VeloCloud Operator Guide

VMware SD-WAN 3.3

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

VMware SD-WAN by VeloCloud Release 3.3

1

The *VMware SD-WAN by VeloCloud Operator Guide release 3.3* includes new and updated content for versions 3.3.0, 3.3.1, and 3.3.2 as described below.

What's Changed in Version 3.3.2?

Status	Section
New	Refresh Application Map
New	Push Application Map
Updated	Customer BGP Priority (Community Additive Support)

What's Changed in Version 3.3.1?

Status	Section
New	Overview of Single Sign On
New	Configure Single Sign On for Operator User
New	Chapter 4 Log in to the SD-WAN Orchestrator Using SSO for Operator User
New	Configure an IDP for Single Sign On
Updated	Configure Orchestrator Authentication
Updated	Create a Customer
Updated	Create a Partner
Updated	Configure System Properties

What's Changed in Version 3.3.0?

Status	Section
New	*User Agreements*
New	*Edge Licensing*
New	*Push Activation*
New	*Orchestrator Diagnostics*

Status	Section
Updated	*Update to Application Maps*
Updated	*Deleting Customers (Important Update)*
New	*Customer Migration Tool*
New	*VCO Upgrade Procedures with DR Deployment*

Previous VMware SD-WAN by VeloCloud Versions

To get product documentation for previous VMware SD-WAN by VeloCloud versions, contact your VMware SD-WAN by VeloCloud representative.

Introduction

2

This guide describes the VCO features that VeloCloud Operator roles can access. The IT Operator roles provide the functionality needed to create, monitor, and manage customers and partners that use the VeloCloud.

Prerequisites

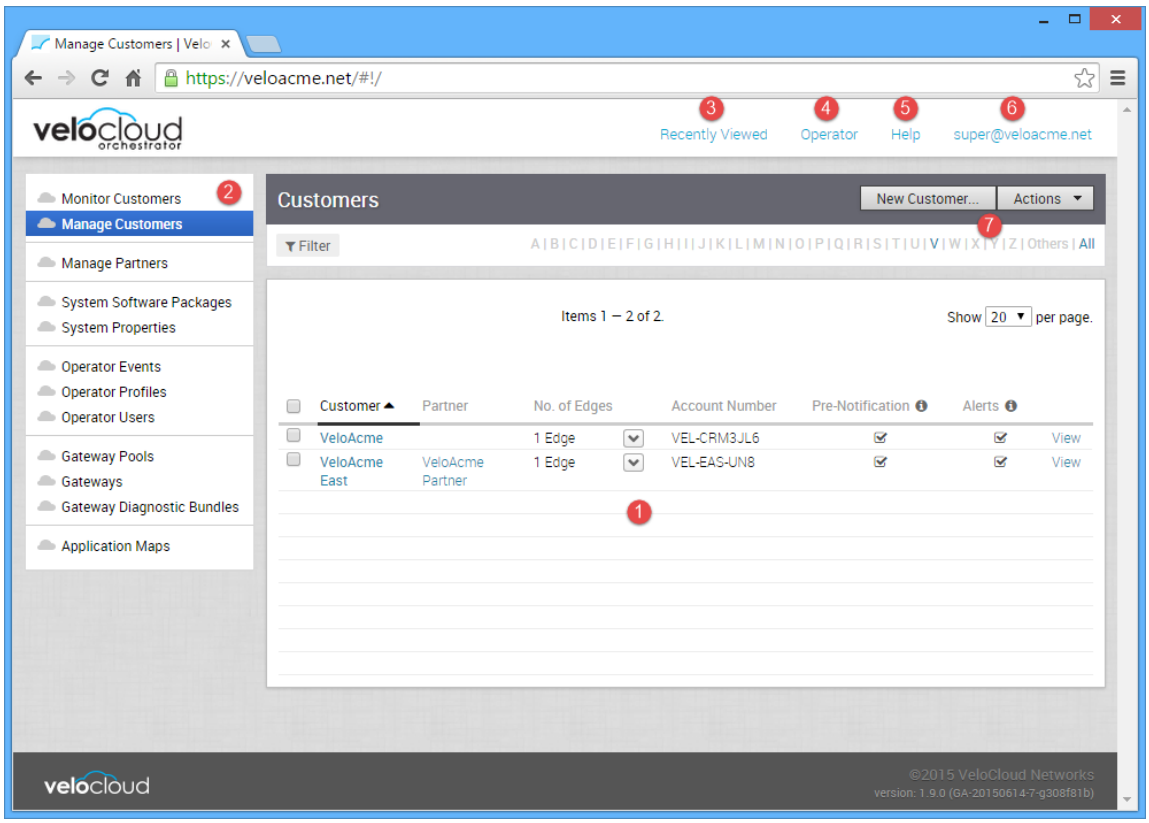
It is assumed that you are thoroughly familiar with the concepts described in the *Overview* . It is also strongly recommended that you read and understand the steps in the *IT Admin Quick Start Guide* and *IT Admin Guide for VeloCloud Orchestrator* to become familiar with the core functionality of the VeloCloud Orchestrator that is used by an Enterprise IT Administrator for a customer.

About this Guide

In this guide, a hypothetical company, VeloAcme, is used to describe the configuration for customers. This guide also provides steps to monitor, test, and troubleshoot the VeloCloud system.

Initial Operator Web Page

The following image shows an example of the initial Operator page after login.



The numbered items in the screen shot correspond to the numbers in the following table.

Numbered Item	Description
1	The list of the Customers that have been created and that are being managed by the operator. Partners that manage a customer are also displayed.
2	The navigation bar for operator function.
3	Quick links to recently accessed Customers. If you click on a customer link, you will be taken to the function provided for the IT Administrator (see the *IT Admin Guide for VeloCloud Orchestrator* for a description of this function).
4	Quick links to the operator function (the same as in item 2).
5	Quick link to this help and about information.
6	The operator that is currently logged in. Clicking the link also provides operator account information and a link to sign out.
7	Buttons to create and manage customers and partners.

Install VeloCloud Orchestrator

3

This section describes VeloCloud Orchestrator installation.

This chapter includes the following topics:

Prerequisites

This section describes the prerequisites that must be met before installing the VeloCloud Operator.

Instance Requirements

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

The VeloCloud Orchestrator requires the following minimal guest instance specifications:

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

  Note The VCO will not start with less than 10GB of memory.

- 2x 1TB 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 VeloCloud 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 VCO 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. VeloCloud does not anticipate exceeding these limits for nominal use of the VCO.

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 VCO through the Operator Portal's **System Properties** page. The account will be provisioned through a system property, as described later in the guide.

MaxMind

MaxMind is geolocations 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 VCO through the Operator Portal's **System Properties** page. The properties are called:

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 VeloCloud Orchestrator supports cloud-init and all essential configurations can be packaged in through 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 call it `meta-data`. This file provides information that identifies the instance of VeloCloud 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 VeloCloud 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 VeloCloud Orchestrator services.

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

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

The `write_files` section allows to replace files on the system. By default, VeloCloud 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 VeloCloud 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 VeloCloud 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 VeloCloud Orchestrator Virtual Machine

To start up the VeloCloud 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 VeloCloud 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 VeloCloud Orchestrator using the libvirt. This deployment was tested in Ubuntu 14.04LTS.

Images

For KVM deployment, VeloCloud will provide the VCO in three qcow images.

- OS
- DATABASE
- LOGS

The images are thin provisioned on deployment.

Start by copying the images to the KVM server. In addition, you will need to 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/vco-root.img'/>
  <target dev='hda' bus='ide'/>
  <alias name='ide0-0-0'/>
  <address type='drive' controller='0' bus='0' target='0' unit='0'/>
</disk>i
<disk type='file' device='disk'>
  <driver name='qemu' type='qcow2'/>
  <source file='/ images/vco/vco-db.img'/>
  <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/vco-binlog.img'/>
  <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='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 VeloCloud Orchestrator on AWS.

Minimum Instance Requirements

See the first section of the VeloCloud 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 VeloCloud. 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 VCO console. If you configured the VeloCloud 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 VCO private key.

Note Do not encrypt the key. It must remain unencrypted on the VCO 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
OU	department (optional)
CN	VCO 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). VCO 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.

```
Service nginx restart
```

Configure System Properties

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

System Properties can be set initially using the cloud-init config file under the VCO section (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 VCO 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` VCO system property to API key.

7 Set `service.client.googleMapsApi.enable` to "true."

Twilio

Twilio is a messaging service that allows you to receive VCO alerts via SMS. It is optional. The account can be provisioned in the VCO 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 VCO
- `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 can be provisioned in the VCO 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 VCO
- `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 VCO 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 VCO.
- `mail.smtp.port` - SMTP port.
- `mail.smtp.secureConnection` - use SSL for SMTP traffic.

Upgrade SD-WAN Orchestrator

This section describes how to upgrade SD-WAN Orchestrator.

