VMware SD-WAN Operator Guide

2020

VMware SD-WAN 4.0

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About VMware SD-WAN Operator Guide

1

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

Intended Audience

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

Overview of VMware SD-WAN Orchestrator

2

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

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

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

3 Supported Browsers

The SD-WAN Orchestrator 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, VMware recommends Google Chrome or Mozilla Firefox.

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

What's New

4

What's New in Version 4.0.0

Feature	Description
BFD Settings	Allows to enable BFD subscription for BGP neighbors while configuring Partner Gateway handoff. See Configure Partner Handoff.
Edge Activation Enhancements	VMware offers new system properties to encode the activation URL parameters when the Edge Activation Email is sent to the Site Contact and to reset the trusted certificate issuer list. See Table 11-6. Edge Activation.
Edge Licensing Enhancements	VMware offers 324 types of licenses available with various combinations. In addition, a new version of license with the Edition named as **POC** is available, which can be assigned to a partner or customer as a trial. Whenever required, the **POC** license can be upgraded to any Edition. See Chapter 16 Edge Licensing.
Certificate Renewal Window for Edges and Gateways	Optional certificate renewal window for Edges and Gateways. This is an optional system propertery, which enables Operators to define one or more maintenence windows during which the Edge or Gateway certificate renewal is enabled. See Table 11-3. Certificate Authority.
Monitoring Enhancements	Allows an Operator user to monitor the Customers, Operator Events, and Gateways using the new redesigned portal. See: ■ Chapter 7 Monitor Customers ■ Monitor Operator Events ■ Monitor Gateways using new Orchestrator UI
Path Calculation with Multiple DSCP Labels per Flow	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. See Configure Path Calculation with Multiple DSCP Labels per Flow.
Rate Limiting APIs	Allows to configure Rate Limit on the API requests using the system properties. See: ■ Chapter 23 Rate Limiting API Requests ■ Table 11-10. Rate Limiting APIs
Role Customization	Allows an Operator Super user to customize the existing set of privileges for the user roles. The customization is applied globally across the Orchestrator. See Chapter 15 Role Customization.

Feature	Description
Software Updates at Enterprise Level	Allows an Operator to assign a list of software images (from a primary list of software images in Orchestrator) to every direct Enterprise and Partner, and enables the Operator to modify the currently assigned list of images for a specific Enterprise or Partner. See: ■ Chapter 8 Manage Customers ■ Create New Customer ■ Clone a Customer ■ Manage Edge Software Images ■ Chapter 10 Software Images ■ Manage Operator Profiles
SD-WAN Orchestrator Upgrade 3.4 to SD-WAN Orchestrator 4.0	Provides instructions on how to upgrade the VMware SD-WAN Orchestrator by VeloCloud from the 3.4 release to the 4.0 release. See Chapter 21 SD-WAN Orchestrator Upgrade 3.3.2 or 3.4 to SD-WAN Orchestrator 4.0 and the Chapter 5 Install SD-WAN Orchestrator section for updates.
Configurable IPsec/IKE rekey timers	Allows customers to configure IKE and IPsec Rekey Timers for the Edges at the Enterprise level, based on their level of security requirements. See Configure Security Policy.

Previous VMware Versions

To get product documentation for previous versions of VMware, contact your VMware representative.

Install SD-WAN Orchestrator

5

This section describes SD-WAN Orchestrator installation.

This chapter includes the following topics:

Prerequisites

This section describes the prerequisites that must be met before installing the SD-WAN Orchestrator.

Instance Requirements

VMware recommends installation of the Orchestrator and Gateway applications as a virtual machine (i.e. guest instance) on an existing hypervisor.

The SD-WAN Orchestrator requires the following minimal guest instance specifications:

- 8 Intel vCPU's at 2.5 Ghz or higher
- 16 GB of memory

  Note The SD-WAN Orchestrator will not start with less than 10GB of memory.

- 2x 1TB 1 x 512GB SSD based persistent volumes (expandable through LVM if needed)
  - Required Minimum IOPS: 5,000 IOPS
- 1 Gbps NIC
- Ubuntu x64 server VM compatibility
- Single public IP address (Can be made available through NAT)

Upstream Firewall Configuration

The upstream firewall needs to be configured to allow inbound HTTP (TCP/80) as well as HTTPS (TCP/443). If a stateful firewall is in place, established connections that are outbound originated should also be allowed to facilitate upgrades and security updates.

External Services

The SD-WAN Orchestrator relies on several external services. Before proceeding with an installation, ensure that licenses are available for each of the services.

Google Maps

Google Maps is used for displaying Edges and data centers on a map. No account needs to be created with Google to utilize the functionality. However, Internet access must be available to the SD-WAN Orchestrator instance in order for the service to be available.

The service is limited to 25,000 map loads each day, for more than 90 consecutive days. VMware does not anticipate exceeding these limits for nominal use of the SD-WAN Orchestrator. For more information, see Google Maps.

Twilio

Twilio is used for SMS-based alerting to enterprise customers to notify them of Edge or link outage events. An account needs to be created and funded at http://www.twilio.com.

The account can be provisioned in the SD-WAN Orchestrator through the Operator Portal's **System Properties** page. The account will be provisioned through a system property, as described later in the guide. See Twilio for more information.

MaxMind

MaxMind is a geolocation service. It is used to automatically detect Edge and Gateway locations and ISP names based on IP address. If this service is disabled, then geolocation information will need to be updated manually. The account can be provisioned in the SD-WAN Orchestrator through the Operator Portal's **System Properties** page. See MaxMind for more information.

Installation Procedures

This section describes installation.

Cloud-init Preparation

This section describes how to use the cloud-init package to handle the early initialization of instances.

About cloud-init

Cloud-init is a Linux package responsible for handling the early initialization of instances. If available in the distributions, it allows for configuration of many common parameters of the instance directly after installation. This creates a fully functional instance that is configured based on a series of inputs.

Cloud-init's behavior can be configured via user-data. User-data can be given by the user at instance launch time. This is typically done by attaching a secondary disk in ISO format that cloud-init will look for at first boot time. This disk contains all early configuration data that will be applied at that time.

The SD-WAN Orchestrator supports cloud-init and all essential configurations can be packaged in an ISO image.

Create the cloud-init meta-data File

The final installation configuration options are set with a pair of cloud-init configuration files. The first installation configuration file contains the metadata. Create this file with a text editor and label it `meta-data`. This file provides information that identifies the instance of SD-WAN Orchestrator being installed. The `instance-id` can be any identifying name, and the `local-hostname` should be a host name that follows your site standards, for example:

```
instance-id: vco01
local-hostname: vco-01
```

Additionally, you can specify network interface information (if the network is not configured via DHCP, for example):

```
instance-id: vco01
local-hostname: vco-01
network-interfaces: |
  auto eth0
  iface eth0 inet static
  address 10.0.1.2
  network 10.0.1.0
  netmask 255.255.255.0
  broadcast 10.0.1.255
  gateway 10.0.1.1
```

Create the cloud-init user-data File

The second installation configuration option file is the user data file. This file provides information about users on the system. Create it with a text editor and call it `user-data`. This file will be used to enable access to the installation of SD-WAN Orchestrator. The following is an example of what the `user-data` file will look like:

```
#cloud-config
            password: Velocloud123
            chpasswd: {expire: False}
            ssh_pwauth: True
            ssh_authorized_keys:
              - ssh-rsa AAA...SDvz user1@yourdomain.com
              - ssh-rsa AAB...QTuo user2@yourdomain.com
            vco:
              super_users:
                list: |
                  user1@yourdomain.com:password1
                remove_default_users: True
              system_properties:
                 list: |
                    mail.smtp.port:34
                    mail.smtp.host:smtp.yourdomain.com
                    service.maxmind.enable:True
                    service.maxmind.license:todo_license
                    service.maxmind.userid:todo_user
                    service.twilio.phoneNumber:222123123
                    network.public.address:222123123
            write_files:
               - path: /etc/nginx/velocloud/ssl/server.crt
                 permissions: '0644'
                 content: "-----BEGIN CERTIFICATE-----\nMI….ow==\n-----END CERTIFICATE-----\n"
               - path: /etc/nginx/velocloud/ssl/server.key
                 permissions: '0600'
                 content: "-----BEGIN RSA PRIVATE KEY-----\nMII...D/JQ==\n-----END RSA
PRIVATE KEY-----\n"
               - path: /etc/nginx/velocloud/ssl/velocloudCA.crt
```

This `user-data` file enables the default user, vcadmin, to login either with a password or with an SSH key. The use of both methods is possible, but not required. The password login is enabled by the `password` and `chpasswd` lines.

- The `password` contains the plain-text password for the vcadmin user.
- The `chpasswd` line turns off password expiration to prevent the first login from immediately prompting for a change of password. This is optional.

Note If you set a password, it is recommended that you change it when you first log in because the password has been stored in a plain text file.

The `ssh_pwauth` line enables SSH login. The `ssh_authorized_keys` line begins a block of one or more authorized keys. Each public SSH key listed on the `ssh-rsa` lines will be added to the vcadmin `~/.ssh/authorized_keys` file.

In this example, two keys are listed. For this example, the key has been truncated. In a real file, the entire public key must be listed. Note that the `ssh-rsa` lines must be preceded by two spaces, followed by a hyphen, followed by another space.

The `vco` section specifies configured SD-WAN Orchestrator services.

`super_users` contains list of VMware Super Operator accounts and corresponding passwords.

The `system_properties` section allows to customize Orchestrator System Properties. See Chapter 11 System Properties for details regarding system properties configuration.

The write_files section allows to replace files on the system. By default, SD-WAN Orchestrator web services are configured with self-signed SSL certificate. If you would like to provide different SSL certificate, the above example replaces the server.crt and server.key files in the /etc/nginx/velocloud/ssl/ folder with user-supplied files.

Note The server.key file must be unencrypted. Otherwise, the service will fail to start without the key password.

Create an ISO file

Once you have completed your files, they need to be packaged into an ISO image. This ISO image is used as a virtual configuration CD with the virtual machine. This ISO image, called vco01-cidata.iso, is created with the following command on a Linux system:

```
genisoimage -output vco01-cidata.iso -volid cidata -joliet -rock user-data meta-data
```

Transfer the newly created ISO image to the datastore on the host running VMware.

Install on VMWare

VMware vSphere provides a means of deploying and managing virtual machine resources. This section explains how to run the SD-WAN Orchestrator using the VMware vSphere Client.

Deploy OVA Template

Note This procedure assumes familiarity with VMware vSphere and is not written with reference to any specific version of VMware vSphere.

1 Log in to the vSphere Client.

2 Select **File > Deploy OVF Template**.

3 Respond to the prompts with information specific to your deployment.

Field	Description
Source	Type a URL or navigate to the OVA package location.
OVF template details	Verify that you pointed to the correct OVA template for this installation.
Name and location	Name of the virtual machine.
Storage	Select the location to store the virtual machine files.
Provisioning	Select the provisioning type. "thin" is recommended for database and binary log volumes.
Network mapping	Select the network for each virtual machine to use. **Important** Uncheck **Power On After Deployment**. Selecting it will start the virtual machine and it should be started later after the cloud-init ISO has been attached.

4 Click **Finish**.

Note Depending on your network speed, this deployment can take several minutes or more.

Attach ISO Image as a CD/DVD to Virtual Machine

1 Right-click the newly-added SD-WAN Orchestrator VM and select **Edit Settings**.

2 From the **Virtual Machine Properties** window, select **CD/DVD Drive**.

3 Select the **Use an ISO image** option.

4 Browse to find the ISO image you created earlier (we called ours `vco01-cidata.iso`), and then select it. The ISO can be found in the datastore that you uploaded it to, in the folder that you created.

5 Select **Connect on Power On**.

6 Click **OK** to exit the **Properties** screen.

Run the SD-WAN Orchestrator Virtual Machine

To start up the SD-WAN Orchestrator virtual machine:

1 Click to highlight it, then select the **Power On** button.

2 Select the **Console** tab to watch as the virtual machine boots up.

Note If you configured SD-WAN Orchestrator as described here, you should be able to log into the virtual machine with the user name vcadmin and password that you defined when you created the cloud-init ISO.

Install on KVM

This section explains how to run the SD-WAN Orchestrator using the libvirt. This deployment was tested in Ubuntu 18.04 LTS.

Images

For KVM deployment, VMware will provide the SD-WAN Orchestrator in four qcow images.

- ROOTFS
- STORE
- STORE2
- STORE3

The images are thin provisioned on deployment.

Start by copying the images to the KVM server. In addition, you must copy the cloud-init iso build as described in the previous section.

XML Sample

Note For the images in the `images/vco` folder, you will need to edit from the XML.

```
<domain type='kvm' id='49'>
  <name>vco</name>
  <uuid>b0ff25bc-72b8-6ccb-e777-fdc0f4733e05</uuid>
  <memory unit='KiB'>12388608</memory>
  <currentMemory unit='KiB'>12388608</currentMemory>
  <vcpu>2</vcpu>
  <resource>
    <partition>/machine</partition>
  </resource>
  <os>
  <type>hvm</type>
  </os>
  <features>
    <acpi/>
    <apic/>
    <pae/>
  </features>
    <cpu mode='custom' match='exact'>
    <model fallback='allow'>SandyBridge</model>
    <vendor>Intel</vendor>
    <feature policy='require' name='vme'/>
    <feature policy='require' name='dtes64'/>
    <feature policy='require' name='invpcid'/>
    <feature policy='require' name='vmx'/>
    <feature policy='require' name='erms'/>
    <feature policy='require' name='xtpr'/>
    <feature policy='require' name='smep'/>
    <feature policy='require' name='pbe'/>
    <feature policy='require' name='est'/>
    <feature policy='require' name='monitor'/>
    <feature policy='require' name='smx'/>
    <feature policy='require' name='abm'/>
    <feature policy='require' name='tm'/>
    <feature policy='require' name='acpi'/>
    <feature policy='require' name='fma'/>
    <feature policy='require' name='osxsave'/>
    <feature policy='require' name='ht'/>
    <feature policy='require' name='dca'/>
    <feature policy='require' name='pdcm'/>
    <feature policy='require' name='pdpe1gb'/>
    <feature policy='require' name='fsgsbase'/>
    <feature policy='require' name='f16c'/>
    <feature policy='require' name='ds'/>
    <feature policy='require' name='tm2'/>
    <feature policy='require' name='avx2'/>
    <feature policy='require' name='ss'/>
    <feature policy='require' name='bmi1'/>
    <feature policy='require' name='bmi2'/>
    <feature policy='require' name='pcid'/>
    <feature policy='require' name='ds_cpl'/>
```

```
     <feature policy='require' name='movbe'/>
     <feature policy='require' name='rdrand'/>
   </cpu>
 <clock offset='utc'/>
   <on_poweroff>destroy</on_poweroff>
   <on_reboot>restart</on_reboot>
   <on_crash>restart</on_crash>
   <devices>
     <emulator>/usr/bin/kvm-spice</emulator>
     <disk type='file' device='disk'>
       <driver name='qemu' type='qcow2'/>
       <source file='/images/vco/rootfs.qcow2'/>
       <target dev='hda' bus='ide'/>
       <alias name='ide0-0-0'/>
       <address type='drive' controller='0' bus='0' target='0' unit='0'/>
     </disk>
     <disk type='file' device='disk'>
       <driver name='qemu' type='qcow2'/>
       <source file='/ images/vco/store.qcow2'/>
       <target dev='hdb' bus='ide'/>
       <alias name='ide0-0-1'/>
       <address type='drive' controller='0' bus='0' target='0' unit='1'/>
     </disk>
     <disk type='file' device='disk'>
       <driver name='qemu' type='qcow2'/>
       <source file='/ images/vco/store2.qcow2'/>
       <target dev='hdc' bus='ide'/>
       <alias name='ide0-0-2'/>
       <address type='drive' controller='0' bus='1' target='0' unit='0'/>
     </disk>
     <disk type='file' device='disk'>
       <driver name='qemu' type='qcow2' />
       <source file='/images/vco/store3.qcow2' />
       <target dev='hdd' bus='ide' />
       <alias name='ide0-0-3' />
       <address type='drive' controller='0' bus='1' target='0' unit='1' />
     </disk>
     <disk type='file' device='cdrom'>
       <driver name='qemu' type='raw'/>
       <source file='/ images/vco/seed.iso'/>
       <target dev='sdb' bus='sata'/>
       <readonly/>
       <alias name='sata1-0-0'/>
       <address type='drive' controller='1' bus='0' target='0' unit='0'/>
     </disk>
     <controller type='usb' index='0'>
       <alias name='usb0'/>
       <address type='pci' domain='0x0000' bus='0x00' slot='0x01' function='0x2'/>
     </controller>
     <controller type='pci' index='0' model='pci-root'>
       <alias name='pci.0'/>
     </controller>
     <controller type='ide' index='0'>
       <alias name='ide0'/>
       <address type='pci' domain='0x0000' bus='0x00' slot='0x01' function='0x1'/>
```

```
    </controller>
    <interface type='direct'>
      <source dev='eth0' mode='vepa'/>
    </interface>
    <serial type='pty'>
      <source path='/dev/pts/3'/>
      <target port='0'/>
      <alias name='serial0'/>
    </serial>
    <console type='pty' tty='/dev/pts/3'>
      <source path='/dev/pts/3'/>
      <target type='serial' port='0'/>
      <alias name='serial0'/>
    </console>
    <memballoon model='virtio'>
      <alias name='balloon0'/>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x03' function='0x0'/>
    </memballoon>
  </devices>
  <seclabel type='none' />
<!--  <seclabel type='dynamic' model='apparmor' relabel='yes'/> -->
</domain>
```

Create the VM

To create the VM using the standard virsh commands:

```
virsh define vco.xml
virsh start vco.xml
```

Install on AWS

This section describes how to install SD-WAN Orchestrator on AWS.

Minimum Instance Requirements

See the first section of the SD-WAN Orchestrator Installation, titled Instance Requirements, and select an AWS instance type matching these requirements. Both CPU and Memory requirements must be satisfied. Example: use c4.2xlarge or larger; r4.2xlarge or larger

Request an AMI Image

Request an AMI ID from VMware. It will be shared with the customer account. Have an Amazon AWS account ID ready when requesting AMI access.

Installation

1 Launch the EC2 instance in AWS cloud.

  Example: http://docs.aws.amazon.com/efs/latest/ug/gs-step-one-create-ec2-resources.html

2 Configure the security group to allow inbound HTTP (TCP/80) as well as HTTPS (TCP/443).

3 After the instance is launched, point the web browser to the Operator login URL:

```
https://<name>/operator
```

Initial Configuration Tasks

Complete the following initial configuration tasks:

- Configure system properties
- Set up initial operator profile
- Set up operator accounts
- Create gateways
- Setup gateway pools
- Create customer account / partner account

Install an SSL Certificate

This section describes how to install an SSL certificate.

To install an SSL certificate:

1 Login into the SD-WAN Orchestrator CLI console through SSH. If you configured the SD-WAN Orchestrator as described here, you should be able to log into the virtual machine with the user name `vcadmin` and password that you defined when you created the cloud-init ISO.

2 Generate the SD-WAN Orchestrator private key.

Note Do not encrypt the key. It must remain unencrypted on the SD-WAN Orchestrator system.

```
openssl genrsa -out server.key 2048
```

3 Generate a certificate request. Customize `-subj` according to your organization information.

```
openssl req -new -key server.key -out
server.csr -subj "/C=US/ST=California/L=Mountain View/O=Velocloud Networks
Inc./OU=Development/CN=vco.velocloud.net"
```

Description of Subject fields:

Field	Description
C	country
ST	state
L	locality (city)
O	company

Field	Description
OU	department (optional)
CN	SD-WAN Orchestrator fully qualified domain name

4 Send `server.csr` to a Certificate Authority for signing. You should get back the SSL certificate (`server.crt`). Ensure that it is in the PEM format.

5 Install the certificate (which requires root access). SD-WAN Orchestrator SSL certificates are located in `/etc/nginx/velocloud/ssl/`.

```
cp server.key server.crt /etc/nginx/velocloud/ssl/
chmod 600 /etc/nginx/velocloud/ssl/server.key
```

6 Restart nginx.

```
systemctl restart nginx
```

Configure System Properties

This section describes how to configure System Properties, which provide a mechanism to control the system-wide behavior of the VMware.

System Properties can be set initially using the cloud-init config file (see *Create the cloud-init meta-data file*. The following properties need to be configured to ensure proper operation of the service.

System Name

Enter a fully qualified VMware domain name in the `network.public.address` system property.

Google Maps

Google Maps is used for displaying edges and data centers on a map. Maps may fail to display without a license key. The Orchestrator will continue to function properly, but browser maps will not be available in this case.

1 Login into https://console.developers.google.com.

2 Create a new project, if one is not already created.

3 Locate the button **Enable API**. Click under the **Google Maps APIs** and enable both **Google Maps JavaScript API** and **Google Maps Geolocation API**.

4 On the left side of the screen, click the **Credentials** link.

5 Under the Credentials page, click **Create Credentials**, then select **API key**. Create an API key.

6 Set the `service.client.googleMapsApi.key` VMware system property to API key.

7 Set `service.client.googleMapsApi.enable` to “true.”

Twilio

Twilio is a messaging service that allows you to receive VMware alerts via SMS. It is optional. The account details can be entered into the VMware through the Operator Portal's **System Properties** page. The properties are called:

- `service.twilio.enable` allows the service to be disabled in the event that no Internet access is available to the VMware
- `service.twilio.accountSid`
- `service.twilio.authToken`
- `service.twilio.phoneNumber` in `(nnn)nnn-nnnn` format

Obtain the service at https://www.twilio.com.

MaxMind

MaxMind is a geolocations service. It is used to automatically detect Edge and Gateway locations and ISP names based on an IP address. If this service is disabled, then geolocation information will need to be updated manually. The account details can be entered into the VMware through the Operator Portal's **System Properties page**. You can configure:

- `service.maxmind.enable` allows the service to be disabled in the event that no Internet access is available to the VMware
- `service.maxmind.userid` holds the user identification supplied by MaxMind during the account creation
- `service.maxmind.license` holds the license key supplied by MaxMind

Obtain the license at: https://www.maxmind.com/en/geoip2-precision-city-service.

Email

Email services can be used for both sending the Edge activation messages as well as for alarms and notifications. It is not required, but it is strongly recommended that you configure this as part of VMware operations. The following system properties are available to configure the external email service used by the Orchestrator:

- `mail.smtp.auth.pass` - SMTP user password.
- `mail.smtp.auth.user` - SMTP user for authentication.
- `mail.smtp.host` - relay server for email originated from the VMware.
- `mail.smtp.port` - SMTP port.
- `mail.smtp.secureConnection` - use SSL for SMTP traffic.

Upgrade SD-WAN Orchestrator

This section describes how to upgrade the SD-WAN Orchestrator.

To upgrade the SD-WAN Orchestrator:

1 Upload the image to the SD-WAN Orchestrator system using any file transfer tool available in your infrastructure, for example “scp.” Copy the image to the following location on the system: `/var/lib/velocloud/software_update/vco_update.tar`.

2 Connect to the SD-WAN Orchestrator console and run:

```
sudo /opt/vc/bin/vco_software_update
```

Note If you configured the SD-WAN Orchestrator as described here, you should be able to log into the virtual machine with the user name `vcadmin` and the password that you defined when you created your the cloud-init configuration files.

For instructions on how to upgrade the SD-WAN Orchestrator with DR deployment, see Chapter 18 Upgrade SD-WAN Orchestrator with DR Deployment.

Expand Disk Size (VMware)

All storage volumes are configured as LVM devices. They can be resized online by providing the underlying virtualization technology to support online disk expansion. Disks are expanded automatically via cloud-init when the VM boots.

To expand disks after boot:

1 Login into the SD-WAN Orchestrator system console.

2 Identify the physical disks that support the database volume.

```
vgs -o +devices store
```

Example:

```
root@vco:~# vgs -o +devices db_data
   \  VG      #PV #LV #SN Attr   VSize   VFree   Devices
     store    1   1   0 wz--n- 500.00g 125.00g /dev/sdb(0)
```

3 Identify the physical disk attachment.

```
lshw -class volume
```

Example:

```
/dev/sdb is attached to scsi@2:0.1.0 (Host: scsi2 Channel: 00 Id: 01 Lun: 00)
```

```
root@vco:~# lshw -class volume
  *-volume
       description: EXT4 volume
       vendor: Linux
       physical id: 1
       bus info: scsi@2:0.0.0,1
```

```
        logical name: /dev/sda1
        logical name: /
        version: 1.0
        serial: 9d212247-77c4-4f98-a5c2-7f8470fa2da8
        size: 10239MiB
        capacity: 10239MiB
        capabilities: primary bootable journaled extended_attributes large_files huge_files
dir_nlink recover extents ext4 ext2 initialized
        configuration: created=2016-02-22 20:49:38 filesystem=ext4 label=cloudimg-
rootfs lastmountpoint=/ modified=2016-02-22 21:18:58 mount.fstype=ext4
mount.options=rw,relatime,data=ordered mounted=2016-10-06 23:22:04 state=mounted
  *-disk:1
        description: SCSI Disk
        physical id: 0.1.0
        bus info: scsi@2:0.1.0
        logical name: /dev/sdb
        serial: v5V2zm-Lvbh-Mfx3-W8ki-COI9-DAtP-RXndhu
        size: 500GiB
        capacity: 500GiB
        capabilities: lvm2
        configuration: sectorsize=512
  *-disk:2
        description: SCSI Disk
        physical id: 0.2.0
        bus info: scsi@2:0.2.0
        logical name: /dev/sdc
        serial: fTQFJ2-giAV-WsXL-1Wha-V305-oQkV-qqS3SA
        size: 100GiB
        capacity: 100GiB
        capabilities: lvm2
        configuration: sectorsize=512
```

4 On the hypervisor host, locate the disk attached to the VM using bus information. Example: `SCSI(0:1)`

5 Extend the virtual disk. For instructions, see VMware KB article 1004047: http://kb.vmware.com/kb/1004047

6 Re-login into the SD-WAN Orchestrator system console.

7 Re-scan the block device for the resized physical volume. Example:

```
echo 1 > /sys/block/$DEVICE/device/rescan
```

Example:

```
echo 1 > /sys/block/sdb/device/rescan
```

8 Resize the LVM physical disk.

```
pvresize /dev/sdb
```

9 Determine the amount of free space in the database volume group.

```
vgdisplay store |grep Free
```

Example:

```
root@vco:~# vgdisplay store |grep Free
Free  PE / Size       34560 / 135.00 GiB
```

10 Extend the database logical volume.

```
lvextend -r -L+#G /dev/store/data
```

Example:

```
root@vco1:~# lvextend -r -L+1G /dev/store/data
  Size of logical volume store/data changed from 400.00 GiB (102400 extents) to 401.00 GiB
(102656 extents).
  Logical volume store/data successfully resized.
resize2fs 1.44.1 (24-Mar-2018)
Filesystem at /dev/mapper/store-data is mounted on /store; on-line resizing required
old_desc_blocks = 50, new_desc_blocks = 51
The filesystem on /dev/mapper/store-data is now 105119744 (4k) blocks long.
```

11 View the new size of the volume.

```
df -h /dev/store/data
```

Example:

```
root@vco:~# df -h /dev/store/data
Filesystem               Size  Used Avail Use% Mounted on
/dev/mapper/store-data  379G  1.2G  359G   1% /store
```

Log in to the SD-WAN Orchestrator Using SSO for Operator User

6

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

To login into SD-WAN Orchestrator using SSO as Operator user:

Note If other authentication mechanisms fail, there must always be a native operator super user as a system fallback.

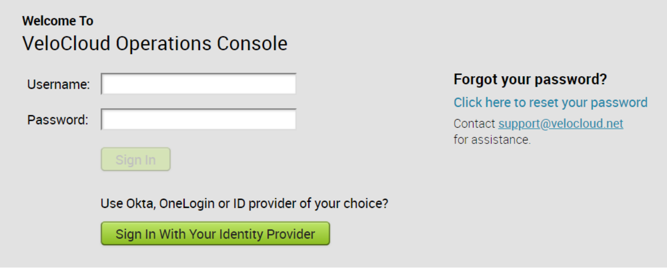
Prerequisites

- Ensure you have configured SSO authentication in SD-WAN Orchestrator. For more information, see Configure Single Sign On for Operator User.
- Ensure you have set up roles, users, and OIDC application for SSO in your preferred IDPs. For more information, see Configure an IDP for Single Sign On.

Procedure

1 In a web browser, launch a SD-WAN Orchestrator application as Operator user.

The **VMware SD-WAN Operations Console** screen appears.



Welcome To

VeloCloud Operations Console

Username:

Password:

Forgot your password?

Click here to reset your password

Contact support@velocloud.net for assistance.

Use Okta, OneLogin or ID provider of your choice?

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

The IDP configured for SSO will authenticate the user and redirect the user to the configured SD-WAN Orchestrator URL.

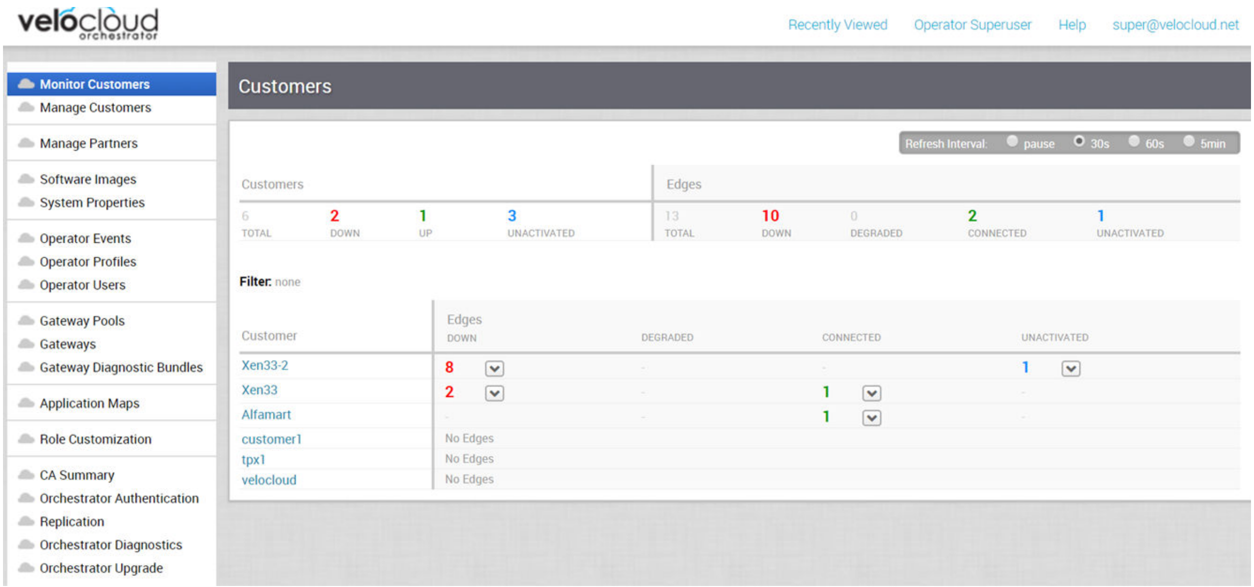
Note Once the users log in to the SD-WAN Orchestrator using SSO, they will not be allowed to login again as native users.

Monitor Customers

7

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

In the Operator portal, click **Monitor Customers**.



Customers

Refresh Interval: ○ pause ● 30s ○ 60s ○ 5min

Customers				Edges				
6 TOTAL	2 DOWN	1 UP	3 UNACTIVATED	13 TOTAL	10 DOWN	0 DEGRADED	2 CONNECTED	1 UNACTIVATED

Filter: none

Customer	Edges DOWN	DEGRADED	CONNECTED	UNACTIVATED
Xen33-2	8	-	-	1
Xen33	2	-	1	-
Alfamart	-	-	1	-
customer1	No Edges			
tpx1	No Edges			
velocloud	No Edges			

In the **Refresh Interval**, you can either pause the monitoring or choose the time interval to refresh the monitoring status.

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

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 *VMware SD-WAN Administration Guide*.

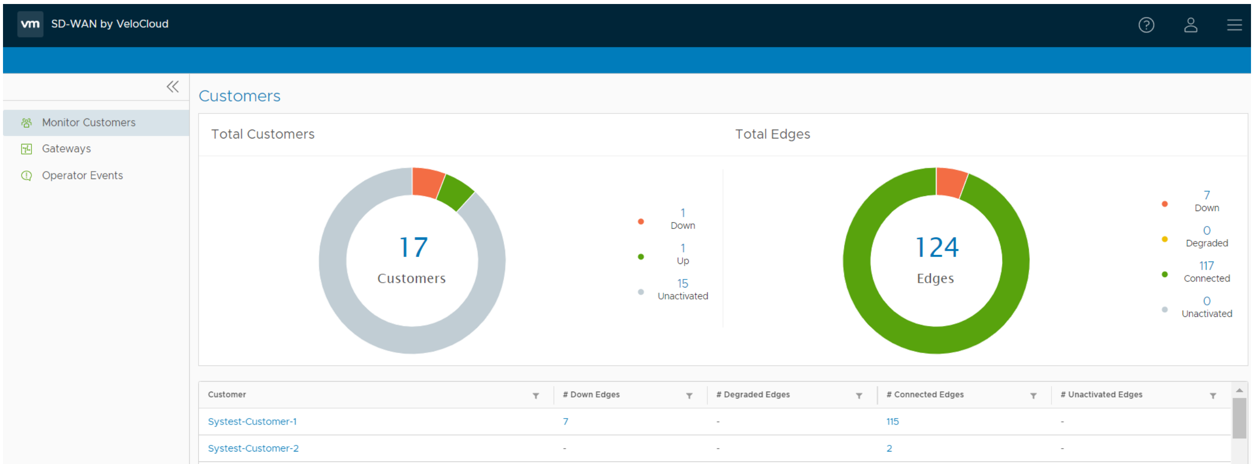
Edges:

- 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 *VMware SD-WAN Administration Guide*.

You can also view the Customers and associated Edges using the new Orchestrator UI.

- In the Operator portal, click the **Open New Orchestrator UI** option available at the top of the Window.
- Click **Launch New Orchestrator UI** in the pop-up window. The UI opens in a new tab displaying the monitoring options.



Customer	# Down Edges	# Degraded Edges	# Connected Edges	# Unactivated Edges
Systest-Customer-1	7	-	115	-
Systest-Customer-2	-	-	2	-

The new Orchestrator UI does not provide the option for Auto Refresh. You can refresh the Window manually to view the current data.

Manage Customers

8

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

In the Operator panel, click **Manage Customers**. Click **Actions** to perform the following activities:

- **New Customer** - Creates a new customer. See Create New Customer.
- **Clone Customer** - Creates a new customer, by cloning the existing configurations from the selected customer. See Clone a Customer.
- **Modify Customer** - Navigates to the **System Settings** in the Enterprise portal, where you can configure other settings corresponding to the selected customer. You can also click a customer name to navigate to the Enterprise portal. For more information see the *VMware SD-WAN Administration Guide*.
- **Delete Customer** - Deletes the selected customers. Ensure that you have removed all the Edges associated to the selected customer, before deleting the customer.
- **Transfer to Partner** - Assigns the selected customers to a partner. You can select an existing partner from the drop-down list and also choose whether to delegate the privileges to Operator and Partner.
- **Release from Partner** - Releases the selected customer from the partner.
- **Support Email: Selected Customer** - Sends customer support messages to the selected customer.
- **Assign operator profile** - Adds an Operator Profile for the selected customers.

  Note This option is available only for Enterprise Super users with Edge Image Management feature-enabled.

- **Update Edge Image Management** - Allows you to enable or disable the Edge Image Management feature for the selected customers.
- **Update Pre-Notifications** - Enables or disables the pre-notification alerts for the selected customers.
- **Update Customer Alerts** - Enables or disables the 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 comma (,) and you can choose to edit the separator to any other special character.
- **Export Customer Edge Inventory** - Exports the inventory details of all the Edges associated with all the customers to a CSV file. The default separator used is comma (,) and you can choose to edit the separator to any other special character.

This chapter includes the following topics:

Create New Customer

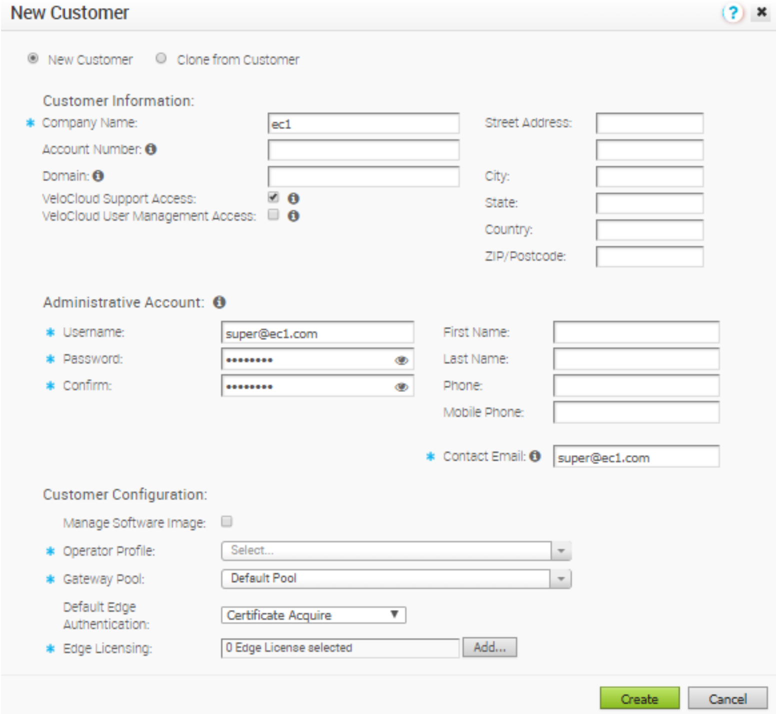
In the Operator portal, you can create customers and configure the customer settings.

Only Operator Super Users and Operator Standard Admins can create a new customer.

Note As an Operator Super User, you can temporarily disable creating new customers by setting the system property `session.options.disableCreateEnterprise` to True. You can use this option when SD-WAN Orchestrator exceeds the usage capacity.

In the Operator portal, navigate to **Manage Customers**.

1. In the **Customers** page, click **New Customer** or click **Actions > New Customer**.
2. In the **New Customer** window, enter the following details. You can also choose the **Clone from Customer** option to clone the configurations from an existing customer. For more information, see Clone a Customer.



New Customer

● New Customer ○ Clone from Customer

Customer Information:

* Company Name: ec1
Account Number:
Domain:
VeloCloud Support Access: ☑
VeloCloud User Management Access: □
Street Address:
City:
State:
Country:
ZIP/Postcode:

Administrative Account:

* Username: super@ec1.com
* Password: ••••••••
* Confirm: ••••••••
First Name:
Last Name:
Phone:
Mobile Phone:
* Contact Email: super@ec1.com

Customer Configuration:

Manage Software Image: □
* Operator Profile: Select...
* Gateway Pool: Default Pool
Default Edge Authentication: Certificate Acquire
* Edge Licensing: 0 Edge License selected

Customer Information

Option	Description
Company Name	Enter your company name
Account Number	Enter a unique identifier for the customer
Domain	Enter the domain name of your company
VeloCloud Support Access	This option is selected by default and grants access to the VMware Support to view, configure, and troubleshoot the Edges connected to the customer. For security reasons, the Support cannot access or view the user identifiable information.
VeloCloud User Management Access	Select the checkbox to enable the VMware 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.
Street Address, City, State, Country, ZIP/Postcode	Enter relevant address details in the respective fields.

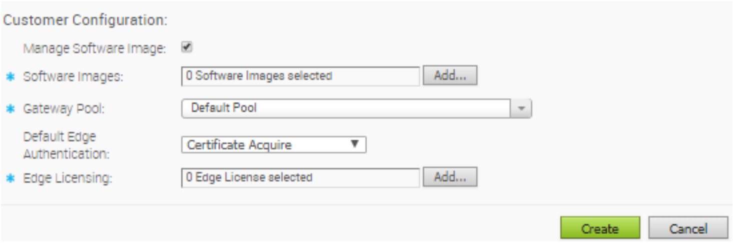
Administrative Account

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

Option	Description
Confirm	Re-enter the password.
First Name, Last Name, Phone, Mobile Phone	Enter the details like name and phone number in the appropriate fields.
Contact Email	Enter the Email address. The alerts on service status are sent to this Email address.

Customer Configuration

As an Operator User, you can manage the software images assigned to an enterprise directly by assigning an **Operator Profile** to an enterprise or allow an Enterprise Super User to manage the available list of software images for an enterprise by enabling **Manage Software Image**.



Customer Configuration:

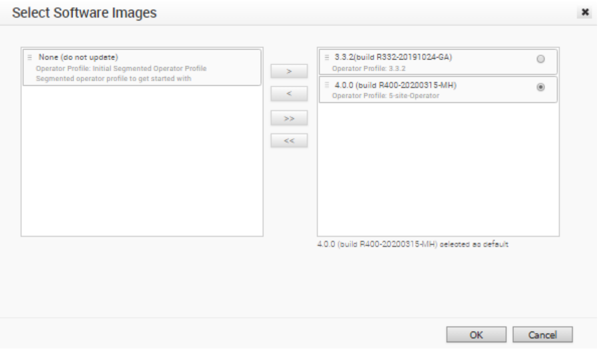
Manage Software Image: ☑

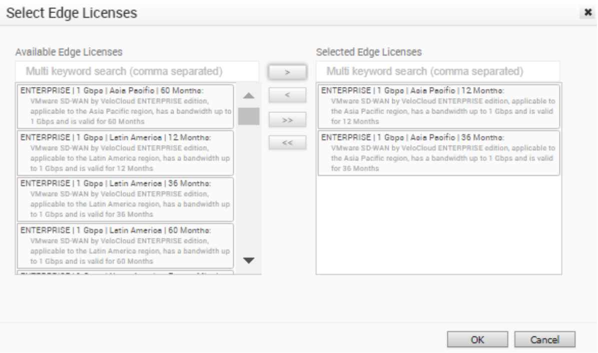
* Software Images: 0 Software Images selected

* Gateway Pool: Default Pool

Default Edge Authentication: Certificate Acquire

* Edge Licensing: 0 Edge License selected

Option	Description
Manage Software Image	Select the checkbox if you want to allow an Enterprise Super user to manage the software images available for the enterprise.
Software Images	Click **Add** and in the **Select Software Images** pop-up window, select and assign the software images from the available list for the enterprise and select an image to be used as default.  Select Software Images None (do not update) Operator Profile: Initial Segmented Operator Profile Segmented operator profile to get started with 3.3.2(build R332-20191024-GA) ○ Operator Profile: 3.3.2 4.0.0 (build R400-20200315-MH) ● Operator Profile: 5-site-Operator 4.0.0 (build R400-20200315-MH) selected as default **Note** This field appears when you enable **Manage Software Image**. After adding the images, you can modify the assigned list of software images to the enterprise by clicking **Modify** under **Customer Configuration** area. **Note** You can remove an assigned image from an enterprise only if the image is not currently used by any edge within the enterprise.
Operator Profile	Select an Operator profile to be associated with the customer from the available list. This field will not be available if **Manage Software Image** is enabled. For more information on Operator profiles, see Manage Operator Profiles.
Gateway Pool	Select an existing Gateway pool from the drop-down list. For more information on Gateway pools, see Gateway Pools.

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Default Edge Authentication</td><td>Choose the default option to authenticate the Edges associated to the customer, from the drop-down list.</td></tr>
<tr><td>Edge Licensing</td><td>Click <b>Add</b> and in the <b>Select Edge Licenses</b> pop-up window, select and assign the edge licenses from the available list for the enterprise.


Select Edge Licenses
Available Edge Licenses
Multi keyword search (comma separated)
ENTERPRISE | 1 Gbps | Asia Pacific | 60 Months: VMware SD-WAN by VeloCloud ENTERPRISE edition, applicable to the Asia Pacific region, has a bandwidth up to 1 Gbps and is valid for 60 Months
ENTERPRISE | 1 Gbps | Latin America | 12 Months: VMware SD-WAN by VeloCloud ENTERPRISE edition, applicable to the Latin America region, has a bandwidth up to 1 Gbps and is valid for 12 Months
ENTERPRISE | 1 Gbps | Latin America | 36 Months: VMware SD-WAN by VeloCloud ENTERPRISE edition, applicable to the Latin America region, has a bandwidth up to 1 Gbps and is valid for 36 Months
ENTERPRISE | 1 Gbps | Latin America | 60 Months: VMware SD-WAN by VeloCloud ENTERPRISE edition, applicable to the Latin America region, has a bandwidth up to 1 Gbps and is valid for 60 Months
Selected Edge Licenses
Multi keyword search (comma separated)
ENTERPRISE | 1 Gbps | Asia Pacific | 12 Months: VMware SD-WAN by VeloCloud ENTERPRISE edition, applicable to the Asia Pacific region, has a bandwidth up to 1 Gbps and is valid for 12 Months
ENTERPRISE | 1 Gbps | Asia Pacific | 36 Months: VMware SD-WAN by VeloCloud ENTERPRISE edition, applicable to the Asia Pacific region, has a bandwidth up to 1 Gbps and is valid for 36 Months

After adding the licenses, you can click <b>Modify</b> under <b>Customer Configuration</b> area to add or remove the licenses.
<b>Note</b> 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 Chapter 16 Edge Licensing.</td></tr>
</table>

Click **Create**.

The new customer name is displayed in 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 and the *Enterprise Administration* section of *VMware SD-WAN Administration Guide*.

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

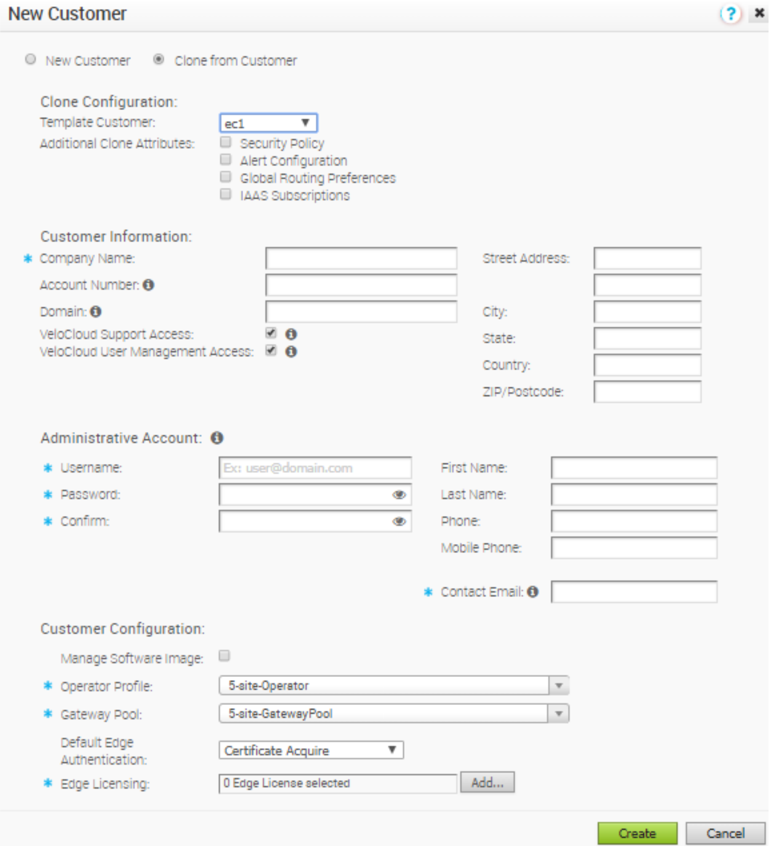
You cannot clone an enterprise if it consists of the following:

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

In the Operator portal, navigate to **Manage Customers**.

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

2 In the **New Customer** window, enter the following details. You can also choose the **New Customer** option to create a new customer without cloning the configurations from the selected customer. See Create New Customer.



New Customer

○ New Customer ● Clone from Customer

Clone Configuration:

Template Customer: ec1

Additional Clone Attributes: □ Security Policy □ Alert Configuration □ Global Routing Preferences □ IAAS Subscriptions

Customer Information:

* Company Name:

Account Number:

Domain:

VeloCloud Support Access: ☑

VeloCloud User Management Access: ☑

Street Address:

City:

State:

Country:

ZIP/Postcode:

Administrative Account:

* Username: Ex: user@domain.com

* Password:

* Confirm:

First Name:

Last Name:

Phone:

Mobile Phone:

* Contact Email:

Customer Configuration:

Manage Software Image: □

* Operator Profile: 5-site-Operator

* Gateway Pool: 5-site-GatewayPool

Default Edge Authentication: Certificate Acquire

* Edge Licensing: 0 Edge License selected

Clone Configuration

Option	Description
Template Customer	By default, the selected customer is considered for the cloning purpose. If required, you can choose a different customer from the drop-down list. If a customer or enterprise does not meet the appropriate cloning conditions, as listed at the beginning of this section, then it is not available in the drop-down list. This list displays only the name of customers that can be cloned.
Additional Clone Attributes	In addition to the default cloned configurations, you can select the following settings to be cloned, as required: ■ Security Policy ■ Alert Configuration ■ Global Routing Preferences ■ IAAS Subscriptions

Enter the **Customer Information** and **Administrative Account** details, as described in Create New Customer.

In the **Customer Configuration** section, the Operator Profile, Software Images, Gateway Pool, and Default Edge Authentication are cloned from the selected customer. If needed, you can modify the cloned customer configuration settings.

You can manage the software image assigned to an enterprise directly by assigning an **Operator Profile** to an enterprise or allow an Enterprise Super user to manage the software images available for the enterprise by enabling **Manage Software Image**.

For more information about **Manage Software Image**, see Create New Customer.

For the Edge Licensing, click **Add** to include the Edge licenses from the available list.

Click **Create**.

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, see Configure Customers and the *VMware SD-WAN Administration Guide*.

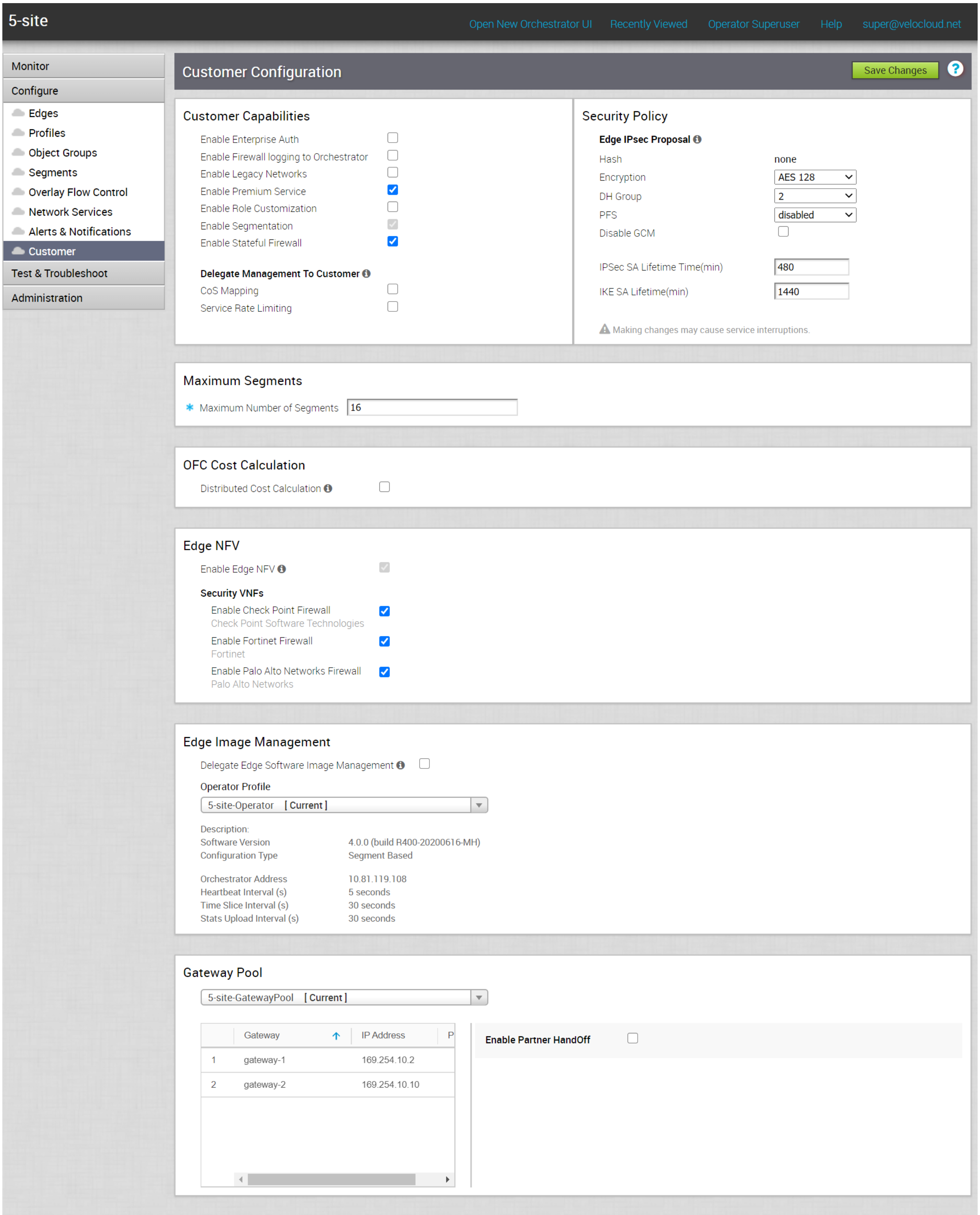
Configure Customers

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 or enterprise can modify.

