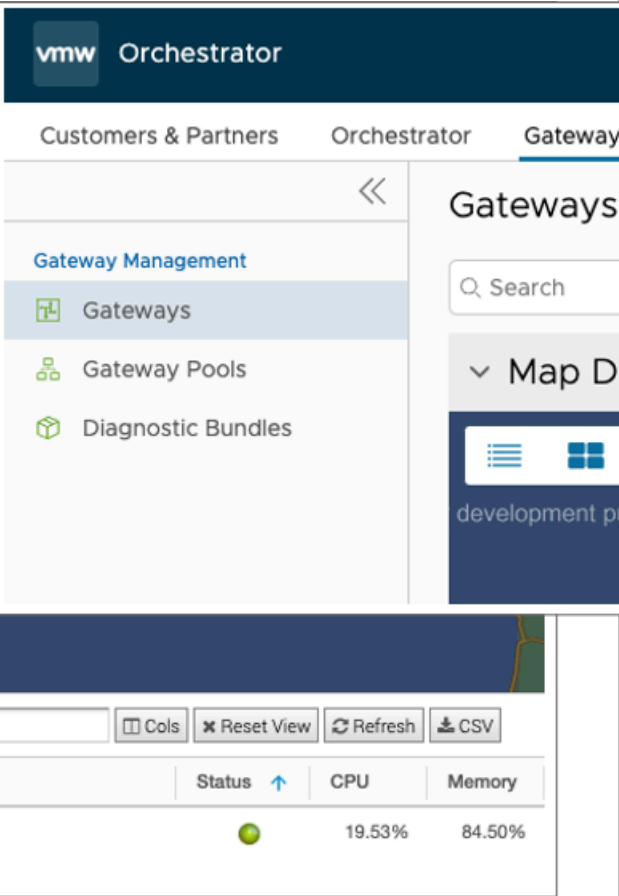
Classic Orchestrator Location	New Orchestrator Location
Operator > Gateway Pools	Operator > Gateway Management > Gateway Pools

Classic Orchestrator Location	New Orchestrator Location
	

Gateways

We have moved the **Gateways** feature to the New Orchestrator UI for enhanced user experience. The New Orchestrator UI has a better design that groups all Gateway related features under the **Gateway Management** tab.

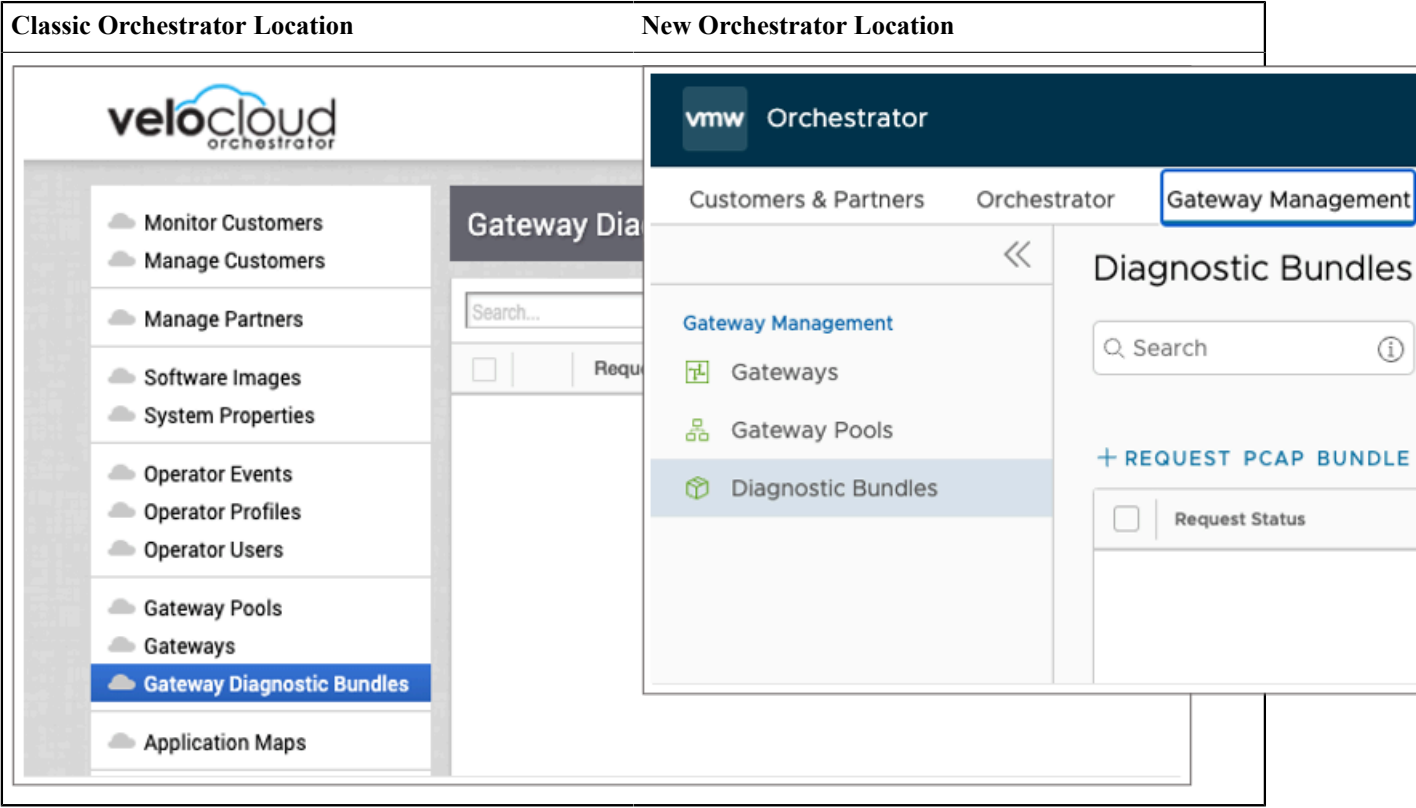
Classic Orchestrator Location	New Orchestrator Location
Operator > Gateways	Operator > Gateway Management > Gateways

Classic Orchestrator Location	New Orchestrator Location
	

Gateway Diagnostic Bundles

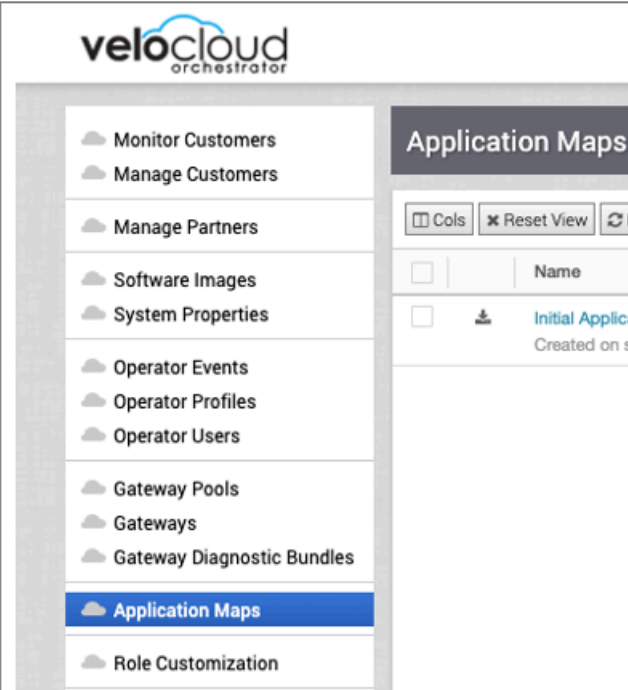
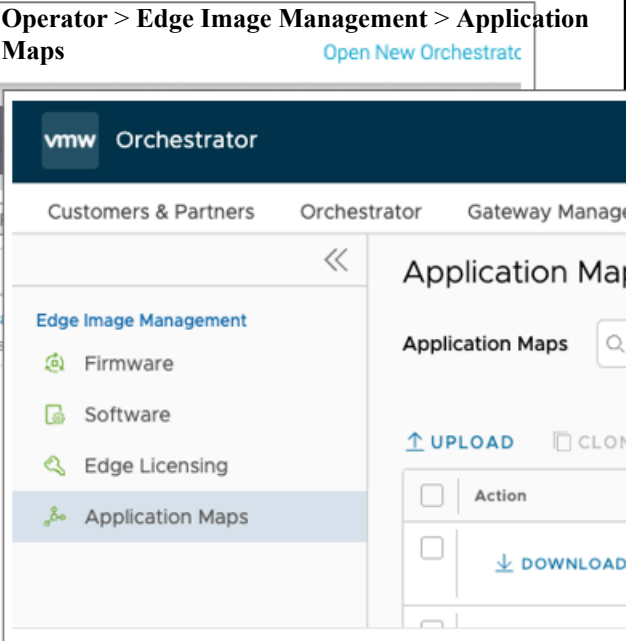
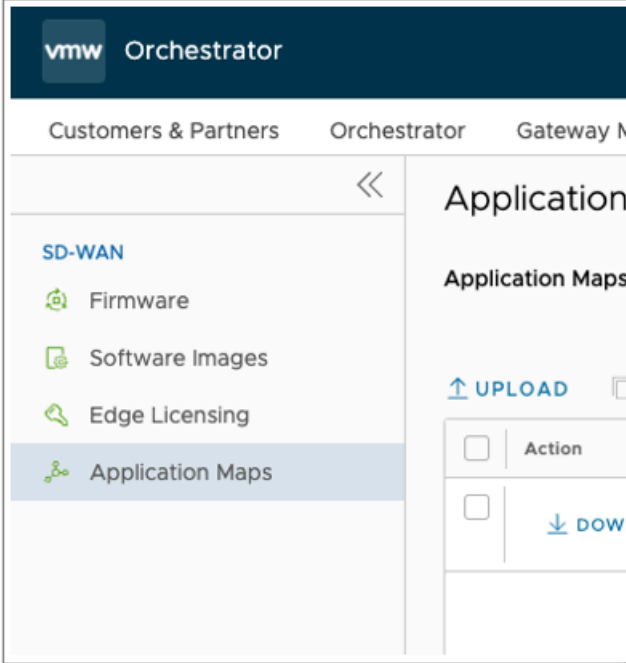
We have moved the **Gateway Diagnostic Bundles** feature to the New Orchestrator UI for enhanced user experience. The New Orchestrator UI has a better design that groups all Gateway related features under the **Gateway Management** tab.

Classic Orchestrator Location	New Orchestrator Location
Operator > Gateway Diagnostic Bundle	Operator > Gateway Management > Gateway Diagnostic Bundle



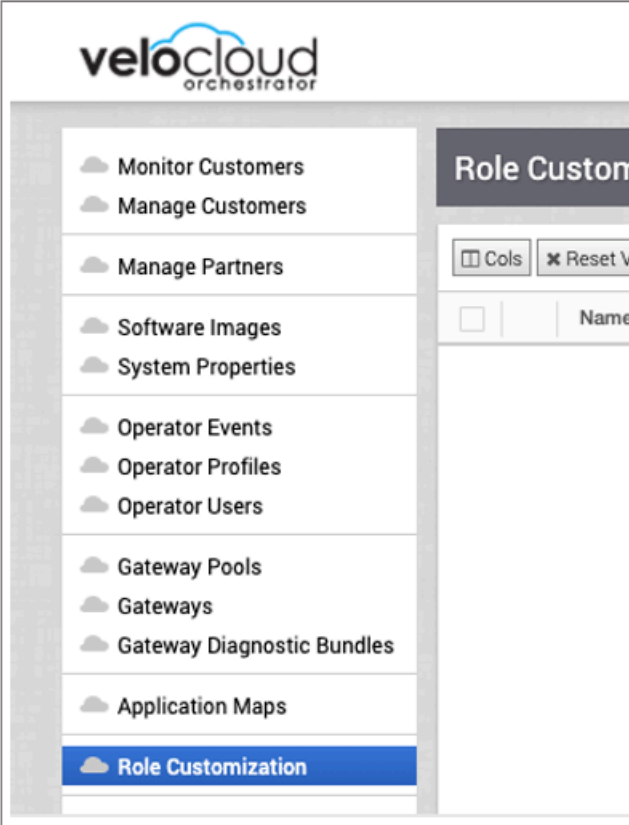
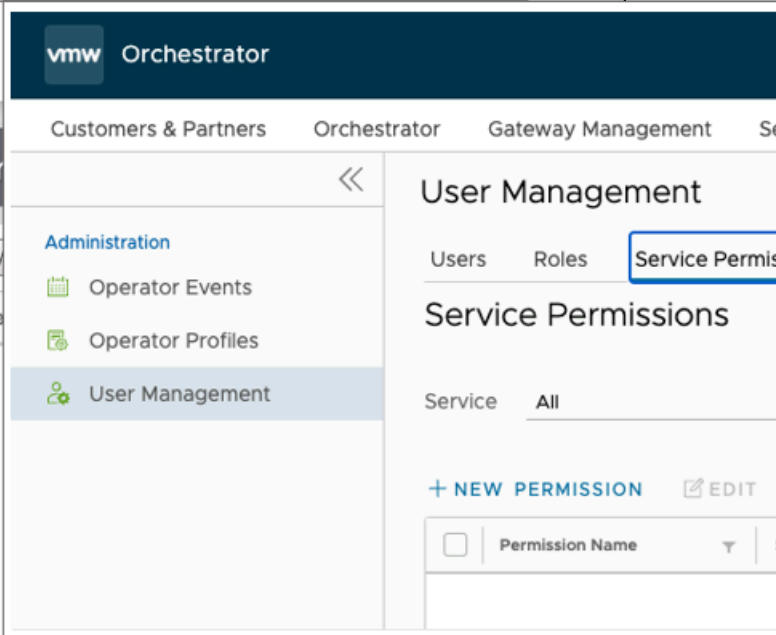
Application Maps

We have relocated the **Application Maps** feature to the New Orchestrator UI for better user experience. **Application Maps** is a feature that only applies to the SD-WAN service and the New Orchestrator UI is a portal for many services, so we have moved this feature under the new **Edge Image Management** (or **Services**) tab within the SD-WAN service.

Classic Orchestrator Location	New Orchestrator Location
Operator > Application Maps	For 5.3.0 and earlier versions: Operator > Edge Image Management > Application Maps Open New Orchestrator
	
	For 5.4.0 and later versions: Operator > Services > Application Maps
	

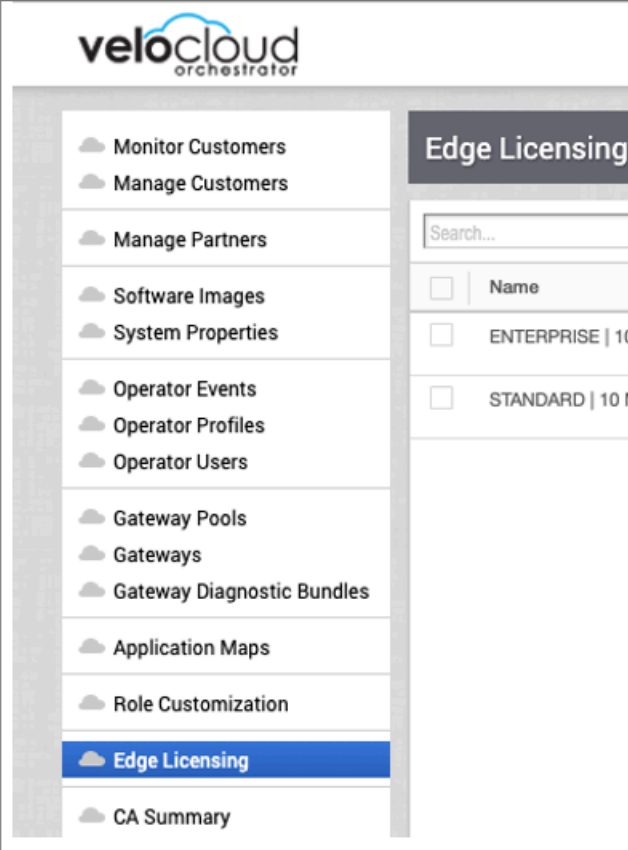
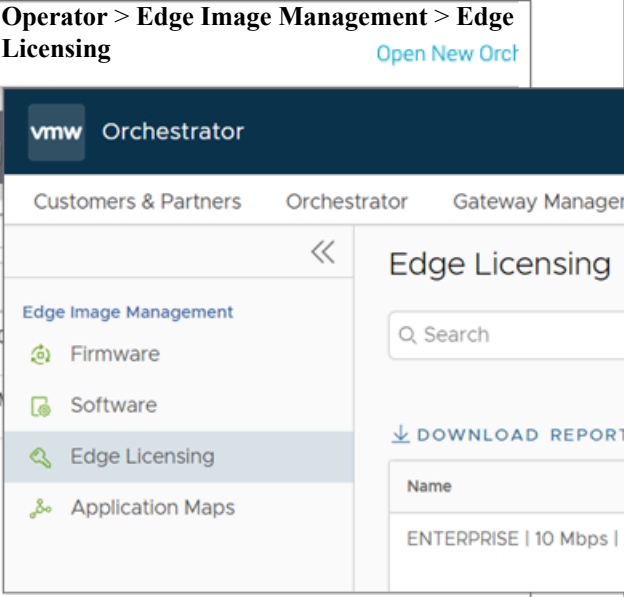
Role Customization (Service Permissions)

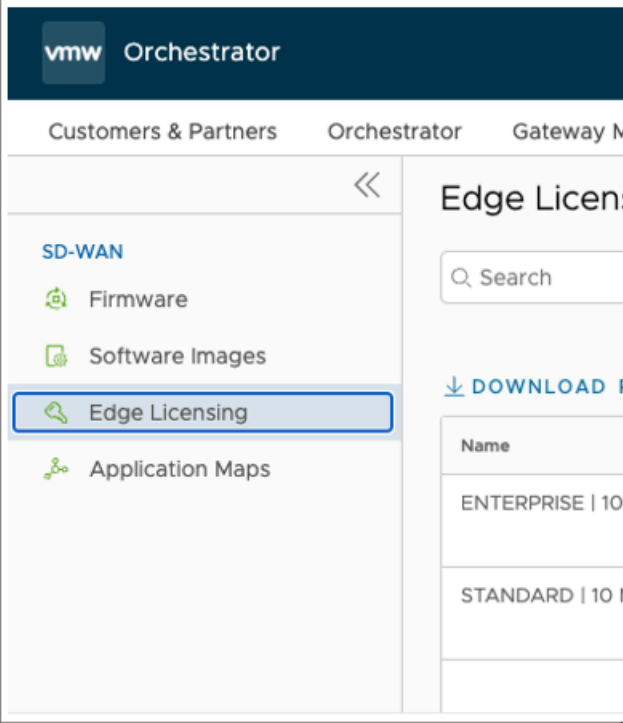
We have changed the name of the "Role Customization" feature to "Service Permissions". This is to make room for the new Role Builder feature that lets you create custom roles by combining different service permissions. **Service Permissions** is a more accurate name for the feature, as it allows you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

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

Edge Licensing

We have relocated the **Edge Licensing** feature to the New Orchestrator UI for better user experience. **Edge Licensing** is a feature that only applies to the SD-WAN service and the New Orchestrator UI is a portal for many services, so we have moved this feature under the new **Edge Image Management** (or **Services**) tab within the SD-WAN service.

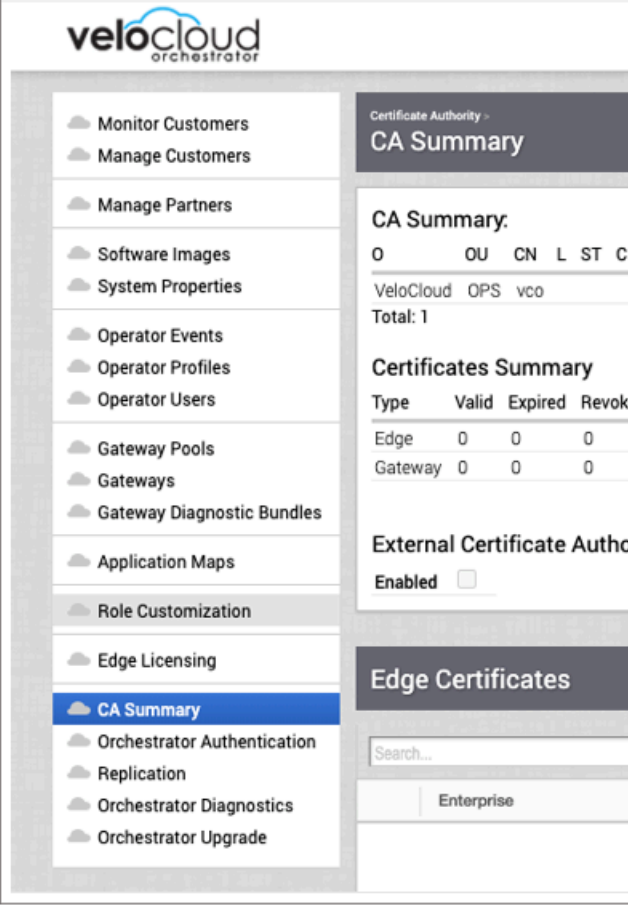
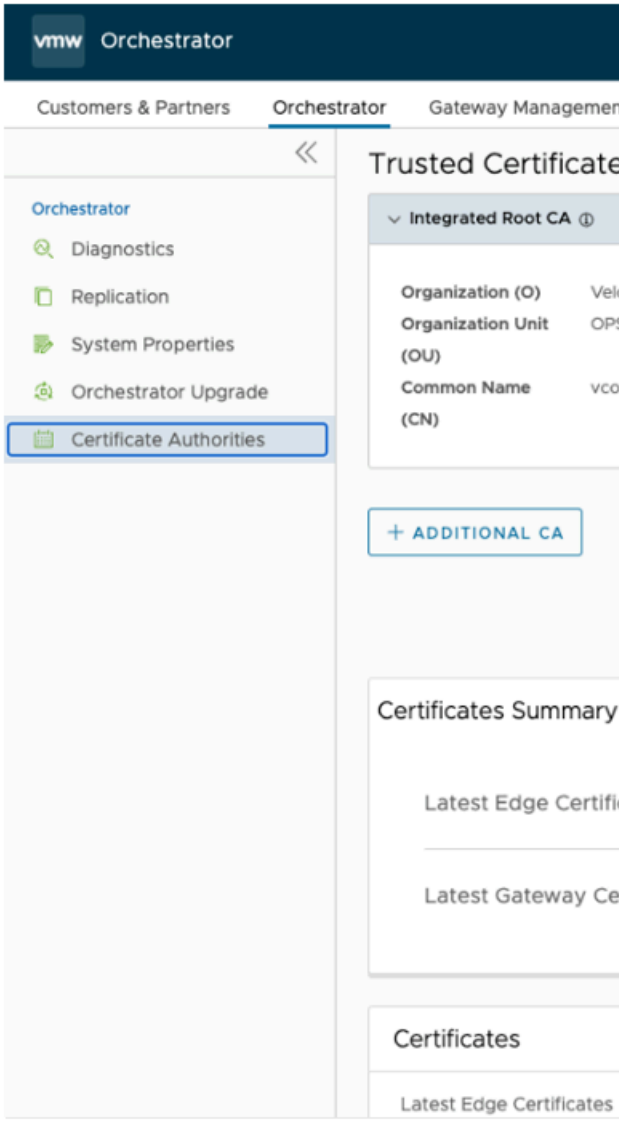
Classic Orchestrator Location	New Orchestrator Location
Operator > Edge Licensing	For 5.3.0 and earlier versions: Operator > Edge Image Management > Edge Licensing Open New Orcl
	

Classic Orchestrator Location	New Orchestrator Location
	<div>For 5.4.0 and later versions: Operator > Services > Edge Licensing</div> <div></div>

CA Summary

"CA Summary" is renamed to "Certificate Authorities" to clearly represent the content of the page for easier on-boarding.

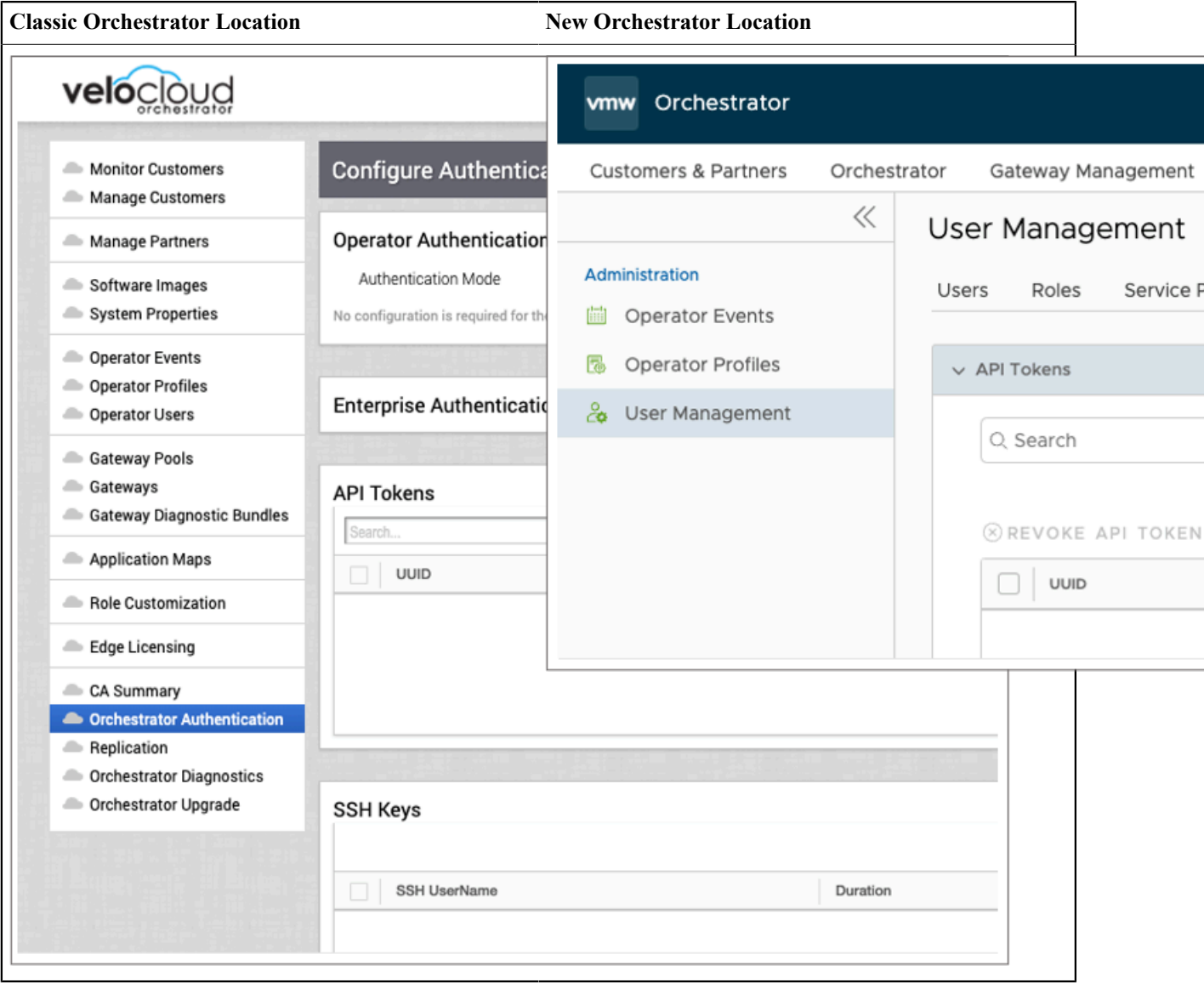
Classic Orchestrator Location	New Orchestrator Location
Operator > CA Summary	Operator > Orchestrator > Certificate Authorities

Classic Orchestrator Location	New Orchestrator Location
	

Orchestrator Authentication

We have reorganized the administrative features for different levels of users. Operators and Partners can find authentication-related features under the **Administration > User Management** section. Enterprises can find them under **Global Settings**. This makes it easier to manage user access across the Operator, MSP (Partner), and Enterprise levels.

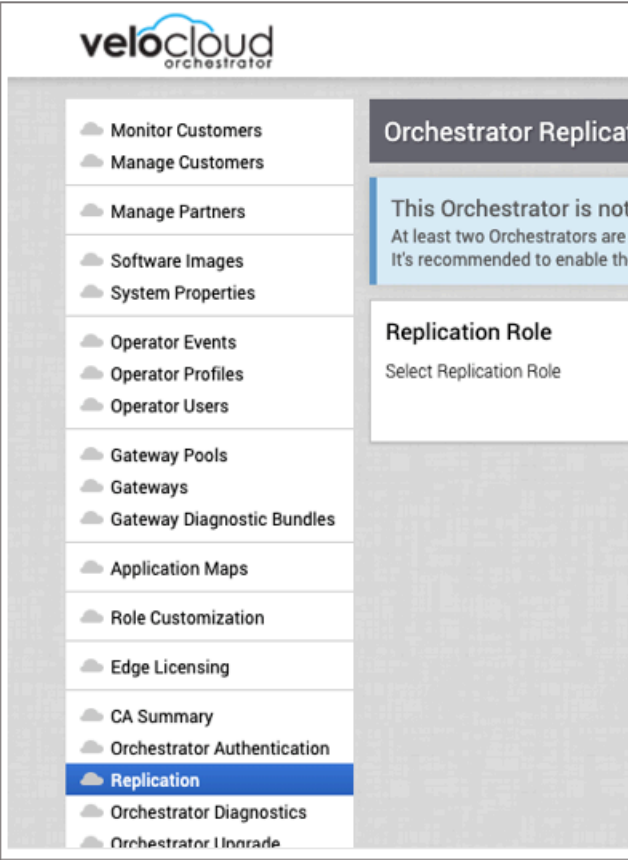
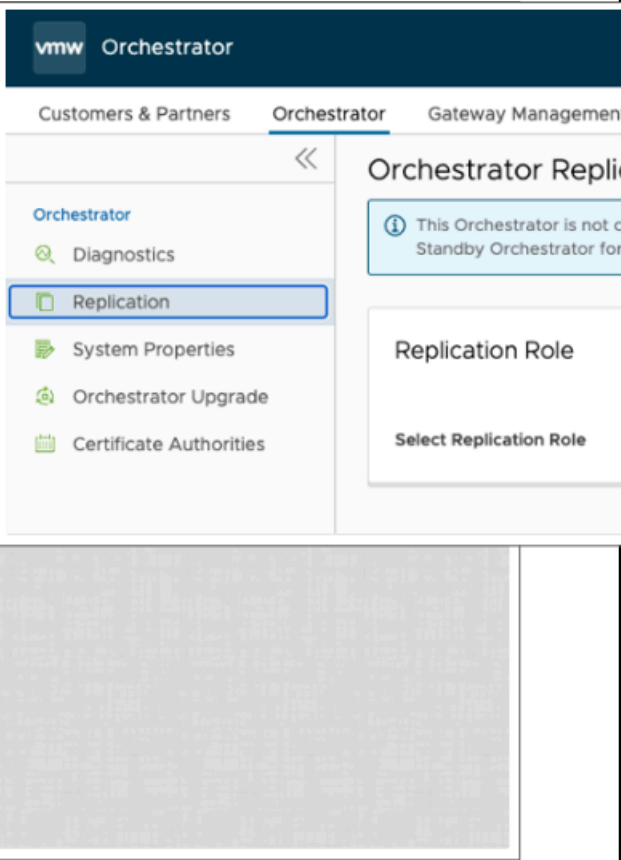
Classic Orchestrator Location	New Orchestrator Location
Operator > Orchestrator Authentication	Operator > Administration > User Management > Authentication



Replication

We have moved the **Replication** feature to improve the organization and hierarchy of the Operator pages. **Replication** is part of the Orchestrator configuration, along with other features such as **Orchestrator Diagnostics**, **System Properties**, **Orchestrator Upgrade**, and **Certificate Authorities**.

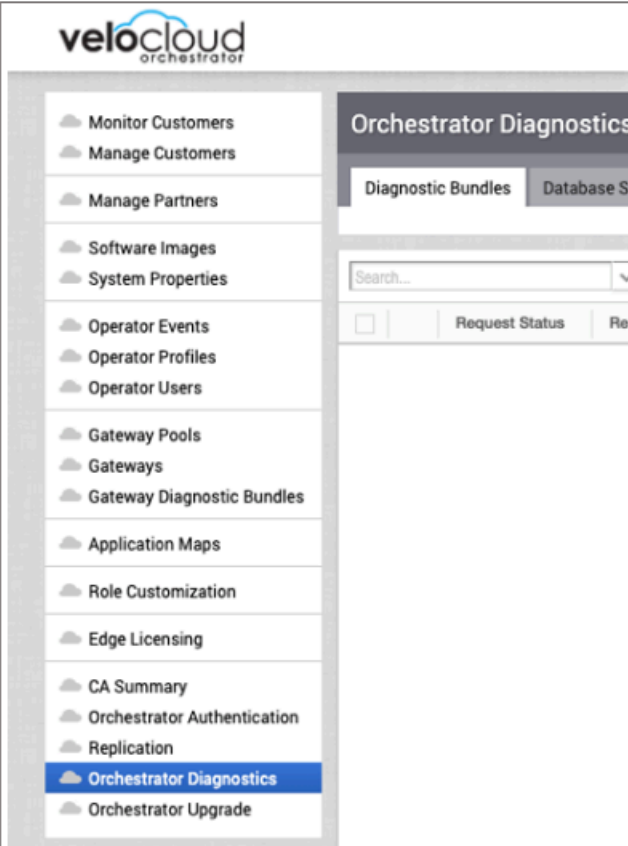
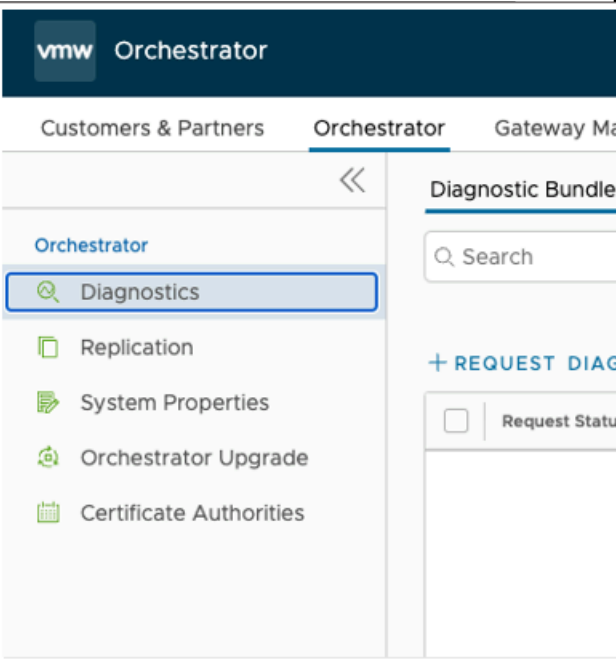
Classic Orchestrator Location	New Orchestrator Location
Operator > Replication	Operator > Orchestrator > Replication

Classic Orchestrator Location	New Orchestrator Location
	

Orchestrator Diagnostics

We have moved the **Orchestrator Diagnostics** feature to improve the organization and hierarchy of the Operator pages. **Orchestrator Diagnostics** is part of the Orchestrator configuration, along with other features such as **Replication**, **System Properties**, **Orchestrator Upgrade**, and **Certificate Authorities**.

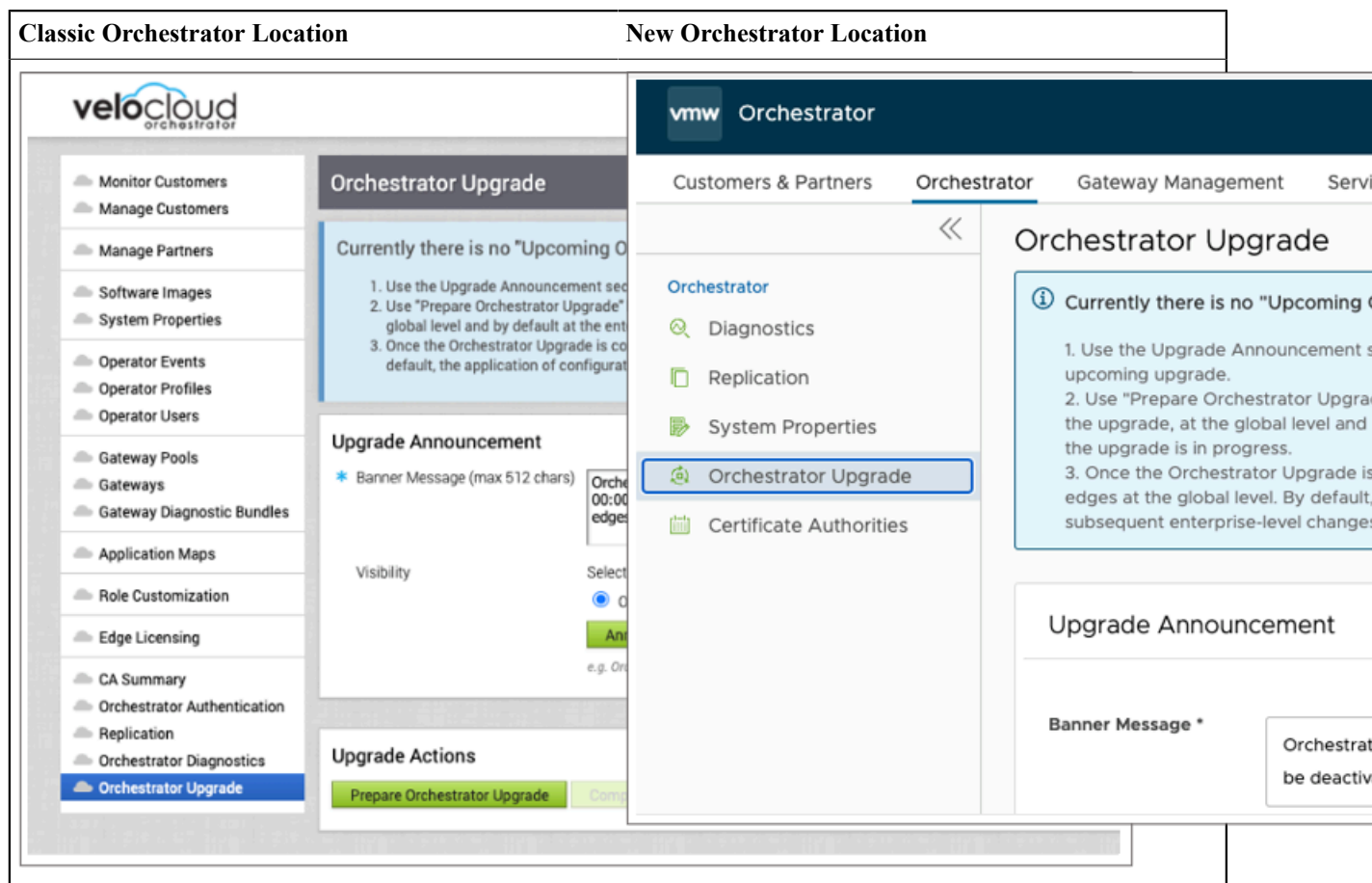
Classic Orchestrator Location	New Orchestrator Location
Operator > Orchestrator Diagnostics	Operator > Orchestrator > Diagnostics

Classic Orchestrator Location	New Orchestrator Location
	

Orchestrator Upgrade

We have moved the **Orchestrator Upgrade** feature to improve the organization and hierarchy of the Operator pages. **Orchestrator Upgrade** is part of the Orchestrator configuration, along with other features such as **Replication**, **System Properties**, **Orchestrator Diagnostics**, and **Certificate Authorities**.

Classic Orchestrator Location	New Orchestrator Location
Operator > Orchestrator Upgrade	Operator > Orchestrator > Orchestrator Upgrade



Log in to the Using SSO for Operator User

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

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

For more information, see Authentication.



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

To login into using the SSO as an Operator user:

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



Welcome to VMware Edge Cloud Orchestrator

Username

Password

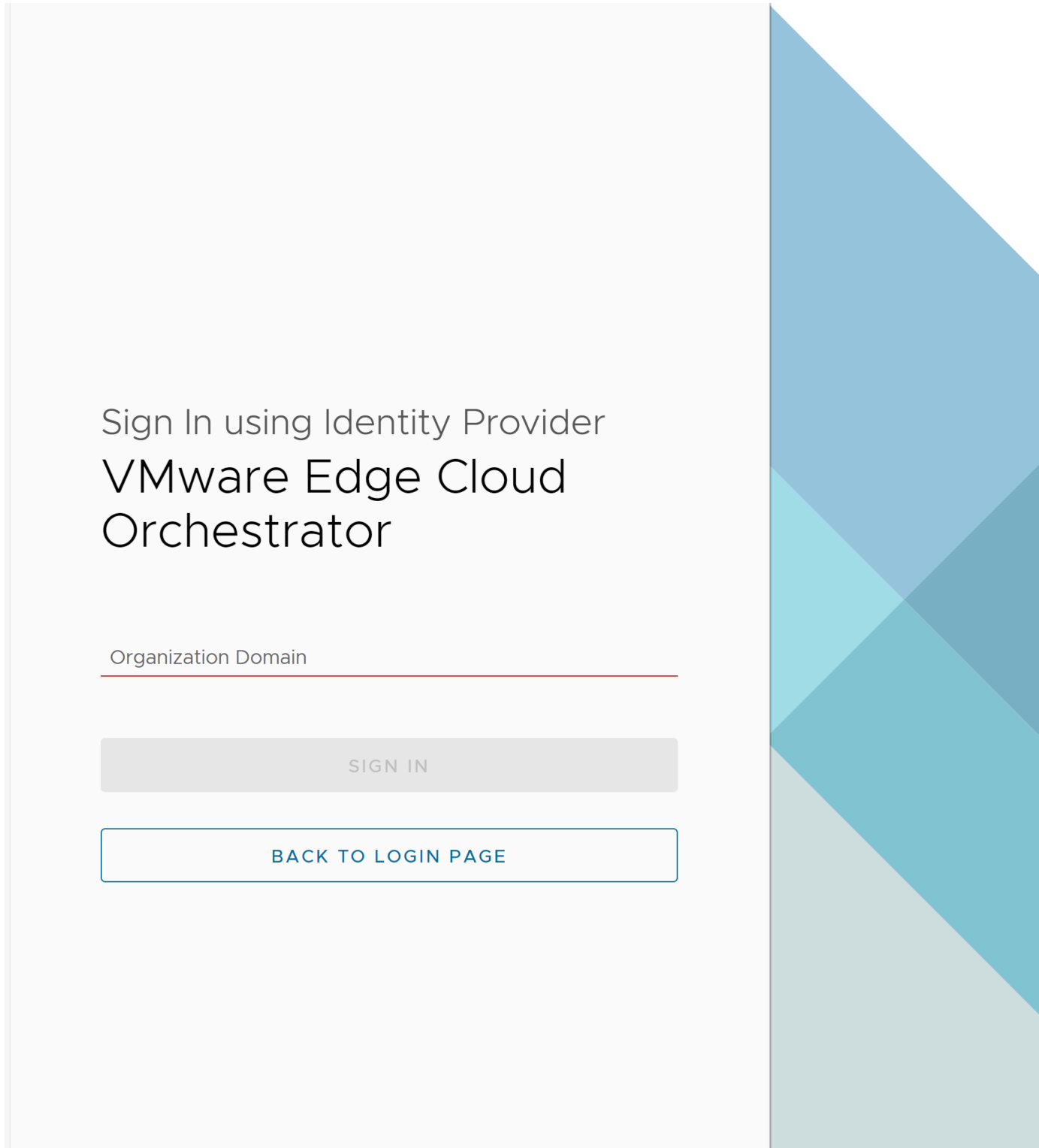


[Forgot Password?](#)

LOGIN

[SIGN IN WITH YOUR IDENTITY PROVIDER](#)

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

The screenshot shows a web interface for signing in using an identity provider. The title is "Sign In using Identity Provider VMware Edge Cloud Orchestrator". Below the title is a text input field labeled "Organization Domain". Underneath the input field is a grey button labeled "SIGN IN". Below that is a blue-outlined button labeled "BACK TO LOGIN PAGE". The background of the page is light grey, and there is a decorative blue and teal geometric pattern on the right side.