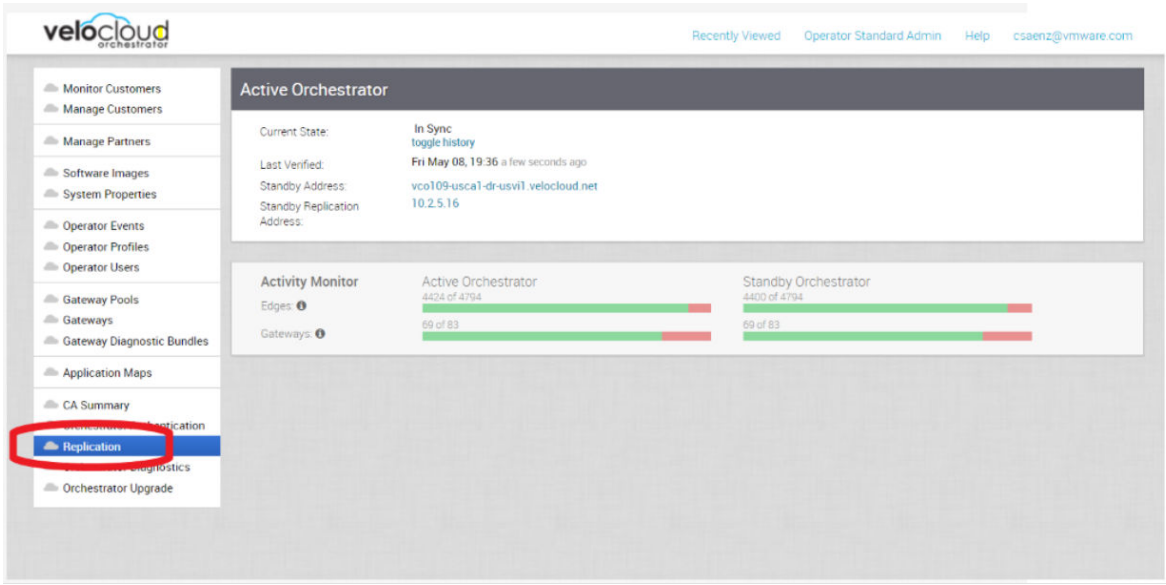
To upgrade SD-WAN Orchestrator:

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.



- 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').

  - LVM layout
    - pvdisplay -v
    - vgdisplay -v
    - lvdisplay -v
    - df -h
    - cat /etc/fstab
  - Memory information
    - free -m
    - cat /proc/meminfo
    - ps -ef
    - top -b -n 2
  - CPU Information
    - cat /proc/cpuinfo
  - 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.

Expand Disk Size (VMware)

The database volume is an LVM device. You can resize it online by provided the underlying virtualization technology supports online disk expansion.

To expand the disk size:

1 Login into the VCO system console.

2 Identify the physical disks backing the database volume.

```
vgs –o +devices db_data
```

Example:

```
root@vco:~# vgs –o +devices db_data
   \  VG      #PV #LV #SN Attr   VSize   VFree   Devices
     db_data   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 info. Example: `SCSI(0:1)`

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

6 Log back into the VCO 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 db_data |grep Free
```

Example:

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

10 Extend the database logical volume.

```
lvextend –L+#G /dev/db_data/vco
```

Example:

```
root@vco:~# lvextend -L+10G /dev/db_data/vco
  Extending logical volume vco to 385.00 GiB
  Logical volume vco successfully resized
```

11 Resize the database volume filesystem:

```
resize2fs /dev/db_data/vco
```

Example:

```
root@vco:~# resize2fs /dev/db_data/vco
resize2fs 1.42.9 (4-Feb-2014)
Filesystem at /dev/db_data/vco is mounted on /store; on-line resizing required
old_desc_blocks = 24, new_desc_blocks = 25
The filesystem on /dev/db_data/vco is now 100924416 blocks long.
```

12 See the new size of the volume.

```
df -h /dev/db_data/vco
```

Example:

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

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

4

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.

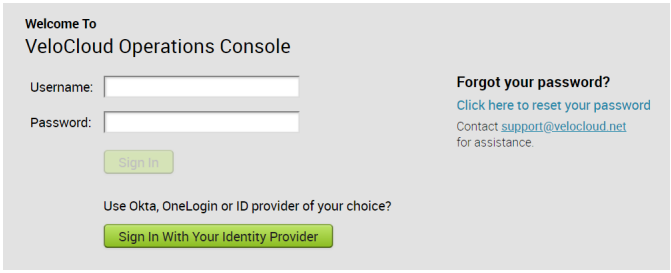
Prerequisites

- 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.



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

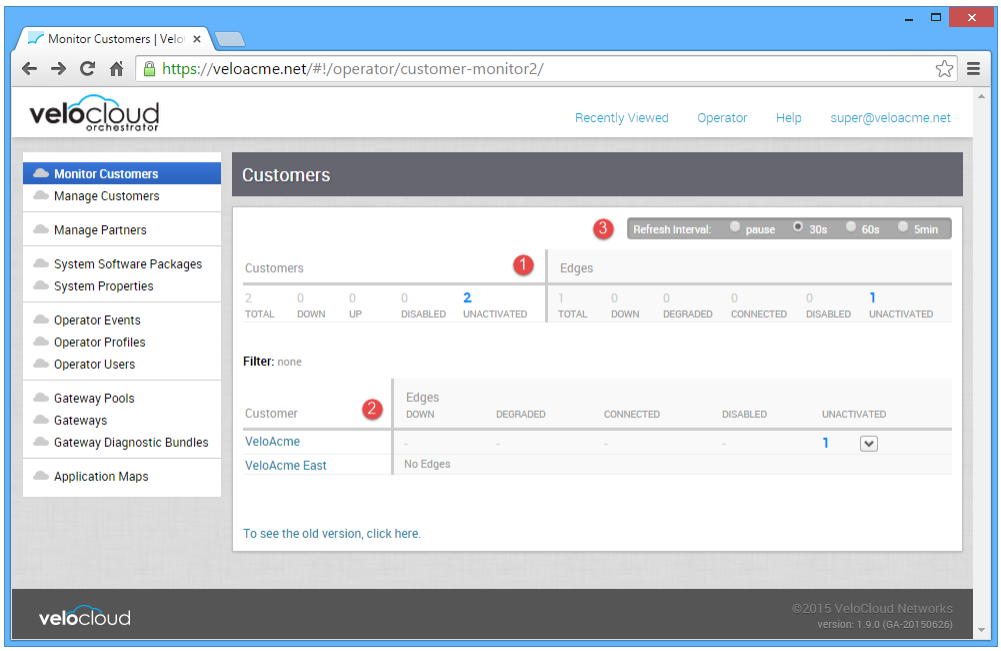
The IDP configured for SSO will authenticate the user and redirect the user to the configured SD-WAN Orchestrator URL.

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

5

An operator can monitor customer status from the **Monitor Customers** link. A web page shows the Edges and Links for all customers managed by this operator. Selections can be made to control the interval for updating the information.



The following describes the major features of the **Monitor Customer** web page. The numbers correspond to the numbers in the screen capture:

1 The list of all Customers, their Edges, and the Links being used by each Edge.

2 A textual log of recent Edge/Link changes in recent chronological order.

3 Filter and Interval selections that can be made to select specific customer monitoring.

4 A color-coded, iconic summary of Customers, Edges, and Links. Red icons indicate an Edge or Link that is down.

Manage Customers

6

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 a Customer.
- **Clone Customer** - Creates a new customer, by cloning the existing configurations from the selected customer. See #unique_31.
- **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 by VeloCloud 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 a Customer

This section describes how to create a customer at the Operator level. Only Operator Superusers, Standard Operators, and Business Specialist Operators can create a new customer.

Note Operator Superusers can temporarily disable the ability to create a new customer by setting the following system property to true: session.options.disableCreateEnterprise. (One of the most common reasons to use this system property is if the VCO is reaching its usage capacity). When this system property is set to true, Operator Superusers, Standard Operators, and Business Specialists Operators will not be able to create a new customer from the VCO API or the VCO UI. (Customer Support Operators do not have the ability to create a new customer; they have read only access to the Customer screen in the VCO).

To create a customer:

1 From the VCO navigation panel, click **Manage Customers**.

2 Click the **New Customer** button (top, right area of the screen) to create a new customer. The **New Customer** dialog box appears.

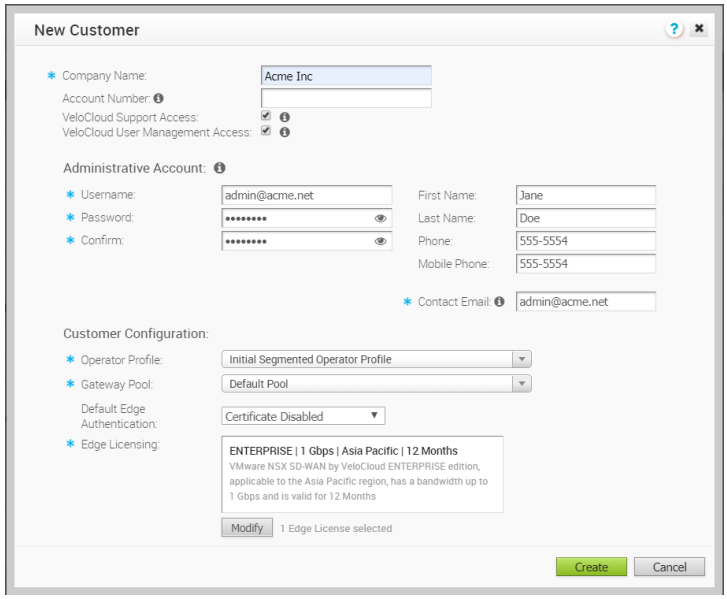
3 In the **New Customer** dialog box, complete the following:

   a Type in the **Company Name** and **Account** number in the appropriate fields.

   b If applicable, check the **VeloCloud Support Access** checkbox and the **VeloCloud User Management Access** checkbox.

   Note If the **VeloCloud Support Access** option is chosen, a VeloCloud Operator with support privileges can configure and troubleshoot the customer's Edges. However, VeloCloud Support will not be able to view user-identifiable information.

c Type in the customer's name (first and last), phone numbers, and email address in the appropriate fields.

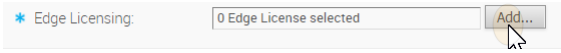


d In the **Customer Configuration** area, choose a profile from the **Operator Profile** drop-down menu.