When you create a new customer, you are redirected to the **Customer Configuration** page, where you can configure the customer settings.

You can also navigate to the Configuration page from the **Manage Customers** page in the Operator portal. Select the customer and click **Actions > Modify** or click the link to the customer.

In the customer or Enterprise portal, click **Configure** > **Customer**, and you can configure the following settings.



Customer Configuration

Customer Capabilities

- Enable Enterprise Auth □
- Enable Firewall logging to Orchestrator □
- Enable Legacy Networks □
- Enable Premium Service ☑
- Enable Role Customization □
- Enable Segmentation ☑
- Enable Stateful Firewall ☑

Delegate Management To Customer

- CoS Mapping □
- Service Rate Limiting □

Security Policy

Edge IPsec Proposal

- Hash: none
- Encryption: AES 128
- DH Group: 2
- PFS: disabled
- Disable GCM □
- IPSec SA Lifetime Time(min): 480
- IKE SA Lifetime(min): 1440

Making changes may cause service interruptions.

Maximum Segments

- * Maximum Number of Segments: 16

OFC Cost Calculation

- Distributed Cost Calculation □

Edge NFV

- Enable Edge NFV ☑

Security VNFs

- Enable Check Point Firewall ☑ Check Point Software Technologies
- Enable Fortinet Firewall ☑ Fortinet
- Enable Palo Alto Networks Firewall ☑ Palo Alto Networks

Edge Image Management

- Delegate Edge Software Image Management □

Operator Profile: 5-site-Operator [Current]

Description:	
Software Version	4.0.0 (build R400-20200616-MH)
Configuration Type	Segment Based
Orchestrator Address	10.81.119.108
Heartbeat Interval (s)	5 seconds
Time Slice Interval (s)	30 seconds
Stats Upload Interval (s)	30 seconds

Gateway Pool

5-site-GatewayPool [Current]

	Gateway	IP Address	P
1	gateway-1	169.254.10.2	
2	gateway-2	169.254.10.10	

Enable Partner HandOff □

You can configure the following settings:

- **Customer Capabilities** – Enable or disable the settings that the selected customer can access, configure, and modify. See Configure Customer Capabilities.
- **Security Policy** – Choose to update the existing security policies while creating Edge to Edge IPSec Tunnels. See Configure Security Policy.
- **Maximum Segments** – Enter the maximum number of segments that can be configured. The range is 1 to 16 and the default value is 16.
- **OFC Cost Calculation** – Choose to distribute the calculation of cost of routes to the Edges and Gateways, to reduce the resource consumption and load of the Orchestrator. See Configure Distributed Cost Calculation.
- **Multiple-DSCP tags per Flow Path Calculation** – Choose to enable path calculation for a single flow with multiple DSCP labels. See Configure Path Calculation with Multiple DSCP Labels per Flow.
- **Edge NFV** – Enable NFV on Edges to deploy security VNFs. See Configure NFV and VNF for Edges.
- **Edge Image Management** – Manage the Edge software images assigned to an enterprise. See Manage Edge Software Images.
- **Gateway Pool** – Choose a Gateway pool to be assigned to the enterprise. See Associate Gateway Pool.
- **Other Settings** – This option is available only when you have enabled the **User Agreement** option. You can choose to override the default display settings of the User Agreement, by selecting relevant option from the **User Agreement Display** drop-down list. By default, the Customer inherits the display mode set in the System Properties. For more information, see Chapter 20 Manage User Agreements.

After making changes to the configurations, click **Save Changes**.

Configure Customer Capabilities

You can enable or disable the capabilities for a selected customer:

In the Operator portal, navigate to **Manage Customers**.

Select a customer and click **Actions > Modify** or click the link to the customer.

In the Enterprise portal, click **Configure > Customers**.

In the **Customer Configuration** page, select to enable or disable the **Customer Capabilities**:

Note To enable Customer Capabilities, any System Properties associated with them must be assigned a `True` value. For more information, see Chapter 11 System Properties.

- **Enable Enterprise Auth** – By default, only the Operator can enable or disable two-factor authentication for an enterprise. When you enable this capability, the Enterprise Admins can configure the two-factor authentication on their own.
- **Enable Firewall logging to Orchestrator** – Allows an enterprise user to enable or disable logging the Firewall information to the Orchestrator, at the Profile level and Edge level. When Firewall logging is enabled, you can monitor the Firewall logs in the Enterprise portal.
- **Enable Legacy Networks** – Allows an enterprise to use legacy networks. You cannot enable this option if you are using a segment-based Operator profile.
- **Enable Premium Service** – Allows to utilize the premium services.
- **Enable Role Customization** – Allows to enable or disable an Enterprise super user to customize the role privileges for other Enterprise users.
- **Enable Segmentation** – Allows to configure segments.
- **Enable Stateful Firewall** – Allows an enterprise user to enable or disable the Stateful Firewall feature at the profile and edge level.
- **Delegate Management To Customer** – The following options are always visible to customers. When you enable these options, customers can modify the settings.
  - CoS Mapping
  - Service Rate Limiting

Note The **Enable Premium Service**, **Enable Segmentation** and **Enable Stateful Firewall** are enabled by default.

After choosing the capabilities, click **Save Changes**.

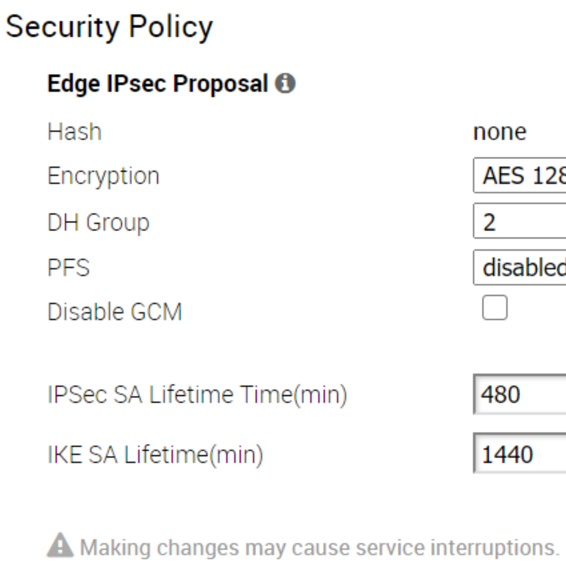
Configure Security Policy

When creating Edge-to-Edge IPSec tunnels, you can modify the security policy configuration settings at the Customer Configuration level.

Procedure

1. In the Operator portal, navigate to **Manage Customers**.
2. Select a customer and click **Actions > Modify** or click the link to the customer.

3 In the Enterprise portal, click **Configure > Customers**. The **Customer Configuration** page appears.



Security Policy

Edge IPsec Proposal

Hash	none
Encryption	AES 128
DH Group	2
PFS	disabled
Disable GCM	□
IPSec SA Lifetime Time(min)	480
IKE SA Lifetime(min)	1440

⚠ Making changes may cause service interruptions.

4 In the **Security Policy** area, you can configure the following security settings:

a **Hash** - By default, there is no authentication algorithm configured for the VPN header. When the Galois/Counter Mode (GCM) is disabled, you can select one of the following as the authentication algorithm for the VPN header, from the drop-down list that appears:

- SHA 1
- SHA 256
- SHA 384
- SHA 512

b **Encryption** - AES 128-Galois/Counter Mode (GCM), AES 256-GCM, AES 128-Cipher Block Chaining (CBC) and AES 256-CBC are the encryption algorithms modes used to provide confidentiality. Select either **AES 128** or **AES 256** as the AES algorithms key size to encrypt data. The default encryption algorithm mode is AES 128-GCM, when the **Disable GCM** checkbox is not selected.

c **DH Group** - Select the Diffie-Hellman (DH) Group algorithm to be used when exchanging a pre-shared key. The DH Group sets the strength of the algorithm in bits. The supported DH Groups are 2, 5, 14, 15, and 16. It is recommended to use DH Group 14.

d **PFS** - Select the Perfect Forward Secrecy (PFS) level for additional security. The supported PFS levels are 2, 5, 14, 15, and 16. By default, PFS is disabled.

e **Disable GCM** - By default, AES 128-GCM is enabled. If needed, select the checkbox to disable this mode. Disabling the checkbox will enable AES 128-CBC mode.

f **IPsec SA Lifetime** - Time when Internet Security Protocol (IPSec) rekeying is initiated for Edges. The minimum IPsec life time is 3 minutes and maximum is 480 minutes. The default value is 480 minutes.

g **IKE SA Lifetime** - Time when Internet Key Exchange (IKE) rekeying is initiated for Edges. The minimum IKE life time is 10 minutes and maximum is 1440 minutes. The default value is 1440 minutes.

Note It is not recommended to configure low life time values for IPsec (less than 10 minutes) and IKE (less than 30 minutes) as it can cause traffic interruption in some deployments due to rekeys. The low life time values are for debugging purposes only.

5 After configuring the settings, click **Save Changes**.

Note When you modify the security 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.

Configure Distributed Cost Calculation

By default, the Orchestrator is actively involved in learning the dynamic routes. VMware 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.

Note Enabling **Distributed Cost Calculation** is recommended for all customers.

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:

Prerequisites

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

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

Procedure

1. In the Operator portal, navigate to **Manage Customers**.
2. Select a customer and click **Actions > Modify** or click the link to the customer.
3. In the Enterprise portal, click **Configure > Customers**.

4 In the **Customer Configuration** page, navigate to the **OFC Cost Calculation** section and select the **Distributed Cost Calculation** checkbox to delegate the cost calculation of routes to Edges and Gateways.

   Note Once you enable **Distributed Cost Calculation**, you cannot downgrade the Edges and Gateways to version earlier than 3.4.0, unless you also disable **Distributed Cost Calculation**. This feature does not work on a network if any Edge or Gateway in that network is using a software version earlier than 3.4.0.

5 Click **Save Changes**.

   Note After enabling **Distributed Cost Calculation**, it is recommended to refresh the routes in the Overlay Flow Control page.

Results

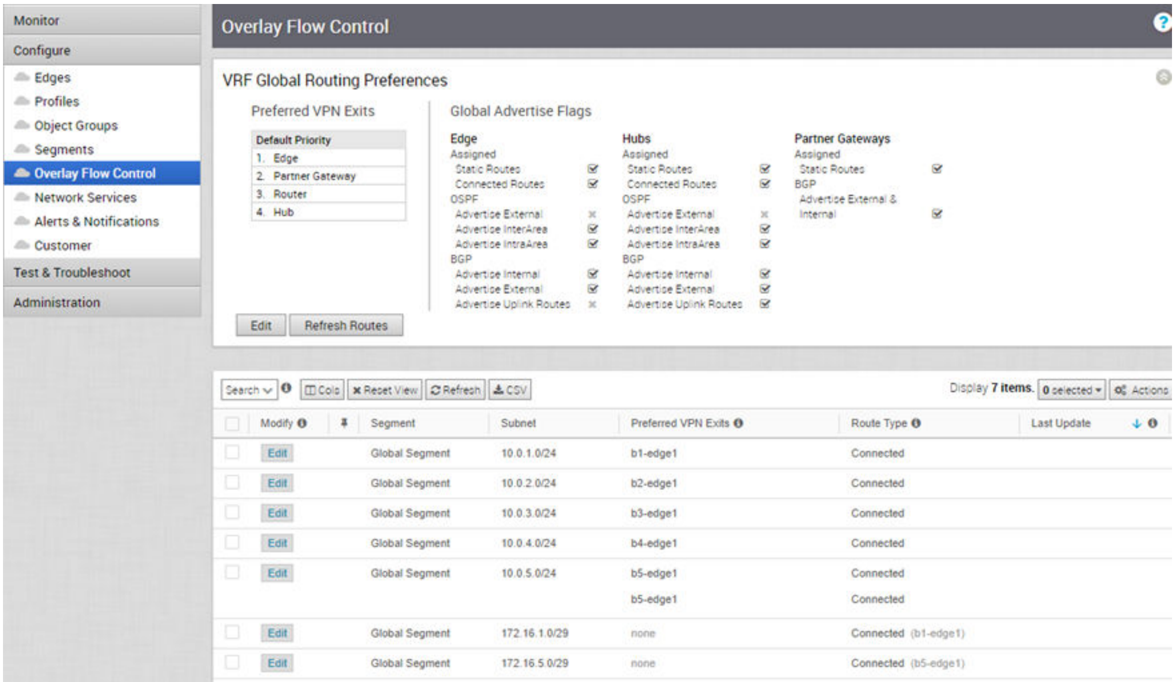
Once **Distributed Cost Calculation** is enabled, all the dynamic routes are assigned with new preferences and advertise action based on the Distributed Cost Calculation and the new information is propagated across the Enterprise Network.

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 Enterprise portal. You can view the routes and advertise action in the **Overlay Flow Control** page.

Once you enable **Distributed Cost Calculation**, the **Refresh Routes** option is available in the **Overlay Flow Control** page.



VRF Global Routing Preferences

Preferred VPN Exits

Default Priority
1. Edge
2. Partner Gateway
3. Router
4. Hub

Global Advertise Flags

Edge		Hubs		Partner Gateways	
Assigned		Assigned		Assigned	
Static Routes	☑	Static Routes	☑	Static Routes	☑
Connected Routes	☑	Connected Routes	☑	BGP	
OSPF		OSPF		Advertise External & Internal	☑
Advertise External	☒	Advertise External	☒		
Advertise InterArea	☑	Advertise InterArea	☑		
Advertise IntraArea	☑	Advertise IntraArea	☑		
BGP		BGP			
Advertise Internal	☑	Advertise Internal	☑		
Advertise External	☑	Advertise External	☑		
Advertise Uplink Routes	☒	Advertise Uplink Routes	☑		

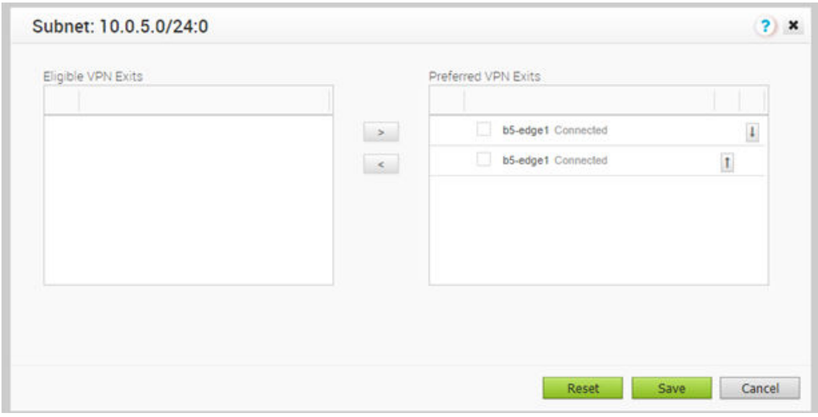
Display **7 items.**

□	Modify		Segment	Subnet	Preferred VPN Exits	Route Type	Last Update
□	Edit		Global Segment	10.0.1.0/24	b1-edge1	Connected	
□	Edit		Global Segment	10.0.2.0/24	b2-edge1	Connected	
□	Edit		Global Segment	10.0.3.0/24	b3-edge1	Connected	
□	Edit		Global Segment	10.0.4.0/24	b4-edge1	Connected	
□	Edit		Global Segment	10.0.5.0/24	b5-edge1 b5-edge1	Connected Connected	
□	Edit		Global Segment	172.16.1.0/29	none	Connected (b1-edge1)	
□	Edit		Global Segment	172.16.5.0/29	none	Connected (b5-edge1)	

When you click **Refresh Routes**, this option forces the Edges and Gateways to recalculate learned route costs and send them to the Orchestrator. In addition, the changes in the Overlay Flow Control are applied immediately on the new and existing learned routes.

Note It is recommended to use **Refresh Routes** in a maintenance window, as the option has a network impact similar to the effect caused by enabling Distributed Cost Calculation.

You can reset the cost calculation for the subnets when there are pinned routes available. Click the **Edit** option for a subnet.



Subnet: 10.0.5.0/24:0

Eligible VPN Exits

Preferred VPN Exits

- □ b5-edge1 Connected
- □ b5-edge1 Connected

Click **Reset**, which enables the Orchestrator to clear the pinned routes, recalculate the cost for the selected subnet based on the policy, and send the results to the Edges and Gateways.

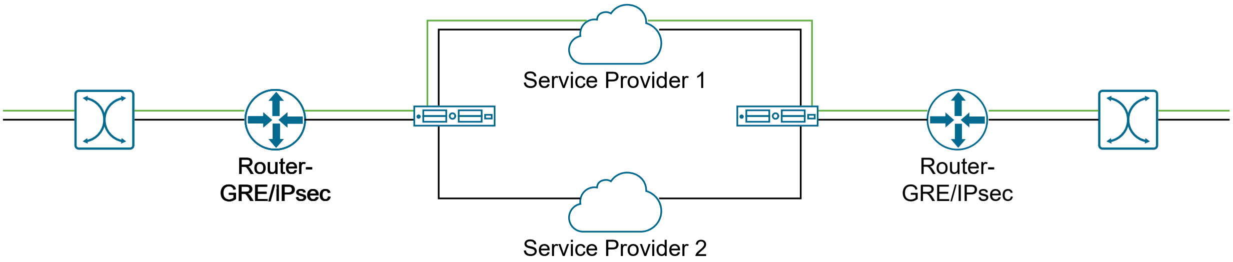
Note The **Reset** option is available only when Distributed Cost Calculation is enabled.

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 are 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 **System Properties**.

2 Click **New System Property**.

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**.
5. In the Operator portal, navigate to **Manage Customers**.
6. Select a customer and click **Actions > Modify** or click the link to the customer.
7. In the Enterprise portal, click **Configure > Customers**.
8. In the **Customer Configuration** page, navigate to the **Multiple-DSCP tags per Flow Path Calculation** section, and select the **Include DSCP value as part of flow lookup** checkbox.

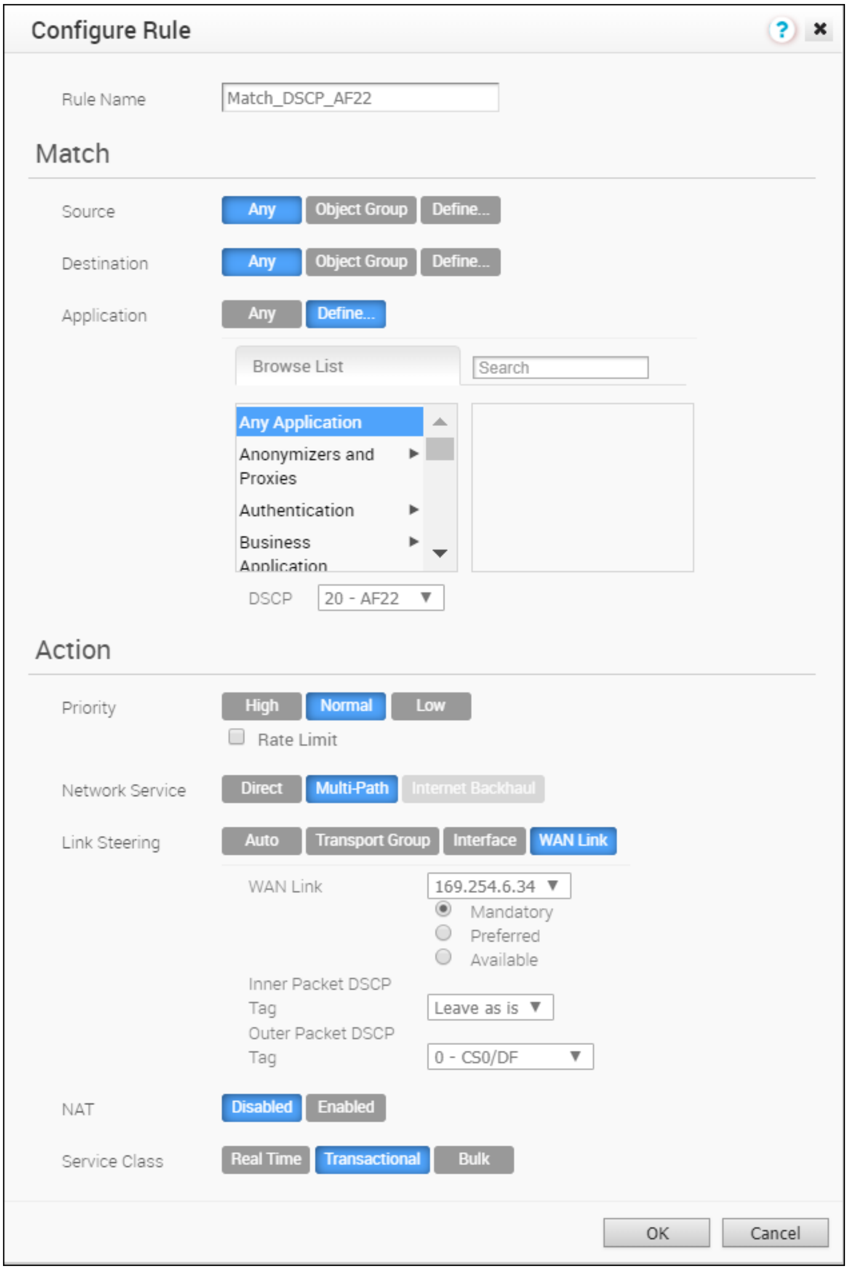
   Note This option is available only when the system property **session.options.enableFlowParametersConfig** is set to True.

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

Note When you enable **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.

- In the Enterprise portal, click **Configure > Edges**.
- Select an Edge, and click the **Business Policy** tab.
- Click **New Rule** or **Actions > New Rule**.
- In the **Configure Rule** window, click **Define** for **Application** and select an application from the list. Choose a DSCP label from the drop-down list.



Configure Rule

Rule Name: Match_DSCP_AF22

Match

Source: Any

Destination: Any

Application: Define...

DSCP: 20 - AF22

Action

Priority: Normal

□ Rate Limit

Network Service: Multi-Path

Link Steering: WAN Link

WAN Link: 169.254.6.34

● Mandatory
○ Preferred
○ Available

Inner Packet DSCP Tag: Leave as is

Outer Packet DSCP Tag: 0 - CS0/DF

NAT: Disabled

Service Class: Transactional

- Choose the relevant actions as required in the **Action** area.
- Click **OK**.

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 *VMware SD-WAN Administration Guide.*

Limitations:

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

  You can use this option for On-Premise deployment where Gateway is used only for control plane functionality and not for data plane traffic.
- The path calculation with multiple DSCP labels per Flow is intended only for GRE or IPSec traffic. The direct Internet traffic does not carry multiple DSCP labels within a single flow.
- After you enable the path calculation option, when the traffic flow consists of packets with same five-tuple information but different DSCP markings, LAN side NAT might not work as expected.

Configure NFV and VNF for Edges

You can enable Network Function Virtualization (NFV) on Edges and deploy Virtual Network Functions (VNF) on the Edges using third party firewalls.

In the Operator portal, navigate to **Manage Customers**.

Select a customer and click **Actions > Modify** or click the link to the customer.

In the Enterprise portal, click **Configure > Customers**.

In the **Customer Configuration** page, the **Edge NFV** section allows to enable 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 enable the Edge NFV, the customers can configure and deploy VNFs and VNF licenses from their network services.

- **Enable Edge NFV** – Select this option to enable the ability to deploy VNFs on Edges. After deploying one or more VNFs on Edges, you cannot disable this option.
- **Security VNFs** – Select the relevant checkboxes next to the third party VNFs, to deploy the corresponding security VNFs on Edges.

After selecting the security VNFs, click **Save Changes**.

Manage Edge Software Images

You can manage the Edge software images assigned to an enterprise directly by assigning an Operator Profile to an enterprise or allow an Enterprise Super User to manage the software images.

In the Operator portal, navigate to **Manage Customers**.

Select a customer and click **Actions** > **Modify** or click the link to the customer.

In the Enterprise portal, click **Configure** > **Customers**.

In the **Customer Configuration** page, the **Edge Image Management** section displays the current operator profile associated with the selected enterprise customer. As an Operator Super User, you can select and assign a different operator profile from the list of operator profiles available for the customer, if needed.

While switching to another operator profile, consider the following restrictions:

- If you switch from a Segment-based Operator Profile to a Network-based Operator Profile, the Edges in the enterprise for the Segment-based Profile do not receive any software image updates.
- If you switch from a Network-based Operator Profile to a Segment-based Operator Profile, the Edges in the enterprise for the Network-based Profile do not receive any software image updates.

If you want an Enterprise Super user to manage Edge software images then you have to enable the **Delegate Edge Software Image Management** checkbox. Once you enable **Delegate Edge Software Image Management** and click **Save Changes**, all the assigned software images for the enterprise customer appears. Click **Modify** to add or remove a software image for the selected customer.

Note You can remove an assigned image from an enterprise customer only if the image is not a default image and it is not currently used by any edges within the enterprise.

Associate Gateway Pool

You can associate a Gateway Pool to an Enterprise. The Edges in the Enterprise connect to the sites using the Gateways in the Gateway pool.

In the Operator portal, navigate to **Manage Customers**.

Select a customer and click **Actions** > **Modify** or click the link to the customer.

In the Enterprise portal, click **Configure** > **Customers**.

In the **Customer Configuration** page, the **Gateway pool** section displays the current Gateway pool associated with the selected customer. If required, you can choose a different Gateway pool available in the drop-down list and click **Save Changes**.

If the Gateways available in the Gateway pool have been assigned with Partner Gateway role, you can handoff the Gateways to partners. Select the **Enable Partner Handoff** to configure the handoff options for the segments and Gateways. For more information, see Configure Partner Handoff.

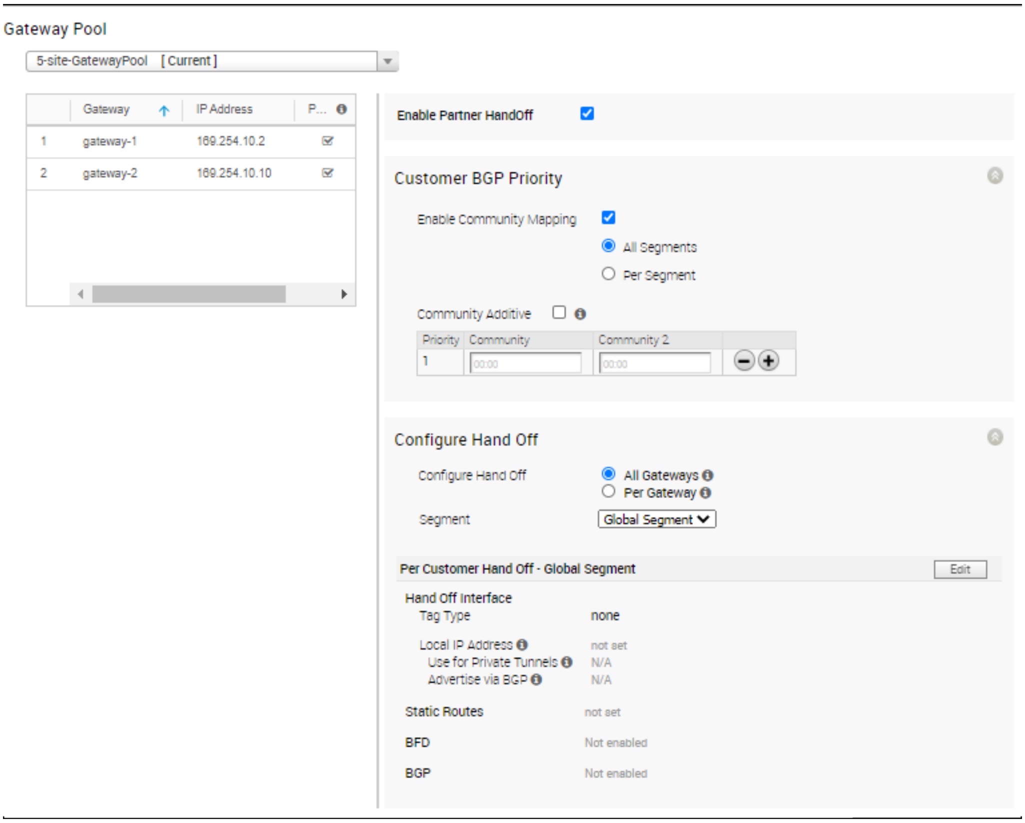
Configure Partner Handoff

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

Ensure that the Gateway to be handed off is assigned with Partner Gateway Role. In the Orchestrator portal, click **Gateways** and click the link to an existing Gateway. In the **Properties** section of the selected Gateway, you can enable the Partner Gateway role.

To configure the handoff settings, go to the **Customer Configuration** page.

- In the Operator portal, click **Manage Customers**.
- Select the customer and click **Actions > Modify** or click the link to the customer.
- In the customer or Enterprise portal, click **Configure > Customer**.
- In the **Customer Configuration**, navigate to the **Gateway Pool** section and select the **Enable Partner Handoff** checkbox.



Gateway Pool

5-site-GatewayPool [Current]

	Gateway	IP Address	P...
1	gateway-1	169.254.10.2	☑
2	gateway-2	169.254.10.10	☑

Enable Partner Handoff ☑

Customer BGP Priority

Enable Community Mapping ☑
● All Segments
○ Per Segment

Community Additive ☐

Priority	Community	Community 2
1	00:00	00:00

Configure Hand Off

Configure Hand Off ● All Gateways ○ Per Gateway

Segment: Global Segment

Per Customer Hand Off - Global Segment — Edit

Hand Off Interface
Tag Type: none
Local IP Address: not set
Use for Private Tunnels: N/A
Advertise via BGP: N/A

Static Routes: not set
BFD: Not enabled
BGP: Not enabled

Configure the following settings:

Customer BGP Priority

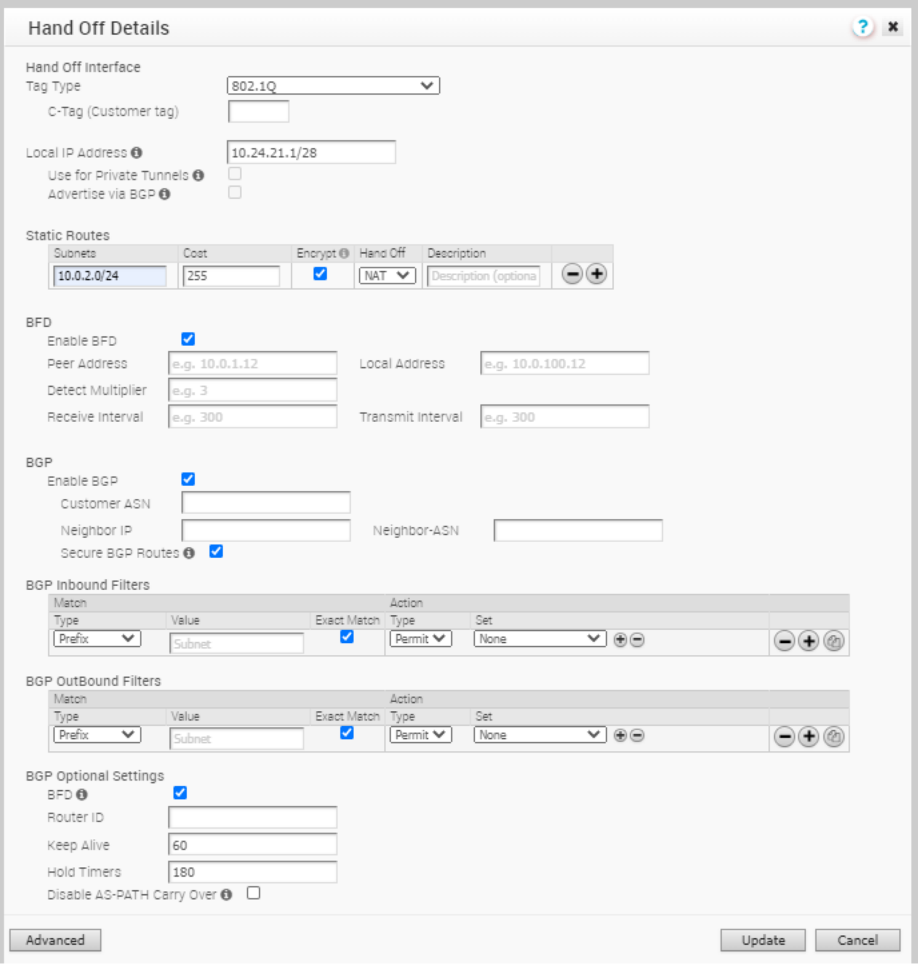
- Select **Enable Community Mapping** to set the Community attributes, which would be tagged in the BGP advertised routes.
- The Community mapping is set to all the segments by default. If you want to configure the Community attributes for a specific segment, choose **Per Segment**, and select the Segment from the drop-down list.

- Select **Community Additive** checkbox to enable the additive option associated with a particular auto community configuration. This option preserves the incoming community attributes for a prefix received from the overlay and appends the configured auto community to the prefix, on the Partner Gateway. As a result, the MPLS PE side receives prefixes with all the community attributes including the auto community attributes.
- Enter the Community attributes in the **Community** and **Community 2** fields. Click the Plus(**+**) Icon to add more community attributes.

Configure Hand Off

- By default, the handoff configuration is applied to all the Gateways. If you want to configure a specific Gateway, choose **Per Gateway** and select the Gateway from the drop-down list.
- By default, the handoff configuration is applied to all the Segments. If you want to configure a specific Segment, select the **Segment** from the drop-down list.
- For configuring all the Gateways, click the **Edit** option. If you have selected a particular Gateway, click the **Click here to configure** link.

The **Hand Off Details** window appears and you can configure the following:



Hand Off Details

Hand Off Interface
Tag Type: 802.1Q
C-Tag (Customer tag):

Local IP Address: 10.24.21.1/28
Use for Private Tunnels: □
Advertise via BGP: □

Static Routes

Subnets	Cost	Encrypt	Hand Off	Description
10.0.2.0/24	255	☑	NAT	Description (optiona

BFD
Enable BFD: ☑
Peer Address: e.g. 10.0.1.12 Local Address: e.g. 10.0.100.12
Detect Multiplier: e.g. 3
Receive Interval: e.g. 300 Transmit Interval: e.g. 300

BGP
Enable BGP: ☑
Customer ASN:
Neighbor IP: Neighbor-ASN:
Secure BGP Routes: ☑

BGP Inbound Filters

Match			Action	
Type	Value	Exact Match	Type	Set
Prefix	Subnet	☑	Permit	None

BGP OutBound Filters

Match			Action	
Type	Value	Exact Match	Type	Set
Prefix	Subnet	☑	Permit	None

BGP Optional Settings
BFD: ☑
Router ID:
Keep Alive: 60
Hold Timers: 180
Disable AS-PATH Carry Over: □

Option	Description
Hand Off Interface	
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 tags available: ■ **None**– Untagged. Choose this during single tenant handoff or a handoff towards shared services VRF. ■ **802.1q** – Single VLAN tag. ■ **802.1ad / QinQ(0x8100) / QinQ(0x9100)** – Dual VLAN tag.
Transport LAN VLAN	This option is available only when you choose the tag type as 802.1ad / QinQ(0x8100) / QinQ(0x9100). Choose the type of tag to configure the transport VLANs.
C-Tag (Customer tag)	Enter the Customer VLAN tag
S-Tag (Service tag)	Enter the service-provider-defined VLAN tag
Local IP Address	Enter the Local IP address for the logical Handoff interface.
Use for Private Tunnels	Select the checkbox so that private WAN links connect to the private IP address of the Partner Gateway. If private WAN connectivity is enabled on a Gateway, the Orchestrator audits to ensure that the local IP address is unique for each Gateway within an enterprise.
Advertise via BGP	Select the checkbox 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 – Click the plus(**+**) Icon to add more routes.	
Subnets	Enter the IP address of the Static Route Subnet that the Gateway should advertise to the Edge.
Cost	Enter the cost to apply weightage on the routes. The range is from 0 to 255.
Encrypt	Select the checkbox 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.
BFD	
Enable BFD	Select the checkbox to enable BFD subscription for BGP neighbors and to configure the BFD settings.
Peer Address	Enter the IP address of the remote peer to initiate a BFD session.
Local Address	Enter a locally configured IP address for the peer listener. This address is used to send the packets.

Option	Description
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 and the default value is 3.
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 and the default value is 300 milliseconds.
Transmit Interval	Enter the minimum time interval, in milliseconds, at which the local system can send the BFD control packets. The range is from 300 to 60000 milliseconds and the default value is 300 milliseconds.
BGP	
Enable BGP	Select the checkbox to enable BGP and set up the BGP configuration.
Customer ASN	Enter the customer Autonomous System Number.
Neighbor IP	Enter the IP address of the configured Neighbor network.
Neighbor-ASN	Enter the ASN of the Neighbor network.
Secure BGP Routes	Select the checkbox to enable encryption for data-forwarding over BGP routes.
BGP Inbound/Outbound Filters – Click the plus(**+**) Icon to add more Filters.	
Type (Match)	Choose the type of the BGP attribute to be considered for matching with the traffic flow. You can choose either **Prefix** or **Community**.
Value	Enter the value according to the BGP attribute selected as Type.
Exact Match	Select the checkbox for matching the attributes exactly.
Type (Action)	Choose the action to be performed if the match is True. You can either Permit or Deny the traffic.
Set	You can set the values of the attributes for the routes matching the filter criteria. Choose from the following attributes, and enter the corresponding values to be set for the matching routes: ■ None – The attributes of the matching routes remain the same. ■ Local Preference ■ Community – You can also enable the **Community Additive** option. ■ Metric ■ AS-Path-Prepend
BGP Optional Settings	

Option	Description
BFD	Select the checkbox 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.
Disable AS-PATH Carry Over	Select the checkbox to disable 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 checkbox.

Click **Update** to save the settings. In addition, click **Save Changes** in the **Customer Configuration** page to activate the settings.

Manage Partners

9

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

In the Operator panel, click **Manage Partners**. Click **Actions** to perform the following activities:

- **New Partner**: Creates a new partner. See Create New Partner.
- **Modify Partner**: Navigates to the **Partner Overview** in the Partner portal, where you can configure other settings corresponding to the selected partner. You can also click a partner name to navigate to the Partner portal. For more information see the Configure Partner Information.
- **Delete Partner**: Deletes the selected partners. Ensure that you have removed all the customers associated to the selected partner, before deleting the partner.
- **Add Operator Profiles**: Assigns an Operator profile to the selected partners, which specifies the network settings managed by SD-WAN Orchestrator. After selecting the partners, click **Actions > Add Operator Profiles**. In the **Add Profile to Selected Partners** window, select a profile from the **Operator profile** drop-down menu and click **Submit**.

  Note The **Operator profile** drop-down menu displays only Operator Profiles with images that have not been deprecated.

  For more information about Operator profiles, see Manage Operator Profiles.

This chapter includes the following topics:

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.

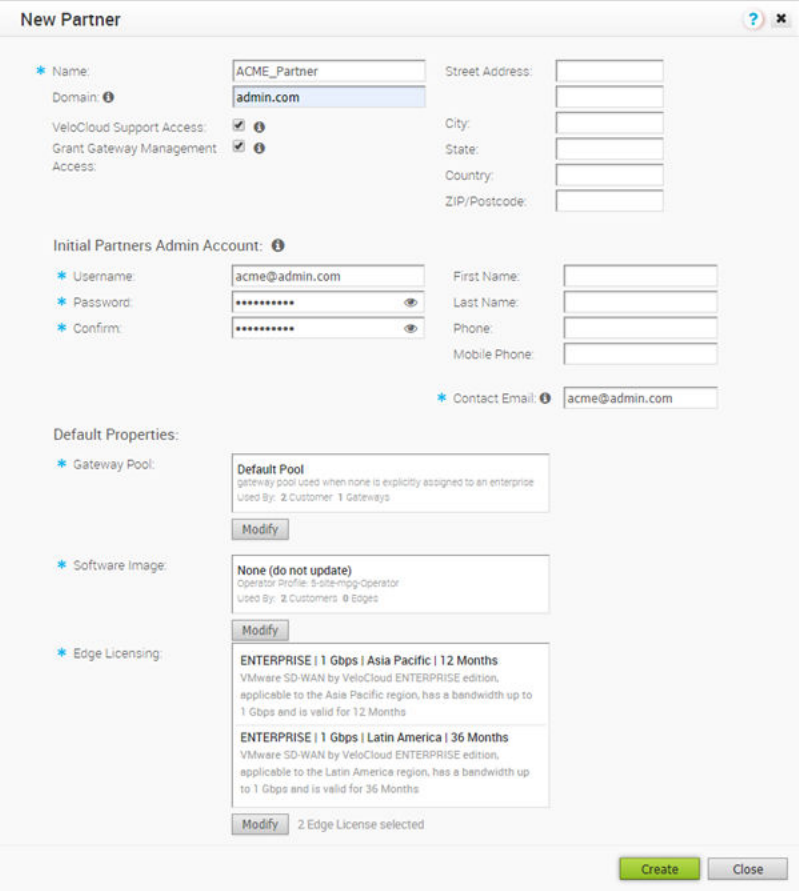
Only Operator Superusers, Standard Operators, and Business Specialist Operators can create a new partner.

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

In the Operator portal, navigate to **Manage Partners**.

1 In the **Manage Partners** page, click **New Partner** or click **Actions > New Partner**.

2 In the **New Partner** window, enter the following details:



New Partner

* Name:	ACME_Partner	Street Address:	
Domain:	admin.com		
VeloCloud Support Access:	☑	City:	
Grant Gateway Management Access:	☑	State:	
		Country:	
		ZIP/Postcode:	

Initial Partners Admin Account:

* Username:	acme@admin.com	First Name:	
* Password:	•••••••••••	Last Name:	
* Confirm:	•••••••••••	Phone:	
		Mobile Phone:	
		* Contact Email:	acme@admin.com

Default Properties:

* Gateway Pool: **Default Pool** gateway pool used when none is explicitly assigned to an enterprise Used By: 2 Customer 1 Gateways

* Software Image: **None (do not update)** Operator Profile: 5-site-mpg-Operator Used By: 2 Customers 0 Edges

* Edge Licensing:
  - **ENTERPRISE | 1 Gbps | Asia Pacific | 12 Months** VMware SD-WAN by VeloCloud ENTERPRISE edition, applicable to the Asia Pacific region, has a bandwidth up to 1 Gbps and is valid for 12 Months
  - **ENTERPRISE | 1 Gbps | Latin America | 36 Months** VMware SD-WAN by VeloCloud ENTERPRISE edition, applicable to the Latin America region, has a bandwidth up to 1 Gbps and is valid for 36 Months

2 Edge License selected

Option	Description
Name	Enter the partner name
Domain	Enter the domain name of the partner
VeloCloud Support Access	This option is selected by default and grants access to the VMware Support to view, configure, and troubleshoot the settings of the partner.

Option	Description
Grant Gateway Management Access	Select the checkbox to allow the partner to create and manage the Gateways.
Street Address, City, State, Country, ZIP/Postcode	Enter relevant address details in the respective fields.

Table 9-1. Initial Partners Admin Account

Option	Description
Username	Enter the username in the **user@domain.com** format.
Password	Enter a password for the partner.
Confirm	Re-enter the password.
First Name, Last Name, Phone, Mobile Phone	Enter the details like name and phone number in the appropriate fields.
Contact Email	Enter the Email address. The alerts on service status are sent to this Email address.

Default Properties

By default, the following properties are assigned to the customers managed by the partner. If required, the partner can modify the settings for each customer.

Table 9-2.

Option	Description
Gateway Pool	Click **Add** to select the Gateway Pool from the available list. After adding the Gateway Pools, you can click **Modify** to add or remove the pools. For more information on Gateway pools, see Gateway Pools.
Software Image	Click **Add** to select the Software Image from the available list. After adding the Software Image, you can click **Modify** to add or remove the Images. For more information on Software Images, see Chapter 10 Software Images.
Edge Licensing	Click **Add** to select the Edge licenses from the available list. After adding the licenses, you can click **Modify** to add or remove the licenses. This option is available only when the value of System Property **session.options.enableEdgeLicensing** is set to True. **Note** The license types can be used on multiple Edges. It is recommended to provide the partners with access to all types of licenses to match their edition and region. For more information, see Chapter 16 Edge Licensing.

Click **Create**.

The new partner name is displayed in the **Manage Partners** page. You can click the partner name to navigate to the Partner portal and add more configurations to the partner. See Configure Partner Information.

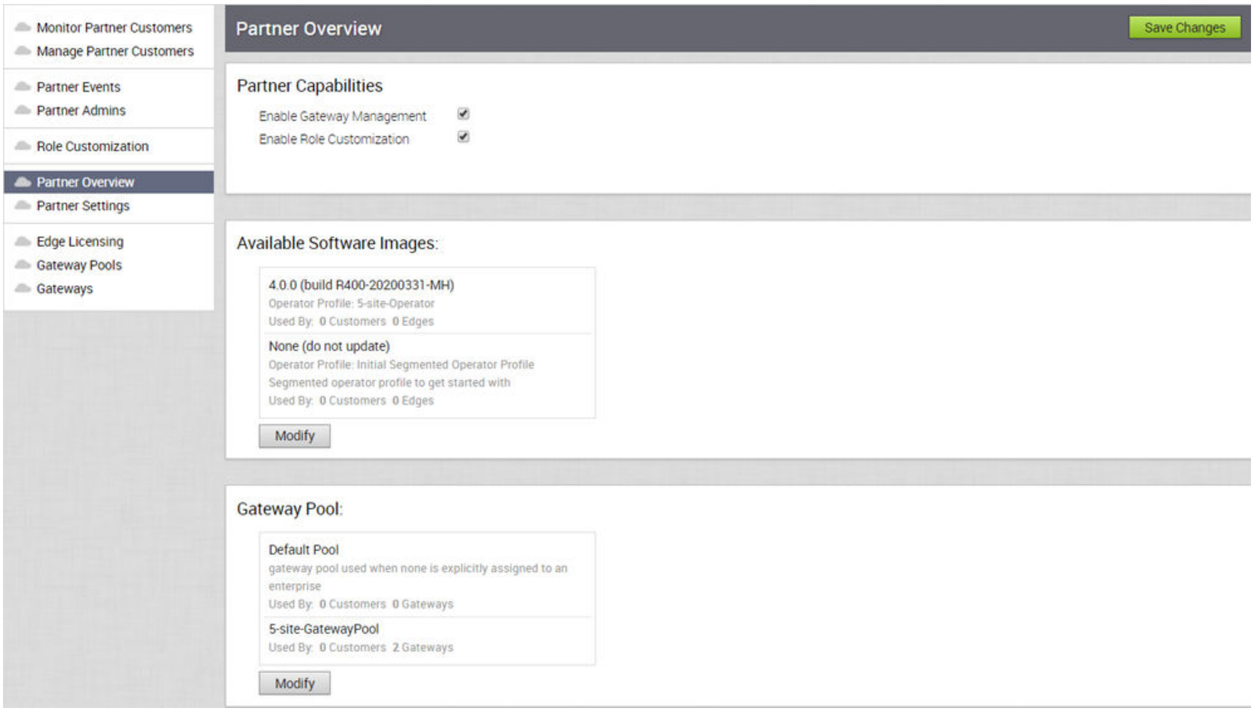
Configure Partner Information

After creating a partner, configure the feature options and settings that the partner can access. As an Operator, you can choose the settings the partner can modify and use to configure the enterprise users of the partner.

When you create a new partner, you are redirected to the **Partner Overview** page, where you can configure the customer settings.

You can also navigate to the Overview page from the **Manage Partners** page in the Orchestrator portal. Select the partner and click **Actions > Modify** or click the link to the partner.

In the Partner portal, click **Partner Overview**, and you can configure the following settings.



Partner Overview

Partner Capabilities

Enable Gateway Management ☑
Enable Role Customization ☑

Available Software Images:

4.0.0 (build R400-20200331-MH)
Operator Profile: 5-site-Operator
Used By: 0 Customers 0 Edges

None (do not update)
Operator Profile: Initial Segmented Operator Profile
Segmented operator profile to get started with
Used By: 0 Customers 0 Edges

Gateway Pool:

Default Pool
gateway pool used when none is explicitly assigned to an enterprise
Used By: 0 Customers 0 Gateways

5-site-GatewayPool
Used By: 0 Customers 2 Gateways

Partner Capabilities

You can enable or disable the following capabilities for the selected partner:

- **Enable Gateway Management** – Allows to enable or disable the Partner users to create, configure, and manage their own Gateways.
- **Enable Role Customization** – Allows to enable or disable a Partner super user to customize the role privileges of other Partner users and Enterprise users of the Partner. By default, this option is enabled.

Available Software Images

Displays all the software images assigned to the Partner. Click **Modify** to add or remove the software images in the list.

Note You cannot remove the software images that are assigned to a Customer.

Gateway Pool

Displays the Gateway pools associated with the selected Partner. Click **Modify** to add or remove the Gateway pools in the list.

Note You cannot remove the Gateway Pools that are assigned to a Customer.

Software Images

10

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

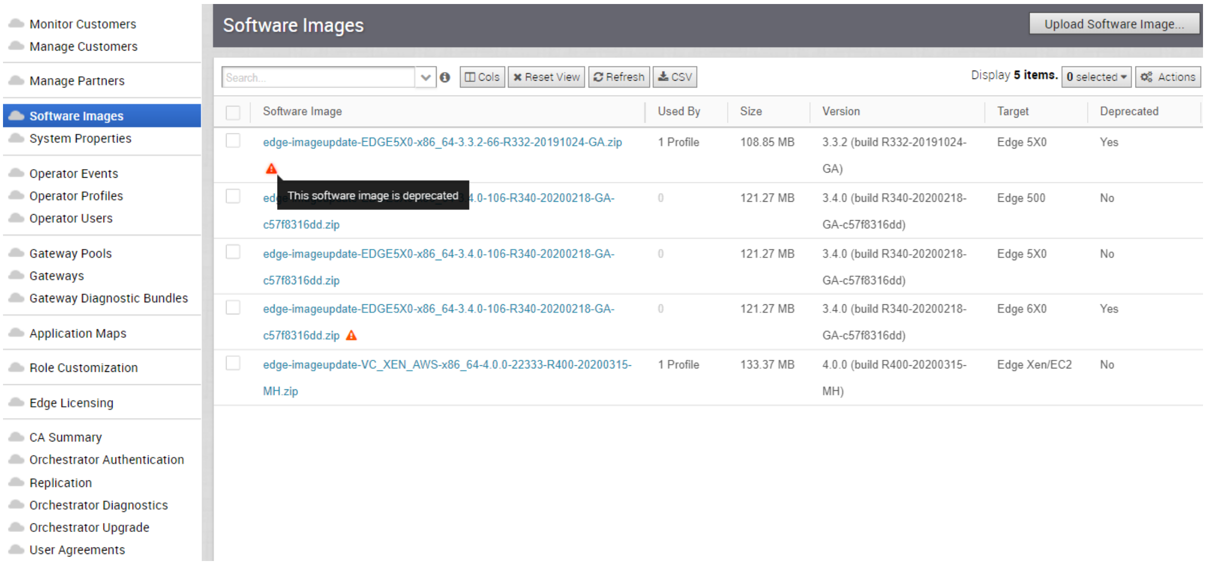
As an Operator Super User, you can upload a new software image, modify the existing software images, and delete a software image associated with the Edges.