Sign In using Identity Provider
VMware Edge Cloud
Orchestrator

Organization Domain

SIGN IN

BACK TO LOGIN PAGE

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 and redirects the user to the configured URL.



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

- Manage Customers and Partner
- Manage Operators

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

Additionally, in the 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](#)

vmw

Orchestrator

Customers & Partners

Orchestrator

Gateway Management

Services

Administ

<<

Customers & Partners

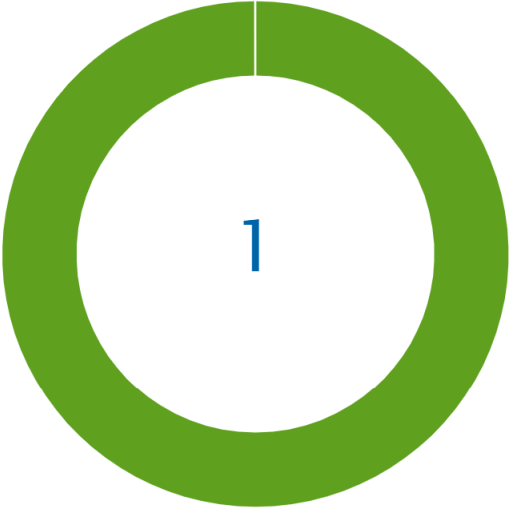
Monitor Customers

Manage Partners

Manage Customers

Customers

Total Customers



1

Customer	# Down Edges
ssk-aug-3-site	-

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 Customers](#).

vmw

Orchestrator

Customer

cust1test

▼

SD-WAN

▼

Monitor

Configure

Diagnostics

Service Settings

Monitor

Network Overview

Edges

Network Services

Routing

Alerts

Events

Reports

Network Overview

Activated Edges

0

Connected

Degr

Hubs

Connected

Degr

Edge Name	Status	Secrets Encryption
-----------	--------	--------------------

COLUMNS

REFRESH

Configure Advisory Notice and Consent Warning Message for

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

To configure the consent warning message:

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

Modify System Property...

Name: login.warning.banner.message

Data Type: JSON

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

Value is Password: ☐ Yes — ☒ No

Value is Read-only: ☐ Yes — ☒ No

Description: Login warning banner message

Update Close

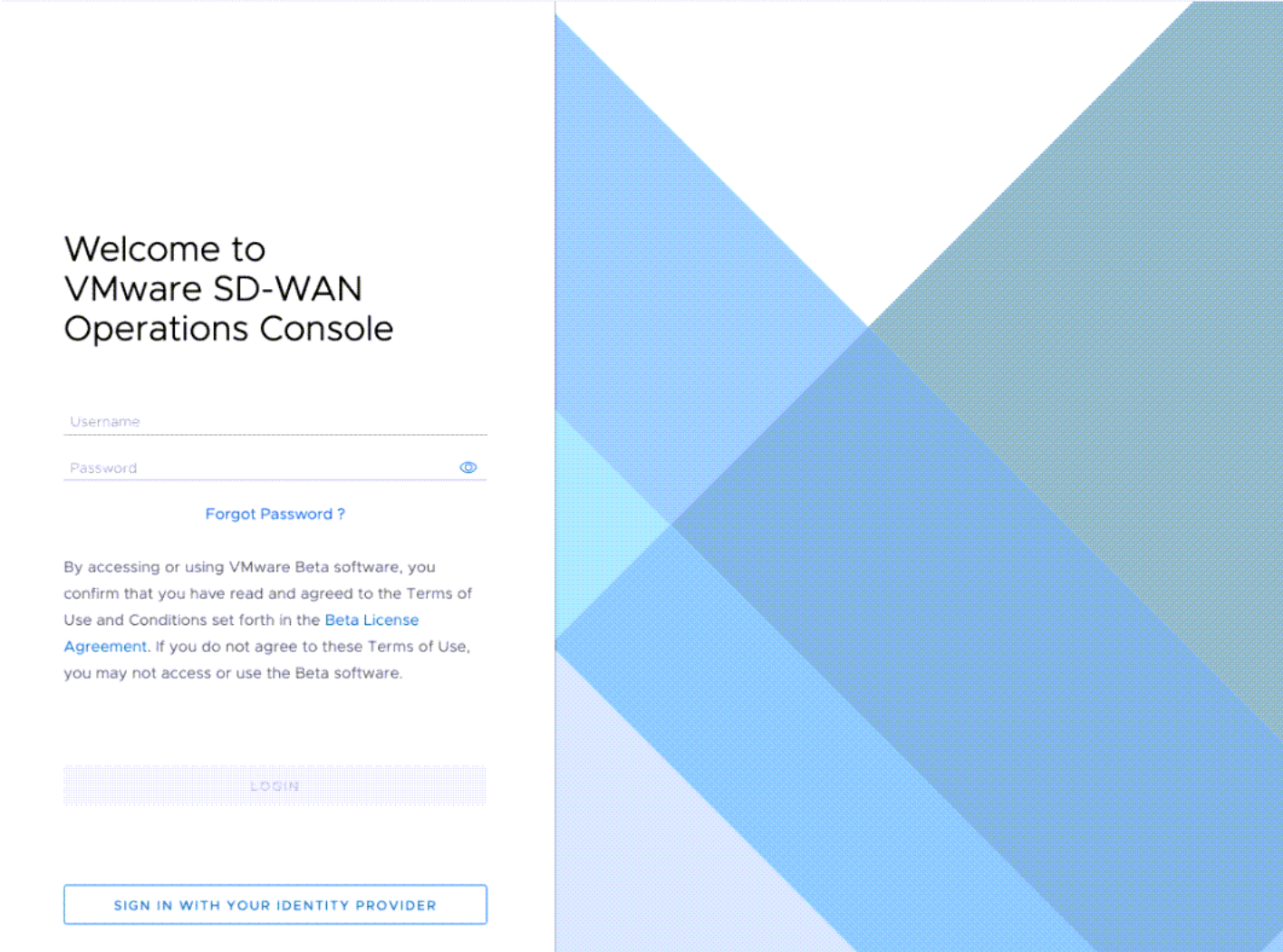
4. Ensure that the **Data Type** field is set to **JSON**.
5. In the **Value** text area, the default value is as follows:

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

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


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

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



Welcome to
VMware SD-WAN
Operations Console

Username

Password 

[Forgot Password ?](#)

By accessing or using VMware Beta software, you confirm that you have read and agreed to the Terms of Use and Conditions set forth in the [Beta License Agreement](#). If you do not agree to these Terms of Use, you may not access or use the Beta software.

LOGIN

SIGN IN WITH YOUR IDENTITY PROVIDER

Monitor Customers

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

Log into the as an Operator user. In the SD-WAN service of the Operator portal, click **Customers & Partners > Monitor Customers**.

vmw

Orchestrator

Customers & Partners

Orchestrator

Gateway Management

Edge

Customers & Partners


Monitor Customers

Manage Partners

Manage Customers

Customers

Total Customers



Customer

SCALE


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

Total Customers

- Customers managed by the Operator.
- Number of Customers that are UP, DOWN, and UNACTIVATED. Click the number to view the corresponding Customer details at 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 other settings corresponding to the selected customer. For more information see the *Administration Guide* published at www.arista.com/en/support/product-documentation.

Total Edges

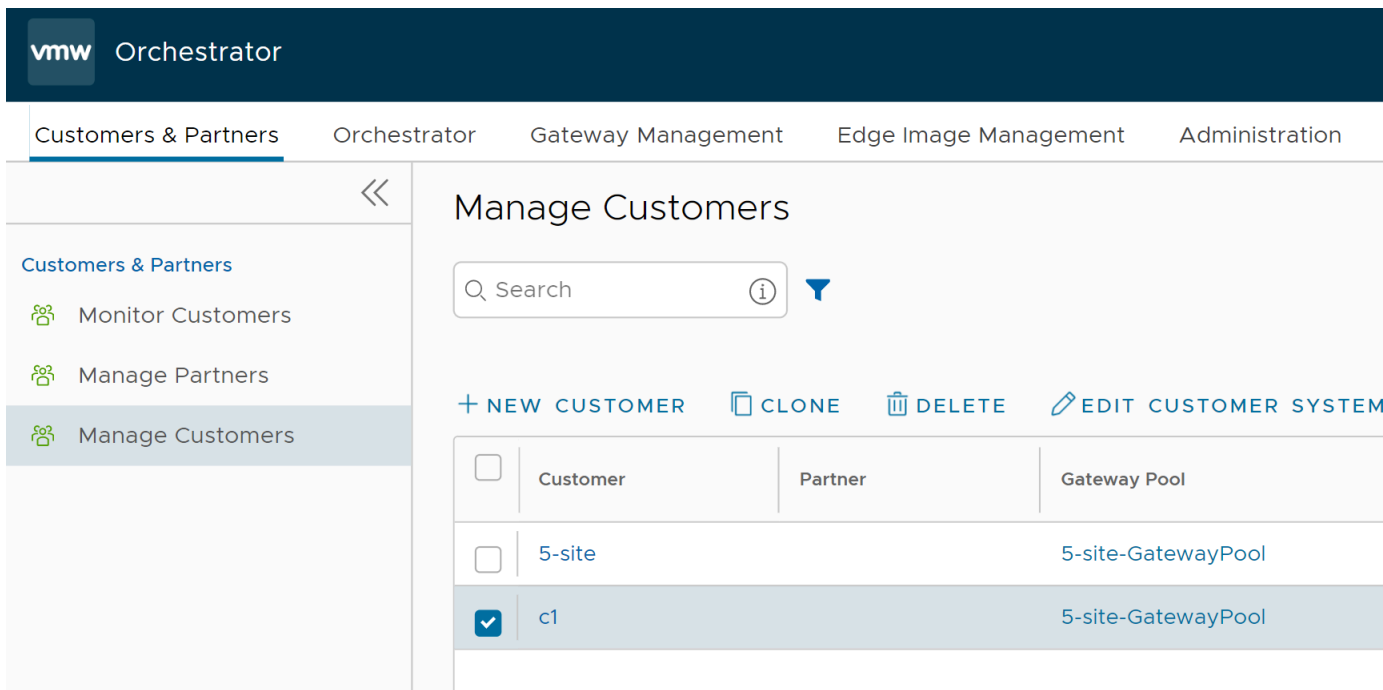
- Edges associated with the Customers.
- Number of Edges that are DOWN, DEGRADED, CONNECTED, and UNACTIVATED. Click the number to view the corresponding details of the Edges in the bottom panel.
- In the bottom panel, place the mouse cursor on the Down Arrow displayed next to the number of Edges, to view the details of each Edge. Click the link to the Edge name to navigate to the Enterprise Monitoring portal, where you can view more details corresponding to the selected Edge. For more information see the *Administration Guide* published at www.arista.com/en/support/product-documentation.

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

Manage Customers

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


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



	Customer	Partner	Gateway Pool
<input type="checkbox"/>	5-site		5-site-GatewayPool
<input checked="" type="checkbox"/>	c1		5-site-GatewayPool

2. 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.


Option	Description
New Customer	Click this option to add a new Customer. For more information, see Create New Customer
Clone	Clones the existing configurations of the selected Customer. You can select any of the additional clone attributes. For more information, see Clone a Customer .
Delete	<p>Deletes the selected Customers. Enter the number of selected Customers in the pop-up window, and then click Delete.</p> <p> Note: Ensure that you have removed all the Edges associated with the selected Customer, before deleting the Customer.</p>
Edit Customer System Settings	Allows you to edit the system settings for the customer. For more information, see the "Enterprise Settings" section in the <i>Administration Guide</i> 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.

3. 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.
Transfer to Partner	Assigns the selected Customer to a Partner. You can select an existing Partner from the drop-down list.
Release from Partner	Releases the selected Customer from the Partner.
Send Support Email	Sends customer support messages to the selected Customer.
Assign Operator Profile	<p>Adds an Operator Profile for the selected Customers.</p> <p> Note: This option is available only for an Enterprise with an activated Edge Image Management feature.</p>
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.
Rebalance Gateways	Rebalances the Gateways of Edges associated with the selected Customer.
Export All Customers	Exports the details of all the Customers in the Operator portal to a CSV file. The default separator used is a comma (,).
Export Customers Edge Inventory	Exports the inventory details of all the Edges associated with all the Customers to a CSV file. The default separator used is a comma (,).

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

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

Create New Customer

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

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

1. Customer Information

Company Name / Account Number

Company Name *

Account Number ⓘ

☒ SASE Support Access ⓘ

☒ SASE User Management Access ⓘ

Location

Address Line 1

Address Line 2

City

State / Province

Zip / Postcode

Country / Region

NEXT

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.

Option	Description
SASE Support Access	<p>This check box is selected by default, and grants access to the Support to view, configure, and troubleshoot the Edges connected to the Customer.</p> <p>For security reasons, the Support cannot access or view the user identifiable information.</p>
SASE User Management Access	Select the check box 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:

2.

Administrative Account

Username / Password / Contact

Username *

admin@test.com

Ex: user@domain.com

Password *

.....

Confirm Password *

.....

First Name

Last Name

Phone

Mobile Phone

+1

12345678909

Contact Email *


admin@test.com

NEXT

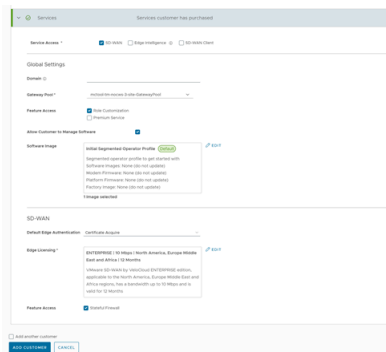
Enter the details in the following fields and click **Next**.



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.
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:



The screenshot shows the 'Services' configuration page for a customer. The 'Feature Access' section is expanded, showing two checkboxes: 'Role Customization' and 'Premium Service'. Both are currently unchecked. The 'Software Image' section shows a dropdown menu with 'Initial Deployment' selected. The 'SD-WAN' section shows a dropdown menu with 'Initial Deployment' selected. The 'Gateway Pool' section shows a dropdown menu with 'Initial Deployment' selected. The 'Global Settings' section shows a dropdown menu with 'Initial Deployment' selected. The 'Feature Access' section shows two checkboxes: 'Role Customization' and 'Premium Service'. Both are currently unchecked. The 'Software Image' section shows a dropdown menu with 'Initial Deployment' selected. The 'SD-WAN' section shows a dropdown menu with 'Initial Deployment' selected. The 'Gateway Pool' section shows a dropdown menu with 'Initial Deployment' selected. The 'Global Settings' section shows a dropdown menu with 'Initial Deployment' selected.

Configure the following global settings:

Option	Description
Domain	Enter the domain name to be used to activate Single Sign On (SSO) authentication for the Orchestrator. This field is required when Edge Intelligence is activated for the Customer.
Gateway Pool	Select an existing Gateway pool from the drop-down list. For more information, see Manage Gateway Pools .
Feature Access	You can select either Role Customization or Premium Service , or both the check boxes.



Option	Description
Allow Customer to Manage Software	<p>Select the check box if you want to allow an Enterprise Super User to manage the software images available for the Enterprise. Once selected, the Software Image field is displayed. 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.</p> <p> Note: You can remove an assigned image from an Enterprise, only if the image is not currently used by any Edge within the Enterprise.</p> <p>For more information, see Platform and Modem Firmware and Factory Images and Software Images.</p>
Operator Profile	<p>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.</p> <p>For more information on Operator profiles, see Manage Operator Profiles.</p>

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



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

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

Option	Description
Default Edge Authentication	<p>Choose the default option to authenticate the Edges associated with the Customer, from the drop-down list.</p> <ul style="list-style-type: none"> • Certificate Deactivated: Edge uses a pre-shared key mode of authentication. • Certificate Acquire: This option is selected by default and instructs the Edge to acquire a certificate from the certificate authority of the, 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. <p> Note: After acquiring the certificate, the option can be updated to Certificate Required.</p> <ul style="list-style-type: none"> • Certificate Required: Edge uses the PKI certificate. Operators can change the certificate renewal time window for Edges using the system property <code>edge.certificate.renewal.window</code>.
Edge Licensing	<p>Click Add and in the Select Edge Licenses pop-up window, select and assign the Edge licenses from the available list for the Enterprise.</p> <p> Note: The license types can be used on multiple Edges. It is recommended to provide your customers with access to all types of licenses to match their edition and region.</p> <p>For more information, see Edge Licensing.</p>
Feature Access	Select the Stateful Firewall check box to override the Stateful Firewall settings activated on the Enterprise Edge.

- **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 the Self Healing check box to allow the 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.
2. 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.
For more information, see [Configure Customers](#).

Clone a Customer

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

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

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

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



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

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

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

Log into the as an Operator user. Navigate to **Customers & Partners > Manage Customers**.

1. In the **Customers** page, select the customer you want to clone, and then click **Clone**.
2. The **Clone Customer** page appears.

[Customers](#) / Clone SCALE Customer

Clone SCALE Customer

▼ 1. Customer Information

Company Name / Account Number

**Additional Clone
Attributes**☐ Security Policy☐ Alert Configuration☐ Global Routing Preference☐ Cloud Subscriptions**Company
Name ***

Clone - SCALE

**Account
Number**☒ SASE Support Access ☒ SASE User Management
Access **Location****Address Line 1****Address Line 2****City****State /
Province****Zip / Postcode****Country /
Region**[NEXT](#)

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

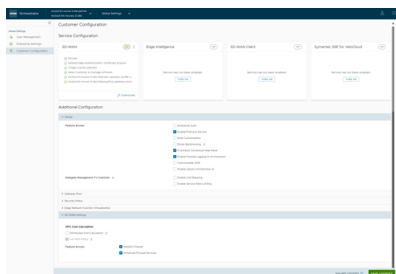
The new customer name is displayed in the **Customers** page. The customer is already configured with the cloned settings. You can click the customer name to navigate to the Enterprise portal and add or modify the configurations. For more information about customer configurations and settings, see [Configure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

Configure Customers

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

When you create a new Customer, you are redirected to the **Customer Configuration** page, where you can configure the Customer settings. You can also navigate to the **Customer Configuration** page directly from the Operator portal, by following the steps below:

1. In the monitoring and configuration options page, select a Customer, and from the top header, click **SD-WAN > Global Settings**.
2. 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**.

SD-WAN Configuration

Domain * ⓘ

5-site

Default Edge Authentication

Certificate Acquire ▾

Edge Licensing *

0 Edge Licenses selected

Allow Customer to manage software ⓘ

☐



Operator Profile *

5-site-Operator ▾

Maximum Number of Segments *

16

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 for the Customer.

Option	Description
Default Edge Authentication	<p>Choose the default option to authenticate the Edges associated to the Customer, from the drop-down menu.</p> <ul style="list-style-type: none"> • Certificate Deactivated: Edge uses a pre-shared key mode of authentication. • Certificate Acquire: This option is selected by default and instructs the Edge to acquire a certificate from the certificate authority of the, 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. <p> Note: After acquiring the certificate, the option can be updated to Certificate Required.</p> <ul style="list-style-type: none"> • Certificate Required: Edge uses the PKI certificate. Operators can change the certificate renewal time window for Edges using the system property <code>edge.certificate.renewal.window</code>.
Edge Licensing	<p>The existing Edge Licenses are displayed. Click Add to add or remove the licenses.</p> <p> Note: The license types can be used on multiple Edges. It is recommended to provide your Customers with access to all types of licenses to match their edition and region. For more information, see Edge Licensing.</p>
Allow Customer to Manage Software	<p>Select the check box if you want to allow an Enterprise Superuser to manage the software images available for the Enterprise. For more information, see the topic <i>Edge Image Management</i> in the <i>Administration Guide</i>.</p>
Operator Profile	<p>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 Manage Operator Profiles</p>
Maximum Number of Segments	<p>Enter the maximum number of segments that can be configured. The valid range is 1 to 16. The default value is 16.</p>

- 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.

Edge Network Intelligence Configuration



Domain *

5-site

Analytics Nodes

☒ unlimited☐ 0

Feature Access

☐ Self Healing


CANCEL

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 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 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*.




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



Option	Description
Global	
User Agreement Display	<p>Select either of the following from the drop-down menu:</p> <ul style="list-style-type: none"> • Inherit • Override to Hide • Override to Show <p> Note:</p> <p>This field is available only when the system property <code>session.options.enableUserAgreements</code> is set to True.</p>

Option	Description
Feature Access	<p>Provides access to the selected features. Select one or more check boxes from the below list to activate these features for the Customer:</p> <ul style="list-style-type: none"> • Enterprise Auth: By default, only the Operator can activate or deactivate two-factor authentication for an Enterprise. When you select this check box, the Enterprise Admins can configure the two-factor authentication on their own. This option also controls the activation and deactivation of Single Sign On (SSO). • Enable Premium Service: This option is selected by default. Premium Service refers to the On-Demand Remediation feature that is a core part of SD-WAN's Dynamic Multipath Optimization (DMPO). DMPO is used for all traffic that traverses a. When Premium Service is selected, the Gateway uses Forward Error Correction (FEC) for customer traffic impacted by high levels of WAN link jitter or loss, and which cannot be steered to a better quality WAN link. When Premium Service is not selected, traffic still traverses the VeloCloud Gateway and benefit from other components of DMPO like Continuous Monitoring, Dynamic Application Steering, and Secure Traffic Transmission. However, traffic impacted by high levels of WAN link jitter or loss does not benefit from error correction by the Gateway. For more information, see the topic <i>Dynamic Multipath Optimization (DMPO)</i> in the <i>Administration Guide</i>. • Role Customization: Allows an Enterprise Super user to customize the role privileges for other Enterprise users. • Route Backtracking: Allows the device to choose the best route in the order of prefix length. • In-product Contextual Help Panel: Provides access to the 'In Product Help' panel integrated within the Orchestrator. This feature is deactivated by default. An Operator must activate this option for the Enterprise Customers. • Enable Firewall Logging to Orchestrator: By default, Edges cannot send their Firewall logs to the Orchestrator. Select this check box to allow an Edge to send the Firewall logs to the Orchestrator. • Customizable QoE: Allows the Customer to configure the minimum and maximum latency threshold values for Voice, Video, and Transactional application categories of an Edge. • Enable Classic Orchestrator UI: Allows the Customer to switch from the Angular Orchestrator UI to the Classic Orchestrator UI. This option is available only when the system property <code>session.options.enableClassicOrchestrator</code> is set to True.

Option	Description
Delegate Management To Customer	<p>Allows the Customer to modify the settings of the selected property. Following two properties are always visible to the Customers:</p> <ul style="list-style-type: none"> • Enable CoS Mapping: Allows to configure CoS mapping while configuring a business policy. • Enable Service Rate Limiting: Allows to rate limit services in a business policy.
Gateway Pool	
Current Gateway Pool	Displays the current Gateway pool associated with the selected Customer. If required, you can choose a different Gateway pool available in the drop-down menu and click Save Changes .
Gateways in this Pool	Displays the Gateway details in the current pool.
Partner Hand Off	Activating the Gateway Pool option displays the Configure Hand Off section. If the Gateways available in the Gateway pool have been assigned with Partner Gateway role, you can handoff the Gateways to Partners. For details, see Configure Partner Gateway Handoff to Production Orchestrator Configure Partner Handoff.
Security Policy	
Hash	<p>By default, there is no authentication algorithm configured for the VPN header as AES-GCM is an authenticated encryption algorithm. When you select the Turn off GCM check box, you can select one of the following as the authentication algorithm for the VPN header, from the drop-down menu:</p> <ul style="list-style-type: none"> • SHA 1 • SHA 256 • SHA 384 • SHA 512
Encryption	Select either AES 128 or AES 256 as the AES algorithm's key size to encrypt data. The default encryption algorithm mode is AES 128 .
DH Group	<p>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.</p> <p> Note:</p> <ul style="list-style-type: none"> • DH Groups 19, 20, and 21 are available starting from Release 5.2.0. • It is recommended to use DH Group 14, which is the default value.

Option	Description
PFS	Select the Perfect Forward Secrecy (PFS) level for additional security. The supported PFS Groups are 2, 5, 14, 15, 16, 19, 20, and 21. PFS Groups 19, 20, and 21 are available starting in Release 5.2.0. By default, PFS is deactivated.
Turn off GCM	Select this check box to activate Hash and select an authentication algorithm for the VPN header.
IPSec SA Lifetime Time(min)	<p>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.</p> <p> Note: It is not recommended to configure low lifetime value for IPsec (less than 10 minutes), as it can cause traffic interruption in some deployments due to rekeys. The low lifetime values are for debugging purposes only.</p>
IKE SA Lifetime(min)	<p>Time when Internet Key Exchange (IKE) rekeying is initiated for Edges. The minimum IKE lifetime is 10 minutes and maximum IKE lifetime is 1440 minutes. The default value is 1440 minutes.</p> <p> Note: It is not recommended to configure low lifetime values IKE (less than 30 minutes), as it can cause traffic interruption in some deployments due to rekeys. The low lifetime values are for debugging purposes only.</p>
Secure Default Route Override	Select the check box so that the destination of traffic matching a secure default route (either Static Route or BGP Route) from a Partner Gateway can be overridden using Business Policy.
Edge Network Function Virtualization: Allows to activate NFV on the Edges and allows Customers to deploy third party VNFs on service ready Edge platforms. Currently, the service ready Edge platform models are 520v and 840. As an Operator User, when you activate the Edge NFV , the Customers can configure and deploy VNFs and VNF licenses from their network services.	
Edge NFV	Select this option to activate the ability to deploy VNFs on Edges. After deploying one or more VNFs on Edges, you cannot deactivate this option.
Security VNFs	Select the relevant check boxes, to deploy the corresponding security VNFs on Edges. For more information, see the topic <i>Security VNFs</i> in the <i>Administration Guide</i> .
SD-WAN Settings	

Option	Description
OFC Cost Calculation	<p>Select the required check box:</p> <ul style="list-style-type: none"> Distributed Cost Calculation: Select this check box to delegate route cost calculation to Edges/Gateways. <div data-bbox="906 373 959 426">  Note: This option is available only for the Edges/Gateways with version 3.4.0 and later. After activating Distributed Cost Calculation, it is recommended to refresh the routes by navigating to Configure > Overlay Flow Control in the SD-WAN service of the Enterprise portal. For more information, see Configure Distributed Cost Calculation. </div> Use NSD Policy: Select this check box to use NSD policy for route cost calculation to Edges/Gateways. <div data-bbox="906 741 959 793">  Note: This option is available only for the Edges/Gateways with version 4.2.0 and later. </div>
Multiple-DSCP tags per Flow Path Calculation	<p>This feature is used when the original user traffic is encapsulated in another tunnel (GRE/IPsec) and the DSCP labels are saved in the new IP header. The feature activates path calculation for a single flow (same source/destination) with multiple DSCP tags and offers path differentiations based on the DSCP values in the flow.</p> <p>Select the Include DSCP value as part of flow lookup check box to include DSCP values as part of flow look-up and path calculation. For more information, see Configure Path Calculation with Multiple DSCP Labels per Flow.</p> <div data-bbox="868 1276 922 1329">  Note: This field is available only when the system property <code>session.options.enableFlowParametersConfig</code> is set to True. </div>
Feature Access Stateful Firewall	<p>Select the Stateful Firewall check box to override the Stateful Firewall settings activated on the Enterprise Edge.</p>

Option	Description
Enhanced Firewall Services	<p>Select the Enhanced Firewall Services check box to activate the Enhanced Firewall Services using the Firewall functionality in.</p> <p> Note: For Enhanced Firewall Services (EFS) to work, ensure the Edge version is upgraded to 5.2.0.0.</p> <p> Note: Unselecting this option will only deactivate the EFS feature in the UI. To deactivate the EFS feature for an existing customer, you must first deactivate the EFS feature in the SD-WAN service of the Enterprise portal by navigating to Configure > Profiles/Edges > Firewall > Firewall Feature Control > Enhanced Security and then by unselecting this check box in Global Settings.</p> <p>For more information about configuring the various Enhanced Security Services and associating to a Firewall rule, see the topic <i>Configure Enhanced Security Services</i> in the <i>Administration Guide</i>.</p>

4. 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 provisioned

Gateways / Gateway - 2

Gateway - 2 ▾

Overview

Monitor

Properties

Name *

Edge

Description

Gateway Roles

Contact & Location

Contact Name *

Procedure:

To configure the handoff settings, perform the following steps:

1. Log in to the as an Operator 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:

Partner Hand Off



On

Configure Hand Off

Configure Hand Off
Segment

☒ All Gateways ⓘ

☐ Per Gateway ⓘ

Global Segment ▼

Per Customer Hand Off - Global Segment

IPv4

IPv6

Hand Off Interface

Tag Type

none

Local IP Address ⓘ

not set

Use for Private
Tunnels ⓘ

N/A

Advertise Local IP
Address via BGP ⓘ

N/A

Static Routes

not set

BFD

Not Enabled

BGP

Not Enabled

CONFIGURE BFD & BGP

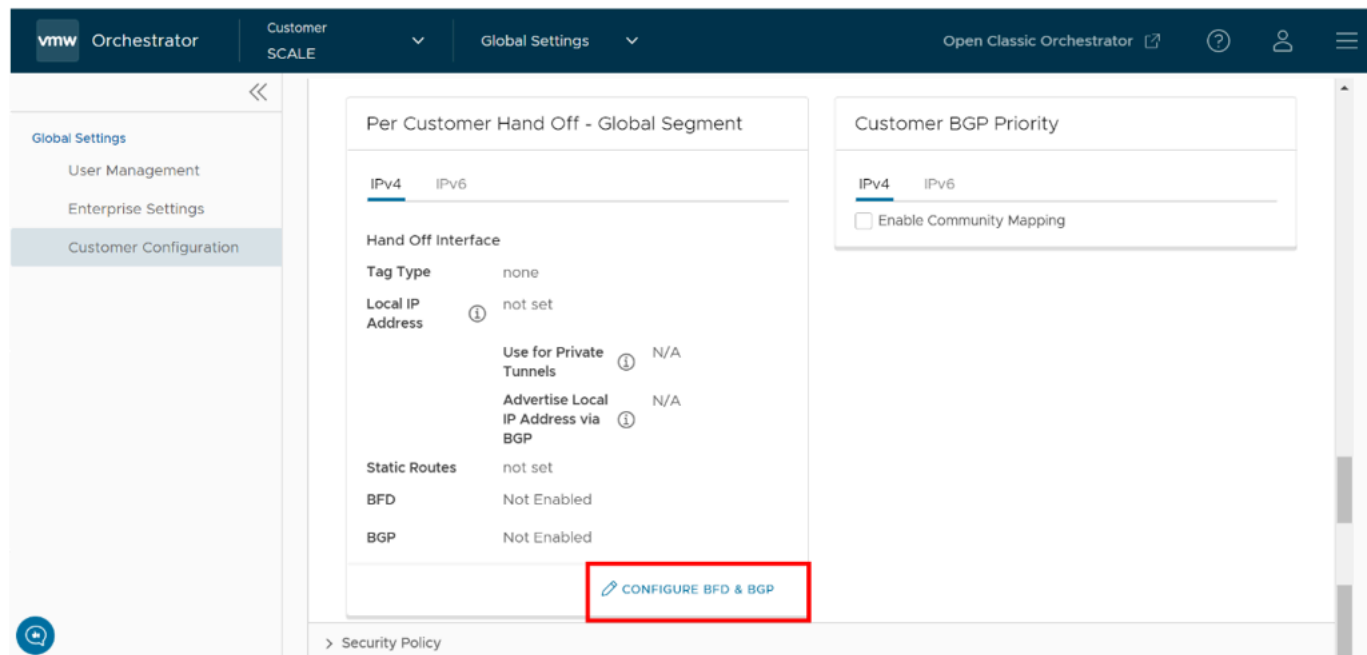
Custom

IPv4

☐ Enable

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

Next Hop IP *

BGP Local IP

BGP Inbound Filters

[None] ▼

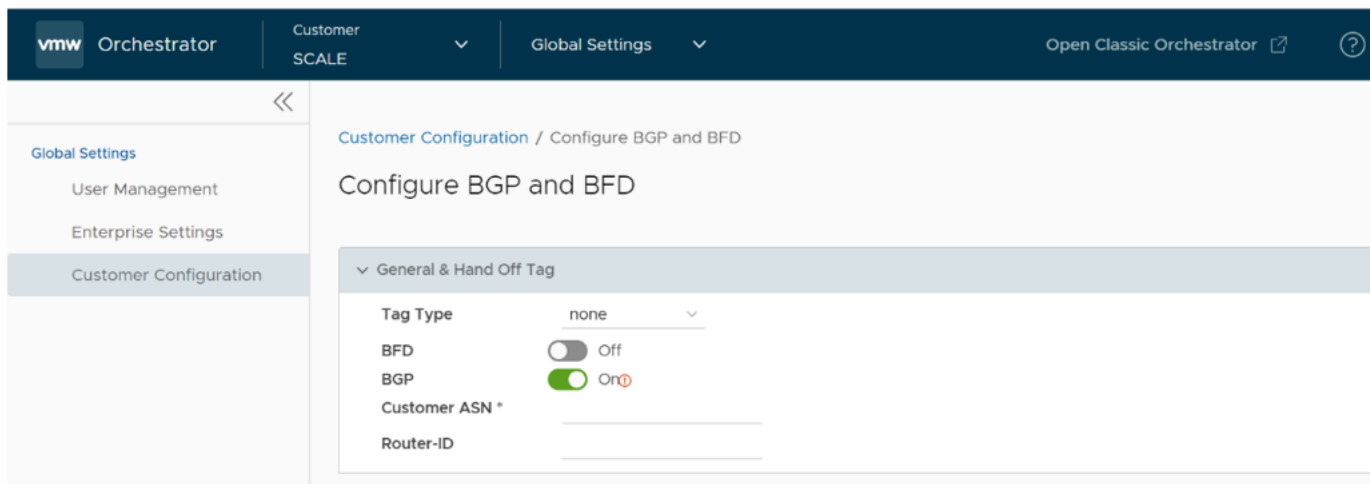
⊖ ⊕

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.

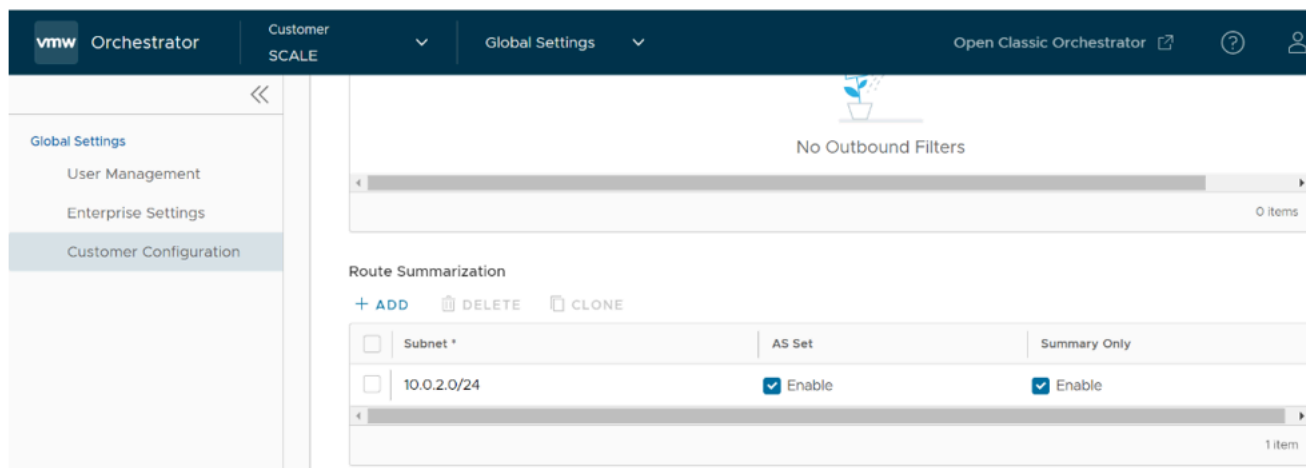
Option	Description
Hand Off Tag	
Tag Type	Choose the tag type, which is the encapsulation, in which the Gateway hands off customer traffic to the Router. The following are the types of tags available: <ul style="list-style-type: none"> • None: Untagged. Choose this during single tenant hand off or a hand off towards shared services VRF. • 802.1Q: Single VLAN tag • 802.1ad / QinQ(0x8100) / QinQ(0x9100): Dual VLAN tag
Customer ASN	Enter the Customer Autonomous System Number.
Hand Off Interface: You can configure the following settings for IPv4 and IPv6.	
Local IP Address	Enter the Local IP address for the logical Hand Off interface.
Use for Private Tunnels	Select the check box so that private WAN links connect to the private IP address of the Partner Gateway. If private WAN connectivity is activated on a Gateway, the Orchestrator audits to ensure that the local IP address is unique for each Gateway within an Enterprise.
Advertise Local IP Address via BGP	Select the check box to automatically advertise the private WAN IP of the Partner Gateway through BGP. The connectivity is provided using the existing Local IP address.
Static Routes: You can add, delete, or clone a static route.	
Subnets	Enter the IP address of the Static Route Subnet that the Gateway should advertise to the Edge.
Cost	Enter the cost to apply weightage on the routes. The range is from 0 to 255.

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	<p>Local IP address is the equivalent of a loopback IP address. Enter an IP address that the BGP neighborships can use as the source IP address for the outgoing BGP packets.</p> <p> Note: The BGP Local IP address must be from a different subnet than a handoff IP address.</p> <p>If you do not enter any value, the IP address of the Hand Off Interface is used as the source IP address.</p>
BGP Filter List	Configure BGP filters.
BGP Inbound Filters	Assign filter to inbound.
BGP Outbound Filters	Assign filter to outbound.
BGP Optional Settings	
BFD	Select the check box to subscribe to the BFD session.
Router-ID	Enter the Router ID to identify the BGP Router.
Keep Alive	Enter the BGP Keep Alive time in seconds. The default timer is 60 seconds.
Hold Timers	Enter the BGP Hold time in seconds. The default timer is 180 seconds.
Turn off AS-PATH Carry Over	Select the check box to turn off AS-PATH carry over, which influences the outbound AS-PATH to make the L3-routers prefer a path towards a PE. If you select this option, ensure to tune your network to avoid routing loops. It is recommended not to select this check box.
MD5 Auth	Select the check box to activate BGP MD5 authentication. This option is used in a legacy network or federal network, and is used as a security guard for BGP peering.
MD5 Password	<p>Enter a password for MD5 authentication.</p> <p> Note: Starting from the 4.5 release, the use of the special character "<" in the password is no longer supported. In cases where users have already used "<" in their passwords in previous releases, they must remove it to save any changes on the page.</p>

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 Distributed Cost Calculation

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

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

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



Note:

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

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

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

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

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

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

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

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



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

To configure Distributed Cost Calculation for a customer:

1. In the Operator portal, navigate to **Manage Customers**.
2. Select a customer and either click **Edit Customer System Settings** or click the link to the customer.
3. In the Enterprise portal, go to **Global Settings > Customer Configuration**.

vmw Orchestrator Customer Global Settings

Global Settings
User Management
Enterprise Settings
Customer Configuration

Customer Configuration

Service Configuration

SD-WAN

Additional Configuration

- > Global
- > Gateway Pool
- > Security Policy
- > Edge Network Function Virtualization
- ✓ SD-WAN Settings
 - OFC Cost Calculation**
 - ☒ Distributed Cost Calculation ⓘ
 - ☐ Use NSD Policy ⓘ Activate if your enterprise uses Non SD-WAN Destinations and you want to route traffic to those sites as well. As with DCC for network routes, this is a...
 - Feature Access**
 - ☒ Stateful Firewall
 - ☐ Enhanced Firewall Services

DISCARD CHANGES ⓘ

4. In the **Customer Configuration** page, navigate to the **Additional Configuration > SD-WAN Settings > OFC Cost Calculation** section and configure the following:

- Select the **Distributed Cost Calculation** checkbox to delegate the cost calculation of routes to Edges and Gateways.
- Select the **Use NSD Policy** checkbox to use the Non SD-WAN Destination policy for route cost calculation of Edges and Gateways. This option is available only for Edges and Gateways that are running Software version 4.3.0 or later.

5. Click **Save Changes**.



Note: After enabling **Distributed Cost Calculation**, it is recommended to refresh the routes in the **Overlay Flow Control** page in the **SD-WAN** service of the Enterprise portal.



Note: When an Enterprise has **Distributed Cost Calculation** activated and a user tries to deactivate the software update in the **Operator Profile** page, then the user must ensure that, in future, no Edges in

the Enterprise are downgraded to software image versions lower than 3.4.0. If one or more Edges in the Enterprise is using software image version below 3.4.0, the Enterprise traffic may take a sub-optimal path. The sub-optimal path will be corrected only when the Edge is upgraded to 3.4.0 or later versions.

The following are some of the scenarios in which the software versions can change and the user must make sure the Edges are using the software image version 3.4.0 or later:

- **Factory Reset** - When an Edge is reset to factory settings, it restores the software version of the Edge to factory image version which can be below 3.4.0.
- **Edge Activation** - When an Edge is activated, it may come up with software versions below 3.4.0.

Once **Distributed Cost Calculation** is activated, all the dynamic routes are assigned with new preferences and advertise action based on the Distributed Cost Calculation and the new information is propagated across the Enterprise Network.

The Orchestrator is no longer actively involved in the route preference calculation and instead the routes are properly inserted in order by the Edge and Gateway instantly upon learning them and then these preferences are conveyed to the Orchestrator.

The Overlay Flow Control policy is sent to Edges and Gateways in Control Plane Configuration updates. Edges and Gateways send the routes with computed cost and advertise action to the Orchestrator. Edges and Gateways handle the order of the routes based on the cost and route attributes.

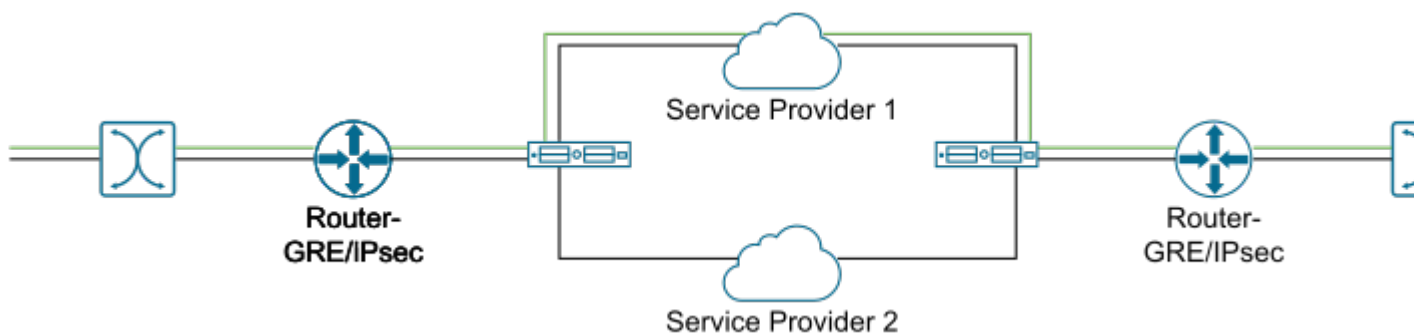
To view a summary of all the routes in your network, click **Configure > Overlay Flow Control** in the **SD-WAN** service of the Enterprise portal. You can view the routes and advertise action in the **Overlay Flow Control** page. For more information, see the topic *Overlay Flow Control* in the *VeloCloud SD-WAN Administration Guide*.