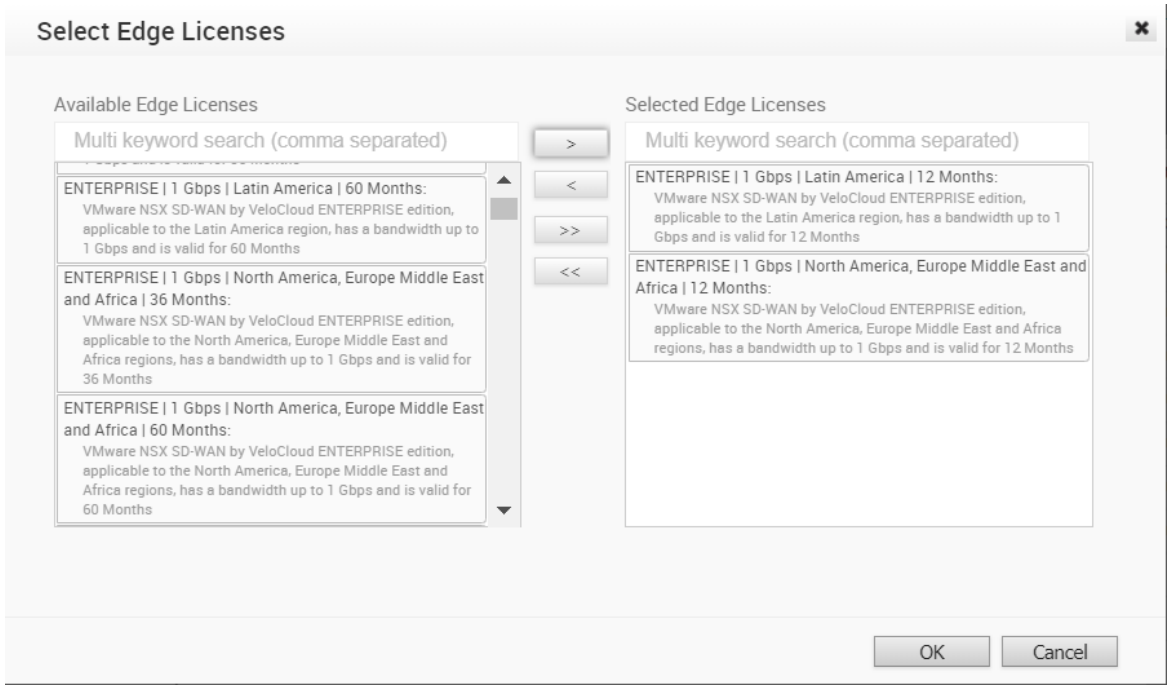
e Choose a Gateway Pool from the **Gateway Pool** drop-down menu.

f From the **Default Edge Authentication** drop-down menu, choose either Certificate Disabled, Certificate Optional, Certificate Required.

g In the **Edge Licensing** area, click the **Add** button.



h In the **Select Edge Licenses** dialog box, use the arrows to move license types from the **Available Edge Licenses** area to the **Selected Edge Licenses** area, as shown in the following image.



If you need to add or remove a license type, click the **Modify** button.

Note License types assigned to an Enterprise can be used on multiple Edges. VeloCloud recommends that you give your customers access to all license types that match their edition and region. For more information, see the section titled *Edge Licensing*.

4 Click the **Create** button.

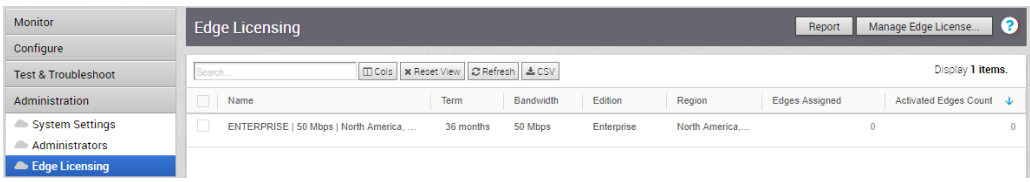
Manage Edge License Types

To add or remove license types for a Customer:

1 From the VCO navigation panel, click **Manage Customers**.

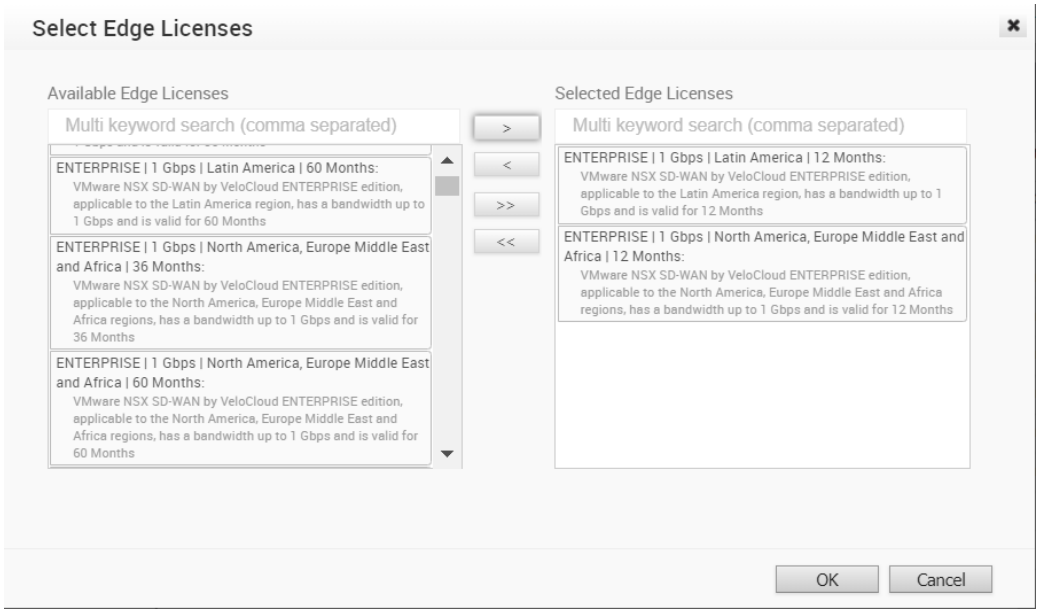
2 In the **Manage Customers** screen, click a Customer's name.

3 From the VCO navigation panel, go to **Administration > Edge Licensing**.



4 In the **Edge Licensing** screen, click the **Manage Edge License** button.

In the **Select Edge Licenses** dialog box, use the arrows to move license types from the **Available Edge Licenses** area to the **Selected Edge Licenses** area, as shown in the following example.



5 Click **OK**.

Upgrade an Edge License Edition

An Operator or MSP can upgrade a Standard Edge license type to either an Enterprise or a Premium edition.

However, after a higher edition license type is assigned, it cannot be downgraded to a lower edition. For more information, see *Edge Licensing*.

To upgrade a Standard Edge License Edition:

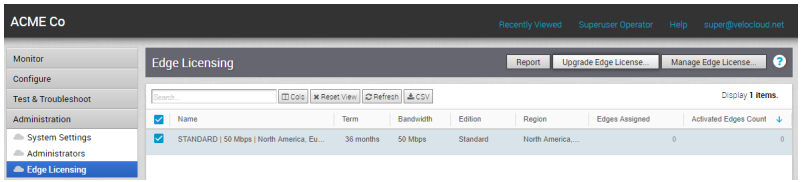
1 From the VCO navigation panel, click **Manage Customers**.

2 In the **Customer** screen, click the Customer link.

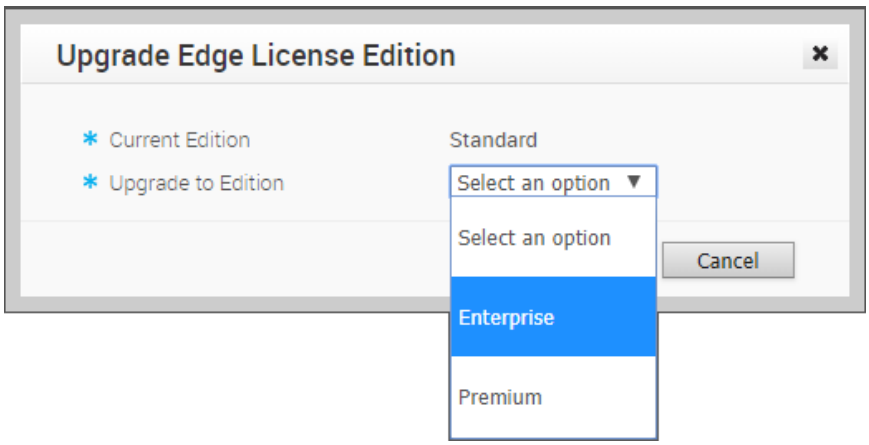
3 From the VCO navigation panel, click **Administration > Edge Licensing**.

4 Select the license type you want to upgrade.

5 In the **Edge Licensing** screen, click the **Upgrade Edge License** button.



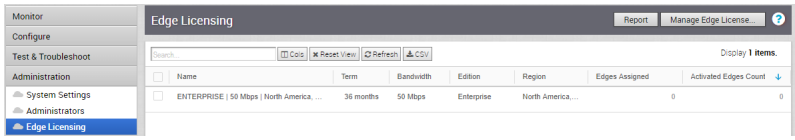
6 In the **Upgrade Edge License Edition** dialog box, choose either **Enterprise** or **Premium** from the **Upgrade to Edition** drop-down menu.



7 Click **OK**.

The **Edge Licensing** screen updates with the upgraded license type.

Note If an Operator or MSP upgrades a license edition for one of the Edges, all Edges will be upgraded to the new license edition.