Procedure

1 To upload a new software image, in the Operator portal, click **Software Images**.

2 Click **Upload Software 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.

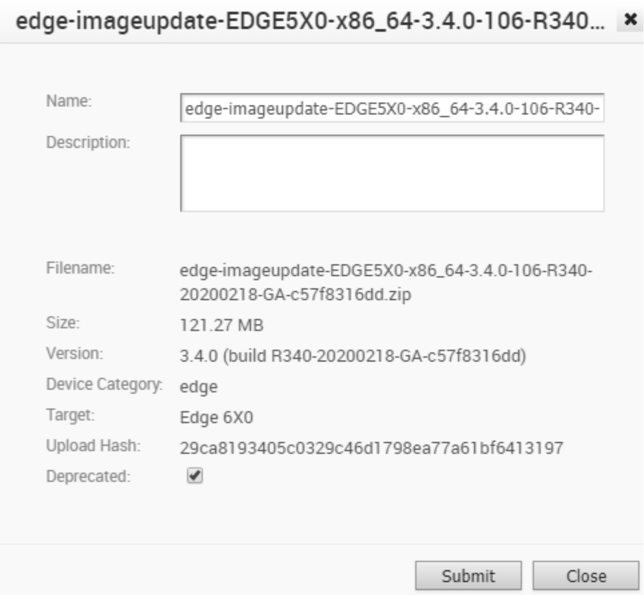
3 The uploaded packages are displayed in the **Software Images** page.



□	Software Image	Used By	Size	Version	Target	Deprecated
□	edge-imageupdate-EDGE5X0-x86_64-3.3.2-66-R332-20191024-GA.zip ⚠	1 Profile	108.85 MB	3.3.2 (build R332-20191024-GA)	Edge 5X0	Yes
□	ed 4.0-106-R340-20200218-GA-c57f8316dd.zip	0	121.27 MB	3.4.0 (build R340-20200218-GA-c57f8316dd)	Edge 500	No
□	edge-imageupdate-EDGE5X0-x86_64-3.4.0-106-R340-20200218-GA-c57f8316dd.zip	0	121.27 MB	3.4.0 (build R340-20200218-GA-c57f8316dd)	Edge 5X0	No
□	edge-imageupdate-EDGE5X0-x86_64-3.4.0-106-R340-20200218-GA-c57f8316dd.zip ⚠	0	121.27 MB	3.4.0 (build R340-20200218-GA-c57f8316dd)	Edge 6X0	Yes
□	edge-imageupdate-VC_XEN_AWS-x86_64-4.0.0-22333-R400-20200315-MH.zip	1 Profile	133.37 MB	4.0.0 (build R400-20200315-MH)	Edge Xen/EC2	No

This software image is deprecated

4 To modify an uploaded software image, click the link to the image name or select the image and click **Actions > Modify Software Image**. The **Edge Image Update** pop-up window appears.



edge-imageupdate-EDGE5X0-x86_64-3.4.0-106-R340... ✖

Name: edge-imageupdate-EDGE5X0-x86_64-3.4.0-106-R340-

Description:

Filename: edge-imageupdate-EDGE5X0-x86_64-3.4.0-106-R340-20200218-GA-c57f8316dd.zip

Size: 121.27 MB

Version: 3.4.0 (build R340-20200218-GA-c57f8316dd)

Device Category: edge

Target: Edge 6X0

Upload Hash: 29ca8193405c0329c46d1798ea77a61bf6413197

Deprecated: ☑

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 **Actions > Delete Software Image**.

What to do next

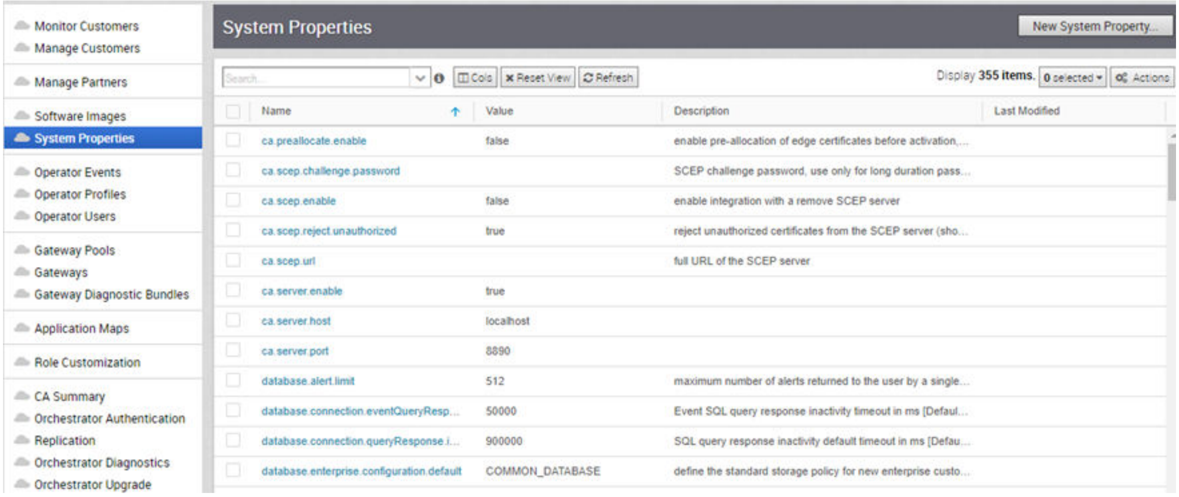
To upgrade the Edges within an Enterprise with a specific Software Image, see Manage Operator Profiles.

System Properties

11

VMware 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.



□	Name	Value	Description	Last Modified
□	ca.preallocate.enable	false	enable pre-allocation of edge certificates before activation,...	
□	ca.scep.challenge.password		SCEP challenge password, use only for long duration pass...	
□	ca.scep.enable	false	enable integration with a remove SCEP server	
□	ca.scep.reject.unauthorized	true	reject unauthorized certificates from the SCEP server (sho...	
□	ca.scep.url		full URL of the SCEP server	
□	ca.server.enable	true		
□	ca.server.host	localhost		
□	ca.server.port	8890		
□	database.alert.limit	512	maximum number of alerts returned to the user by a single...	
□	database.connection.eventQueryResp...	50000	Event SQL query response inactivity timeout in ms [Defaul...	
□	database.connection.queryResponse.i...	900000	SQL query response inactivity default timeout in ms [Defau...	
□	database.enterprise.configuration.default	COMMON_DATABASE	define the standard storage policy for new enterprise custo...	

To configure the system properties:

1. Click **New System Property** to add a new property.
2. In the **New System Property** window, enter a name for the new property and choose the **Data Type** from the drop-down list.
3. Enter the **Value** for the property according to the data type.
4. Enter a description for the property.
5. Click **Save**.
6. To modify the values of a property, click the link to the property or select the property and click **Actions** > **Modify System Property**.
7. To remove a property, select the property and click **Actions** > **Delete System Property**.

You can use the **Search** field to find a specific system property. See List of System Properties, which lists some of the system properties that you can modify as an Operator.

Note It is recommended to contact VMware Support before making changes to the system properties.

This chapter includes the following topics:

List of System Properties

As an Operator, you can add or modify the values of the system properties.

The following tables describe some of the system properties. As an Operator, you can set the values for these properties.

- Table 11-1. Alert Emails
- Table 11-2. Alerts
- Table 11-3. Certificate Authority
- List item.
- Table 11-6. Edge Activation
- Table 11-6. Edge Activation
- Table 11-7. Monitoring
- Table 11-8. Notifications
- Table 11-9. Password Reset and Lockout
- Table 11-10. Rate Limiting APIs
- Table 11-11. Remote Diagnostics
- Table 11-12. Self-service Password Reset
- Table 11-13. Two-factor Authentication
- Table 11-14. VNF Configuration
- Table 11-15. VPN

Table 11-1. Alert Emails

System Property	Description
vco.alert.mail.to	When an alert is triggered, a notification is sent immediately to the list of Email addresses provided in the Value field of this system property. You can enter multiple Email IDs separated by commas. If the property does not contain any value, then the notification is not sent. The notification is meant to alert VMware support / operations personnel of impending issues before notifying the customer.
vco.alert.mail.cc	When alert emails are sent to any customer, a copy is sent to the Email addresses provided in the Value field of this system property. You can enter multiple Email IDs separated by commas.
mail.*	There are multiple system properties available to control the Alert Emails. You can define the Email parameters like SMTP properties, username, password, and so on.

Table 11-2. Alerts

System Property	Description
vco.alert.enable	Globally enables or disables the generation of alerts for both Operators and Enterprise customers.
vco.enterprise.alert.enable	Globally enables or disables the generation of alerts for Enterprise customers.
vco.operator.alert.enable	Globally enables or disables the generation of alerts for Operators.

Table 11-3. Certificate Authority

System Property	Description

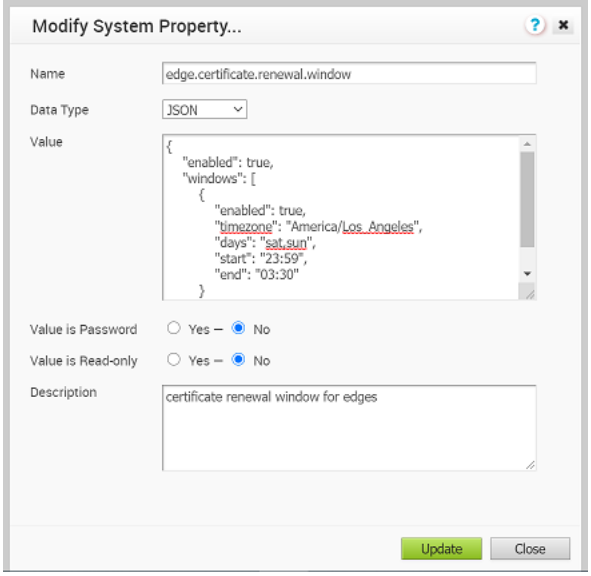
edge.certificate.renewal.window	This optional system property allows the Operator to define one or more maintenance windows during which the Edge certificate renewal is enabled. Certificates scheduled for renewal outside of the windows will be deferred until the current time falls within one of the enabled windows.
	Enable System Property:
	To enable this system property, type "true" for "enabled" in the first part of the **Value** text area in the **Modify System Property** dialog box. An example of the first part of this system property when it is enabled is shown below.
	Operators can define multiple windows to restrict the days and hours of the day during which Edge renewals are enabled. Each window can be defined by a day, or a list of days (separated by a comma), and a start and end time. Start and end times can be specified relative to an Edge's local time zone, or relative to UTC. See image below for an example.
	
	Modify System Property...
	Name: edge.certificate.renewal.window
	Data Type: JSON
	Value:
	`{`
	`    "enabled": true,`
	`    "windows": [`
	`        {`
	`            "enabled": true,`
	`            "timezone": "America/Los_Angeles",`
	`            "days": "sat,sun",`
	`            "start": "23:59",`
	`            "end": "03:30"`
	`        }`
	Value is Password: ○ Yes – ● No
	Value is Read-only: ○ Yes – ● No
	Description: certificate renewal window for edges
	Update Close
	Note If attributes are not present, the default is enabled "false."
	When defining window attributes, adhere to the following:
	■ Use IANA time zones, not PDT or PST (e.g. America/Los_Angeles) See https://en.wikipedia.org/wiki/List_of_tz_database_time_zones for more information.
	■ Use UTC for days (e.g. SAT, SUN).
	  ■ Separated by comma.
	  ■ Days in three letters in English.
	  ■ Not case sensitive.
	■ Use Military 24 hour time format only (HH:MM) for start times (e.g. 01:30) and end times (e.g. 05:30).

Table 11-3. Certificate Authority (continued)

System Property	Description
	If the above-mentioned values are missing, the attribute defaults in each window definition are as follow: - If enabled is missing, the default value = false. - If timezone is missing, the default = 'local.' - If one of either 'days' or end and start times are missing, the defaults are as follows: - If 'days' is missing, the start/end is applied to each day of the week (mon, tue, wed, thu, fri, sat, sun). - If end and start times are missing, then any time in the specified day will match (start = 00:00 and end = 23:59). - NOTE: One of either 'days' or end and start times must be present. However, if they are missing, the defaults will be as indicated above. Disable System Property: This system property is disabled by default, which means the certificate will automatically renew after it expires. "Enabled" will be set to "false in the first part of the **Value** text area in the **Modify System Property** dialog box. An example of this property when it is disabled is shown below. { "enabled": false, "windows": [{ NOTE: This system property requires that PKI be enabled.
gateway.certificate.renewal.window	This optional system property allows the Operator to define one or more maintenance windows during which the Gateway certificate renewal is enabled. Certificates scheduled for renewal outside of the windows will be deferred until the current time falls within one of the enabled windows. Enable System Property: To enable this system property, type "true" for "enabled" in the first part of the **Value** text area in the **Modify System Property** dialog box. See image below for an example. Operators can define multiple windows to restrict the days and hours of the day during which edge renewals are enabled. Each window can be defined by a day, or list of days (separated by a comma), and a start and end time. Start and end times can be specified relative to an edge's local timezone, or relative to UTC. See image below for an example.

Table 11-3. Certificate Authority (continued)

System Property	Description

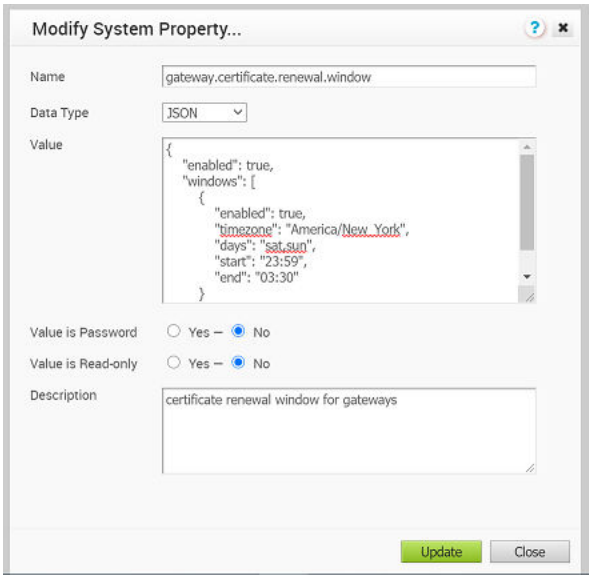
	
	Modify System Property...
	Name: gateway.certificate.renewal.window
	Data Type: JSON
	Value:
	`{`
	`    "enabled": true,`
	`    "windows": [`
	`        {`
	`            "enabled": true,`
	`            "timezone": "America/New_York",`
	`            "days": "sat,sun",`
	`            "start": "23:59",`
	`            "end": "03:30"`
	`        }`
	Value is Password: ○ Yes – ● No
	Value is Read-only: ○ Yes – ● No
	Description: certificate renewal window for gateways
	Update Close
	
	Note If attributes are not present, the default is enabled "false."
	
	When defining window attributes, adhere to the following:
	■ Use IANA time zones, not PDT or PST (e.g. America/Los_Angeles) See https://en.wikipedia.org/wiki/List_of_tz_database_time_zones for more information.
	■ Use UTC for days (e.g. SAT, SUN).
	    ■ Separated by comma.
	    ■ Days in three letters in English.
	    ■ Not case sensitive.
	■ Use Military 24 hour time format only (HH:MM) for start times (e.g. 01:30) and end times (e.g. 05:30).
	
	If the above-mentioned values are missing, the attribute defaults in each window definition are as follow:
	■ If enabled is missing, the default value = false.
	■ If timezone is missing, the default = 'local."
	■ If one of either 'days' or end and start times are missing, the defaults are as follows:
	    ■ If 'days' is missing, the start/end is applied to each day of the week (mon, tue, wed, thu, fri, sat, sun).
	    ■ If end and start times are missing, then any time in the specified day will match (start = 00:00 and end = 23:59).
	    ■ NOTE: One of either 'days' or (end and start) must be present. However, if they are missing, the defaults will be as indicated above.
	
	Disable System Property:
	
	This system property is disabled by default, which means the certificate will automatically renew after it expires. "Enabled" will be set to "false in the first part of the **Value** text area in the **Modify System Property** dialog box. An example of this property when it is disabled is shown below.

Table 11-3. Certificate Authority (continued)

System Property	Description
	{ "enabled": false, "windows": [{ NOTE: This system property requires that PKI be enabled.

Table 11-4. Data Retention

System Property	Description
retention.highResFlows.days	This system property enables Operators to configure high resolution flow stats data retention anywhere between 1 and 90 days.
retention.lowResFlows.months	This system property enables Operators to configure low resolution flow stats data retention anywhere between 1 and 365 days.
session.options.maxFlowstatsRetentionDays	This property enables Operators to query more than two weeks of flows stats data.

Table 11-5. Edges

System Property	Description
edge.offline.limit.sec	If the Orchestrator does not detect a heartbeat from an Edge for the specified duration, then the state of the Edge is moved to OFFLINE mode.
edge.link.unstable.limit.sec	When the Orchestrator does not receive link statistics for a link for the specified duration, the link is moved to UNSTABLE mode.
edge.link.disconnected.limit.sec	When the Orchestrator does not receive link statistics for a link for the specified duration, the link is disconnected.
edge.deadbeat.limit.days	If an Edge is not active for the specified number of days, then the Edge is not considered for generating Alerts.
vco.operator.alert.edgeLinkEvent.enable	Globally enables or disables Operator Alerts for Edge Link events.
vco.operator.alert.edgeLiveness.enable	Globally enables or disables Operator Alerts for Edge Liveness events.

Table 11-6. Edge Activation

System Property	Description
edge.activation.key.encode.enable	Base64 encodes the activation URL parameters to obscure values when the Edge Activation Email is sent to the Site Contact.
edge.activation.trustedIssuerReset.enable	Resets the trusted certificate issuer list of the Edge to contain only the Orchestrator Certificate Authority. All TLS traffic from the edge are restricted by the new issuer list.
network.public.certificate.issuer	Set the value of **network.public.certificate.issuer** equal to the PEM encoding of the issuer of Orchestrator server certificate, when **edge.activation.trustedIssuerReset.enable** is set to True. This will add the server certificate issuer to the trusted issuer of the Edge, in addition to the Orchestrator Certificate Authority.

Table 11-7. Monitoring

System Property	Description
vco.monitor.enable	Globally enables or disables monitoring of Enterprise and Operator entity states. Setting the Value to **False** prevents SD-WAN Orchestrator from changing entity states and triggering alerts.
vco.enterprise.monitor.enable	Globally enables or disables monitoring of Enterprise entity states.
vco.operator.monitor.enable	Globally enables or disables monitoring of Operator entity states.

Table 11-8. Notifications

System Property	Description
vco.notification.enable	Globally enables or disables the delivery of Alert notifications to both Operator and Enterprises.
vco.enterprise.notification.enable	Globally enables or disables the delivery of Alert notifications to the Enterprises.
vco.operator.notification.enable	Globally enables or disables the delivery of Alert notifications to the Operator.

Table 11-9. Password Reset and Lockout

System Property	Description
vco.enterprise.resetPassword.token.expirySeconds	Duration of time, after which the password reset link for an enterprise user expires.
vco.enterprise.authentication.passwordPolicy	Defines the password expiration and password history policy for enterprise users. Edit the JSON template in the Value field to define the following: **expiry**: ■ **enable**: Set this to **true** to enable automatic expiry of enterprise user passwords. ■ **days**: Enter the number of days that an enterprise password may be used before forced expiry. **history**: ■ **enable**: Set this to **true** to enable recording of enterprise users' previous Passwords. ■ **count**: Enter the number of previous Passwords to be saved in the history. When an enterprise user tries to change the password, the system does not allow the user to enter a password that is already saved in the history.
enterprise.user.lockout.defaultAttempts	Number of times the enterprise user can attempt to login. If the login fails for the specified number of times, the account is locked.
enterprise.user.lockout.defaultDurationSeconds	Duration of time, for which the enterprise user account is locked.
enterprise.user.lockout.enabled	Enables or disables the lockout option for the enterprise login failures.
vco.operator.resetPassword.token.expirySeconds	Duration of time, after which the password reset link for an Operator user expires.

Table 11-9. Password Reset and Lockout (continued)

System Property	Description
vco.operator.authentication.passwordPolicy	Defines the password expiration and password history policy for Operator users. Edit the JSON template in the Value field to define the following: **expiry**: ■ **enable**: Set this to **true** to enable automatic expiry of Operator user passwords. ■ **days**: Enter the number of days that an Operator password may be used before forced expiry. **history**: ■ **enable**: Set this to **true** to enable recording of Operator users' previous Passwords. ■ **count**: Enter the number of previous Passwords to be saved in the history. When an Operator user tries to change the password, the system does not allow the user to enter a password that is already saved in the history.
operator.user.lockout.defaultAttempts	Number of times the Operator user can attempt to login. If the login fails for the specified number of times, the account is locked.
operator.user.lockout.defaultDurationSeconds	Duration of time, for which the Operator user account is locked.
operator.user.lockout.enabled	Enables or disables the lockout option for the Operator login failures.

Table 11-10. Rate Limiting APIs

System Property	Description
vco.api.rateLimit.enabled	Allows Operator Super users enable or disable the rate limiting feature at the system level. By default, the value is **False**. **Note** The rate-limiter is not enabled in earnest, that is, it will not reject API requests that exceed the configured limits, unless the **vco.api.rateLimit.mode.logOnly** setting is disabled.
vco.api.rateLimit.mode.logOnly	Allows Operator Super user to use rate limit in a **LOG_ONLY** mode. When the value is set as **True** and if a rate limit exceeds, this option logs only the error and fires respective metrics allowing clients to make requests without rate limiting. When the value is set to **False**, the request API is restricted with defined policies and HTTP 429 is returned.

Table 11-10. Rate Limiting APIs (continued)

System Property	Description
vco.api.rateLimit.rules.global	Allows to define a set of globally applicable policies used by the rate-limiter, in a JSON array. By default, the value is an empty array. Each type of user (Operator, Partner, and Customer) can make up to 500 requests for every 5 seconds. The number of requests is subject to change based on the behavior pattern of the rate limited requests. The JSON array consists of the following parameters: **Types**: The type objects represent different contexts in which the rate limits are applied. The following are the different type objects that are available: ■ **SYSTEM**: Specifies a global limit shared by all the users. ■ **OPERATOR_USER**: A limit that can be set in general for all the Operator users. ■ **ENTERPRISE_USER**: A limit that can be set in general for all the Enterprise users. ■ **MSP_USER**: A limit that can be set in general for all the MSP users. ■ **ENTERPRISE**: A limit that can be shared between all users of an Enterprise and is applicable to all the Enterprises in the network. ■ **PROXY**: A limit that can be shared between all users of a Proxy and is applicable to all proxies. **Policies**: Add rules to the policies to apply the requests that match the rule, by configuring the following parameters: ■ **Match**: Enter the type of requests to be matched: ■ **All**: Rate-limit all requests matching one of the type objects. ■ **METHOD**: Rate-limit all requests matching the specified method name. ■ **METHOD_PREFIX**: Rate-limit all requests matching the specified method group. ■ **Rules**: Enter the values for the following parameters: ■ **maxConcurrent**: Number of jobs that can be performed at the same time. ■ **reservoir**: Number of jobs that can be performed before the limiter stops performing jobs. ■ **reservoirRefreshAmount**: Value to set the reservoir to when **reservoirRefreshInterval** is in use. ■ **reservoirRefreshInterval**: For every millisecond of **reservoirRefreshInterval**, the **reservoir** value will be automatically updated to the value of **reservoirRefreshAmount**. The **reservoirRefreshInterval** value should be a multiple of 250 (5000 for Clustering).

Table 11-10. Rate Limiting APIs (continued)

System Property	Description
	Enabled: Each type limit can be enabled or disabled by including the **enabled** key in **APIRateLimiterTypeObject**. By default, the value of **enabled** is True, even if the key is not included. You need to include **"enabled": false** key to disable the individual type limits. The following example shows a sample JSON file with default values:

```
[
    {
        "type": "OPERATOR_USER",
        "policies": [
            {
                "match": {
                    "type": "ALL"
                },
                "rules": {
                    "reservoir": 500,

"reservoirRefreshAmount": 500,

"reservoirRefreshInterval": 5000
                }
            }
        ]
    },
    {
        "type": "MSP_USER",
        "policies": [
            {
                "match": {
                    "type": "ALL"
                },
                "rules": {
                    "reservoir": 500,

"reservoirRefreshAmount": 500,

"reservoirRefreshInterval": 5000
                }
            }
        ]
    },
    {
        "type": "ENTERPRISE_USER",
        "policies": [
            {
                "match": {
                    "type": "ALL"
                },
                "rules": {
                    "reservoir": 500,

"reservoirRefreshAmount": 500,

"reservoirRefreshInterval": 5000
                }
            }
        ]
```

Table 11-10. Rate Limiting APIs (continued)

System Property	Description

	`    }`
	`]`
	Note It is recommended not to change the default values of the configuration parameters.

vco.api.rateLimit.rules.enterprise.default	Comprises the default set of Enterprise-specific policies applied to newly created Customers. The Customer-specific properties are stored in the Enterprise property **vco.api.rateLimit.rules.enterprise**.
vco.api.rateLimit.rules.enterpriseProxy.default	Comprises the default set of Enterprise-specific policies applied to newly created Partners. The Partner-specific properties are stored in the Enterprise proxy property **vco.api.rateLimit.rules.enterpriseProxy**.

For more information on Rate limiting, see Chapter 23 Rate Limiting API Requests.

Table 11-11. Remote Diagnostics

System Property	Description
network.public.address	Specifies the browser origin address/DNS hostname that is used to access the SD-WAN Orchestrator UI.
network.portal.websocket.address	Allows to set an alternate DNS hostname/address to access the SD-WAN Orchestrator UI from a browser, if the browser address is not the same as the value of `network.public.address` system property. As remote diagnostics now uses a WebSocket connection, to ensure web security, the browser origin address that is used to access the Orchestrator UI is validated for incoming requests. In most cases, this address is same as the `network.public.address` system property. In rare scenarios, the Orchestrator UI can be accessed using another DNS hostname/address that is different from the value set in the `network.public.address` system property. In such cases, you can set this system property to the alternate DNS hostname/address. By default, this value is not set.
session.options.websocket.portal.idle.timeout	Allows to set the total amount of time (in seconds) the browser WebSocket connection is active in an idle state. By default, the browser WebSocket connection is active for 300 seconds in an idle state.

Table 11-12. Self-service Password Reset

System Property	Description
vco.enterprise.resetPassword.twoFactor.mode	Defines the mode for the second level for password reset authentication, for all the Enterprise users. Currently, only the SMS mode is supported.
vco.enterprise.resetPassword.twoFactor.required	Enables or disables the two-factor authentication for password reset of Enterprise users.
vco.enterprise.selfResetPassword.enabled	Enables or disables self-service password reset for Enterprise users.
vco.enterprise.selfResetPassword.token.expirySeconds	Duration of time, after which the self-service password reset link for an Enterprise user expires.
vco.operator.resetPassword.twoFactor.required	Enables or disables the two-factor authentication for password reset of Operator users.
vco.operator.selfResetPassword.enabled	Enables or disables self-service password reset for Operator users.
vco.operator.selfResetPassword.token.expirySeconds	Duration of time, after which the self-service password reset link for an Operator user expires.

Table 11-13. Two-factor Authentication

System Property	Description
vco.enterprise.authentication.twoFactor.enable	Enables or disables the two-factor authentication for Enterprise users.
vco.enterprise.authentication.twoFactor.mode	Defines the mode for the second level authentication for Enterprise users. Currently, only SMS is supported as the second level authentication mode.
vco.enterprise.authentication.twoFactor.require	Defines the two-factor authentication as mandatory for Enterprise users.
vco.operator.authentication.twoFactor.enable	Enables or disables the two-factor authentication for Operator users.
vco.operator.authentication.twoFactor.mode	Defines the mode for the second level authentication for Operator users. Currently, only SMS is supported as the second level authentication mode.
vco.operator.authentication.twoFactor.require	Defines the two-factor authentication as mandatory for Operator users.

Table 11-14. VNF Configuration

<table>
<tr><th>System Property</th><th>Description</th></tr>
<tr><td>edge.vnf.extraImageInfos</td><td>

Defines the properties of a VNF Image.

You can enter the following information for a VNF Image, in JSON format in the **Value** field:

```
[
  {
    "vendor": "Vendor Name",
    "version": "VNF Image Version",
    "checksum": "VNF Checksum Value",
    "checksumType": "VNF Checksum Type"
  }
]
```

Example of JSON file for Check Point Firewall Image:

```
[
  {
    "vendor": "checkPoint",
    "version": "r80.40_no_workaround_46",
    "checksum":
"bc9b06376cdbf210cad8202d728f1602b79cfd7d",
    "checksumType": "sha-1"
  }
]
```

Example os JSON file for Fortinet Firewall Image:

```
[
   {
      "vendor": "fortinet",
      "version": "624",
      "checksum":
"6d9e2939b8a4a02de499528c745d76bf75f9821f",
      "checksumType": "sha-1"
   }
]
```

</td></tr>
<tr><td>edge.vnf.metric.record.limit</td><td>Defines the number of records to be stored in the database</td></tr>
<tr><td>enterprise.capability.edgeVnfs.enable</td><td>Enables VNF deployment on supported Edge models.</td></tr>
<tr><td>enterprise.capability.edgeVnfs.securityVnf.checkPoint</td><td>Enables Check Point Networks Firewall VNF</td></tr>
<tr><td>enterprise.capability.edgeVnfs.securityVnf.fortinet</td><td>Enables Fortinet Networks Firewall VNF</td></tr>
<tr><td>enterprise.capability.edgeVnfs.securityVnf.paloAlto</td><td>Enable Palo Alto Networks Firewall VNF</td></tr>
<tr><td>session.options.enableVnf</td><td>Enables VNF feature</td></tr>
<tr><td>vco.operator.alert.edgeVnfEvent.enable</td><td>Enables or disables Operator alerts for Edge VNF events globally.</td></tr>
<tr><td>vco.operator.alert.edgeVnfInsertionEvent.enable</td><td>Enables or disables Operator alerts for Edge VNF Insertion events globally.</td></tr>
</table>

Table 11-15. VPN

System Property	Description
vpn.disconnect.wait.sec	The time interval for the system to wait before disconnecting a VPN tunnel.
vpn.reconnect.wait.sec	The time interval for the system to wait before reconnecting a VPN tunnel.

Manage Operators

12

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

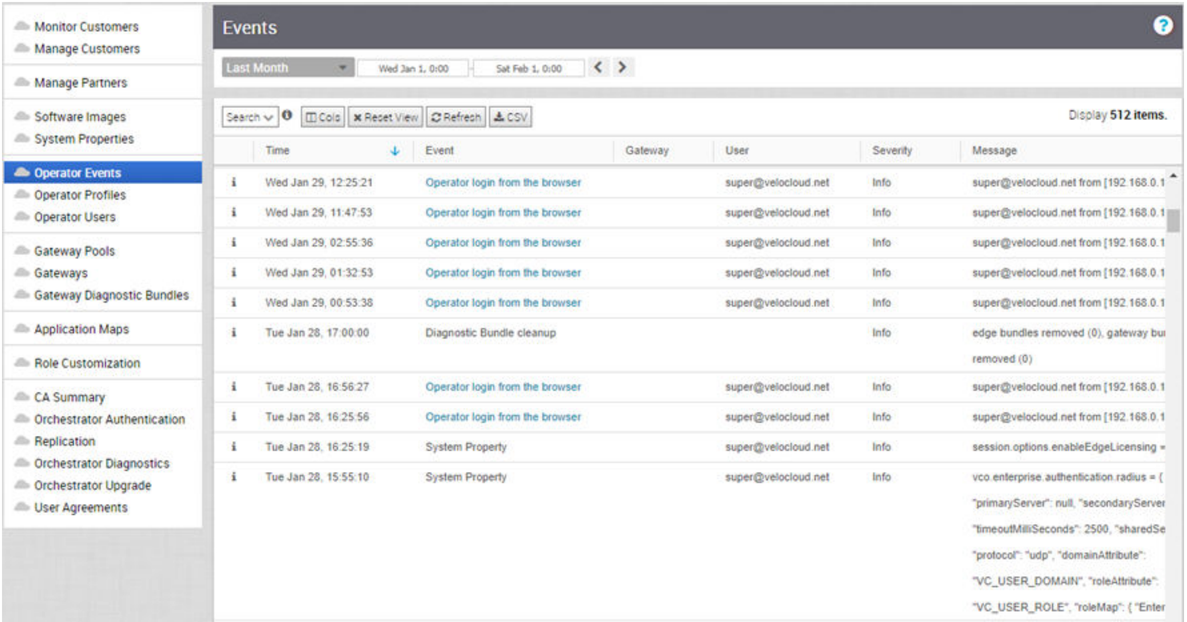
This chapter includes the following topics:

- Monitor Operator Events
- Manage Operator Profiles
- Manage Operator Users

Monitor Operator Events

Operator events are triggered by the activities of Operators. These events help to determine the status of VMware System.

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



Display **512 items.**

	Time	Event	Gateway	User	Severity	Message
i	Wed Jan 29, 12:25:21	Operator login from the browser		super@velocloud.net	Info	super@velocloud.net from [192.168.0.1
i	Wed Jan 29, 11:47:53	Operator login from the browser		super@velocloud.net	Info	super@velocloud.net from [192.168.0.1
i	Wed Jan 29, 02:55:36	Operator login from the browser		super@velocloud.net	Info	super@velocloud.net from [192.168.0.1
i	Wed Jan 29, 01:32:53	Operator login from the browser		super@velocloud.net	Info	super@velocloud.net from [192.168.0.1
i	Wed Jan 29, 00:53:38	Operator login from the browser		super@velocloud.net	Info	super@velocloud.net from [192.168.0.1
i	Tue Jan 28, 17:00:00	Diagnostic Bundle cleanup			Info	edge bundles removed (0), gateway bu removed (0)
i	Tue Jan 28, 16:56:27	Operator login from the browser		super@velocloud.net	Info	super@velocloud.net from [192.168.0.1
i	Tue Jan 28, 16:25:56	Operator login from the browser		super@velocloud.net	Info	super@velocloud.net from [192.168.0.1
i	Tue Jan 28, 16:25:19	System Property		super@velocloud.net	Info	session.options.enableEdgeLicensing =
i	Tue Jan 28, 15:55:10	System Property		super@velocloud.net	Info	vco.enterprise.authentication.radius = { "primaryServer": null, "secondaryServer "timeoutMilliSeconds": 2500, "sharedSe "protocol": "udp", "domainAttribute": "VC_USER_DOMAIN", "roleAttribute": "VC_USER_ROLE", "roleMap": { "Enter

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

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

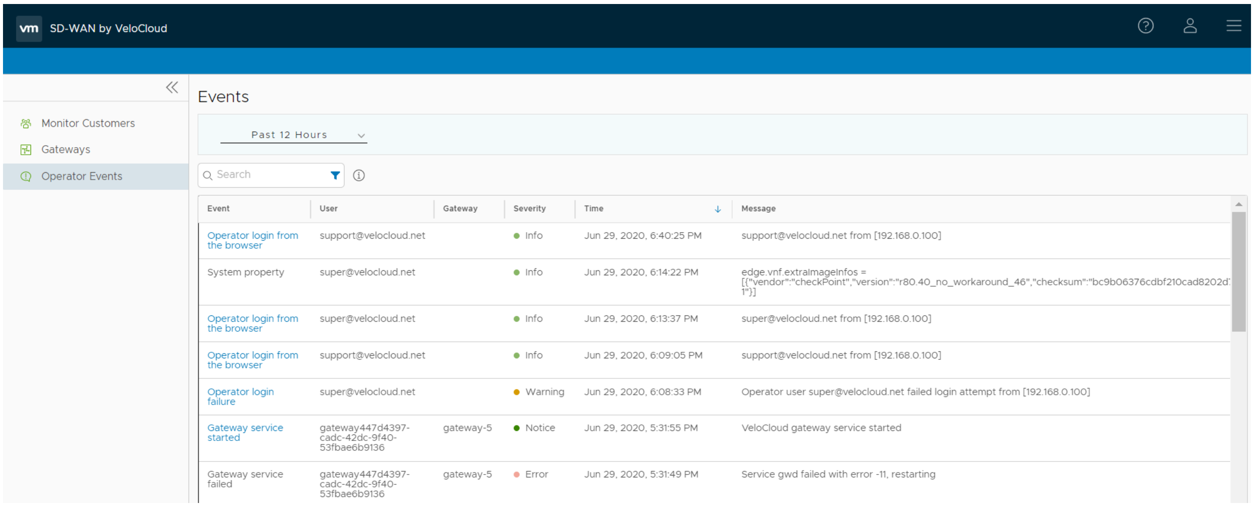
Once you choose or setup the duration, the page displays the events triggered during the selected period.

The page displays the following options:

- **Search** – Enter a term to search for a specific detail. Click the drop-down arrow to filter the view by specific criteria.
- **Cols** – Click and select the columns to be shown or hidden in the view.
- **Reset View** – Click to reset the view to default settings.
- **Refresh** – Click to refresh the details displayed with the most current data.
- **CSV** – Click to export all data to a file in CSV format.

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

- In the Operator portal, click the **Open New Orchestrator UI** option available at the top of the Window.
- Click **Launch New Orchestrator UI** in the pop-up window. The UI opens in a new tab displaying the monitoring options.
- Click **Operator Events** to view the events.



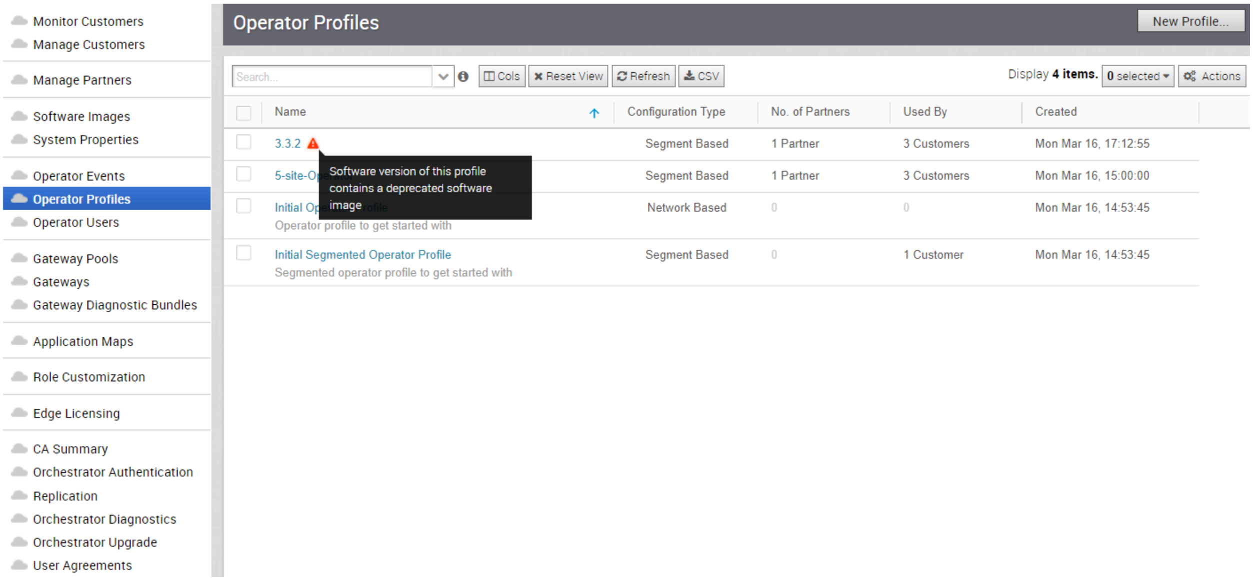
Event	User	Gateway	Severity	Time ↓	Message
Operator login from the browser	support@velocloud.net		● Info	Jun 29, 2020, 6:40:25 PM	support@velocloud.net from [192.168.0.100]
System property	super@velocloud.net		● Info	Jun 29, 2020, 6:14:22 PM	edge.vnf.extraImageInfos = [{"vendor":"checkPoint","version":"r80.40_no_workaround_46","checksum":"bc9b06376cdbf210cad8202d 1"}]
Operator login from the browser	super@velocloud.net		● Info	Jun 29, 2020, 6:13:37 PM	super@velocloud.net from [192.168.0.100]
Operator login from the browser	support@velocloud.net		● Info	Jun 29, 2020, 6:09:05 PM	support@velocloud.net from [192.168.0.100]
Operator login failure	super@velocloud.net		● Warning	Jun 29, 2020, 6:08:33 PM	Operator user super@velocloud.net failed login attempt from [192.168.0.100]
Gateway service started	gateway447d4397-cadc-42dc-9f40-53fbae6b9136	gateway-5	● Notice	Jun 29, 2020, 5:31:55 PM	VeloCloud gateway service started
Gateway service failed	gateway447d4397-cadc-42dc-9f40-53fbae6b9136	gateway-5	● Error	Jun 29, 2020, 5:31:49 PM	Service gwd failed with error -11, restarting

In the **Search** field, enter a term to search for specific details. Click the Filter Icon to filter the view by a specific criteria.

Manage Operator Profiles

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

In the Operator portal, click **Operator Profiles**. The **Operator Profiles** page displays the available profiles.



□	Name	Configuration Type	No. of Partners	Used By	Created
□	3.3.2 ⚠	Segment Based	1 Partner	3 Customers	Mon Mar 16, 17:12:55
□	5-site-Op	Segment Based	1 Partner	3 Customers	Mon Mar 16, 15:00:00
□	Initial Op rofile Operator profile to get started with	Network Based	0	0	Mon Mar 16, 14:53:45
□	Initial Segmented Operator Profile Segmented operator profile to get started with	Segment Based	0	1 Customer	Mon Mar 16, 14:53:45

Software version of this profile contains a deprecated software image

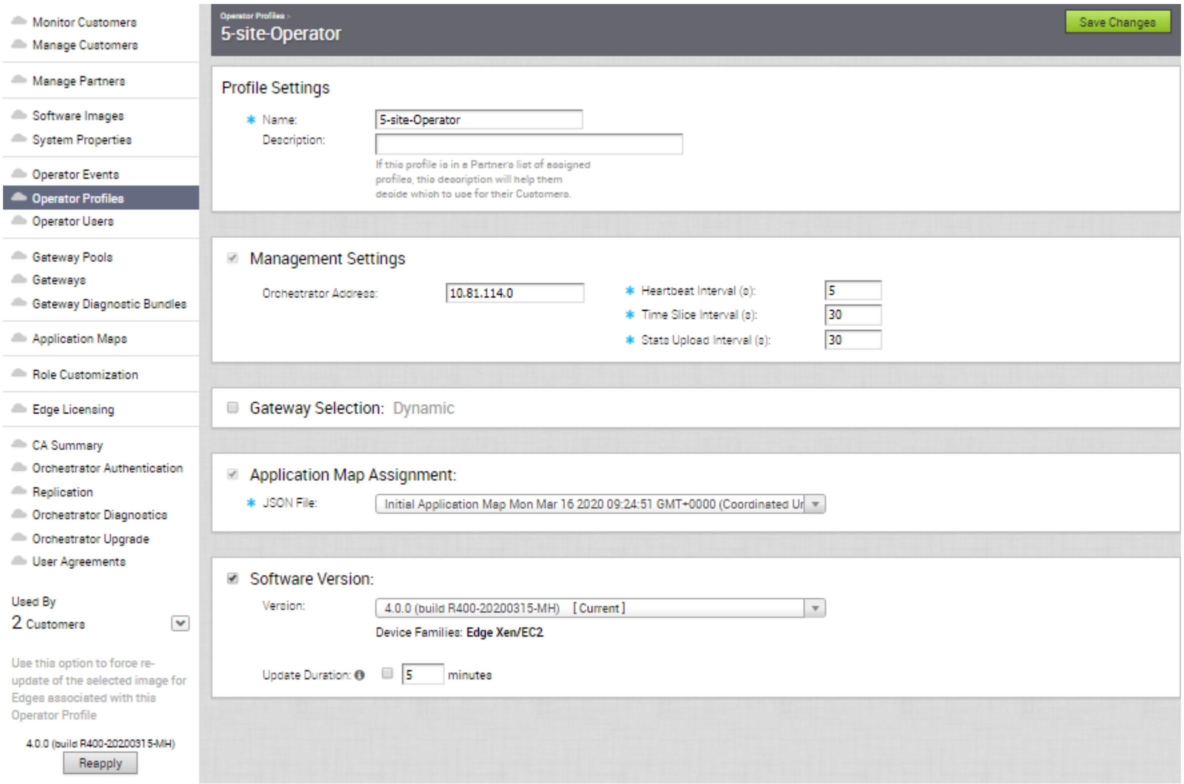
Note The Operator Profiles that contain a deprecated image is flagged to notify the user that the software version of the profile contains a deprecated software image.

As an Operator user, you can create a new Operator profile, duplicate an existing profile, modify or remove or delete a profile using the **Actions** button at the right-hand top corner of the **Operator Profiles** page as follows:

- **New Profile** – Creates a new Operator profile. See Create New Operator Profile.
- **Duplicate Profile** – Creates a copy of the selected Operator profile. See Duplicate Operator Profile.
- **Modify Profile** – Enables to update the network settings in the selected Operator Profile. See Modify Operator Profile.
- **Remove Profile** - Removes a selected Operator profile from all associated partners and customers.
- **Delete Profile** – Deletes the selected profiles.

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

To update the Operator Profile that has a deprecated image with another software image, click the link to that Operator Profile name. The selected Operator Profile page appears.



5-site-Operator

Profile Settings

* Name: 5-site-Operator

Description:

If this profile is in a Partner's list of assigned profiles, this description will help them decide which to use for their Customers.

☑ Management Settings

Orchestrator Address: 10.81.114.0

* Heartbeat Interval (s): 5

* Time Slice Interval (s): 30

* Stats Upload Interval (s): 30

□ Gateway Selection: Dynamic

☑ Application Map Assignment:

* JSON File: Initial Application Map Mon Mar 16 2020 09:24:51 GMT+0000 (Coordinated Ur

☑ Software Version:

Version: 4.0.0 (build R400-20200315-MH) [Current]

Device Families: **Edge Xen/EC2**

Update Duration: □ 5 minutes

Used By

2 Customers

Use this option to force re-update of the selected image for Edges associated with this Operator Profile

4.0.0 (build R400-20200315-MH)

Under **Software Version**, from the **Version** drop-down menu select the software image and click Save Changes.

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.

Click **Reapply** to force re-update of the selected software image for the edges associated with the selected Operator Profile.

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 Chapter 9 Manage Partners.

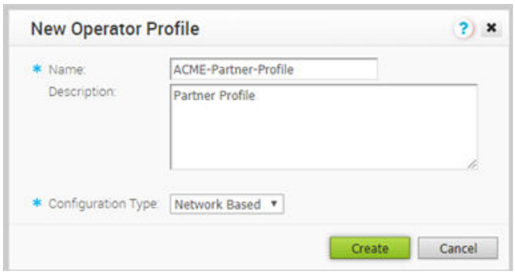
Create New Operator Profile

When you install SD-WAN Orchestrator, an initial Operator profile is available. If required, you can create additional profiles.

In the Operator portal, click **Operator Profiles**.

1 Click **New Profile** or click **Actions > New Profile**.

2 In the **New Operator Profile** window, enter the Name and Description, and choose the Configuration Type.



New Operator Profile

* Name: ACME-Partner-Profile

Description: Partner Profile

* Configuration Type: Network Based

3 Click **Create**.

The new profile appears in the **Operator Profiles** page.

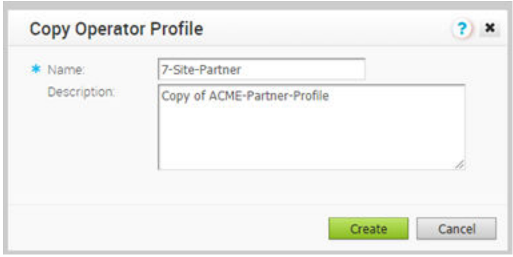
Duplicate Operator Profile

You can duplicate an Operator profile to create a copy of the profile.

In the Operator portal, click **Operator Profiles**.

1 Select the profile to be duplicated and click **Actions > Duplicate Profile**.

2 In the **Copy Operator Profile** window, update the Name and Description.



Copy Operator Profile

* Name: 7-Site-Partner

Description: Copy of ACME-Partner-Profile

3 Click **Create**.

A copy of the profile appears in the **Operator Profiles** page.

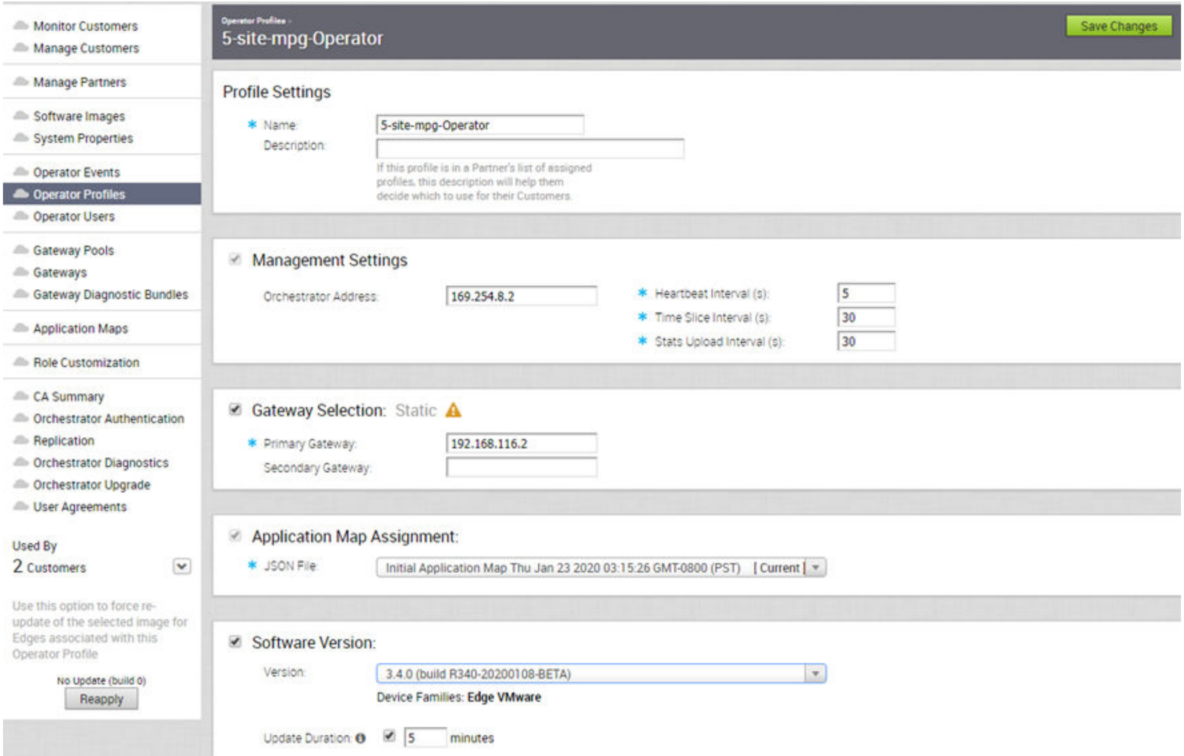
Modify Operator Profile

You can modify an Operator profile to update the profile settings.

In the Operator portal, click **Operator Profiles**.

Click the link to a profile, or select the profile and click **Actions > Modify Profile**.

The existing settings of the selected profile are displayed and you can configure the following:



Used By
2 Customers

Use this option to force re-update of the selected image for Edges associated with this Operator Profile

No Update (build 0)

5-site-mpg-Operator

Profile Settings

* Name: 5-site-mpg-Operator

Description:

If this profile is in a Partner's list of assigned profiles, this description will help them decide which to use for their Customers.