Configure Path Calculation with Multiple DSCP Labels per Flow

An Edge classifies a traffic flow based on the first packets in the flow. You can create business policies with application based on Differentiated Service Code Point (DSCP) and with different DSCP markings to determine the flow treatment.

By default, an Edge classifies a flow based on the first few packets received in the flow. Business Policy and QoS marking determine the flow treatment. Once the flow is classified, an entry with five tuple information of the flow is created in the flow cache table. Subsequent packets in the flow will use the five-tuple lookup against the flow cache table.

For network topologies with Layer 3 network devices doing encapsulation and/or encryption before the traffic arrives at the Edge, this creates a challenge for the Edge to forward traffic based on the Business Policy. The traffic from the end users is multiplexed into single flow with the same source and destination IP addresses, and protocols by the Layer 3 encapsulation/encryption device, as illustrated in the following image.



The impact of multiplexing end user flows into a single tunnel creates polarization of flow forwarding using the five tuples of flow cache table, which results in WAN links not being utilized.

The Path Calculation with Multiple DSCP Labels per Flow allows the DSCP value to be included, in addition to the five tuples, as part of the flow cache table lookup. Use the path calculation with multiple DSCP tags when the original user traffic is encapsulated in another tunnel like GRE or IPsec, and DSCP labels are preserved in the new IP header.

This option enables path calculation for a single flow with multiple DSCP labels, which consists of same source and destination IP addresses, and offers path differentiations based on the DSCP labels in the flow.

When you enable the **Multiple-DSCP tags per Flow Path Calculation**, the Edges can differentiate the traffic flows based on the DSCP marked labels.

To enable Multiple-DSCP tags per Flow Path Calculation:

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



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

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



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

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

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

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

Limitations:

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

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

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


Activate on a

is a vendor agnostic AIOps solution focused on the enterprise Edge that ensures end-user and Internet of Things (IoT) client performance, security, and self-healing through wireless and wired LAN, SD-WAN, and Secure Access

Service Edge (SASE). Integration of with helps extend visibility from SD-WAN to branch, campus, and home. This integration helps to get 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 Intelligence Configuration Guide*.

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	<p>Activate the Analytics service on a . By default, Analytics is activated for Cloud-hosted Orchestrators.</p> <p> Note: For On-prem Orchestrators, this system property is set to <i>false</i> by default. Ensure to change the value to <i>true</i> if you want to activate the Edge Intelligence feature.</p>	<i>true</i>
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 .
service.analytics.configEndpoint	Configuration endpoint of Analytics service	<ul style="list-style-type: none"> 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.

System Property	Description	Value
service.analytics.analyticsEndpointStatic	IP analytics endpoint of Analytics service	<ul style="list-style-type: none"> 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.analyticsEndpointStatic

Activate Analytics for a New Customer

When creating a new SD-WAN customer (Enterprise or Partner), allows Operator Super Users and Operator 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.

Ensure that the following system properties are properly set in the :

- session.options.enableEdgeAnalytics
- service.analytics.apiURL
- service.analytics.apiToken
- service.analytics.configEndpoint
- service.analytics.analyticsEndpointStatic
- service.analytics.analyticsEndpointDynamic

For more information, see Activate on a.

To activate Analytics for a new customer, see Create New 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 Operator Super Users and Operator Standard Admins to activate Analytics for an existing SD-WAN customer (Enterprise or Partner).

Ensure that the following system properties are properly set in the :

- session.options.enableEdgeAnalytics
- service.analytics.apiURL
- service.analytics.apiToken

For more information, see [Activate on a](#).

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 Enterprise customer, allows Operator Super Users and Operator Standard Admins, 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 an Operator user.
2. Navigate to **Customers & Partners > Manage Customers**, and then click **New Customer**.

The **New Customer** page appears.

Customers / New Customer

New Customer

>

Customer Information

Company Name / Account Number / Location

>

Administrative Account

Username / Password / Contact Information

>

3. Services

Services customer has purchased

Service Access *

☒ SD-WAN
☒ Edge Network Intelligence (ENI) ⓘ
☐ Cloud Web Security (CWS)
☐ Secure Access

Global Settings

Domain * ⓘ

VeloCust

Gateway Pool *

5-site-GatewayPool

Feature Access

☐ Role Customization
☐ Premium Service

Allow Customer to Manage Software

☐

Operator Profile *

Initial Segmented Operator Profile

SD-WAN

Default Edge Authentication

Certificate Acquire

Edge Licensing *

ENTERPRISE | 10 Mbps | North America, Europe Middle East and Africa | 12 Months

[EDIT](#)

VMware SD-WAN by VeloCloud ENTERPRISE edition, applicable to the North America, Europe Middle East and Africa regions, has a bandwidth up to 10 Mbps and is valid for 12 Months

Feature Access

☒ Stateful Firewall

Edge Network Intelligence (ENI)

Nodes

☒ Unlimited
☐ 5



Feature Access

☒ Self Healing

☐ Add another customer

ADD CUSTOMER

CANCEL

- Enter all the mandatory Customer information and Administrative account details and click **Next**.
- 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.
- 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 www.arista.com/en/support/product-documentation.
- 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 Enterprise customer, perform the following steps:

1. Log in to the as an Operator user.
2. In the Operator 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.

Edge Network Intelligence Configuration ×

Domain * ⓘ

5-site

Analytics Nodes

☒ unlimited
 ☐ 0

Feature Access

☒ Self Healing

CANCEL

UPDATE

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.

Manage Partners

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

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

Customers & PartnersAdministrationGateway ManagementEdge Image Management

<<

Customers & Partners

Monitor Customers

Manage Partners

Manage Customers

Manage Partners

Q Search

+ NEW PARTNER

EDIT

DELETE

+ ADD OPERATIONS


<input type="checkbox"/>	Partner	Operate Gateways
<input type="checkbox"/>	partner1	Enabled

COLUMNS

REFRESH

2. 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.

Option	Description
New Partner	Click this option to add a new Partner. For more information, see Create New Partner.
Edit	This option takes you to the Partner Overview page in the Partner portal, where you can edit the Partner Capabilities, Available Software Images, and Gateway Pool of the selected Partner. For more information, see Configure Partner.
Delete	Deletes the selected Partners. Enter the number of selected Partners in the pop-up window, and then click Delete .  Note: Ensure that you have removed all the Customers associated to the selected Partner, before deleting the Partner.
Add Operator Profile	Assigns an Operator profile to the selected Partners, which specifies the network settings managed by . In the Add Profiles to Selected Partners pop-up window, select a profile and click the arrow to add it. Click Save . For more information, see Manage Operator Profiles
More	Click this option, and then click Download to download the list of Partners' profiles in a CSV format.

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

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

Create New Partner

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

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



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


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


New Partner


▼  Partner Information

Name *

test

Domain 

☒ SASE Support Access 

☒ Grant Gateway Management Access 

Location

Address Line 1

97 Columbia Place

Address Line 2

Campbell Park

City

Milton Keynes

State / Province

Country

United Kingdom

Zip / Postcode

NEXT


▼  Initial Partner Admin Account


Us

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



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

Option	Description
Partner Information	
Name	Enter the Partner name.
Domain	Enter the domain name of the Partner.
SASE Support Access	This option is selected by default and grants access to the Support to view, configure, and troubleshoot the settings of the Partner.
Grant Gateway Management Access	Select the checkbox to allow the Partner to create and manage the Gateways.
Location	Enter relevant address details in the respective fields.
Initial Partner Admin Account	
Username	Enter the username in the user@domain.com format.
Password	Enter a password for the Partner.  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	Re-enter the password.
First Name, Last Name, Phone, Mobile Phone	Enter relevant details in the respective fields.
Contact Email	Enter the email address. The alerts on service status are sent to this email address.
Default Properties	
Gateway Pool	Click Add to select the from the available list. After adding the , you can click Edit to add or remove the pools. For more information on , see Manage Gateway Pools.
Software Image	Click Add to select the Software Image from the available list. After adding the Software Image, you can click Edit to add or remove the images. For more information on Software Images, see Firmware and Software Images with New Orchestrator UI.

Option	Description
Edge Licensing	<p>Click Add to select the licenses from the available list. After adding the licenses, you can click Edit to add or remove the licenses. This option is available only when the value of System Property <code>session.options.enableEdgeLicensing</code> is set to True.</p> <p> Note: The license types can be used on multiple . It is recommended to provide the Partners with access to all types of licenses to match their edition and region. For more information, see Edge Licensing.</p>

3. Select the **Add Another Partner** checkbox, to create another new Partner, or directly click the **Add Partner** button.

The new Partner name is displayed on the **Manage Partners** page. You can click the Partner name to navigate to the Partner portal and add more configurations to the Partner. For more information, see Configure Partner.

Configure Partner

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

To configure Partner information for an existing Partner:

1. In the Operator portal of the , click **Manage Partners**, and then click the Partner name to navigate to the Partner portal and add more configurations to the Partner.

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

Customers & Partners Gateway Management Edge Management **Administration**

Administration

- Partner Events
- Partner Configuration**
- Partner Settings
- User Management

Partner Overview

Partner Capabilities

☐ Enable Gateway Management
☒ Enable Edge License
☐ Enable Role Customization

Classic Orchestrator Access

For all Customers *

Turn On
 Turn OFF
 ✓ Keep Existing

Current Access Status ON 0 OFF 1 [VIEW](#)

[SAVE](#) [CANCEL](#)

Available Software Images

Software Image

[EDIT](#)

Initial Segmented Operator Profile

Segmented operator profile to get started with

Software Images: None (do not update)

Modem Firmware: None (do not update)

Platform Firmware: None (do not update)

Factory Image: None (do not update)

Used By: 1 Customer 0 Edges

Gateway Pool

Gateway Pools

[EDIT](#)

Default Pool




gateway pool used when none is explicitly assigned to an enterprise

Used By: 1 Customer 2 Gateways

Other Settings

User Agreement Display [Override to Hide](#) [EDIT](#)

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

Option	Description
Partner Capabilities	<p>Clicking Edit allows you to select the following capabilities for the current Partner:</p> <ul style="list-style-type: none"> • Enable Gateway Management – Allows the Partner users to create, configure, and manage their own Gateways. • Enable Edge License – Allows the Partner users to manage their Edge Licenses. • Enable Role Customization – Allows a Partner Super user to customize the service permissions of other Partner users and Enterprise users of the Partner.
Classic Orchestrator Access	<p>Displays the Classic Orchestrator accessibility settings for the Partner Customers.</p> <p>For All Customers: An Operator can choose any one of the following options from the drop-down menu:</p> <ul style="list-style-type: none"> • Turn On: Allows Partner Customers to access the Classic Orchestrator. • Turn Off: Does not allow Partner Customers to access the Classic Orchestrator. • Keep Existing: This option indicates no change to the settings. <p>Current Access Status: Displays the access information (On/Off) for the existing Partner Customers. Click View to view the list of names and statuses of the Partner Customers.</p> <p> Note: You must refresh the page to see the Classic Orchestrator UI button at the top right of the screen.</p>
Available Software Images	<p>Displays all the software images assigned to the Partner. Click Edit to add or remove the software images in the list.</p> <p> Note: You cannot remove the software images that are assigned to a Customer.</p>
Gateway Pool	<p>Displays the Gateway pools associated with the selected Partner. Click Edit to add or remove the Gateway pools in the list.</p> <p> Note: You cannot remove the Gateway Pools that are assigned to a Customer.</p>

Option	Description
Other Settings	<p>Displays the settings of the User Agreement only if you have activated the User Agreement feature. By default, the User Agreement feature is not activated. To enable the User Agreement feature, navigate to the System Properties in the Operator portal, and set the value of the <code>session.options.enableUserAgreements</code> system property as True.</p> <p>You can choose to override the default display settings of the User Agreement, by clicking the Edit button and selecting relevant option from the User Agreement Display drop-down menu. By default, the Customer inherits the display mode set in the system properties.</p>

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

Partner Settings

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

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

Partner Settings

▼ General Information

Name *

abc

Domain

Enter domain

Example: vmware

Description

Enter Description
(Optional)

▼ Information Privacy Settings

Operator Support Access

Allow Support Access



On

VMware Support is granted access to view your events. Granting VMware Support access to your customers is individual

▼ Partner Business Contact Information

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

Primary Business Contact

Contact Name

test123

Contact Email

test@vmware.com

Phone


+1 ▼ 12345889990

Mobile Phone

+1 ▼ 12345678990

Primary Business Location

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	<p>This option is activated by default, indicating that Support can view Partner level events.</p> <p> Note: When deactivated, the Operator can no longer edit the settings of the selected Partner. Only the Partner can activate this setting from the Partner portal.</p>
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**.


Manage Operators

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

Monitor Operator Events

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

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


Orchestrator

Customers & Partners
Orchestrator
Gateway Management
Edges

<<

Administration

Operator Events

Operator Profiles

User Management

Events

Past 2 Weeks

Event	User
Auto Rate-Limit Disabled	
Auto Rate-Limit Enabled	
Auto Rate-Limit Disabled	
Auto Rate-Limit Enabled	
Auto Rate-Limit Enabled	
Auto Rate-Limit Enabled	

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

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

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

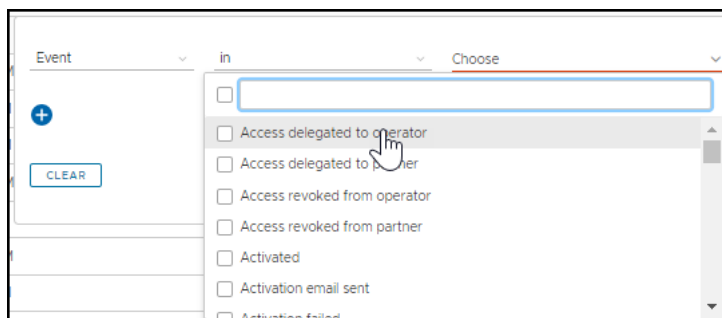
Event Detail

```
Auto rate-limit enabled peers: [{"name": "b4-edge1",
"enterprise": "perf-3s-2", "rate_limit_percent": "4.9805"},
{"name": "b6-edge1", "enterprise": "perf-3s-3",
"rate_limit_percent": "4.9805"}, {"name": "b1-edge1",
"enterprise": "perf-3s", "rate_limit_percent": "4.9805"}]
```

CLOSE

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 then click the drop-down arrow next to the field to view the list of Operator Events available and to filter by specific Events.



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



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

Manage Operator Profiles

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

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

- Firmware Platform images for 6x0, 7x0, and 3x00 (3400/3800/3810) Edge device models

- Firmware Modem images for 510-LTE (Edge 510LTE-AE, Edge 510LTE-AP) and 610-LTE (Edge 610LTE-AM, Edge 610LTE-RW)
- Factory images for all physical devices

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

See Platform Firmware and Factory Images with New Orchestrator UI for more information.

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

Customers & Partners

Administration

Gateway Management

Edge Image Management

<<

Administration

Operator Events

Operator Profiles

Operator Profiles

Q Search

i

▼

+ NEW

DUPLICATE

DOWNLOAD

REMOVED

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	Initial Operator Profile	Operator profile to g
<input type="checkbox"/>	Initial Segmented Operator Profi...	Segmented operator with
<input type="checkbox"/>	3-site-Operator	


COLUMNS

REFRESH



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

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

Option	Description
Search	Enter a search term to search for a matching text across the page. You can use the Advanced Search option to narrow down the search results.
New	Click this option to create a new Operator Profile. Enter the desired name and description in the dialog and click Create .
Duplicate	Click this option to create a copy of the selected Operator Profile. You can update the name and description.
Download	Click this option to download the csv file containing a list of all or the selected Operator Profiles.
Remove	Click this option to remove the selected Operator Profile(s) from all the associated Partners and Customers. You can complete this action only after you enter the correct number of profiles selected.
Delete	<p>Click this option to delete the selected profile(s). You can complete this action only after you enter the correct number of profiles selected.</p> <p> Note: You cannot delete a profile that has already been assigned to a Customer or Partner.</p>
Columns	You can select the desired columns to be displayed in the table.
Refresh	Click this option to refresh the page.



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

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

Initial Operator Profile Used by 0 Customers

Profile Settings

Name * Initial Operator Profile

Description Operator profile to get started with

If this profile is in a Partner's list of assigned profiles, this description is visible to their Customers.

Management Settings

Orchestrator Address	IP Address	Heartbeat
Orchestrator IPv4 Address	10.81.114.61	Time Slice
Orchestrator IPv6 Address		Stats Uplo

Gateway Selection

Gateway Mode ☒ Dynamic ☐ Static ⚠



Application Map Assignment


JSON File * Initial Application Map Mon Oct 10 2022 06:38:03 G...

> Software Version ☐ Off i

Firmware Version

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

Option	Description
Profile Settings	
Name	Edit the existing name of the Operator Profile.
Description	Edit the existing description of the Operator Profile.
Management Settings	
Orchestrator Address	Choose to use either FQDN or IP address as the Orchestrator Address. If you select FQDN, enter the FQDN address.
Orchestrator IPv4 Address	Enter the IPv4 address to be used as Orchestrator Address.
Orchestrator IPv6 Address	Enter the IPv6 address to be used as Orchestrator Address.
Heartbeat Interval (s)	<p>Displays the time interval between the heartbeat messages sent from the to. The default value is 30 seconds and minimum interval must be 10 seconds. If an does not receive two heartbeats continuously, then the is marked as Down.</p> <p> Note: When you modify the heartbeat interval, make sure to update the Offline Alert Notification Delay time accordingly, to avoid sending unnecessary alerts.</p>
Time Slice Interval (s)	Displays the time interval over which the monitoring data is collected for a flow. The default value is 300 seconds.
Stats Upload Interval (s)	Displays the time interval for uploading the monitoring data. All the data for each Timeslice is collected during the Stats Upload Interval and then uploaded. The default value is 300 seconds.
Gateway Selection	
Gateway Mode	<p>By default, the selection is Dynamic and the are chosen dynamically from the. Ensure that the consists of at least two, for the selection to be efficient.</p> <p>Select the check box to make the selection as Static. For the Static selection, you must specify the Primary. You can also enter an optional Secondary.</p> <p> Note: Use the Static Selection only for testing or debugging purposes. You must not use this option for-to- VPN or Partner handoff configurations.</p>
Application Map Assignment	
JSON File	By default, the initial Application Map is assigned to the Operator Profile. You can choose a different Application Map from the drop-down list. For more information, see Application Maps.

Option	Description
Software Version: You can choose to push the latest Software Image to the. By default, no updates are applied to the devices. Activate the toggle button to display the following fields.	
Version	Choose the Software Image from the drop-down list. For more information on the Software Images, see Software Images.
Update Duration	Select the Update Duration check box, and then enter the duration time in minutes. When you activate this option, the updates all the devices associated with the Enterprise customer within the specified time duration.
Firmware Version	
 Note: This section is available only for Edge versions 5.0.0 and above. This section is activated only when we deactivate the Software Version section.	

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

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

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



Note:

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



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

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

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

Table 1: Supported Images and Compatibility Matrix

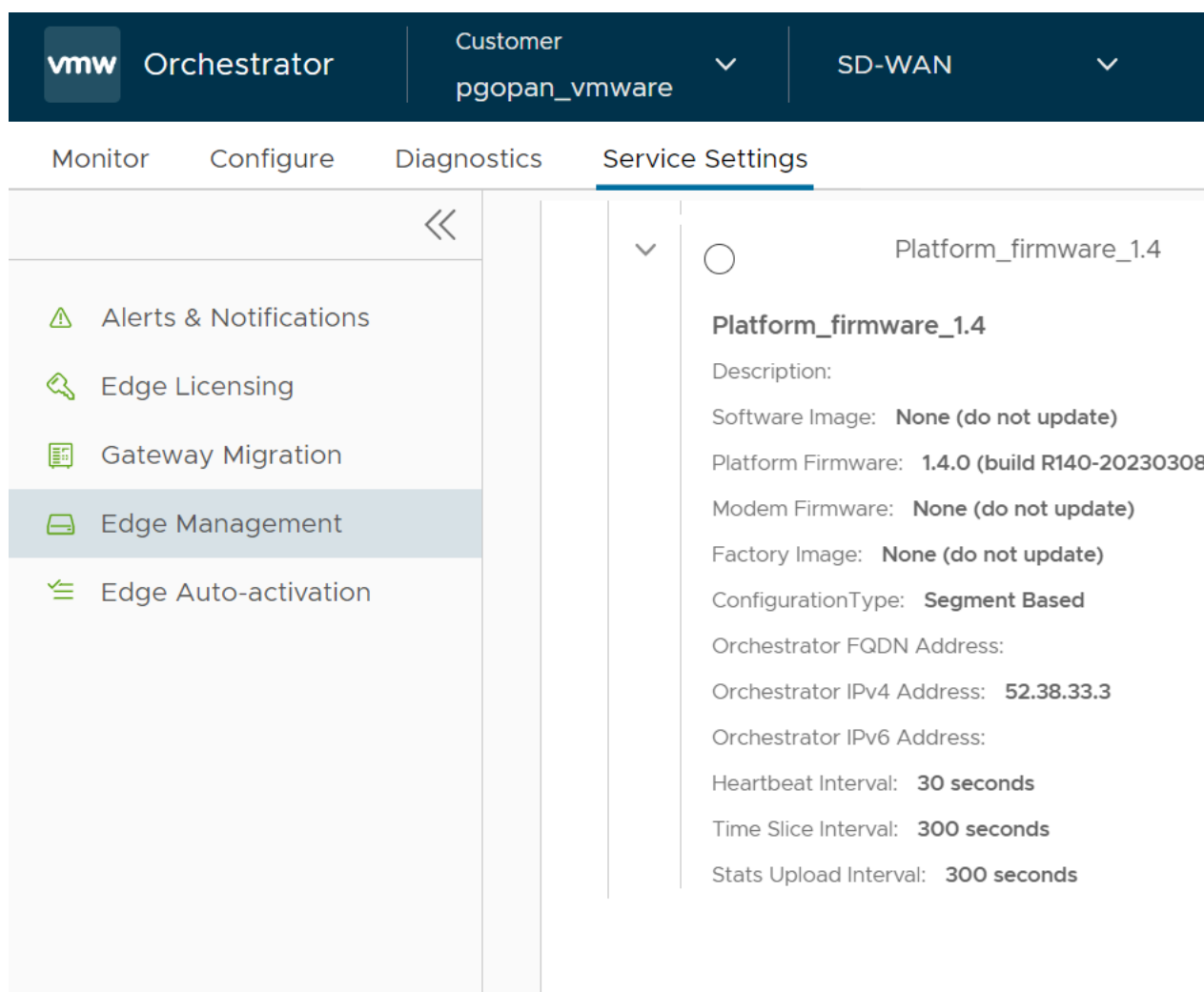
Device Family	Software Image (Device Family)	Platform Firmware (Device Family)	Modem Firmware (Device Family)	Factory Default (Device Family)
• EDGE 6x0	• EDGE 6X0	EDGE 6X0	610-LTE	• EDGE 6X0
EDGE 3x00	<ul style="list-style-type: none"> • EDGE 8X0 • EDGE 1000 • EDGE 3X00 	Edge 3X00	NA	<ul style="list-style-type: none"> • EDGE 8X0 • EDGE 1000 • EDGE 3X00
510LTE	<ul style="list-style-type: none"> • Edge 510LTE-AE • Edge 510LTE-AP 	NA	<ul style="list-style-type: none"> • Edge 510LTE-AE • Edge 510LTE-AP 	Edge 5X0
610-LTE	<ul style="list-style-type: none"> • Edge 610LTE-AM • Edge 61LTE-RW 	Edge 6X0	<ul style="list-style-type: none"> • Edge 610LTE-AM • Edge 61LTE-RW 	Edge 6X0
EDGE 7x0 (EDGE 710-W, EDGE 710-5G, EDGE 720, EDGE 740)	EDGE 7x0	EDGE 7x0	EDGE 7x0	EDGE 7x0

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



Note:

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



vmw Orchestrator

Customer
pgopan_vmware

SD-WAN

Monitor Configure Diagnostics **Service Settings**

Platform_firmware_1.4

Platform_firmware_1.4

Description:

Software Image: **None (do not update)**

Platform Firmware: **1.4.0 (build R140-20230308)**

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

Factory Image: **None (do not update)**

ConfigurationType: **Segment Based**

Orchestrator FQDN Address:

Orchestrator IPv4 Address: **52.38.33.3**

Orchestrator IPv6 Address:

Heartbeat Interval: **30 seconds**

Time Slice Interval: **300 seconds**

Stats Upload Interval: **300 seconds**

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

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



Note: It is important that you update the software version first. Then, after completion, update the Factory image or Platform or Modem Firmware. Do not update the software version and the firmware at the same time.



Note: The **Version** drop-down menu displays the software images that are deprecated with a flag, but you will not be able to select the deprecated images.

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

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

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



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

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

Related Links

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

User Management - Operator

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

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

Customers & Partners

Orchestrator

Gateway Management

Edge Image Management

<<

Administration

Operator Events

Operator Profiles

User Management

User Management

Users

Roles

Service Permissions

Authentication

Q Search

i

Y

+ NEW USER

MODIFY

PASSWORD RESET

D

	Username	Bastion State
<input type="checkbox"/>	operator@velocloud.net	UNCONFIGURED
<input type="checkbox"/>	super@velocloud.net	UNCONFIGURED
<input type="checkbox"/>	business@velocloud.net	UNCONFIGURED
<input type="checkbox"/>	support@velocloud.net	UNCONFIGURED

COLUMNS

REFRESH

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

To access the **Users** tab:

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

Customers & Partners Orchestrator Gateway Management Edge Image Management

<<

Administration

Operator Events

Operator Profiles

User Management

User Management

Users

Roles

Service Permissions

Authentication

Q Search

i

▼

+ NEW USER

✎ MODIFY

🔑 PASSWORD RESET

🗑️

<input type="checkbox"/>	Username	Bastion State
<input type="checkbox"/>	operator@velocloud.net	UNCONFIGURED
<input type="checkbox"/>	super@velocloud.net	UNCONFIGURED
<input type="checkbox"/>	business@velocloud.net	UNCONFIGURED
<input type="checkbox"/>	support@velocloud.net	UNCONFIGURED

☰ COLUMNS

🔄 REFRESH

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

Option	Description
New User	Creates a new Operator user. For more information, see Add New User.

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

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

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 New User

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

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

The following screen appears:

▼

✓

General Information

User Name / Set Password / Contact Information

Authentication ⓘ

☒ Local

☐ Remote

Username *

test@vmware.com

Contact Email * ⓘ

test@vmware.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 service

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


🔍 Search

ⓘ

🔼

		Role	Descriptions
<input type="radio"/>	»	Operator Superuser 🔒	Can view, edit and create additional operators
<input type="radio"/>	»	Operator Standard Admin 🔒	Can view and manage Operator customers
<input type="radio"/>	»	Operator Business 🔒	Can create and manage customer accounts
<input type="radio"/>	»	Operator Support 🔒	Can monitor Edges and activity on the cloud

4. Enter the following details for the new user:

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



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

5. Select the **Add another user** check box if you wish to create another user, and then 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.

API Tokens

You can access the Orchestrator APIs using tokens instead of session-based authentication. As an Operator Superuser, you can manage the API tokens. You can create multiple API tokens for a user.



Note: For Enterprise Read Only users and MSP Business Specialist users, token-based authentication is not activated.

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



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

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

To manage the API tokens:

1. In the Operator portal, navigate to **Administration > User Management > Users**.
2. Select a user and click **Modify** or click the link to the username. Go to the **API Tokens** section.

API Tokens

 Search

[+ NEW API TOKEN](#)
[↓ DOWNLOAD API TOKEN](#)
[⊗ REVOKE API TOKEN](#)
[↓ CSV](#)

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

3. Click **New API Token**.

New Token

[View documentation](#)


Name *

Description

Lifetime * Months

[CANCEL](#)
[SAVE](#)

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 download the token, select the token, and then click **Download API Token**.
7. To deactivate a token, select the token, and then click **Revoke API Token**. The status of the token is displayed as **Revoked**.
8. Click **CSV** to download the complete list of API tokens in a .csv file format.
9. When the Lifetime of the token is over, the status changes to **Expired**.



Note: Only the user who is associated with a token can download it and after downloading, the ID of the token alone is displayed. You can download a token only once. After downloading the token, the user can send it as part of the Authorization Header of the request to access the Orchestrator API.

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 } }'
```

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

- 'Users' topic in the *Administration Guide*
- 'Users' topic in the *Partner Guide*

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 functionality. 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 an Operator user:

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

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

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

To access the **Roles** tab:

- 1. In the Operator portal, click **Administration** from the top menu.
- 2. From the left menu, click **User Management**, and then click the **Roles** tab. The following screen appears:

Customers & PartnersOrchestratorGateway ManagementEdge Image Management

<<

Administration

- Operator Events
- Operator Profiles
- User Management

User Management

UsersRolesService PermissionsAuthentication

Roles

Q Search

i

▼

+ ADD ROLE

✎ EDIT

📄 CLONE ROLE

🗑 DELETE

<input type="checkbox"/>		Role	Des
<input type="checkbox"/>	⋮ >>	Operator Standard Admin 🔒	Can
<input type="checkbox"/>	⋮	Operator Superuser 🔒	Can
<input type="checkbox"/>	⋮ >>	Operator Business 🔒	Can
<input type="checkbox"/>	⋮ >>	Operator Support 🔒	Can

☰ COLUMNS

🔄 REFRESH

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

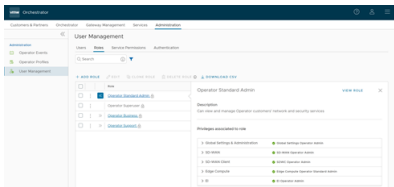
Option	Description
Add Role	Creates a new custom role. For more information, see Add Role.

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



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

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



- 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
- The following are the other options available in the **Roles** tab:

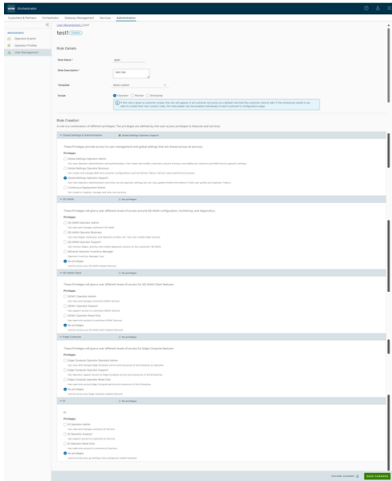
Option	Description
Search	Enter a search term to search for the matching text across the table. Use the advanced search option to narrow down the search results.
Columns	Click and select the columns to be displayed or hidden on the page.
Refresh	Click to refresh the page to display the most current data.

Add Role

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

- In the Operator portal, click **Administration** from the top menu.
- From the left menu, click **User Management**, and then click the **Roles** tab.
- Click **Add Role**.

The following screen appears:



4. 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.
Template	Optionally, select an existing role as template from the drop-down list. The privileges of the selected template are assigned to the new role.
Scope	Select Operator , Partner , or Customer as the scope for the new role. The new role appears in all the accounts for the selected user, as a default role. If an Operator creates a role for a Partner, it appears in the Partner's roles' list and can be edited only by an Operator and a Partner user who has the required permissions.
Role Creation: The options in this section vary depending on the selected Scope .	
Global Settings & Administration	These privileges provide access to user management and global settings that are shared across all services. Choosing one of the privileges is mandatory. By default, Global Settings Operator Support is selected for the Operator scope.
SD-WAN	These privileges provide the Operator, Partner, or Enterprise Administrator with different levels of read and/or write access around SD-WAN configuration, monitoring, and diagnostics. You can optionally choose an SD-WAN privilege. The default value is No Privileges .
SD-WAN Client	These privileges provide the Operator, Partner, or Enterprise Administrator with different levels of read and/or write access around SD-WAN Client features. You can optionally choose a SD-WAN Client privilege. The default value is No Privileges .

Option	Description
Edge Compute	These privileges provide the Operator, 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 Operator, 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 .

5. 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.

Enterprise Security Admin Role

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

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

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

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

Create a Permission

To create a new permission, follow the below steps:

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

3. Click **New Permission**. The following screen

[Service Permissions](#) / Enterprise Security Admin

Enterprise Security Admin

Permission Details

Name *

Enterprise Security Admin

Description

Enter Description
(Optional)

Scope *

☐ Operator ☐ Partner ☒ Enterprise

Service *

SD-WAN


Privilege Bundle *

SD-WAN Security Enterprise Admin

Privileges

Privileges	Description
Authentication Service	Privilege controlling the creation and configuration of hosted 802.1x service providing LAN-side user authentication
Client Device	This privilege controls visibility to unique the identifiers (IP or MAC address) of LAN-side client devices
Client User	This privilege control visibility to potentially PII data in flow statistics
Cloud Security Service	Privilege controlling the creation and configuration of third party cloud security services to which traffic can be steered by business policy
Cloud Subscription Service	Privilege granting the ability to view and manage the configuration of access to IAAS providers, such as Azure, AWS and Google Cloud
Customer Alert Notification	Privilege granting the ability to view and manage customer alert configuration
Customer Edge Settings	Privilege granting the ability to activate or deactivate Configuration Updates for an Edge.
Customer General Information	Privilege granting the ability to choose a default certificate for an Edge, and activate or deactivate Secure Edge Access.
Customer Keys	Privilege granting the ability to view and manage enterprise security keys such as edge administrator credentials and IPSEC keys
Customer Privacy Settings	Privilege granting the ability to control access to sensitive Customer data.

4. 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 Enterprise as the scope.
Service	<p>Select SD-WAN service to create the SD-WAN Enterprise Security Admin service permission.</p> <p>Select Global Settings service to create the Global Settings Enterprise Admin service permission.</p>
Privilege Bundle	<p>Select an appropriate privilege bundle from the drop-down menu. The privileges are populated depending on the selected Service.</p> <p> Note: Operator Superuser role is not available.</p>
Privileges	Displays the list of privileges based on the selected Privilege Bundle . You can edit only those privileges that are eligible for customization.

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



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

Upload a Permission

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

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

SD-WAN Enterprise Security Admin

```
{
  "roleCustomizations": [
    {
      "forRoleId": 151,
      "addPrivileges": [
        {
          "object": "EDGE_DEVICE_DEVICE_SETTINGS",
          "action": "UPDATE",
          "isDeny": 1
        },
        {
          "object": "EDGE_DEVICE_CLOUD_SECURITY_SERVICE",
          "action": "UPDATE",
          "isDeny": 1
        },
        {
          "object": "EDGE_DEVICE_GLOBAL_IPV6_SETTINGS",
          "action": "UPDATE",
          "isDeny": 1
        }
      ]
    }
  ]
}
```

```

    },
    {
      "object": "EDGE_DEVICE_L2_SETTINGS",
      "action": "UPDATE",
      "isDeny": 1
    },
    {
      "object": "EDGE_DEVICE_WIFI_SETTINGS",
      "action": "UPDATE",
      "isDeny": 1
    },
    {
      "object": "EDGE_DEVICE_CC_FIREWALL",
      "action": "UPDATE",
      "isDeny": 1
    },
    {
      "object": "EDGE_DEVICE_HIGH_AVAILABILITY",
      "action": "UPDATE",
      "isDeny": 1
    },
    {
      "object": "EDGE_DEVICE_CONFIG_VISIBILITY_MODE",
      "action": "UPDATE",
      "isDeny": 1
    },
    {
      "object": "EDGE_DEVICE_SNMP_SETTINGS",
      "action": "UPDATE",
      "isDeny": 1
    },
    {
      "object": "EDGE_DEVICE_SECURITY_VNF",
      "action": "UPDATE",
      "isDeny": 1
    },
    {
      "object": "EDGE_DEVICE_NTP_SETTINGS",
      "action": "UPDATE",
      "isDeny": 1
    },
    {
      "object": "EDGE_DEVICE_ANALYTICS_SETTINGS",
      "action": "UPDATE",
      "isDeny": 1
    },
    {
      "object": "PROFILE_DEVICE_DEVICE_SETTINGS",
      "action": "UPDATE",
      "isDeny": 1
    },
    {
      "object": "PROFILE_DEVICE_L2_SETTINGS",
      "action": "UPDATE",
      "isDeny": 1
    },
    {
      "object": "PROFILE_DEVICE_GLOBAL_IPV6_SETTINGS",
      "action": "UPDATE",
      "isDeny": 1
    },
    {
      "object": "PROFILE_DEVICE_WIFI_SETTINGS",
      "action": "UPDATE",

```

```

        "isDeny": 1
      },
      {
        "object": "PROFILE_DEVICE_CC_FIREWALL",
        "action": "UPDATE",
        "isDeny": 1
      },
      {
        "object": "PROFILE_DEVICE_CONFIG_VISIBILITY_MODE",
        "action": "UPDATE",
        "isDeny": 1
      },
      {
        "object": "PROFILE_DEVICE_NTP_SETTINGS",
        "action": "UPDATE",
        "isDeny": 1
      },
      {
        "object": "PROFILE_DEVICE_SNMP_SETTINGS",
        "action": "UPDATE",
        "isDeny": 1
      },
      {
        "object": "EDGE_OVERVIEW",
        "action": "UPDATE",
        "isDeny": 1
      },
      {
        "object": "PROFILE",
        "action": "CREATE",
        "isDeny": 1
      },
      {
        "object": "OVERLAY_FLOW_CONTROL",
        "action": "UPDATE",
        "isDeny": 1
      },
      {
        "object": "EDGE_MANAGEMENT",
        "action": "UPDATE",
        "isDeny": 1
      }
    ],
    "removePrivileges": []
  }
]
}

```

Global Settings Enterprise Admin

```

{
  "roleCustomizations": [
    {
      "forRoleId": 551,
      "addPrivileges": [
        {
          "object": "SYSTEM_SETTINGS_GENERAL_INFO",
          "action": "UPDATE",
          "isDeny": 1
        }
      ],
      "removePrivileges": []
    }
  ],
}

```