Once a customer has been created, selections under the **Actions** button can be chosen to delete or modify the customer configuration, or to send a support email.

Delete a Customer

This section describes how to delete a Customer. If the Customer has associated Edges, the Edges must be deleted first.

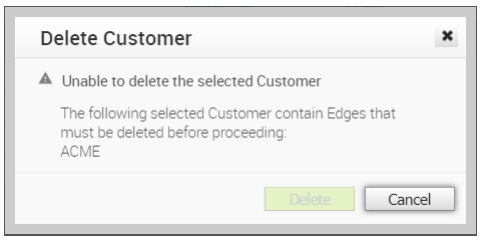
Note This section is new for the 3.3.0 release.

To delete a customer:

1 From the **Customers** screen, select a customer.

2 From the **Actions** drop-down menu, choose **Delete**.

Note If there are Edges associated with the customer, those Edges must be deleted first, before the customer can be deleted. In this type of scenario, the following dialog box displays indicating that the customer deletion is not possible until the Edges are deleted.



Configure Customers

This section describes the Operator Customer configuration.

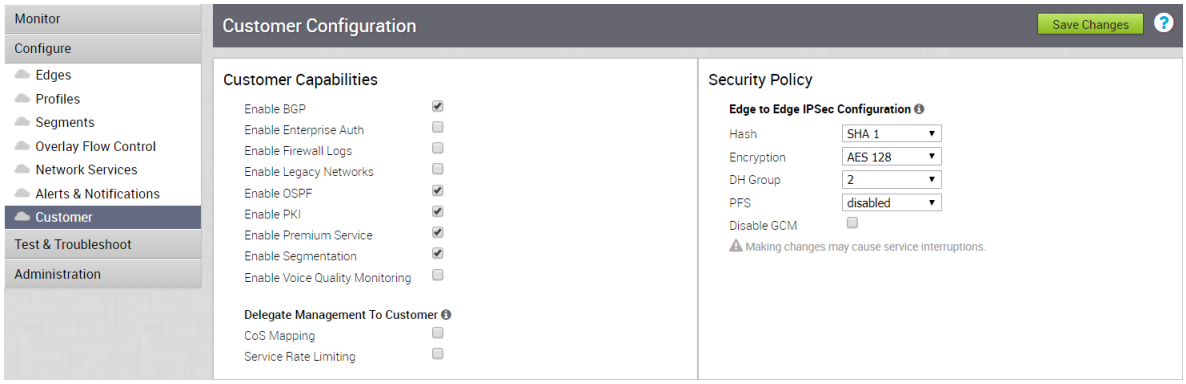
Customer Capabilities

An Operator must select the checkboxes in the **Customer Capabilities** area before an Enterprise Admin can have access to them. In the **Customer Configuration** screen, Operators can enable the following capabilities for customers:

- Enable BGP
- Enable Enterprise Auth
- Enable Legacy Networks
- Enable OSPF
- Enable PKI
- Enable Segmentation
- Enable Voice Quality Monitoring
- Delegate Management To Customer: CoS Mapping
- Delegate Management To Customer: Service Rate Limiting

Note The **Delegate Management To Customer** capabilities (**CoS Mapping** and **Service Rate Limiting**) are always visible to Customers. When Operators enable these settings, Customers can modify the settings.

To access the **Customer Configuration** screen, go to **Configure > Customer** in the Navigation Panel.



Note To enable Customer Capabilities, any System Properties associated with them must be assigned a `true` value. See Configure System Properties for more information.

Enable Segmentation

An Operator can enable Segmentation by checking the **Enable Segmentation** checkbox. For more information about Segmentation, see the *Configure Segments* and the *Overview* sections of the *Administration Guide*.

Enable BGP

An Operator can enable BGP for both Partner Gateways and VeloCloud Edge (VCE) by selecting the Enable BGP checkbox in the **Customer Capabilities** area.

Enable CoS Mapping and Service Rate Limiting

When the CoS Mapping and Service Rate Limiting are not enabled, the dialog boxes for these capabilities are Read Only. To enable customers to edit these dialog boxes, an Operator must check the **Enable Cos Mapping** and **Enable Service Rate Limiting** checkboxes.

Edge NFV

The **Edge NFV** section enables customers to deploy third party Virtual Network Functions (VNF) on service ready Edge platforms.

The current service ready Edge platform models are 520v and 840. When the Operator enables Edge NFV (by selecting BOTH the **Enable Edge NFV** and the corresponding **Security VNFs** checkboxes), the customer will be able to configure and deploy VNFs and VNF licenses from the their network services. The Operator must check BOTH checkboxes in the Edge NFV area:

- the **Enable Edge NFV** checkbox enables the ability to deploy VNF on the Edge
- the **Security VNFs** checkbox will specifically enable the ability to deploy security VNFs on the Edge

Operator Profile

This section describes the Operator profile.

Restrictions When Switching the Operator Profile

Consider the following restrictions when switching the Operator Profile:

- 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 will 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 will not receive any software image updates.

Operator Profile Area Field Description

Field	Description
Software Version	Displays the software version and build number of the Orchestrator.
Configuration Type	Indicates if the configuration type is Segment-based or Network-based.
Orchestrator Address	Displays the IP address of the Orchestrator.
Heartbeat Interval(s)	The interval between Heartbeat messages from the VeloCloud Orchestrator to Edges. The default value is 30 seconds and should not be less than 10 seconds. For more information, see the *Heartbeat* section in Chapter 9 Configure Operators.
Time Slice Interval(s)	The Timeslice value specifies the interval over which monitoring data is collected for a flow.
Stats Upload Interval(s)	The Stats Upload Interval specifies the interval for uploading monitoring data. All data for each Timeslice collected during the 'Stats Upload Interval' is uploaded.

Gateway Pool Area

The **Gateway Pool** area is located in the **Customer Configuration** screen (**Manage Customers > Configure > Customer Configurations**).

The Gateway Pool area consists of the Gateway Pool drop-down menu and display table, the Enable Partner Handoff checkbox, the Customer BGP Priority area (new for version 3.2), and the Configure Handoff area.

Customer BGP Priority

This section describes the Customer BGP priority area.

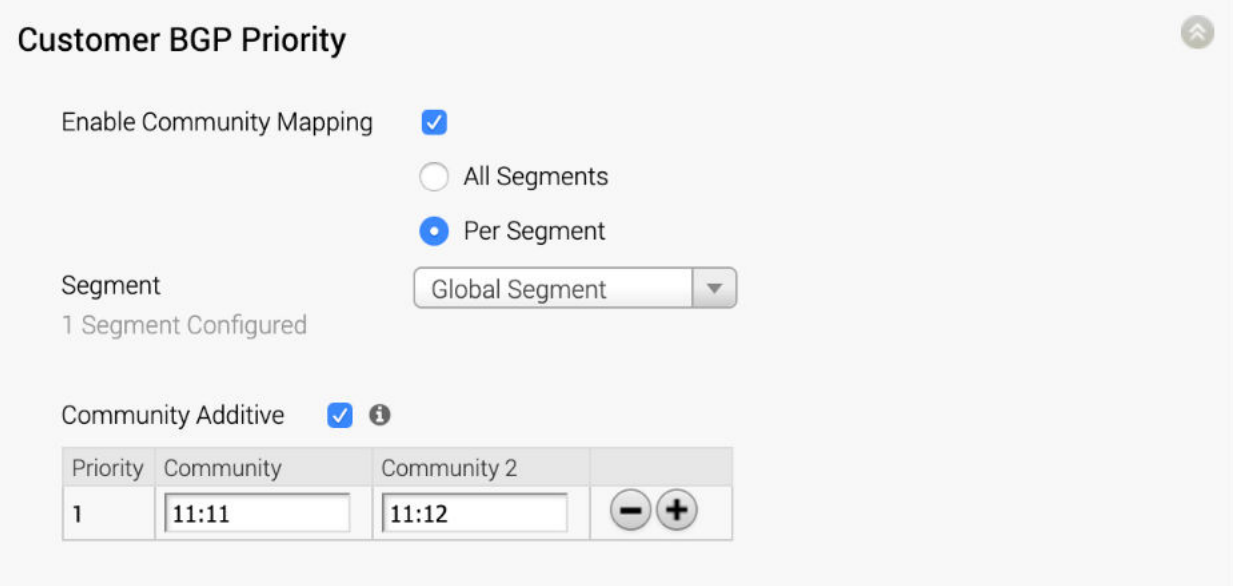
The **Customer BGP Priority** area includes the **Enable Community Mapping** checkbox. When checked, two mapping modes are available to configure communities: **All Segments** and **Per Segment**. There are two parts to the community: **Community** and **Community 2**

BGP Auto Community Additive Support

Segment-based auto community settings act as an override of incoming community attributes for a route prefix. This restricts the retaining of community attributes carried across overlay routes and the transiting via Partner Gateway to peering L3 switches.

The 3.3.2 release provides support to specify the additive option associated with a particular auto community configuration. This would in turn preserve the incoming community attributes for a prefix received from the overlay and append the configured auto community along with the Partner Gateway. Eventually, the MPLS PE side would receive prefixes with all community attributes along with the auto community attributes carried along with it. You can enable this option by checking the **Community Additive** checkbox.