☑ Management Settings

Orchestrator Address: 169.254.8.2

* Heartbeat Interval (s): 5

* Time Slice Interval (s): 30

* Stats Upload Interval (s): 30

☑ Gateway Selection: Static ⚠

* Primary Gateway: 192.168.116.2

Secondary Gateway:

☑ Application Map Assignment:

* JSON File: Initial Application Map Thu Jan 23 2020 03:15:26 GMT-0800 (PST) [Current]

☑ Software Version:

Version: 3.4.0 (build R340-20200108-BETA)

Device Families: **Edge VMware**

Update Duration: ☑ 5 minutes

Profile Settings

If required, you can modify the Name and Description of the selected profile.

Management Settings

The IP address of the Orchestrator is displayed. You can configure the following management intervals:

- **Heartbeat Interval** – The time interval between the heartbeat messages sent from the Orchestrator to Edges. The default value is 30 seconds and minimum interval must be 10 seconds. If an Edge does not receive two heartbeats continuously, then the Edge is marked as Down.

  Note When you modify the heartbeat interval, make sure to update the Edge Offline Alert Notification Delay time accordingly, to avoid sending unnecessary alerts.

- **Timeslice Interval** – The time interval over which the monitoring data is collected for a flow.
- **Stats Upload Interval** – The time interval for uploading the monitoring data. All the data for each Timeslice are collected during the Stats Upload Interval and then uploaded.

Gateway Selection

By default, the Gateway selection is Dynamic and the Gateways are chosen dynamically from the Gateway pool. Ensure that the Gateway pool consists of at least two Gateways, for the Gateway selection to be efficient. For more information on Gateway Pools, see Gateway Pools.

Select the checkbox to make the Gateway selection as Static. For Static Gateway selection, you must specify the Primary Gateway. You can also enter an optional Secondary Gateway.

Note Use the Static Gateway Selection only for testing or debugging purposes. You must not use this option for Edge-to-Edge VPN or Partner handoff configurations.

Application Map Assignment

By default, the initial Application Map is assigned to the Operator Profile. You can choose a different Application Map available in the drop-down list. See Also Chapter 14 Application Maps.

Software Version

You can choose to push the latest Software Image to the Edges. By default, no updates are applied to the devices. Select the checkbox and choose the Software Image from the **Version** drop-down list. For more information on the Software Images, see Chapter 10 Software Images.

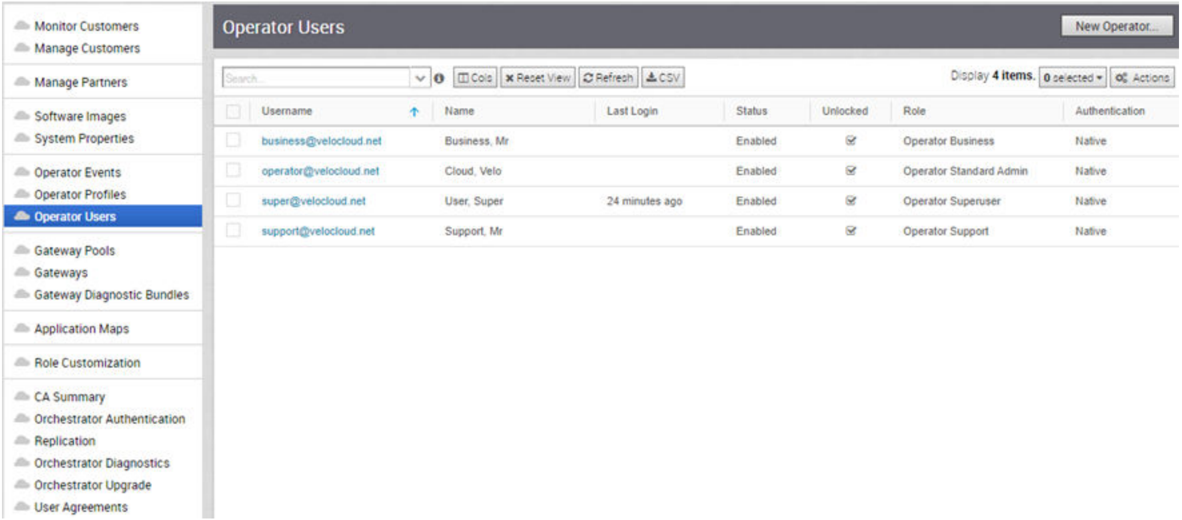
Select the **Update Duration** checkbox and enter the duration time in minutes. When you enable this option, the Orchestrator updates all the devices associated with the Enterprise customer within the specified time duration.

After updating the above settings, click **Save Changes**.

Manage Operator Users

The **Operator Users** page displays the existing Operator users. An Operator Super User can create new Operator users with different role privileges and configure API tokens for each Operator user.

In the Operator portal, click **Operator Users**, and you can configure the following.



□	Username	Name	Last Login	Status	Unlocked	Role	Authentication
□	business@velocloud.net	Business, Mr		Enabled	☑	Operator Business	Native
□	operator@velocloud.net	Cloud, Velo		Enabled	☑	Operator Standard Admin	Native
□	super@velocloud.net	User, Super	24 minutes ago	Enabled	☑	Operator Superuser	Native
□	support@velocloud.net	Support, Mr		Enabled	☑	Operator Support	Native

Click **Actions** to perform the following activities:

- **New Operator**: Creates new Operator users. See Create New Operator User.

- **Modify Operator**: Modifies the properties of the selected Operator user. You can also click the link to the username to modify the properties. See Configure Operator Users.
- **Password Reset**: Sends an Email to the selected user with a link to reset the password.
- **Delete Operator**: Deletes the selected users.

Create New Operator User

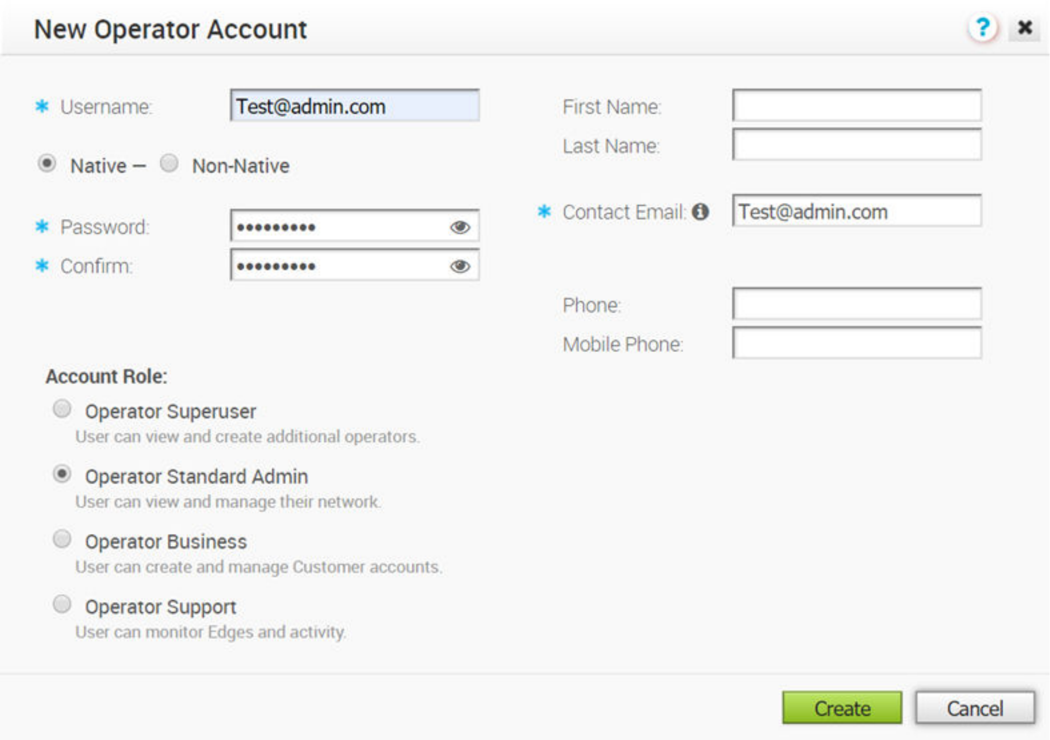
Operator Super Users can create new operator users.

In the Operator portal, click **Operator Users**.

Procedure

1 You can create new operator users by clicking either **New Operator**, or **Actions > New Operator** .

2 In the **New Operator Account** window, enter the following details:



New Operator Account

* Username: Test@admin.com

● Native – ○ Non-Native

* Password: •••••••••
* Confirm: •••••••••

First Name:
Last Name:
* Contact Email: Test@admin.com
Phone:
Mobile Phone:

Account Role:

○ Operator Superuser
User can view and create additional operators.

● Operator Standard Admin
User can view and manage their network.

○ Operator Business
User can create and manage Customer accounts.

○ Operator Support
User can monitor Edges and activity.

a Enter the user details like username, password, Name, Email, and Phone numbers.

b If you have chosen the authentication mode as Native in Chapter 17 Orchestrator Authentication, then the type of the user is selected as Native. If you have chosen a different authentication mode, you can choose the type of the user. If you choose the user to be Non-Native, the password option is not available, as it is inherited from the authentication mode.

c **Account Role**: Choose the user role from the available options.

3 Click **Create**.

Results

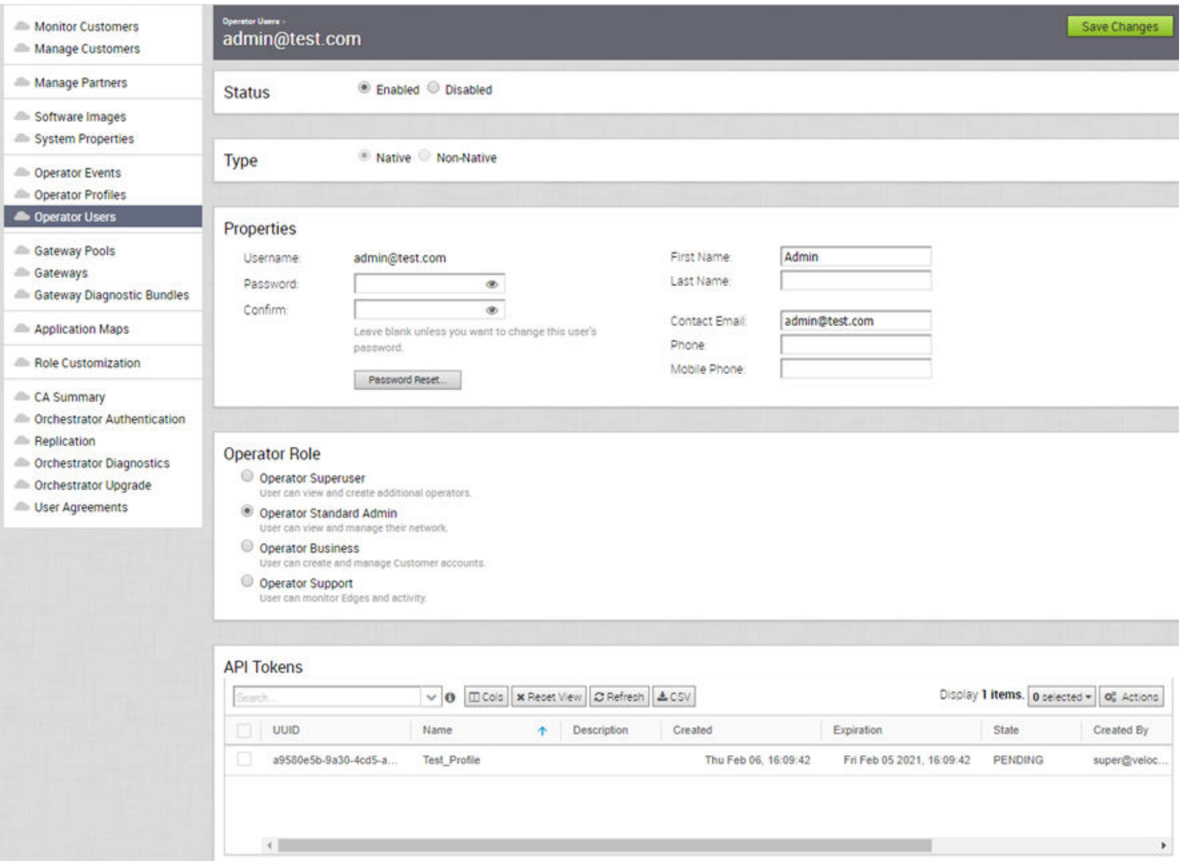
The user details are displayed in the **Operator Users** page.

Configure Operator Users

You can configure additional properties and create API tokens for an Operator user.

In the Operator portal, click **Operator Users**. To configure an Operator user, click the link to a username or select the user and click **Actions > Modify Operator**.

The existing properties of the selected user are displayed and if required, you can add or modify the following:



admin@test.com

Status ● Enabled ○ Disabled

Type ● Native ○ Non-Native

Properties

Username: admin@test.com
Password:
Confirm:
Leave blank unless you want to change this user's password.

First Name: Admin
Last Name:
Contact Email: admin@test.com
Phone:
Mobile Phone:

Operator Role

○ Operator Superuser
User can view and create additional operators.

● Operator Standard Admin
User can view and manage their network.

○ Operator Business
User can create and manage Customer accounts.

○ Operator Support
User can monitor Edges and activity.

API Tokens

Display **1 items.**

□	UUID	Name	Description	Created	Expiration	State	Created By
□	a9580e5b-9a30-4cd5-a...	Test_Profile		Thu Feb 06, 16:09:42	Fri Feb 05 2021, 16:09:42	PENDING	super@veloc...

Status

By default, the status is in **Enabled** state. If you choose **Disabled**, the user is logged out of all the active sessions.

Type

If you have chosen the Operator authentication mode as **Native** in Chapter 17 Orchestrator Authentication, then the type of the user is selected as **Native**. If you have chosen a different authentication mode, you can choose the type of the user. If you choose the user to be **Non-Native**, then you cannot reset the password or modify the user role.

Properties

The existing contact details of the user are displayed. If required, you can modify the details and choose to reset the password. If you click **Password Reset**, an email is sent to the user with a link to reset the password.

Role

The existing type of the user role is displayed. If required, you can choose a different role for the user. The role privileges change accordingly.

API Tokens

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

For Enterprise Read Only Users and MSP Business Specialist users, token-based authentication is not enabled.

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

Configure API Tokens:

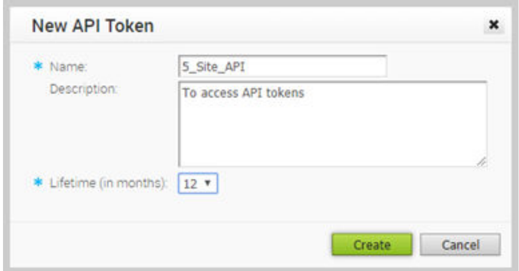
Any user can create tokens based on the privileges they have been assigned to their user roles, except the Enterprise Read-Only users and MSP Business Specialist users.

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

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

To manage the API tokens:

- In the **API Tokens** section, click **Actions > New API Token**, to create a new token.
- In the **New API Token** window, enter a **Name** and **Description** for the token, and choose the **Lifetime** from the drop-down menu.



New API Token

* Name: 5_Site_API

Description: To access API tokens

* Lifetime (in months): 12

- Click **Create** and the new token is displayed in the **API Tokens** grid.
- Initially, the status of the token is displayed as **Pending**. To download the token, select the token, and click **Actions > Download API Token**. The status changes to **Enabled**, which means that the API token can be used for API access.
- To disable a token, select the token and click **Actions > Revoke API Token**. The status of the token is displayed as **Revoked**.
- When the Lifetime of the token is over, the status changes to **Expired** state.