```
"networkId": 1
}
```

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

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

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:

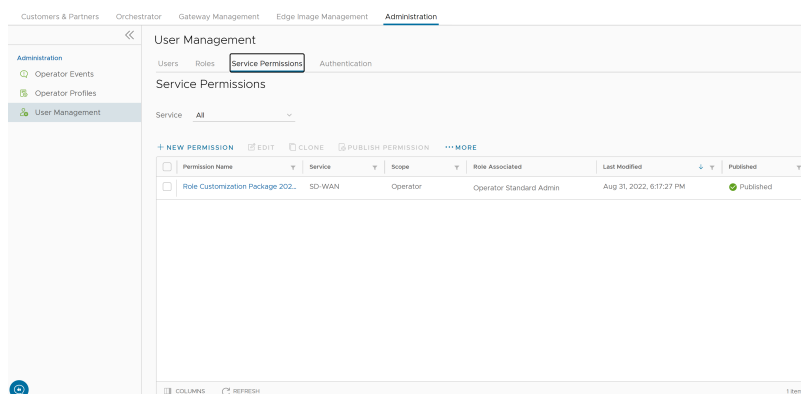
- The customizations done at the Enterprise level override the Partner or Operator level customizations.
- The customizations done at the Partner level override the Operator level customizations.
- Only when there are no customizations done at the Partner level or Enterprise level, the customizations 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:

- In the Operator Portal, click **Administration** from the top menu.
- From the left menu, click **User Management**, and then click the **Service Permissions** tab. The following screen appears:



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

Option	Description
Service	<p>Select a service from the drop-down menu. The available services are:</p> <ul style="list-style-type: none"> • All • Global Settings • SD-WAN • Edge Intelligence <p>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.</p>
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	<p>Allows you to select from the following additional options:</p> <ul style="list-style-type: none"> • Delete: Deletes the selected permission. You cannot delete a permission if it is already in use. <p> Note: A permission can only be deleted if it is in a draft state. 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 state and activates the Delete option for the permission.</p> <ul style="list-style-type: none"> • Download JSON: Downloads the list of permissions into a file in JSON format. • Upload Permission: Allows you to upload a JSON file of a customized permission. • 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.

4. 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.

5. 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. In the Operator portal, click **Administration** from the top menu.
2. From the left menu, click **User Management**, and then click the **Service Permissions** tab.
3. Click **New Permission**.

The following screen appears:

Service Permissions / test

test

Permission Details

Name *

Description

Scope * ☒ Operator ☐ Partner ☐ Enterprise

Service *

Privilege Bundle *

Privileges ⓘ

[RESET PRIVILEGES](#) [DOWNLOAD CSV](#) ☐ Show Only Modified

Privileges	Description	Read ⓘ	Create	Update	Delete	Feature ⓘ
Authentication Service ⓘ	Privilege controlling the creation and configuration of hosted 802.1x service providing LAN-side user authentication	<input checked="" type="checkbox"/> On	<input type="checkbox"/> Off ⓘ	<input checked="" type="checkbox"/> On	<input checked="" type="checkbox"/> On	
BRANDING_ASSET ⓘ		<input checked="" type="checkbox"/> On	<input checked="" type="checkbox"/> On	<input type="checkbox"/> Off ⓘ	<input checked="" type="checkbox"/> On	
Bastion VCO	This privilege controls access to Bastion VCO configuration and monitoring information	<input checked="" type="checkbox"/> On	<input checked="" type="checkbox"/> On ⓘ	<input checked="" type="checkbox"/> On ⓘ	<input checked="" type="checkbox"/> On ⓘ	
CUSTOM_APPLICATIONS		<input checked="" type="checkbox"/> On	<input type="checkbox"/> Off	<input checked="" type="checkbox"/> On	<input checked="" type="checkbox"/> On	
Cloud Security Service	Privilege controlling the creation and configuration of third party cloud security services to which traffic can be steered by business policy	<input checked="" type="checkbox"/> On	<input checked="" type="checkbox"/> On	<input checked="" type="checkbox"/> On	<input checked="" type="checkbox"/> On	
Cloud Subscription Service	Privilege granting the ability to view and manage the configuration of access to IAAS providers, such as Azure, AWS and Google Cloud	<input checked="" type="checkbox"/> On	<input checked="" type="checkbox"/> On	<input checked="" type="checkbox"/> On	<input checked="" type="checkbox"/> On	
Customer Alert	Privilege granting the ability to view and manage customer alert configuration and generated alerts	<input checked="" type="checkbox"/> On	<input type="checkbox"/> Off	<input checked="" type="checkbox"/> On	<input type="checkbox"/> Off	
Customer Alert Notification	Privilege granting the ability to view and manage customer alert configuration	<input checked="" type="checkbox"/> On	<input type="checkbox"/> Off	<input type="checkbox"/> Off	<input type="checkbox"/> Off	
Customer Edge Settings	Privilege granting the ability to activate or deactivate Configuration Updates for an Edge.	<input checked="" type="checkbox"/> On	<input type="checkbox"/> Off	<input checked="" type="checkbox"/> On	<input type="checkbox"/> Off	
Customer Event	Privilege granting the ability to view customer level events	<input checked="" type="checkbox"/> On	<input checked="" type="checkbox"/> On	<input checked="" type="checkbox"/> On	<input checked="" type="checkbox"/> On	

Objects per page 178 items |< < 1 / 18 > >|

[CANCEL](#) [SAVE](#) [SAVE AND APPLY](#)

4. 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 Operator , Partner , or Enterprise as the scope. An Operator can apply the permissions for Operators, Partners, and Customers.
Service	Select a service from the drop-down menu. The available services are: <ul style="list-style-type: none"> • Global Settings • SD-WAN • 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, in a tabular format, based on the selected Privilege Bundle .

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. Operator Superuser role cannot be customized.

5. Slide the **Show Only Modified** toggle button, located at the top right of the privileges table, to view only the modified privileges.
6. Click **Reset Privileges** to reset all the changes.
7. 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.

8. 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.

List of User Privileges

This section lists all the privileges available in the Operator portal.

The columns in the table indicate the following:

- **Allow Privilege** – Do the privileges have allow access?
- **Deny Privilege** – Do the privileges have deny access?
- **Customizable** – Is the privilege available for customization in the **Service Permissions** tab?

Feature	Name of the Privilege	Description	Allow Privilege	Deny Privilege	Customizable
Manage Customers	Create Customer	Grants ability to view and manage Enterprise Customers as an Operator or a Partner	Yes	No	No
	Read Customer				
	Update Customer			Yes	Yes
	Delete Customer			No	No
	Manage Customer				
Manage Partners	Create Partner	Grants ability to view and manage Partners	Yes	No	No
	Read Partner				
	Update Partner				
	Delete Partner				
	Manage Partner				

Feature	Name of the Privilege	Description	Allow Privilege	Deny Privilege	Customizable
Software Images	Create Software Package	Grants access to upload and assign Edge Software Images and Application Maps	Yes	Yes	Yes
	Read Software Package				
	Update Software Package				
	Delete Software Package				
	Manage Software Package				
System Properties	Create System Property	Grants access to view and manage System Properties	Yes	Yes	No
	Read System Property				Yes
	Update System Property				No
	Delete System Property				No
	Manage System Property				Yes
	Edit Restricted System Properties	Controls the ability of user to edit restricted system properties	Yes	No	No
Operator Events	Create Operator Event	Grants ability to view Operator events	Yes	Yes	Yes
	Read Operator Event				
	Update Operator Event				
	Delete Operator Event				
	Manage Operator Event				
Operator Profiles	Create Operator Profile	Grants ability to view and manage Operator profiles	Yes	Yes	Yes
	Read Operator Profile				
	Update Operator Profile				
	Delete Operator Profile				

Feature	Name of the Privilege	Description	Allow Privilege	Deny Privilege	Customizable
	Manage Operator Profile				
	View Tab Operator Profile	Controls ability of the user to view and configure within the Operator profile menu	No	Yes	Yes
Operator Users	Create Operator User	Grants ability to view and manage Operator administrative users	Yes	Yes	No
	Read Operator User				Yes
	Update Operator User				No
	Delete Operator User				No
	Manage Operator User				Yes
Operator Users > API Tokens	Create Operator Token	Grants ability to view and manage the operator Authentication Tokens	Yes	No	No
	Read Operator Token				
	Update Operator Token				
	Delete Operator Token				
	Manage Operator Token				
Gateway Pools Gateways Gateway Diagnostic bundles	Create Gateway	Grants ability to view and manage Gateway pools and Gateways as an Operator or a Partner	Yes	Yes	Yes
	Read Gateway				
	Update Gateway				
	Delete Gateway				
	Manage Gateway				
	View Tab Gateway List	Controls the ability of user to view the list of Gateways	No	Yes	Yes

Feature	Name of the Privilege	Description	Allow Privilege	Deny Privilege	Customizable
Gateways > New Gateway	Create Operator PKI	Grants ability to view and manage Operator level PKI configuration including Gateway certificates and certificate authority	Yes	Yes	No
Gateway > Gateway Authentication Mode	Read Operator PKI				Yes
	Update Operator PKI				No
	Manage Operator PKI				Yes
Gateway Diagnostic bundles > Download Diagnostic Bundles	Download Gateway Diagnostics	Grants ability to download Gateway Diagnostics	No	Yes	Yes
Application Maps	Create Software Package	Grants access to upload and assign Edge software images and Application Maps	Yes	Yes	Yes
	Read Software Package				
	Update Software Package				
	Delete Software Package				
	Manage Software Package				
Service Permissions	Create Service Permissions Package	Grants access to manage Service Permissions packages	Yes	No	No
	Read Service Permissions Package				
	Update Service Permissions Package				
	Delete Service Permissions Package				
	Manage Service Permissions Package				

Feature	Name of the Privilege	Description	Allow Privilege	Deny Privilege	Customizable
Edge Licensing	Create License	Grants ability to view and manage Edge licensing	Yes	No	No
	Read License			Yes	Yes
	Update License			No	No
	Delete License				
	Manage License				
CA Summary > Gateway Certificates > Revoke Certificate	Read Operator PKI	Grants ability to view and manage operator level PKI configuration including Gateway certificates and certificate authority	Yes	Yes	Yes
	Delete Operator PKI				No
	Manage Operator PKI				Yes
	Read Customer PKI	Grants ability to view and manage Enterprise PKI settings	Yes	No	No
	Delete Customer PKI				
	Manage Customer PKI				
Orchestrator Authentication > Operator Authentication	Create Operator Authentication	Grants ability to view and manage Operator authentication mode, like SSO, RADIUS, or Native	Yes	Yes	Yes
	Read Operator Authentication				
	Update Operator Authentication				
	Delete Operator Authentication				
	Manage Operator Authentication				
Orchestrator Authentication > Enterprise Authentication	Create Customer Authentication	Grants ability to view and manage Customer authentication mode, like RADIUS or Native	Yes	Yes	Yes
	Read Customer Authentication				
	Update Customer Authentication				
	Delete Customer Authentication				

Feature	Name of the Privilege	Description	Allow Privilege	Deny Privilege	Customizable
	Manage Customer Authentication				
Replication	Create Replication	Grants access to view and configure Orchestrator disaster recovery	Yes	Yes	No
	Read Replication				Yes
	Update Replication				No
	Delete Replication				
	Manage Replication				Yes
Orchestrator Diagnostics > Diagnostic Bundles	Create Orchestrator Diagnostics	Grants access to request and view Orchestrator diagnostic bundles	Yes	Yes	Yes
Orchestrator Diagnostics > Database Statistics	Read Orchestrator Diagnostics				
	Update Orchestrator Diagnostics				
	Delete Orchestrator Diagnostics				
	Manage Orchestrator Diagnostics				
Orchestrator Upgrade for Standalone	Create Software Package	Grants access to upload and assign Edge software images and Application Maps	Yes	Yes	Yes
	Read Software Package				
	Update Software Package				
	Delete Software Package				
	Manage Software Package				

Feature	Name of the Privilege	Description	Allow Privilege	Deny Privilege	Customizable
Orchestrator Upgrade for DR Setup	Create Replication	Grants access to view and configure Orchestrator disaster recovery	Yes	Yes	No
	Read Replication				Yes
	Update Replication				No
	Delete Replication				
	Manage Replication				Yes
User Agreements	Create User Agreement	Grants access to configure the customer user agreement	Yes	No	No
	Read User Agreement				
	Update User Agreement				
	Delete User Agreement				
	Manage User Agreement				
Orchestrator Owners Manage Orchestrators Edge Inventory	Create Edge Inventory	Grants ability to view and manage Edge inventory as needed for Redirect configuration	Yes	No	No
	Read Edge Inventory				
	Update Edge Inventory				
	Delete Edge Inventory				
	Manage Edge Inventory				

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

Below table provides a list of customizable feature privileges:

Navigation Path in the Enterprise Portal	Name of the Tab	Name of the Privilege	Description
Configure > Edges > Select Edge	Overview	Assign Edge Profile	Grants ability to assign a Profile to Edges
Configure > Edges > Select Edge	Firewall	Configure Edge Firewall Logging	Grants ability to configure Edge level firewall logging
Configure > Profiles > Select Profile	Firewall	Configure Profile Firewall Logging	Grants ability to configure Profile level firewall logging

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



Note: This is for 610-LTE and 710 5G devices only.

Navigation Path in the Enterprise Portal	Name of the Tab	Name of the Privilege	Description
Diagnostics > Remote Diagnostics	List Paths	Remote List Paths	Grants ability to view the list of active paths between local WAN links and each peer
Diagnostics > Remote Diagnostics	List current IKE Child SAs	Remote List current IKE Child SAs	Grants ability to use filters to view the exact Child SAs you want to see
Diagnostics > Remote Diagnostics	List current IKE SAs	Remote List Current IKE SAs	Grants ability to use filters to view the exact SAs you want to see
Diagnostics > Remote Diagnostics	MIBs for Edge	Remote MIBS for Edge	Grants ability to dump Edge MIBs
Diagnostics > Remote Diagnostics	NAT Table Dump	Remote NAT Table Dump	Grants ability to view the contents of the NAT table
Diagnostics > Remote Diagnostics	Select Edge > Rebalance Hub Cluster	Remote Rebalance Hub Cluster	Grants ability to either redistribute Spokes in Hub Cluster or redistribute Spokes excluding this Hub
Diagnostics > Remote Diagnostics	Select Edge (with SFP module) > Reset SFP Firmware Configuration	Remote Reset SFP Firmware Configuration	Grants ability to reset the SFP Firmware Configuration
Diagnostics > Remote Actions	Reset USB Modem	Remote Reset USB Modem	Grants ability to execute the Edge USB modem reset remote action
Diagnostics > Remote Diagnostics	Scan for WiFi Access Points	Remote Scan for WiFi Access Points	Grants ability to scan the Wi-Fi functionality for the
Diagnostics > Remote Diagnostics	System Information	Remote System Information	Grants ability to view system information such as system load, recent WAN stability statistics, monitoring services
Diagnostics > Remote Diagnostics	VPN Test	Remote VPN Test	Grants ability to execute the Edge VPN test remote action
Diagnostics > Remote Diagnostics	WAN Link Bandwidth Test	Remote WAN link Bandwidth Test	Grants ability to re-test the bandwidth of a WAN link
Diagnostics > Remote Actions	Select Edge > Shutdown	Shutdown Edge	Grants ability to execute the Edge shutdown remote action
Service Settings > Alerts & Notifications	Notifications > Email/SMS	Update Customer SMS Alert	Grants ability to configure SMS alerts at the customer level
Monitor > Edges > Select Edge	Top Sources	View Edge Sources	Grants ability to view Monitor Edge Sources tab

Navigation Path in the Enterprise Portal	Name of the Tab	Name of the Privilege	Description
Monitor > Firewall	Firewall Logging	View Firewall Logs	Grants ability to view collected firewall logs
Monitor > Edges > Select Edge	Top Sources	View Flow Stats	Grants ability to view collected flow statistics
Monitor > Firewall Logs	Firewall Logs	View Profile Firewall Logging	Grants ability to view the details of firewall logs originating from
Configure > Profiles	Firewall	View Stateful Firewall	Grants ability to view collected flow statistics
Configure > Profiles	Firewall tab > Configure Firewall > Syslog Forwarding	View Syslog Forwarding	Grants ability to view logs that are forwarded to a configured syslog collector
Operator portal > Gateway Management	Gateways	View Tab Gateway List	Grants ability to view the Gateway list tab
Operator portal > Administration	Operator Profiles	View Tab Operator Profile	Grants ability to view and configure settings within the Operator Profile menu tab
Monitor > Edges > Select Edge	Top Sources	View User Identifiable Flow Stats	Grants ability to view potentially user identifiable flow source attributes

Authentication

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

To access the **Authentication** tab:

1. In the Operator portal, click **Administration** from the top menu.
2. From the left menu, click **User Management**, and then click the **Authentication** tab. The following screen appears:



Administration

Operator Events

Operator Profiles

User Management

User Management

Users

Roles

Service Permissions

Authentication

API Tokens

Search



REVOKE API TOKEN

CSV

<input type="checkbox"/>	UUID	Name
<input type="checkbox"/>	08655e51-a06f-49ce-adae...	111
<input type="checkbox"/>	e6313e59-d2a5-4367-afa5...	222
<input type="checkbox"/>	67c4c354-6c7d-486a-b9d...	2323
<input type="checkbox"/>	ba950228-928d-47ad-b7e...	444
<input type="checkbox"/>	0589e477-3399-4838-904...	555
<input type="checkbox"/>	2f987ab0-4e19-42ec-997d...	45
<input type="checkbox"/>	a0557b39-5aab-4dff-b644...	65656
<input type="checkbox"/>	df7cc53f-a1ce-434f-9a3b-...	ooo
<input type="checkbox"/>	d0d16548-bbc1-4ef2-8f60-...	etr

COLUMNS

REFRESH

Operator Authentication

Authentication Mode

Local



No configuration is required for native

UPDATE

Enterprise Authentication

API Tokens

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

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



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

The following are the options available in this section:

Option	Description
Search	Enter a search term to search for the matching text across the table. Use the advanced search option to narrow down the search results.
Revoke API Token	Select the token and click this option to revoke it. Only an Operator Super User or the user associated with an API token can revoke the token.
CSV	Click this option to download the complete list of API tokens in a .csv file format.
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.

As an Operator Super User, you can manage the API tokens for Enterprise users. For information on creating and downloading API tokens, see API tokens.

Operator Authentication / Enterprise Authentication

Select one of the following Authentication modes:

- **Local:** This is the default option and does not require any additional configuration.
- **Single Sign-On:** Operator users with Superuser permission can set up and configure Single Sign On (SSO) in. 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 the to authenticate users from an OpenID Connect (OIDC)-based Identity Providers (IdPs).



Note:

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

Pre-requisites:

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



Note:

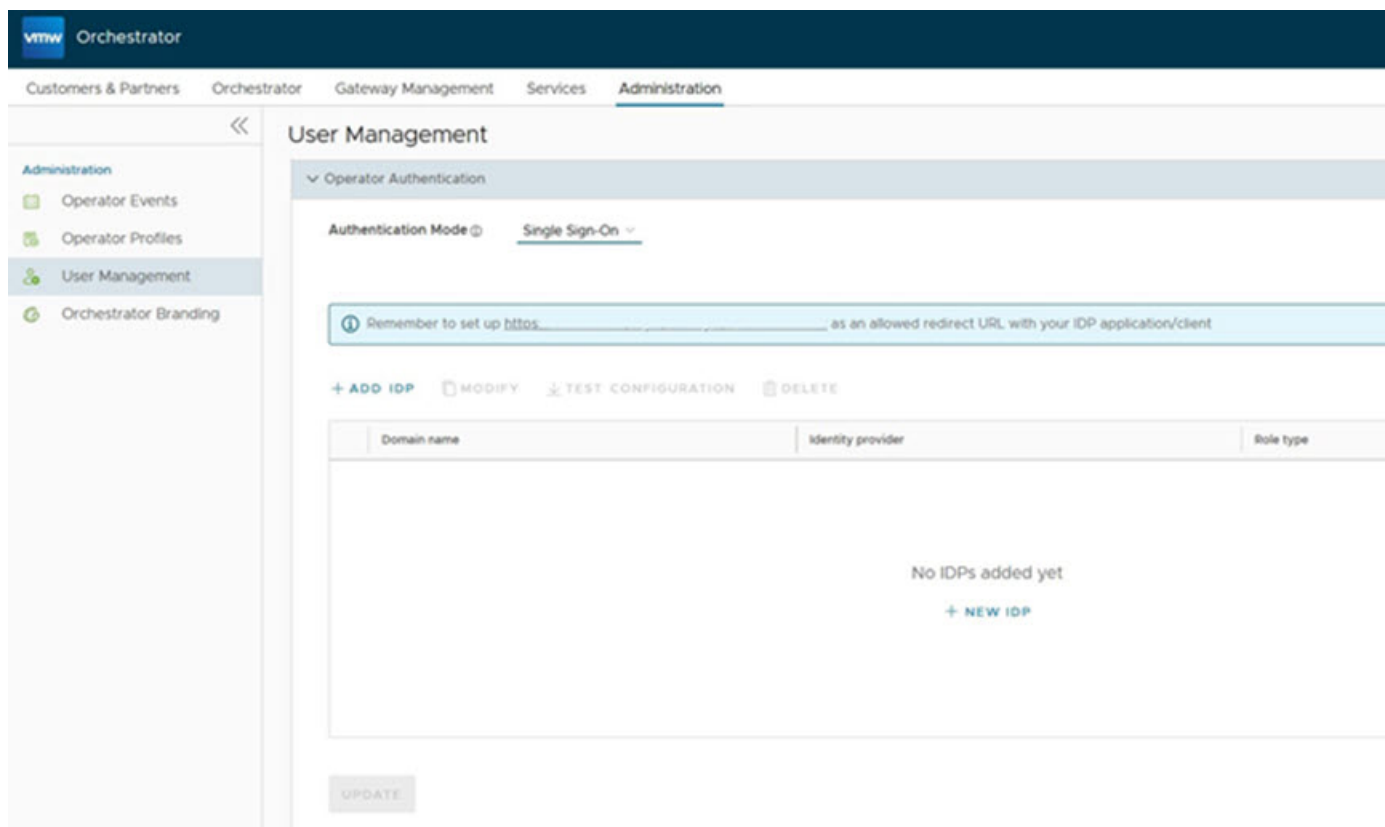
- **Single Sign-On** mode is available only for **Operator Authentication** in the Operator portal.
- Token-based authentication is deactivated for SSO users.

To enable Single Sign On (SSO) for, 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

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

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



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

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

Setup IDP

1 Single Sign-On Setup

2 Role Setup

Single Sign-On Setup

Domain Name

Test

Identity Provider Template ⓘ

Okta

OIDC well-known config URL * ⓘ

https:

Issuer

https: .ok

Authorization Endpoint

https

Token Endpoint

https ok

JSON Web KeySet URI

https ok

User Information Endpoint

https ok

Client ID * ⓘ

t2oi4n

Client Secret * ⓘ

Figure 1: Single Sign-On Setup Screen

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

Option	Description
Identity Provider Template	From the drop-down menu, select your preferred Identity Provider (IdP) that you have configured for Single Sign On. This pre-populates fields specific to your IdP.
OIDC well-known config URL	Enter the OpenID Connect (OIDC) configuration URL for your IdP. For example, the URL format for Okta will be: 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.

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

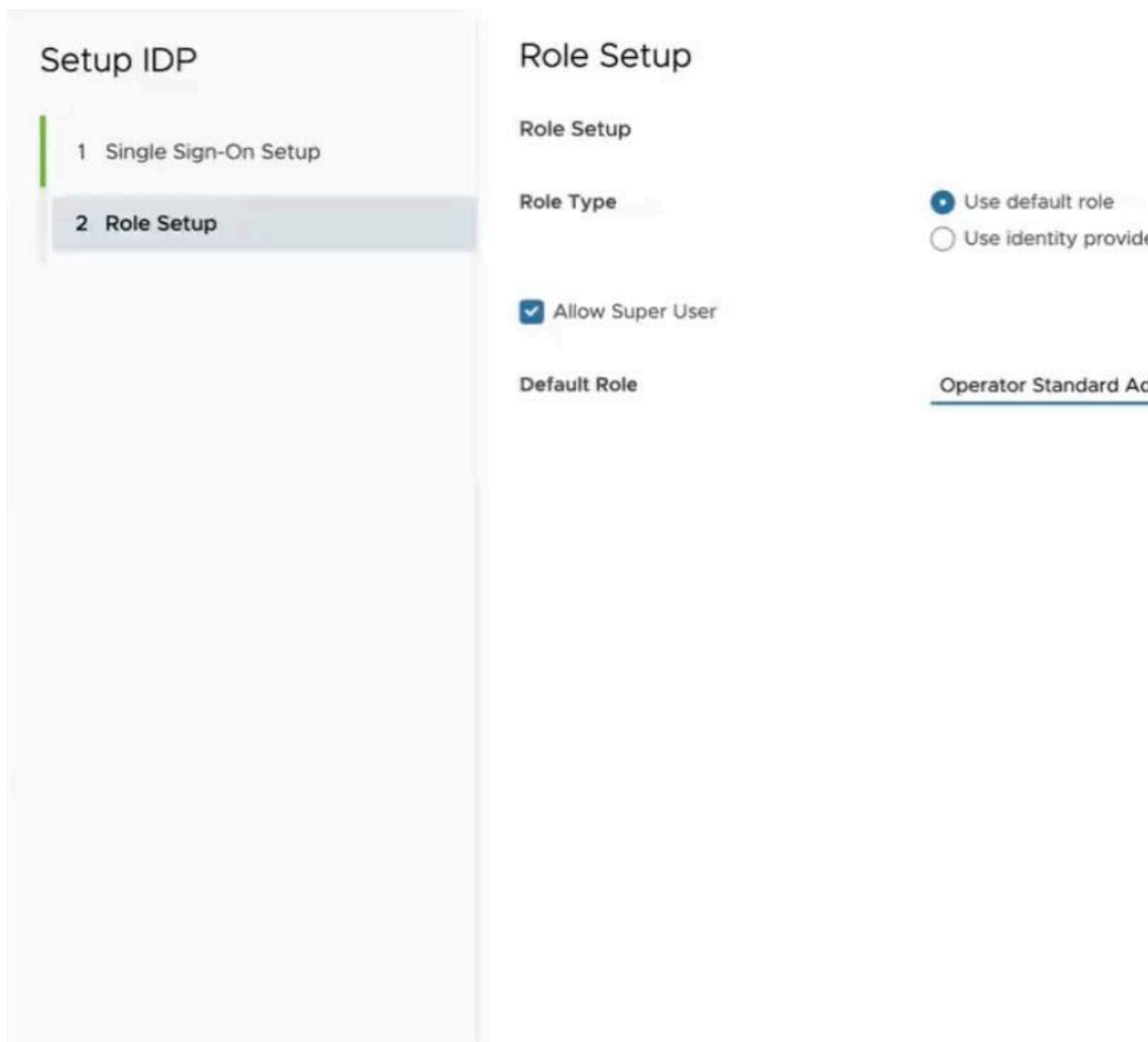


Figure 2: Role Setup - Use Default Role

Setup IDP

- Single Sign-On Setup
- Role Setup**

Role Setup

Role Setup

Role Type

☐ Use default role
☒ Use identity provider

☒ Allow Super User

Role Attribute ⓘ groups

Operator Role Map ⓘ

Orchestrator Role Name	Iden
Operator Superuser	
Operator Standard Admin	
Operator Business	
Operator Support	
4 items	

Figure 3: Role Setup - Use Identity Provider Roles (Default)

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

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

Operator Role Map

Map the IdP-provided roles to each of the Operator user roles.



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

The screenshot displays the 'Setup IDP' configuration interface. On the left, a sidebar lists two steps: '1 Single Sign-On Setup' and '2 Role Setup', with the latter being the active step. The main content area is titled 'Role Setup'. Under the 'Role Type' section, the 'Use default role' radio button is selected. Below this, the 'Allow Super User' checkbox is unchecked and highlighted with a red rectangular box. In the 'Default Role' section, the text 'Operator Superuser' is entered, and a red horizontal line with the word 'Invalid' in red text appears underneath it, indicating an error.

Figure 4: Role Setup for a Partner-added second IdP where the Allow Super User box is unchecked. This screen also shows that if you enter Operator Superuser as a default role, the UI will throw an error when that box is unchecked. The Default Role should be Operator Standard Admin for Partner Operator users.

Setup IDP

1 Single Sign-On Setup

2 Role Setup

Role Setup

Role Setup

Role Type ☐ Use default role ☒ Use identity provider

☐ Allow Super User

Role Attribute ⓘ groups

Operator Role Map ⓘ

Orchestrator Role Name	Id
Operator Superuser	
Operator Standard Admin	
Operator Business	
Operator Support	
4 items	

Figure 5: Role Setup for a Partner-added second IdP where the Operator Superuser role must be removed.

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

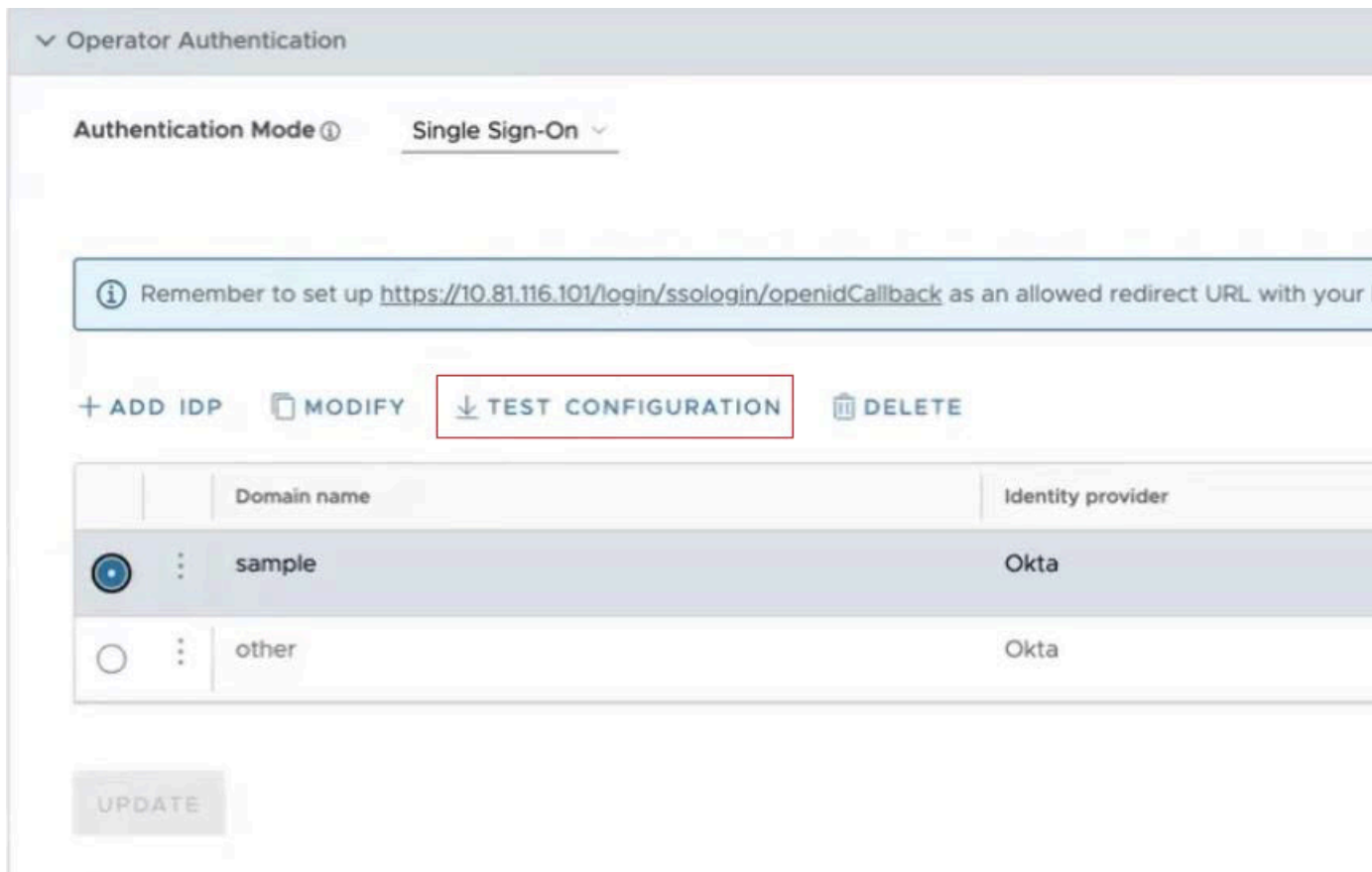


Figure 6: Test Configuration option for an SSO/IdP. Clicking on it runs the test.

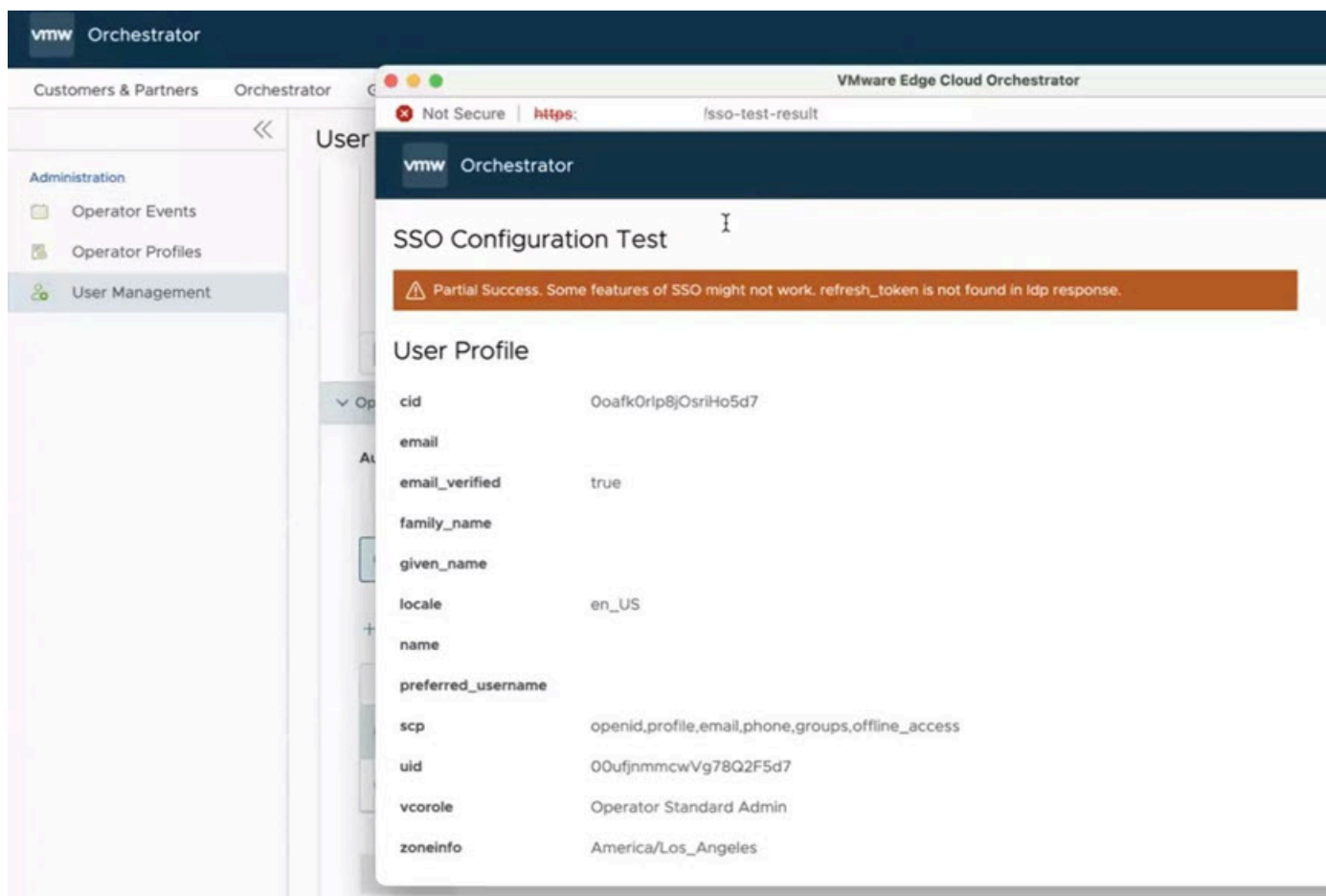


Figure 7: Successful SSO Configuration Test. The "Partial Success" message only indicates this configuration does not have a refresh token configured. It is still a valid configuration.

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

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

← ↻ Not Secure | <https://10.81.116.101/ui/operator/login?code=-32902>

vmware
by Broadcom

Welcome to
VMware Edge Cloud
Orchestrator

Username

Password

[Forgot Password?](#)

LOGIN

Successfully logged out

SIGN IN WITH YOUR IDENTITY PROVIDER

Copyright 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

Figure 8: The Operator login screen. This screen will have '/operator' in the URL and include the 'Sign In With Your Identity Provider' button. Click on this button to move on to the SSO screen.

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



Figure 9: Where there are multiple IdPs configured, all users including the Partner would be moved to this screen. The URL will include the text string 'domainFinder', but where it reads Organization Domain, you actually enter your 'Domain Name' for the IdP as configured earlier.



Note: An easier method for a Partner using their own IdP is to bookmark the following their Orchestrator URL with this format: *https://orchestrator hostname or IP address/ui/operator/login?domain=IdP Domain Name*. This will automatically take you to the login screen and prepopulate the IdP Domain Name. For example for an Orchestrator with hostname **vco11-usor1.velocloud.net** where the IdP Domain Name is **Acme**, the Partner Operator could bookmark: *https://vco11-usor1.velocloud.net/ui/operator/login?domain=Acme* and when they clicked that bookmark, the browser would still go to the Operator login screen. The difference is that now when they click **SIGN IN WITH YOUR IDENTITY**

PROVIDER, the user is immediately logged in the Orchestrator with no extra step, as the domain is already provided in the URL.

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

- **RADIUS:** Remote Authentication Dial-In User Service (RADIUS) is a client-server protocol that enables remote access servers to communicate with a central server. RADIUS authentication provides a centralized management for users. You can configure the Orchestrator Authentication in RADIUS mode, so that the Operator and Enterprise Customers log into the portals using the RADIUS servers. Enter appropriate details in the following fields:


Authentication Mode ⓘ RADIUS ▼

Primary Server *	test
------------------	------

Secondary Server

Optional

Timeout Sessions *	2500	milliseconds
--------------------	------	--------------

Shared Secret * 

Enter new value to change shared secret

Protocol * UDP 

Domain Attribute *	VC_USER_DOMAIN
--------------------	----------------

Operator Domain *	OPERATOR
-------------------	----------

Role Attribute *	VC_USER_ROLE
------------------	--------------

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

- You can edit the **Protocol** value only in the **System Properties**. Navigate to **Orchestrator > System Properties**, and edit the protocol in the **Value** field of the system property `vco.operator.authentication.radius`.
- **Operator Domain** field is available only for Operators.

- In the **Operator Role Map / Enterprise Role Map** section, map the RADIUS server attributes to each of the Operator or Enterprise user roles. This role mapping is used to determine the role the users would be assigned when they login to the Orchestrator using the RADIUS server for the first time.
- Click **Update** to save the entered values.

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 an Operator, 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.

Session Limits



Note: To view this section, an Operator user must navigate to **Orchestrator > System Properties**, and set the value of the system property `session.options.enableSessionTracking` to **True**.

The following are the options available in this section:

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	<p>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.</p> <div>  <p>Note: The roles that are already created by the Operator in the Roles tab, are displayed in this section.</p> </div>

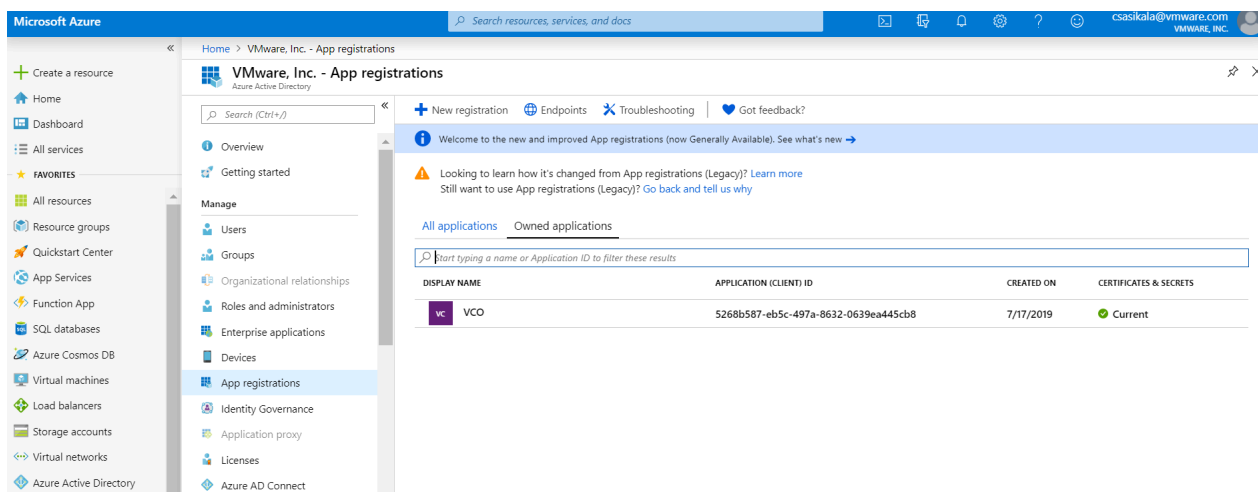
Click **Update** to save the selected values.

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.

Register an application

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

Supported account types
Who can use this application or access this API?
☒ Accounts in this organizational directory only (VeloCloud Networks, Inc@velo)
☐ Accounts in any organizational directory
☐ Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)
[Help me choose...](#)

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

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

Register

- c) In the **Name** field, enter the name for your 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.

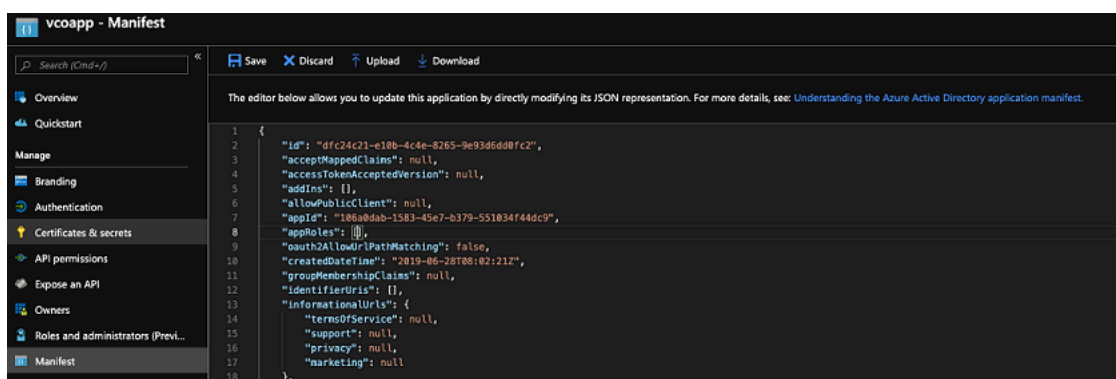
- i) Provide details such as description and expiry value for the secret and click **Add**.

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.

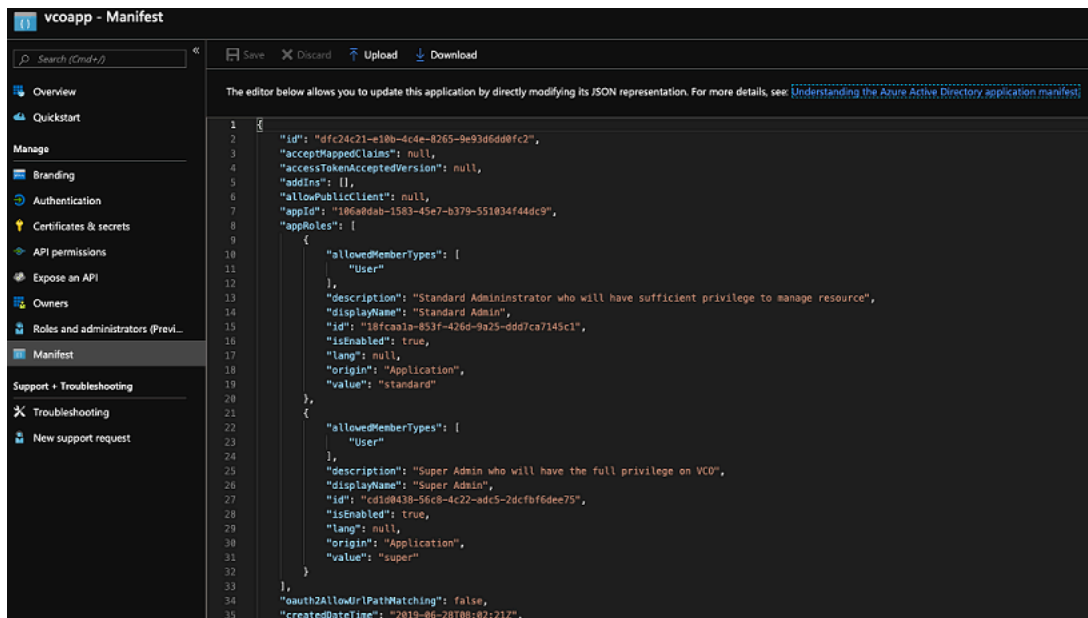
Sample role objects

```
{
  "allowedMemberTypes": [
    "User"
  ],
  "description": "Standard Administrator who will have
sufficient privilege to manage resource",
  "displayName": "Standard Admin",
  "id": "18fca1a1-853f-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-SSO](#)



VCO-ONE-SSO | App



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.

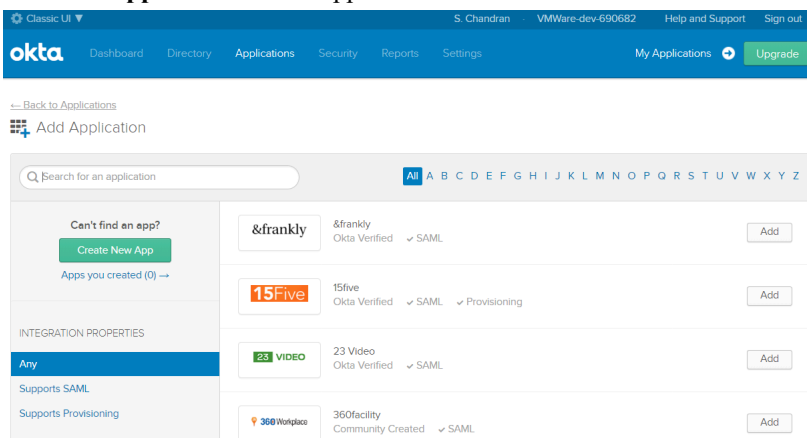
1. Log in to your Okta account as an Admin user.
The **Okta** home screen appears.



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.

 Create OpenID Connect Integration

- e) Under the **General Settings** area, in the **Application name** text box, enter the name for your application.
- f) Under the **CONFIGURE OPENID CONNECT** area, in the **Login redirect URIs** text box, enter the redirect URL that your 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

General Sign On Assignments

General Settings

Edit

APPLICATION

Application label

VMWare SD-WAN VCO

Application type

Web

Allowed grant types

Client acting on behalf of itself

☐ Client Credentials

Client acting on behalf of a user

☒ Authorization Code

☒ Refresh Token

☐ Implicit (Hybrid)

LOGIN

Login redirect URIs

https://vco13-usv11.velocloud.net/login/ssologin/openidCallback

Logout redirect URIs

Login initiated by

App Only

Initiate login URI

https://vco13-usv11.velocloud.net/

Client Credentials

Edit

Client ID

0ospekj5x5c7n5H6Qh7

Public identifier for the client that is required for all OAuth flows.

Client secret

- 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.