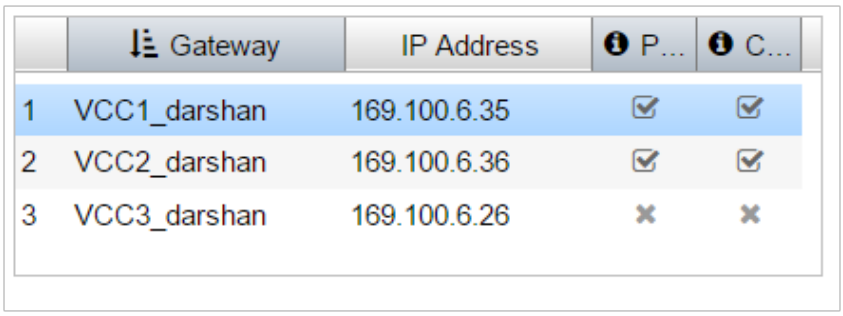
Note If you don't see the **Enable Partner HandOff** checkbox, make sure you have at least one Gateway with a Partner Gateway role in your pool.



Procedure:

1 Select a Gateway Pool from the **Gateway Pool** drop-down menu. If Gateways are available in the Pool, their names and IP addresses will display in the Gateway Pool section.

2 Click a Gateway to select it.



	Gateway	IP Address	P...	C...
1	VCC1_darshan	169.100.6.35	☑	☑
2	VCC2_darshan	169.100.6.36	☑	☑
3	VCC3_darshan	169.100.6.26	✖	✖

Note If a Gateway can be used as a Partner Handoff, you will see a checkmark under the **P** column. Gateways that have a checkmark under the **C** column have been configured for Handoff for that customer.

3 Select the **Enable Handoff Partner** checkbox.

4 For **Configure Handoff**, choose either **All Gateways** or **Per Gateway**. If you select the **Per Gateway** option, select a Gateway from the **Select Gateway** drop-down menu.

5 If you want to use Auto Community, click the **Enable Community Mapping** checkbox.

6 Choose one of two modes of configuration: **All Segments** (to configure across all communities) or **Per Segment**. (If you choose the **Per Segment mode**, select a segment from the **Segment** drop-down menu.

7 Check the **Community Additive** checkbox (new for the 3.3.2 release), if you want to preserve the incoming community attributes for a prefix received from overlay and appends the configured auto community along with it on the Partner Gateway side. See section aboved titled, "BGP Auto Community Additive Support" for more information.

8 In the **Community and Priority** area, enter a tag for the single community in the **Community** textbox. New for the 3.2 release is the option for dual community, enter a tag for **Community 2** in the appropriate textbox.

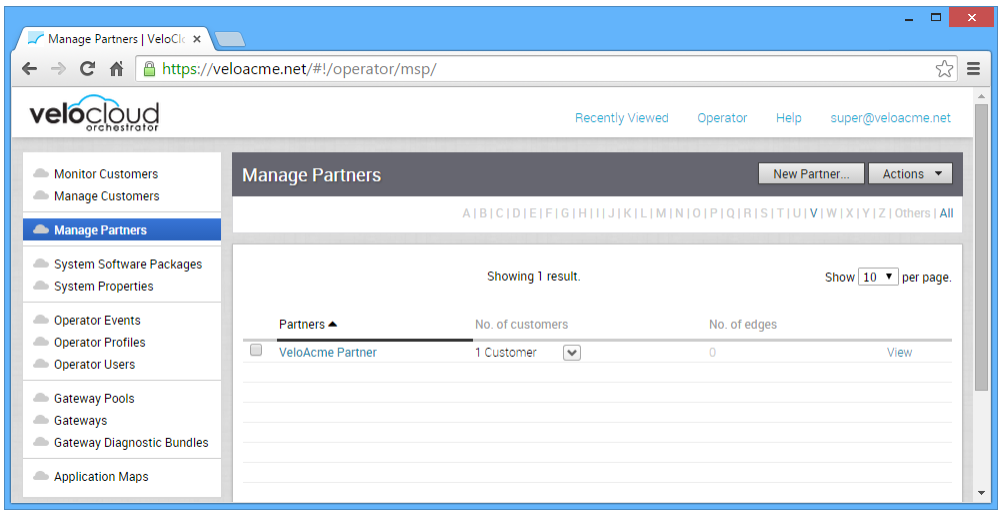
Manage Partners

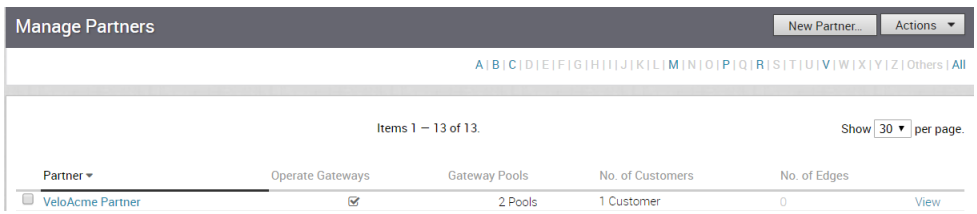
7

Operators can create and configure Partners by clicking the **Manage Partners** link from the Navigation panel on the VCO. The **Manage Partners** web page allows an Operator to create a Partner that can independently manage a group of customers.

New enhancements have been added to this feature, which allows Partners better visibility and control of Gateway assignments. Operators can now not only assign multiple Gateways to Partners and but also give them access to create and modify their own Partner Gateways that are deployed in Partner's network (Managed Gateways). See the following sections for more information on how to give Partners access to this new feature.

The **Manage Partners** web page allows an operator to create a partner that can independently manage a group of customers. The **Manage Partner** web page allows an operator with the Customer Support Role to view Partner details.





This chapter includes the following topics:

- Create a Partner

- Assign Edge License Types in Bulk
- Manage Edge Licenses

Create a Partner

This section describes how to create a partner at the Operator level. Only Operator Superusers, Standard Operators, and Business Specialist Operators can create a new partner.

Note Operator Superusers can temporarily disable the ability to create a new partner by setting the following system property to true: session.options.disableCreateEnterpriseProxy. (One of the most common reasons to use this system property is if the VCO is reaching its usage capacity). When this system property is set to true, Operator Superusers, Standard Operators, and Business Specialists will not be able to create a new partner from the VCO API or the VCO UI. However, setting this system property to true, will not prevent partners from creating Partner Admins. (Customer Support Operators do not have the ability to create a new partner; they have read only access to the Manage Partners screen in the VCO).

To create a Partner:

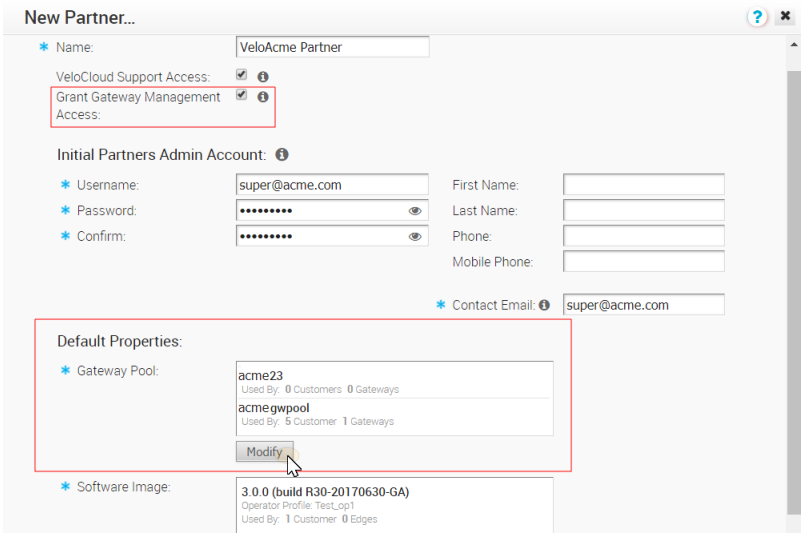
1 Click the **New Partner** button (right-hand, corner of the **Manage Partners** screen). The **New Partner** dialog box appears. Enter the name, account, and property details for the Partner.

2 If applicable, select the **VeloCloud Support Access** checkbox in the **New Partner** dialog box.

Note If the **VeloCloud Support Access** option is selected, a VeloCloud Operator with support privileges so Partners can configure and troubleshoot the customer's Edges. However, VeloCloud Support will not be able to view user-identifiable information.

3 Select the **Grant Gateway Management Access** checkbox to enable Partners to create and manage Gateways and Gateway Pools. (See image below).

Note If the **Grant Gateway Management Access** checkbox is not selected, Partners will not be able to manage or create Gateways and Gateway Pools.

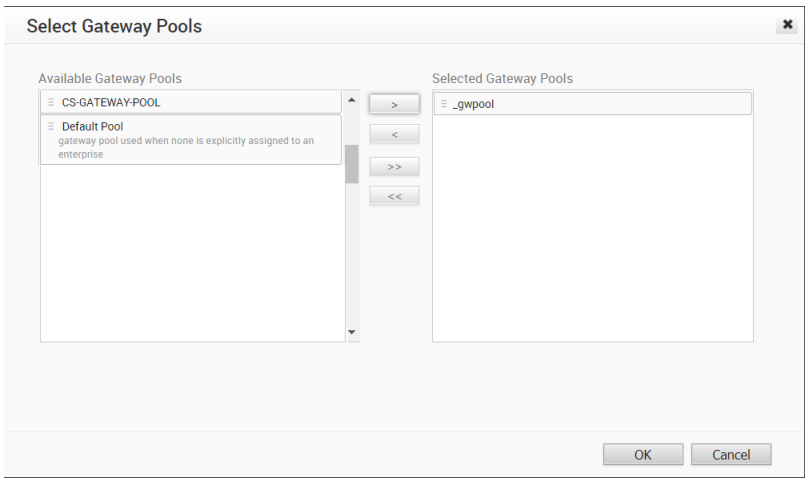


4 In the **Default Properties** area, an Operator can select gateway pools for the Partner by clicking the **Modify** button.

Note The Gateways within the selected Gateway Pools will be available to the Partner whether you select the **Grant Gateway Management Access** checkbox or not.