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 }}'
```

After modifying the settings and API Tokens, click **Save Changes**.

Manage Gateway Pools and Gateways

13

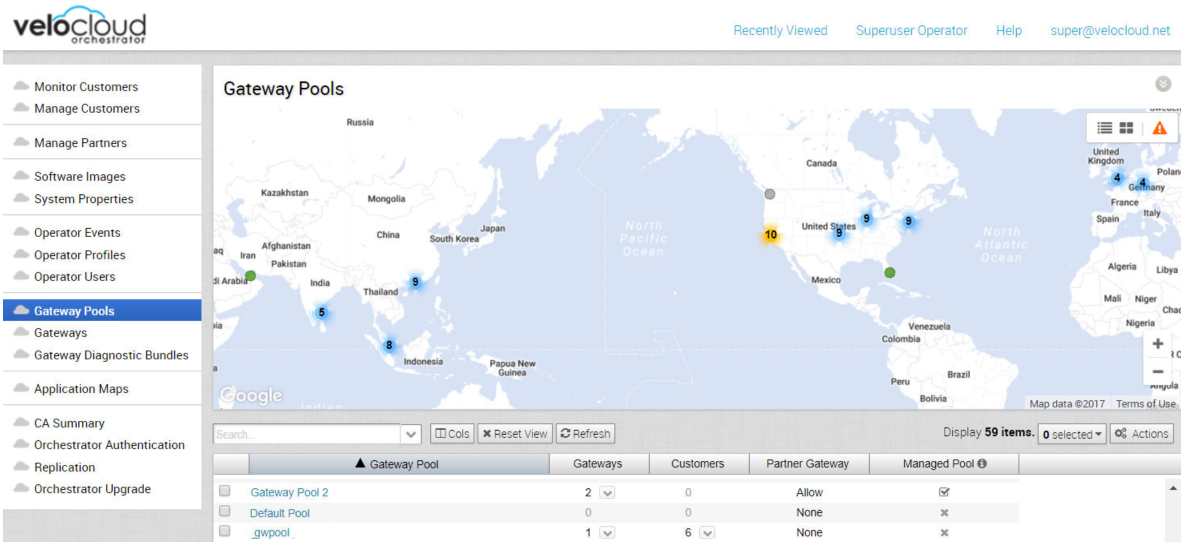
VMware network consists of multiple service Gateways deployed at top tier network and cloud data centers. The SD-WAN Gateway provides the advantage of cloud-delivered services and optimized paths to all applications, branches, and data centers. Service providers can also deploy their own Partner Gateways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

This chapter includes the following topics:

- Gateway Pools
- Partner Gateways
- Run Diagnostics for Gateways
- Monitor Gateways
- Monitor Gateways using new Orchestrator UI

Gateway Pools

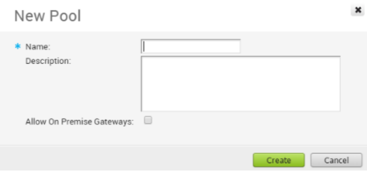
Gateways can be organized into pools that are then assigned to a network. An unpopulated default pool exists after a SD-WAN Orchestrator is installed. You can create additional Gateway Pools.



	▲ Gateway Pool	Gateways	Customers	Partner Gateway	Managed Pool
□	Gateway Pool 2	2	0	Allow	☑
□	Default Pool	0	0	None	✗
□	gwpool	1	6	None	✗

Create a Gateway Pool

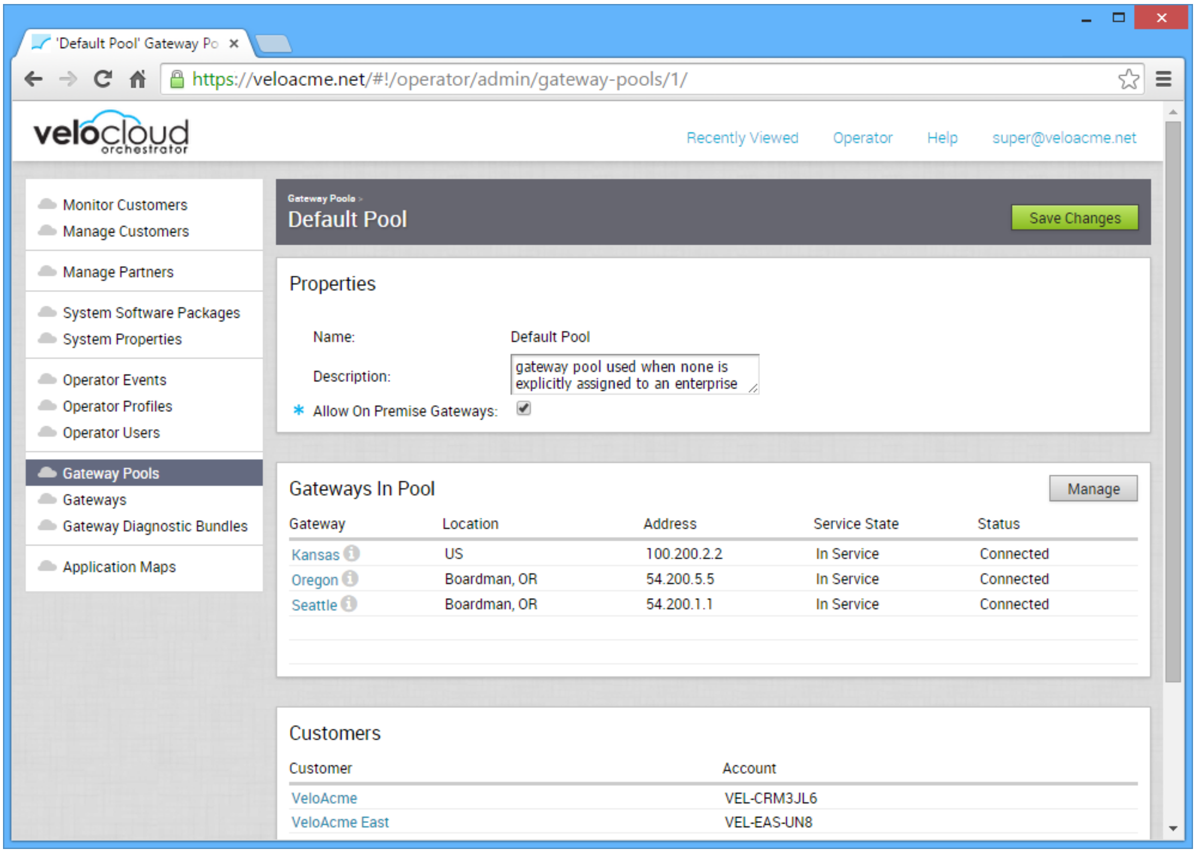
If you click **New Pool**, the following dialog box prompts you to enter a name for a new Gateway Pool. You can also specify whether Partner Gateways will be allowed in the new pool.



* Name:	
Description:	
Allow On Premise Gateways:	☐

If you click a Gateway Pool, the properties for the pool, the Gateways that are in the pool, and the Customers using the pool appear. Note that one of the properties is whether the pool allows On Premise Gateways to be part of the pool.

Note A VMware SD-WAN Gateway can function as a standard Gateway that provides VMware network services, or as a Partner Gateway that allows network traffic to be routed into a service provider's network. A Gateway cannot be used for both functions. A Gateway Pool can contain Gateways that are configured as Partner Gateways or standard Gateways. However, if a Partner Gateway is placed in a Gateway Pool where the **Allow Partner Gateways** option is unselected, the gateway will function as a standard Gateway.



Properties

Name:	Default Pool
Description:	gateway pool used when none is explicitly assigned to an enterprise
* Allow On Premise Gateways:	☑

Gateways In Pool

Gateway	Location	Address	Service State	Status
Kansas ⓘ	US	100.200.2.2	In Service	Connected
Oregon ⓘ	Boardman, OR	54.200.5.5	In Service	Connected
Seattle ⓘ	Boardman, OR	54.200.1.1	In Service	Connected

Customers

Customer	Account
VeloAcme	VEL-CRM3JL6
VeloAcme East	VEL-EAS-UN8

Creating Partner Specific Gateway Pools

This section describes how to create Gateways and Gateway Pools for a Partner. The Gateways and Gateway Pools you create will be used only by the Partner.

To creating a Gateway or Gateway Pool from the SD-WAN Orchestrator Partner Portal:

1 From the SD-WAN Orchestrator Navigation panel, click the **Manage Partners** link. The **Manage Partners** window appears.

2 In the **Manage Partners** window, click one of the available Partners displayed in the **Partner** column. The **Manage Partner Customers** window appears.

3 In the Navigation panel, click the **Gateway Pool** link to create a new Gateway Pool, or click the **Gateway** link to create a new Gateway.

4 In the **Actions** button (located above the table grid in the top, right corner), click **New Gateway Pool** (or **New Gateway** if you selected the **Gateway** link).

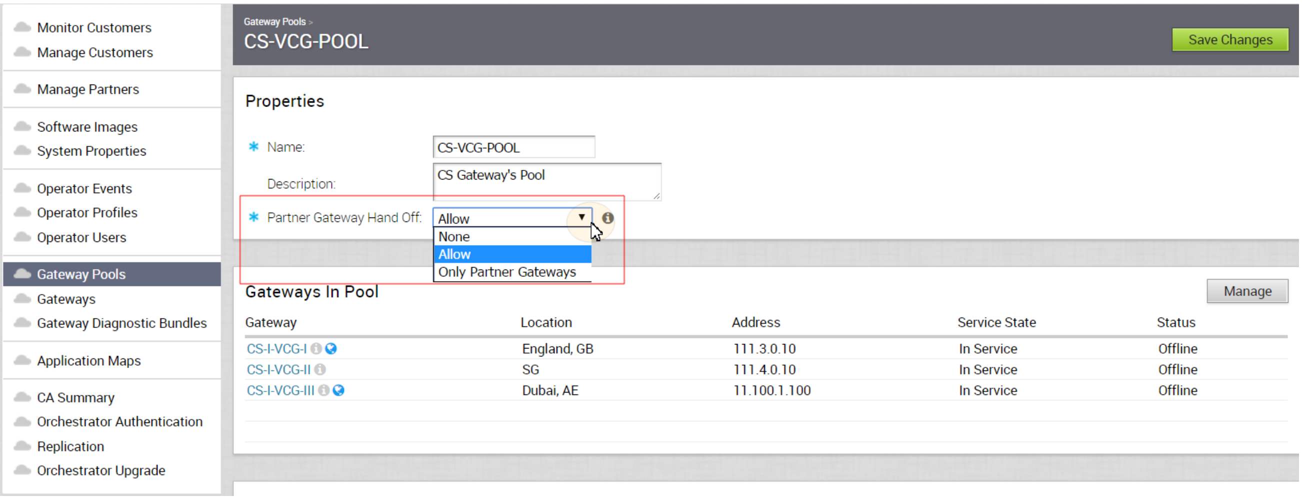
> **Note** In the above steps, you are creating Partner specific Gateways; therefore, any Gateways or Gateway Pools you create will only be associated with this Partner.

Delete a Gateway Pool

To delete partner-owned Gateways and Gateway Pools, Operators must delete the Gateways from the Partner Portal. In addition, if the Gateway is in use by a Partner, the Operator will not be able to delete it. The Operator must wait until the Gateway is available before they can delete it.

Partner Gateway Hand Off

This section describes the **Partner Gateway Hand Off** drop-down menu



Gateway Pools >

CS-VCG-POOL

Properties

* Name: CS-VCG-POOL

Description: CS Gateway's Pool

* Partner Gateway Hand Off: Allow

Gateways In Pool

Gateway	Location	Address	Service State	Status
CS-I-VCG-I	England, GB	111.3.0.10	In Service	Offline
CS-I-VCG-II	SG	111.4.0.10	In Service	Offline
CS-I-VCG-III	Dubai, AE	11.100.1.100	In Service	Offline

The Gateway Pools **Properties** area displays the **Name** text box, **Description** text box, and a **Partner Gateway Hand Off** drop-down menu.

The **Partner Gateway Hand Off** drop-down menu includes the following three options:

Option	Description
None	Use when Enterprises assigned to this Gateway Pool do not require Partner Gateway Hand Offs.
Allow	Use when the pool should support mix of Partner Gateway and Cloud Gateways.
Only Partner Gateways	Use when Edges in the Enterprises should NOT be assigned cloud Gateways from the pool, and will only be assigned Gateway 1 and Gateway 2 that are set for the individual Edge.

If you click a specific Gateway, additional details about the Gateway are displayed. The details include properties, Contact and Location information, which customers are using the Gateway, and any pools of which the Gateway is a member.

Partner Gateways

A Gateway can be configured as a Partner Gateway and can function as a Partner Gateway if it is part of a Gateway Pool that allows Partner Gateways.

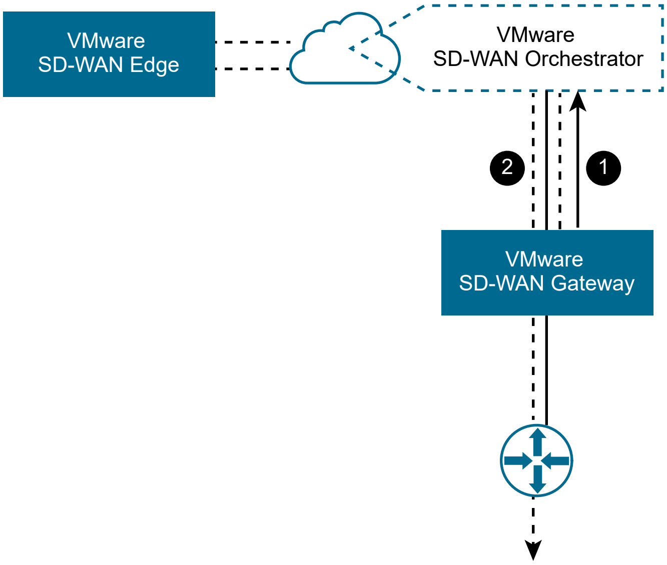
Overview of Partner Gateways

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

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

Gateway Configuration Use Case #1

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

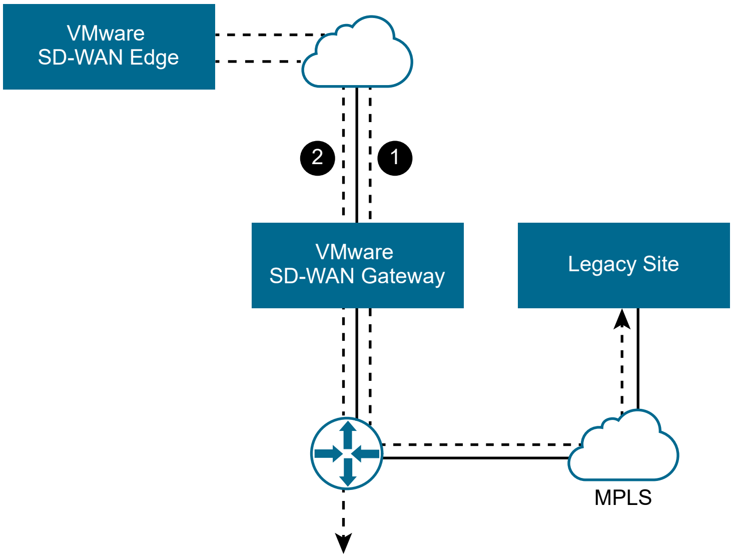


- #1 - SD-WAN Orchestrator traffic is routed using IP addresses to NAT.
- #2 - Corporate Traffic is routed through subnets to VLAN/VRF.

Gateway Configuration Use Case #2

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

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

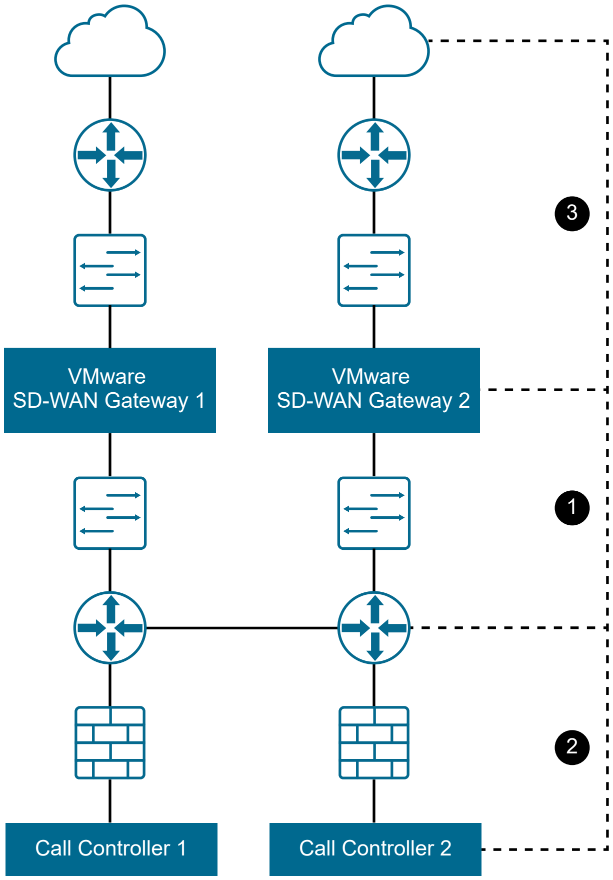


- #1 - Subnet (e.g. 10.0.0.0/8) defined for Legacy Sites and marked for encryption. Traffic is transmitted between SD-WAN Edge and SD-WAN Gateway over the IPsec tunnel.
- #2 - Remaining traffic is sent unencrypted to the SD-WAN Edge, and then to its final destination.

Partner Gateway Resiliency

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

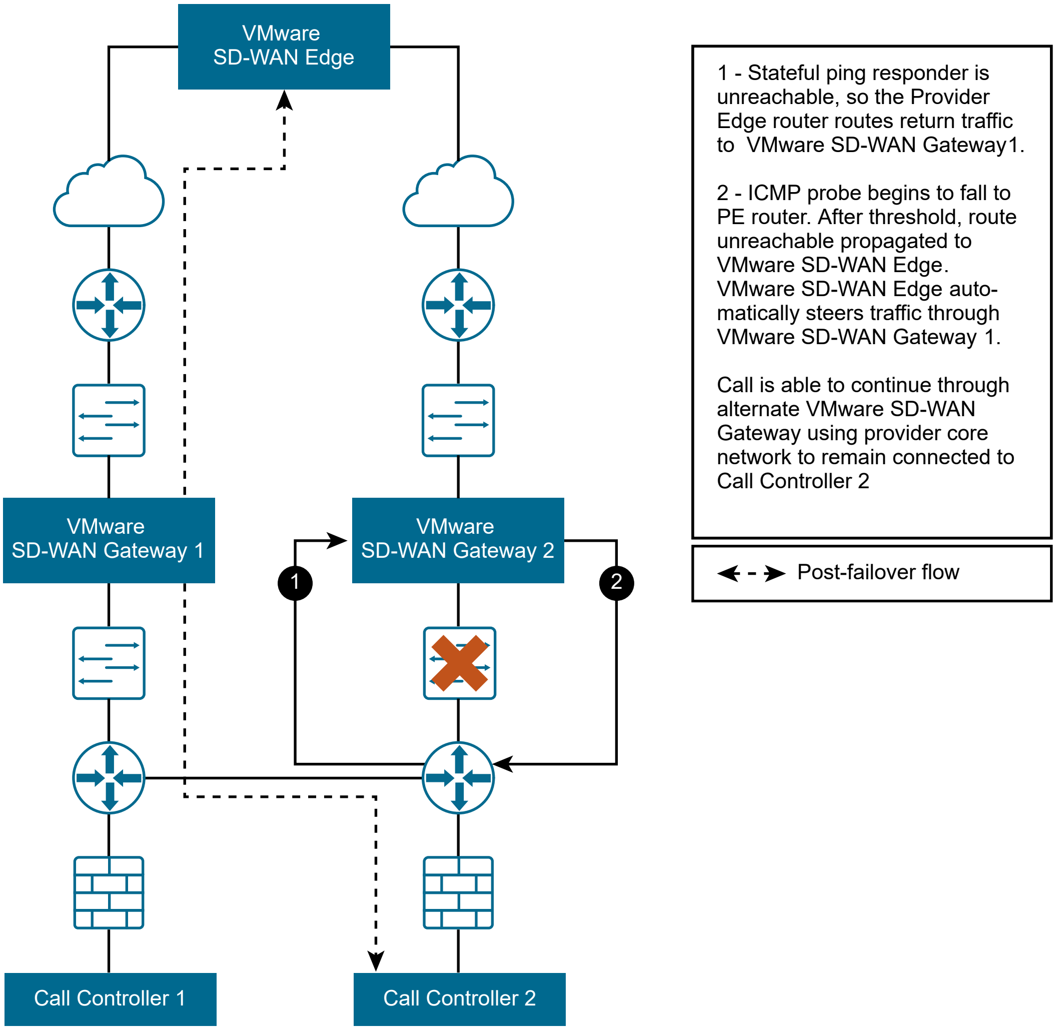
Consider the following Gateway topology:



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 SD-WAN Gateway, or from the SD-WAN Gateway to the Provider Edge router.
2	Call Controller	The SD-WAN Gateway should be able to ping the Provider Edge router or Call Controller to verify connectivity.
3	WAN	The SD-WAN Gateway should have a stateful ping responder that responds only if the WAN zone is available.

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



1 - Stateful ping responder is unreachable, so the Provider Edge router routes return traffic to VMware SD-WAN Gateway1.

2 - ICMP probe begins to fall to PE router. After threshold, route unreachable propagated to VMware SD-WAN Edge. VMware SD-WAN Edge automatically steers traffic through VMware SD-WAN Gateway 1.

Call is able to continue through alternate VMware SD-WAN Gateway using provider core network to remain connected to Call Controller 2

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

ICMP Failover Probes

This section describes ICMP failover probes.

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

Example Scenario

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

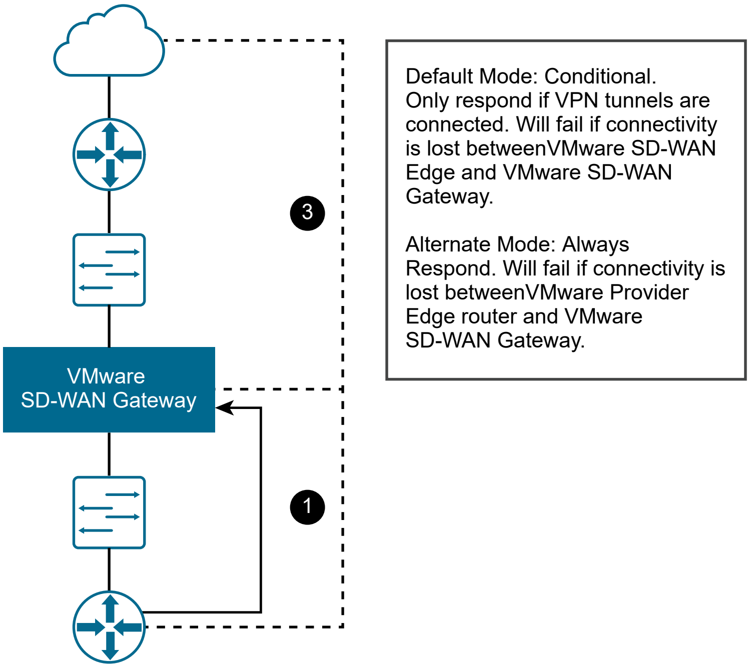
1. VMware SD-WAN Edges connect to the primary SD-WAN Gateway. The primary SD-WAN Gateway marks routes as reachable.
2. The Primary SD-WAN Gateway fails to receive a reply for three successive probes (~6 seconds).
3. The Primary SD-WAN Gateway marks routes as unreachable and communicates this to all connected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

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

Stateful Ping Responder

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

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



Default Mode: Conditional.
Only respond if VPN tunnels are connected. Will fail if connectivity is lost betweenVMware SD-WAN Edge and VMware SD-WAN Gateway.

Alternate Mode: Always Respond. Will fail if connectivity is lost betweenVMware Provider Edge router and VMware SD-WAN Gateway.

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

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

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

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

Caveats When Using NAT Hand-off Mode

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

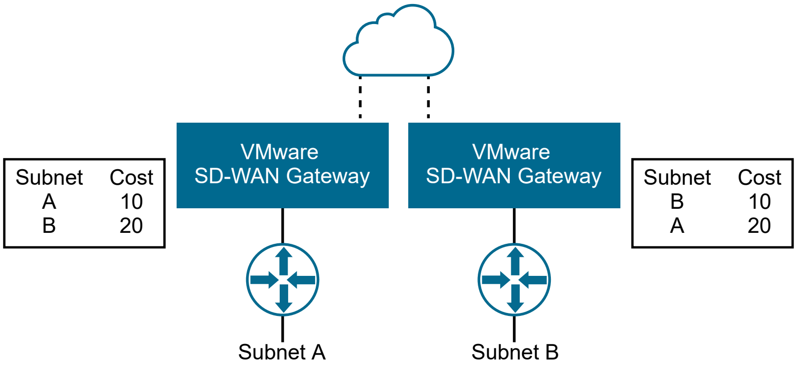
- For VLAN hand-off mode, the Partner Gateway can listen on any IP if it is reachable to the PE router (including its interface IP). For NAT hand-off mode, the Partner Gateway will not respond if the ICMP request comes to its own interface (WAN) IP address.
- Reverse flow is not supported in the NAT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

Active/Backup Subnets

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

Subnets on a Partner Gateway

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



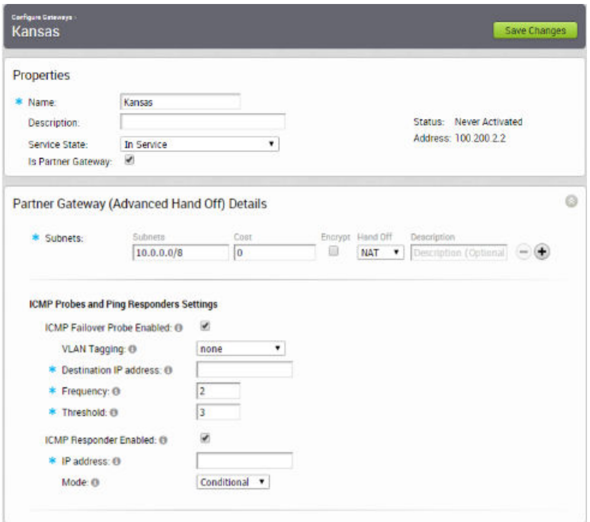
Subnet	Cost
A	10
B	20

Subnet	Cost
B	10
A	20

Partner Gateway Configuration and Use

If the **Is Partner Gateway** option is selected for a Gateway, additional configuration is required:

1 Select the Gateway that will be a Partner Gateway, then select the **Is Partner Gateway** check box. A **Partner Gateway (Advanced Hand Off) Details** section appears for the Gateway.



Configure Gateways >

Kansas

Properties

* Name: Kansas
Description:
Service State: In Service
Is Partner Gateway: ☑

Status: Never Activated
Address: 100.200.2.2

Partner Gateway (Advanced Hand Off) Details

* Subnets:

Subnets	Cost	Encrypt	Hand Off	Description
10.0.0.0/8	0	□	NAT	Description (Optional)

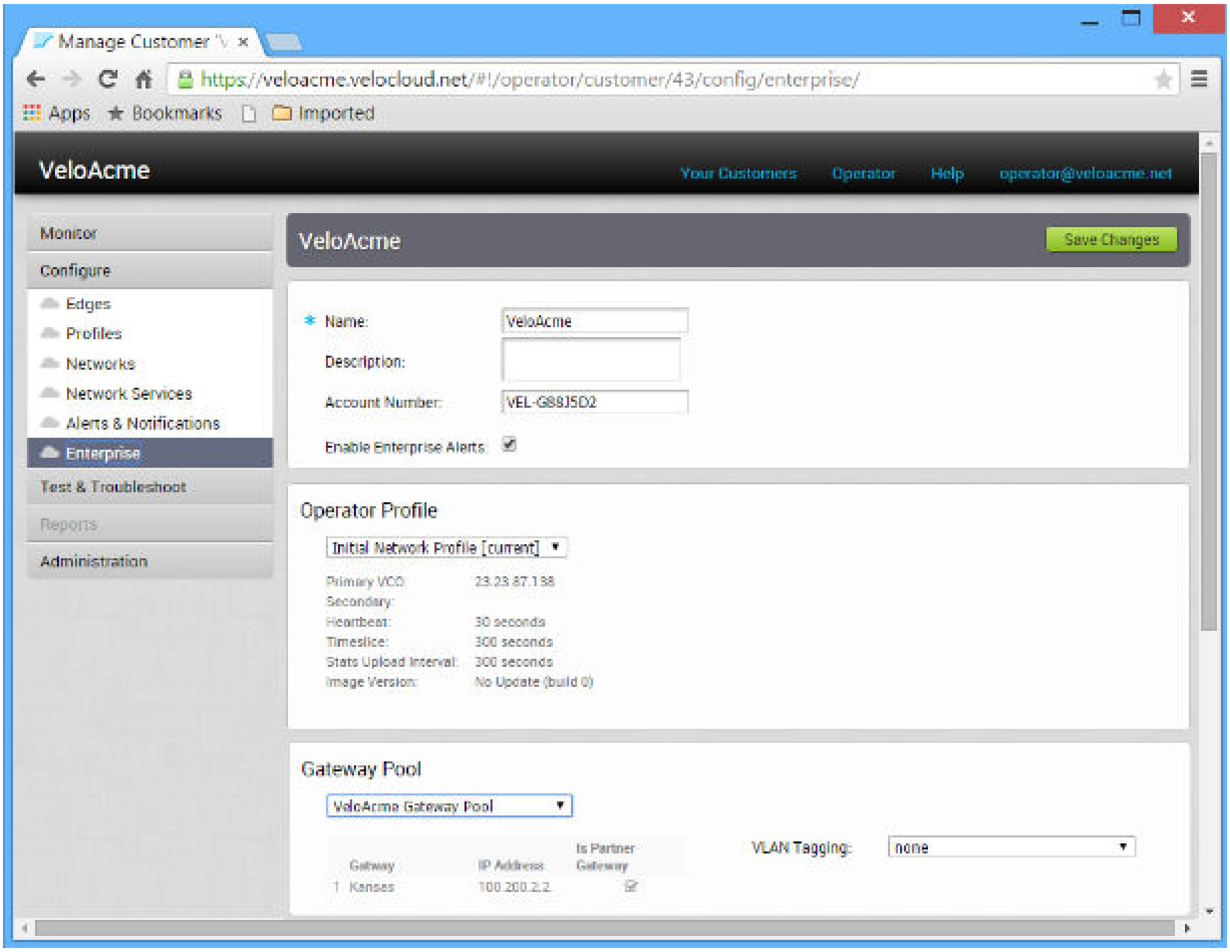
ICMP Probes and Ping Responders Settings

ICMP Failover Probe Enabled: ☑
VLAN Tagging: none
* Destination IP address:
* Frequency: 2
* Threshold: 3

ICMP Responder Enabled: ☑
* IP address:
Mode: Conditional

In this section, you can configure one or more Subnets that will forward traffic to the Partner Gateway. For each subnet, you can select a **Hand Off** type (VLAN or NAT) and whether the traffic will be encrypted or not. ICMP Probes and Ping Responders settings and contact and location information for the Gateway can also be entered.

2 For each Customer that uses Partner Gateways, select a Gateway Pool that contains the Partner Gateway by selecting a customer, then choosing **Configure -> Enterprise**.



* Name: VeloAcme

Description:

Account Number: VEL-G88J5D2

Enable Enterprise Alerts: ☑

Operator Profile

Initial Network Profile [current]

Primary VCO: 23.23.87.138
Secondary:
Heartbeat: 30 seconds
Timeslice: 300 seconds
Stats Upload Interval: 300 seconds
Image Version: No Update (build 0)

Gateway Pool

VeloAcme Gateway Pool

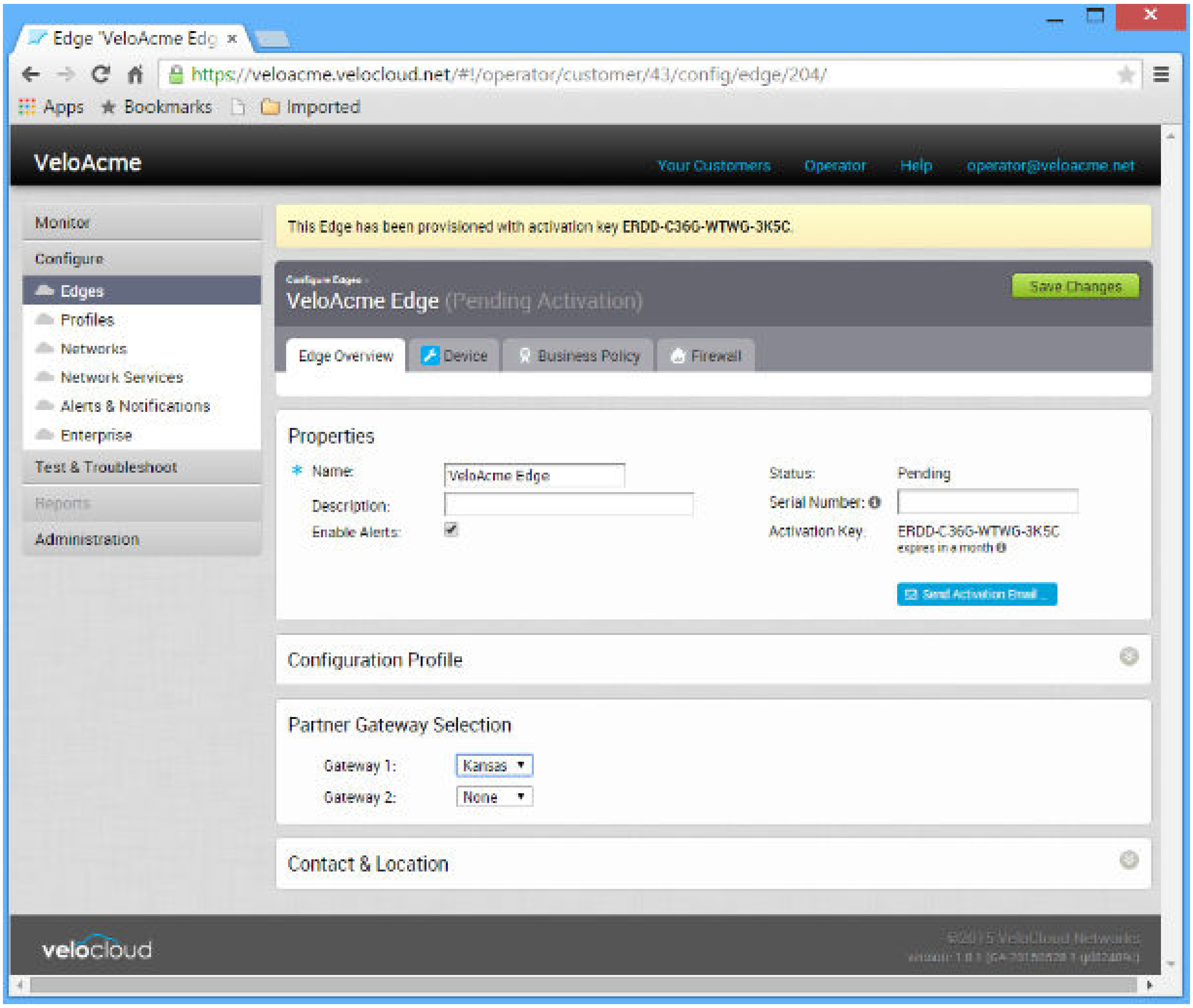
VLAN Tagging: none

	Gatway	IP Address	Is Partner Gateway
1	Kansas	100.200.2.2	☑

You can also choose VLAN tagging for the pool.

3 If you want to make the Partner Gateway VRF-aware and enable BGP, then go to **Configure > Customer** in the **Gateway Pool** screen. See Configure Gateway BGP for more configuration details.

4 For each Customer Edge that uses a Partner Gateway, configure the Partner Gateway Selection to choose **Gateways**. First, choose a customer, then select **Configure -> Edges ->** select **Edge**.



This Edge has been provisioned with activation key ERDD-C36G-WTWG-3K5C.

VeloAcme Edge (Pending Activation)

Properties

* Name: VeloAcme Edge

Description:

Enable Alerts: ☑

Status: Pending

Serial Number:

Activation Key: ERDD-C36G-WTWG-3K5C
expires in a month

Configuration Profile

Partner Gateway Selection

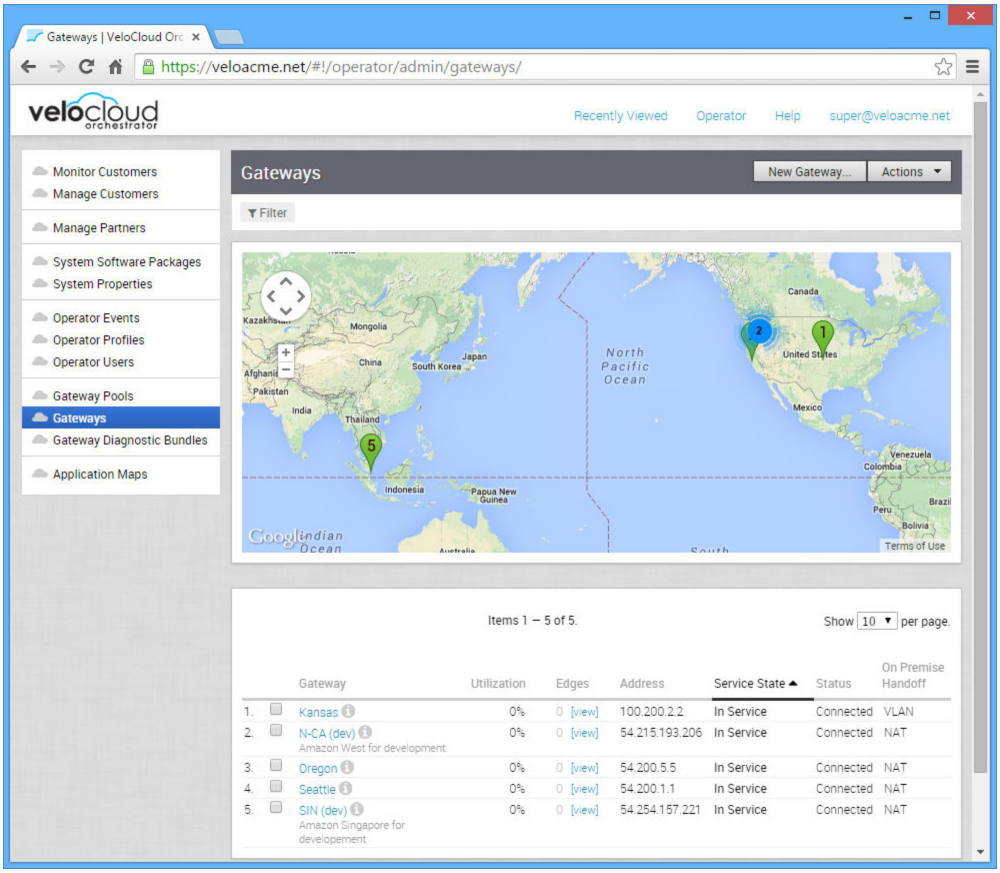
Gateway 1: Kansas

Gateway 2: None

Contact & Location

Gateways Page

If you click the **Gateways** link, all gateways managed by the SD-WAN Orchestrator are displayed as a list with details about the gateways and as a location on a map. Click a Gateway to display Gateway details.



Items 1 – 5 of 5.

Show 10 ▾ per page.

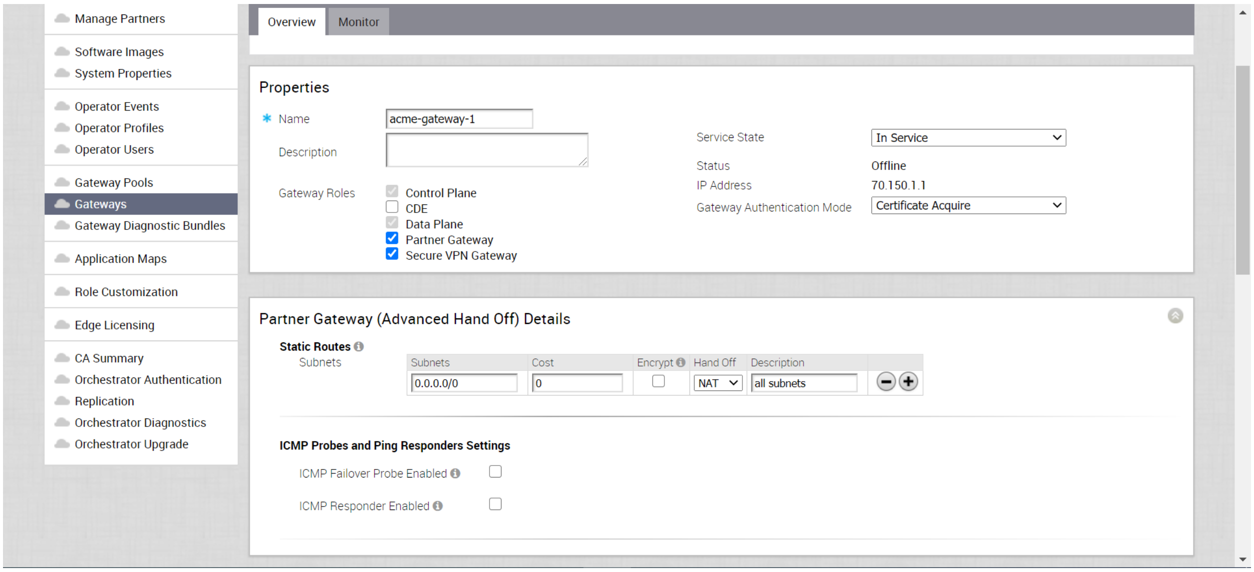
		Gateway	Utilization	Edges	Address	Service State ▲	Status	On Premise Handoff
1.	□	Kansas	0%	0 [view]	100.200.2.2	In Service	Connected	VLAN
2.	□	N-CA (dev) Amazon West for development	0%	0 [view]	54.215.193.206	In Service	Connected	NAT
3.	□	Oregon	0%	0 [view]	54.200.5.5	In Service	Connected	NAT
4.	□	Seattle	0%	0 [view]	54.200.1.1	In Service	Connected	NAT
5.	□	SIN (dev) Amazon Singapore for developement	0%	0 [view]	54.254.157.221	In Service	Connected	NAT

Enable Partner Gateway Mode

In the same **Gateway** page (**Operator > Gateways**), enable the Partner Gateway mode by selecting the **Partner Gateway** checkbox. Unselect the **Secure VPN Gateway** checkbox (which is needed only if you plan to use this SD-WAN Gateway to establish an IPSec tunnel to a Non VMware SD-WAN Site).

Overview Tab

The **Gateways** screen includes the following sections: Properties, Partner Gateway (Advanced Handoff) Details, Contact & Location, Customer Usage, Pool Membership. See the sections for information about these sections.



Properties

* Name: acme-gateway-1

Description:

Gateway Roles: ☑ Control Plane, □ CDE, ☑ Data Plane, ☑ Partner Gateway, ☑ Secure VPN Gateway

Service State: In Service

Status: Offline

IP Address: 70.150.1.1

Gateway Authentication Mode: Certificate Acquire

Partner Gateway (Advanced Hand Off) Details

Static Routes

Subnets

Subnets	Cost	Encrypt	Hand Off	Description
0.0.0.0/0	0	□	NAT	all subnets

ICMP Probes and Ping Responders Settings

ICMP Failover Probe Enabled □

ICMP Responder Enabled □

Properties Area

In addition to the Name and Description text boxes, the **Properties** area includes the following options:

- Service State:
- Status:
- IP Address
- Gateway Authentication Mode:
  - **Certificate Disabled** : 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 SD-WAN Orchestrator, by generating a key pair and sending a certificate signing request to the Orchestrator. Once acquired, the Edge uses the certificate for authentication to the SD-WAN Orchestrator and for establishment of VCMP tunnels.

    Note After acquiring the certificate, the option can be updated to **Certificate Required**.
  - **Certificate Required**: Edge uses the PKI certificate. (Operators can change the certificate renewal time window for Gateways via system properties. See Table 11-3. Certificate Authority for more information).
- Gateway Roles:
  - Control Plane:
  - CDE:
  - Data Plane:
  - Partner Gateway:

- Secure VPN Gateway:

Partner Gateway (Advanced Handoff) Details Area

- Static Routes: Specify the subnets or routes that the SD-WAN Gateway should advertise to the SD-WAN Edge, along with the handoff mode and whether or not to encrypt the traffic. This is global per SD-WAN Gateway and applies to ALL customers. With BGP, this section is typically used only if there is a shared subnet that all customers need to access and if NAT handoff is required.

  Remove the unused subnets from the Static Route list above if you do not have any subnets that you need to advertise to the SD-WAN Edge and have the handoff of type NAT.

  The ICMP probe parameters are optional and recommended only if you want to use ICMP to check the health of the SD-WAN Gateway. With BGP support on the Partner Gateway, using ICMP probe for failover and route convergence is no longer required.
- ICMP Failover Probe: The SD-WAN Gateway can use ICMP probe to check for the reachability of a particular IP. It can notify the SD-WAN Edge to failover to the secondary Gateway if the SD-WAN Gateway detects that the particular IP is not reachable.
- ICMP Responder Enabled: This will allow the SD-WAN Gateway to respond to the ICMP probe from the next hop router when its tunnels are up.
- Mode=Conditional: The SD-WAN Gateway will respond to the ICMP request only when its service is up and when at least one tunnel is up.
- Mode=Always: The SD-WAN Gateway will always respond to the ICMP request from its peer.

Configure Gateway BGP

This section describes Gateway BGP configuration.

Configure BGP

This section describes how to configure BGP on Partner Gateways. By default, BGP is enabled on Partner Gateways.

For information on BGP for SD-WAN Edge, refer to *Configure Dynamic Routing with OSPF or BGP* in the Admin Guide.

Note We support 4-Byte ASN BGP:

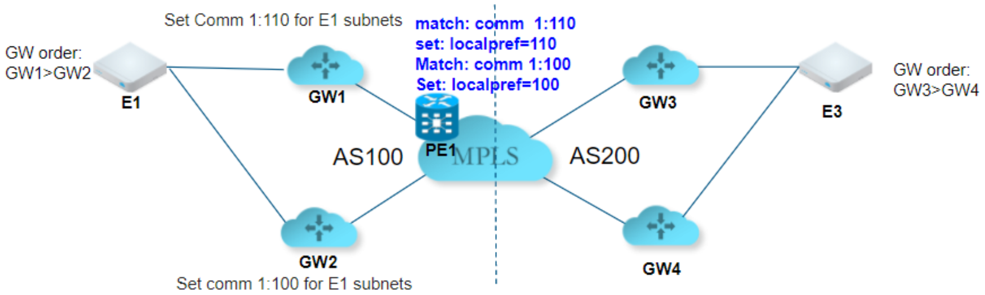
- As the ASN of the SD-WAN Edge itself
- Peer to a neighbor with 4-Byte ASN
- Accept 4-Byte ASNs in route advertisements

Customer BGP Priority (Auto Community)

The **Customer BGP Priority** area includes the **Enable Community Mapping** checkbox. When checked, two mapping modes are available to configure communities, **All Segments** and **Per Segment**. There are two parts to the community: **Community** and **Community 2**.

For SPs who deploy a customer across multiple BGP AS and prefer to use BGP community values to control path symmetry, there is an option for them to assign BGP community values automatically to the branch prefixes based on the Partner Gateway preference orders for that branch. By default, VMware automatically assigns BGP MED values for the branch prefix to influence the BGP path and achieve path symmetry, which applies to a single AS scenario.

The following topology gives an example of this use case.



In the above topology, multiple MPLS BGP ASs, BGP community values, and local preference values are used on PEs to achieve path symmetry. For branch E1, the Partner Gateway order is GW1>GW2, which means that for the outbound traffic, GW1 is preferred. To keep path symmetry, GW1 needs to assign a community value of 1:110 to match the configured PE BGP route-map, so the return path will also prefer GW1.

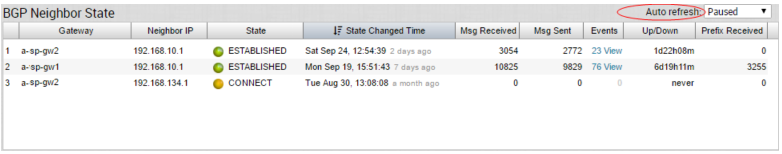
Similarly, GW2 needs to assign a community value of 1:00 to match the configured PE BGP route-map, which will make it less preferred. This will be automated via the Auto-community feature (introduced in 2.5). By giving community values to GW priorities, the Partner Gateways will assign corresponding community values to the branch prefixes dynamically. This configuration is at the customer level.

Monitoring

To view configured Gateways:

1 Go to **Monitor > Network Services**.

2 In the **Network Services** screen, scroll down to the **BGP Neighbor State** area to view your configured Gateways.



BGP Neighbor State

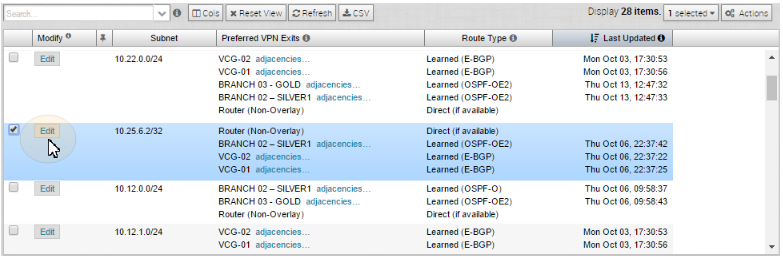
Auto refresh: Paused ▾

	Gateway	Neighbor IP	State	State Changed Time	Msg Received	Msg Sent	Events	Up/Down	Prefix Received
1	a-sp-gw2	192.168.10.1	● ESTABLISHED	Sat Sep 24, 12:54:39 2 days ago	3054	2772	23 View	1d22h08m	0
2	a-sp-gw1	192.168.10.1	● ESTABLISHED	Mon Sep 19, 15:51:43 7 days ago	10825	9829	76 View	6d19h11m	3255
3	a-sp-gw2	192.168.134.1	● CONNECT	Tue Aug 30, 13:08:08 a month ago	0	0	0	never	0

Note In the **Auto refresh** drop-down menu, you can designate how often the **BGP Neighbor State** area auto refreshes (5, 30, 60 seconds), or you can stop the **Auto Refresh** feature by choosing **Paused** from the drop-down menu.

Overlay Flow Control

All routes are displayed in the **Overlay Flow Control** table. You can change the Preferred VPN Exits order for a particular Subnet by clicking the **Edit** button in the **Modify** column.



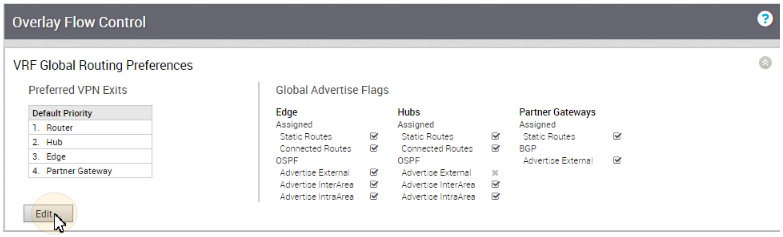
	Modify		Subnet	Preferred VPN Exits	Route Type	Last Updated
□	Edit		10.22.0.0/24	VCG-02 adjacencies... VCG-01 adjacencies... BRANCH 03 - GOLD adjacencies... BRANCH 02 – SILVER1 adjacencies... Router (Non-Overlay)	Learned (E-BGP) Learned (E-BGP) Learned (OSPF-OE2) Learned (OSPF-OE2) Direct (if available)	Mon Oct 03, 17:30:53 Mon Oct 03, 17:30:56 Thu Oct 13, 12:47:32 Thu Oct 13, 12:47:33
☑	Edit		10.25.6.2/32	Router (Non-Overlay) BRANCH 02 – SILVER1 adjacencies... VCG-02 adjacencies... VCG-01 adjacencies...	Direct (if available) Learned (OSPF-OE2) Learned (E-BGP) Learned (E-BGP)	 Thu Oct 06, 22:37:42 Thu Oct 06, 22:37:22 Thu Oct 06, 22:37:25
□	Edit		10.12.0.0/24	BRANCH 02 – SILVER1 adjacencies... BRANCH 03 - GOLD adjacencies... Router (Non-Overlay)	Learned (OSPF-O) Learned (OSPF-OE2) Direct (if available)	Thu Oct 06, 09:58:37 Thu Oct 06, 09:58:43
□	Edit		10.12.1.0/24	VCG-02 adjacencies... VCG-01 adjacencies...	Learned (E-BGP) Learned (E-BGP)	Mon Oct 03, 17:30:53 Mon Oct 03, 17:30:56

Column Name	Description
Modify	Access to edit the Global Configs.
Subnet	The network that this route corresponds to, along with a list of Edges that learned this route.
Route Type	Types include: BGP, OSPF-O, OSPF-OE2, Static, and Connected.
Preferred VPN Exits	The order of the VPN exit.
Last Updated	The date and time the routes are learned.

Edit Global Configs

To edit Global Configs:

1 Click the **Edit** button at the bottom of the VRF **Global Routing Preferences** area to open the **Edit Global Configs** dialog box.



Overlay Flow Control

VRF Global Routing Preferences

Preferred VPN Exits

Default Priority
1. Router
2. Hub
3. Edge
4. Partner Gateway

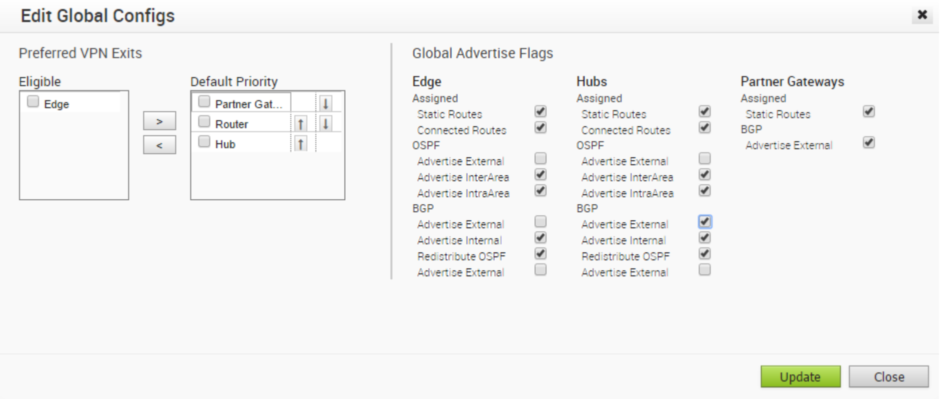
Global Advertise Flags

Edge
Assigned
Static Routes ☑
Connected Routes ☑
OSPF
Advertise External ☑
Advertise InterArea ☑
Advertise IntraArea ☑

Hubs
Assigned
Static Routes ☑
Connected Routes ☑
OSPF
Advertise External ☒
Advertise InterArea ☑
Advertise IntraArea ☑

Partner Gateways
Assigned
Static Routes ☑
BGP
Advertise External ☑

2 In the **Edit Global Configs** dialog box, edit the **Global Advertise Flags** area.



Preferred VPN Exits

Eligible
- □ Edge

Default Priority
- □ Partner Gat...
- □ Router
- □ Hub

Global Advertise Flags

Edge
Assigned
Static Routes ☑
Connected Routes ☑
OSPF
Advertise External □
Advertise InterArea ☑
Advertise IntraArea ☑
BGP
Advertise External □
Advertise Internal ☑
Redistribute OSPF ☑
Advertise External □

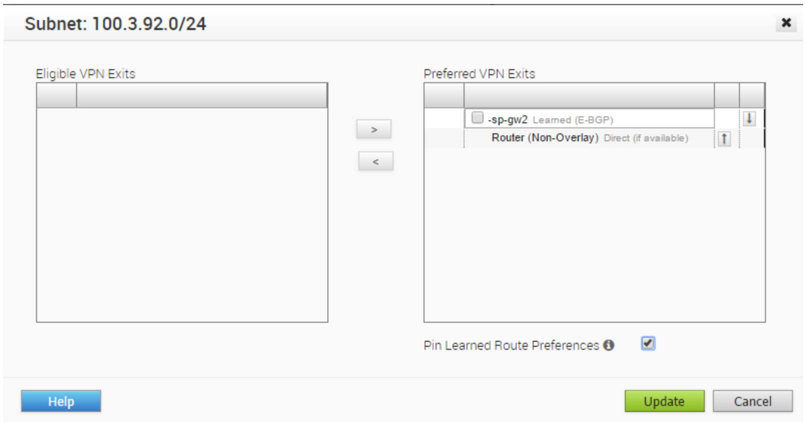
Hubs
Assigned
Static Routes ☑
Connected Routes ☑
OSPF
Advertise External □
Advertise InterArea ☑
Advertise IntraArea ☑
BGP
Advertise External ☑
Advertise Internal ☑
Redistribute OSPF ☑
Advertise External □

Partner Gateways
Assigned
Static Routes ☑
BGP
Advertise External ☑

Edit Subnet

As an additional option, you can change the order of the VPN exit by editing the Subnet.

To access this dialog, click the **Edit** link in the **Modify** column on the **Overlay Control** table.



Subnet: 100.3.92.0/24

Eligible VPN Exits

Preferred VPN Exits
- □ -sp-gw2 Learned (E-BGP)
- Router (Non-Overlay) Direct (if available)

Pin Learned Route Preferences ☑

Run Diagnostics for Gateways

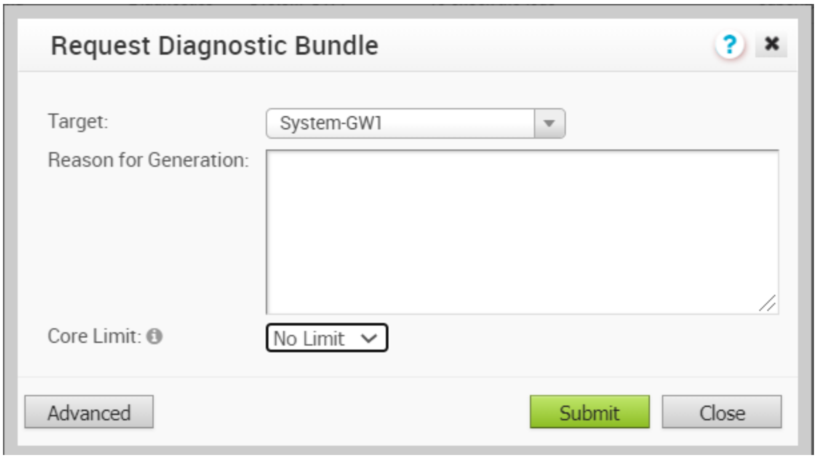
Diagnostic bundles allow users to collect all the configuration files and log files from a specific VMware SD-WAN Gateway into a consolidated zipped file. The data available in the diagnostic bundles can be used by the VMware Support Engineers for troubleshooting the SD-WAN Gateways.

In the Operator portal, click **Gateway Diagnostic Bundles**.

To generate a Diagnostic bundle:

1 Click **Request Diagnostic Bundle**.

2 In the **Request Diagnostic Bundle** window, configure the following:



Target: System-GW1

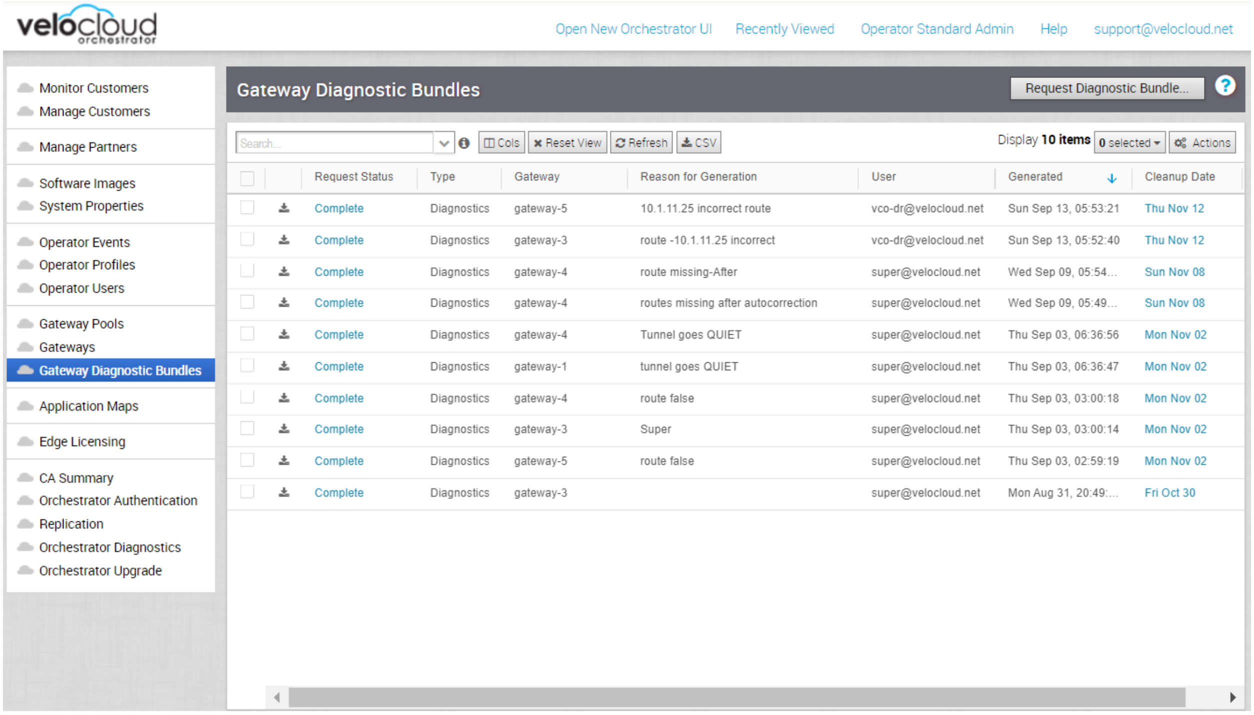
Reason for Generation:

Core Limit: No Limit

- **Target** – Select the target VMware SD-WAN Gateway from the drop-down list. The data is collected from the selected VMware SD-WAN Gateway.
- **Reason for Generation** – Optionally, you can enter your reason for generating the bundle.
- If required, click the **Advanced** button and choose a value from the **Core Limit** drop-down list. The Core Limit is used to reduce the size of the uploaded bundle when the Internet connectivity is experiencing issues.

3 Click **Submit**.

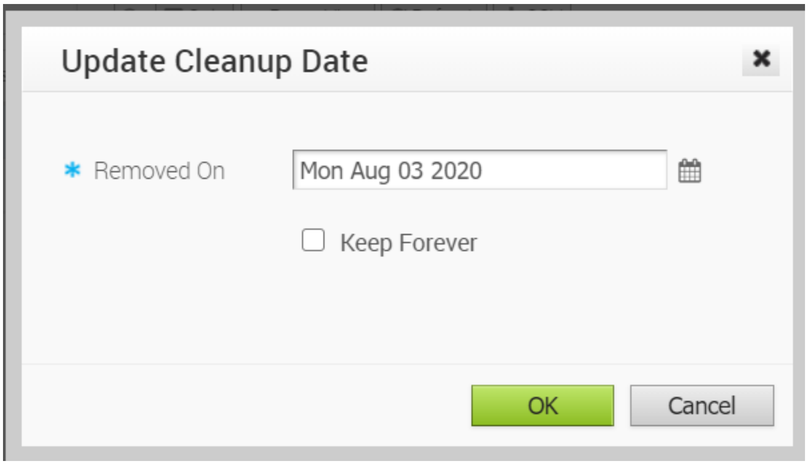
The **Gateway Diagnostic Bundles** window displays the details of the bundles generated, along with the status.



Request Status	Type	Gateway	Reason for Generation	User	Generated	Cleanup Date
Complete	Diagnostics	gateway-5	10.1.11.25 incorrect route	vco-dr@velocloud.net	Sun Sep 13, 05:53:21	Thu Nov 12
Complete	Diagnostics	gateway-3	route -10.1.11.25 incorrect	vco-dr@velocloud.net	Sun Sep 13, 05:52:40	Thu Nov 12
Complete	Diagnostics	gateway-4	route missing-After	super@velocloud.net	Wed Sep 09, 05:54...	Sun Nov 08
Complete	Diagnostics	gateway-4	routes missing after autocorrection	super@velocloud.net	Wed Sep 09, 05:49...	Sun Nov 08
Complete	Diagnostics	gateway-4	Tunnel goes QUIET	super@velocloud.net	Thu Sep 03, 06:36:56	Mon Nov 02
Complete	Diagnostics	gateway-1	tunnel goes QUIET	super@velocloud.net	Thu Sep 03, 06:36:47	Mon Nov 02
Complete	Diagnostics	gateway-4	route false	super@velocloud.net	Thu Sep 03, 03:00:18	Mon Nov 02
Complete	Diagnostics	gateway-3	Super	super@velocloud.net	Thu Sep 03, 03:00:14	Mon Nov 02
Complete	Diagnostics	gateway-5	route false	super@velocloud.net	Thu Sep 03, 02:59:19	Mon Nov 02
Complete	Diagnostics	gateway-3		super@velocloud.net	Mon Aug 31, 20:49:...	Fri Oct 30

To download a generated bundle, click the **Complete** link or select the bundle and click **Actions > Download Diagnostic Bundle**. The bundle is downloaded as a ZIP file.

The completed bundles get deleted automatically on the date displayed in the **Cleanup Date** column. You can click the link to the Cleanup Date to modify the Date.



In the **Update Cleanup Date** window, 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 **Actions > Delete**.

Monitor Gateways

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

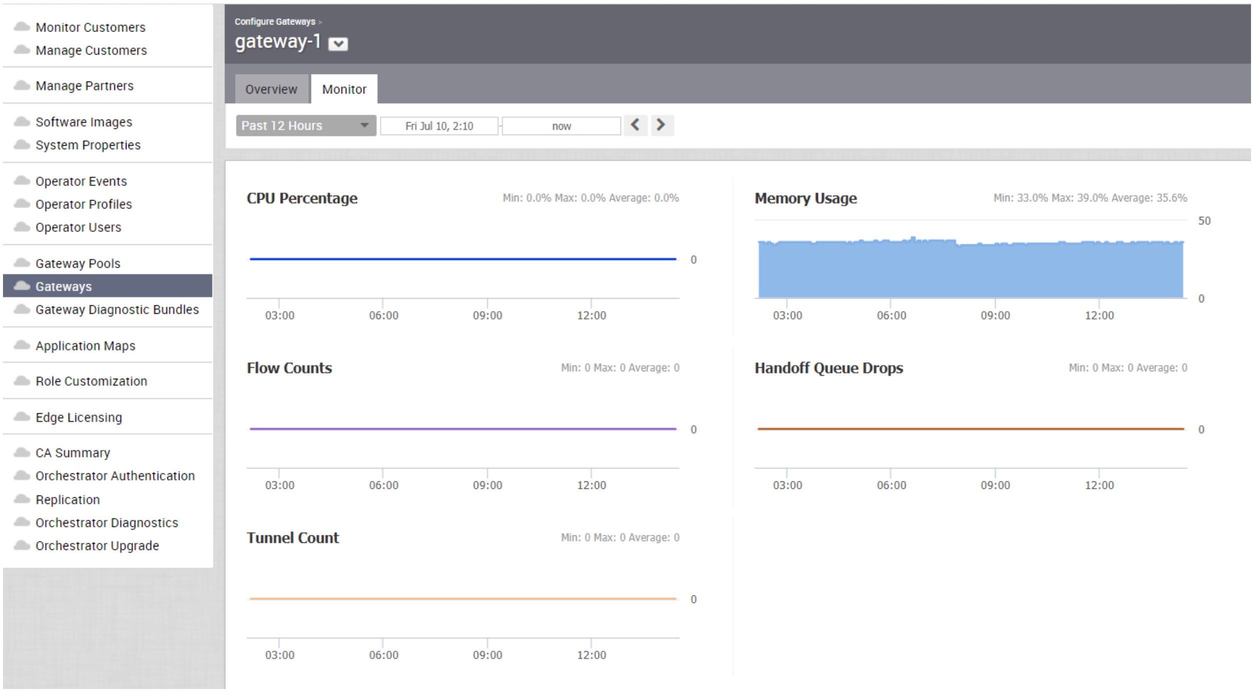
To monitor the Gateways:

Procedure

1. In the Operator portal, click **Gateways**.
2. The **Gateways** page displays the list of available Gateways.
3. Click the link to a Gateway. The details of the selected Gateway are displayed.
4. Click the **Monitor** tab to view the usage data of the selected Gateway.

Results

The **Monitor** tab of the selected Gateway displays the following details:



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.
- **Handoff Queue Drops** – Count of packets dropped due to queued handoff.
- **Tunnel Count** – Count of tunnel sessions.

Hover the mouse on the graphs to view more details.

You can also view the details using the new Orchestrator UI. See Monitor Gateways using new Orchestrator UI.

Monitor Gateways using new Orchestrator UI

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

To monitor the Gateways:

Procedure

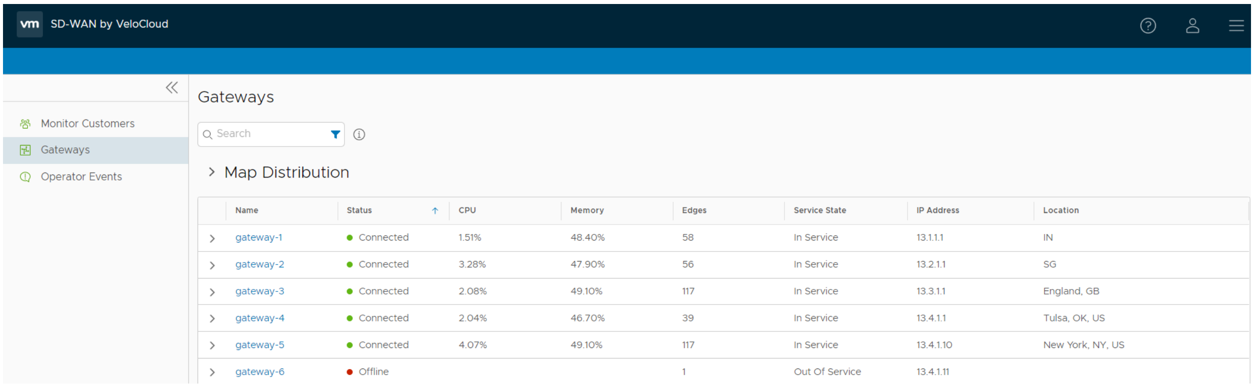
1 In the Operator portal, click the **Open New Orchestrator UI** option available at the top of the Window.

2 Click **Launch New Orchestrator UI** in the pop-up window. The UI opens in a new tab displaying the monitoring options.

3 Click **Gateways** .

Results

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



Gateways

	Name	Status	CPU	Memory	Edges	Service State	IP Address	Location
›	gateway-1	● Connected	1.51%	48.40%	58	In Service	13.1.1.1	IN
›	gateway-2	● Connected	3.28%	47.90%	56	In Service	13.2.1.1	SG
›	gateway-3	● Connected	2.08%	49.10%	117	In Service	13.3.1.1	England, GB
›	gateway-4	● Connected	2.04%	46.70%	39	In Service	13.4.1.1	Tulsa, OK, US
›	gateway-5	● Connected	4.07%	49.10%	117	In Service	13.4.1.10	New York, NY, US
›	gateway-6	● Offline			1	Out Of Service	13.4.1.11	

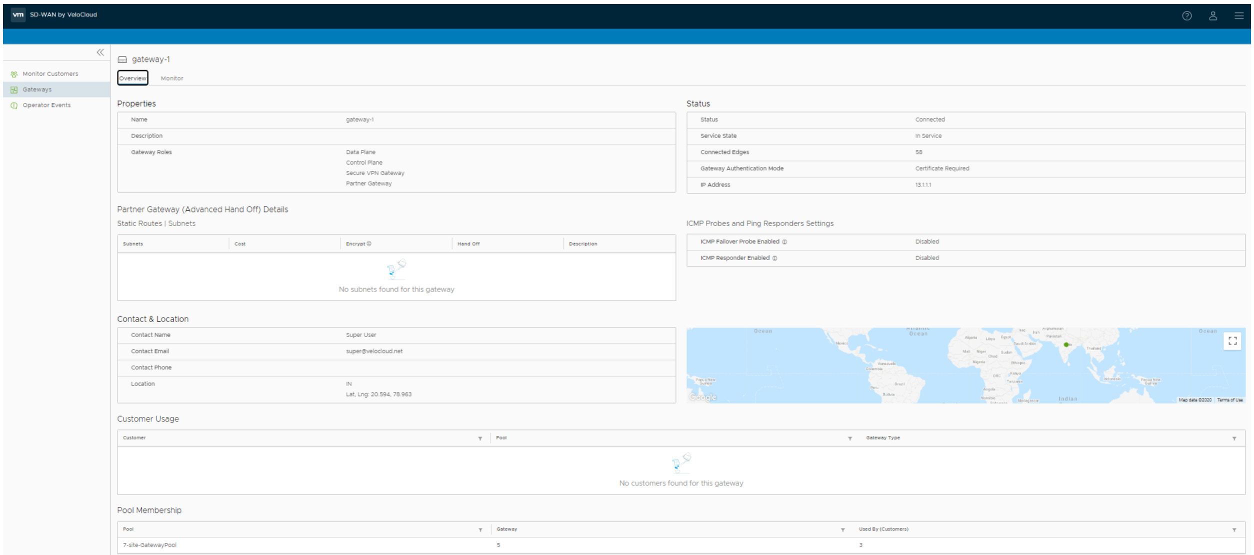
Click **Map Distribution** to expand and view the locations of the Gateways in the Map. By default, this view is collapsed.

You can also click the arrows prior to each Gateway name to view more details.

The page displays the following details:

- **Name** – Name of the Gateway.
- **Status** – Current status of the Gateway. The status may be one of the following: Connected, Degraded, Disabled, Never Activated, Offline, Out of Service, or Quiesced.
- **CPU** – Percentage of CPU utilization by the Gateway.
- **Memory** – Percentage of memory utilization by the Gateway.
- **Edges** – Number of Edges connected to the Gateway.
- **Service State** – Service state of the Gateway. 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 Gateway.
- **Location** – Location of the Gateway.

Click the link to a Gateway to view the details of the selected Gateway.



gateway-1

Properties

Name	gateway-1
Description	
Gateway Roles	Data Plane Control Plane Secure VPN Gateway Partner Gateway

Status

Status	Connected
Service State	In Service
Connected Edges	58
Gateway Authentication Mode	Certificate Required
IP Address	13.1.1.1

Partner Gateway (Advanced Hand Off) Details

Static Routes | Subnets

Subnets	Cost	Encrypt ⓘ	Hand Off	Description

No subnets found for this gateway

ICMP Probes and Ping Responders Settings

ICMP Failover Probe Enabled ⓘ	Disabled
ICMP Responder Enabled ⓘ	Disabled

Contact & Location

Contact Name	Super User
Contact Email	super@velocloud.net
Contact Phone	
Location	IN Lat, Lng: 20.594, 78.963

Customer Usage

Customer	Pool	Gateway Type

No customers found for this gateway

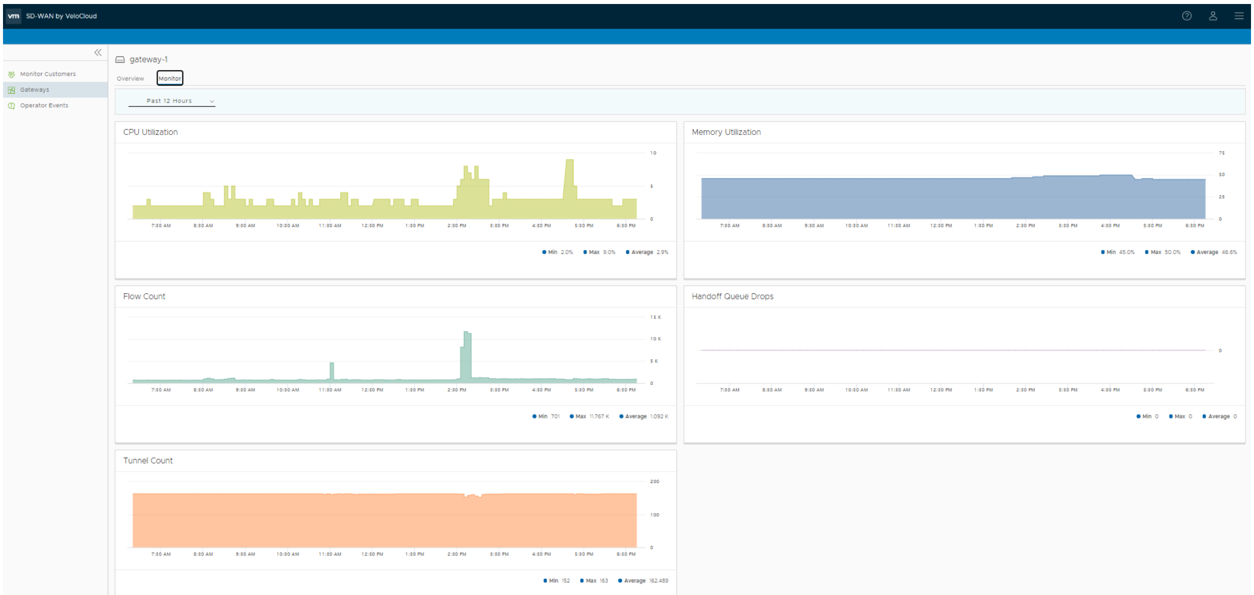
Pool Membership

Pool	Gateway	Used By (Customers)
7-site-GatewayPool	5	3

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

Note You can only view the Gateway details, using this tab. To configure the Gateway information, navigate to the **Gateways** page in the Operator portal.

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



gateway-1

Past 12 Hours

CPU Utilization: ● Min 2.0% ● Max 9.0% ● Average 2.9%

Memory Utilization: ● Min 45.0% ● Max 50.0% ● Average 46.6%

Flow Count: ● Min 701 ● Max 11.767 K ● Average 1.092 K

Handoff Queue Drops: ● Min 0 ● Max 0 ● Average 0

Tunnel Count: ● Min 152 ● Max 163 ● Average 162.489

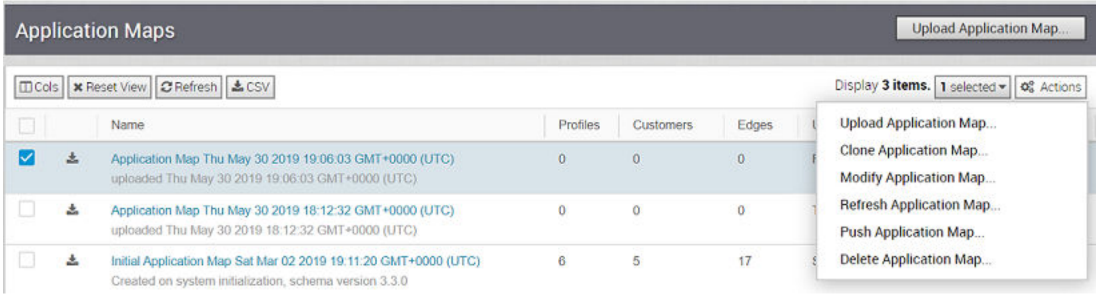
For more information on the data displayed, see Monitor Gateways.

Application Maps

14

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

In the Operator panel, click **Application Maps > Actions** to perform the following activities.


Application Maps
Upload Application Map...
Cols
Reset View
Refresh
CSV
Display 3 items.
1 selected
Actions
Upload Application Map...
Clone Application Map...
Modify Application Map...
Refresh Application Map...
Push Application Map...
Delete Application Map...

		Name	Profiles	Customers	Edges
☑		Application Map Thu May 30 2019 19:06:03 GMT+0000 (UTC) uploaded Thu May 30 2019 19:06:03 GMT+0000 (UTC)	0	0	0
□		Application Map Thu May 30 2019 18:12:32 GMT+0000 (UTC) uploaded Thu May 30 2019 18:12:32 GMT+0000 (UTC)	0	0	0
□		Initial Application Map Sat Mar 02 2019 19:11:20 GMT+0000 (UTC) Created on system initialization, schema version 3.3.0	6	5	17

- **Upload Application Map** – Allows to upload the JSON file with the applications and definitions. See Upload Application Map.
- **Clone Application Map** – Creates a new Application Map by cloning an existing Application Map file. See Clone Application Map.
- **Modify Application Map** – Allows to add or update the application details available in the selected Application Map. See Modify Application Map.
- **Refresh Application Map** – Updates the Application definitions listed in the selected Application Maps. See Refresh Application Map.
- **Push Application Map** – Pushes the latest updates of the Application definitions available in the Application Maps to the associated SD-WAN Edges. See Push Application Map.
- **Delete Application Map** – Deletes the selected Application Maps. You cannot delete a map that has been assigned to an Operator profile.

This chapter includes the following topics:

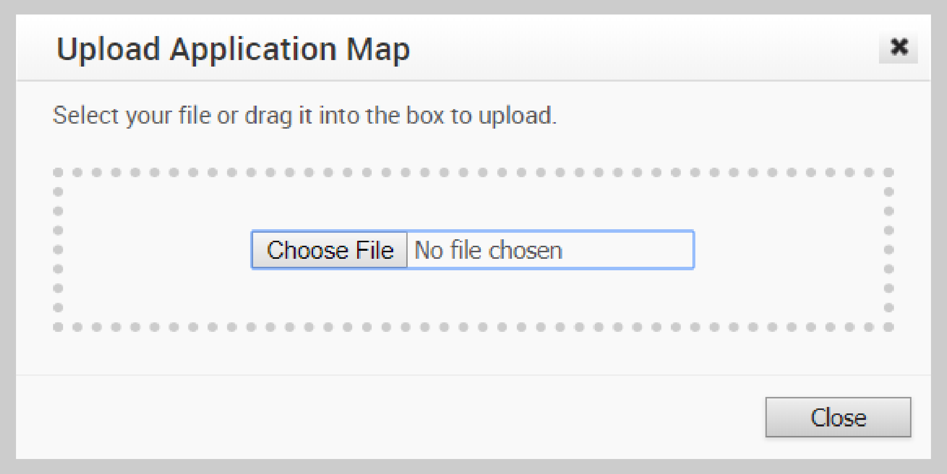
Upload Application Map

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

In the Operator portal, click **Application Maps**.

1 To upload a map file, either click **Upload Application Map** or **Actions > Upload Application Map**.

2 In the **Upload Application Map** window, choose the Application Map file.



Upload Application Map

Select your file or drag it into the box to upload.

After validating the contents, the file is uploaded.

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
        }
```

You can view the uploaded files in the **Application Maps** window and if required, you can download the file.

To assign an Application Map to an Operator Profile, see Manage Operator Profiles.

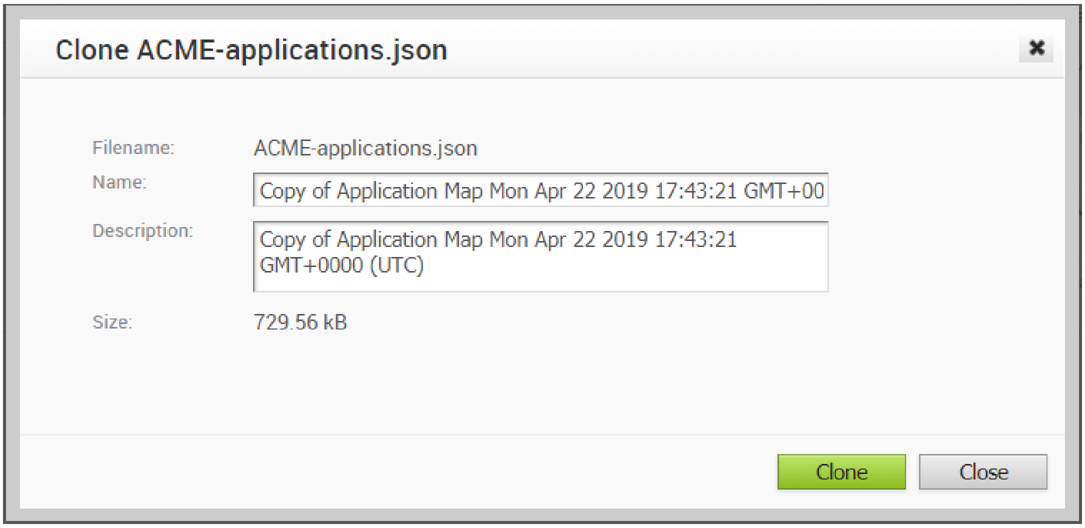
Clone Application Map

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

In the Operator portal, click **Application Maps**.

1 Select the Application Map to be cloned and click **Actions > Clone Application Map**.

2 In the **Clone Application Map** window, enter a new name and description for the Application Map.



Clone ACME-applications.json

Filename: ACME-applications.json

Name: Copy of Application Map Mon Apr 22 2019 17:43:21 GMT+00

Description: Copy of Application Map Mon Apr 22 2019 17:43:21 GMT+0000 (UTC)

Size: 729.56 kB

3 Click **Clone**.

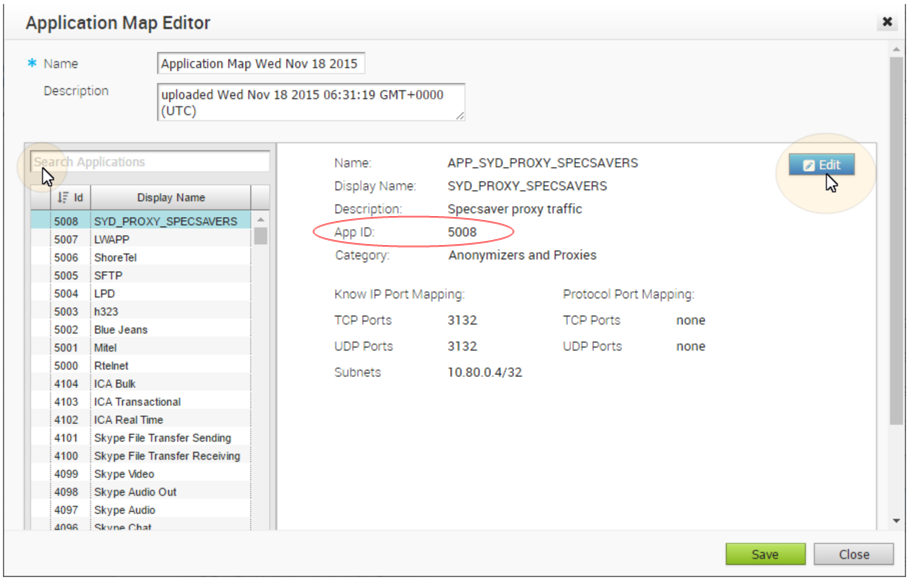
Modify Application Map

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

In the Operator portal, click **Application Maps**.

1 Select the Application Map to be updated and click **Actions > Modify Application Map** or click the link to the Application Map.

2 The **Application Map Editor** displays the list of application definitions available in the Map file.



Application Map Editor

* Name: Application Map Wed Nov 18 2015

Description: uploaded Wed Nov 18 2015 06:31:19 GMT+0000 (UTC)

Search Applications

Id	Display Name
5008	SYD_PROXY_SPECSAVERS
5007	LWAPP
5006	ShoreTel
5005	SFTP
5004	LPD
5003	h323
5002	Blue Jeans
5001	Mitel
5000	Rtelnet
4104	ICA Bulk
4103	ICA Transactional
4102	ICA Real Time
4101	Skype File Transfer Sending
4100	Skype File Transfer Receiving
4099	Skype Video
4098	Skype Audio Out
4097	Skype Audio
4096	Skype Chat

Name: APP_SYD_PROXY_SPECSAVERS

Display Name: SYD_PROXY_SPECSAVERS

Description: Specsaver proxy traffic

App ID: 5008

Category: Anonymizers and Proxies

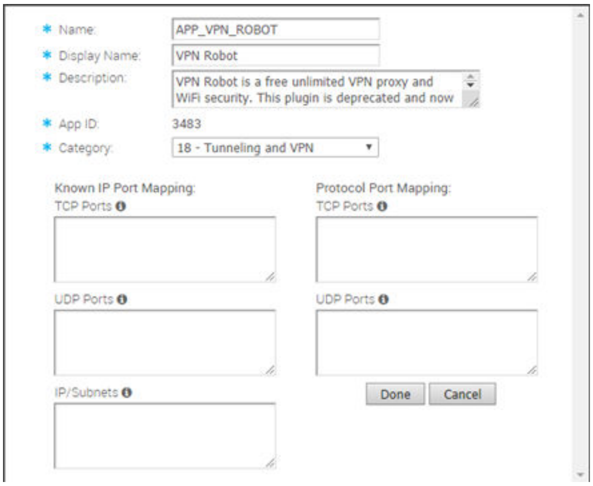
Know IP Port Mapping:		Protocol Port Mapping:	
TCP Ports	3132	TCP Ports	none
UDP Ports	3132	UDP Ports	none
Subnets	10.80.0.4/32		

Select an Application definition and view detailed information about the selected definition. You can also search for an Application definition, sort the definitions by App ID or display name, create a new Application definition, or remove an existing definition.