General **Sign On** Assignments

Settings

SIGN ON METHODS

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. [Configure profile mapping](#)

☒ OpenID Connect

Token Credentials

Edit

Signing credential rotation ⓘ Automatic

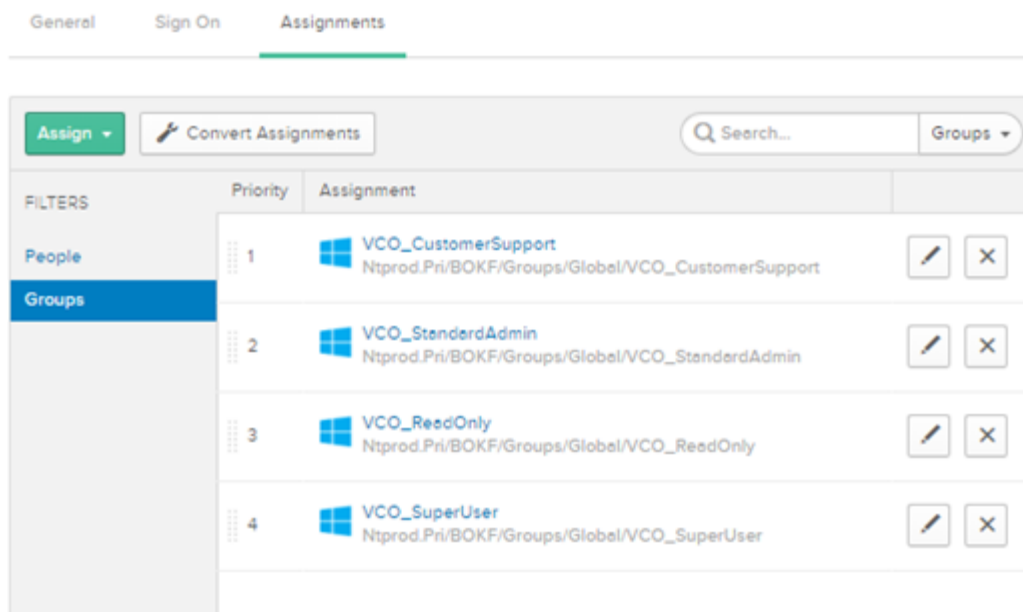
OpenID Connect ID Token

Edit

Issuer	https://bokf-sandbox.oktapreview.com
Audience	0ospekyj5x5c7h5H60h7
Claims	Claims for this token include all user attributes on the app profile.
Groups claim type	Expression
Groups claim expression ⓘ	groups Groups.startsWith("active_directory", "VCO_", 100) Using Groups Claim

3. To assign groups and users to your application:

- Go to **Application > Applications** and click on your application link.
- 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.
- 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.

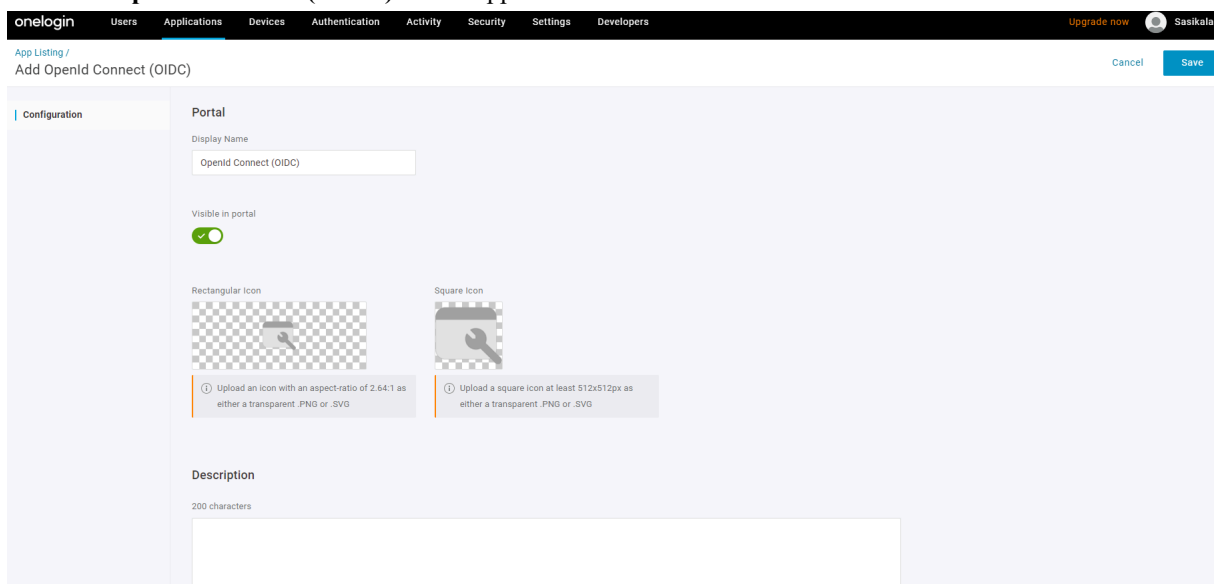
Configure Single Sign On in .

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:

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

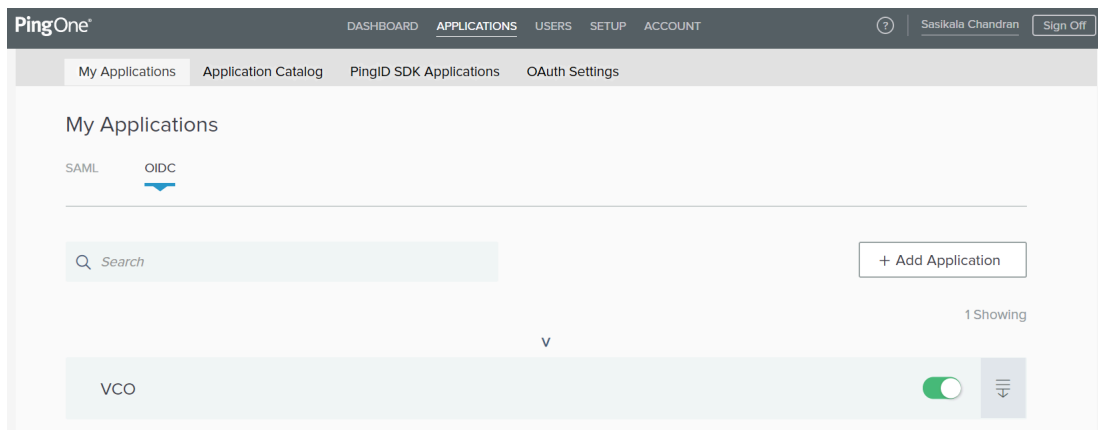
To set up an OpenID Connect (OIDC)-based application in PingIdentity for Single Sign On (SSO), perform the steps on this procedure.

Ensure you have a PingOne account to sign in.

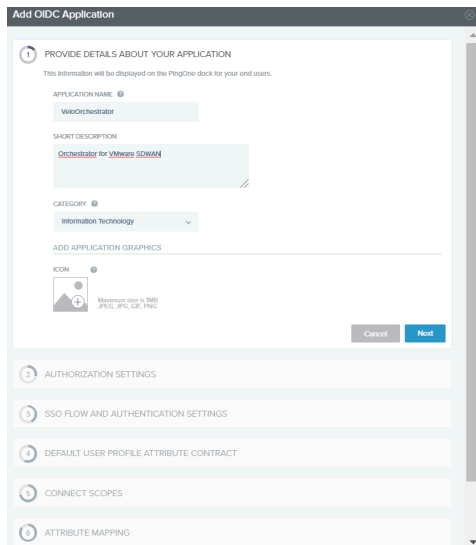


Note: Currently, supports PingOne as the Identity Partner (IDP); however, any PingIdentity product supporting OIDC can be easily configured.

- Log in to your PingOne account as an Admin user.
The **PingOne** home screen appears.
- To create a new application:
 - 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.
2. 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
3. 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.
4. 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.
5. 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.
6. 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 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.

Configure Authentication Save Changes ?

Operator Authentication

Authentication Mode: SSO

Identity Provider template: VMwareCSP

Organization Id: /csp/gateway/am/api/orgs/d94fb648-cbb3-4863-t

OIDC well-known config URL: https://console-stg.cloud.vmware.com/csp/gateway/am/api/.well-known/op

Issuer: https://gaz-preview.csp-vidm-prod.com

Authorization Endpoint: https://console-stg.cloud.vmware.com/csp/gateway/discovery?orgLink=%2

Token Endpoint: https://console-stg.cloud.vmware.com/csp/gateway/am/api/auth/authorize

User Information Endpoint: https://console-stg.cloud.vmware.com/csp/gateway/am/api/userinfo

Client Id: e1UmTD4TPps0h8vak0UMIOF0HCvWmW0MDta

Client Secret: *****

Scopes: openid

☐ Use Default Role ☒ Use Identity Provider Roles

Role Attribute: perms

Role Map

Operator Role	Arista CSP Role
Operator Superuser	external/1e73b58c-475f-4065-95d8-5f
Operator Standard Admin	external/1e73b58c-475f-4065-95d8-5f
Operator Support	support
Operator Business	business

Remember to set <https://13.52.173.235/login/ssologin/openidCallback> as an allowed redirect URL with your IDP application/client

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.

User Management with Arista Cloud Services Platform as the Identity Provider

This section covers customers managing their user accounts through the Arista Cloud Services Platform (CSP) as the Identity Provider (IdP) for Single Sign On (SSO).

Overview

Customers configured to use Single Sign On (SSO) can use several Identity Providers (IdP) to manage their users. This section covers VMware's IdP: Cloud Services Platform (CSP).



Tip: CSP is a common life cycle management platform for all Arista SaaS offerings. With other Arista SaaS offerings, CSP includes onboarding, authentication, billing, ordering, support, and customer notification. The CSP integration with (including SD-WAN) in Release 5.2.0, is limited to authentication and authorization with additional integration coming in later releases.

CSP consolidates and simplifies user management across multiple Orchestrators while integrating with IdPs that support SAML and OIDC, and provides a single touch point to ensure compliance with governmental regulations.



Important: Customers created on a Release 5.2.0 Hosted Orchestrator who are not assigned to a Partner are automatically configured for SSO using CSP as the IdP. As a result:

- New administrators are created by an administrator with a Superuser role through the CSP portal.
- In the event of a CSP outage, the customer is permitted one "break glass" administrator account with local authentication (username/password) to allow them to access their portal.
- New direct customers will need to use token-based authentication for API access. They will not be able to use cookie-based authentication as user creation moves to CSP.

In a later SD-WAN Release, Arista will require all customers using a Hosted Orchestrator, whether new or existing to configure their enterprise to use CSP as their IdP.

On Premise Orchestrators are not subject to CSP requirements and their customers would continue to use Orchestrator-based authentication.

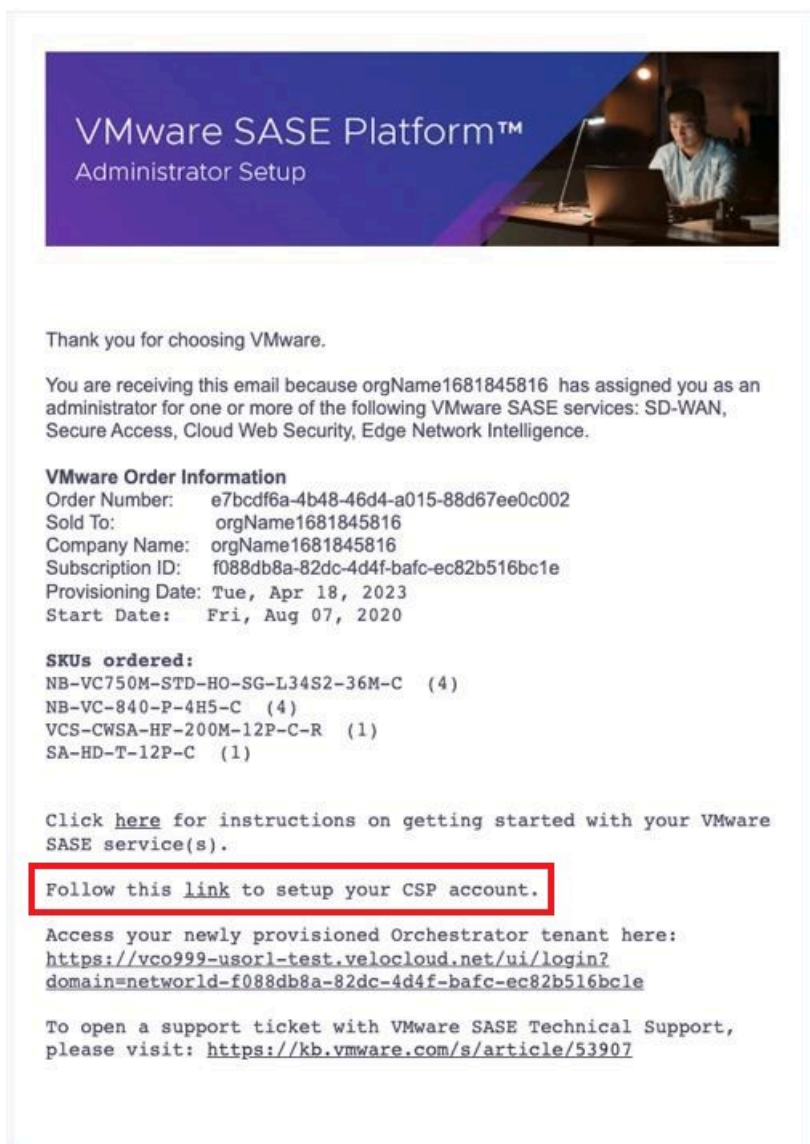
Prerequisites

Before you can configure your SD-WAN account on the assigned, you must first buy SD-WAN.

Creating a Customer Organization on the Cloud Services Platform

Once the customer's SD-WAN order is confirmed:

1. Arista sends you an invitation email similar to the one shown below:



This email includes a link to the Orchestrator you will be using to manage your enterprise along with a **link** to create your organization on CSP.



Note: Your customer domain details form the basis for your customer account on the Orchestrator along with determining the Orchestrator to which your enterprise will be assigned based on your geolocation.

2. Where the email reads "Follow this link to setup your CSP account" click on the **link** to set up your CSP organization.
3. Clicking the link redirects you to the CSP site where you will configure your CSP account, this can be an existing organization or a new one.
4. Under **Organization** > **Details** configure the details of your account, including the Organization ID provided by, as part of your order.

ORGANIZATION

Details

Organization Name [EDIT](#)

Display Name: VeloCloud

Organization ID

Organization ID: jxm0dl5c [COPY](#)

Long Organization ID: d94fb648-cbb3-4863-b0c9-23e50c21180c [COPY](#)

Organization Address [EDIT](#)

Country/Region: United States Of America

Address Line 1: 6500 RiverPlace Blvd

City: Austin

State/Province: TX

Zip/Postal Code: 78730



Important: During CSP customer onboarding, you must provide a physical address. In addition, your customer domain name will be validated prior to configuring federation.

Then click on the **Organization > OAuth Apps** tab to configure the **Domains Linked to Identity Provider** along with the other fields and options on this page.

Domains Linked to Identity Provider

To enable advanced Identity Governance features, please link your organization to your identity provider.
[Learn more about advanced features](#)

LINK IDENTITY PROVIDER

Language and Regional Format [EDIT](#)

Language	English
Regional Format	United States

Data Disclosure to Partners

By clicking "ACCEPT" below, I confirm that I have the authority to accept the following terms on behalf of my organization, and agree that VMware may disclose to any VMware author VMware software licenses, VMware cloud services entitlements, and other VMware products and services that my organization has ordered, licensed, or consumed, including active er

VMware acknowledges and agrees that this authorization does not allow VMware to disclose any business contact information or user data, including names and/or email addresses, c

I understand that my organization may revoke this authorization at any time through Organization Settings.

☒ Accept
☐ Decline for now

SAVE [CANCEL](#)

Usage Notifications [EDIT](#)

☒ Activated

Notifications sent to Organization Owners as a daily summary when usage exceeds the committed capacity.

- Once you have completed configuring your CSP organization you can now add new users to your CSP organization.

Add Users to Your CSP Organization

- Click on the **Identity & Access Management** tab on the Arista Cloud Services page and then click on **Active Users** and then click **Add New Users**.

VMware Cloud Services

IDENTITY & ACCESS MANAGEMENT

Add New Users

Add/invite new users to your organization Orca and allow access to the organization and services. To send invitations to new users, leave the **Send emails** checkbox checked.

Users

john@acme.com

Enter the email address or account name of each user delimited by comma, space or a new line.

Role Assignment

Assign Organization Roles

Mandatory Roles

- ☐ Organization Administrator
- ☒ Organization Member
Organization members hold the default organization role that grants users access to the organization.
- ☐ Organization Owner

Additional Roles

- ☐ Access Log Auditor
- ☐ Billing Read-only
- ☐ Developer
- ☐ Project Administrator
- ☐ Software Installer
- ☐ Support User

Assign Service Roles

Test SDWAN in vco999-usor1-test.veloci with roles Enterprise Support with never expire access

☒ Send emails to all invited users notifying them of this role assignment.

Note that if the account name is not a real email destination, then the user will not receive a notification about the invitation.

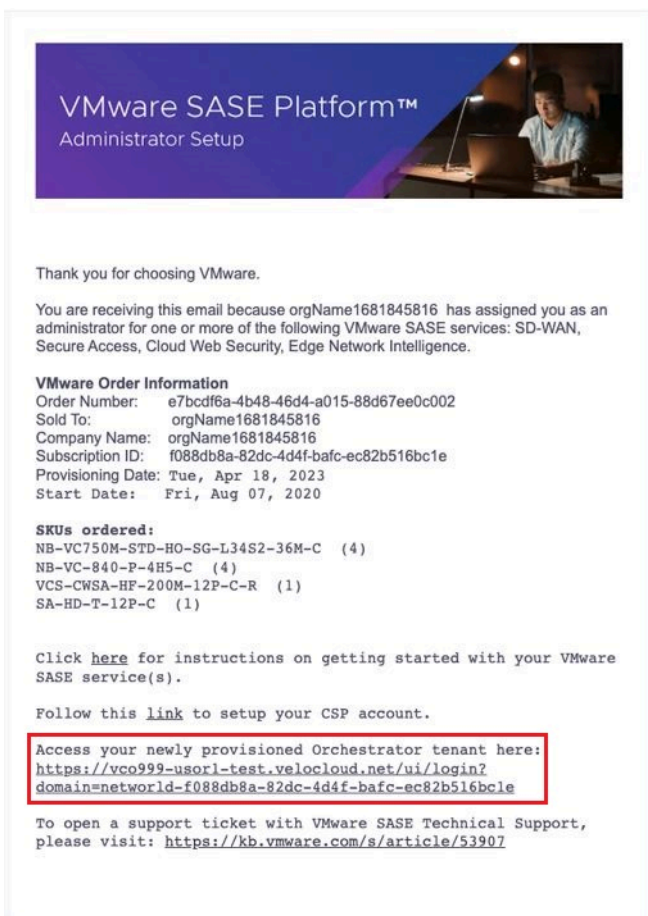
ADD **CANCEL**

2. On the **Add New Users** page you can add new users by email address. The users will need to be assigned two roles:
 - a. Assign them an **Organization Role** (or roles), this is their role within your CSP Organization.
 - b. Assign them a **Service Role**, this is their role when logged into the Orchestrator.
3. Once all roles have been configured, click **ADD** to add these users to your CSP Organization.

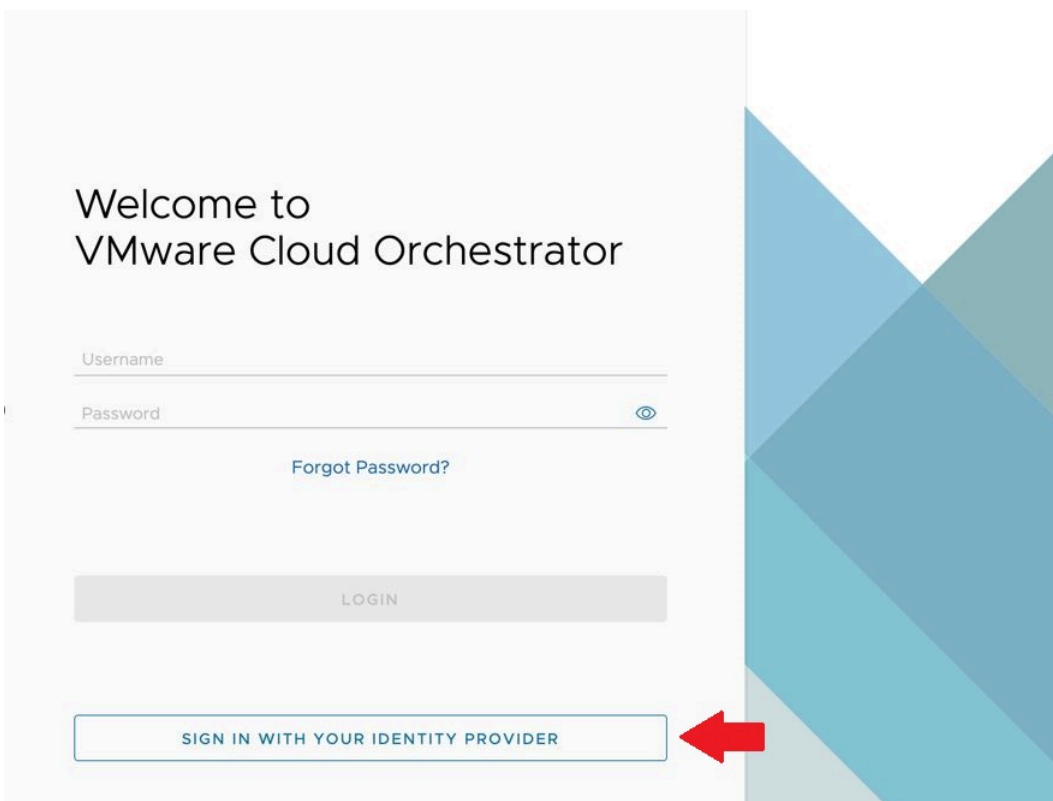
Logging into the Orchestrator using CSP

Anyone added as a user in the previous step may now log into their Enterprise on the Orchestrator. To log into the Orchestrator:

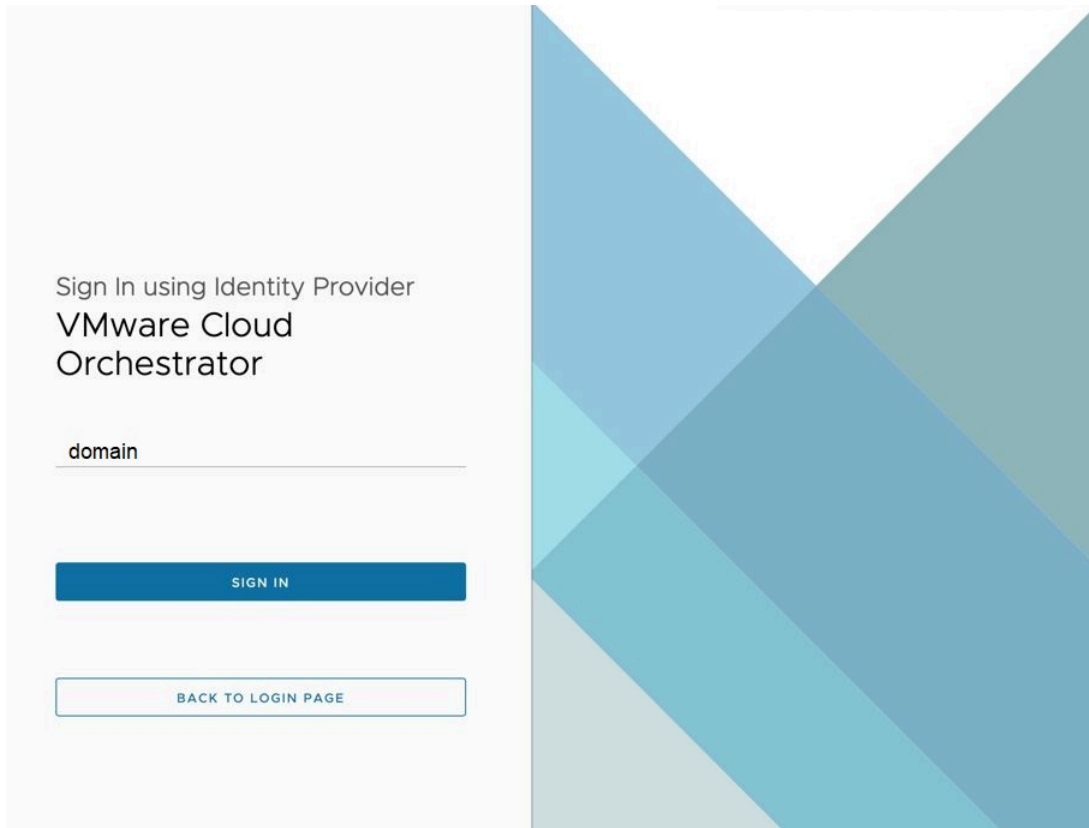
1. Navigate to the Orchestrator's login page by referring back to the email invite you received and click on the URL link in the section highlighted below:



2. On the Orchestrator login screen, click **SIGN IN WITH YOUR IDENTITY PROVIDER**.



3. On the Sign in using Identity Provider page, enter the domain for your account and click **SIGN IN**.



Sign In using Identity Provider
VMware Cloud Orchestrator

domain

SIGN IN

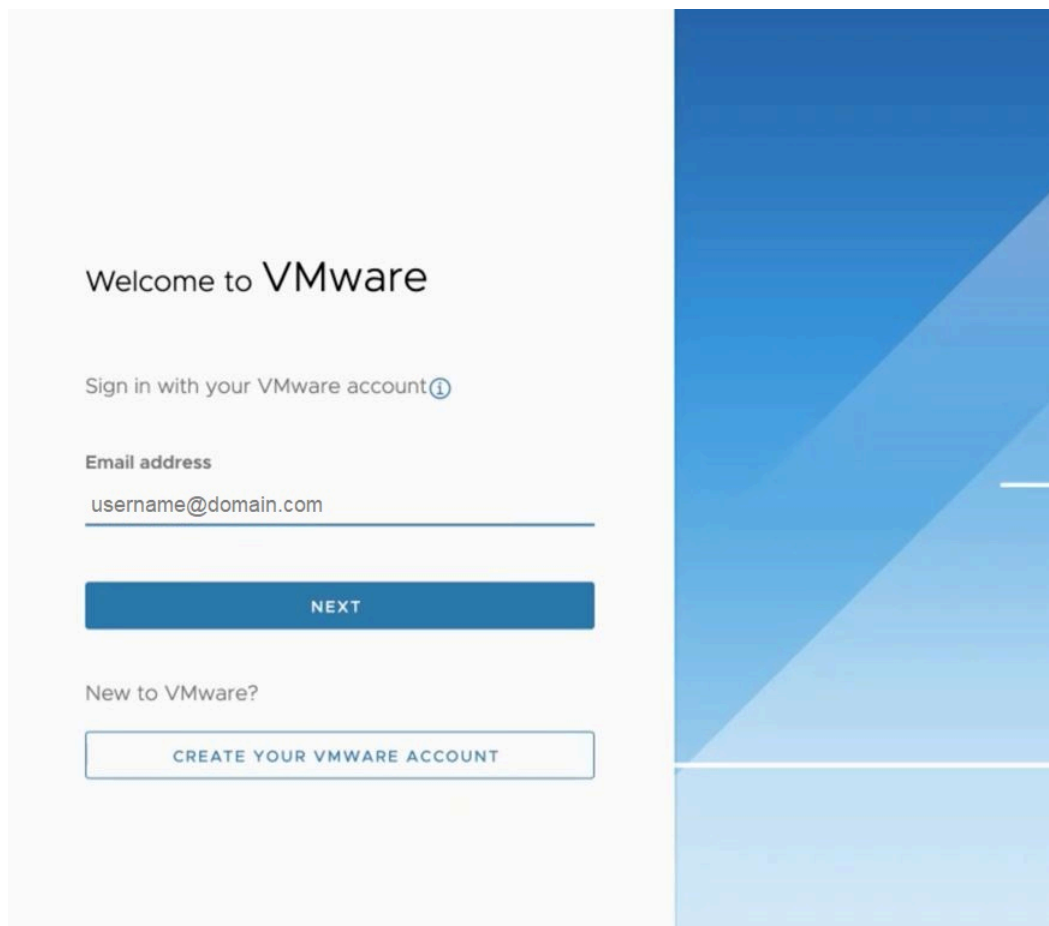
BACK TO LOGIN PAGE

The image shows a sign-in page for VMware Cloud Orchestrator. It features a light gray background on the left and a decorative graphic of overlapping blue and teal triangles on the right. The sign-in form includes a text input field labeled 'domain', a solid blue 'SIGN IN' button, and a 'BACK TO LOGIN PAGE' link.

4. You will then be redirected back to CSP.



5. On the CSP login screen, enter your email address and click **NEXT**.



Welcome to VMware

Sign in with your VMware account ⓘ

Email address

username@domain.com

NEXT

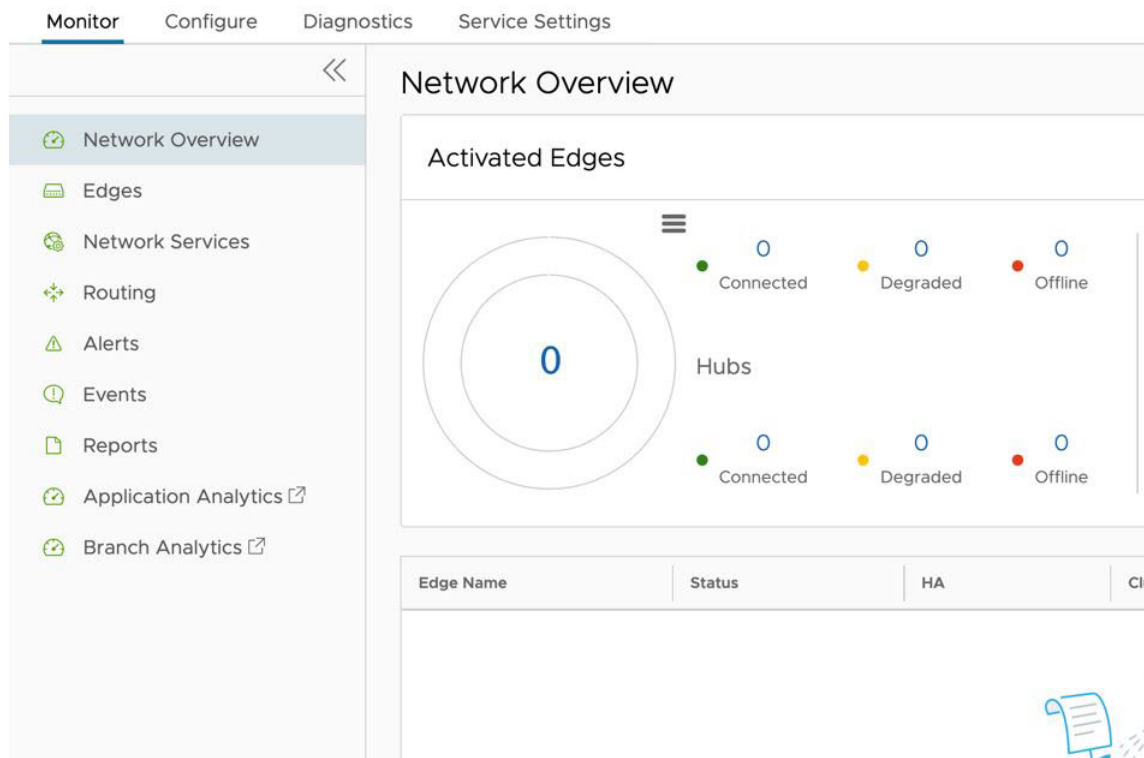
New to VMware?

CREATE YOUR VMWARE ACCOUNT



Note: Two Factor Authentication (2FA) is done using Google Authenticator. Twilio is not used for new direct customers.

6. A successful login with your CSP account will redirect you back to your enterprise home page on the Orchestrator. Your view will be consistent with the view you have been assigned in CSP.



Additional Resources

For more information about using CSP as an IdP in, see [Configure Arista CSP for Single Sign On](#).

Orchestrator Branding - Operator

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



Note: Orchestrator Branding is for dedicated Orchestrator instances only. For shared Orchestrator instances, the branding feature is not available.

To enable Operator users to customize the orchestrator UI branding at a global level, you must first activate the "Operator only Branding" feature. To activate "Operator only Branding", in the Operator portal, go to **Orchestrator > System Properties**, and set the value of the system property "operator.branding.enabled" to True.

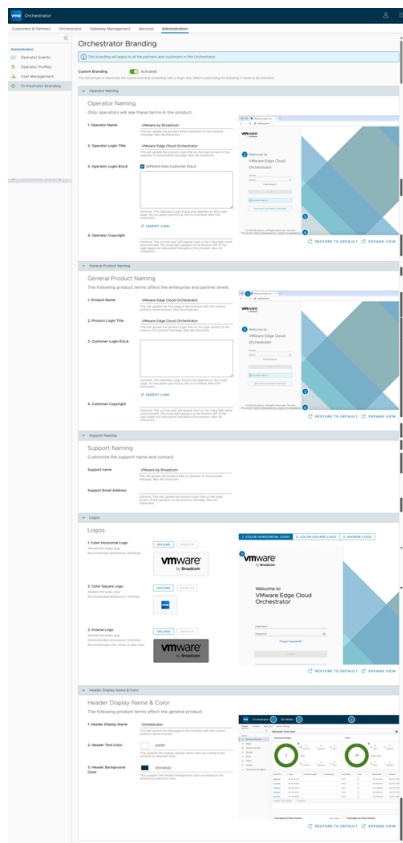


Note: Changing the operator.branding.enabled property to true will immediately override any Partner/Enterprise branding even if the Operator branding is unchanged.

By default, the value of this system property is set to False, which allows the Partner and Enterprise users to customize the Orchestrator UI branding for their Orchestrator instances at the Partner and Enterprise level, respectively.

As an Operator user, to customize the branding at a global level for all the Partners and Enterprises in the Orchestrator, perform the following steps:

1. In the Operator 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. Operator Naming
 - b. General Product Naming
 - c. Support Naming
 - d. Logos
 - e. 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 applied custom branding.



Note: The branding will apply to all the Partners and Enterprises in the Orchestrator.

7. To deactivate the "Custom Branding" feature, turn off the **Custom Branding** toggle button. All the branding settings will restored back to default.

Operator Naming Branding

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

Element	Description
Operator Name	Enter your Operator name. This updates the product title of Operator to the entered text. The Operator name can be a maximum of 48 characters.

Element	Description
Operator Login Title	Enter your Operator login title. This updates the product login title on the login screen of the Operator to the entered text. The Operator login title can be a maximum of 48 characters.
Operator Login EULA	<p>This is optional. Add your Operator login EULA with a maximum of 200 characters. The Operator login EULA only appears on the login screen.</p> <p>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.</p>
Operator Copyright	<p>This is optional. Enter your Operator copyright name and text. The current year will appear next to the copyright name automatically. The copyright appears in the bottom left of the login page and help panel throughout the product. The Operator copyright text can be a maximum of 30 characters.</p> <p>If you have not entered any customized copyright text, the default copyright will be displayed.</p>

Add link to EULA Login

Link Text

EULA

URL

https://vco/ui/operator/admin/branding

Web or any other internet address

CANCEL

SAVE

Operator Naming

Only operators will see these terms in the product.

1. Operator Name

VMware by Broadcom

This will update the product title of operator to the entered message. Max 48 characters

2. Operator Login Title

VMware Edge Cloud Orchestrator

This will update the product login title on the login screen of the operator to the entered message. Max 48 characters

3. Operator Login EULA

☒ Different than Customer EULA

Optional. The Operator Login EULA only appears on the Login page. Do not paste your EULA, link to it instead. Max 200 characters

INSERT LINK

4. Operator Copyright

Optional. The current year will appear next to the Copyright name automatically. The Copyright appears in the bottom left of the login page and help panel throughout the product. Max 30 characters

VMware Edge Cloud Orchestrator

Welcome to VMware Edge Cloud Orchestrator

Username

Password

Forgot Password?

Log In

Successfully logged out

Log in with your identity provider

© 2025 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

RESTORE TO DEFAULT

EXPAND VIEW

General Product Naming Branding

You can customize the following textual elements located on the Partner and Enterprise 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.
Customer Login EULA	<p>This is optional. Add your Customer login EULA with a maximum of 200 characters. The Customer login EULA only appears on the login screen.</p> <p>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.</p>
Customer Copyright	<p>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.</p> <p>If you have not entered any customized copyright text, the default copyright will be displayed.</p>

General Product Naming

General Product Naming

The following product terms affect the enterprise and partner levels.

1. Product Name

VMware Edge Cloud Orchestrator

This will update the title page in the browser with the custom product name entered. Max 48 characters

2. Product Login Title

VMware Edge Cloud Orchestrator

This will update the product login title on the login screen of the users to the entered message. Max 48 characters

3. Customer Login EULA

Optional. The Operator Login EULA only appears on the Login page. Do not paste your EULA, link to it instead. Max 200 characters

[INSERT LINK](#)

4. Customer Copyright

Optional. The current year will appear next to the Copyright name automatically. The Copyright appears in the bottom left of the login page and help panel throughout the product. Max 30 characters

The screenshot shows the login interface for VMware Edge Cloud Orchestrator. It includes a header with the VMware logo, a login form with fields for Username and Password, and a 'Log In' button. Below the login form, there is a 'Successfully logged in!' message and a 'Link in with your identity provider' button. The footer contains copyright information: '© 2025 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.' The interface is annotated with numbered circles 1 through 4, corresponding to the branding elements listed in the table: 1 points to the browser title, 2 points to the login title, 3 points to the EULA section, and 4 points to the copyright text.

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.

Support Naming

Support Naming

Customize the support name and contact.

Support name

VMware by Broadcom

This will update the product title of operator to the entered message. Max 48 characters

Support Email Address

Optional. This will update the product login title on the login screen of the operator to the entered message. Max 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	<p>Select and upload your custom horizontal logo by clicking Upload.</p> <p>Adhere to the following Logo requirements:</p> <ul style="list-style-type: none"> Allowed file types: png Recommended dimensions: 150X50px
Color Square Logo	<p>Select and upload your custom square logo by clicking Upload.</p> <p>Adhere to the following Logo requirements:</p> <ul style="list-style-type: none"> Allowed file types: png Recommended dimensions: 30X30px
Inverse Logo	<p>Select and upload your custom inverse logo by clicking Upload.</p> <p>Adhere to the following Logo requirements:</p> <ul style="list-style-type: none"> Allowed file types: png Recommended dimensions: 150X50px Recommended color: white or light color

Logos

Logos

1. Color Horizontal Logo

Allowed file types: png
Recommended dimensions: 150X50px

UPLOAD

REMOVE

2. Color Square Logo

Allowed file types: png
Recommended dimensions: 30X30px

UPLOAD

REMOVE

3. Inverse Logo

Allowed file types: png
Recommended dimensions: 150X50px
Recommended color: white or light color

UPLOAD

REMOVE

1. COLOR HORIZONTAL LOGO

2. COLOR SQUARE LOGO

3. INVERSE LOGO

RESTORE TO DEFAULT

EXPAND VIEW

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.

Header Display Name & Color

The following product terms affect the general product.

1. Header Display Name

Orchestrator

This will update the title page in the browser with the custom product name entered.

2. Header Text Color

#ffffff

This updates the header display name color according to the entered or selected color.

3. Header Background Color

#00364D

This updates the header background color according to the entered or selected color.

Orchestrator

SD-WAN

Network Overview

Activated Edges

Links

Edge Name

Status

Secrets Encryption

HA (Nodes)

Cluster Name

Links

Rollout State

Activated

RESTORE TO DEFAULT

EXPAND VIEW

Manage User Agreements

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

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

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

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

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

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

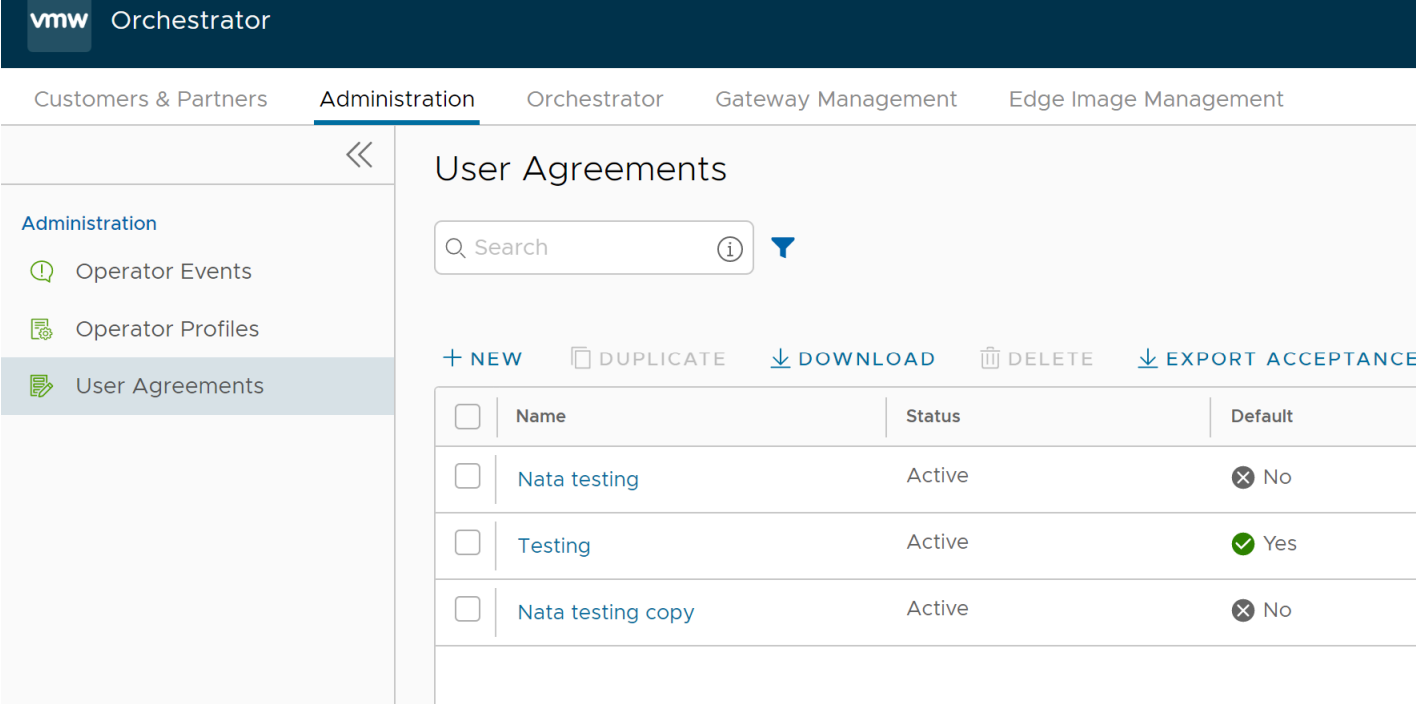
Option	Description
New	Creates a new End User License Agreement.
Duplicate	Duplicates and creates a copy of the selected User Agreement.
Download	Downloads a copy of the User Agreement details.
Delete	Deletes the selected User Agreements.
Export Acceptance Report	Exports a report of all the customers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



Note: To **Update**, click on the existing agreement in the table and update as required.