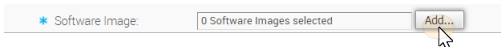
5 In the **Select Gateway Pools** dialog box, the Operator can select available Gateway Pools.

Note Operators cannot deselect a Gateway Pool that is in use by a Partner. In addition, Operators will not be able to assign a Partner owned Gateway Pool to any other Partner.

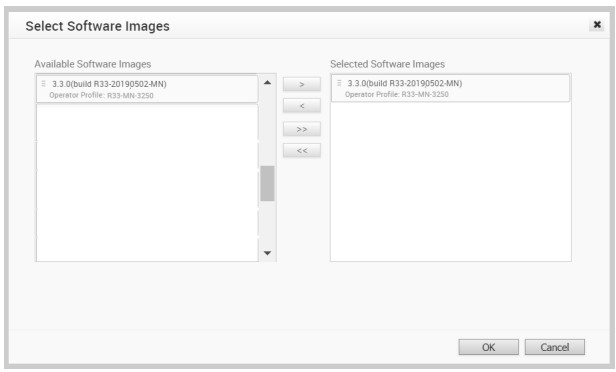


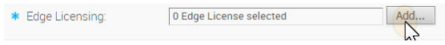
Note Operators can assign multiple Gateways and Gateway Pools to partners and give them access to create and manage their own Gateway Pools.

6 In the **Software Image** area, click the **Add** button.



7 In the **Select Software Images** dialog box, use the arrows to move software images from the **Available Software Images** area to the **Selected Software Images** area.

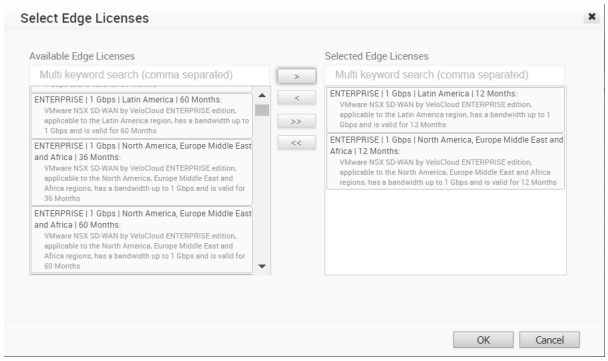


8 In the **Edge Licensing** area, click the **Add** button. 

Notes for Edge Licensing:

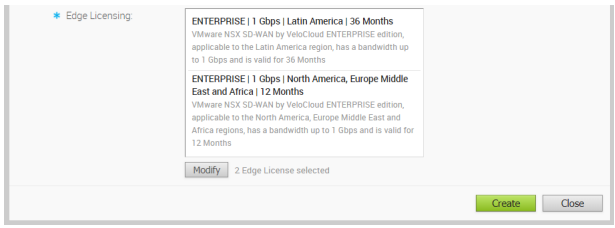
- Only a VCO Operator can assign license types to an MSP.
- Any license type in the catalog can be assigned to an MSP.
- VeloCloud recommends that Operators assign all 270 license types to Partners or all license types in the Partner's region.
- For more information about Edge Licensing, see *Edge Licensing*.

9 In the **Select Edge Licenses** dialog box, use the arrows to move license types from the **Available Edge Licenses** area to the **Selected Edge Licenses** area, as shown in the following image.



10 Click **OK** to apply the selected license types to the new Partner.

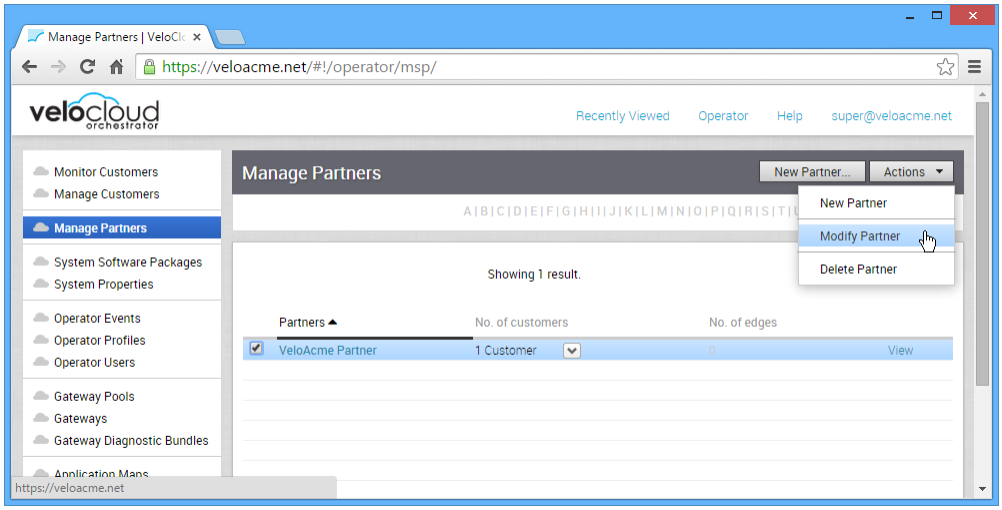
The **Edge Licensing** area refreshes to reflect the chosen license types.



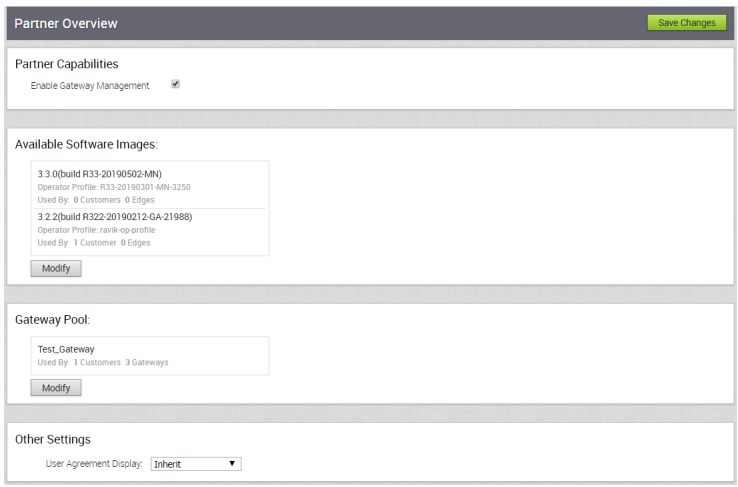
11 If you need to add or remove licenses that you have applied to a partner, click the **Modify** button.

12 Click **OK**.

Once a Partner has been created, you can choose selections under the **Actions** button to delete or modify the Partner or to add Operator Profiles.



When the **Modify Partner** option is chosen by an Operator from the **Actions** drop-down menu, the **Partner Overview** page appears. The page can be used to update the Partner's available software images, user agreement display, modify Gateway Pools, and enable Partner Capabilities.



Assign Edge License Types in Bulk

Operators, MSP, and Enterprise users can select multiple Edges and assign a single license type to all of them. This bulk assignment feature saves time when license types must be assigned to multiple Edges. It's useful when changing license types from one Edge to another is necessary.

For Operators who want to assign Edge license types in bulk:

1 From the VCO navigation panel, choose **Manage Partners**. (Operators can also assign Edge license types in bulk for Customers by choosing **Manage Customers** instead of **Manage Partners**).

2 From the **Manage Partners** screen, select a Partner.

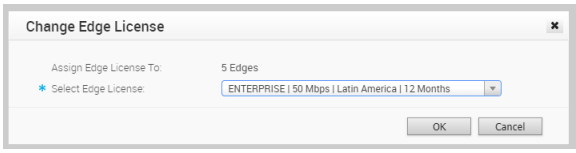
3 From the **Partner** screen, select a customer.

4 From the VCO navigation panel, go to **Configure > Edges**.

5 Select all Edges that need to be assigned a license type.

6 From the **Actions** drop-down menu, choose **Assign Edge License**.

7 From the **Change Edge License** dialog box, choose an Edge license type.



8 Click **OK**.

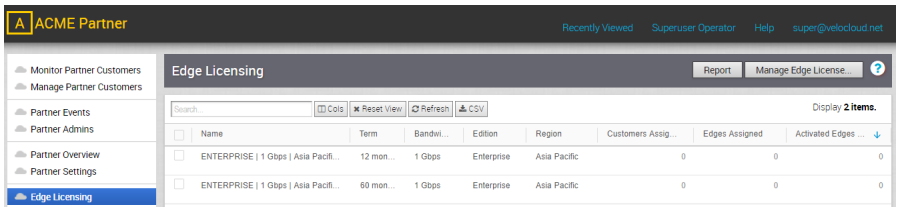
Manage Edge Licenses

To add or remove license types for an MSP:

1 From the VCO navigation panel, click **Manage Partners**.

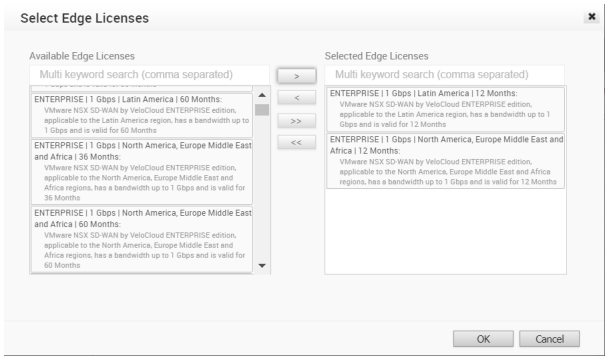
2 In the **Manage Partners** screen, click a Partner's name.

3 From the **Edge Licensing** screen for the Partner, click the **Edge Licensing** link.



4 In the **Edge Licensing** screen, click the **Manage Edge License** button.

5 In the **Select Edge Licenses** dialog box, use the arrows to move licenses from the **Available Edge Licenses** area to the **Selected Edge Licenses** area.