3 To add a definition to the list, click **Add New**.

4 To delete a definition from the list, click **Remove**.

5 To modify the details of the selected definition, click **Edit**.



* Name: APP_VPN_ROBOT

* Display Name: VPN Robot

* Description: VPN Robot is a free unlimited VPN proxy and WiFi security. This plugin is deprecated and now

* App ID: 3483

* Category: 18 - Tunneling and VPN

Update the details like Name, Display Name, Description, Category, Ports, and click **Done**.

When you create a new definition, the Application ID is assigned automatically.

You can download the Application Map as a JSON file to assign additional flags to the application definitions. You can modify the Application ID as well and it is recommended to define the IDs as follows:

For releases earlier than 3.3.2:

- 0-4999 for DPI Apps

- 5000-5999 for VMware SD-WAN Apps
- 6000-6999 for User-defined Apps

For releases 3.3.2 and later:

- 0-4999 for DPI Apps
- 5000-5999 for VMware SD-WAN Apps
- 6000-9999 for User-defined Apps

6 In the **Application Map Editor**, click **Save**.

To upload a customized Application Map, see Upload Application Map.

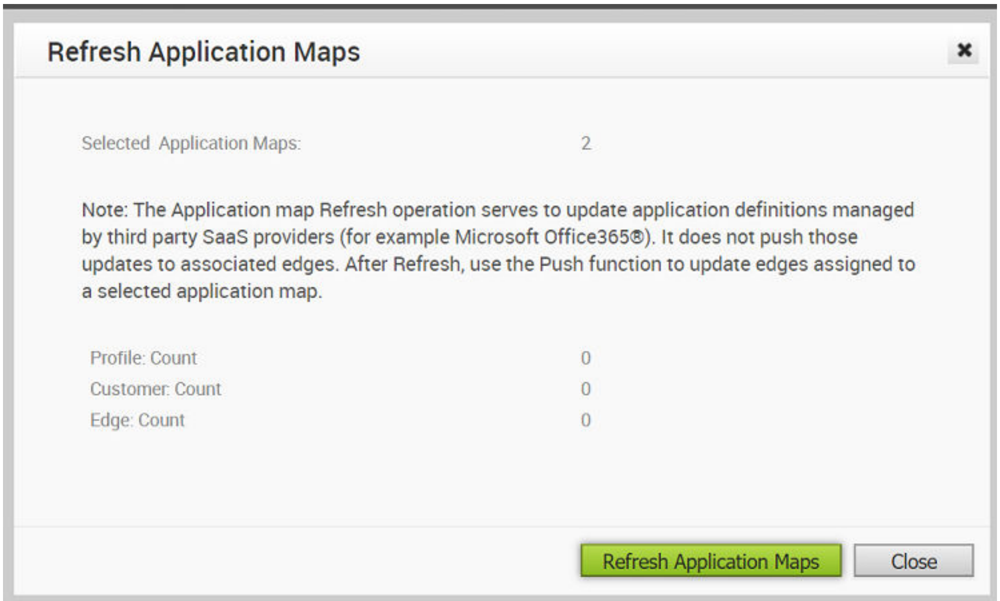
Refresh Application Map

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

In the Operator portal, click **Application Maps**.

1 Select the Application maps that you want to refresh and click **Actions > Refresh Application Map**.

2 The **Refresh Application Maps** page opens, which lists the number of Operator profiles, Customers, and SD-WAN Edges associated with the selected Application Maps.



Refresh Application Maps

Selected Application Maps: 2

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.

Profile: Count 0
Customer: Count 0
Edge: Count 0

3 Click **Refresh Application Maps** to refresh the selected Application Maps.

Note You can only update the Application definitions in the Application Maps using the Refresh option. If you want to update the associated SD-WAN Edges with the latest definitions, then use the Push Application Map option.

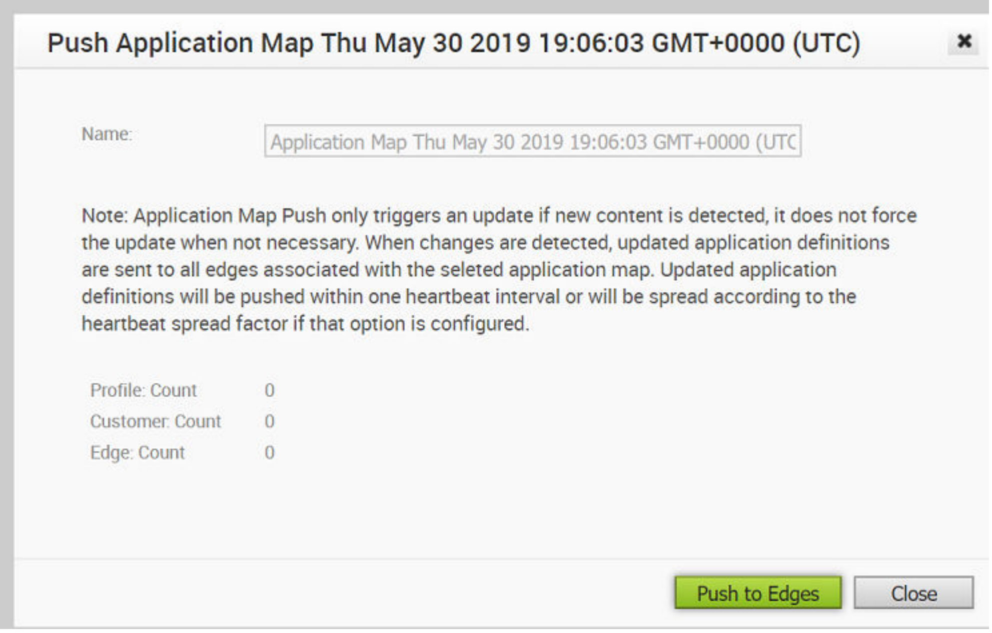
Push Application Map

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

In the Operator portal, click **Application Maps**.

1 Select the Application Map that you want to push to the associated SD-WAN Edges and click **Actions > Push Application Map**.

2 The **Push Application Map** page opens, which lists the number of Operator profiles, customers, and SD-WAN Edges associated with the selected Application Map.



Push Application Map Thu May 30 2019 19:06:03 GMT+0000 (UTC)

Name: Application Map Thu May 30 2019 19:06:03 GMT+0000 (UTC

Note: Application Map Push only triggers an update if new content is detected, it does not force the update when not necessary. When changes are detected, updated application definitions are sent to all edges associated with the seleted application map. Updated application definitions will be pushed within one heartbeat interval or will be spread according to the heartbeat spread factor if that option is configured.

Profile: Count 0
Customer: Count 0
Edge: Count 0

3 Click **Push to Edges** to update the SD-WAN Edges with the latest Application definitions available in the selected Application Map.

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

Role Customization

15

SD-WAN Orchestrator consists of user roles with different set of privileges. As an Operator super user, you can assign a pre-defined role to a user. Role Customization allows you to customize the existing set of privileges for the user roles.

To enable or disable a Partner super user to customize the role privileges of other Partner users and Enterprise users of the Partner, see Configure Partner Information.

To enable or disable an Enterprise super user to customize the role privileges of other Enterprise users, see Configure Customers.

The Role customization is applied to the user roles as follows:

- The customizations done at the Enterprise level will override the customizations made at the Partner or Operator level.
- The customizations done at the Partner level will override the customizations made at the Operator level.
- 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 SD-WAN Orchestrator.

In the Operator portal, click **Role Customization**.

You can perform the following operations:

- **Show Current Privileges** – Displays the current user role privileges. You can view the privileges of all the user roles and download them in CSV format.
- **New Package** – Enables to create a new package with customized role privileges. See Create New Customized Package.
- **Reset to System Default** – Allows to reset the current role privileges to default settings. Only the customized privileges applied to the user roles in the Operator portal are reset to the default settings. If your partners or customers have customized their user role privileges in the Partner or Enterprise portal, those settings remain the same.

Click **Actions** to perform the following activities:

- **Upload Package** – Allows to upload a customized package. See Upload Customized Package.
- **Clone Package** – Enables to create a copy of the selected package.

- **Modify Package** – Enables to edit the customization settings in the selected package. You can also click the link to the package to edit the settings.
- **Delete Package** – Removes the selected package. You cannot delete a package if it is already in use.
- **Apply Package** – Applies the customization available in the selected package to the existing user roles. This option modifies the role 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.

You can also click the Download Icon prior to the package name to download the package as a JSON file.

Note Role customization packages are version dependent, and a package created on an Orchestrator using an earlier software release will not be compatible with an Orchestrator using a later release. For example, a role customization package 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 role customization package 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 role customization package for the newer release to ensure proper enforcement of all roles.

This chapter includes the following topics:

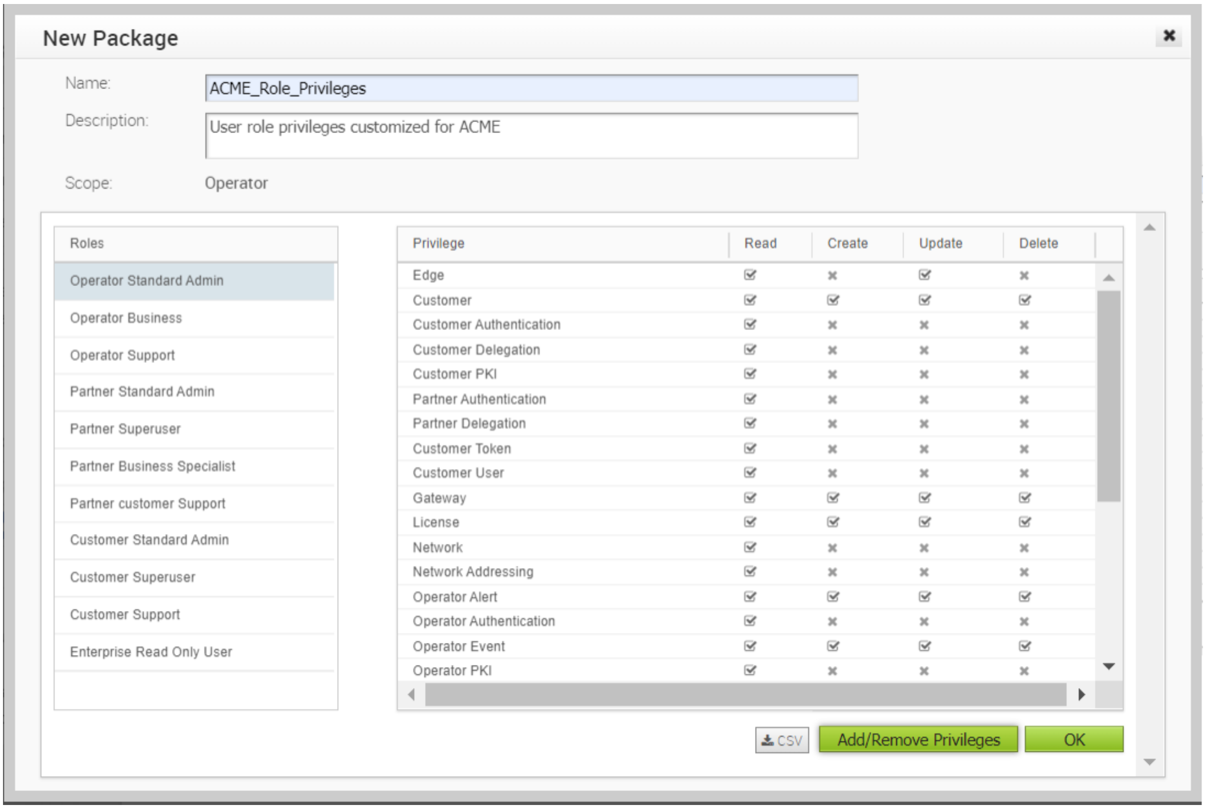
Create New Customized Package

You can create a customized package and apply the package to the existing user roles in the SD-WAN Orchestrator.

Procedure

1. In the Operator portal, click **Role Customization**.
2. Click **New Package**.

3 In the **Role Customization Package Editor** window, enter the following:



New Package

Name: ACME_Role_Privileges

Description: User role privileges customized for ACME

Scope: Operator

Roles
Operator Standard Admin
Operator Business
Operator Support
Partner Standard Admin
Partner Superuser
Partner Business Specialist
Partner customer Support
Customer Standard Admin
Customer Superuser
Customer Support
Enterprise Read Only User

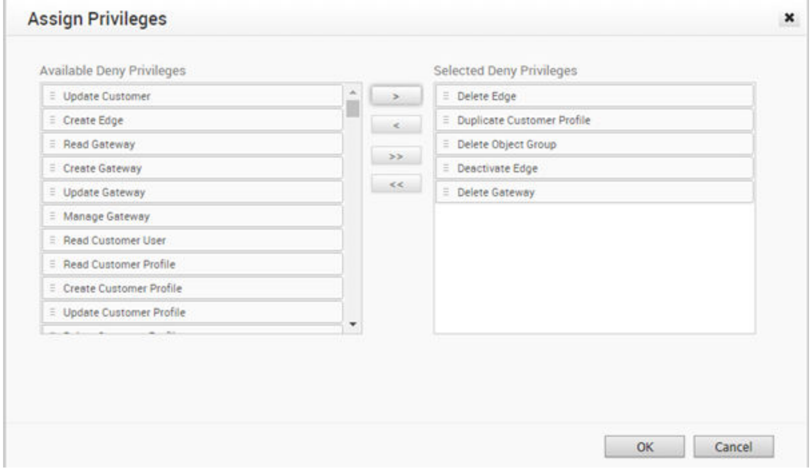
Privilege	Read	Create	Update	Delete
Edge	☑	☒	☑	☒
Customer	☑	☑	☑	☑
Customer Authentication	☑	☒	☒	☒
Customer Delegation	☑	☒	☒	☒
Customer PKI	☑	☒	☒	☒
Partner Authentication	☑	☒	☒	☒
Partner Delegation	☑	☒	☒	☒
Customer Token	☑	☒	☒	☒
Customer User	☑	☒	☒	☒
Gateway	☑	☑	☑	☑
License	☑	☑	☑	☑
Network	☑	☒	☒	☒
Network Addressing	☑	☒	☒	☒
Operator Alert	☑	☑	☑	☑
Operator Authentication	☑	☒	☒	☒
Operator Event	☑	☑	☑	☑
Operator PKI	☑	☒	☒	☒

a Enter a **Name** and a **Description** for the new custom package.

b In the **Roles** pane, select a user role and click **Add/Remove Privileges** to customize the privileges for the selected role.

Note You can only add or remove Deny Privileges, that is take away privileges from the system default. You cannot grant additional privileges to a role using this option.

In the **Assign Privileges** window, select the features from the **Available Deny Privileges** and move them to the **Selected Deny Privileges** pane.



Assign Privileges

Available Deny Privileges
- Update Customer
- Create Edge
- Read Gateway
- Create Gateway
- Update Gateway
- Manage Gateway
- Read Customer User
- Read Customer Profile
- Create Customer Profile
- Update Customer Profile

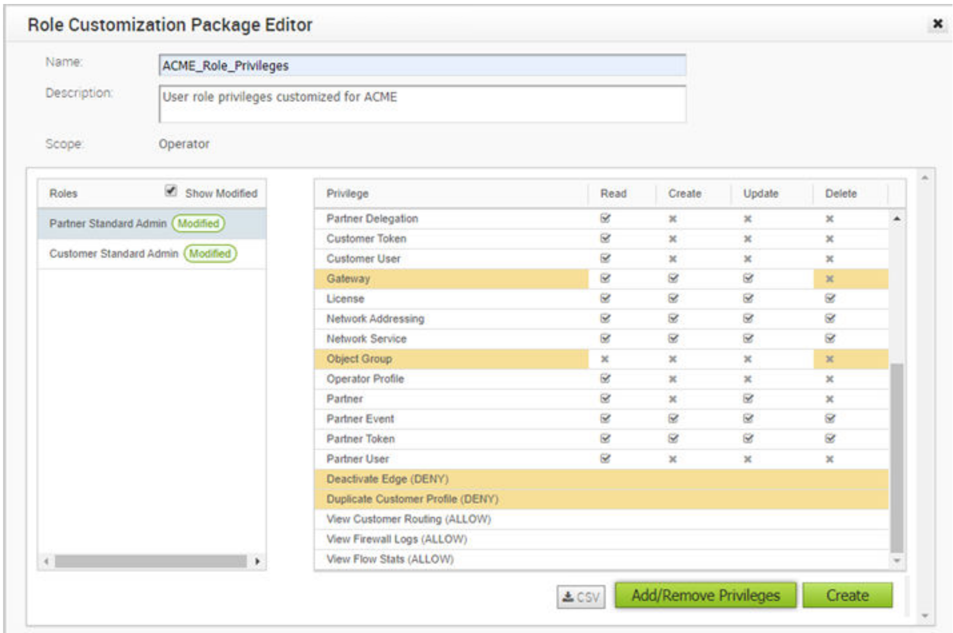
Selected Deny Privileges
- Delete Edge
- Duplicate Customer Profile
- Delete Object Group
- Deactivate Edge
- Delete Gateway

Note You can assign only **Deny** privileges to the user roles.

Click **OK**.

4 Repeat assigning privileges to the user roles in the **Role Customization Package Editor** window.

5 Select the **Show Modified** checkbox to filter and view the customized privileges. The changes to the privileges are highlighted in a different color.



Role Customization Package Editor

Name: ACME_Role_Privileges

Description: User role privileges customized for ACME

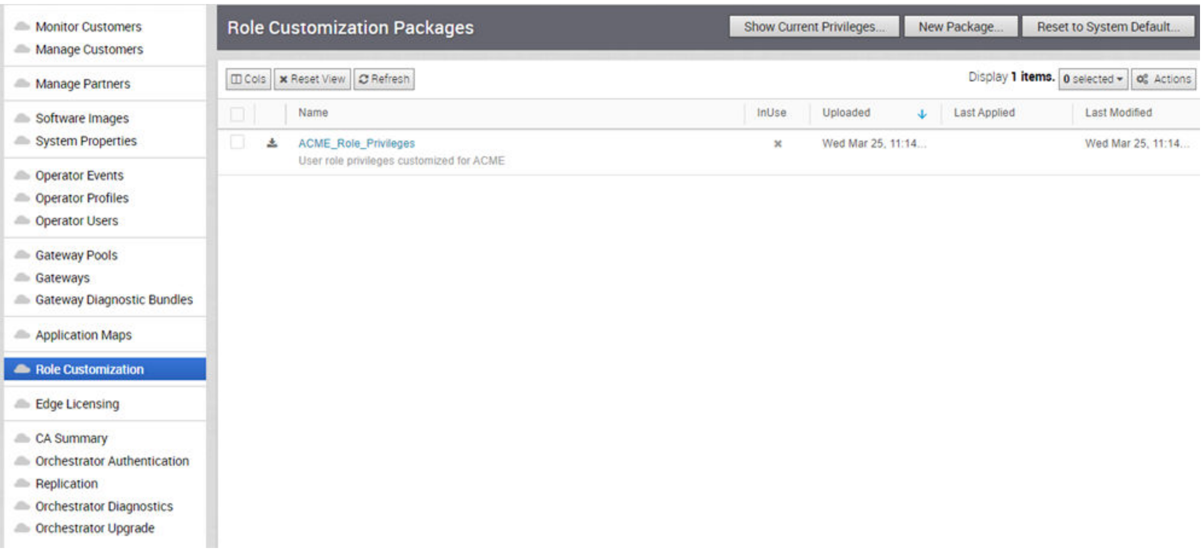
Scope: Operator

Roles	☑ Show Modified
Partner Standard Admin	Modified
Customer Standard Admin	Modified

Privilege	Read	Create	Update	Delete
Partner Delegation	☑	✕	✕	✕
Customer Token	☑	✕	✕	✕
Customer User	☑	✕	✕	✕
Gateway	☑	☑	☑	✕
License	☑	☑	☑	☑
Network Addressing	☑	☑	☑	☑
Network Service	☑	☑	☑	☑
Object Group	✕	✕	✕	✕
Operator Profile	☑	✕	✕	✕
Partner	☑	✕	☑	✕
Partner Event	☑	☑	☑	☑
Partner Token	☑	☑	☑	☑
Partner User	☑	✕	✕	✕
Deactivate Edge (DENY)				
Duplicate Customer Profile (DENY)				
View Customer Routing (ALLOW)				
View Firewall Logs (ALLOW)				
View Flow Stats (ALLOW)				

6 Click **Create**. You can click **CSV** to download the user role privileges of selected user role, in a CSV format.

7 The new package details are displayed in the **Role Customization Packages** window.



Role Customization Packages

Display **1 items.** 0 selected

		Name	InUse	Uploaded	Last Applied	Last Modified
□		ACME_Role_Privileges User role privileges customized for ACME	✕	Wed Mar 25, 11:14...		Wed Mar 25, 11:14...

8 To edit the privileges, click the link to the package or select the package and click **Actions > Modify Package**. In the **Role Customization Package Editor** window that opens, add or remove Deny Privileges to the user roles in the package and click **OK**.

What to do next

Select the customized package and click **Actions > Apply Package** to apply the customization available in the selected package to the existing user roles across the SD-WAN Orchestrator.

You can edit the Deny privileges in an applied package whenever required. After modifying the privileges in the **Role Customization Package Editor** window, click **OK** to save and apply the changes to the user roles.

Note You can download the customized user role privileges as a JSON file and upload the customized package to another Orchestrator. For more information, see Upload Customized Package.

Upload Customized Package

You can upload a package with customized role privileges assigned to different set of user roles in the SD-WAN Orchestrator.

You can download the already customized user role privileges as a package and upload the package to another Orchestrator.

Procedure

1 In the Operator portal, click **Role Customization**.

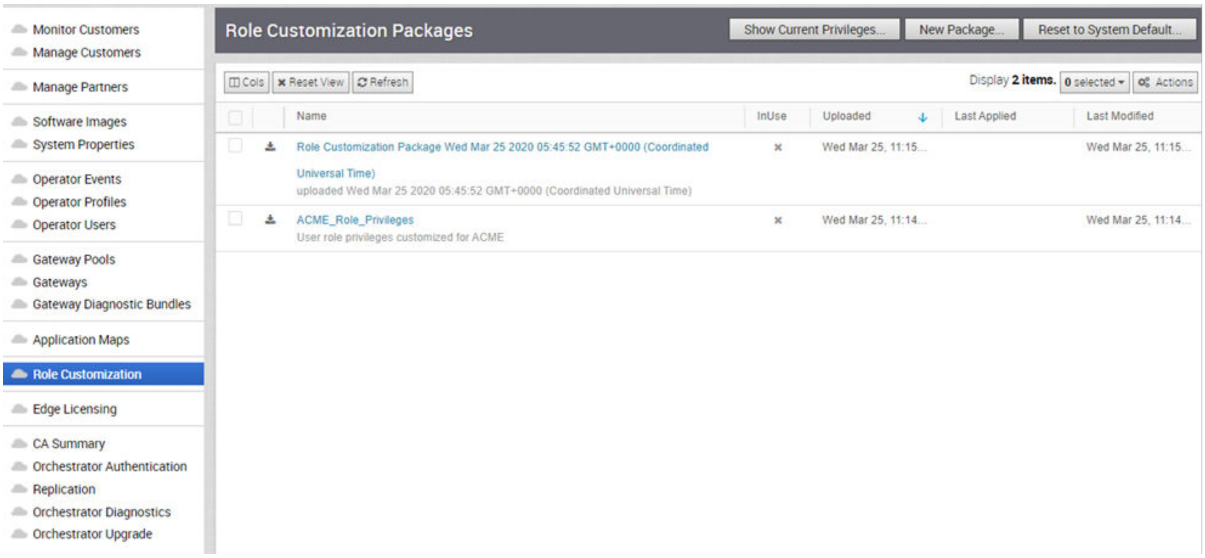
2 Click the Download Icon prior to a package name, which downloads the package as a JSON file.

3 Navigate to the Orchestrator to which you want to upload the customized package.

4 Click **Actions > Upload Package**.

5 Choose the JSON file you have downloaded, and the package is uploaded automatically.

6 The uploaded package is displayed in the **Role Customization Packages** window.



□		Name	InUse	Uploaded ↓	Last Applied	Last Modified
□	⤓	Role Customization Package Wed Mar 25 2020 05:45:52 GMT+0000 (Coordinated Universal Time) uploaded Wed Mar 25 2020 05:45:52 GMT+0000 (Coordinated Universal Time)	×	Wed Mar 25, 11:15...		Wed Mar 25, 11:15...
□	⤓	ACME_Role_Privileges User role privileges customized for ACME	×	Wed Mar 25, 11:14...		Wed Mar 25, 11:14...

7 You can view the privileges in the uploaded package and add more Deny privileges. Click the link to the package or select the package and click **Actions > Modify Package**. In the **Role Customization Package Editor** window that opens, add or remove Deny privileges to the user roles in the package and click **OK**. For more information on the **Role Customization Package Editor**, see Create New Customized Package.

What to do next

Select the customized package and click **Actions > Apply Package** to apply the customization available in the selected package to the existing user roles across the SD-WAN Orchestrator.

You can edit Deny privileges in an applied package whenever required. After modifying the privileges in the **Role Customization Package Editor** window, click **OK** to save and apply the changes to the user roles.

Edge Licensing

16

SD-WAN Orchestrator provides different types of Licenses for the SD-WAN Edges. An Operator can manage and assign Edge Licenses to Partners and Enterprise Customers. Partners can assign Edge License types their Enterprise Customers.

The Edge Licensing is enabled by default.

To disable Edge Licensing, set the value of System Property **session.options.enableEdgeLicensing** to **False**. In the Operator portal, click **System Properties** to update the property value.

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, VMware 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 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.

To view and generate a report of available Edge License types, see Generate Edge Licenses Report.

This chapter includes the following topics:

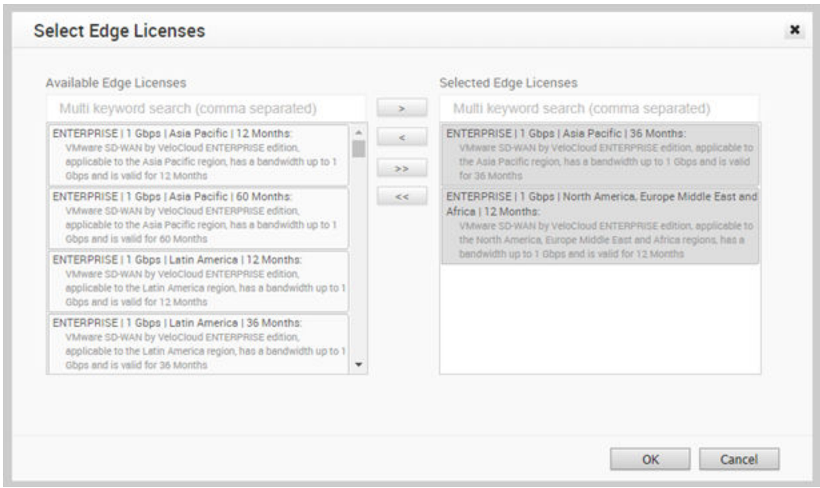
- Manage Edge Licenses for Partners
- Manage Edge Licenses for Customers
- Generate Edge Licenses Report

Manage Edge Licenses for Partners

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

The following procedure is 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 Licensing**.
4. Click **Manage Edge License**.
5. In the **Select Edge Licenses** window, choose the relevant licenses based on the Bandwidth, Term, Edition, and Region.



Available Edge Licenses:

ENTERPRISE | 1 Gbps | Asia Pacific | 12 Months:
VMware SD-WAN by VeloCloud ENTERPRISE edition, applicable to the Asia Pacific region, has a bandwidth up to 1 Gbps and is valid for 12 Months

ENTERPRISE | 1 Gbps | Asia Pacific | 60 Months:
VMware SD-WAN by VeloCloud ENTERPRISE edition, applicable to the Asia Pacific region, has a bandwidth up to 1 Gbps and is valid for 60 Months

ENTERPRISE | 1 Gbps | Latin America | 12 Months:
VMware SD-WAN by VeloCloud ENTERPRISE edition, applicable to the Latin America region, has a bandwidth up to 1 Gbps and is valid for 12 Months

ENTERPRISE | 1 Gbps | Latin America | 36 Months:
VMware SD-WAN by VeloCloud ENTERPRISE edition, applicable to the Latin America region, has a bandwidth up to 1 Gbps and is valid for 36 Months

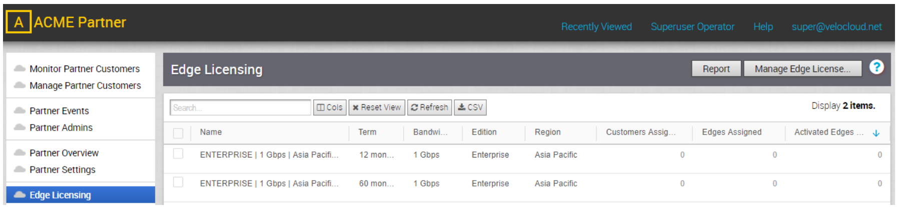
Selected Edge Licenses:

ENTERPRISE | 1 Gbps | Asia Pacific | 36 Months:
VMware SD-WAN by VeloCloud ENTERPRISE edition, applicable to the Asia Pacific region, has a bandwidth up to 1 Gbps and is valid for 36 Months

ENTERPRISE | 1 Gbps | North America, Europe Middle East and Africa | 12 Months:
VMware SD-WAN by VeloCloud ENTERPRISE edition, applicable to the North America, Europe Middle East and Africa regions, has a bandwidth up to 1 Gbps and is valid for 12 Months

6. Click **OK**.

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



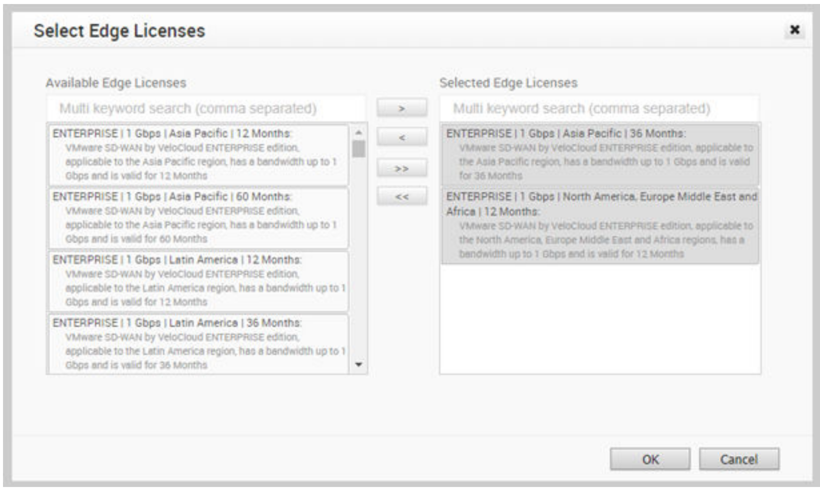
□	Name	Term	Bandwi...	Edition	Region	Customers Assig...	Edges Assigned	Activated Edges ...
□	ENTERPRISE | 1 Gbps | Asia Pacifi...	12 mon...	1 Gbps	Enterprise	Asia Pacific	0	0	0
□	ENTERPRISE | 1 Gbps | Asia Pacifi...	60 mon...	1 Gbps	Enterprise	Asia Pacific	0	0	0

Click **Report** to generate a report of the licenses along with the associated customers and SD-WAN Edges in a CSV format.

Manage Edge Licenses for Customers

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

- In the Operator portal, click **Manage Customers**.
- Click the link to a customer name to navigate to the Enterprise portal.
- In the Enterprise portal, click **Administration** > **Edge Licensing**.
- Click **Manage Edge License**.
- In the **Select Edge Licenses** window, choose the relevant licenses based on the Bandwidth, Term, Edition, Region and move them to the **Selected Edge Licenses** pane.



Available Edge Licenses:

ENTERPRISE | 1 Gbps | Asia Pacific | 12 Months:
VMware SD-WAN by VeloCloud ENTERPRISE edition, applicable to the Asia Pacific region, has a bandwidth up to 1 Gbps and is valid for 12 Months

ENTERPRISE | 1 Gbps | Asia Pacific | 60 Months:
VMware SD-WAN by VeloCloud ENTERPRISE edition, applicable to the Asia Pacific region, has a bandwidth up to 1 Gbps and is valid for 60 Months

ENTERPRISE | 1 Gbps | Latin America | 12 Months:
VMware SD-WAN by VeloCloud ENTERPRISE edition, applicable to the Latin America region, has a bandwidth up to 1 Gbps and is valid for 12 Months

ENTERPRISE | 1 Gbps | Latin America | 36 Months:
VMware SD-WAN by VeloCloud ENTERPRISE edition, applicable to the Latin America region, has a bandwidth up to 1 Gbps and is valid for 36 Months

Selected Edge Licenses:

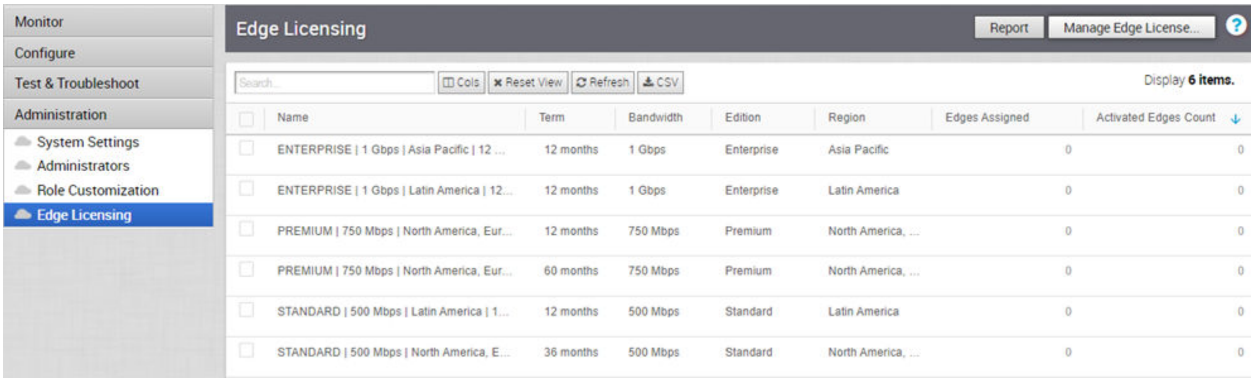
ENTERPRISE | 1 Gbps | Asia Pacific | 36 Months:
VMware SD-WAN by VeloCloud ENTERPRISE edition, applicable to the Asia Pacific region, has a bandwidth up to 1 Gbps and is valid for 36 Months

ENTERPRISE | 1 Gbps | North America, Europe Middle East and Africa | 12 Months:
VMware SD-WAN by VeloCloud ENTERPRISE edition, applicable to the North America, Europe Middle East and Africa regions, has a bandwidth up to 1 Gbps and is valid for 12 Months

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

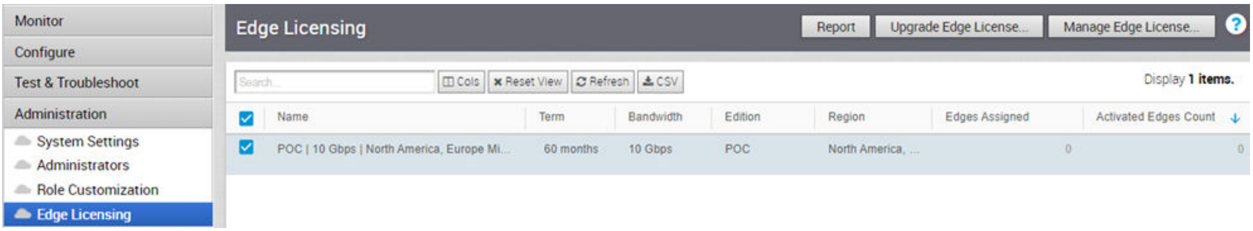
- Click **OK**.

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



□	Name	Term	Bandwidth	Edition	Region	Edges Assigned	Activated Edges Count
□	ENTERPRISE | 1 Gbps | Asia Pacific | 12 ...	12 months	1 Gbps	Enterprise	Asia Pacific	0	0
□	ENTERPRISE | 1 Gbps | Latin America | 12...	12 months	1 Gbps	Enterprise	Latin America	0	0
□	PREMIUM | 750 Mbps | North America, Eur...	12 months	750 Mbps	Premium	North America, ...	0	0
□	PREMIUM | 750 Mbps | North America, Eur...	60 months	750 Mbps	Premium	North America, ...	0	0
□	STANDARD | 500 Mbps | Latin America | 1...	12 months	500 Mbps	Standard	Latin America	0	0
□	STANDARD | 500 Mbps | North America, E...	36 months	500 Mbps	Standard	North America, ...	0	0

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.



☑	Name	Term	Bandwidth	Edition	Region	Edges Assigned	Activated Edges Count
☑	POC | 10 Gbps | North America, Europe Mi...	60 months	10 Gbps	POC	North America, ...	0	0

Note You cannot downgrade a License type to the previous Edition.

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

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

You can assign a license to an existing Edge:

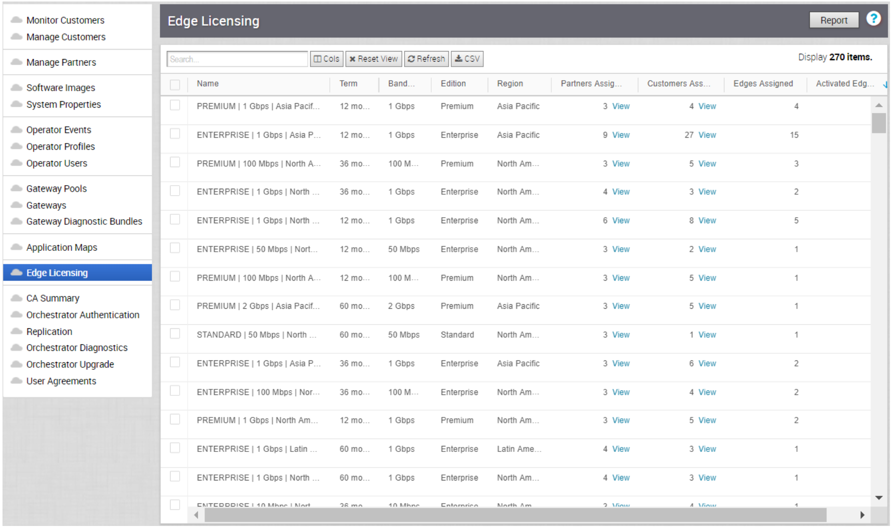
- In the Enterprise portal, click **Configure > Edges**.
- To assign license to each Edge, click the link to the Edge and select the License in the **Edge Overview** page. You can also select the Edge and click **Actions > Assign Edge License** to assign the License.
- To assign a license to multiple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

Note If Edge Licensing is disabled, then the **Assign Edge License** option is not available for the Edges. The Enterprise Admin user can create an Edge without the Edge license.

Generate Edge Licenses Report

Operator Superusers, Standard Operators, Business Specialists, and Customer Support Operators can generate a report of the existing Edge licenses.

In the Operator portal, navigate to **Edge Licensing**.



Display **270 items.**

□	Name	Term	Band...	Edition	Region	Partners Assig...	Customers Ass...	Edges Assigned	Activated Edg...
□	PREMIUM | 1 Gbps | Asia Pacif...	12 mo...	1 Gbps	Premium	Asia Pacific	3 View	4 View	4	
□	ENTERPRISE | 1 Gbps | Asia P...	12 mo...	1 Gbps	Enterprise	Asia Pacific	9 View	27 View	15	
□	PREMIUM | 100 Mbps | North A...	36 mo...	100 M...	Premium	North Am...	3 View	5 View	3	
□	ENTERPRISE | 1 Gbps | North ...	36 mo...	1 Gbps	Enterprise	North Am...	4 View	3 View	2	
□	ENTERPRISE | 1 Gbps | North ...	12 mo...	1 Gbps	Enterprise	North Am...	6 View	8 View	5	
□	ENTERPRISE | 50 Mbps | Nort...	12 mo...	50 Mbps	Enterprise	North Am...	3 View	2 View	1	
□	PREMIUM | 100 Mbps | North A...	12 mo...	100 M...	Premium	North Am...	3 View	5 View	1	
□	PREMIUM | 2 Gbps | Asia Pacif...	60 mo...	2 Gbps	Premium	Asia Pacific	3 View	5 View	1	
□	STANDARD | 50 Mbps | North ...	60 mo...	50 Mbps	Standard	North Am...	3 View	1 View	1	
□	ENTERPRISE | 1 Gbps | Asia P...	36 mo...	1 Gbps	Enterprise	Asia Pacific	3 View	6 View	2	
□	ENTERPRISE | 100 Mbps | Nor...	36 mo...	100 M...	Enterprise	North Am...	3 View	4 View	2	
□	PREMIUM | 1 Gbps | North Am...	12 mo...	1 Gbps	Premium	North Am...	3 View	5 View	2	
□	ENTERPRISE | 1 Gbps | Latin ...	60 mo...	1 Gbps	Enterprise	Latin Ame...	4 View	3 View	1	
□	ENTERPRISE | 1 Gbps | North ...	60 mo...	1 Gbps	Enterprise	North Am...	4 View	3 View	1	
□	ENTERPRISE | 10 Mbps | Nort...	36 mo...	10 Mbps	Enterprise	North Am...	3 View	4 View	1	

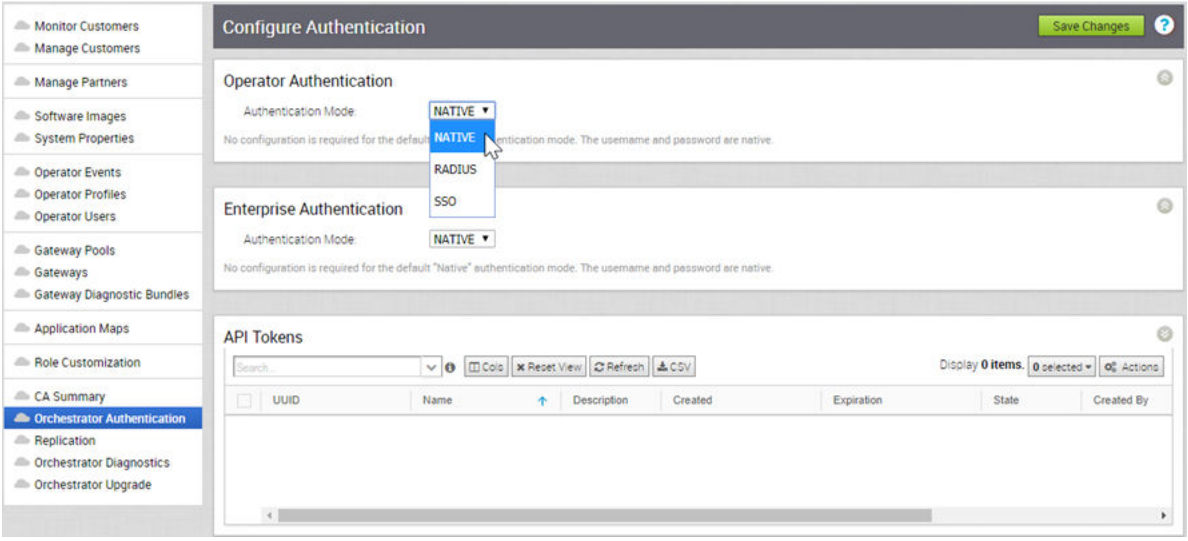
Click **Report** to generate a report of the licenses, associated partners, customers, and SD-WAN Edges in a CSV format.

Orchestrator Authentication

17

The Orchestrator Authentication option allows you to set the authentication modes for both the Operator and Enterprise Users. You can also view the existing API tokens.

In the Operator portal, click **Orchestrator Authentication** and select the authentication modes from the drop-down menu for Operator and Enterprise users.



Configure Authentication

Operator Authentication

Authentication Mode: NATIVE

No configuration is required for the default "Native" authentication mode. The username and password are native.

Enterprise Authentication

Authentication Mode: NATIVE

No configuration is required for the default "Native" authentication mode. The username and password are native.

API Tokens

Display **0 items.**

	UUID	Name	Description	Created	Expiration	State	Created By

The following are the authentication modes available. Only an Operator User can enable the Native and RADIUS modes for both Operator and Enterprise authentication. Any Operator user with super user permission can set up and configure the SSO mode.

- **Native** – The default authentication mode of the SD-WAN Orchestrator. This mode does not require any configuration.
- **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. For more information, see Configure RADIUS Authentication
- **SSO** – Single Sign On (SSO) is a session and user authentication service that allows the Operator Users to log into the Orchestrator with one set of login credentials to access multiple applications. For more information, see Configure Operator Single Sign On.

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, in this section. If required, an Operator Administrator can revoke the API tokens.

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

Only the Operator Super User or the User associated with an API token can revoke the token. Select the token and click **Actions > Revoke** . As an Operator Super User, you can manage the API tokens for enterprise users. To create and download the API tokens, see API Tokens.

This chapter includes the following topics:

- Configure RADIUS Authentication
- Configure Operator Single Sign On

Configure RADIUS Authentication

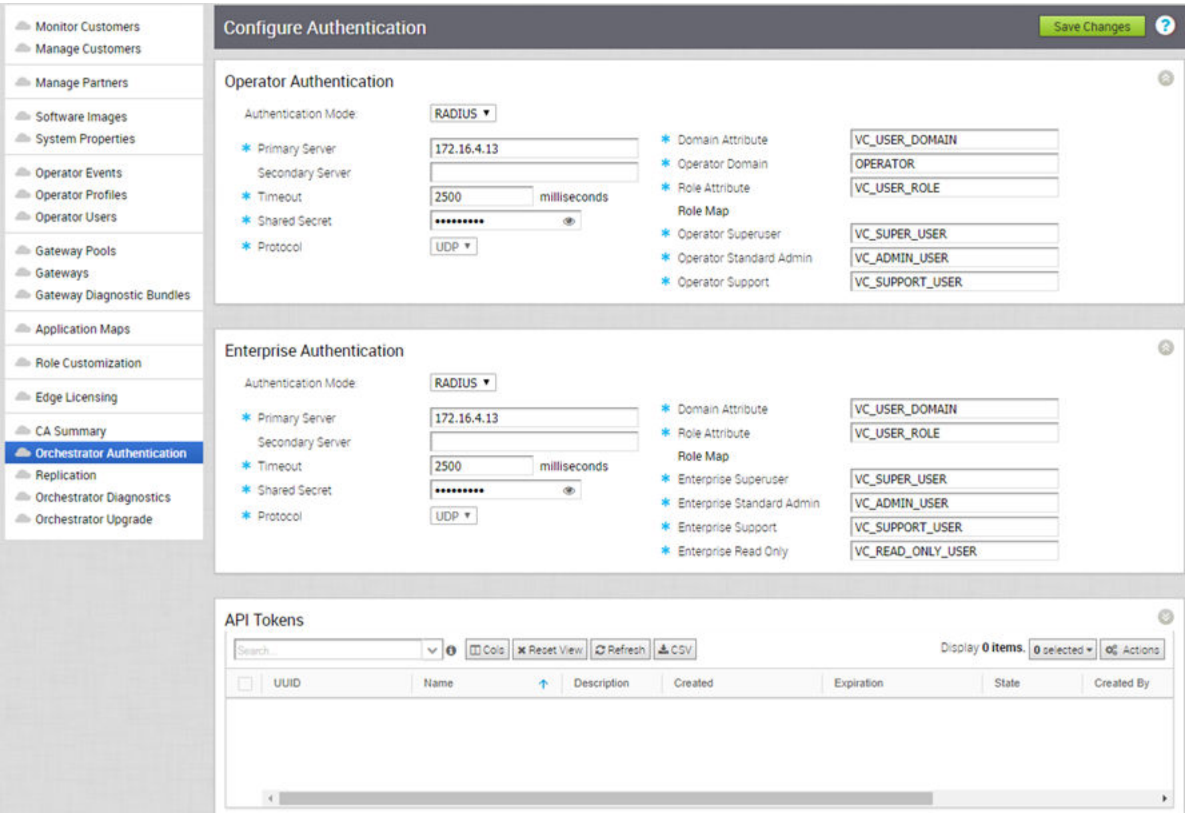
You can configure the Orchestrator Authentication in RADIUS mode, so that the Operator and Enterprise Customers log into the portals using the RADIUS servers.

Choose to deploy one of the following in the RADIUS authentication mode:

- Single RADIUS Server – Share the same radius server between the Operator and the Enterprise Customer.
- Separate RADIUS Servers – Configure one Radius server for Operator/SP and another one for all the Enterprise Customers.

To configure the RADIUS mode, click **Orchestrator Authentication** in the Operator portal.

Choose the **Authentication Mode** as RADIUS for **Operator Authentication** and **Enterprise Authentication**. Enter the appropriate details.



Configure Authentication

Operator Authentication

Authentication Mode: RADIUS

* Primary Server 172.16.4.13

Secondary Server

* Timeout 2500 milliseconds

* Shared Secret •••••••••

* Protocol UDP

* Domain Attribute VC_USER_DOMAIN

* Operator Domain OPERATOR

* Role Attribute VC_USER_ROLE

Role Map

* Operator Superuser VC_SUPER_USER

* Operator Standard Admin VC_ADMIN_USER

* Operator Support VC_SUPPORT_USER

Enterprise Authentication

Authentication Mode: RADIUS

* Primary Server 172.16.4.13

Secondary Server

* Timeout 2500 milliseconds

* Shared Secret •••••••••

* Protocol UDP

* Domain Attribute VC_USER_DOMAIN

* Role Attribute VC_USER_ROLE

Role Map

* Enterprise Superuser VC_SUPER_USER

* Enterprise Standard Admin VC_ADMIN_USER

* Enterprise Support VC_SUPPORT_USER

* Enterprise Read Only VC_READ_ONLY_USER

API Tokens

	UUID	Name	Description	Created	Expiration	State	Created By

You can enter or modify the values in the fields, except the **Protocol**. You can edit the protocol value only in the System Properties. Edit the protocol in the Value fields of `vco.operator.authentication.radius` for the Operator and `vco.enterprise.authentication.radius` for the Enterprises.

Instead of configuring the values in the **Configure Authentication** page, you can also define the values of RADIUS server in the System Properties. In the Operator portal, navigate to the **System Properties** page and configure the following system properties:

- `vco.enterprise.authentication.mode` – Enter the Value as **RADIUS** to enable RADIUS authentication for Enterprises.
- `vco.enterprise.authentication.radius` – In the Value field, edit the JSON template with the server details and other attributes for Enterprises.
- `vco.operator.authentication.mode` – Enter the Value as **RADIUS** to enable RADIUS authentication for Operators.
- `vco.operator.authentication.radius` – In the Value field, edit the JSON template with the server details and other attributes for Operators.

After defining the system properties with relevant values, click **Orchestrator Authentication**.

The **Authentication Mode** is changed to **RADIUS** and the fields popup with the attributes you have defined in the System Properties.

If required, you can modify the values in the corresponding fields. After updating the fields, click **Save Changes**.

Configure Operator Single Sign On

The Single Sign On (SSO) mode is newly added in **Orchestrator Authentication** screen.

Overview of Single Sign On

The SD-WAN Orchestrator supports a new type of user authentication called Single Sign On (SSO) for all Orchestrator user types: Operator, Partner, and Enterprise.

Single Sign On (SSO) is a session and user authentication service that allows SD-WAN Orchestrator users to log in to the SD-WAN Orchestrator with one set of login credentials to access multiple applications. Integrating the SSO service with SD-WAN Orchestrator improves the security of user authentication for SD-WAN Orchestrator users and enables SD-WAN Orchestrator to authenticate users from other OpenID Connect (OIDC)-based Identity Providers (IDPs). The following IDPs are currently supported:

- Okta
- OneLogin
- PingIdentity
- AzureAD
- VMwareCSP

Configure Single Sign On for Operator User

Operator users with super user permission can set up and configure Single Sign On (SSO) in SD-WAN Orchestrator. To setup SSO authentication for Operator user, perform the steps on this procedure.

To configure single sign on for an Operator user:

Prerequisites

- Ensure that you have the Operator super user permission.
- Before setting up the SSO authentication in SD-WAN Orchestrator, make sure that you have set up roles, users, and OpenID connect (OIDC) application for SD-WAN Orchestrator in your preferred identity provider’s website. For more information, see Configure an IDP for Single Sign On.