Create a User Agreement

Only Operator Super Users and Operator Standard Administrator can create a new user agreement. You can create multiple active user agreements and configure the default one from the list of active user agreements. You can also choose and configure an active user agreement that you want to show for a particular customer.



vmw Orchestrator

Customers & Partners Administration Orchestrator Gateway Management Edge Image Management

Administration

- Operator Events
- Operator Profiles
- User Agreements

User Agreements

Q Search ⓘ

+ NEW DUPLICATE DOWNLOAD DELETE EXPORT ACCEPTANCE

<input type="checkbox"/>	Name	Status	Default
<input type="checkbox"/>	Nata testing	Active	⊗ No
<input type="checkbox"/>	Testing	Active	✓ Yes
<input type="checkbox"/>	Nata testing copy	Active	⊗ No

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

User Agreement



Enabled



Default



Effective Start Date

07/27/2022



Effective End Date

10/28/2022



Dialog Title Text *

End User License Agreeer

Dialog Body Text *

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

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

This field supports [Common Mark](#)

Dialog Button Text *

Agree

CANCEL

SAVE

Option	Description
Name	Enter the name for the user agreement.
Enabled	By default, this check box is selected. If unselected, the user agreement is Inactive.

Option	Description
Effective Start Date	Enter the date from which the user agreement is effective.
Effective End Date	Enter the date until which the user agreement is effective.
Dialog Title Text	Enter a title for the user agreement.
Dialog Body Text	Enter the descriptive user agreement text that would be visible to the Customer.
Dialog Button Text	Enter the text to be displayed on the button that customer would click to accept the agreement.

- Click **Create**.


The agreements get displayed on the User Agreements page.

User Agreement



Name *

Enabled ☒

Effective Start Date 

Effective End Date 

Dialog Title Text *

Dialog Body Text *

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

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

This field supports [Common Mark](#)

Dialog Button Text *

CANCEL

CREATE

- Select an inactive agreement and click **Delete**, to delete it.



Note: Active agreements cannot be deleted.

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

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



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

To manage Gateway pools, perform the following steps:

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

The **Gateway Pools** page appears.

Customers Administration **Gateway Management** Edge Image Management

Gateway Management

- Gateways
- Gateway Pools**
- Diagnostic Bundles

Gateway Pools

Q Search ⓘ

> Map Distribution


+ NEW GATEWAY POOL CLONE DOWNLOAD DELETE

<input type="checkbox"/>	Name	Gateways
<input type="checkbox"/>	5-site-GatewayPool	2
<input type="checkbox"/>	Default Pool	0

COLUMNS REFRESH

- 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.
- 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: <ul style="list-style-type: none"> • None - Use this option when Enterprises assigned to this Gateway pool do not require Gateway Partner handoffs. • Allow - Use this option when the Gateway pool must support both Partner Gateways and Cloud Gateways. • Only (Partner Gateways) - Use this option when Edges in the Enterprise should not be assigned Cloud Gateways from the Gateway pool, but can use only the Gateway-1 and Gateway-2 that are set for the individual Edge.
Managed Pool	Specifies if a Partner can manage the Gateway pool.

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

- **New Gateway Pool** – Creates a new Gateway pool. See Create New Gateway Pool.
- **Clone** – Creates a new Gateway pool, by cloning the existing configurations from the selected Gateway pool. See Clone a Gateway Pool.
- **Download** - Downloads the CSV file for all Gateway pools or the selected Gateway pool.
- **Delete** – Deletes the selected Gateway pool. You cannot delete a Gateway pool that is already being used by a Partner or an Enterprise Customer.
- You can also configure the existing Gateway pools by 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**.

New Gateway Pool

Name *

VC GW pool

Description

Enter Description
(Optional)

Maximum 256 characters

Partner Gateway Hand Off ⓘ

Allow ▾


IP Version *

☒ IPv4
 ☐ IPv4 and IPv6

CANCEL

CREATE

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

Field	Description
IP Version	<p>Choose one of the following address types with which the Gateway pool should be enabled:</p> <ul style="list-style-type: none"> • IPv4 – Allows to add IPv4 only Gateways. • IPv4 and IPv6 – Allows to add Gateways with IPv4 and IPv6 addresses. <p> Note: If you want to use Edges with IPv6 support, then choose IPv4 and IPv6.</p>

- 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.

New Gateway Pool

×

Name *

Copy of VC GW pool

Description

Enter Description
(Optional)

Maximum 256 characters

Partner Gateway Hand Off ⓘ

Allow ▾

IP Version *

☒ IPv4
☐ IPv4 and IPv6

CANCEL

CREATE

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.

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:



Gateway Pools

Gateway Pools / Operator Pool

Properties

Operator Pool

Enter Description (Optional)

None ▾

- ☒ IPv4
- ☐ IPv4 and IPv6

✓ ASSIGN GATEWAYS

Customers




- 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**.

Assign Gateways

The option "Unassigned" lists all gateways that have not yet been assigned to a pool.

Available **UNASSIGNED (0)** ALL (0)

<input type="checkbox"/>	Name
 No Available Gateways	
0 items	



Assigned

<input type="checkbox"/>		Name
<input type="checkbox"/>	>	gateway-1
<input type="checkbox"/>	>	gateway-2
2 items		

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

CustomersAdministrationGateway ManagementEdge Image Management

<<

Gateway Management

Gateways

Gateway Pools

Diagnostic Bundles

Gateway Pools / Operator Pool

Operator Pool

Properties

Name *

Operator Pool

Description

Enter Description (Optional)

Partner Gateway Hand Off * ⓘ

None ▾

IP Version *

☒ IPv4

☐ IPv4 and IPv6

Gateways in Pool

✓ ASSIGN GATEWAYS

	Name	Location
>	gateway-1	Palo Alto, US
>	gateway-2	Palo Alto, US

2 Gateways

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

Refer to the following links to associate the Gateway pool:

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

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. They 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.

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



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

To manage Gateways, perform the following steps:

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

The **Gateways** page appears.

vmw Orchestrator

Customers Administration Gateway Management Edge Image Management

<<

Gateway Management

Gateways

Gateway Pools

Diagnostic Bundles

+

 NEW GATEWAY

🗑

 DELETE GATEWAY

⚙

 SUPPORT R

<input type="checkbox"/>		Name	Status <div>↑</div>	CPU
<input type="checkbox"/>	>	gateway-1	● Connected	38.81%
<input type="checkbox"/>	>	gateway-2	● Connected	22.09%
<input type="checkbox"/>	>	N-CA (dev)	● Offline	
<input type="checkbox"/>	>	SIN (dev)	● Offline	

☰

 COLUMNS

↺

 REFRESH

🗨

Gateways

ⓘ

🔼


📄 CSV

> Map Distribution

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	<p>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:</p> <ul style="list-style-type: none"> • Connected – Gateway is heart beating successfully to the Orchestrator. • Degraded – Orchestrator has not heard from the Gateway for at least one minute. • Offline – Orchestrator has not heard from the Gateway for at least two minutes.
CPU	Average CPU utilization of all the cores in the system at the time of the last heartbeat.
Memory	Percentage usage of the physical memory by all processes in the system as reported by 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	<p>Number of Edges connected to the Gateway at the time of the last heartbeat.</p> <p> 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.</p>
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 a Partner or an Enterprise Customer.

- **Stage to Bastion** - Stages a Gateway to the Bastion Orchestrator.
- **Unstage from Bastion** - Removes a Gateway from the Production Orchestrator.



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

For more information, see *Bastion Orchestrator Configuration Guide* available at www.arista.com/en/support/product-documentation.

- **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:

New Gateway

×

Property

Name *

GW1

IPv4 Address *

12.1.1.1

IPv6 Address

Enter IPv6

Service State

Out Of Service ▾

Gateway Pool

Default Pool (IPv4) ▾

Authentication Mode

Certificate Acquire ▾

Site Contact

Contact Name *

Super User




Contact Email *

super@velocloud.net

CANCEL

CREATE

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.

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



Note:

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

- Release 4.5.0 supports both the Greenfield and Brownfield deployment of Gateways for IPv6. If you have upgraded a Gateway from a previous version earlier than 4.5.0, you can dynamically configure IPv6 address for the Gateway.
- IPv4/IPv6 dual-stack mode is not supported for Bastion Orchestrator configuration.

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

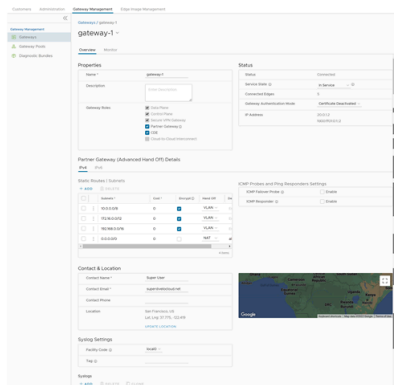
To configure additional settings for the Gateway, see [Configure Gateways](#).

Configure Gateways



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


To configure an existing Gateway:



1. In the Operator portal of the, 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:






Option	Description
Properties	<p data-bbox="870 210 1406 300">Displays the existing Name and Description of the selected Gateway. If required, you can modify the information.</p> <p data-bbox="870 321 1458 350">You can also configure the Gateway Roles, as required:</p> <ul data-bbox="870 369 1461 955" style="list-style-type: none"> • 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. <div data-bbox="907 982 956 1033"></div> <p data-bbox="992 976 1502 1102">Note: This Gateway Role option is shown if the <code>session.options.enableZscalerCci</code> system property is set to <code>True</code>.</p> <ul data-bbox="870 1108 1433 1264" style="list-style-type: none"> • Symantec Web Security Service: Enables the Gateway's Symantec Web Security Service capability. The Orchestrator assigns this Gateway to the Edge as WSS Primary Gateway or WSS Secondary Gateway. <div data-bbox="907 1287 956 1337"></div> <p data-bbox="992 1283 1430 1373">Note: This assignment works only when the Gateway Pool's Partner Gateway Handoff is not set to Only.</p>

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

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

Option	Description
IP Address	<p>Displays the public IP address that public WAN links of an Edge use to connect to the Gateway. This IP address is used to uniquely identify the Gateway. If you have configured the Gateway with both IPv4 and IPv6 addresses, this field displays both the IP addresses. If you have created IPv4 only Gateway or if there is an existing IPv4 Gateway upgraded from previous versions, you can enter the IPv6 address to support the dual stack. After you save the changes, the IPv6 address is not sent to the Edges immediately. You can trigger the rebalance operation to push the IPv6 address to the customer and the associated Edges manually or the IPv6 address is sent to the Edges during the next Control Plane update.</p> <p> Note: Adding IPv6 address is a one-time activity and once you save the changes, you cannot modify the IP addresses.</p> <p> CAUTION: An incorrectly configured IPv6 address, when pushed to Edges, might lead to failure of the IPv6 tunnelling to the IPv6 Gateway. In such cases, you need to deactivate the Gateway and create a new one to activate both the IPv4 and IPv6 addresses.</p>
Contact & Location	<p>Displays the existing contact details. If required, you can modify the information.</p>

Option	Description								
NSD IP Portability	<p>Beginning with the 6.0 Orchestrator release, selecting this option will activate NSD IP Portability for the Gateway. Portable NSD IPs allow an Operators to move NSD configurations to different Gateways in the POP without requiring the customer to reconfigure their tunnels. When the NSD Portability check box is selected, the Orchestrator fetches the following data such as SASE PoP name, NSD Virtual IPv4 Address, and NSD Virtual IPv6 Prefix currently assigned to the Gateway from the Global Services Manager (GSM) and displays it. Click Refresh POP to retrieve the current and updated data.</p> <p> Note: For the "NSD Portability" feature to work as designed, the Operators must ensure that the Gateways are associated with the corresponding PoPs in GSM.</p> <div> <h3>NSD IP Portability</h3> <p> REFRESH POP</p> <table> <tr> <td>NSD Portability</td><td><input checked="" type="checkbox"/> Enabled</td></tr> <tr> <td>SASE PoP</td><td>Hapy_Palo_Alto</td></tr> <tr> <td>NSD Virtual IPv4 Address</td><td>1.1.1.1</td></tr> <tr> <td>NSD Virtual IPv6 Prefix</td><td>2:2:2::2</td></tr> </table> </div> <p> Important: There are two important caveats with NSD IP Portability:</p> <ol style="list-style-type: none"> NSD peers must operate as an IKE responder. In the past, some configurations would permit an initiator-only setup, but that will no longer function. Peers must allow NAT-T (NAT Traversal). The current implementation of NSD Portable IP uses NAT which is internal to the POP. 	NSD Portability	<input checked="" type="checkbox"/> Enabled	SASE PoP	Hapy_Palo_Alto	NSD Virtual IPv4 Address	1.1.1.1	NSD Virtual IPv6 Prefix	2:2:2::2
NSD Portability	<input checked="" type="checkbox"/> Enabled								
SASE PoP	Hapy_Palo_Alto								
NSD Virtual IPv4 Address	1.1.1.1								
NSD Virtual IPv6 Prefix	2:2:2::2								
Syslog Settings	Beginning with the 4.5 release, Gateways can export NAT information via a remote syslog server or via telegraf to the desired destination. For more information, see the <i>Configure NAT Entry Syslog for Gateways</i> section in the <i>Operator Guide</i> 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.								

Option	Description
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 <i>Partner Gateway (Advanced Handoff) Details</i> section below.

Partner Gateway (Advanced Handoff) Details

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



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

Option	Description
<p>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.</p> <p>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.</p> <p>You can click the IPv4 or IPv6 tab to configure the corresponding address type for the Subnets.</p>	
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	
<p>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.</p>	
VLAN Tagging	<p>Select the VLAN tag from the drop-down list to apply to the ICMP probe packets. The following are the available options:</p> <ul style="list-style-type: none"> • None – Untagged • 802.1q – Single VLAN tag • 802.1ad / QinQ(0x8100) / QinQ(0x9100) – Dual VLAN tag
Destination IP address	Enter the IP address to be pinged.
Frequency	Enter the time interval, in seconds, to send the ping request. The range is from 1 to 60 seconds.
Threshold	Enter the number of times the ping replies can be missed to mark the routes as unreachable. The range is from 1 to 10.

Option	Description
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	<p>Select one of the following modes from the drop-down list:</p> <ul style="list-style-type: none"> • 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**.

Upgrade for Dual Stack Support

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

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

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

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

vmw Orchestrator

Customers & Partners
Orchestrator
Gateway Management
Edge Image Management
Administration

Administration

Operator Events
Operator Profiles
User Management

Operator Profiles / Operator profile R510

Operator profile R510 Used by 0 Customers

Profile Settings

Name *

Operator profile R510

Description

If this profile is in a Partner's Customers.

Management Settings

Orchestrator Address

IP Address ▾

Orchestrator IPv4 Address

169.254.8.2

Orchestrator IPv6 Address

Gateway Selection

Gateway Mode

☒ Dynamic
☐ Static

- Click **Save Changes**.

Configure IPv6 Address on Gateways

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

Prerequisites

Ensure that the is running version 5.0.0 as described in Upgrade for Dual Stack Support.

Deploy on AWS

Consider the following guidelines while deploying on AWS.

- While migrating Gateways on cloud, it is recommended to destroy and create new instance of Gateways with the IPv6 option enabled.
- When a is freshly deployed with a AWS c5.4xlarge instance type from the AWS portal with IPv6 option selected, it is required to only use the static mode of IPv4/IPv6 address assignment on interfaces for the Gateway because does not support DHCP on the Gateway side.

Setup IPv6 Address on Gateways for a new Deployment

1. Create a Gateway pool with IP version type as **IPv4 and IPv6**.
2. Deploy a new Gateway with version 5.0.0. You can configure IPv4 and IPv6 addresses on public interface using netplan, if IPv6 is not available in metadata.

The following example shows a sample configuration:

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

3. After updating the netplan, run `sudo netplan apply` to apply the configuration.

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

4. Activate the Gateway using IPv4 address of the Orchestrator. If the Orchestrator is provisioned with dual stack, you can activate the Gateway using either IPv4 or IPv6 address of the Orchestrator.
5. After activating, the Orchestrator will push both the IPv4 and IPv6 information to Edges.
6. Upgrade the Software version of Edge to version 5.0.0. Once the Edges are upgraded, the Orchestrator enables options to setup IPv6 related device settings.

Setup IPv6 Address on Gateways Upgraded from Previous Release

1. Upgrade the Gateways to release 5.0.0.
2. In Gateway shell, update the netplan configurations with IPv6 address. The following example shows a sample configuration:

```
vcadmin@vcg2:~$ cat /etc/netplan/50-cloud-init.yaml
network:
  ethernets:
```

```

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

```

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

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

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

For more information, refer to the following topics:

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

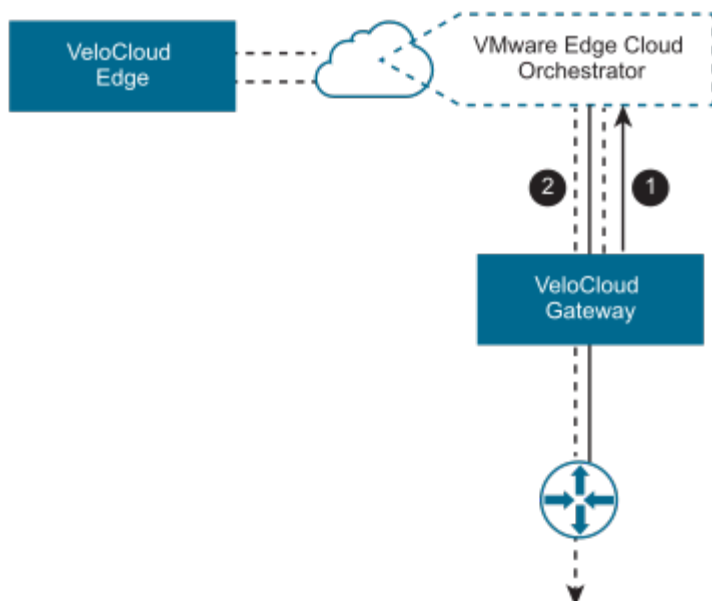
Partner Gateways

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

The examples below illustrate two use cases for Partner configuration.

Gateway Configuration Use Case #1

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

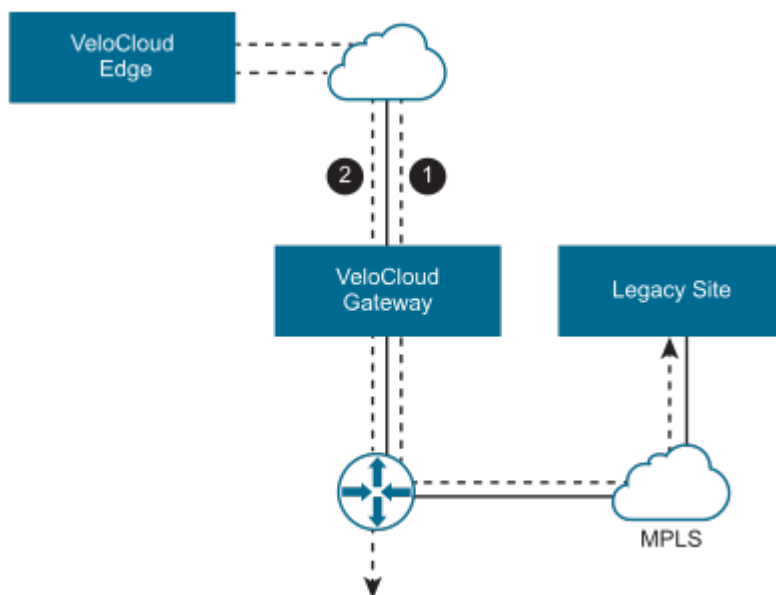


- #1 - traffic is routed using IP addresses to NAT.
- #2 - Corporate Traffic is routed through subnets to VLAN/VRF.

Configuration Use Case #2

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

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



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



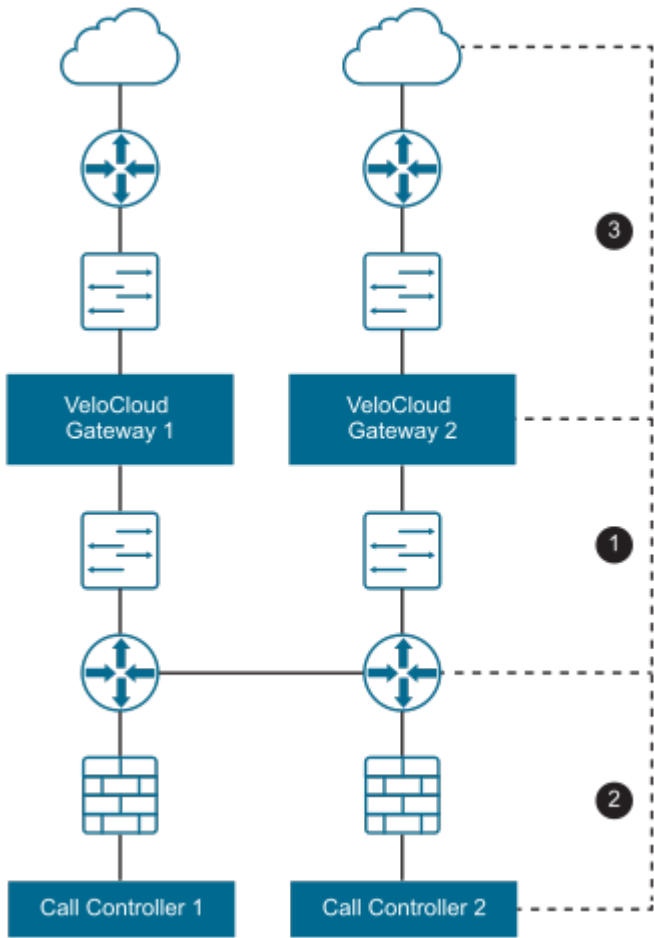
Note:

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

Partner Gateway Resiliency

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

Consider the following topology:

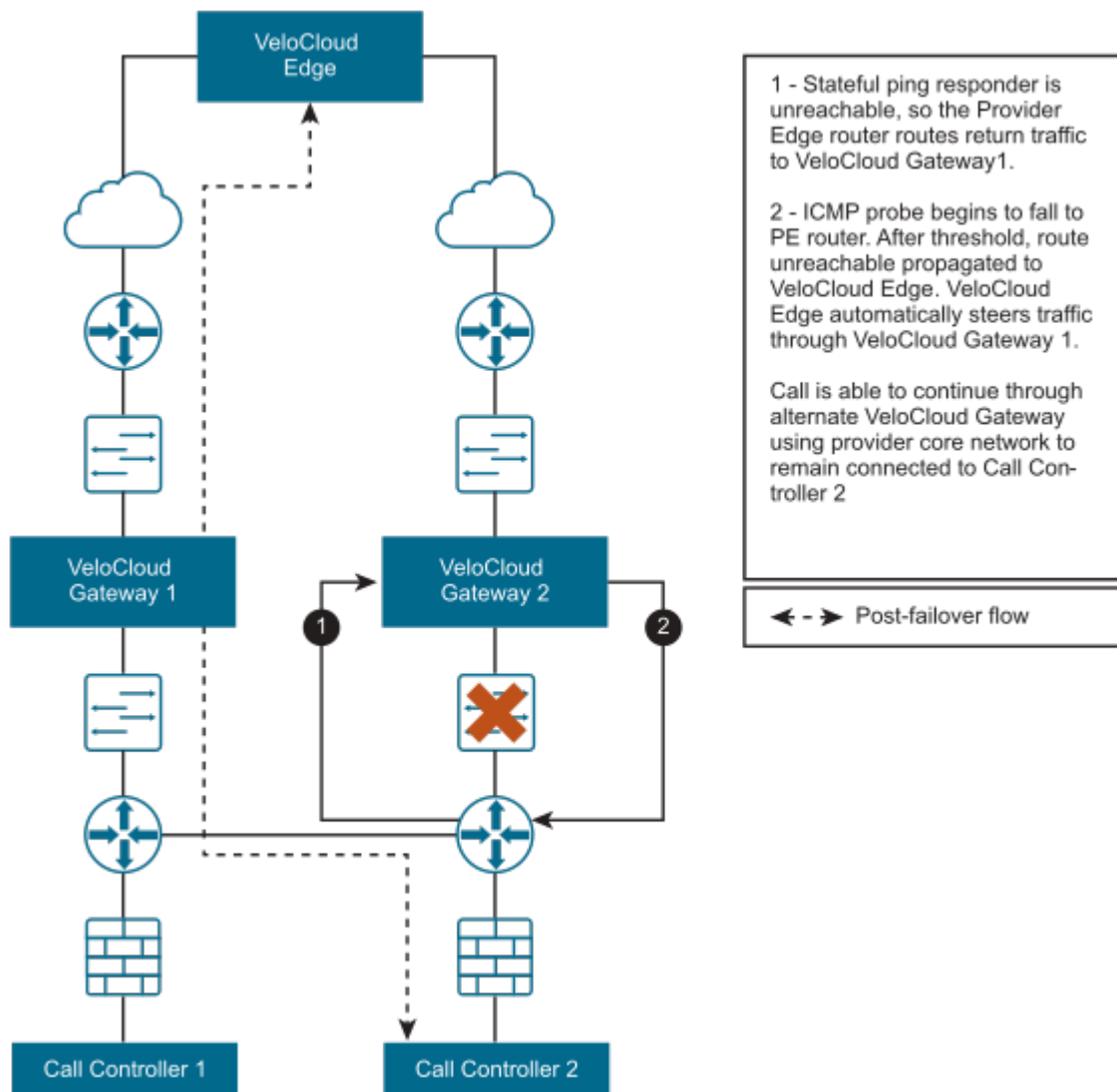


This figure shows three distinct failure zones:

Failure Zone	Component	Description
1	Provider Edge	The Provider Edge is one instance in which failure can be detected either from the Provider Edge router pinging the , or from the to the Provider Edge router.

Failure Zone	Component	Description
2	Call Controller	The should be able to ping the Provider Edge router or Call Controller to verify connectivity.
3	WAN	The should have a stateful ping responder that responds only if the WAN zone is available.

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



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

ICMP Failover Probes

This section describes ICMP failover probes.

In order to address a failure in zones #1 or #2 of the topology diagram, the supports the optional ability to send failover probes. These probes will ping a single destination IP address at the specified frequency. If the threshold for

successive missed ping replies is exceeded, the will mark the 's routes as unreachable. While the routes are marked as unreachable due to this probe failure state, probes continue to be sent. If the same threshold is exceeded for successive successful pings replies, the will mark the routes as reachable again.

Example Scenario

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

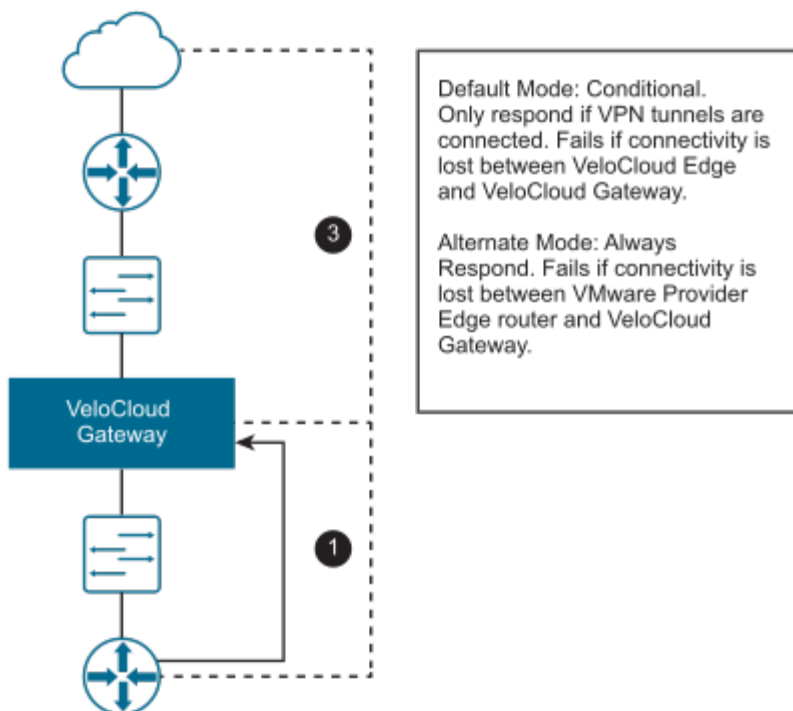
1. connect to the primary . The primary marks routes as reachable.
2. The Primary fails to receive a reply for three successive probes (~6 seconds).
3. The Primary marks routes as unreachable and communicates this to all connected .
4. begin routing traffic via the alternate .
5. Connectivity is restored and the primary receives three successive replies from probes.
6. The Primary marks routes as reachable and communicates this to all connected .
7. route traffic back through the primary .

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

Stateful Ping Responder

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

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



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

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

!tracking the IP SLA for its reachability
track 1 ip sla 1 reachability

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

Caveats When Using NAT Hand-off Mode

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

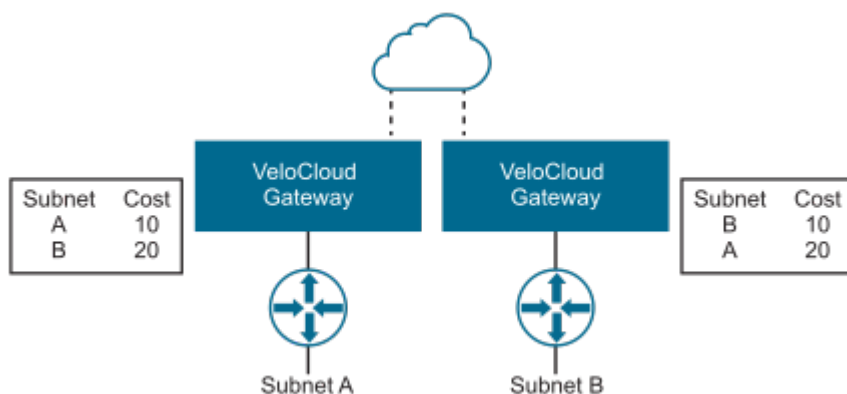
- For VLAN hand-off mode, the Partner can listen on any IP if it is reachable to the PE router (including its interface IP). For NAT hand-off mode, the Partner will not respond if the ICMP request comes to its own interface (WAN) IP address.
- Reverse flow is not supported in the NAT hand-off mode.

Active/Backup Subnets

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

Subnets on a Partner

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



Monitor Gateways

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

To monitor the :

1. In the Operator 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

Dagnostic Bundles

Gateways

Search

> Map Distribution

+ NEW GATEWAY

<input type="checkbox"/>		Name
<input type="checkbox"/>	>	gateway
<input type="checkbox"/>	>	gateway
<input type="checkbox"/>	>	N-CA (d
<input type="checkbox"/>	>	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 .

gateway-1

Overview

Monitor

Properties

Name	gateway-1
Description	<div>Enter Description</div>
Gateway Roles	<div><div><input checked="" type="checkbox"/> Data Plane</div><div><input checked="" type="checkbox"/> Control Plane</div><div><input checked="" type="checkbox"/> Secure VPN Gateway</div><div><input type="checkbox"/> Partner Gateway</div><div><input type="checkbox"/> CDE</div></div>

Status

Status

Service State

Connected Edges

Gateway Authentication M

IP Address

Contact & Location

Contact Name	Super User
Contact Email	super@velocloud.net
Contact Phone	
Location	<div>Palo Alto, US</div> <div>Lat, Lng: 37.4, -122.142</div>

For development

Google


Customer Usage

Customer	Pool
<div>No customers found for this gateway</div>	

Pool Membership

Pool	Gateway
5-site-GatewayPool	2

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

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

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

vmwOrchestrator

Customers & PartnersOrchestratorGateway ManagementEdge Im

<<

Gateway Management

Gateways

Gateway Pools

Diagnostic Bundles

Gateways / gateway-1

gateway-1

OverviewMonitor

Past 12 Hours

CPU Utilization

6:00 AM8:00 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

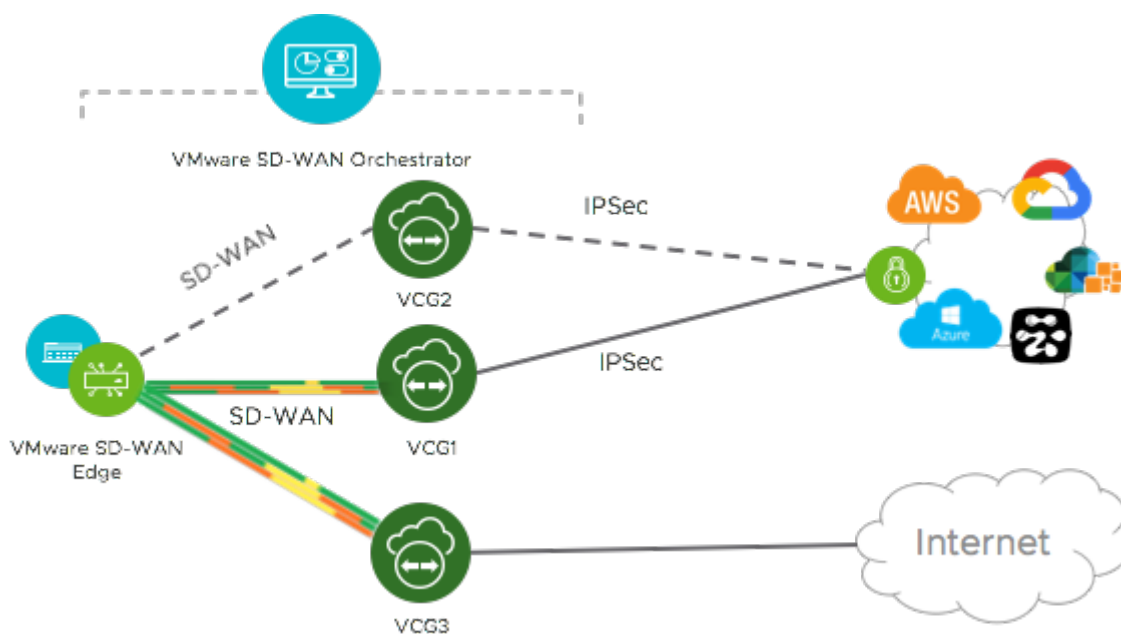
provides a self-service migration functionality that allows you to migrate from your existing Gateway to a new Gateway without your Operator's support.

Gateway migration may be required in the following scenarios:

- Achieve operational efficiency.
- Decommission old Gateways.

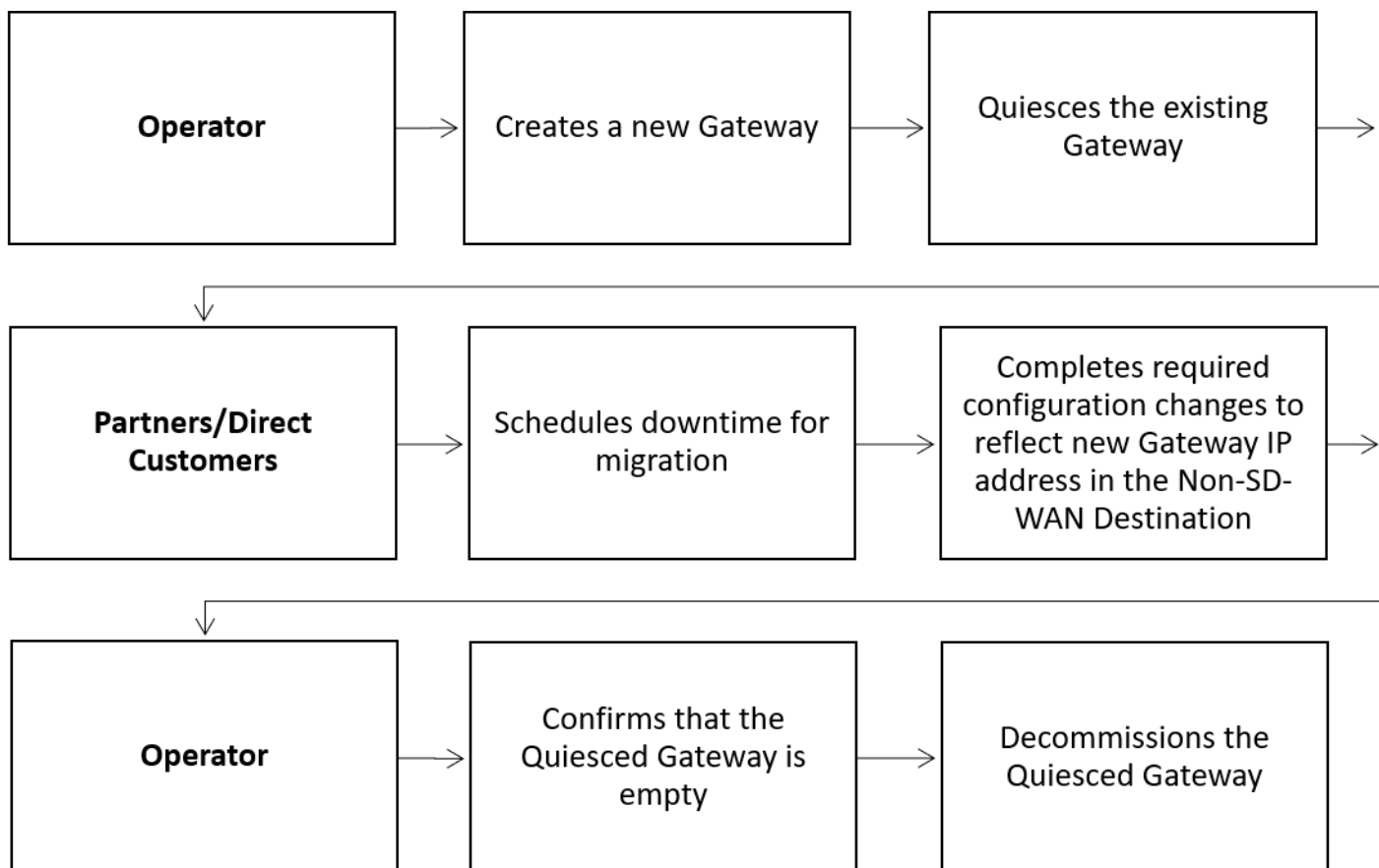
Gateways are configured with specific roles. For example, a Gateway with data plane role is used to forward data plane traffic from source to destination. Similarly, a Gateway with Control Plane role is called a Super Gateway and is assigned to an Enterprise. Edges within the Enterprise are connected 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 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.

Quiesce Gateways

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

Before you quiesce the existing Gateway, ensure that you create a new Gateway as a replacement. Assign the new Gateway with the same role and attach it to the same Gateway pool as the existing Gateway. For instructions, see the “Configure Gateways” section in the *Operator Guide* available at www.arista.com/en/support/product-documentation. Also, review the Migration - Limitations before you proceed with quiescing the Gateway.



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

To quiesce the Gateway and enable self-service migration:

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

The screenshot shows the VMware Orchestrator interface. The top navigation bar includes 'Customers & Partners', 'Orchestrator', 'Gateway Management' (selected), 'Edge Image Management', and 'Administration'. The left sidebar under 'Gateway Management' lists 'Gateways' (selected), 'Gateway Pools', and 'Diagnostic Bundles'. The main content area shows the breadcrumb 'Gateways / gateway-1' and the title 'gateway-1'. Below the title are tabs for 'Overview' (selected) and 'Monitor'. The 'Properties' section contains a form with the following fields:

Name *	gateway-1
Description	<input type="text" value="Enter Description"/>
Gateway Roles	<input checked="" type="checkbox"/> Data Plane <input checked="" type="checkbox"/> Control Plane <input type="checkbox"/> Secure VPN Gateway <input type="checkbox"/> Partner Gateway ⓘ <input checked="" type="checkbox"/> CDE <input type="checkbox"/> Cloud Web Security

3. In the **Status** section, from the **Service State** drop-down menu, select **Quiesced**.
4. Select the **Enable Self-Service Migration** check box.
5. From the **New Gateway** drop-down list, select the Gateway that you have created as a replacement to the Gateway that you are quiescing.
6. In the **Migration Deadline** date picker, select a date by when you want the Partners or direct customers to complete the migration. Ensure that the date is within 60 days from the current date.
7. Click **Save Changes**.

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

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

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



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

Decommission Quiesced Gateways

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

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

To decommission a quiesced Gateway:

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

The screenshot shows the VMware Orchestrator interface. The top navigation bar includes 'Customers & Partners', 'Orchestrator', 'Gateway Management' (selected), 'Edge Image Management', and 'Administ...'. The left sidebar shows 'Gateway Management' with sub-items: 'Gateways' (selected), 'Gateway Pools', and 'Diagnostic Bundles'. The main content area displays 'Gateways / gateway-1' and 'gateway-1' with a dropdown arrow. Below this are tabs for 'Overview' (selected) and 'Monitor'. The 'Properties' section shows a form for 'gateway-1' with fields for 'Name *', 'Description', and 'Gateway Roles'. The 'Gateway Roles' section includes checkboxes for 'Data Plane' (checked), 'Control Plane' (checked), 'Secure VPN Gateway' (unchecked), 'Partner Gateway ⓘ' (unchecked), 'CDE' (checked), and 'Cloud Web Security' (unchecked).

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

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

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 .

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



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

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**.

Request Diagnostic Bundle

×

Target

gateway-1

Reason for Generation

For troubleshooting purpose

Core Limit ⓘ

No Limit

CLOSE

SUBMIT

Table 2:

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

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

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



Gateway Management



Gateways



Gateway Pools



Diagnostic Bundles

Diagnostic Bundles

Search

+ REQUEST PCAP BUNDLE



Request Status



Complete

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.

Update Cleanup Date



☒ Remove bundle on
05/17/2022 

☐ Keep Forever

CANCEL

SAVE

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.

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



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

To generate a PCAP bundle:

1. In the Operator portal, 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**.

Request PCAP Bundle

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

Target

gateway-1

Connectivity

eth0

Duration

5 seconds

Reason for Generation

Enter reason for generation

Optional

PCAP FILTERS

ADVANCED FILTERS

IP2

is

10.0.0.0/32

IP2: Port 2

is


80

+

CLEAR

CLOS

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	<p>You can define PCAP filters by which you want to control the PCAP data to be generated by choosing the following options:</p> <ul style="list-style-type: none"> • IP1 - Enter an IPv4 address, or IPv6 address, or Subnet mask. • IP2 - Enter an IPv4 address, or IPv6 address, or Subnet mask. • IP1:Port1 - Enter a Port ID associated with IP1. • IP2:Port2 - Enter a Port ID associated with IP2. • Protocol - Select a protocol from the list. <p> Note: If you choose to use the PCAP filtering capability then you must define at least one filter.</p>
Advanced Filters	You can define free form filters by which you want to control the PCAP data to be generated.

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

4. To download a generated bundle, 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**.

Platform and Modem Firmware and Factory Images

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

Procedure

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



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

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

For more information about uploading/managing Firmware images, see the topic *Manage Operator Profiles*.

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



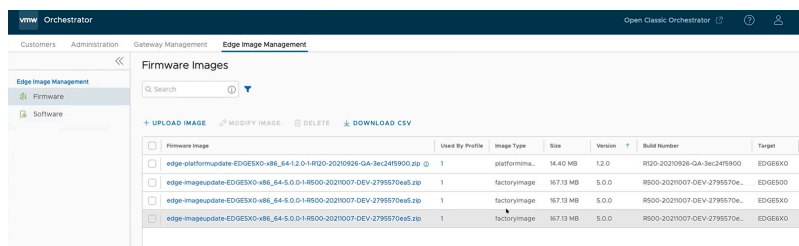
Note: It is important that you update the software version first. Then, after completion, update the firmware (Platform or Modem) and the factory default. Do not update the software version, the firmware, and the factory default at the same time.