6 Click **OK**.

Configure the System

8

Operators can configure system software packages and system properties.

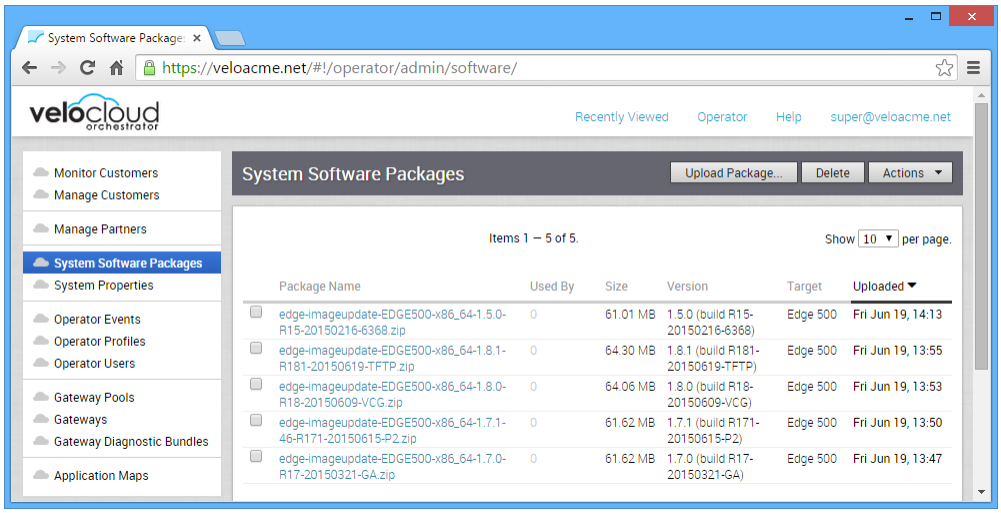
Two links, **System Software Packages** and **System Properties** are used to manage Edge software packages and to configure the operation of the VeloCloud Orchestrator. One link, **System Software Packages**, is used to view the Edge software packages available to the VeloCloud Orchestrator.

This chapter includes the following topics:

Manage System Software Packages

Operators can manage Edge software packages.

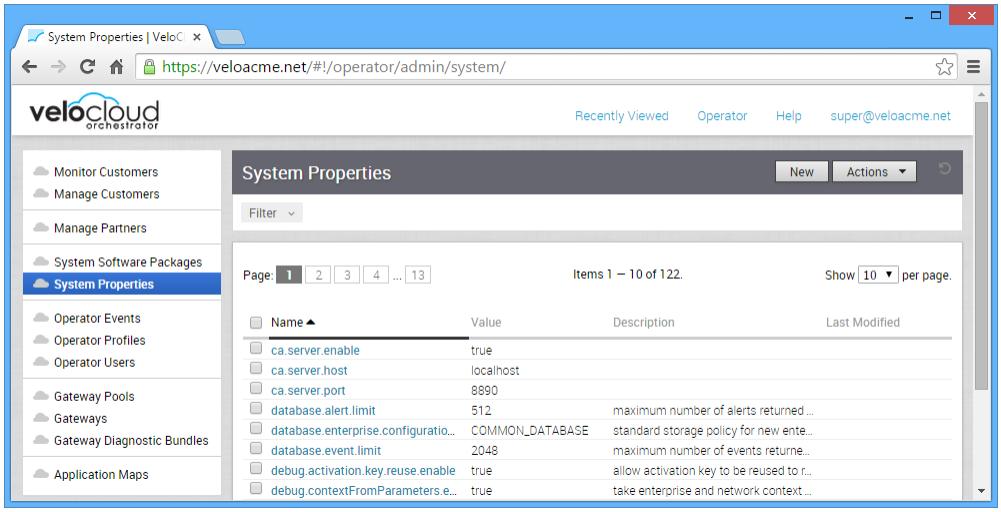
An Operator uses the **System Software** page to upload and manage Edge software packages.



Configure System Properties

Operators can configure system properties.

Numerous system properties are provided to configure the operation of the VeloCloud Orchestrator. The **System properties** page can be used to update the properties.



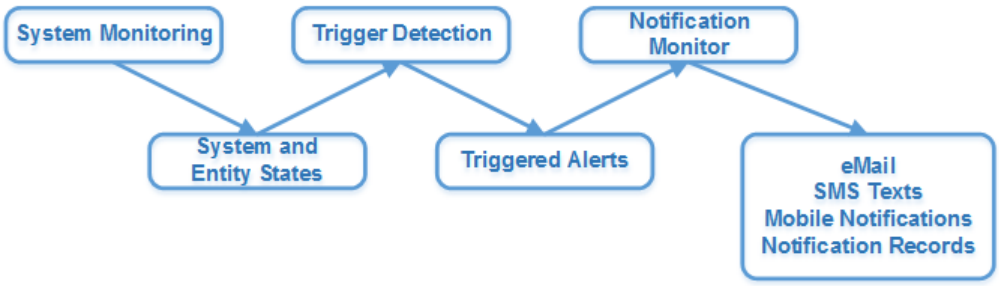
In general, you should contact a VeloCloud Support representative before making changes to the system properties. However, the following sections describe properties that can be updated by an Operator.

Properties for Alerts

This section describes the features of the VeloCloud Orchestrator alerting subsystem.

Alerts and Notifications

The following figure provides a basic overview of the alerts and notifications.



The alerting subsystem implements three pipelined functions.

Function	Description
System Monitoring	Detection and tracking of system status, including Edge, VPN, Gateway and VeloCloud Orchestrator states. System and entity states are recorded in a database.
Trigger Detection	Firing and recording of alert-triggers when system states are considered notification-worthy. The transition from a monitored state to an alert trigger is configurable, for example how long a state should persist before an alert-trigger is fired. The triggers are recorded in a database.
Notification Monitor	Notification of interested parties when alerts triggers are recorded. Notification is configurable by a customer. Customers can define who should receive notification for each event type, how soon, and how often. This process results in the delivery of notifications to configured recipients and the recording of notification entries in a database.

System States

The Alert feature will detect and monitor three system states:

State	Description
Edge Up / Down	Determined by the presence or absence of heartbeats from the Edge.
Link Up / Down	Determined by the presence of link statistics from the Edge.
VPN Tunnel Up / Down	Derived from status events from the gateway to the VeloCloud Orchestrator

Notifications

When an alert trigger is recorded in the database, notification is sent immediately to the comma / space separated list of email address in the vco.alert.mail.to system property. If no value is configured there, no notification is delivered. This notification is meant to alert VeloCloud support / operations personnel of impending issues before the customer is notified.

The customer is notified after the 'notification delay' that was configured for the corresponding alert type. If the customer has not configured the alert type, no notification is sent other than the operator notification. If the vco.alert.mail.cc property is configured, a copy of the customer's email will be sent to the list of addresses defined.

Parameterization of the alert emails is controlled by the 'mail.*' system properties. These define the SMTP relay server, the reply-to address, etc.

The following system properties configure the behavior of state monitoring, alert generation, and notification.

Monitoring

- **vco.monitor.enable** - boolean that globally enables or disables monitoring of enterprise states (Edge, Link, and VPN tunnel). This flag supercedes vco.enterprise.monitor.enable and vco.operator.monitor.enable so it can be used to turn off all monitoring with a single property. The default value is **true**.
- `vco.enterprise.monitor.enable` - boolean that globally enables or disables monitoring of enterprise states (Edge, Link and VPN tunnel). This property can be used to terminate

monitoring when a VeloCloud Orchestrator will be brought down / up or when network connectivity to the VeloCloud Orchestrator is down. Setting the flag to false prevents the VeloCloud Orchestrator from changing entity states and triggering alerts. The default value is **true**.

- **vco.operator.monitor.enable** - boolean that globally enables or disables monitoring of operator entity states (gateways only in Bacardi release). This property can be used to terminate monitoring when a VeloCloud Orchestrator will be brought down / up or when network connectivity to the VeloCloud Orchestrator is down. Setting the flag to false prevents the VeloCloud Orchestrator from changing gateway states. The default value is **true**.

Alerts

- `vco.alert.enable` - boolean that globally enables or disables the generation of alert triggers. This flag supercedes `vco.enterprise.alert.enable` and `vco.operator.alert.enable` so it can be used to turn off all alerting with a single property. The default value is **true**.
- `vco.enterprise.alert.enable` - boolean that globally enables or disables the generation of alert triggers. If `true`, state changes are allowed to generate alert triggers in the database. If `false` (and if `vco.enterprise.monitor.enable` is `true`), state changes are monitored and recorded but no alerts will occur and no triggers will be visible on the VeloCloud Orchestrator. The default value is `true`.
- `vco.operator.alert.enable` - The default value is `true`.

Notification

- `vco.notification.enable` - boolean that globally enables or disables the delivery of notifications to both operator and enterprise recipients. This flag supercedes `vco.enterprise.notification.enable` and `vco.operator.notification.enable` so it can be used to turn off all alert notifications with a single property. The default value is `true`.
- `vco.enterprise.notification.enable` - boolean that globally enables or disables the delivery of notifications to enterprise recipients. If monitoring and alerts are enabled, the effect of notification disable is to processes alert triggers as normal but notifications are not sent (they are permanently lost, they will not be sent at a later time). The default value is **true**.
- `vco.operator.notification.enable` - boolean that globally enables or disables the delivery of notifications to operator recipients. If enterprise monitoring and alerts are enabled, the effect of notification disable is to skip the notification of operator recipients (notifications are permanently lost, they will not be sent at a later time). The default value is **true**.