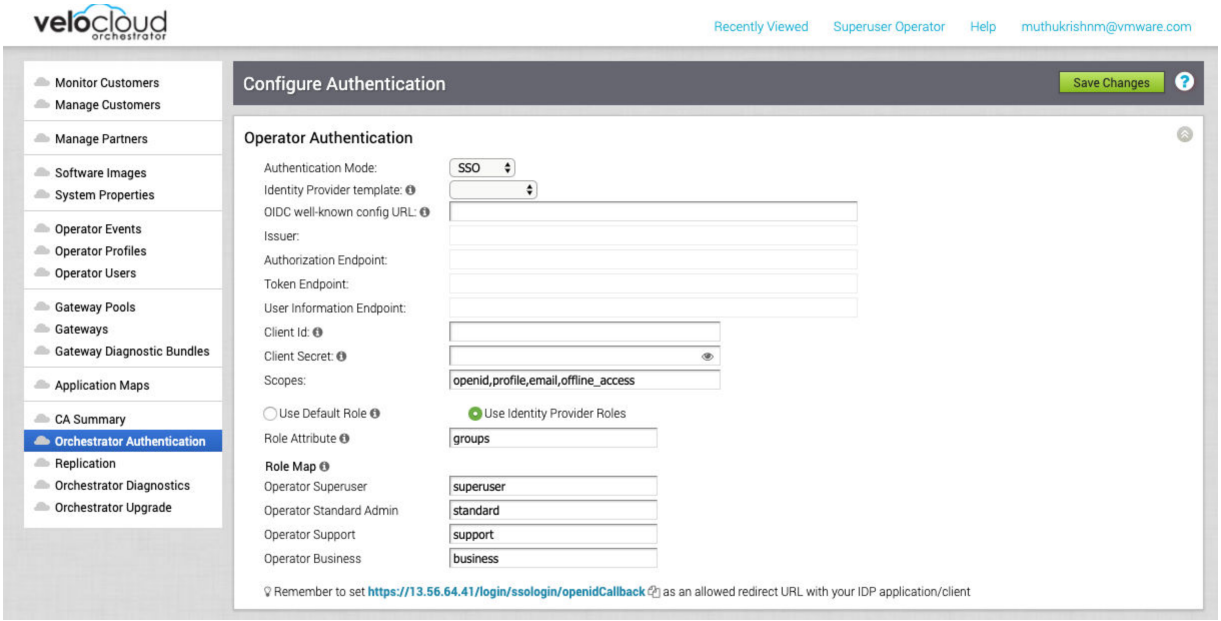
Note SSO integration at the Operator management level of a VMware hosted Orchestrator is reserved for the VMware SD-WAN TechOPS operators. Partners with Operator level access of a hosted orchestrator do not have the option to integrate to an SSO service.

Procedure

1 Log in to the SD-WAN Orchestrator application as Operator super user.

2 Click **Orchestrator Authentication**.

The **Configure Authentication** screen appears.



Configure Authentication

Operator Authentication

Authentication Mode: SSO
Identity Provider template:
OIDC well-known config URL:
Issuer:
Authorization Endpoint:
Token Endpoint:
User Information Endpoint:
Client Id:
Client Secret:
Scopes: openid,profile,email,offline_access

○ Use Default Role ● Use Identity Provider Roles

Role Attribute: groups

Role Map
Operator Superuser: superuser
Operator Standard Admin: standard
Operator Support: support
Operator Business: business

Remember to set https://13.56.64.41/login/ssologin/openidCallback as an allowed redirect URL with your IDP application/client

3 From the **Authentication Mode** drop-down menu, select **SSO**.

4 From the **Identity Provider template** drop-down menu, select your preferred Identity Provider (IDP) that you have configured for Single Sign On.

Note When you select VMwareCSP as your preferred IDP, ensure to provide your Organization ID in the following format: */csp/gateway/am/api/orgs/<full organization ID>.*

When you sign in to VMware CSP console, you can view the organization ID you are logged into by clicking on your username. A shortened version of the ID is displayed under the organization name. Click the ID to display the full organization ID.

You can also manually configure your own IDPs by selecting **Others** from the **Identity Provider template** drop-down menu.

5 In the **OIDC well-known config URL** text box, 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`

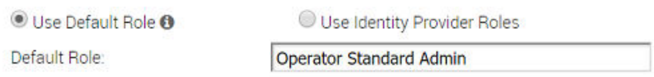
6 The SD-WAN Orchestrator application auto-populates endpoint details such as Issuer, Authorization Endpoint, Token Endpoint, and User Information Endpoint for your IDP.

7 In the **Client Id** text box, enter the client identifier provided by your IDP.

8 In the **Client Secret** text box, enter the client secret code provided by your IDP, that is used by the client to exchange an authorization code for a token.

9 To determine user's role in SD-WAN Orchestrator, select one of the options:

- **Use Default Role** – Allows user to configure a static role as default by using the **Default Role** text box that appears on selecting this option. The supported roles are: Operator Superuser, Operator Standard Admin, Operator Support, and Operator Business.

  ● Use Default Role ○ Use Identity Provider Roles

  Default Role: Operator Standard Admin

  Note In an SSO configuration setup, if **Use Default Role** option is selected and a default user role is defined, then all the SSO user will be assigned the specified default role. Instead of assigning a user with the default role, an Operator Super User can pre-register a specific user as a Non-Native user and define a specific user role by using the **Operator Users** tab. For steps to configure a new Operator User, see Create New Operator User.

- **Use Identity Provider Roles** – Uses the roles set up in the IDP.

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

11 In the **Role Map** area, map the IDP-provided roles to each of the SD-WAN Orchestrator roles, separated by using commas.

Roles in VMware CSP will follow this format: *external/<service definition uuid>/<service role name mentioned during service template creation>.*

12 Update the allowed redirect URLs in OIDC provider website with SD-WAN Orchestrator URL (`https://<vco>/login/ssologin/openidCallback`).

13 Click **Save Changes** to save the SSO configuration.

14 Click **Test Configuration** to validate the specified OpenID Connect (OIDC) configuration.

The user is navigated to the IDP website and allowed to enter the credentials. On IDP verification and successful redirect to SD-WAN Orchestrator test call back, a successful validation message appears.

Results

The SSO authentication setup is complete in SD-WAN Orchestrator.

What to do next

Chapter 6 Log in to the SD-WAN Orchestrator Using SSO for Operator User

Configure an IDP for Single Sign On

To enable Single Sign On (SSO) for SD-WAN Orchestrator, you must configure an Identity Partner (IDP) with details of SD-WAN Orchestrator. Currently, the following IDPs are supported: Okta, OneLogin, PingIdentity, AzureAD, and VMware CSP.

For step-by-step instructions to configure an OpenID Connect (OIDC) application for SD-WAN Orchestrator in various IDPs, see:

- Configure Okta for Single Sign On
- Configure OneLogin for Single Sign On
- Configure PingIdentity for Single Sign On
- Configure Azure Active Directory for Single Sign On
- Configure VMware CSP for Single Sign On

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.

Prerequisites

Ensure you have an Okta account to sign in.

Procedure

1 Log in to your Okta account as an Admin user.

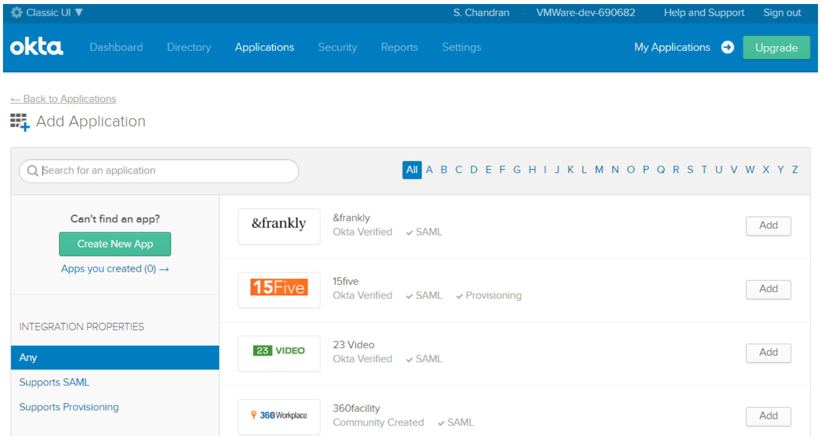
The **Okta** home screen appears.

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

2 To create a new application:

a In the upper navigation bar, click **Applications** > **Add Application**.

The **Add Application** screen appears.



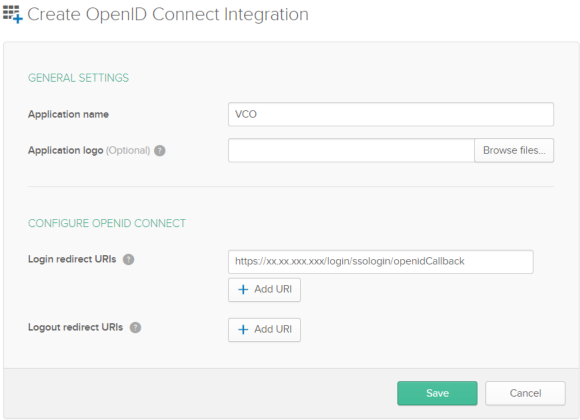
b Click **Create New App**.

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

GENERAL SETTINGS

Application name: VCO

Application logo (Optional)

CONFIGURE OPENID CONNECT

Login redirect URIs: https://xx.xx.xxx.xxx/login/ssologin/openidCallback

Logout redirect URIs

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

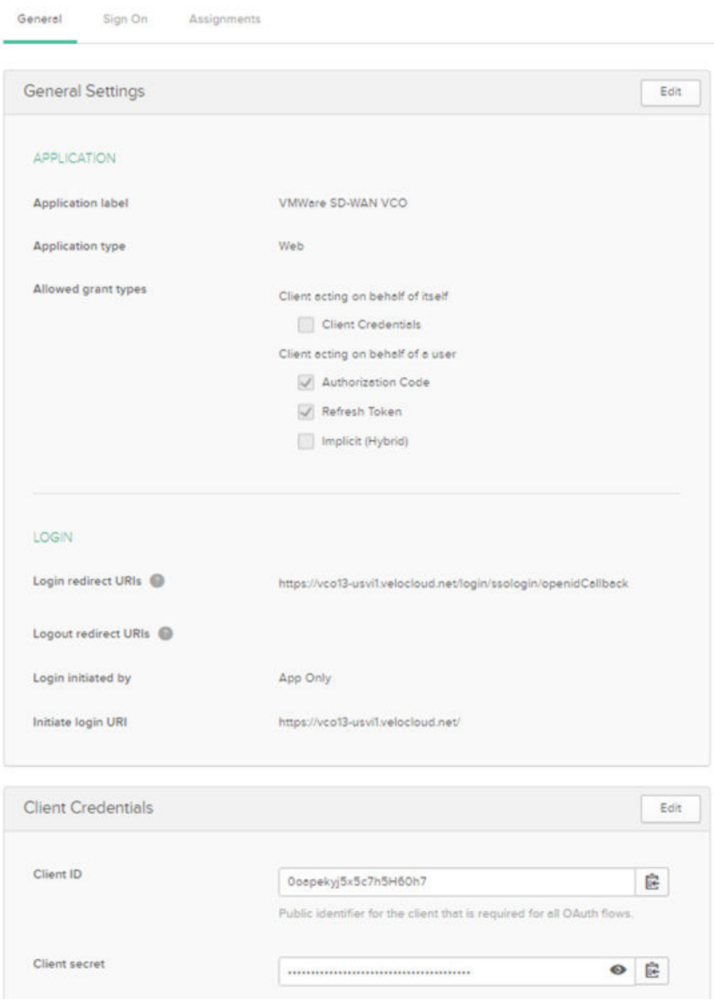
f Under the **CONFIGURE OPENID CONNECT** area, in the **Login redirect URIs** text box, enter the redirect URL that your SD-WAN Orchestrator application uses as the callback endpoint.

In the SD-WAN Orchestrator application, at the bottom of the **Configure Authentication** screen, you can find the redirect URL link. Ideally, the SD-WAN Orchestrator 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 SD-WAN Orchestrator.



General Settings

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-usvi1.velocloud.net/login/ssologin/openidCallback

Logout redirect URIs:

Login initiated by: App Only

Initiate login URI: https://vco13-usvi1.velocloud.net/

Client Credentials

Client ID: 0oapekyj5x5c7h5H60h7

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

Client secret: ••

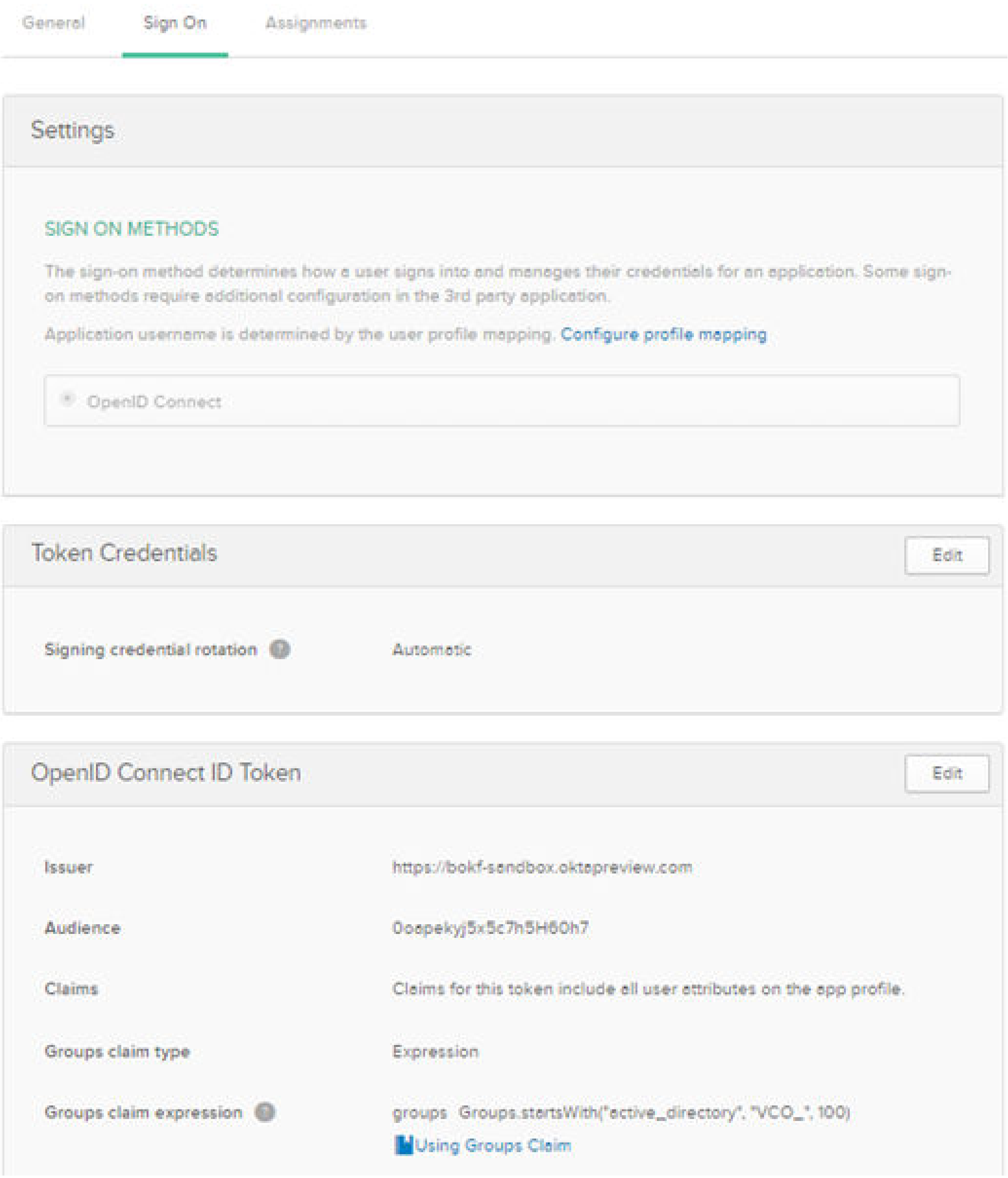
i Click the **Sign On** tab and under the **OpenID Connect ID Token** area, click **Edit**.

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 SD-WAN Orchestrator application.



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

Signing credential rotation	Automatic

OpenID Connect ID Token

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

3 To assign groups and users to your SD-WAN Orchestrator application:

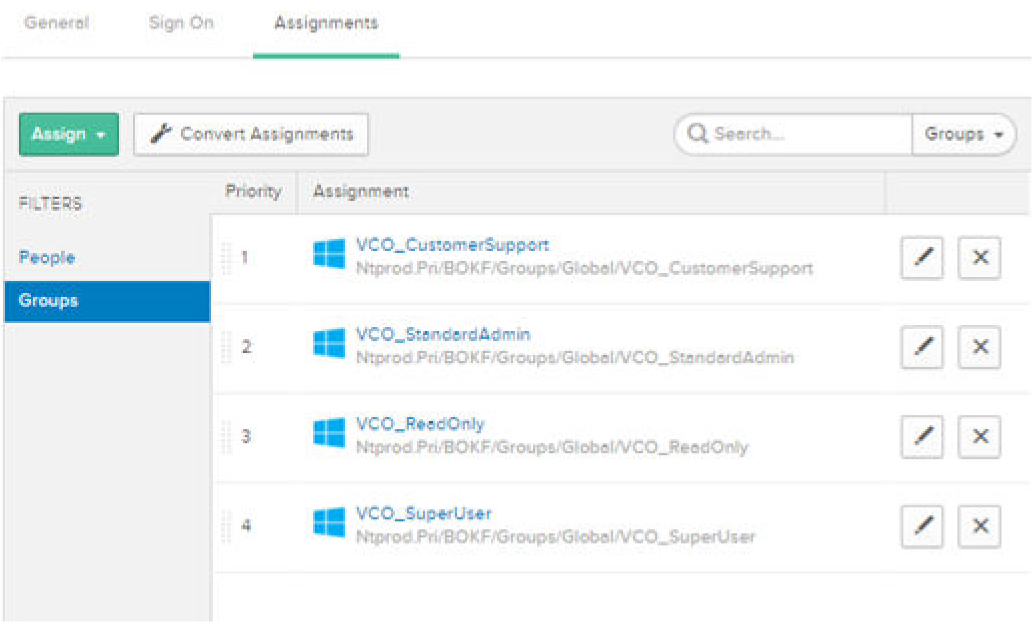
   a Go to **Application** > **Applications** and click on your SD-WAN Orchestrator application link.

   b On the **Assignments** tab, from the **Assign** drop-down menu, select **Assign to Groups** or **Assign to People**.

   The **Assign <Application Name> to Groups** or **Assign <Application Name> to People** dialog box appears.

   c Click **Assign** next to available user groups or users you want to assign the SD-WAN Orchestrator application and click **Done**.

   The users or user groups assigned to the SD-WAN Orchestrator application will be displayed.



Priority	Assignment
1	VCO_CustomerSupport Ntprod.Pri/BOKF/Groups/Global/VCO_CustomerSupport
2	VCO_StandardAdmin Ntprod.Pri/BOKF/Groups/Global/VCO_StandardAdmin
3	VCO_ReadOnly Ntprod.Pri/BOKF/Groups/Global/VCO_ReadOnly
4	VCO_SuperUser Ntprod.Pri/BOKF/Groups/Global/VCO_SuperUser

Results

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

What to do next

Configure Single Sign On in SD-WAN Orchestrator.

Create a New User Group in Okta

To create a new user group, perform the steps on this procedure.

Procedure

1 Click **Directory** > **Groups**.

2 Click **Add Group**.

   The **Add Group** dialog box appears.

3 Enter the group name and description for the group and click **Save**.

Create a New User in Okta

To add a new user, perform the steps on this procedure.

Procedure

1 Click **Directory** > **People**.

2 Click **Add Person**.

The **Add Person** dialog box appears.

3 Enter all the mandatory details such as first name, last name, and email ID of the user.

4 If you want to set the password, select **Set by user** from the **Password** drop-down menu and enable **Send user activation email now**.

5 Click **Save**.

An activation link email will be sent your email ID. Click the link in the email to activate your Okta user account.

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 on this procedure.

Prerequisites

Ensure you have an OneLogin account to sign in.

Procedure

1 Log in to your OneLogin account as an Admin user.

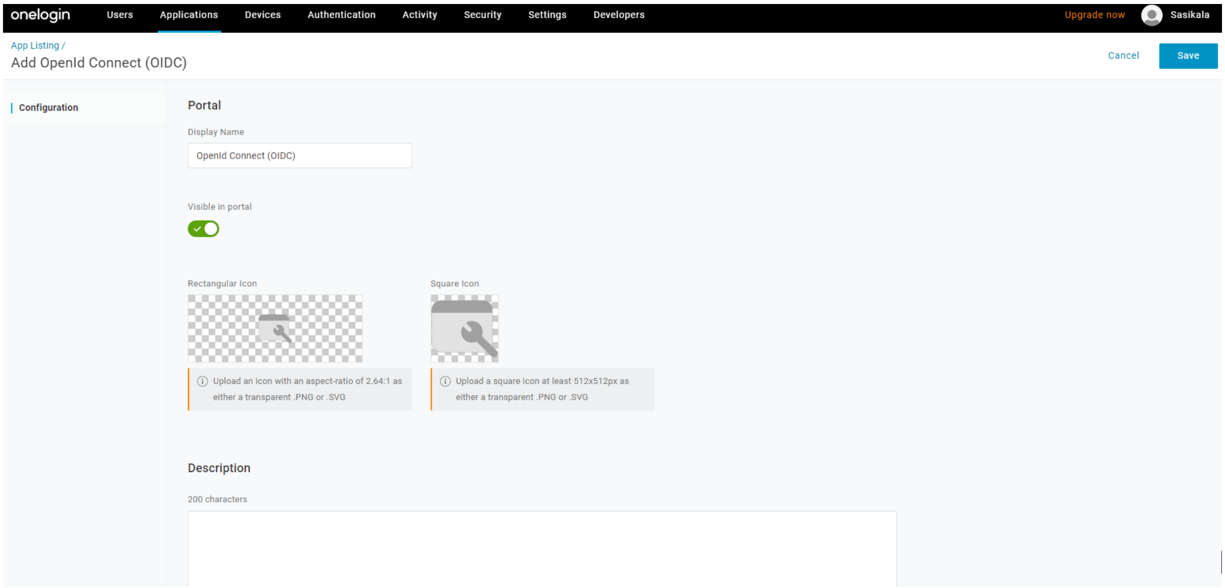
The **OneLogin** home screen appears.

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.



Add OpenId Connect (OIDC)

Portal

Display Name

OpenId Connect (OIDC)

Visible in portal

Rectangular Icon

Upload an icon with an aspect-ratio of 2.64:1 as either a transparent .PNG or .SVG

Square Icon

Upload a square icon at least 512x512px as either a transparent .PNG or .SVG

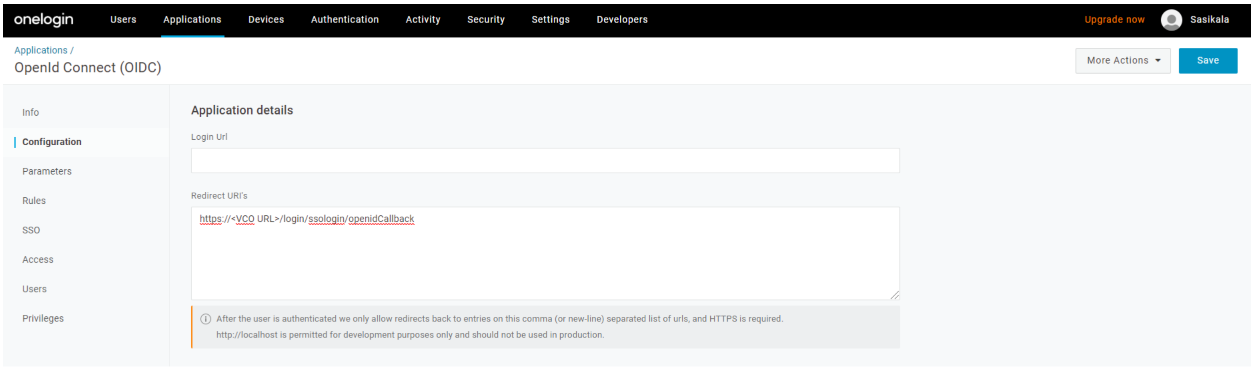
Description

200 characters

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

d On the **Configuration** tab, enter the redirect URI that SD-WAN Orchestrator uses as the callback endpoint and click **Save**.

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



OpenId Connect (OIDC)

Application details

Login Url

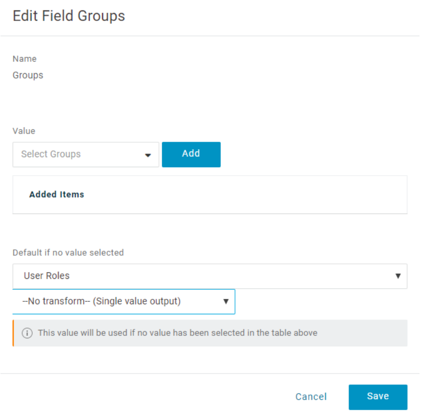
Redirect URI's

https://<VCO URL>/login/ssologin/openidCallback

After the user is authenticated we only allow redirects back to entries on this comma (or new-line) separated list of urls, and HTTPS is required. http://localhost is permitted for development purposes only and should not be used in production.

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

The **Edit Field Groups** popup appears.



Edit Field Groups

Name
Groups

Value
Select Groups

Added Items

Default if no value selected
User Roles
--No transform-- (Single value output)

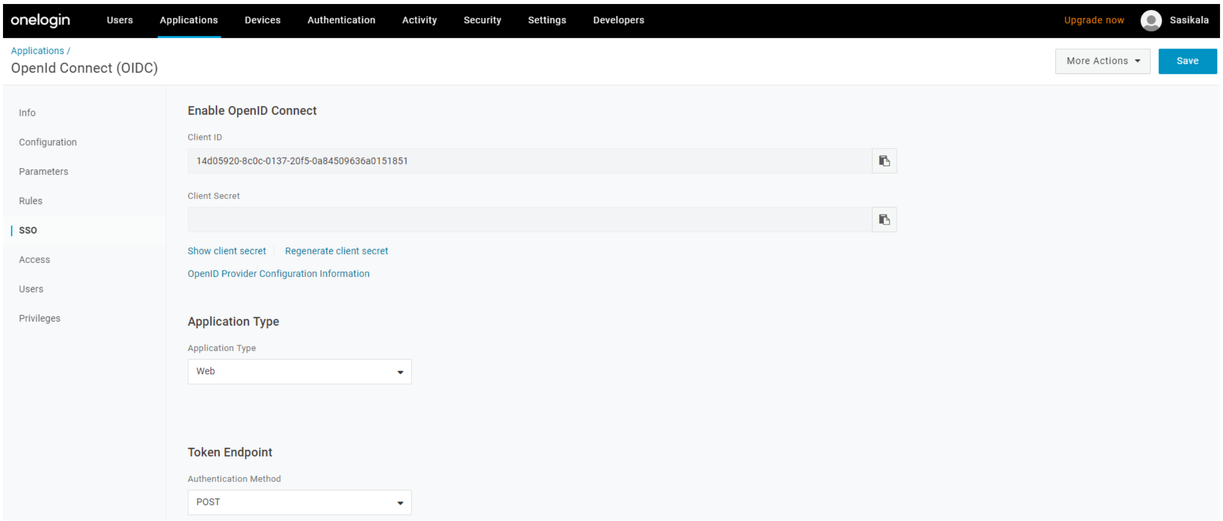
This value will be used if no value has been selected in the table above

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 SD-WAN Orchestrator.



Applications /
OpenId Connect (OIDC)

Enable OpenID Connect

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

Client Secret

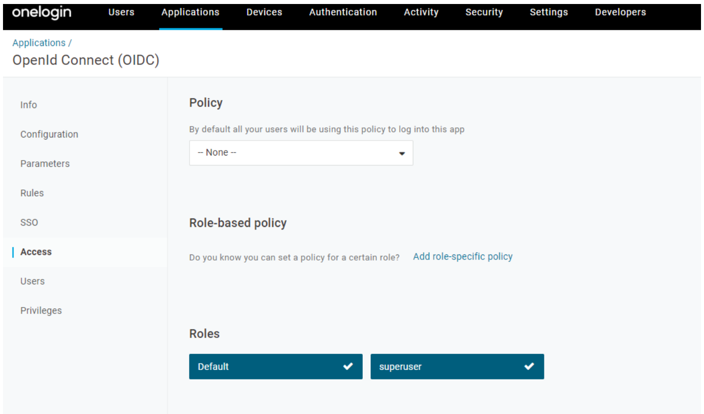
Application Type

Application Type
Web

Token Endpoint

Authentication Method
POST

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



Applications /
OpenId Connect (OIDC)

Policy

By default all your users will be using this policy to log into this app
-- None --

Role-based policy

Do you know you can set a policy for a certain role?

Roles

Default ✓
superuser ✓

3 To add roles and users to your SD-WAN Orchestrator application:

a Click **Users** > **Users** and select a user.

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

c Click **Save Users**.

Results

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

What to do next

Configure Single Sign On in SD-WAN Orchestrator.

Create a New Role in OneLogin

To create a new role, perform the steps on this procedure.

Procedure

1 Click **Users** > **Roles**.

2 Click **New Role**.

3 Enter a name for the role.

When you first set up a role, the **Applications** tab displays all the apps in your company catalog.

4 Click an application to select it and click **Save** to add the selected apps to the role.

Create a New User in OneLogin

To create a new user, perform the steps on this procedure.

Procedure

1 Click **Users** > **Users** > **New User**.

The **New User** screen appears

2 Enter all the mandatory details such as first name, last name, and email ID of the user and click **Save User**.

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.

Prerequisites

Ensure you have a PingOne account to sign in.

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

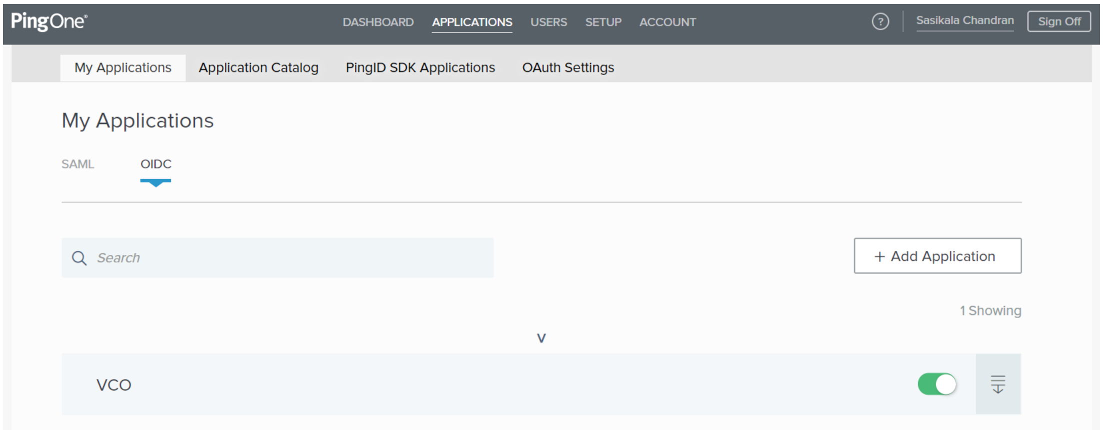
Procedure

1 Log in to your PingOne account as an Admin user.

The **PingOne** home screen appears.

2 To create a new application:

a In the upper navigation bar, click **Applications**.



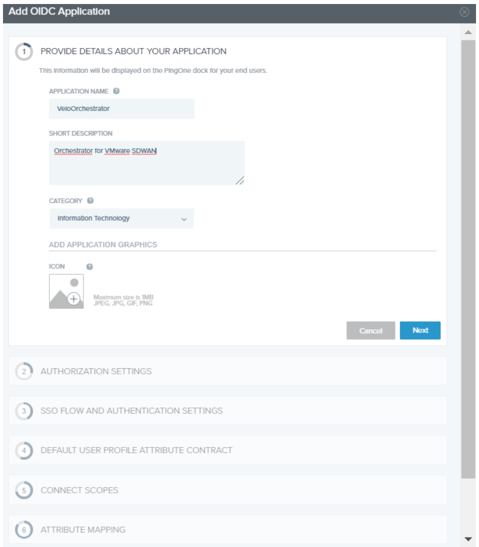
My Applications

1 Showing

VCO

b On the **My Applications** tab, select **OIDC** and then click **Add Application**.

The **Add OIDC Application** pop-up window appears.



1 PROVIDE DETAILS ABOUT YOUR APPLICATION

This information will be displayed on the PingOne dock for your end users.

APPLICATION NAME: VeloOrchestrator

SHORT DESCRIPTION: Orchestrator for VMware SDWAN

CATEGORY: Information Technology

ADD APPLICATION GRAPHICS

ICON

Maximum size is 1MB
JPEG, JPG, GIF, PNG

2 AUTHORIZATION SETTINGS

3 SSO FLOW AND AUTHENTICATION SETTINGS

4 DEFAULT USER PROFILE ATTRIBUTE CONTRACT

5 CONNECT SCOPES

6 ATTRIBUTE MAPPING

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 SD-WAN Orchestrator.

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

In the SD-WAN Orchestrator application, at the bottom of the **Configure Authentication** screen, you can find the redirect URL link. Ideally, the SD-WAN Orchestrator redirect URL will be in this format: https://<Orchestrator URL>/login/ssologin/openidCallback. The Start SSO URL will be in this format: https://<vco>/<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 SD-WAN Orchestrator application during authentication and click **Next**.

i Under **Attribute Mapping**, map your identity repository attributes to the claims available to your SD-WAN Orchestrator application.

Note The minimum required mappings for the integration to work are email, given_name, family_name, phone_number, sub, and group_membership (mapped to memberOf).

j Under **Group Access**, select all user groups that should have access to your SD-WAN Orchestrator application and click **Done**.

The application will be added to your account and will be available in the **My Application** screen.

Results

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

What to do next

Configure Single Sign On in SD-WAN Orchestrator.

Create a New User Group in PingIdentity

To create a new user group, perform the steps on this procedure.

Procedure

1 Click **Users** > **User Directory**.

2 On the **Groups** tab, click **Add Group**

The **New Group** screen appears.

3 In the **Name** text box, enter a name for the group and click **Save**.

Create a New User in PingIdentity

To add a new user, perform the steps on this procedure.

Procedure

1. Click **Users** > **User Directory**.
2. On the **Users** tab, click the **Add Users** drop-down menu and select **Create New User**.

   The **User** screen appears.
3. Enter all the mandatory details such as username, password, and email ID of the user.
4. Under **Group Memberships**, click **Add**.

   The **Add Group Membership** pop-up window appears.
5. Search and add the user to a group and click **Save**.

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 steps on this procedure.

Prerequisites

Ensure you have an AzureAD account to sign in.

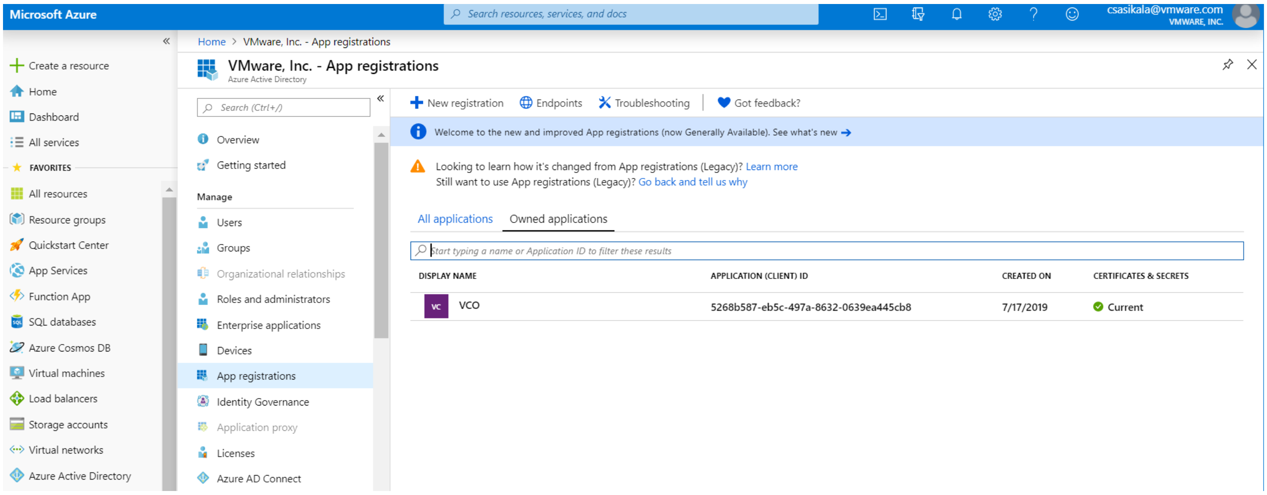
Procedure

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.



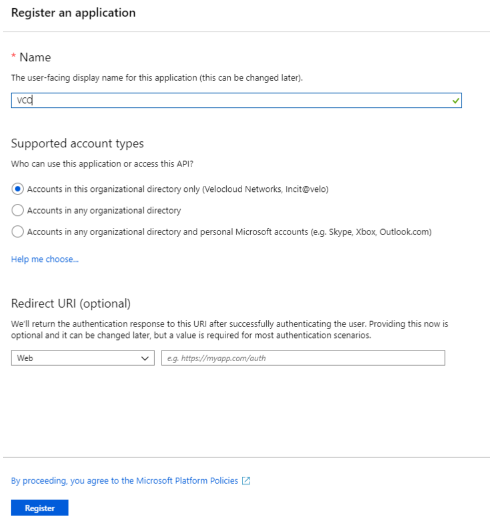
Welcome to the new and improved App registrations (now Generally Available). See what's new →

Looking to learn how it's changed from App registrations (Legacy)? Learn more
Still want to use App registrations (Legacy)? Go back and tell us why

DISPLAY NAME	APPLICATION (CLIENT) ID	CREATED ON	CERTIFICATES & SECRETS
VC VCO	5268b587-eb5c-497a-8632-0639ea445cb8	7/17/2019	✓ Current

   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).

vcc

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Velocloud Networks, Incit@velo)

○ Accounts in any organizational directory

○ Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)

Help me choose...

Redirect URI (optional)

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

Web | e.g. https://myapp.com/auth

By proceeding, you agree to the Microsoft Platform Policies

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

   d In the **Redirect URL** field, enter the redirect URL that your SD-WAN Orchestrator application uses as the callback endpoint.

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

e Click **Register**.

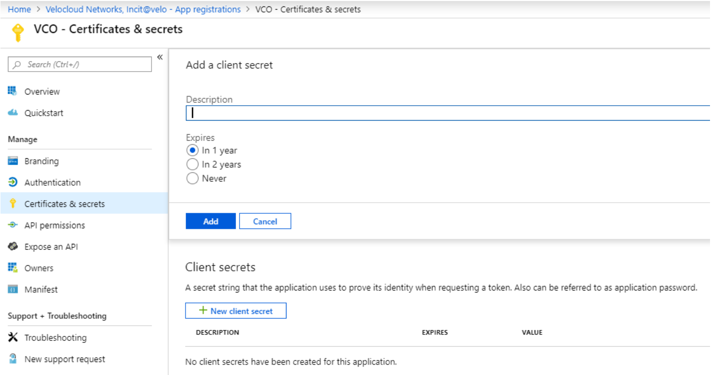
Your SD-WAN Orchestrator application will be registered and displayed in the **All applications** and **Owned applications** tabs. Make sure to note down the Client ID/ Application ID to be used during the SSO configuration in SD-WAN Orchestrator.

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

g To create a client secret for your SD-WAN Orchestrator application, on the **Owned applications** tab, click on your SD-WAN Orchestrator application.

h Go to **Certificates & secrets** > **New client secret**.

The **Add a client secret** screen appears.



Add a client secret

Description

Expires

● In 1 year

○ In 2 years

○ Never

Client secrets

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

DESCRIPTION	EXPIRES	VALUE

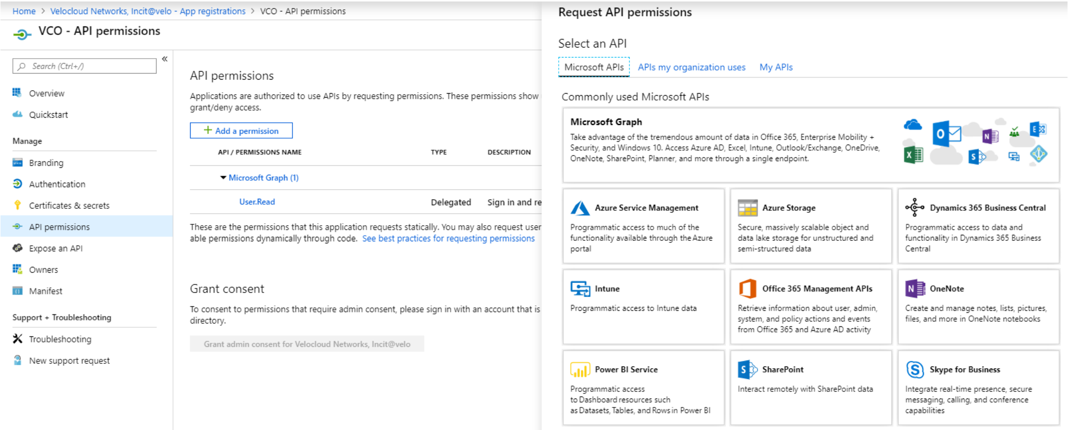
No client secrets have been created for this application.

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

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

j To configure permissions for your SD-WAN Orchestrator application, click on your SD-WAN Orchestrator application and go to **API permissions** > **Add a permission**.

The **Request API permissions** screen appears.



API permissions

Applications are authorized to use APIs by requesting permissions. These permissions show grant/deny access.

API / PERMISSIONS NAME	TYPE	DESCRIPTION
▾ Microsoft Graph (1)		
User.Read	Delegated	Sign in and re

These are the permissions that this application requests statically. You may also request user able permissions dynamically through code. See best practices for requesting permissions

Grant consent

To consent to permissions that require admin consent, please sign in with an account that is directory.

Request API permissions

Select an API

Commonly used Microsoft APIs

Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure Service Management
Programmatic access to much of the functionality available through the Azure portal

Azure Storage
Secure, massively scalable object and data lake storage for unstructured and semi-structured data

Dynamics 365 Business Central
Programmatic access to data and functionality in Dynamics 365 Business Central

Intune
Programmatic access to Intune data

Office 365 Management APIs
Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity

OneNote
Create and manage notes, lists, pictures, files, and more in OneNote notebooks

Power BI Service
Programmatic access to Dashboard resources such as Datasets, Tables, and Rows in Power BI

SharePoint
Interact remotely with SharePoint data

Skype for Business
Integrate real-time presence, secure messaging, calling, and conference capabilities

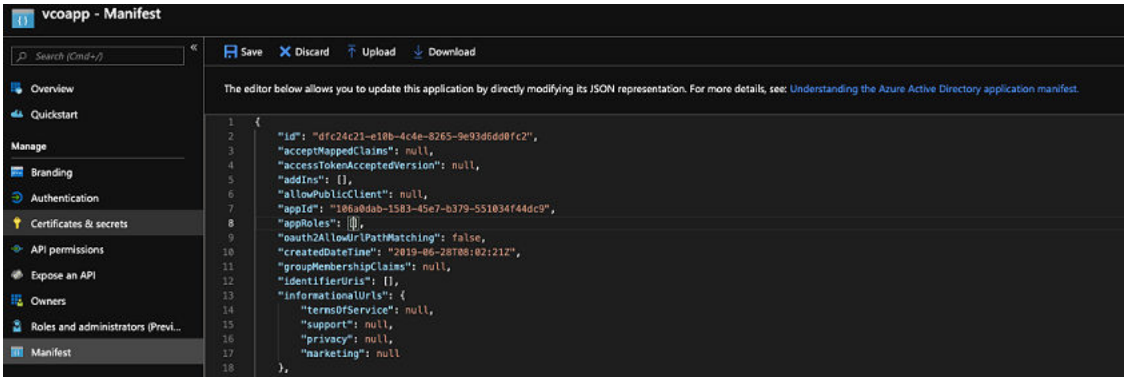
k Click **Microsoft Graph** and select **Application permissions** as the type of permission for your application.

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 SD-WAN Orchestrator 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.



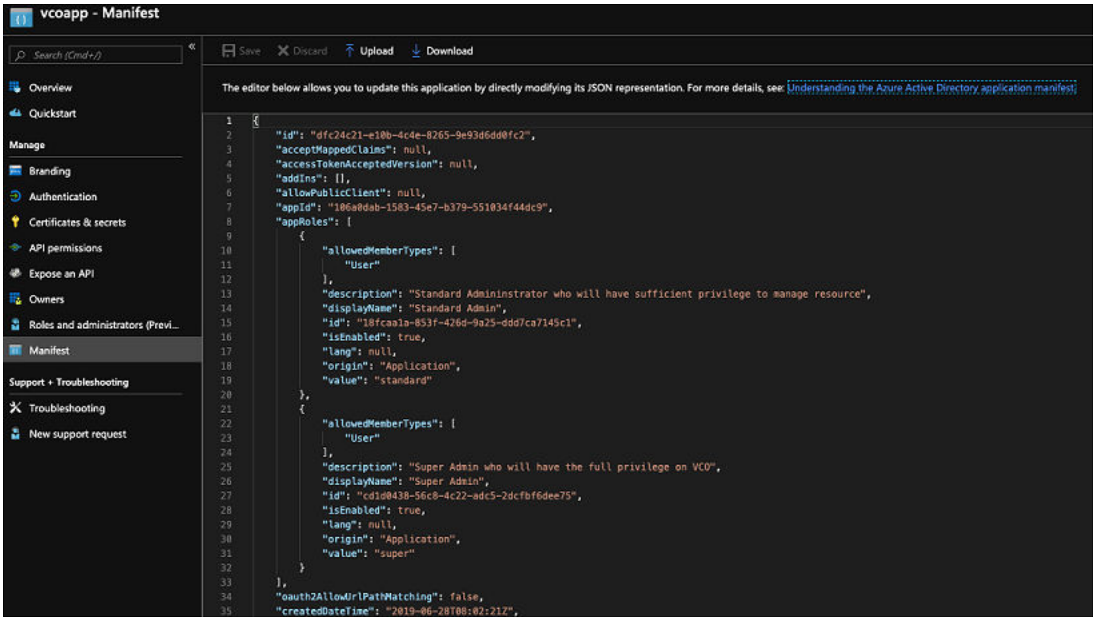
The editor below allows you to update this application by directly modifying its JSON representation. For more details, see: Understanding the Azure Active Directory application manifest.

```
{
    "id": "dfc24c21-e10b-4c4e-8265-9e93d6dd0fc2",
    "acceptMappedClaims": null,
    "accessTokenAcceptedVersion": null,
    "addIns": [],
    "allowPublicClient": null,
    "appId": "106a0dab-1583-45e7-b379-551034f44dc9",
    "appRoles": [],
    "oauth2AllowUrlPathMatching": false,
    "createdDateTime": "2019-06-28T08:02:21Z",
    "groupMembershipClaims": null,
    "identifierUris": [],
    "informationalUrls": {
        "termsOfService": null,
        "support": null,
        "privacy": null,
        "marketing": null
    },
```

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**.

Sample role objects

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



The editor below allows you to update this application by directly modifying its JSON representation. For more details, see: Understanding the Azure Active Directory application manifest.

```
{
    "id": "dfc24c21-e10b-4c4e-8265-9e93d6dd0fc2",
    "acceptMappedClaims": null,
    "accessTokenAcceptedVersion": null,
    "addIns": [],
    "allowPublicClient": null,
    "appId": "106a0dab-1583-45e7-b379-551034f44dc9",
    "appRoles": [
        {
            "allowedMemberTypes": [
                "User"
            ],
            "description": "Standard Admininstrator who will have sufficient privilege to manage resource",
            "displayName": "Standard Admin",
            "id": "18fcaa1a-853f-426d-9a25-ddd7ca7145c1",
            "isEnabled": true,
            "lang": null,
            "origin": "Application",
            "value": "standard"
        },
        {
            "allowedMemberTypes": [
                "User"
            ],
            "description": "Super Admin who will have the full privilege on VCO",
            "displayName": "Super Admin",
            "id": "cd1d0438-56c8-4c22-adc5-2dcfbf6dee75",
            "isEnabled": true,
            "lang": null,
            "origin": "Application",
            "value": "super"
        }
    ],
    "oauth2AllowUrlPathMatching": false,
    "createdDateTime": "2019-06-28T08:02:21Z",
```

Note Make sure to set `id` to a newly generated GUID value.

3 To assign groups and users to your SD-WAN Orchestrator application:

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

   b Search and select your SD-WAN Orchestrator application.

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

   d Click **Submit**.

Results

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

What to do next

Configure Single Sign On in SD-WAN Orchestrator.

Create a New Guest User in AzureAD

To create a new guest user, perform the steps on this procedure.

Procedure

1 Go to **Azure Active Directory** > **Users** > **All users**.

2 Click **New guest user**.

   The **New Guest User** pop-up window appears.

3 In the **Email address** text box, enter the email address of the guest user and click **Invite**.

   The guest user immediately receives a customizable invitation that lets them to sign into their Access Panel.

4 Guest users in the directory can be assigned to apps or groups.

Configure VMware CSP for Single Sign On

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

Prerequisites

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

Procedure

1 Contact the VMware Support Provider for receiving a Service invitation URL link to register your SD-WAN Orchestrator application to VMware CSP. For information on how to contact the Support Provider, see https://kb.vmware.com/s/article/53907 and https://www.vmware.com/support/contacts/us_support.html.

   The VMware Support Provider will create and share:

   - a Service invitation URL that needs to be redeemed to your Customer organization
   - a Service definition uuid and Service role name to be used for Role mapping in Orchestrator

2 Redeem the Service invitation URL to your existing Customer Organization or create a new Customer Organization by following the steps in the UI screen.

   You need to be a Organization Owner to redeem the Service invitation URL to your existing Customer Organization.

3 After redeeming the Service invitation, when you sign in to VMware CSP console, you can view your application tile under **My Services** area in the **Vmware Cloud Services** page.

   The Organization you are logged into is displayed under your username on the menu bar. Make a note of the Organization ID by clicking on your username, to be used during Orchestrator configuration. A shortened version of the ID is displayed under the Organization name. Click the ID to display the full Organization ID.

4 Log in to VMware 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 VMware CSP console, make a note of IDP integration details such as Client ID and Client Secret. These details will be needed for SSO configuration in Orchestrator.

5 Log in to your SD-WAN Orchestrator 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 SD-WAN Orchestrator, you must set up the domain name for your enterprise.

   c Click the **Authentication** tab and from the **Authentication Mode** drop-down menu, select **SSO**.

   d From the **Identity Provider template** drop-down menu, select **VMwareCSP**.

   e In the **Organization Id** text box, enter the Organization ID (that you have noted down in Step 3) in the following format: */csp/gateway/am/api/orgs/<full organization ID>*.

   f In the **OIDC well-known config URL** text box, enter the OpenID Connect (OIDC) configuration URL (https://console.cloud.vmware.com/csp/gateway/am/api/.well-known/openid-configuration) for your IDP.

     The SD-WAN Orchestrator 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 SD-WAN Orchestrator, select either **Use Default Role** or **Use Identity Provider Roles**.