- After the file is successfully attached, click the **Done** button in the **File Upload** dialog.

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

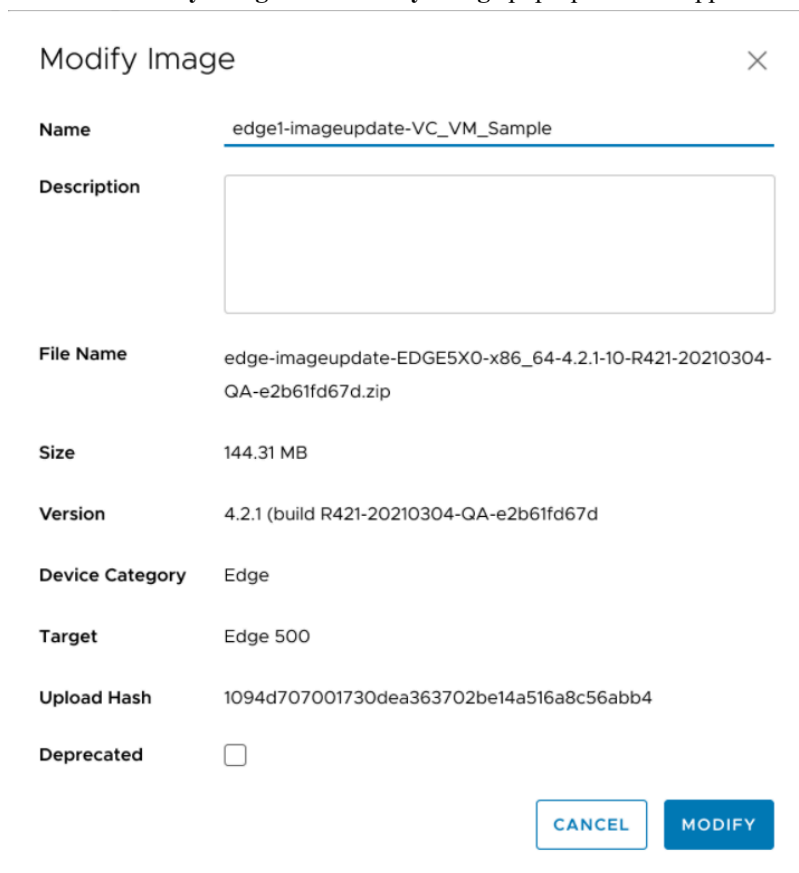


Note: When **Firmware** is selected, note the **Image Type** column which indicates if the image is (Platform Firmware or Factory Default).



	Used By Profile	Image Type	Size	Version	Build Number	Target
<input type="checkbox"/> edge-platformupdate-EDGE5X0-v86_64-4.2.1-10-R421-20210304-QA-3e24f5900.zip	1	platform	14.40 MB	4.2.0	R421-20210304-QA-3e24f5900	EDGE5X0
<input type="checkbox"/> edge-imageupdate-EDGE5X0-v86_64-5.0.0-1-R500-2021007-DEV-2795570e5.zip	1	factoryimage	167.13 MB	5.0.0	R500-2021007-DEV-2795570e5	EDGE500
<input type="checkbox"/> edge-imageupdate-EDGE5X0-v86_64-5.0.0-1-R500-2021007-DEV-2795570e5.zip	1	factoryimage	167.13 MB	5.0.0	R500-2021007-DEV-2795570e5	EDGE5X0
<input type="checkbox"/> edge-imageupdate-EDGE5X0-v86_64-5.0.0-1-R500-2021007-DEV-2795570e5.zip	1	factoryimage	167.13 MB	5.0.0	R500-2021007-DEV-2795570e5	EDGE5X0

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



×

Name

edge1-imageupdate-VC_VM_Sample

Description

File Name

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

Size

144.31 MB

Version

4.2.1 (build R421-20210304-QA-e2b61fd67d)

Device Category

Edge

Target

Edge 500

Upload Hash

1094d707001730dea363702be14a516a8c56abb4

Deprecated

☐

CANCEL

MODIFY

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



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



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

8. To delete a package from the portal, select the image and click **Delete** (depending upon which option you have chosen).

Delete Image

×

Are you sure you want to delete these images? This action cannot be undone.

☒ Yes, I want to permanently delete these images.

CANCEL

DELETE

What to do next

To manage within an Enterprise with a specific Software/Firmware Image, see the topic *Manage Operator Profiles* .

Software Images

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

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

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

[illegible]



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

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



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



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

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

To upgrade the Edges within an Enterprise with a specific Software Image, see Manage Operator Profiles.

Edge Licensing

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

The Edge Licensing feature is activated by default.

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

The Edge Licenses are available with the following components:

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



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

Edge Licensing

Q Search

i

[↓ DOWNLOAD REPORT](#)

Name	Term	Bandwidth	Edition	Region
ENTERPRISE 10 Mbps ...	60 Months	10 Mbps	Enterprise	North America, Europe..
ENTERPRISE 10 Mbps ...	12 Months	10 Mbps	Enterprise	Asia Pacific
ENTERPRISE 10 Mbps ...	36 Months	10 Mbps	Enterprise	Asia Pacific
ENTERPRISE 10 Mbps ...	60 Months	10 Mbps	Enterprise	Asia Pacific
ENTERPRISE 10 Mbps ...	12 Months	10 Mbps	Enterprise	Latin America
ENTERPRISE 10 Mbps ...	36 Months	10 Mbps	Enterprise	Latin America
ENTERPRISE 10 Mbps ...	60 Months	10 Mbps	Enterprise	Latin America
PREMIUM 10 Mbps N...	12 Months	10 Mbps	Premium	North America, Europe..
<div></div> COLUMNS	<div></div> REFRESH			

- 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.
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 assign Edge Licenses to new Partners, see Create New Partner.

To manage and assign Edge Licenses to existing Partners, see Manage Edge Licenses for Partners.

To assign Edge Licenses to new Customers, see Create New Customer.

To manage and assign Edge Licenses to existing Customers, see Manage Edge Licenses for Customers.

Manage Edge Licenses for Partners

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

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

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

MonitorConfigureDiagnosticsService Settings

<<

Alerts & Notifications

Edge Licensing

Gateway Migration

Edge Management

Edge Auto-activation

Edge Licensing

Q Search

ⓘ

⌵

↓ CSV

MANAGE EDGE LICENSING

DOWNLOAD REPORT

Name
STANDARD 10 Mbps North America, Europe Middle East and A

◀

COLUMNS

REFRESH

4. Click **Manage Edge Licensing**.

Select Edge Licenses

Search for Available Edge Licenses

Start typing License information or SKU

Search for Selected Edge Licenses

Start typing License information or SKU

☐

Available Edge Licenses

☐

STANDARD | 10 Mbps | North America, Europe Middle East and Africa | 60 Months

VMware SD-WAN by VeloCloud STANDARD edition, applicable to the North America, Europe Middle East and Africa regions, has a bandwidth up to 10 Mbps and is valid for 60 Months

☐

STANDARD | 10 Mbps | Asia Pacific | 12 Months

VMware SD-WAN by VeloCloud STANDARD edition, applicable to the Asia Pacific region, has a bandwidth up to 10 Mbps and is valid for 12 Months

☐

STANDARD | 10 Mbps | Asia Pacific | 36 Months

VMware SD-WAN by VeloCloud STANDARD edition, applicable to the Asia Pacific region, has a bandwidth up to 10 Mbps and is valid for 36 Months

☐

STANDARD | 10 Mbps | Asia Pacific | 60 Months

1 - 20 of 317 items

<<

<

1

>

>>

☐

Select Edge Licenses

☐

ENTERPRISE | 100 Mbps | North America, Europe Middle East and Africa | 60 Months

VMware SD-WAN by VeloCloud ENTERPRISE edition, applicable to the North America, Europe Middle East and Africa regions, has a bandwidth up to 100 Mbps and is valid for 60 Months

☐

ENTERPRISE | 100 Mbps | Asia Pacific | 12 Months

VMware SD-WAN by VeloCloud ENTERPRISE edition, applicable to the Asia Pacific region, has a bandwidth up to 100 Mbps and is valid for 12 Months

☐

ENTERPRISE | 100 Mbps | Asia Pacific | 36 Months

VMware SD-WAN by VeloCloud ENTERPRISE edition, applicable to the Asia Pacific region, has a bandwidth up to 100 Mbps and is valid for 36 Months

☐

ENTERPRISE | 100 Mbps | Asia Pacific | 60 Months

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

Manage Edge Licenses for Customers

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

- 1. In the Operator portal, click **Manage 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**.

MonitorConfigureDiagnosticsService Settings

<<

Alerts & Notifications

Edge Licensing

Gateway Migration

Edge Management

Edge Auto-activation

Edge Licensing

Q Search

i

Filter

Download CSV

MANAGE EDGE LICENSING

Download Report

Name
STANDARD 10 Mbps North America, Europe Middle East and Africa

Columns

Refresh

- 4. Click **Manage Edge Licensing**.

Select Edge Licenses

Search for Available Edge Licenses

Start typing License information or SKU

<input type="checkbox"/>	Available Edge Licenses
<input type="checkbox"/>	STANDARD 10 Mbps North America, Europe Middle East and Africa 60 Months VMware SD-WAN by VeloCloud STANDARD edition, applicable to the North America, Europe Middle East and Africa regions, has a bandwidth up to 10 Mbps and is valid for 60 Months
<input type="checkbox"/>	STANDARD 10 Mbps Asia Pacific 12 Months VMware SD-WAN by VeloCloud STANDARD edition, applicable to the Asia Pacific region, has a bandwidth up to 10 Mbps and is valid for 12 Months
<input type="checkbox"/>	STANDARD 10 Mbps Asia Pacific 36 Months VMware SD-WAN by VeloCloud STANDARD edition, applicable to the Asia Pacific region, has a bandwidth up to 10 Mbps and is valid for 36 Months
<input type="checkbox"/>	STANDARD 10 Mbps Asia Pacific 60 Months
1 - 20 of 317 items	

Search for Selected Edge Licenses

Start typing License information or SKU

<input type="checkbox"/>	Selected Edge Licenses
<input type="checkbox"/>	ENTERPRISE 10 Mbps North America, Europe Middle East and Africa 60 Months VMware SD-WAN by VeloCloud ENTERPRISE edition, applicable to the North America, Europe Middle East and Africa regions, has a bandwidth up to 10 Mbps and is valid for 60 Months
<input type="checkbox"/>	ENTERPRISE 10 Mbps Asia Pacific 12 Months VMware SD-WAN by VeloCloud ENTERPRISE edition, applicable to the Asia Pacific region, has a bandwidth up to 10 Mbps and is valid for 12 Months
<input type="checkbox"/>	ENTERPRISE 10 Mbps Asia Pacific 36 Months VMware SD-WAN by VeloCloud ENTERPRISE edition, applicable to the Asia Pacific region, has a bandwidth up to 10 Mbps and is valid for 36 Months
<input type="checkbox"/>	ENTERPRISE 10 Mbps Asia Pacific 60 Months

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



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

- 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 **Report** to generate a report of the licenses and the associated in a CSV format.

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

To assign a license to an existing :

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

Application Maps

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

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

Action	Name	Profiles	Uploaded	Last Modified
Download	Initial Application Map Tue Mar 04 2025 12:52:48 GMT+0000 (Coordinated Universal Time) Created on system initialization, schema version 4.1.0	3	Mar 4, 2025, 6:22:48 P.	Mar 4, 2025, 6:22:49 P.



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

You can perform the following actions on this page:

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

Upload Application Map

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

- To upload a map file, click **Upload**.
- In the **File Upload** window, you can either drag and drop, or browse and choose the Application Map file to be uploaded.
- Click **Done**. The file is uploaded after the content is validated.
- The Application Map file is in JSON format and you can customize the applications as per your requirements. The following example illustrates a customized JSON file for the application `bittorrent`.

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

```

"protocolPortMapping": {},
"doNotSlowLearn": 1,
"mustNotUseGateway": 1
}

```

Clone Application Map

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

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

Refresh Application Map

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

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



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

Push Application Map

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

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



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



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



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

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

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

Edit Application Map

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

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

Application Maps / Initial Application Map Mon Jul 04 2022 07:48:08 GMT+0000 (Coordinated Universal Time)

Initial Application Map Mon Jul 04 2022 07:4...

Name *

Initial Application Map Mon Jul 04 2022 07:48:08 GMT+00

Description

Created on system initialization, schema version 4.1.0

Applications

+ ADD  DELETE

		Id	↓
<input checked="" type="radio"/>	<<	5014	
<input type="radio"/>	>>	5013	
<input type="radio"/>	>>	5012	
<input type="radio"/>	>>	5011	
<input type="radio"/>	>>	5010	
<input type="radio"/>	>>	5009	
<input type="radio"/>	>>	5008	
<input type="radio"/>	>>	5007	
<input type="radio"/>	>>	5006	
<input type="radio"/>	>>	5005	
<input type="radio"/>	>>	5004	
<input type="radio"/>	>>	5003	
<input type="radio"/>	>>	5002	

TencentMeeting

Name *

APP_TENCENT_MEETING

Display Name *

TencentMeeting

Description *

Tencent and VooV Meeting

App ID 5014

Category *

Business Collaboration

Known IP Port Mapping

TCP Ports

Delete Application Map

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

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

Edge Management

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

1. In the Operator portal, on the **Monitor Customers** screen, click on a Customer name.
2. 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 10 days)

Number of days

▼ Edge Authentication

Default Certificate

☒ Certificate Acquire (Certificate Authority)

Edge Authentication ⓘ

ACTIVATE SECURE EDGE

▼ Device Secret Encryption

Enable Encrypt Device Secrets ⓘ

ENABLE FOR ALL EDGES

▼ Configuration Updates

Enable Edge Configuration Updates

☒ On

When this option is set to on, configuration updates are actively pushed to Edges. When this option is turned off, pending configuration 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 Edge configuration updates automatically, and after the upgrade the Operator resumes these Edge configuration updates. When this option is turned off, Edge configuration updates after the Orchestrator is upgraded, and these Edge configuration updates would only resume after the next Orchestrator upgrade.

▼ Software & Firmware Images

	Is Default?	Operator Profile	Software & Firmware Images
▼	<input checked="" type="radio"/>	3-site-Operator	5.2.0.0 (build R5200-20230323)
		3-site-Operator	
		Description:	
		Software Image:	5.2.0.0 (build R5200-20230323-MH-feOc25d5bf)
		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 <code>edge.link.show.limit.sec</code> .
Number of days	Enter a value in the range 1 to 365 . The default value is 1 .
Edge Authentication	
Default Certificate	<p>Choose the default option to authenticate the Edges associated to the Customer.</p> <ul style="list-style-type: none"> Certificate Acquire: This option instructs the Edge to acquire a certificate from the certificate authority of the , 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. <p> Note: Only after acquiring the certificate, the option can be updated to Certificate Required.</p> 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. <p> 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.</p>
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. For more details, see Configure User Account details.
Device Secret Encryption	

Option	Description
Enable Encrypt Device Secrets	<p>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.</p> <p> Note: You can activate this option for individual Edges at the time of creating a new Edge. For more information, see the topic <i>Provision a New Edge</i> in the Arista SD-WAN Administration Guide.</p>
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

To view this section, an Operator user must follow the below steps:

1. Navigate to the **Global Settings** service of the Enterprise portal.
2. Go to **Customer Configuration > SD-WAN Configuration**.
3. Select the **Allow Customer to manage software** check box.



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

For more information, see the topics Platform and Modem Firmware and Factory Images and Software Images.

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 Operator User
 - Configure Operator 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 Operator users:

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

Commands	Description	Access Level = Basic	Access Level = Privileged
pagination	Paginates the output.	Yes	Yes
clear	Clears the screen.	Yes	Yes
EOF	Exits the secure Edge CLI.	Yes	Yes
Debug Commands			
edgeinfo	Displays the Edge's hardware and firmware information. For a sample output of the command, see edgeinfo.	Yes	Yes
seainfo	Displays details about the secure Edge access of the user. For a sample output of the command, see seainfo.	Yes	Yes
ping, ping6	Pings a URL or an IP address.	Yes	Yes
tcpdump	Displays TCP/IP and other packets being transmitted or received over a network to which the Edge is attached. For a sample output of the command, see tcpdump.	Yes	Yes
pcap	Captures the packet data pulled from the network traffic and prints the data to a file. For a sample output of the command, see pcap.	Yes	Yes
debug	Runs the debug commands for Edges. Run <code>debug -h</code> to view a list of available commands and options. For a sample output of one of the debug commands, see <code>debug --dpdk_ports_dump</code> .	Yes	Yes
diag	Runs the remote diagnostics commands. Run <code>diag -h</code> to view a list of available commands and options. For a sample output of one of the diag commands, see <code>diag ARP_DUMP</code> .	Yes	Yes
ifstatus	Fetches the status of all interfaces. For a sample output of the command, see ifstatus.	Yes	Yes

Commands	Description	Access Level = Basic	Access Level = Privileged
getwanconfig	Fetches the configuration details of all WAN interfaces. Use the logical names such as "GE3" or "GE4" as arguments to fetch the configuration details of that interface. Do not use the physical names such as "ge3" or "ge4" of the WAN interfaces. For example, run <code>getwanconfig GE3</code> to view the configuration details of the GE3 WAN interface. Run the <code>ifstatus</code> command to know the interface name mappings. For a sample output of the command, see <code>getwanconfig</code> .	Yes	Yes
Configuration Command			
setwanconfig	Configures WAN interfaces (wired interfaces only). Run <code>setwanconfig -h</code> to view configuration options.	Yes	Yes
Edge Actions Commands			
deactivate	Deactivates the Edges and reapplies the initial default configuration.	No	Yes
restart	Restarts the SD-WAN service.	No	Yes
reboot	Reboots the Edge.	No	Yes
shutdown	Powers off the Edge.	No	Yes
hardreset	Deactivates the Edges, restores the Edge's default configuration, and restores original software version.	No	Yes
edged	Activates or deactivates the Edge processes.	No	Yes
restartdhcpserver	Restarts the DHCP server.	No	Yes
Linux Shell Command			
shell	Takes you into the Linux shell. Type <code>exit</code> 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:

vmw

Orchestrator

Customers & Partners

Orchestrator

Gateway Management

Services

Administration

<<

Customers & Partners

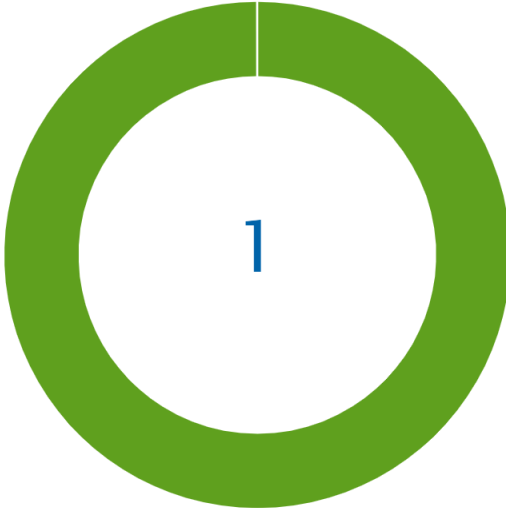
Monitor Customers

Manage Partners

Manage Customers

Customers

Total Customers






A donut chart with a green ring and a white center. The number '1' is displayed in the center, indicating the total number of customers.

Customer	# Down Edges
5-site-cluster	-

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

My Account


Profile Role & Privileges API Tokens SSH Keys

Username	super@velocloud.net	
Contact Email * ⓘ	test@vmware.com	
Current Password *	
New Password	
Confirm Password *	
First Name	Super	
Last Name	User	
Phone		
Mobile Phone	+1 ▾	

UPDATE

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.

My Account

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

Role

Operator Superuser

Description

Can view, edit and create additional operators, global settings, and has full access across the system.

Privileges associated to role

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

Privileges

Edge Access

Basic ⓘ

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

My Account

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

New Token

Name *	test
Description	test123
Lifetime *	12 <small>Months</small>

GENERATE KEY
CANCEL

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

My Account

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

Generate SSH Key

User Name *

o2super_velocloud_net

Actions *

☐ Generate Key ☒ Enter Key

Enter Key

test11234@

Duration * ⓘ



30 Days

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

GENERATE KEY

CANCEL

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

Option	Description
Actions	<p>Select either one of the following options:</p> <ul style="list-style-type: none"> • Generate key: Use this option to generate a new pair of public and private SSH keys. <p> Note: The generated key gets downloaded automatically. The default file format in which the SSH key is generated is .pem. If you are using a Windows operating system, ensure that you convert the file format from .pem to .ppk, and then import the key. For instructions to convert .pem to .ppk, see Convert Pem to Ppk File Using PuTTYgen.</p> • Enter key: Use this option to paste or enter the public key if you already have a pair of SSH keys.
PassPhrase	<p>If Generate key option is selected, then you have to enter a unique passphrase to further safeguard the private key stored on your computer.</p> <p> Note: This is an optional field and is available only if you select the Generate Key action.</p>
Duration	<p>Select the number of days by when the SSH key must expire.</p>

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.

Orchestrator Diagnostics

The Diagnostics bundle is a collection of diagnostic information to troubleshoot the. For Orchestrator on-prem installation, Operators can collect the Diagnostic bundle from the Orchestrator UI and provide it to the Arista Support team for offline analysis and troubleshooting.

In the Operator portal, navigate to **Orchestrator > System Properties**, and then set the System property `session.options.enableBastionOrchestrator` to **True** to view the **Diagnostics** tab.

vmw Orchestrator

Customers & Partners **Orchestrator** Gateway Management Edge Image Management

Diagnostic Bundles Database Statistics

Q Search ⓘ ⚙ ⬇ CSV

+ REQUEST DIAGNOSTIC BUNDLE ⬇ DOWNLOAD BUNDLE

<input type="checkbox"/>	Request Status	Reason for Generation
<input type="checkbox"/>	COMPLETE	

The following are the options available to troubleshoot Diagnostics:

- **Diagnostic Bundles:** Request and download a diagnostic bundle.
- **Database Statistics:** Provides read-only access view of some of the information from a diagnostic bundle.

Diagnostic Bundles

To access the diagnostic bundles perform the following steps:

1. In Operator portal, click the **Orchestrator** tab.
2. In the left navigation pane, click **Diagnostics**.

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

vmw Orchestrator

Customers & Partners
Orchestrator
Gateway Management
Edge Image Manager

<<

Bastion
Diagnostics
Replication
System Properties
Orchestrator Upgrade
Certificate Authorities

Diagnostic Bundles Database Statistics

Q Search ⓘ
F
↓ CSV

+ REQUEST DIAGNOSTIC BUNDLE
↓ DOWNLOAD BUNDLE

<input type="checkbox"/>	Request Status	Reason for Generation
<input type="checkbox"/>	COMPLETE	

The Orchestrator Diagnostics table grid includes the following information:

Field	Description
Request Status	<p>The following are the request status:</p> <ul style="list-style-type: none"> Complete In Progress <p>If a bundle has not completed the download, the In Progress status appears.</p>
Reason for Generation	The specific reason given for generating a diagnostic bundle. Click the Request Diagnostic Bundle button to include a description of the bundle.
User	The individual logged into the SD-WAN Orchestrator.
Generated	The date and time when the diagnostic bundle request was sent.
Update Cleanup Date	The default Cleanup Date is three months after the generated date, when the bundle will be automatically deleted. If you wish to extend the cleanup date, then select the bundle and then click this option to make the required changes. For more information, see the Update Cleanup Date section below..

Request Diagnostic Bundle

To generate a new Diagnostic bundle perform the following steps:

1. Click the **Request Diagnostic Bundle** button.
2. In the **Request Diagnostic Bundle** dialog, enter the reason for generation.

Request Diagnostic Bundle



Reason for Generation

CLOSE

SUBMIT

Field	Description
Reason for Generation	Optionally, you can enter your reason for generating the bundle.

3. Click **Submit**.

The **Diagnostics 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.

Download Bundle

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

To download a generated bundle, select the required check box in the **Request Status** column 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.

Update Cleanup Date

The completed bundles get deleted automatically on the date displayed in the column called **Cleanup Date**.

1. To update the cleanup date of a generated bundle, select the required check box in the **Request Status** column and click **Update Cleanup Date**.
2. In the **Update Cleanup Date** pop-up window, choose the date on which the selected bundles should be deleted and click **Update**.

Update Cleanup Date



☒ Remove bundle on*

10/03/2022 17:01



☐ Keep Forever

CANCEL

UPDATE

3. Select the **Keep Forever** check box to retain the bundle, so that the bundle does not get deleted automatically.

The Orchestrator Diagnostics table grid updates to reflect the changes to the Cleanup Date.

Delete

To delete a bundle manually, select the required check box in the **Request Status** column and click **Delete**.

Database Statistics

The Database Statistics tab provides read-only access view of the information from a diagnostic bundle. To view it, click **Database Statistics** option available at the top of the window.

If you require additional information, go to the **Diagnostic Bundles** tab, request a diagnostic bundle, and download it locally.

The Database Statistics tab displays the following information:

vmw

Orchestrator

Customers & Partners

Administration

Orchestrator

Gateway Management

Edge Image

<<

Bastion

Diagnostics

System Properties

Orchestrator Upgrade

Diagnostics Bundles

Database Statistics

Database Sizes

Size of all Orchestrator databases.

Database Name
Total Size
velocloud
velocloud_ca
velocloud_dr
velocloud_stats
<div>COLUMNS</div>

Database Table Statistics

Statistics details of all tables in Orchestrator databases.

Q Search

i

↓ CSV

Database Name	Table Name
velocloud_stats	VELOCLOUD_FLOW_STATS_WEEKLY
velocloud_stats	VELOCLOUD_FLOW_STATS_DAILY
velocloud	VELOCLOUD_ENTERPRISE_EVENT
velocloud	VELOCLOUD_CONFIGURATION_MODU
velocloud	VELOCLOUD_EDGE_FIREWALL_LOGS
velocloud	VELOCLOUD_EDGE_STATS
velocloud	VELOCLOUD_FLOW_STATS
velocloud	VELOCLOUD_FLOW_STATS_RES_24
velocloud	VELOCLOUD_FLOW_STATS_RES_576

Field	Description
Database Sizes	Sizes of the Orchestrator databases.
Database Table Statistics	Statistical details of all tables in the Orchestrator database.
Database Storage Info	Storage details of the mounted locations.
Database Process List	The top 20 records of long-running SQL queries.
Database Status Variable	The status variables of the MySQL server
Database System Variable	System variables of the MySQL server.
Database Engine Status	The InnoDB engine status of the MySQL server.

Orchestrator Upgrade with New Orchestrator UI

This section describes the prerequisites and steps required to upgrade a. Orchestrator allows you to configure and send a banner message about an upcoming Orchestrator upgrade. The banner is displayed to users the next time they login to the. You can customize the banner message and visibility for the users.

To upgrade a, perform the following steps:

1. Configure Orchestrator Upgrade Announcement
2. Prepare Orchestrator Upgrade
3. Complete Orchestrator Upgrade

Configure Orchestrator Upgrade Announcement

The **Upgrade Announcement** area enables you to configure and send a message about an upcoming upgrade. To send an Orchestrator Upgrade announcement, perform the following steps:

1. In the Operator portal, click the **Orchestrator** tab, and go to **Orchestrator Upgrade** in the left navigation pane. The **Orchestrator Upgrade** screen appears.



Bastion



System Properties



Orchestrator Upgrade

Orchestrator Upgrade



Currently there is no "Upcoming"

- 1. Use the Upgrade Announcement
- 2. Use "Prepare Orchestrator Upg
- level and (b) Display the system c
- 3. Once the Orchestrator Upgrad
- updates to edges continues to be

Upgrade Announcement

Banner Message *

Visibility

Upgrade Actions

PREPARE ORCHESTRATOR UPGRAD

- Under Upgrade Announcement, set the banner message and visibility for the users.

Option	Description
Banner Message	<p>Enter the required Banner Message in the textbox to announce the status of an upcoming upgrade.</p> <p>A popup message appears indicating that you have successfully created your announcement, and your banner message displays at the top of the Orchestrator.</p>
Visibility	<p>You can choose the banner Visibility for the users. By default, Operator only is selected.</p>

- Click the **Announce Orchestrator Upgrade** button to display the banner message.

A popup message appears indicating that you have successfully created your announcement, and that your banner message displays at the top of the Orchestrator.

- If you want to remove the announcement from the Orchestrator, click the **Unannounce Orchestrator Upgrade** button.

A popup message appears indicating that you have successfully unannounced the Orchestrator upgrade.

Prepare Orchestrator Upgrade

After you have configured the Orchestrator upgrade banner message and visibility for the users, click the **Prepare Orchestrator Upgrade** button. This pauses the application of the configuration updates of Edges during the upgrade, at the global level and by default at the enterprise level. It displays the system configured message as the banner message while the upgrade is in progress.



Customers & Partners

Administration

Orchestrator

Orchestrator
deactivated

Bastion



System Properties



Orchestrator Upgrade

Orchestrator Upgrade



The upgrade announcement mes

1. Click the "Unannounce Orchestrator
2. Use "Prepare Orchestrator Upgrade" level and (b) Display the system con
3. Once the Orchestrator Upgrade is updates to edges continues to be p

Upgrade Announcement

Banner Message ***Visibility**

Upgrade Actions

Contact the Support team to prepare for the Orchestrator upgrade.

1. Collect the following information prior to contacting Support:

- Provide the current and target Orchestrator versions, for example: current version (ie 2.5.2 GA-20180430), target version (3.3.2 p2).



Note: For the current version, this information can be found on the top, right corner of the Orchestrator by clicking the **Help** icon.

- Provide a screenshot of the replication dashboard of the Orchestrator as shown below.
- Hypervisor Type and version (ie vSphere 6.7)
- Commands from the Orchestrator:



Note: Commands must be run as root (e.g. 'sudo <command>' or 'sudo -i').

- Run the script `/opt/vc/scripts/vco_upgrade_check.sh` to check:

- LVM layout
- Memory Information
- CPU Information
- Kernel Parameters
- Some system properties
- ssh configurations
- Mysql schema and database sizes
- File_store locations and sizes

- Copy of `/var/log`

```
tar -czf /store/log-`date +%Y%M%S`.tar.gz --newer-mtime="36 hours ago" /var/log
```

- From the Standby Orchestrator:

```
sudo mysql --defaults-extra-file=/etc/mysql/velocloud.cnf velocloud -e 'SHOW SLAVE STATUS \G'
```



- From the Active Orchestrator:

```
sudo mysql --defaults-extra-file=/etc/mysql/velocloud.cnf velocloud -e 'SHOW MASTER STATUS \G'
```

2. Contact Support at www.arista.com/en/support/product-documentation with the above-mentioned information for assistance with the Orchestrator upgrade.

Complete Orchestrator Upgrade

After you have complete the Orchestrator upgrade, click the **Complete Orchestrator Upgrade** button under **Upgrade Actions**. This re-enables the application of the configuration updates of Edges at the global level.

 Bastion System Properties **Orchestrator Upgrade**

Orchestrator Upgrade



The Orchestrator is currently in t

- Once the Orchestrator Upgrade updates to edges continues to be p

Upgrade Announcement

Banner Message *

Visibility

Upgrade Actions

To verify that the status of the upgrade is complete, run the following command to display the correct version number for all the packages:

```
dpkg -l | grep vco
```

When you are logged in as an Operator, you can confirm if the same version displays by clicking the Help icon at the top right corner of the page.

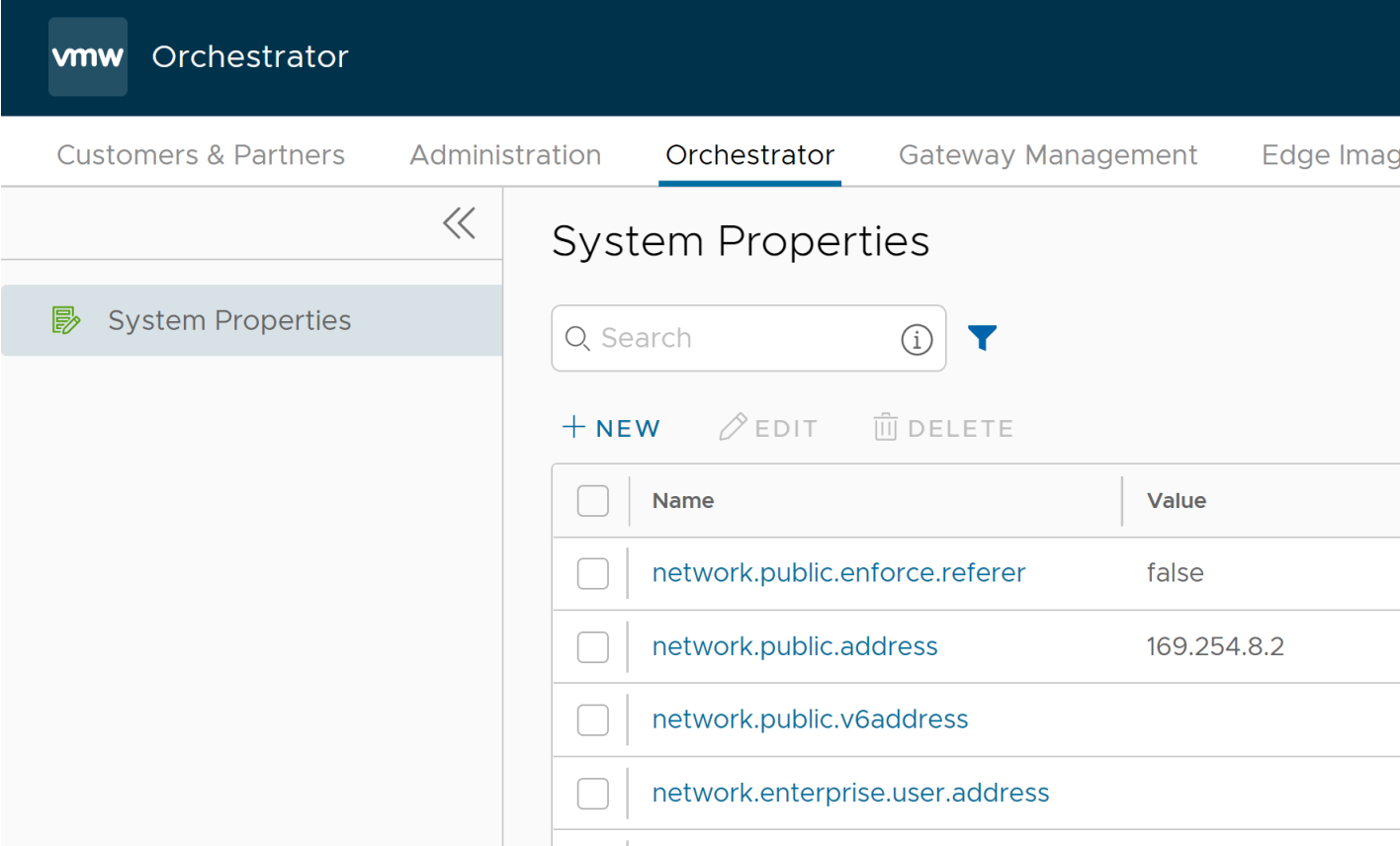
Replication

Information regarding how to set up Replication, also known as disaster recovery (DR), is available in the section *Configure Disaster Recovery* of the *Deployment and Monitoring Guide* published at www.arista.com/en/support/product-documentation.

System Properties

provides System Properties to configure various features and options available in the Orchestrator portal.

In the Operator portal, navigate to the **System Properties** page, which lists the available pre-defined system properties. See *List of System Properties*, which lists some of the system properties that you can modify as an Operator.



The screenshot shows the VMware Orchestrator interface. The top navigation bar includes 'Customers & Partners', 'Administration', 'Orchestrator' (selected), 'Gateway Management', and 'Edge Images'. The left sidebar has a 'System Properties' link. The main content area is titled 'System Properties' and contains a search bar, a filter icon, and a table of properties.

<input type="checkbox"/>	Name	Value
<input type="checkbox"/>	network.public.enforce.referer	false
<input type="checkbox"/>	network.public.address	169.254.8.2
<input type="checkbox"/>	network.public.v6address	
<input type="checkbox"/>	network.enterprise.user.address	

To configure the system properties:

1. Click **New System Property** to add a new property.

2. In the **New System Property** window, configure the following

New System Property

Name *

Data Type

Value

Value is Password ☐ Yes ☒ No

Value is Read-only ☐ Yes ☒ No

Description

CANCEL **SAVE CHANGES**

parameters:

- 3.
- | Option | Description |
|--------------------|---|
| Name | Enter the Name for the new system property. |
| Data Type | Choose the required Data Type from the drop-down menu. |
| Value | Enter the Value for the property according to the data type. |
| Value is Password | Select Yes or No as required. |
| Value is Read-only | Select Yes or No for as required. |
| Description | Enter the Description for the new system property |

4. Click **Save Changes**.

You can use the **Search** field to find a specific system property.

See the section titled, "List of System Properties" in the Deployment and Monitoring Guide, which lists some of the system properties that you can modify as an Operator.



Note: It is recommended to contact Support before making changes to the system properties.

External Certificate Authority

The External Certificate Authority (CA) feature is for large enterprises and government customers who deploy an on-premise Orchestrator and have a requirement to use their own certificate authority (CA) rather than the default self-signed Orchestrator certificate authority. This section covers how to enable and configure External CA.

When External CA is configured, instead of the Orchestrator receiving a certificate signing request (CSR) and issuing the device certificates itself, the Orchestrator is required to pass the CSR to an external CA for issuance of the certificate. The device certificate will be returned to the Orchestrator and sent to the Edge or Gateway.

A customer using this feature would be expected to have deployed a commercial certificate authority, for example from PrimeKey (EJBCA PKI), or in some cases, may have implemented their own proprietary CA.

Beginning with Release 5.1.0, an Orchestrator where external CA is activated may be configured with two new API-ready modes:

- **Manual Mode** provides support for any certificate authority and provides flexibility and control with the user manually performing each step in the certificate process.
- **Asynchronous Mode** provides support for any certificate authority with the ability to script the manual steps and automating the recurring tasks.

These modes are added to **Synchronous or Automated Mode**, which was the first mode introduced. With Synchronous mode, the Orchestrator integrates directly with an external CA (which, for Release 5.0.0 and forward, offered PrimeKey EJBCA PKI as the only available external certificate authority) and through REST APIs for certificate request, renewal, and revocation.

Enable External CA

The External CA feature is enabled through two System Properties. Enabling these system properties may only be done by an Operator with a Superuser role.

Procedure

The first system property that must be enabled is `ca.external.configuration`. This property is manually created with a JSON data type and the JSON is populated consistent with the example seen below in the Sample External CA Configuration section.

Only after `ca.external.configuration` is created and enabled, should the Operator enable the second system property: `ca.external.enable`.

1. On the Orchestrator UI select **System Properties**
2. Using the search box on the **System Properties** page enter **`ca.external.enable`** as shown in the images below.

vmw Orchestrator

Customers & Partners Orchestrator Gateway Management Edge Image Management

<<

Diagnostics

Replication

System Properties

Orchestrator Upgrade

Certificate Authorities

System Properties

ca.external.enable × ⓘ

+ NEW EDIT DELETE

<input checked="" type="checkbox"/>	Name	Value	Description
<input checked="" type="checkbox"/>	ca.external.enable	false	enable integr

3. Once the **ca.external.enable** property is located, either click on that property or check the box and click **Edit**.
4. Change the **ca.external.enable** property to **True** and select **Save Changes** to complete the change as shown in the image below.

vmw Orchestrator

Customers & Partners Orchestrator Gateway Management Edge Image Management

System Properties

ca.external.enable

Modify System Property

Name * ca.external.enable

Data Type Boolean

Value ☒ True ☐ False

Value is Password ☐ Yes ☒ No

Value is Read-only ☐ Yes ☒ No

Description enable integration with an external CA

CANCEL SAVE CHANGES

The **System Property** page displays a confirmation that the property was successfully modified, and will now show that **ca.external.enable** is **True**.

vmw Orchestrator

Customers & Partners Orchestrator

System Property has been modified successfully

System Properties

ca.external.enable x i

+ NEW EDIT DELETE

	Name	Value	Description
<input checked="" type="checkbox"/>	ca.external.enable	true	enable integr...

Configure External CA

Having enabled the External CA System Property, the Operator can now click on **Orchestrator > Certificate Authorities** to begin configuring an external certificate authority.

vmw Orchestrator

Customers & Partners Orchestrator Gateway Management Edge Image Management

Trusted Certificate Authorities

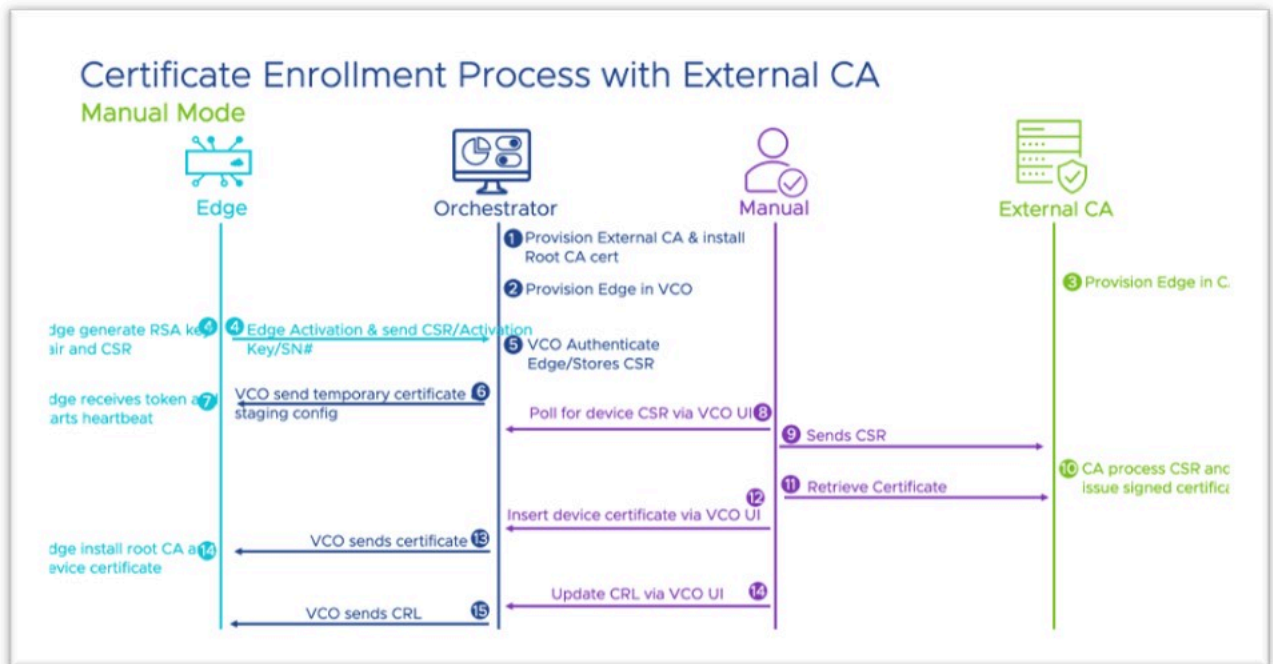
Integrated Root CA Current Issuer

Organization (O)	VeloCloud	City (L)
Organization Unit (OU)	OPS	State (ST)
Common Name (CN)	vco	Country (C)

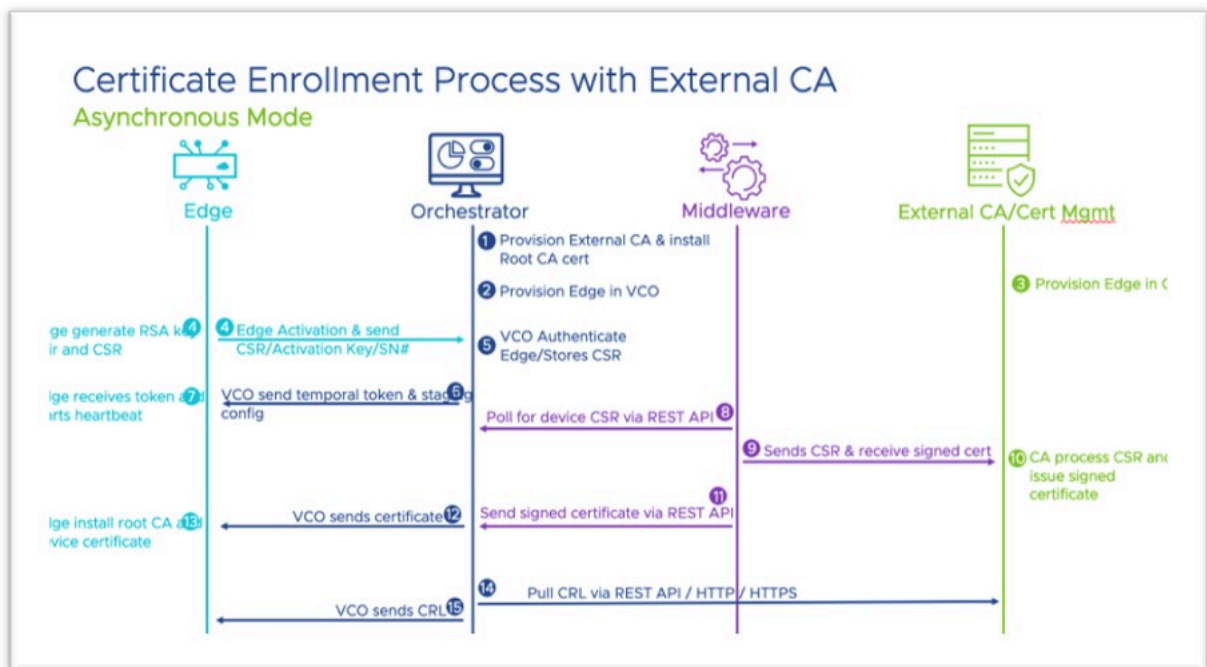
+ ADDITIONAL CA

Configuring External CA can be done using one of three modes:

1. **Automated (Synchronous):** With **Automated** mode, only one external certificate authority is supported: PrimeKey EJBCA PKI.
2. **Manual:** Manual mode provides support for any certificate authority and provides flexibility and control with the user manually performing each step in the certificate process.