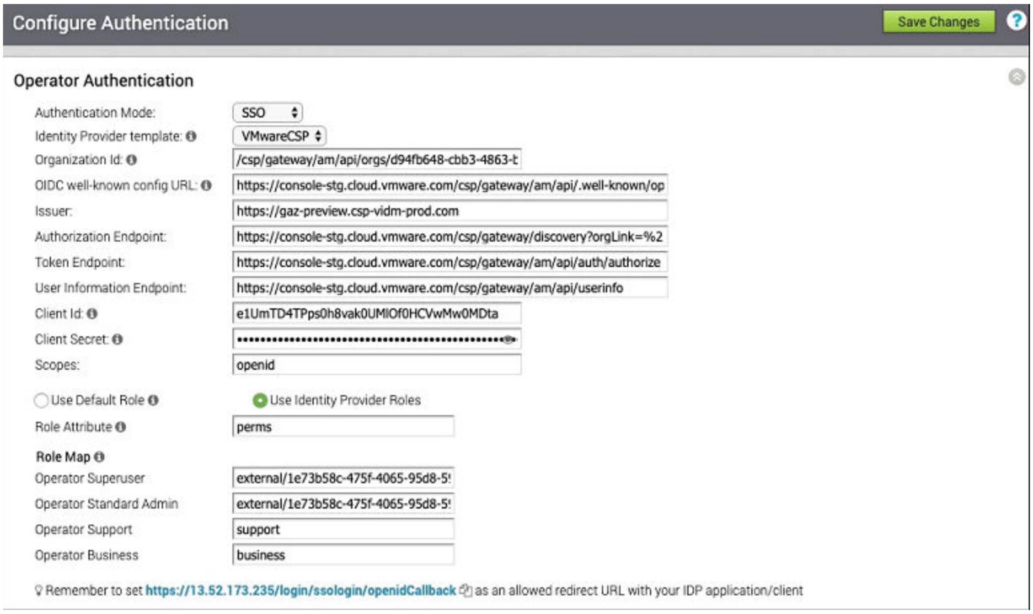
   j On selecting the **Use Identity Provider Roles** option, in the **Role Attribute** text box, enter the name of the attribute set in the VMware CSP to return roles.

   k In the **Role Map** area, map the VMwareCSP-provided roles to each of the SD-WAN Orchestrator roles, separated by using commas.

     Roles in VMware 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.



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 Superuser	external/1e73b58c-475f-4065-95d8-5!
Operator Standard Admin	external/1e73b58c-475f-4065-95d8-5!
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 VMware CSP website and allowed to enter the credentials. On IDP verification and successful redirect to SD-WAN Orchestrator test call back, a successful validation message will be displayed.

Results

You have completed integrating SD-WAN Orchestrator application in VMware CSP for SSO and can access the SD-WAN Orchestrator application logging in to the VMware CSP console.

What to do next

- 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 Vmware Cloud documentation.

Upgrade SD-WAN Orchestrator with DR Deployment

18

This section describes how to upgrade the SD-WAN Orchestrator with DR deployment.

This chapter includes the following topics:

SD-WAN Orchestrator Upgrade Overview

The following steps are required to upgrade a SD-WAN Orchestrator.

For SD-WAN Orchestrator Disaster Recovery, see " Set Up DR in the VMware" and " Upgrade the DR Setup."

1. Step 1: Prepare for the Orchestrator Upgrade
2. Step 2: Send Upgrade Announcement
3. Step 3: Proceed with the SD-WAN Orchestrator upgrade
4. Step 4: Complete the Orchestrator Upgrade

Upgrade an Orchestrator

This section describes how to upgrade an Orchestrator.

Step 1: Prepare for the Orchestrator Upgrade

Contact the VMware SD-WAN by VeloCloud Support team to prepare for the SD-WAN Orchestrator upgrade as described in this section.

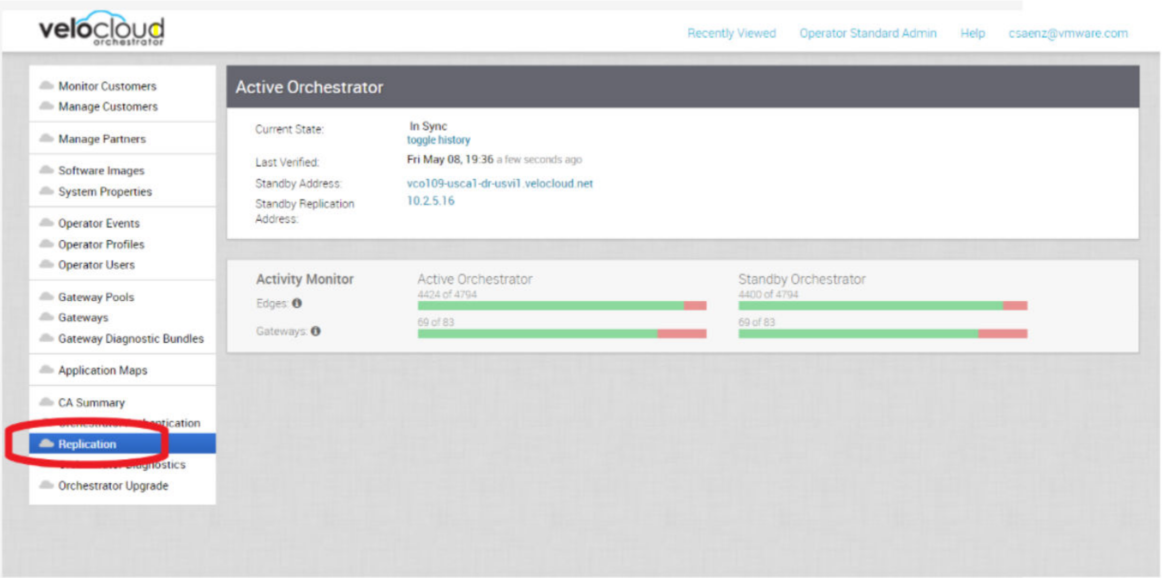
To upgrade SD-WAN Orchestrator:

1 VMware SD-WAN by VeloCloud Support will assist you with your upgrade. Collect the following information prior to contacting Support.

   - Provide the current and target SD-WAN 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 SD-WAN Orchestrator by clicking the **Help** link and choosing **About**.

   - Provide a screenshot of the replication dashboard of the SD-WAN Orchestrator as shown below.



Active Orchestrator

Current State: In Sync
toggle history

Last Verified: Fri May 08, 19:36 a few seconds ago

Standby Address: vco109-usca1-dr-usvi1.velocloud.net

Standby Replication Address: 10.2.5.16

Activity Monitor	Active Orchestrator	Standby Orchestrator
Edges: ❶	4424 of 4794	4400 of 4794
Gateways: ❶	69 of 83	69 of 83

   - Hypervisor Type and version (ie vSphere 6.7)

   - Commands from the SD-WAN 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 VMware SD-WAN Orchestrator Support at https://kb.vmware.com/s/article/53907 with the above-mentioned information for assistance with the SD-WAN Orchestrator upgrade.

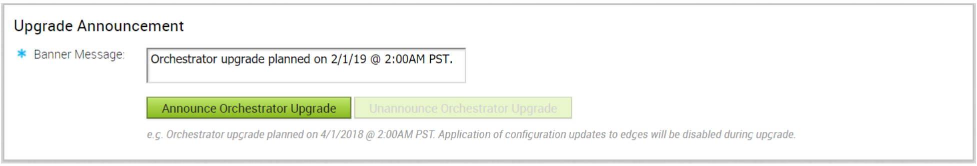
Step 2: Send Upgrade Announcement

The **Upgrade Announcement** area enables you to configure and send a message about an upcoming upgrade. This message will be displayed to all users the next time they login to the SD-WAN Orchestrator.

To send an upgrade announcement:

1 From the SD-WAN Orchestrator, select **Orchestrator Upgrade** from the navigation panel.

2 In the **Upgrade Announcement** area, type in your message in the **Banner Message** text box.



Upgrade Announcement

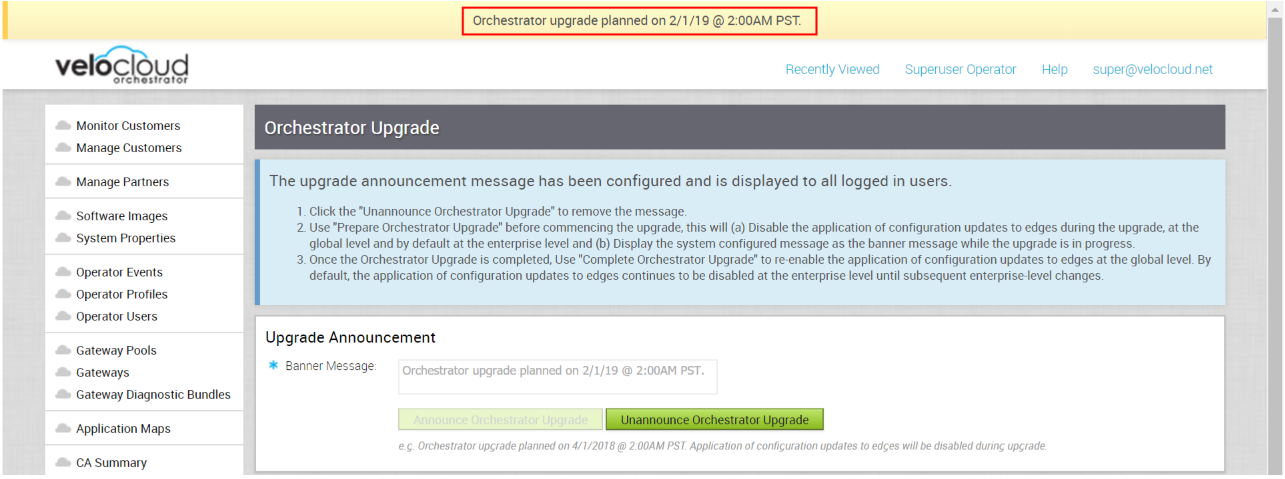
* Banner Message: Orchestrator upgrade planned on 2/1/19 @ 2:00AM PST.

e.g. Orchestrator upgrade planned on 4/1/2018 @ 2:00AM PST. Application of configuration updates to edges will be disabled during upgrade.

Announce Orchestrator Upgrade
Unannounce Orchestrator Upgrade

3 Click the **Announce Orchestrator Upgrade** button.

A popup message appears indicating that you have successfully created your announcement, and that your banner message displays at the top of the SD-WAN Orchestrator.



Orchestrator upgrade planned on 2/1/19 @ 2:00AM PST.

The upgrade announcement message has been configured and is displayed to all logged in users.

1. Click the "Unannounce Orchestrator Upgrade" to remove the message.
2. Use "Prepare Orchestrator Upgrade" before commencing the upgrade, this will (a) Disable the application of configuration updates to edges during the upgrade, at the global level and by default at the enterprise level and (b) Display the system configured message as the banner message while the upgrade is in progress.
3. Once the Orchestrator Upgrade is completed, Use "Complete Orchestrator Upgrade" to re-enable the application of configuration updates to edges at the global level. By default, the application of configuration updates to edges continues to be disabled at the enterprise level until subsequent enterprise-level changes.

Upgrade Announcement

* Banner Message: Orchestrator upgrade planned on 2/1/19 @ 2:00AM PST.

e.g. Orchestrator upgrade planned on 4/1/2018 @ 2:00AM PST. Application of configuration updates to edges will be disabled during upgrade.

Announce Orchestrator Upgrade
Unannounce Orchestrator Upgrade

4. (Optional) You can remove the announcement from the SD-WAN Orchestrator by clicking the **Unannounce Orchestrator Upgrade** button. A popup message will appear indicating that you have successfully unannounced the Orchestrator upgrade. The announcement that was displayed at the top of the SD-WAN Orchestrator will be removed.

Step 3: Proceed with the SD-WAN Orchestrator Upgrade

Contact VMware SD-WAN by VeloCloud Support at `https://kb.vmware.com/s/article/53907` for assistance with the VMware SD-WAN Orchestrator upgrade.

Step 4: Complete the Orchestrator Upgrade

After you have completed the Orchestrator upgrade, click the **Complete Orchestrator Upgrade** button. This re-enables the application of the configuration updates of Edges at the global level.

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, the same version number should display at the bottom right corner of the SD-WAN Orchestrator.

SD-WAN Orchestrator Disaster Recovery

This section describes how to set up and upgrade disaster recovery in the SD-WAN Orchestrator.

Set Up DR in the VMware

To set up disaster recovery in the SD-WAN Orchestrator:

1. Install a new SD-WAN Orchestrator whose version matches the version of the VMware that is currently the Active SD-WAN Orchestrator.
2. Set the following properties on the Active and Standby SD-WAN Orchestrator, if necessary.
   - `vco.disasterRecovery.transientErrorToleranceSecs` to a non-zero value (Defaults to 900 seconds in version 3.3 and later, zero in earlier versions). This prevents any transient errors from resulting in an Edge/Gateway management plane update.
   - `vco.disasterRecovery.mysqlExpireLogsDays` (Defaults to 1 day). This is the amount of time the Active SD-WAN Orchestrator keeps the mysql binlog data.
3. Set up the `network.public.address` property on the Active and Standby to the address contacted by the Edges (Heartbeats).
4. Set up DR by following the usual DR Setup procedure that is described in *SD-WAN Orchestrator Disaster Recovery*.

Upgrade the DR Setup

To upgrade a DR-enabled SD-WAN Orchestrator pair, follow the steps below.

To upgrade a DR-enabled VCO pair:

Note If the SD-WAN Orchestrator upgrade is from 2.X -> 3.2.X, run dr-standby-schema.sh on the Standby before starting the upgrade.

1 Prepare for the Upgrade. For instructions, go to Step 1: Prepare for the Orchestrator Upgrade of the section titled, Upgrade an Orchestrator with DR Deployment.

2 Proceed with the SD-WAN Orchestrator Upgrade. For instructions, go to Step 3: Proceed with the SD-WAN Orchestrator Upgrade of the section titled, Upgrade an Orchestrator with DR Deployment.

Configure SD-WAN Orchestrator Disaster Recovery 19

This section provides disaster recovery (DR) instructions for SD-WAN Orchestrator.

This chapter includes the following topics:

SD-WAN Orchestrator Disaster Recovery Overview

The SD-WAN Orchestrator Disaster Recovery (DR) feature prevents the loss of stored data and resumes SD-WAN Orchestrator services in the event of system or network failure.

SD-WAN Orchestrator DR involves setting up an active/standby SD-WAN Orchestrator pair with data replication and a manually-triggered failover mechanism.

- The recovery time objective (RTO), therefore, is dependent on explicit action by the operator to trigger promotion of the standby.
- The recovery point objective (RPO), however, is essentially zero, regardless of the recovery time, because all configuration is instantaneously replicated. Monitoring data that would have been collected during the outage is cached on the edges and gateways pending promotion of the standby.

Note DR is mandatory. For licensing and pricing, contact the VMware sales team for support.

Active/Standby Pair

In a SD-WAN Orchestrator DR deployment, two identical SD-WAN Orchestrator systems are configured as an active / standby pair. The operator can view the state of DR readiness through the web UI on either of the servers. Edges and gateways are aware of both SD-WAN Orchestrators, and while they receive configuration changes only from the active SD-WAN Orchestrator, they periodically send DR heartbeats to both systems to report their view of both servers and to query the DR system status. When the operator triggers a failover, the edges and gateways are informed of the change in their next DR heartbeat.

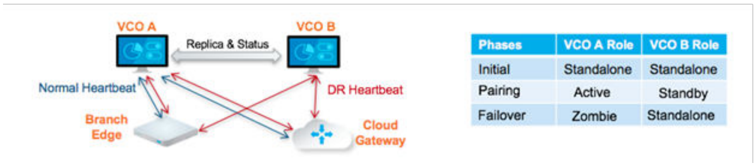
DR States

From the view of an operator, and of the edges and gateways, a SD-WAN Orchestrator has one of four DR states:

DR State	Description
Standalone	No DR configured.
Active	DR configured, acting as the primary SD-WAN Orchestrator server.
Standby	DR configured, acting as an inactive replica SD-WAN Orchestrator server.
Zombie	DR formerly configured and active but no longer acting as the active or standby.

Run-time Operation

When DR is configured, the standby server runs in a limited mode, blocking all API calls except those related to the DR status and the DR heartbeats. When the operator invokes a failover, the standby is promoted to become fully operational as a Standalone server. The server that was formerly active is automatically transitioned to a Zombie state if it is responsive and visible from the promoted standby. In the Zombie state, management configuration services are blocked and any contact from edges and gateways that have not transitioned to the new active SD-WAN Orchestrator are redirected to the promoted server.



Phases	VCO A Role	VCO B Role
Initial	Standalone	Standalone
Pairing	Active	Standby
Failover	Zombie	Standalone

Set Up SD-WAN Orchestrator Replication

Two installed SD-WAN Orchestrator instances are required to initiate replication.

- The selected standby is put into a `STANDBY_CANDIDATE` state, enabling it to be configured by the active server.
- The active server is then given the address and credentials of the standby and it enters the `ACTIVE_CONFIGURING` state.

When a `STANDBY_CONFIG_RQST` is made from active to standby, the two servers synchronize through the state transitions.

The two Orchestrators on which Disaster Recovery (DR) need to be established must have same time. Before you initiate SD-WAN Orchestrator replication, ensure you check the following NTP configurations:

- The Gateway time zone must be set to **Etc/UTC**. Use the following command to view the NTP time zone.

  ```
  vcadmin@vcg1-example:~$ cat /etc/timezone
  Etc/UTC
  vcadmin@vcg1-example:~$
  ```

  If the time zone is incorrect, use the following commands to update the time zone.

  ```
  echo "Etc/UTC" | sudo tee /etc/timezone
  sudo dpkg-reconfigure --frontend noninteractive tzdata
  ```

- The NTP offset must be less than or equal to 15 milliseconds. Use the following command to view the NTP offset.

  ```
  sudo ntpqvcadmin@vcg1-example:~$ sudo ntpq -p
       remote           refid      st t when poll reach   delay   offset  jitter
  ==============================================================================
  *ntp1-us1.prod.v 74.120.81.219    3 u  474 1024  377   10.171   -1.183   1.033
   ntp1-eu1-old.pr .INIT.          16 u    - 1024    0    0.000    0.000   0.000
  vcadmin@vcg1-example:~$
  ```

  If the offset is incorrect, use the following commands to update the NTP offset.

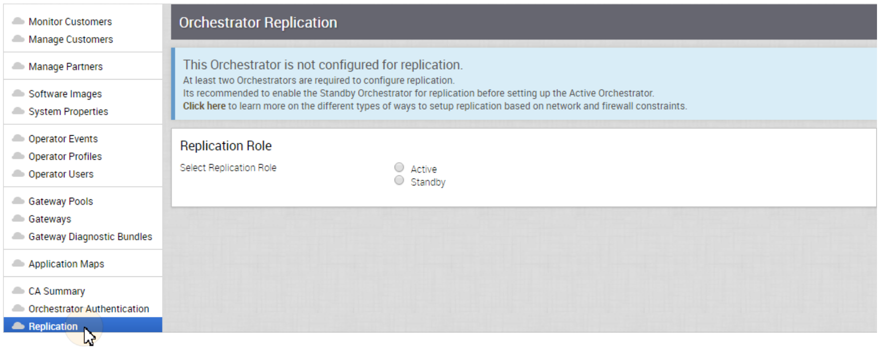
  ```
  sudo systemctl stop ntp
  sudo ntpdate <server>
  sudo systemctl start ntp
  ```

- By default, a list of NTP Servers are configured in the `/etc/ntpd.conf` file. The Orchestrators on which DR need to be established must have Internet to access the default NTP Servers and ensure the time is in sync on both the Orchestrators. Customers can also use their local NTP server running in their environment to sync time.

Set Up the Standby Orchestrator

To set up SD-WAN Orchestrator replication, perform the following steps:

1 Click **Replication** from the Navigation panel to display the **Orchestrator Replication** screen.



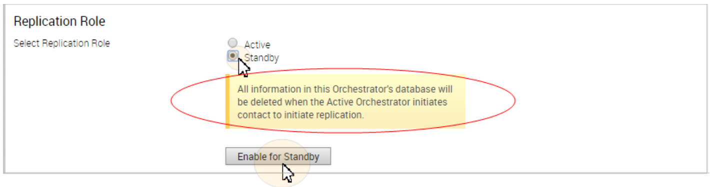
Orchestrator Replication

This Orchestrator is not configured for replication.
At least two Orchestrators are required to configure replication.
Its recommended to enable the Standby Orchestrator for replication before setting up the Active Orchestrator.
Click here to learn more on the different types of ways to setup replication based on network and firewall constraints.

Replication Role

Select Replication Role ○ Active ○ Standby

2 Enable the Standby Orchestrator by selecting the **Standby (Replication Role)** radio button.



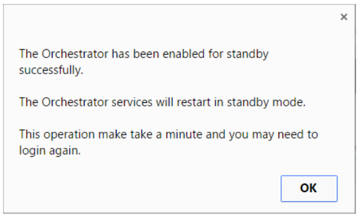
Replication Role

Select Replication Role ○ Active ● Standby

All information in this Orchestrator's database will be deleted when the Active Orchestrator initiates contact to initiate replication.

3 Click the **Enable for Standby** button.

The **Orchestrator Success** dialog box appears, indicating that the Orchestrator has been enabled for Standby, and that the Orchestrator will restart in Standby mode.

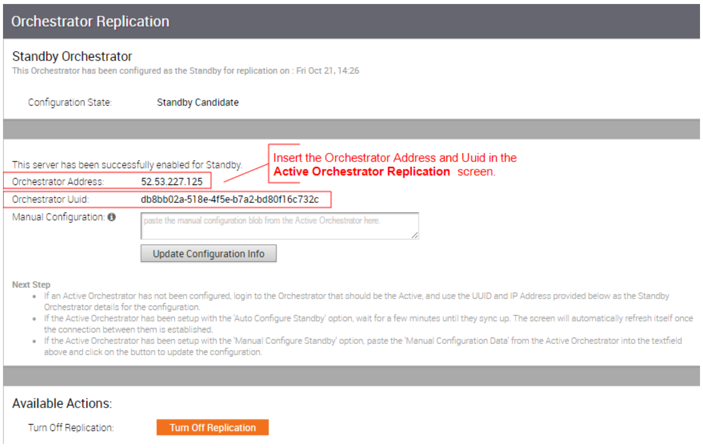


The Orchestrator has been enabled for standby successfully.

The Orchestrator services will restart in standby mode.

This operation make take a minute and you may need to login again.

4 Click **OK**.



Orchestrator Replication

Standby Orchestrator

This Orchestrator has been configured as the Standby for replication on : Fri Oct 21, 14:26

Configuration State: Standby Candidate

This server has been successfully enabled for Standby.

Orchestrator Address: 52.53.227.125

Orchestrator Uuid: db8bb02a-518e-4f5e-b7a2-bd80f16c732c

Manual Configuration: paste the manual configuration blob from the Active Orchestrator here.

Insert the Orchestrator Address and Uuid in the **Active Orchestrator Replication** screen.

Next Step

- If an Active Orchestrator has not been configured, login to the Orchestrator that should be the Active, and use the UUID and IP Address provided below as the Standby Orchestrator details for the configuration.
- If the Active Orchestrator has been setup with the 'Auto Configure Standby' option, wait for a few minutes until they sync up. The screen will automatically refresh itself once the connection between them is established.
- If the Active Orchestrator has been setup with the 'Manual Configure Standby' option, paste the 'Manual Configuration Data' from the Active Orchestrator into the textfield above and click on the button to update the configuration.

Available Actions:

Turn Off Replication:

After the Standby Orchestrator has been configured for replication, configure the Active Orchestrator according to the instructions below.

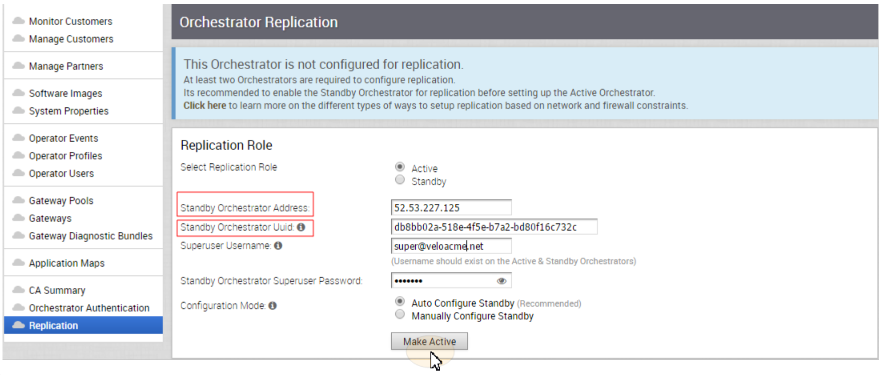
Set Up the Active Orchestrator

To configure the second SD-WAN Orchestrator to be the Active Orchestrator:

1 Click **Replication** from the Navigation panel. The **Orchestrator Replication** screen appears.

2 Choose the **Active Replication Role**.

3 Type in the **Standby Orchestrator Address** and the **Standby Orchestrator Uuid**.
The Orchestrator Address and Uuid are displayed in the **Standby Orchestrator** screen.



Orchestrator Replication

This Orchestrator is not configured for replication.
At least two Orchestrators are required to configure replication.
Its recommended to enable the Standby Orchestrator for replication before setting up the Active Orchestrator.
Click here to learn more on the different types of ways to setup replication based on network and firewall constraints.

Replication Role

Select Replication Role: ● Active ○ Standby

Standby Orchestrator Address: 52.53.227.125

Standby Orchestrator Uuid: db8bb02a-518e-4f5e-b7a2-bd80f16c732c

Superuser Username: super@veloacme.net
(Username should exist on the Active & Standby Orchestrators)

Standby Orchestrator Superuser Password: •••••••

Configuration Mode: ● Auto Configure Standby (Recommended) ○ Manually Configure Standby

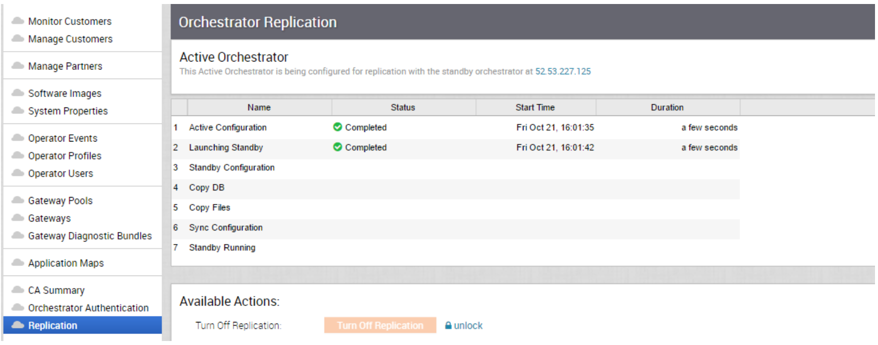
Make Active

4 Type in the username and password for the Orchestrator Superuser to be used for replication.

Note This Superuser should already exist on both systems.

5 Click the **Make Active** button.

The **Active Orchestrator** screen displays showing a status of the current state.



Orchestrator Replication

Active Orchestrator
This Active Orchestrator is being configured for replication with the standby orchestrator at 52.53.227.125

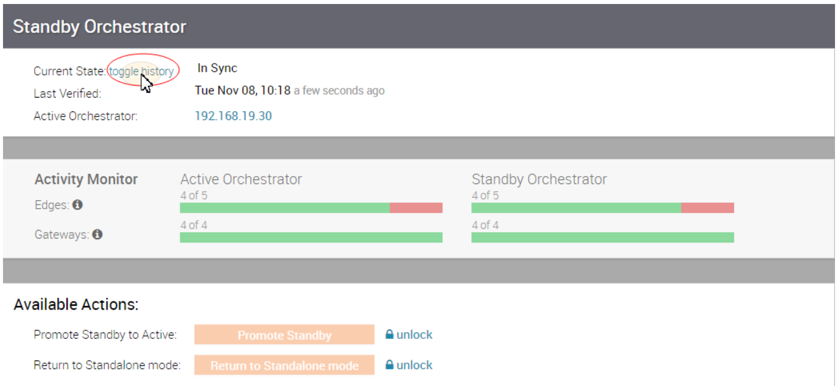
	Name	Status	Start Time	Duration
1	Active Configuration	✓ Completed	Fri Oct 21, 16:01:35	a few seconds
2	Launching Standby	✓ Completed	Fri Oct 21, 16:01:42	a few seconds
3	Standby Configuration			
4	Copy DB			
5	Copy Files			
6	Sync Configuration			
7	Standby Running			

Available Actions:

Turn Off Replication: Turn Off Replication unlock

When configuration is complete, both Orchestrators (Standby and Active) will be in sync.

Standby Orchestrator in Sync



Standby Orchestrator

Current State: toggle history In Sync

Last Verified: Tue Nov 08, 10:18 a few seconds ago

Active Orchestrator: 192.168.19.30

Activity Monitor

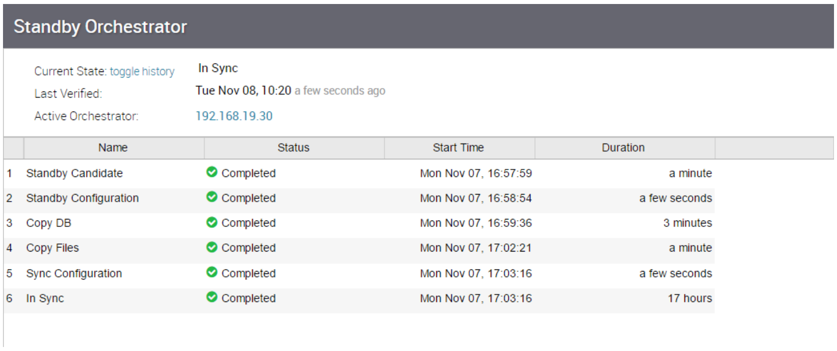
	Active Orchestrator	Standby Orchestrator
Edges:	4 of 5	4 of 5
Gateways:	4 of 4	4 of 4

Available Actions:

Promote Standby to Active: Promote Standby unlock

Return to Standalone mode: Return to Standalone mode unlock

You can click the **toggle history** link to view the status of each state.



Standby Orchestrator

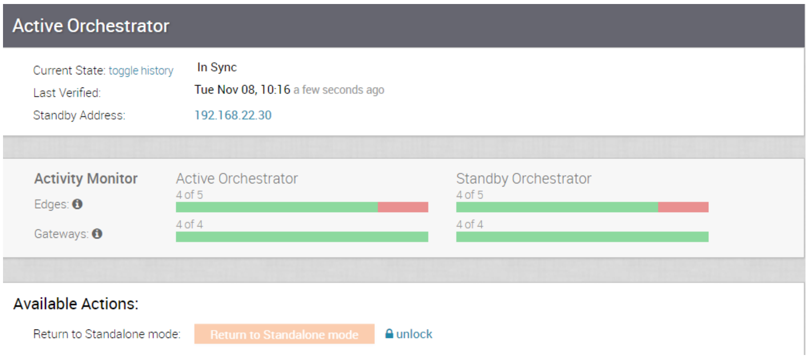
Current State: toggle history In Sync

Last Verified: Tue Nov 08, 10:20 a few seconds ago

Active Orchestrator: 192.168.19.30

	Name	Status	Start Time	Duration
1	Standby Candidate	✓ Completed	Mon Nov 07, 16:57:59	a minute
2	Standby Configuration	✓ Completed	Mon Nov 07, 16:58:54	a few seconds
3	Copy DB	✓ Completed	Mon Nov 07, 16:59:36	3 minutes
4	Copy Files	✓ Completed	Mon Nov 07, 17:02:21	a minute
5	Sync Configuration	✓ Completed	Mon Nov 07, 17:03:16	a few seconds
6	In Sync	✓ Completed	Mon Nov 07, 17:03:16	17 hours

Active Orchestrator in Sync



Active Orchestrator

Current State: toggle history In Sync

Last Verified: Tue Nov 08, 10:16 a few seconds ago

Standby Address: 192.168.22.30

Activity Monitor

	Active Orchestrator	Standby Orchestrator
Edges:	4 of 5	4 of 5
Gateways:	4 of 4	4 of 4

Available Actions:

Return to Standalone mode: Return to Standalone mode unlock

Test Failover

The following testing failover scenarios are forced failovers for example purposes. You can perform these actions in the **Available Actions** area of the **Active** and **Standby** screens.

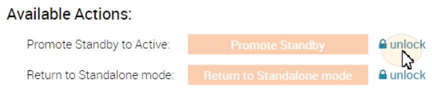
Promote a Standby Orchestrator

This section describes how to promote a Standby Orchestrator.

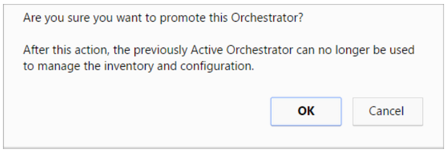
To promote a Standby Orchestrator

1 Click the **unlock** link.

2 Click the **Promote Standby** button in the **Available Actions** area on the Standby Orchestrator screen.


Available Actions:
Promote Standby to Active:
Promote Standby
unlock
Return to Standalone mode:
Return to Standalone mode
unlock

The following dialog box appears, indicating that when you promote your Standby Orchestrator, administrators will no longer be able to manage the SD-WAN Orchestrator using the previously Active Orchestrator.



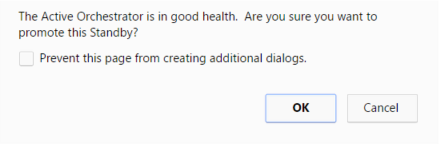
Are you sure you want to promote this Orchestrator?

After this action, the previously Active Orchestrator can no longer be used to manage the inventory and configuration.

3 Click the **OK** button to promote the Standby Orchestrator.

Another message dialog box appears to verify your request to promote the Standby Orchestrator. This message will appear only if the Standby Orchestrator perceives the Active Orchestrator to be in good health, meaning the Standby is communicating with the Active and duplicating data.

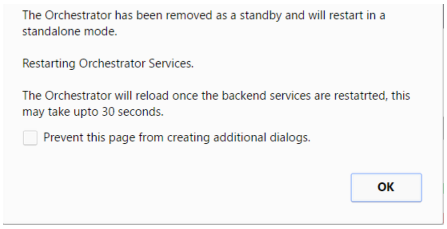
4 Click **OK** to promote the Orchestrator.



The Active Orchestrator is in good health. Are you sure you want to promote this Standby?

□ Prevent this page from creating additional dialogs.

A final dialog box appears indicating that the Orchestrator is no longer a Standby and will restart in Standalone mode.



The Orchestrator has been removed as a standby and will restart in a standalone mode.

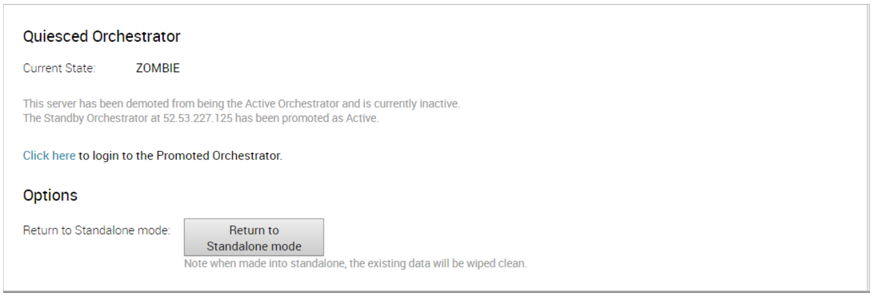
Restarting Orchestrator Services.

The Orchestrator will reload once the backend services are restatrted, this may take upto 30 seconds.

□ Prevent this page from creating additional dialogs.

When you promote a Standby Orchestrator, it restarts in Standalone mode.

If the Standby can communicate with the formerly Active Orchestrator, it will instruct that Orchestrator to enter a Zombie state. In Zombie state, the Orchestrator communicates with its clients (edges, gateways, UI/API) that it is no longer active, and that they must communicate with the newly promoted Orchestrator. If the promoted Standby cannot communicate with the formerly Active Orchestrator, the operator should, if possible, manually demote the formerly Active Orchestrator.



Quiesced Orchestrator

Current State: ZOMBIE

This server has been demoted from being the Active Orchestrator and is currently inactive.
The Standby Orchestrator at 52.53.227.125 has been promoted as Active.

Click here to login to the Promoted Orchestrator.

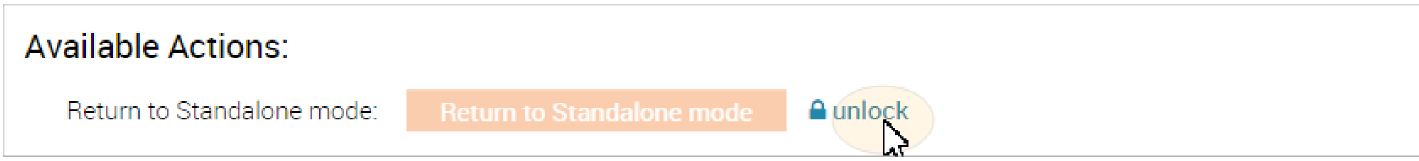
Options

Return to Standalone mode:

Note when made into standalone, the existing data will be wiped clean.

Return to Standalone Mode

To return the Zombie to standalone mode, click the **Return to Standalone Mode** button in the **Available Actions** area on the **Active Orchestrator** or **Standby Orchestrator** screens.



Available Actions:

Return to Standalone mode:

Note The SD-WAN Orchestrator can be returned to the Standalone mode from the Zombie state after the time specified in the system property "vco.disasterRecovery.zombie.expirySeconds," which is defaulted to 1800 seconds.

Troubleshooting SD-WAN Orchestrator DR

This section describes the failure states of the system. These are also listed in the UI, along with a more detailed description of the failure. Additional information is available in the VMware log.

Recoverable Failures

The following errors are recoverable failures that can occur after SD-WAN Orchestrator DR reaches an in sync state. If the problem causing these failures is corrected, SD-WAN Orchestrator DR will automatically return to normal operation.

- `FAILURE_SYNCING_FILES`
- `FAILURE_GET_STANDBY_STATUS`
- `FAILURE_MYSQL_ACTIVE_STATUS`
- `FAILURE_MYSQL_STANDBY_STATUS`

Unrecoverable Failures

The following failures can occur during configuration of the SD-WAN Orchestrator DR. SD-WAN Orchestrator DR will not automatically recover from these failures.

- `FAILURE_ACTIVE_CONFIGURING`
- `FAILURE_LAUNCHING_STANDBY`

- `FAILURE_STANDBY_CONFIGURING`
- `FAILURE_COPYING_DB`
- `FAILURE_COPYING_FILES`
- `FAILURE_SYNC_CONFIGURING`
- `FAILURE_GET_STANDBY_CONFIG`
- `FAILURE_STANDBY_CANDIDATE`
- `FAILURE_STANDBY_UNCONFIG`
- `FAILURE_STANDBY_PROMOTION`
- `FAILURE_ACTIVE_DEMOTION`

Manage User Agreements

20

SD-WAN Orchestrator allows an Operator Super User to create and manage End User License Agreements.

Only an Operator Superuser can create an End User License Agreement.

By default, the User Agreement option is disabled. To enable 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 Superuser or Partner Superuser can accept a license agreement, based on the System Property settings.

To create and manage User Agreement, navigate to the **User Agreements** page in the Operator portal. Click **Actions** to perform the following:

- **New** – Creates a new End User License Agreement. See Also Create a User Agreement.
- **Clone** – Clones and creates a copy of the selected User Agreement.
- **Update** – Allows to modify the values in the selected User Agreement.
- **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.

This chapter includes the following topics:

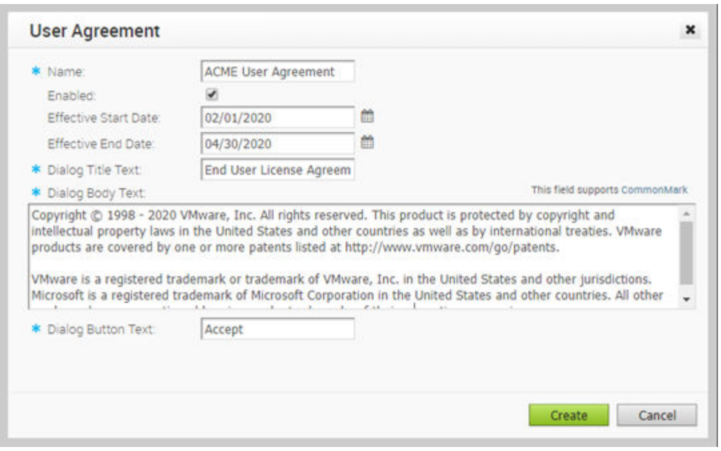
- Create a User Agreement

Create a User Agreement

Only Operator Superusers can create a new user agreement. You can create multiple agreements, but only one agreement can be active at a time.

In the Operator portal, click **User Agreements**.

1. Click **New User Agreement** or **Actions > New**.
2. In the **User Agreement** window, enter the following:



User Agreement

* Name:	ACME User Agreement
Enabled:	☑
Effective Start Date:	02/01/2020
Effective End Date:	04/30/2020
* Dialog Title Text:	End User License Agreem
* Dialog Body Text:	This field supports CommonMark

Copyright © 1998 - 2020 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. Microsoft is a registered trademark of Microsoft Corporation in the United States and other countries. All other

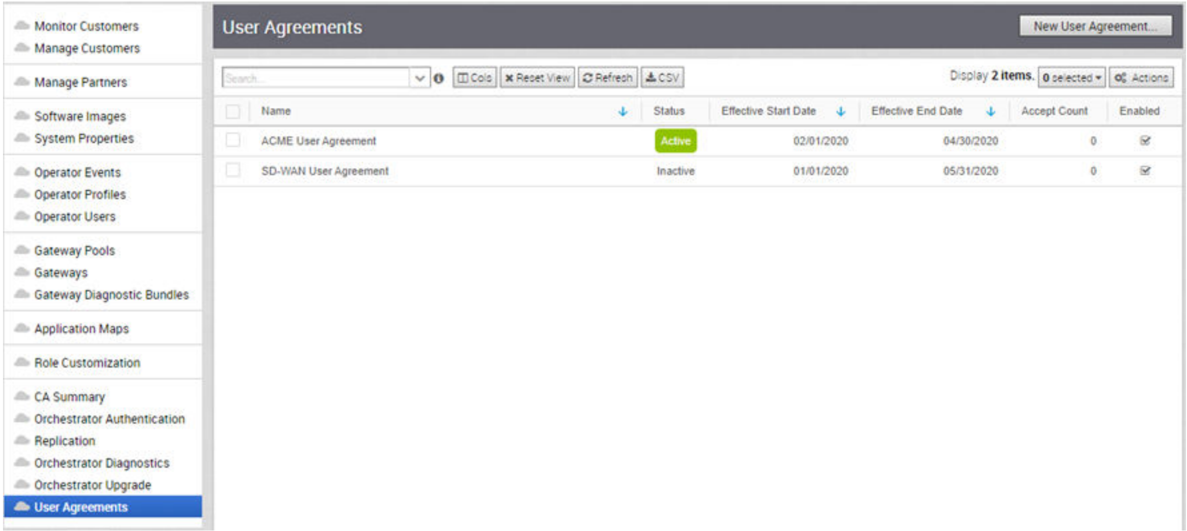
* Dialog Button Text:	Accept

   - **Name** – Enter the name of the customer.
   - **Enabled** – By default, this checkbox is selected. If you clear the checkbox, then the User Agreement is Inactive.

     Note Only one User Agreement can be active at a time. When you have multiple Agreements, ensure to select the **Enabled** option only for the Agreement that needs to be in the Active state, and disable this option for the other User Agreements.

   - **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.
3. Click **Create**.

The Agreements are displayed in the **User Agreements** page.



User Agreements

Display 2 items.

	Name	Status	Effective Start Date	Effective End Date	Accept Count	Enabled
□	ACME User Agreement	Active	02/01/2020	04/30/2020	0	☑
□	SD-WAN User Agreement	Inactive	01/01/2020	05/31/2020	0	☑

When an Enterprise Superuser or Partner Superuser logs into the SD-WAN Orchestrator, User Agreement window prompts them to accept the Agreement. If the Users do not accept the agreement, they are automatically logged out.

The Operator can view the number of customers that have accepted the Agreement in the **User Agreements** page. The accepted Agreements are archived, and you cannot delete them.

SD-WAN Orchestrator Upgrade 3.3.2 or 3.4 to SD-WAN Orchestrator 4.0

21

This document provides and overview and best practices on how to upgrade the VMware SD-WAN Orchestrator from the 3.3.2 or 3.4 release to the 4.0 release. However, please contact VMware Support to asssit you with the 3.3.2 or 3.4 to 4.0 upgrade at `https://kb.vmware.com/s/article/53907`

Only 3.3.2 and 3.4 SD-WAN Orchestrators can be upgraded to the 4.0 release. If you are running a 3.3.1 or lower version of the SD-WAN Orchestrator, you must upgrade to at least the 3.3.2 version before upgrading to the 4.0 version.

Consider the following when upgrading:

- This upgrade work does not modify any existing APIs.
- Just like other releases, there are schema changes with the 4.0 release. However, these changes will not impact the upgrade process.

The OS for the SD-WAN Orchestrator virtual appliance and the underlying data stores that store the configuration and statistics data are being upgraded. The specific upgrades include the following:

- The OS version is changing from Ubuntu 14.04 to 18.04.
- The Config store is moving to MySQL 8.0.
- The Stats store is moving to ClickhouseDB.

Note The Orchestrator OS, database, and several other dependent components currently in use have reached their end of life, and will no longer be supported.

The benefits to upgrading to the 4.0 release are as follows:

- A better scale overall in terms of number of Edges, flows, and UI.
- Faster query performance for statistics, longer retention out of the box for flow stats.
- Faster initial Disaster Recovery (DR) setup performance.
- Lower resource utilization - Disk, CPU, RAM.
- Better security due to components with active LTS.

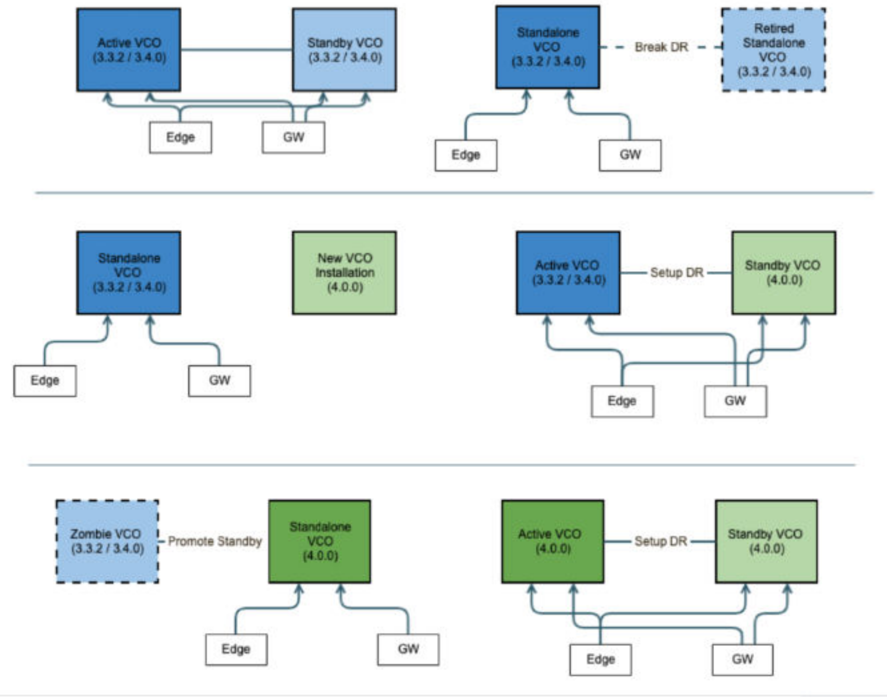
Best Practices/Recommendations:

Listed below are some upgrade best practices:

- From the System Properties page in the SD-WAN Orchestrator, make a note of the value of the edge.heartbeat.spread.factor system property. Then, change the heartbeat spread factor to a relatively high value for a large SD-WAN Orchestrator (e.g. 20, 40, 60). This will help reduce the sudden spike of the resource utilization (CPU, IO) on the system. Make sure to verify that all Gateways and Edges are in a connected state before restoring the previous edge.heartbeat.spread.factor value from the System Property page in the SD-WAN Orchestrator.
- Leave the demoted SD-WAN Orchestrator up for a few hours before complete shutdown or decommission.
- Freeze configuration modifications to avoid any additional configuration changes until the upgrade process is completed.

Upgrade Procedure Overview

This document provides the steps required to upgrade 3.3.2 or 3.4 release to the 4.0 release. The SD-WAN Orchestrator OS and Disaster Recovery upgrade have some of the same steps as the Disaster Recovery procedures as found in the “Configure SD-WAN Orchestrator Disaster Recovery” guide. However, follow the steps in Upgrade Procedures section in this document to complete the 3.3.2 or 3.4 release to the 4.0 release upgrade process. The image below depicts an illustration of the upgrade process. See the Upgrade Procedures below.


Active VCO (3.3.2 / 3.4.0)
Standby VCO (3.3.2 / 3.4.0)
Edge
GW
Standalone VCO (3.3.2 / 3.4.0)
Break DR
Retired Standalone VCO (3.3.2 / 3.4.0)
Edge
GW
Standalone VCO (3.3.2 / 3.4.0)
New VCO Installation (4.0.0)
Edge
GW
Active VCO (3.3.2 / 3.4.0)
Setup DR
Standby VCO (4.0.0)
Edge
GW
Zombie VCO (3.3.2 / 3.4.0)
Promote Standby
Standalone VCO (4.0.0)
Edge
GW
Active VCO (4.0.0)
Setup DR
Standby VCO (4.0.0)
Edge
GW

Upgrade Procedures

Please contact VMware Support to assist you with the 3.3.2 or 3.4 to 4.0 upgrade at https://kb.vmware.com/s/article/53907

Orchestrator Diagnostics

22

This section describes Orchestrator Diagnostics.

This chapter includes the following topics:

SD-WAN Orchestrator Diagnostics Overview

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

Rate Limiting API Requests

23

When there are too many API requests sent at a time, it affects the performance of the system. You can enable Rate Limiting, which enforces a limit on the number of API requests sent by each user.

The SD-WAN Orchestrator makes use of certain defence mechanisms that curb API abuse and provides system stability. API requests that exceed the allowed request limits are blocked and returned with HTTP 429 (Too many Requests). The system needs to go through a cool down period before making the requests again.

The following types of Rate-Limiters are deployed on SD-WAN Orchestrator:

- **Leaky bucket limiter** – Smooths the burst of requests and only allows a pre-defined number of requests. This limiter takes care of limiting the number of requests allowed in a given time window.
- **Concurrency limiter** – Limits the number of requests that occur in parallel which leads to concurrent requests fighting for resources and may result in long running queries.

The following are the major reasons that lead to rate limiting of the API requests:

- Large number of active or concurrent requests.
- Sudden spikes in request volume.
- Requests resulting in long running queries on the Orchestrator holding system resources for long being dropped.

Developers that rely on the API can adopt the following measures to improve the stability of their code when the VCO rate-limiting capability is enabled.

- Handle HTTP 429 response code when requests exceed rate limits.
- The penalty time duration is 5000 ms when the rate limiter reaches the maximum allowed requests in a given period. If blocked, the clients are expected to have a cool down period of 5000 ms before making requests again. The requests made during the cool down period of 5000 ms will still be rate limited.
- Use shorter time intervals for time series APIs which will not let the request to expire due to long running queries.

- Prefer batch query methods to those that query individual Customers or Edges whenever possible.

Note Operator Super users configure Rate limits discretely based on the environment. For any queries on relevant policies, contact your Operator.

Configure Rate Limiting Policies using System Properties

You can use the following system properties to enable Rate Limiting and define the default set of policies:

- vco.api.rateLimit.enabled
- vco.api.rateLimit.mode.logOnly
- vco.api.rateLimit.rules.global
- vco.api.rateLimit.rules.enterprise.default
- vco.api.rateLimit.rules.enterpriseProxy.default

For more information on the system properties, see Table 11-10. Rate Limiting APIs.

Configure Rate Limiting Policies using APIs

It is recommended to configure the rate limiter policies as global rules using the system properties, as this approach produces the best possible API performance, facilitates troubleshooting, and ensures a consistent user experience across all Partners and Customers. In rare cases, however, Operators may determine that global policies are too lax for a particular tenant or user. For such cases, VMware supports the following operator-only APIs to set policies for specific partners and enterprises.

- **enterpriseProxy/insertOrUpdateEnterpriseProxyRateLimits** – Used to configure Partner-specific policies.
- **enterprise/insertOrUpdateEnterpriseRateLimits** – Used to configure Customer-specific policies.

For more information on the APIs, see https://code.vmware.com/apis/1037/velocloud-sdwan-vco-api.