3. **Asynchronous:** Asynchronous Mode provides support for any certificate authority with the ability to script the manual steps while automating the recurring tasks.



1. On the **Orchestrator** > **Certificate Authorities** page, click on + **Additional CA**.
2. After clicking + **Additional CA**, the UI will change to **CA Type** with a drop down menu with the options of **Intermediate CA** and **External CA**. Click on **External CA**.

vmw Orchestrator

Customers & Partners **Orchestrator** Gateway Management Edge Image Management

<<

Diagnostics
Replication
System Properties
Orchestrator Upgrade
Certificate Authorities

Trusted Certificate Authorities

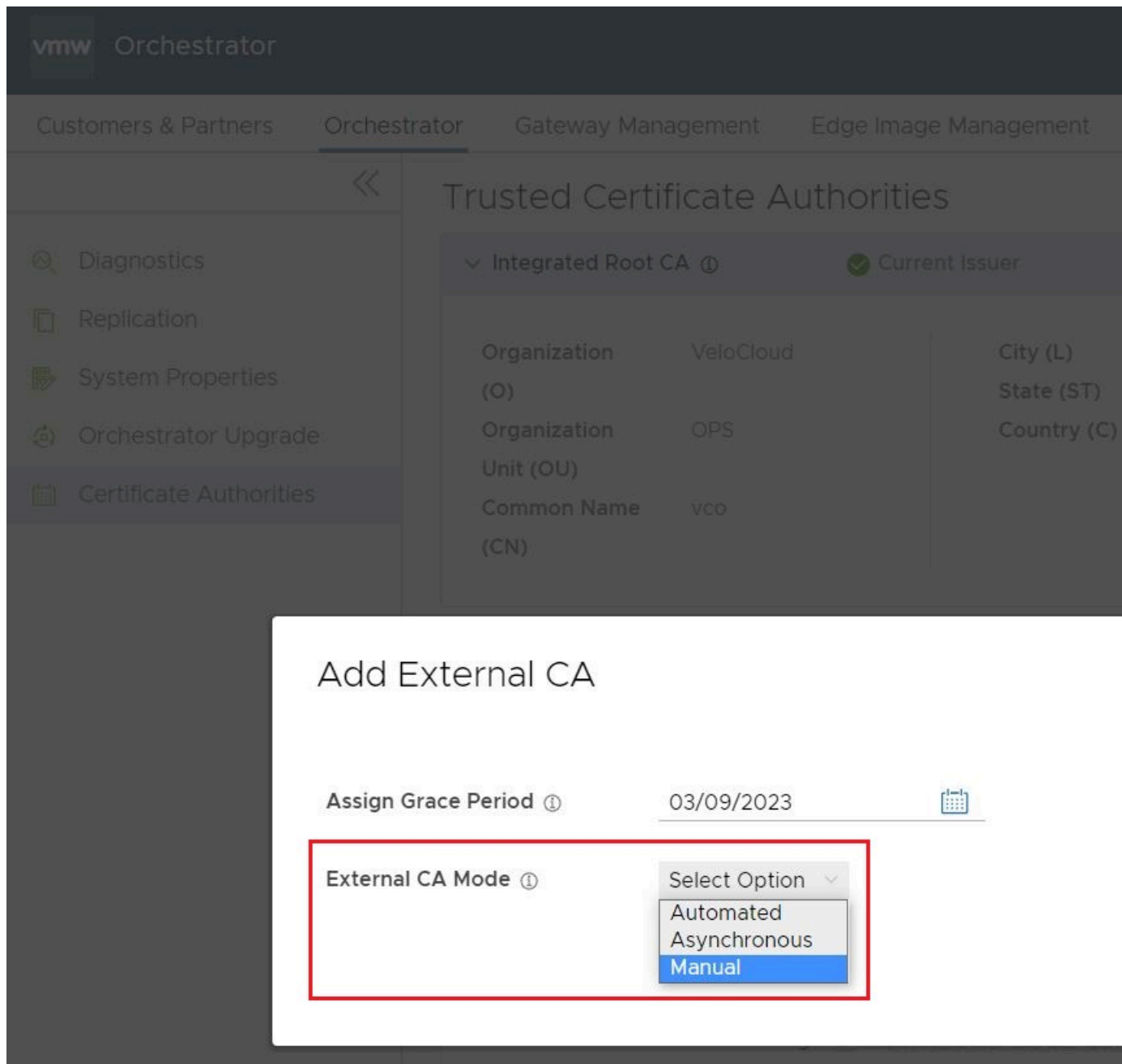
▼ Integrated Root CA ⓘ ✓ Current Issuer

Organization (O)	VeloCloud	City (L)
Organization (O)	OPS	State (ST)
Unit (OU)		Country (C)
Common Name (CN)	vco	

CA Type: Select Option ▼
Intermediate CA
External CA

↑ ADDITIONAL CA

- Once External CA is clicked, the screen changes to the Add External CA screen where an Operator can choose between the three previously mentioned External CA Modes: Automated (Synchronous), Asynchronous, and Manual.



4. Having selected a CA Mode, the **Add External CA** screen changes to allow additional configuration of the external CA. This is where the Operator would paste in the **CA Root Certificate**.

By checking the box for **Activate VCO to poll for CRL**, the Operator elects to have the Orchestrator to conduct certificate revocation checks using the Certificate Revocation List (CRL). If this option is checked, two additional configuration parameters appear to be configured by the Operator:

- a. **CRL Poll Interval in Minutes** determines how often in minutes the Orchestrator will conduct certificate revocation checking against the latest CRL.
- b. **CRL Distribution Point** is the URL where the Orchestrator retrieves the latest CRL.

The screenshot shows the VMware Orchestrator interface. The main page is titled 'Trusted Certificate Authorities' and shows a table with one entry: 'Integrated Root CA' with a status of 'Current Issuer'. The organization is 'VeloCloud'. A modal window titled 'Add External CA' is open in the foreground, containing the following fields:

- Assign Grace Period**: 03/10/2023
- External CA Mode**: Manual
- CA Root Certificate**: A text area containing a certificate snippet:


```
-----BEGIN CERTIFICATE-----
MIIDRjCCAi6gAwIBAgIJAMMisggkkfAhMA
-----
```

 Below the text area, it says: 'If this is a chain certificate, paste in order: root, sub...'
- Activate VCO to poll for CRL**: ☒
- CRL Poll Interval Minutes**: 1
- CRL Distribution Point**: <http://crl3.digicert.com/X>

5. Once the Operator has filled out all the required fields, they would click **Save**.
6. Once an external CA is configured the Operator will have newly available options to **Import CRL** and **Download CRL**.

Trusted Certificate Authorities

▼ External CA: Automated ⓘ

✓ Current Issuer

Organization (O)	VeloCloud	City	San Jo
Organization Unit (OU)	OPS	State	Californ
Common Name (CN)	vco58-usvi1	Country	United

+ ADDITIONAL CA

Trusted Certificate Authorities

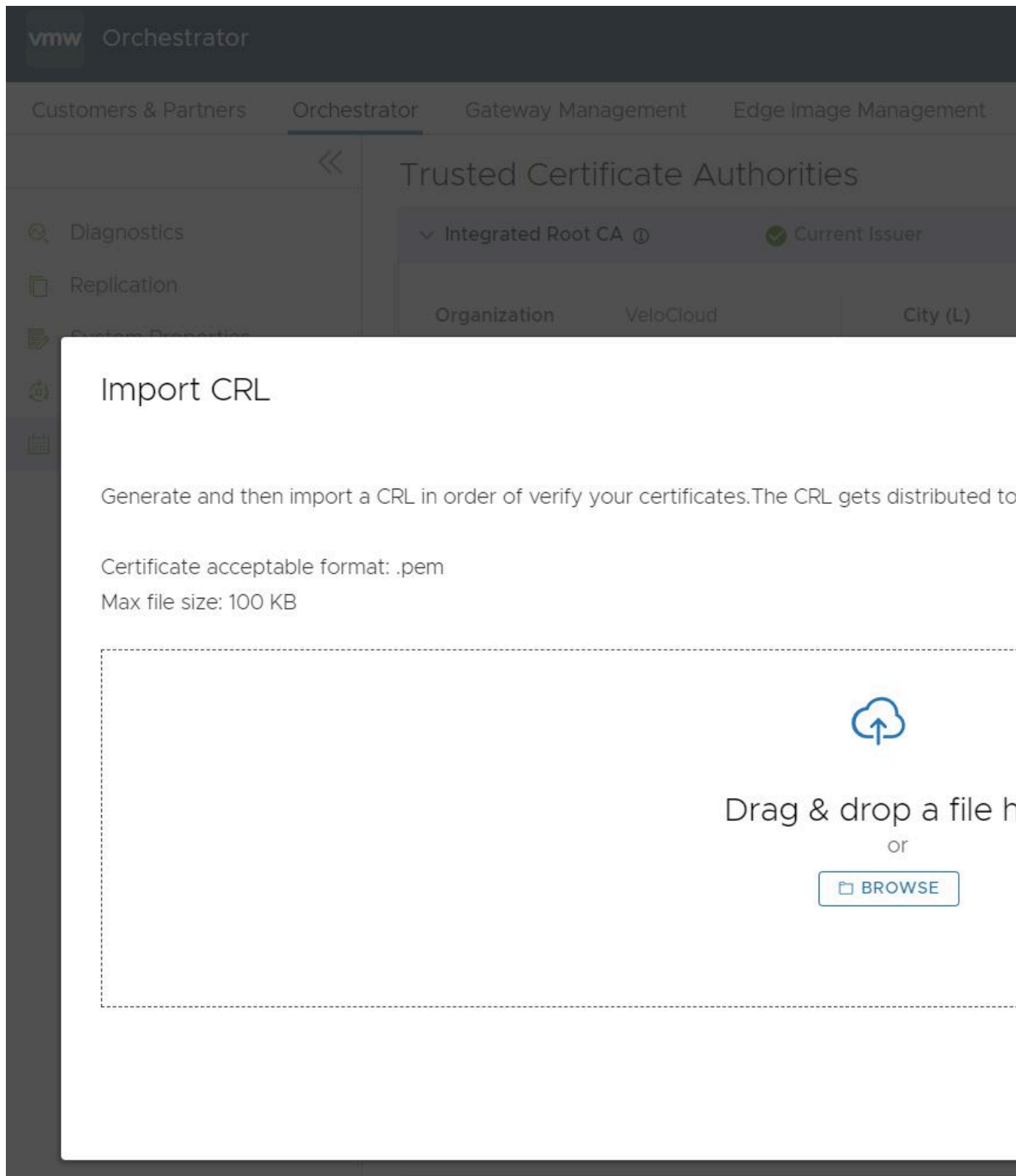
▼ External CA: Automated ⓘ

✓ Current Issuer

Organization (O)	VeloCloud	City	San Jo
Organization Unit (OU)	OPS	State	Californ
Common Name (CN)	vco58-usvi1	Country	United

+ ADDITIONAL CA

Using **Import CRL** while also having **Orchestrator CRL Polling** configured, an Operator can perform batch or individual imports and exports.



The CRL would perform a validation after any import of your certificates, and the Orchestrator distributes your CRL to every Edge and Gateway connected to your Orchestrator.



Note: There is a third System Property: `ca.external.caCertificate`. This System Property will appear once External CA is enabled and there is connectivity to a valid external CA. This property requires a PEM (privacy enhanced mail) encoded certificate.



Note: Edge/Gateway generated Certificate Sign Request (CSR) has only a Common Name (CN). While signing the CSR, the External CA adds the required subject.

Sample External CA Configuration

This section provides an example of a configuration for the `ca.external.configuration` field.

```
{
  "integrationType": "SYNCHRONOUS",
  "csrDistinguishedName": {
    "CN_PID_SN": "Arista-SDWAN"
  },
  "synchronous": {
    "synchronousIntegrationType": "EJBCA",
    "ejbca": {
      "serverCaCertificate": "-----BEGIN CERTIFICATE-----
\nMIIEFFzCCA3+gAwIBAgIUgGattlewRnm/gyPxJ7PW6uJOjCcwDQYJKoZIhvcNAQEL
\nBQAwgZixIzAhBgGjKiaJk/IsZAEBDBNyLTA1OTVhMTNjMTUzZDc2YWU1MRUwEwYD
\nVQQDDAxNYW5hZ2VtZW50Q0ExHjAcBgNVBAsMFwFtaS0wMmE0NDc0YzFmNzQ5NDBh
\nODE0MDIGA1UECgwraXAtMTAtODEtMTI1LTEzMi5lcyl3ZXN0LTlUy29tcHV0ZS5p
\nbnRlcm5hbDAeFw0yMTAyMDQxOTA0MTRaFw00NjAyMDUxOTA0MTNaMIGSMsMwIQYK
\nCZImiZPyLGQBAQwTci0wNTk1YTEzYzE1M2Q3NmF1NTEVMBMGAlUEAwMTWFWuYWdl
\nbWVudENBMR4wHAYDVQQQLDBVhbWktMDJhNDQ3NGMxZjc0OTQwYTg3NDAyBgNVBAoM
\nK21wLWTEwLTGxLTEyNS0xMzIudXMtd2VzdC0yLmNvbXBldGUuaW50ZXJuYWwwwggGi
\nMA0GCSqGSIB3DQEBAQUAA4IBjwAwggGKAoIBGQC2r0YYVKnusa7NS6aCSjbRdzMA
\nNgbF1j3+aeWn6ZokjpfFsk9Tavnu0c9gETIMfVVFj6jCyTLZcHWuPt2r1aEfVuDyk
\nW/u4kY8IaGSE5Z5+QH2I8giffTfegQBqFBSk8q4dN7o0noXFKhUgCRtTf6hd7aSji
\nynIUKEV6P/t5q+Mwql1EK6RdZzL6w9ycQOkG7mitfW4onJJCbIKy3abB/
vkiTmd8\nsQ10DyDXOzN6gwCrcUV0RfxIgd4YKN8Cj+/+bMw+It8mn5Dd/xl9FutYAO
+brZhy\nsDw5m2W66y/znh3Fr1+DUN8b0wlgHrwPSi9i/QlOefRDMvFmjiDyXq+E/peirDyl
\njVxYwn0ySgO5TympwkWw1Riibp4fJpYtwYT4EJU85emlrD6PPrzfBPsGQeG4ljqE
\nCZ2YrnOLctbv+sF5rYQzTl0lOrLMAuqJLyV4Shv+3Oj1SzxKwkqJC0sCLCx+djmq
\nYOJ9YxBke7DQKubTezHkyuk9tarEq5iHr68Ig3sCAwEAAANjMGEwDwYDVR0TAQH/
\nBAUwAwEB/zAfBgNVHSMEGDAwGBRp8EFk1aYW+s/tweOUwuXh/
xuMJzAdBgNVHQ4E\nnFgQUafBBZNWmFvrP7cHj1ML14f8bjCcwDgYDVR0PAQH/
BAQDAGGMA0GCSqGSIB3\nnDQEBcWUAA4IBGQCZA00RZIHJUJw2xhcLr2Cvr0tj+3qbY5f/
LYN5GfyMk5RjLK+u\nnbaius7FxpRpw40oZ/FH2ichDD4FO8ulqJt4znU3VtwJ0/
jmaY2xXqweI0CWIEiE\nnaKiSMzaHjsMvJ7gNQSfcb+QEm8IM/
PSPKcxNj2+QnHtDnQwgb5iMN6n88Bjeygrk\nnJG0RH0EUJ0sQr9pXo
+Gcn66b99HgEyIjojqSGCldYzkZVHQuFH7RINFU//10mnRN
\nnmb6JggNGgbdPKKHdWrfwrGpCiz1c44yznlkWVFrMdbLAlB+1uLpb8Xka7Hq5qZZn
\nLVC007Q483FBa8Lkg+RXQjIxYXgx4wkiV600UyKPlpwnSLMJvUUBmIM/Byl1h8xR
\nnyKIIzn7rc5wA4aKcfnJ9CUVfKcjtUPZffOWlvMt8bDZfaloiF20Z0KyDjyAST13Z
\nnQbsMvca6747aQQ25JD4tid5rDeRdb2bYi7nLl+1Nnhmn5ZB4qGgnaXGj3oFDoNOR\n
+KEK69DlZRNudn4=\n-----END CERTIFICATE-----",
      "apiCertificate": "-----BEGIN CERTIFICATE-----
\nMIIEKzCCApoOgAwIBAgIU83EYfZz4vi4ty1EOJr+n6wMksAwDQYJKoZIhvcNAQEL
\nBQAwgZixIzAhBgGjKiaJk/IsZAEBDBNyLTA1OTVhMTNjMTUzZDc2YWU1MRUwEwYD
\nVQQDDAxNYW5hZ2VtZW50Q0ExHjAcBgNVBAsMFwFtaS0wMmE0NDc0YzFmNzQ5NDBh
\nODE0MDIGA1UECgwraXAtMTAtODEtMTI1LTEzMi5lcyl3ZXN0LTlUy29tcHV0ZS5p
\nbnRlcm5hbDAeFw0yMTAyMDUwMDA1MTRaFw00NjAyMDUwMDA1MTNaMmBUxExZARBgNV
\nBAMMC1NlcGVyQWRtaW4wggeIMA0GCSqGSIB3DQEBAQUAA4IBDwAwggEKAoIBAQC/
\nnrPdG0oY89GGUgHbV9iG3n3Y1mPBmQ+ivBvKYD3YpM7fG+KnVQTdJLrYoH5vP7lVY
\nnQj9H6pjxq0Bh53Mse2F19UE/Gew6IZiRd2OK9yM1xRKH7hjPB3tqFLA98mar+BYA
\nnGPhapmq+sSFz6TS2ssToUllG8QgJeMxh6+vSP/Ca90+HiDB7TqECufVv61rL7sfK
\nnqfyQ5YzITKm7IGDQfdCiorwndvdli1NB+vviiYsk1fEW8gvRUu7wMR1zmPwxnUxd
\nnKmb/b7+O65md7+F1kqU6EzYMQ/224ZJonwJfzmNT01AGt4aaJDnKn1i5wV22xqqQ
\nnZvA6nrkBd+06pUwVTen1AgMBAAGjdTBZMAwGA1UdEwEB/wQCMAAwHwYDVR0jBBgw
\nnFoAUafBBZNWmFvrP7cHj1ML14f8bjCcwEwYDVR0lBAwwCgYIKwYBBQUHAWIwHQYD
```

```

\nVR0OBBYEFFj+bk/epA/jPXZywy1D4XV5sWlMMA4GA1UdDwEB/wQEAwIF4DANBgkq
\nhkiG9w0BAQsFAAOCAQEARNN08PUMCAWI+wLpu4FRuApRJRwn7U07D2ZDirV5a7pq
\nICCbREe34EYmbLyqdUCMHS8xJlPun5ER3E5YFzckC7wJ9y2h8giB7O3cjx/wWkax
\nNEkz/Is634XZveIRNf1TmV9/71LnFUBDJjHYFPNzyw6CBtVn/niL1Q9o3SvbbZLQ
\nCcdcpFmlrxku0UOuCaQgOSuLn5nqTFCNi4Sx40shg8wDrclAUuv+yX09dM2G+27h
\nndCJrkqHwbtWQMY2sOBdTIq6TMyJyrsvTCTQ67vqRtdJuSqOw/CnPNso2/lSrknWC
\nl17mQzq6+2ayQBxsm6xuHXD0INoRB+flq/QhY+CQIaTLyLezVITo0bZhe0TpNqYK
\nl1INUWjxI8mCBBiXZZ9zxbYQqZouZcNH12OCEqU8a1TfyW0EpGYClemRTgXxbODK
\n+uEwKH6sngYMkG0Usni4WIKBvZV2dJa5o8RhuCUFhwBJ2aHuiTq86RLrazJBE3wa
\nGvpl0ZmGVYmond3aBOYu\n-----END CERTIFICATE-----",
"apiKey": "-----BEGIN PRIVATE KEY-----
\nMIIEvgIBADANBgkqhkiG9w0BAQEFAASCCKgwggSkAgEAAoIBAQC/rPdG0oY89GGU
\nngHbV9iG3n3Y1mPBmQ+iVBvKYD3YpM7fG+KnVQTdJLrYoH5vP71VYQj9H6pJxq0Bh
\n53Mse2F19UE/Gew6IZiRd2OK9yM1xRKH7hjPB3tqFLA98mar
+BYAGPhapmq+sSFz\n6TS2ssToUllG8QgJeMxh6+vSP/Ca90
+HiDB7TqECufVv6lrL7sfKqfyQ5YzITKm7\nIGDQfdCiorwndvdli1NB
+vviiYsk1fEW8gvRUu7wMR1zmPwxnUxdKmb/b7+O65md
\n7+FlkqU6EzYMQ/224ZJonwJfzmNT01AGt4aaJDnKn1i5wV22xqqQZvA6nrkBd
+06\npUwVTen1AgMBAAECggEAL5DVVnp0/
JhqxMbydptbd613UMqw0bgFdkIgnrKrkIL4\nnlsRrpPPHq/4PDzr02C9dd4cNHCQwKzzjv8gHkWDW5U3tEKM2t6
\naxAfKPTa4BNee3L1nrR0hTatHxXQRJ1BX3nebn5DliGlbRDwfSVA1wZMYcMjStiS
\nzNyS71vrXrmYfYUNyjGDCZsBDRdSb41cQJ0GmwMd2B8AE5I0spMZm2Y5FM0ZcddX
\nlDcELonz1LCTNZaXyhdDBCQ8ecWrSWJZ8REhTlK/wsTtPhLiLOxIAemcLxzTJQRC
\n0tyWzA2z190hmpJs3of7geGvDCDwRu/MgvuH31MFwQKBgQDxbHm/982/txuB440+
\nMm+x/Ma5HzZg018sMdH0wQ5qJYd/lrgz2Ik79FqmFPh016LcekA0zGri+4PiRVRx
\nAlY9pLFdegIY6jJpvJxJH+kQ00xEdeUSZ100aAn4dlsHaX3wg+SBj0NiZxsOeQ9m
\nrMDKYT7LE3F5indOimDCug2GoQKBgQDLP5FPvA3uWh5Lff14yhVb0Tloiyeiqe01\nnyl07LkCI0s002/
M7U0gWXd2XNqAr98KRfTvsbf9gZxsKXTvDI+Vsdl1xGGfNZXmM\nnwodSK9zIeL4Eve7mRtcB/
ZDjtgOn0Um2YeVfXZrEacQoopYo7B4pwjPjMiq/40w3\nnOlhXOXEm1QKBgQDpKd9/8LQCwJEy9Q1sS3sDQf0uDy
+0W0NQSKuOeuCEOp\nnrmQXmzkREHip7fIFtEpd2t+PdoZm1gsK+uJhL6ebYhpJh5p
+1L6eliQThkhNmDuy
\nvgow01i30jN7xPSWBSBC9xoVkeaOZAGC2q0Lk96kRXxL7oQzkAAvjD2y4QKBgHEe
\nneQaSmIJO/8tuXLNsbYTDqNTVlgKvZoloiT+FV3+PK4y+2dnr2RQxu9GcIns2EsDj
\nnn3cQpXCHEgKrr0ZFZTwAFy6JscQcNRFFd0Ehjmi44rEK8LqTNLkz4f8KuHz/O3JZ
\nne+qe0zn71iPzkXVHLOZ65ivtzVNM8y9NtrsdCj/dAoGBAJNM0+Fbt3i1El+U/jOQ
\nKwD8vBVwsJEZ0UspoxETTAnu0sgIUbRECVhn/BQ5ja3HusRaDRsKb7ROLyjnRuC7\nnnR/
wM//oENnRm50hEi4Ocfp0eAOx7XQOUe08XhUMyXp0mOC01NwOfTL0WdG6Bk\nnSNV2aPx
+2+DGSZEVbuLXviHs\n-----END PRIVATE KEY-----",
"host": "ip-10-81-125-132.us-west-2.compute.internal",
"port": "443",
"distinguishedName":
  "UID=r-0595a13c153d76ae5,CN=ManagementCA,OU=ami-02a4474c1f74940a8,O=ip-10-81-125-132.us
west-2.compute.internal",
"certificateProfile": "ENDUSER",
"endEntityProfile": "EMPTY"
}
}
}

```

Monitoring External CA

Monitoring certificates is done on the same **Orchestrator > Certificate Authorities** page.

The **Certificates Summary** page provides an Operator with a visual status of key indicators for their certificates' life cycle. The Operator would also import certificates and download CSRs in this section.

Certificates Summary						12 CSRs Pending	DOWNLOAD CSR	IMPORT CERTIFICATES
Edge Certificates	201 Total	97 Valid	51 Expired	201 Revoked	View	6 CSRs Pending		
Gateway Certificates	43 Total	97 Valid	21 Expired	201 Revoked	View	6 CSRs Pending		

In the **Certificates** section, the Operator can download a complete list of all Edge or Gateway certificates in the .csv format.

Certificates

Edge Certificates

[↓ DOWNLOAD CSV](#)

<input type="checkbox"/>	Enterprise	Edge Name	Serial number	Issued On	Expires On
	COLUMNS				

Gateway Certificates

[↓ DOWNLOAD CSV](#)

<input type="checkbox"/>	Network	Gateway Name	Issued On	Expires On
	COLUMNS			

An Operator, Partner, or Customer administrator can also examine a particular Edge's certificate by navigating to **Configure > Edge > Overview**.

Limitations

- External CA can only be enabled on an On-Premise Orchestrator managed by a single customer. This feature is not available on Orchestrators hosted by Arista.
- On an Orchestrator using Release 5.0.0, this feature can only use PrimeKey EJBCA PKI as an external CA.

Appendix

Operator-Level Orchestrator Alerts and Events

Describes a summary of alerts and events generated within the at the Operator level.

The document provides details about all Operator-level Orchestrator events. Although these events are stored within the and displayed on the Orchestrator UI, most of them are generated by either an and/or one of its running components (MGD, PROCMON, and so on) with the exception of a few which are generated by the Orchestrator itself. You can configure notifications/alerts for events in Orchestrator only.

The following table provides an explanation for each of the columns in the "Operator-level Orchestrator Events" table:

Column name	Details
EVENT	Unique name of the event
DISPLAYED ON ORCHESTRATOR UI AS	Specifies how the event is displayed on the Orchestrator.
SEVERITY	The severity with which this event is usually generated.
GENERATED BY	The component generating the notification can be one of the following: <ul style="list-style-type: none"> • •
GENERATED WHEN	Technical reason(s) and circumstances under which this event is generated.
RELEASE ADDED IN	The release this event was first added. If not specified, this event existed prior to release 2.5.
DEPRECATED	Specifies if the event is deprecated from a specific release.

Operator-level Orchestrator Events

EVENT	DISPLAYED ON ORCHESTRATOR UI AS	SEVERITY	GENERATED BY	GENERATED WHEN	RELEASE ADDED IN	DEPRECATED
GATEWAY_UP	Gateway up	INFO		A Gateway restores after losing connectivity with the Orchestrator.		
GATEWAY_DOWN	Gateway down	INFO		A Gateway fails to communicate after losing connectivity with the Orchestrator.		

EVENT	DISPLAYED ON ORCHESTRATOR UI AS	SEVERITY	GENERATED BY	GENERATED WHEN	RELEASE ADDED IN	DEPRECATED
GATEWAY_LARGE_PACKET_SIZE	Packet size limit exceeded	INFO			The packet size limit incoming from a Gateway's peer exceeded.	
GATEWAY_SERVICE_FAILED	Gateway service failed	ERROR			The GWD service on the Gateway fails.	
GATEWAY_BFD_NEIGHBOR_UP	BFD neighbor established to Gateway neighbor	INFO			A Gateway BFD neighbor comes back up	
GATEWAY_BFD_NEIGHBOR_DOWN	Gateway BFD neighbor unavailable	DOWN			A Gateway BFD neighbor comes back down	
GATEWAY_ICMP_PROBE_UNSTABLE	ICMP probe unstable	UNSTABLE			The ICMP probe goes down on Partner Gateway.	
GATEWAY_REBALANCE	Gateway rebalanced	INFO				
PROXY_ENABLE_PLATFORM_ACCESS	Platform access delegated to operator	INFO				
PROXY_DISABLE_PLATFORM_ACCESS	Platform access revoked to operator	INFO				
VRF_ROUTE_MAP_RULES_MAX_HIT	VRF route map rules limit exceeded	WARNING			The VRF Inbound/ Outbound route map maximum limit exceeded (32).	
VRF_LIMIT_EXCEEDED	VRF entries exceeded	ALERT			The VRF entries configured exceeded maximum limit (1000).	
ENABLE_EXTERNAL_CA	External CA Enabled	CRITICAL			The 4.3.0 ca.external.enable property is set to true.	

EVENT	DISPLAYED ON ORCHESTRATOR UI AS	SEVERITY	GENERATED BY	GENERATED WHEN	RELEASE ADDED IN	DEPRECATED
DISABLE_EXTERNAL_CA	External CA Disabled	CRITICAL		The ca.external.enable property is set to false.	4.3.0	
INSERT_EXTERNAL_CA	External CA Inserted	CRITICAL		External CA is inserted into the VELOCITY_CLOUD_CERTIFICATE_AUTHORITY table and becomes a trusted issuer.	4.3.0	
CREATE_COMPOSITE_ROLE	Composite Role Role Created	INFO		A composite role is created by an Enterprise, Partner, or Operator.	4.5.0	
UPDATE_COMPOSITE_ROLE	Composite Role Role Updated	INFO		A composite role is updated by an Enterprise, Partner, or Operator.	4.5.0	
DELETE_COMPOSITE_ROLE	Composite Role Role Deleted	INFO		A composite role is deleted by an Enterprise, Partner, or Operator.	4.5.0	
CA_VALIDATION_FAIL	CA validation failure	ALERT		The CA certificate attributes are rejected.	5.0.0	
EI_ACTIVATION_CONFIG_SENT	EI activation config sent	INFO		The activation config has been successfully sent to the EI server.	5.0.0	

EVENT	DISPLAYED ON ORCHESTRATOR UI AS	SEVERITY	GENERATED BY	GENERATED WHEN	RELEASE ADDED IN	DEPRECATED
Auto_Rate_Limit_Enabled	Auto_Rate_Limit Enabled	WARNING		The auto rate-limit capability is activated on Gateways if the Gateway detects that certain Edges are sending large amount of traffic which might be causing the Gateway to be unstable and drop packets. The event message includes the information about the list of Edges (Enterprise, Rate Limit Percentage) on which the auto rate-limit is activated.	5.2.0	
Auto_Rate_Limit_Disabled	Auto_Rate_Limit Disabled	WARNING		Gateway auto rate-limit condition is restored.	5.2.0	
SELF_HEALING_REPORT	Self-Healing Report: ALERT <Remote Route inconsistency>, num_routes_recovered:<number>, shr state: <DONE>	ALERT		Generated when routes are detected as missing from a customer enterprise connected to a , and the Gateway corrects this issue by using the Self-Healing Routing feature to recover the missing routes.	5.2.0	

EVENT	DISPLAYED ON ORCHESTRATOR UI AS	SEVERITY	GENERATED BY	GENERATED WHEN	RELEASE ADDED IN	DEPRECATED
POLL_IDPS_SIGNATURE_FAIL	Signature poll job that queries and downloads signature file from GSM	ERROR		When backend poll job has failed to retrieve or download suricata signature from GSM and update profiles with the new signature metadata.	5.2.0	
IDPS_SIGNATURE_VERSION_CHECK_FAIL	Querying existing signature version from local DB failed	ERROR		When backend poll job has failed to retrieve existing suricata signature version from Orchestrator's local database.	5.2.0	
IDPS_SIGNATURE_GSM_VERSION_CHECK_FAIL	Querying signature metadata from GSM failed	ERROR		When backend poll job has failed to retrieve existing suricata signature metadata (that includes signature version) from GSM.	5.2.0	
IDPS_SIGNATURE_SKIP_DOWNLOAD_NO_UPDATE	Skipping signature download due to no change in signature version	INFO		When backend poll job skips downloading suricata signature file due to no change in suricata signature file version.	5.2.0	

EVENT	DISPLAYED ON ORCHESTRATOR UI AS	SEVERITY	GENERATED BY	GENERATED WHEN	RELEASE ADDED IN	DEPRECATED
IDPS_SIGNATURE_STORE_FAILURE	RESTORE_FAILURE not set to store signature file	ERROR	NO_PATH	When backend poll job fails to store suricata signature file due to filestore path not being set.	5.2.0	
IDPS_SIGNATURE_DOWNLOAD_SUCCESS	RE_DOWNLOAD_SUCCESS downloaded signature file from GSM	INFO		When backend poll job successfully downloads suricata signature file from GSM.	5.2.0	
IDPS_SIGNATURE_DOWNLOAD_FAILURE	RE_DOWNLOAD_FAILURE download signature file from GSM	ERROR		When backend poll job fails to download suricata signature file from GSM.	5.2.0	
IDPS_SIGNATURE_STORE_SUCCESS	RE_STORE_SUCCESS stored the signature file in filestore	INFO		When backend poll job successfully stores the suricata signature file in local file store.	5.2.0	
IDPS_SIGNATURE_STORE_FAILURE	RE_STORE_FAILURE the signature file in filestore	ERROR		When backend poll job fails to store the suricata signature file in local file store.	5.2.0	
IDPS_SIGNATURE_METADATA_INSERT_SUCCESS	RE_METADATA_INSERT_SUCCESS added metadata of the signature file to local DB	INFO		When backend poll job successfully adds metadata of the suricata signature file to local DB.	5.2.0	

EVENT	DISPLAYED ON ORCHESTRATOR UI AS	SEVERITY	GENERATED BY	GENERATED WHEN	RELEASE ADDED IN	DEPRECATED
IDPS_SIGNATURE_METADATA_INSERT_FAILURE	Return metadata of the signature file to local DB	ERROR	When backend poll job fails to add metadata of the suricata signature file to local DB.	5.2.0		
POLL_URL_CATEGORIES_FAILURE	URL_CATEGORIES_FAILURE	ERROR	Generated when URL categories poll job fails.	6.0.0		
URL_CATEGORIES_STORE_SUCCESS	URL_CATEGORIES_STORE_SUCCESS	SUCCESS	Generated when URL categories are stored successfully.	6.0.0		
URL_CATEGORIES_STORE_FAILURE	URL_CATEGORIES_STORE_FAILURE	ERROR	Generated when URL categories storage job fails.	6.0.0		
VCO_ENTERPRISE_NTICS_LICENSE_REQUEST_FAILED	VCO_ENTERPRISE_NTICS_LICENSE_REQUEST_FAILED	ERROR	Generated when Enterprise NTICS license request fails.	6.0.0		
VCO_ENTERPRISE_NTICS_LICENSE_REQUEST_SUCCEEDED	VCO_ENTERPRISE_NTICS_LICENSE_REQUEST_SUCCEEDED	INFO	Generated when Enterprise NTICS license request succeeds.	6.0.0		

Capacity Events

Currently, the assignment is based on Geo-proximity and doesn't take capacity health metrics into account. To improve the Edge-to-Gateway assignment the capacity health metrics (Edge Count, Tunnel Count, PKI Activated Tunnel Count, Flow count, NAT Count, Packet Queue Watermark, and Packet Drops) are monitored periodically based on warning and critical thresholds. When any of the metrics count is above the defined warning and critical thresholds, Gateway capacity events are generated and reported to the . These events provide the Operator and Partners a clear visibility about the Gateway health for making intelligent and correct Gateway assignments.

The following are the capacity events generated based on the capacity threshold limits.

Metric	Trigger	Event	Severity	Message	Event Detail
--------	---------	-------	----------	---------	--------------

Edge Count	<p>Above Warning Threshold. The Warning threshold value is 90% of following Supported values:</p> <ul style="list-style-type: none"> • 4 CPU, 32G MEM - 2000 • 8 CPU, 32G MEM - 4000 	GATEWAY_DEGRADE	Over capacity alert due to high number of connected Edges as Gateway has crossed warning threshold.	<ul style="list-style-type: none"> • 4 CPU: The number of connected Edges is above the warning threshold (1800). • 8 CPU: The number of connected Edges is above the warning threshold (3600).
Edge Count	<p>Above Critical Threshold. The Critical threshold value is 95% of following Supported values:</p> <ul style="list-style-type: none"> • 4 CPU, 32G MEM - 2000 • 8 CPU, 32G MEM - 4000 	GATEWAY_CRITICAL	Over capacity alert due to high number of connected Edges as Gateway has crossed critical threshold.	<ul style="list-style-type: none"> • 4 CPU: The number of connected Edges is above the critical threshold (1900). • 8 CPU: The number of connected Edges is above the critical threshold (3800).
Edge Count	Below Warning Threshold	GATEWAY_STABLE	Over capacity condition due to high number of connected Edges restored.	The number of connected Edges is within the acceptable threshold.
Tunnel Count	<p>Above Warning Threshold. The Warning threshold value is 90% of following Supported values:</p> <ul style="list-style-type: none"> • 4 CPU, 32G MEM - 3000 • 8 CPU, 32G MEM - 6000 	GATEWAY_DEGRADE	Over capacity alert due to high number of tunnels.	<ul style="list-style-type: none"> • 4 CPU: The number of tunnels is above the warning threshold (2700). • 8 CPU: The number of tunnels is above the warning threshold (5400).

Tunnel Count	Above Critical Threshold. The Critical threshold value is 95% of following Supported values: <ul style="list-style-type: none"> • 4 CPU, 32G MEM - 3000 • 8 CPU, 32G MEM - 6000 	GATEWAY_CRITICAL	NOTICE	Over capacity alert due to high number of tunnels.	<ul style="list-style-type: none"> • 4 CPU: The number of tunnels is above the critical threshold (2850). • 8 CPU: The number of tunnels is above the critical threshold (5700).
Tunnel Count	Below Warning Threshold	GATEWAY_STABLE	INFO	Over capacity condition due to high number of tunnels restored.	The number of tunnels is within the acceptable threshold.
Flow Count	Above Warning Threshold. The Warning threshold value is 50% of Supported value 1920000.	GATEWAY_DEGRADE	NOTICE	Over capacity alert due to high number of flows.	The number of flows is above the warning threshold (960000).
Flow Count	Above Critical Threshold. The Critical threshold value is 75% of Supported value 1920000.	GATEWAY_CRITICAL	NOTICE	Over capacity alert due to high number of flows.	The number of flows is above the critical threshold (1440000)
Flow Count	Below Warning Threshold	GATEWAY_STABLE	INFO	Over capacity condition due to high number of flows restored.	The number of flows is within the acceptable threshold.
NAT Entries Count	Above Warning Threshold. The Warning threshold value is 50% of Supported value 1920000.	GATEWAY_DEGRADE	NOTICE	Over capacity alert due to high number of NAT entries.	The number of NAT entries is above the warning threshold (960000).
NAT Entries Count	Above Critical Threshold. The Critical threshold value is 75% of Supported value 1920000.	GATEWAY_CRITICAL	NOTICE	Over capacity alert due to high number of NAT entries.	The number of NAT entries is above the critical threshold (1440000).
NAT Entries Count	Below Warning Threshold	GATEWAY_STABLE	INFO	Over capacity condition due to high number of NAT entries restored.	The number of NAT entries is within the acceptable threshold.

Packet Queue Watermark	Above Critical Threshold	GATEWAY_CRITICAL	NOTICE	Over capacity alert due to high packet queue watermark.	The packet queue watermark is above the critical threshold (6000) for 5 consecutive seconds.
Packet Queue Watermark	Above Warning Threshold	GATEWAY_DEGRADE	WARNING	Over capacity alert due to high packet queue watermark.	The packet queue watermark is above the warning threshold (2000) for 10 consecutive seconds.
Packet Queue Watermark	Below Warning Threshold	GATEWAY_STABLE	INFO	Over capacity condition due to high packet queue watermark restored.	The packet queue watermark is within the acceptable threshold.
Packet Drop Count	Above Critical Threshold	GATEWAY_CRITICAL	NOTICE	Over capacity alert due to high number of packet drops.	The number of packet drops is above the critical threshold (2000) for 5 consecutive seconds.
Packet Drop Count	Above Warning Threshold	GATEWAY_DEGRADE	WARNING	Over capacity alert due to high number of packet drops.	The number of packet drops is above the warning threshold (500) for 10 consecutive seconds.
Packet Drop Count	Below Warning Threshold	GATEWAY_STABLE	INFO	Over capacity condition due to high number of packet drops restored.	The number of packet drops is within the acceptable threshold.

Index

V

VCO VCG VCE 5
VeloCloud Gateways 5
VeloCloud Operator Guide 5
VeloCloud Orchestrator 5 Arista
SD-WAN by VeloCloud 5