Mail

- `vco.alert.mail.to` - all triggered alerts generate an email to the list of addresses configured in this system property. This is meant to be used to pre-alert VeloCloud support before the customer sees an alert. If the value is empty or contains bad email addresses, no pre-notification will be sent.

- `vco.alert.mail.cc` - alert emails sent to customers will be CC'd to the list of email addresses configured in this system property. This is meant to be used as a ' VeloCloud-sees-what-the-customer-sees' support feature. If the value is empty or contains bad email addresses, no cc notification will be sent.

SMTP

SMTP must be configured or emails will not be sent.

- **mail.*** - configure the SMTP parameters for email sent from the VeloCloud 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 VCO.
- `mail.smtp.port` - SMTP port.
- `mail.smtp.secureConnection` - use SSL for SMTP traffic.

PKI

- `session.options.pkiEnabled` - expose PKI configuration and status pages.
- `session.options.enablePki` - enable PKI.

Edge

- `edge.offline.limit.sec` - if this number of seconds passes without detecting a heartbeat from an Edge, a state transition from CONNECTED → DEGRADED or DEGRADED → OFFLINE is made. The default value is 60 seconds.
- `edge.link.unstable.limit.sec` - if this number of seconds passes without the receipt of link statistics for a link, a state transition from STABLE -> UNSTABLE is made. The default value is 360 seconds (one minute longer than the link status push interval).
- `edge.link.disconnected.limit.sec` - if this number of seconds passes with the receipt of link statistics for a link, a state transition to DISCONNECTED is made regardless of the current state. The default value is 720 seconds.
- `edge.deadbeat.limit.days` - edges that have not been heard from in this many days are not considered for alert generation. This is primarily used to prevent large numbers of alerts from being generated when the feature is first deployed.

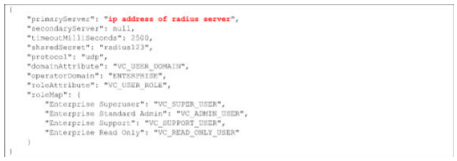
VPN

- `vpn.disconnect.wait.sec` - system wait interval after receipt of a VPN DISCONNECTED or VPN_FAIL event before a transition from CONNECTED → DISCONNECTED is made. The default value is 90 seconds.
- `vpn.reconnect.wait.sec` - system wait interval after receipt of a VPN CONNECTED event before a transition from DISCONNECTED → CONNECTED is made. The default value is 45 seconds.

Radius Authentication

The image below represents an example of the first two attributes listed below (radius authentication for both Operator and Enterprise).

- `vco.operator.authentication.radius`
- `vco.enterprise.authentication.radius`



- `vco.enterprise.authentication.mode`
- `vco.operator.authentication.mode`

Self-service Password Reset

Note Content for 'Self-service Password Reset' is new for the 3.3 release.

- **Enterprise:**
  - `vco.enterprise.resetPassword.token.expirySeconds`- For Enterprise users who will initiate the reset of their own password: After a self-service password reset link is emailed to a user, this property represents the length of time the self-service password reset link will be valid. After the length of time has passed, the link will expire.
  - `vco.enterprise.selfResetPassword.token.expirySeconds`- For Operators or Customer Admins who initiate the reset of an Enterprise user's password: After a self-service password reset link is emailed to a user, this property represents the length of time the self-service password reset link will be valid. After the length of time has passed, the link will expire.
  - `vco.enterprise.resetPassword.twoFactor.mode`- The second factor password reset authentication mode for all Enterprise users. Currently, the only option is SMS.
  - `vco.enterprise.resetPassword.twoFactor.required`- For Enterprise, the require/not required two factor authentication for password reset.
  - `vco.enterprise.selfResetPassword.enabled`- For Enterprise, the enable/disable self-service password reset.
- **Operator:**
  - `vco.operator.selfResetPassword.enabled`- For Operators, the enable/disable self service password reset.
  - `vco.operator.selfResetPassword.token.expirySeconds`- After a self-service password reset link is emailed to a user, this property represents the length of time the self-service password reset link will be valid. After the length of time has passed, the link will expire.

- `vco.operator.selfResetPassword.twoFactor.required`- Operator require/ not required two factor authentication for self service password reset.

Two-factor Authentication

- `vco.enterprise.authentication.twoFactor.enable` - Enterprise enable / disable for second factor authentication.
- `vco.enterprise.authentication.twoFactor.mode` - Second factor authentication mode for all enterprise users. Presently, the only option is SMS.
- `vco.enterprise.authentication.twoFactor.require` - Second factor authentication required for all Enterprise Users.
- `vco.operator.authentication.twoFactor.enable` - Operator enable / disable for second factor authentication.
- `vco.operator.authentication.twoFactor.mode` - Second factor authentication mode for all operator users. Presently, the only option is SMS.
- `vco.operator.authentication.twoFactor.require` - Second factor authentication required for all Operators.

When the required property is set to false (the default):

- Only enforce two factor authentication on users with mobile phone numbers.
- Allow a super user to disable two factor authentication temporarily for specific user.
- When users don't have mobile phone numbers, bypass the two factor authentication screen altogether.

When the required property is set to true:

- Enforce two factor authentication on all users by default there for locking out users that do not have mobile phone numbers.
- Allow a super user to disable two factor authentication temporarily for specific user.
- Mobile phones should be required when creating users impacted by two factor authentication.

User Agreements

`session.options.enableUserAgreements` - Enables the end user service or license agreement functionality.

`vco.enterprise.userAgreement.display.mode` - Displays the end user service or license agreement to the superusers specified in the Value text field. Set the **Value** text field to one of the following, “NONE,” “ALL,” “WITH_MSPS,” “WITHOUT_MSPS.” The default value is set to “NONE.” The “ALL” value includes Enterprise Superusers and Partner Superusers.

Edge License

`session.options.enableEdgeLicensing`- Enables Edge the licensing feature Orchestrator-wide.

Segmentation

`enterprise.capability.enableSegmentation`- Enable or disable the segmentation capability for enterprise. When the value is set to true, a default Profile (Initial Segmented Operator Profile) will be created in the **Operator Profiles** area. When the value is set to false, a default Profile (Initial Operator Profile) will be created in the **Operator Profiles** area.

Edge Link Event

- `vco.operator.alert.edgeLinkEvent.enable` - Global enable / disable operator alert for edge link event. Default value : True

Edge Liveness Event

- `vco.operator.alert.edgeLiveness.enable` - Global enable / disable operator alert for edge liveness event. Default value: True

Disable Creating New Customers

- `session.options.disableCreateEnterprise` Operator Superusers can disable the ability to create a new customer by setting this system property to true. (One of the most common reasons to use this system property is if the VCO is reaching its usage capacity). When this system property is set to true, Operator Superusers, Standard Operators, and Business Specialists Operators will not be able to create a new customer from the VCO API or the VCO UI. Default value: False
- `session.options.disableCreateEnterpriseProxy` Operator Superusers can disable the ability for partners to create a new customer. (One of the most common reasons to use this system property is if the VCO is reaching its usage capacity). When this system property is set to true, Partner Superusers and Partner Standard Admins will not be able to create a new customer from the VCO API or the VCO UI. Default value: False (NOTE: Setting this system property to true, will not prevent Partner Superusers from creating Partner Admins).

Disable Creating New Partners

- `session.options.disableCreateEnterpriseProxy` Operator Superusers can disable the ability to create new partners. (One of the most common reasons to use this system property is if the VCO is reaching its usage capacity). When this property is set to true, Operator Superusers, Standard Operators, and Business Specialists will not be able to create a new Partner from the VCO API or the VCO UI. Default value: False (NOTE: Setting this system property to true, will not prevent Partners from creating Partner Admins).

Configure Operators

9

Three links, **Operator Events**, **Operator Profiles**, and **Operator Users**, are used to view events, manage profiles, and manage users.

This chapter includes the following topics:

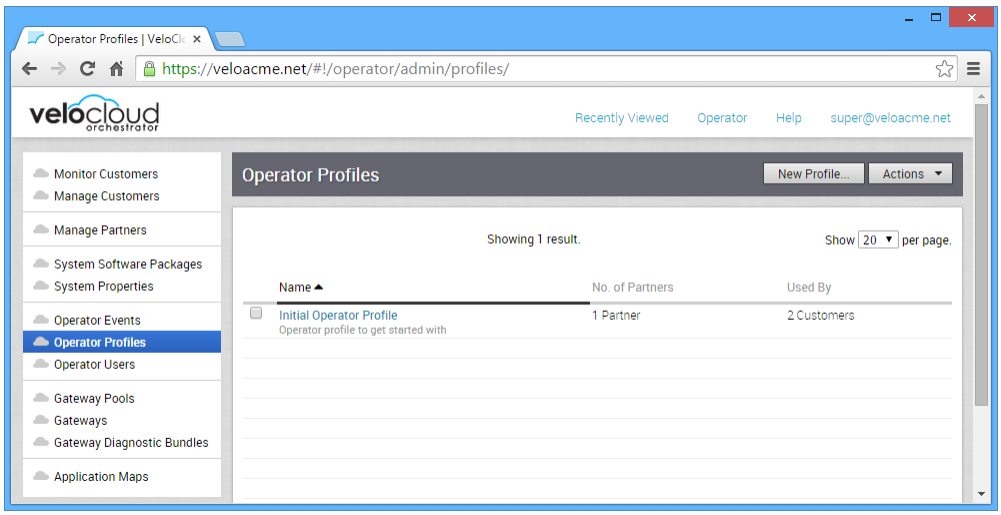
Monitor Operator Events

The **Operator Events** web page displays the operator events generated by the VeloCloud.

These events can help you determine the status of the VeloCloud system. For some events, you can click on a link in the event to display more information.

Configure Operator Profiles

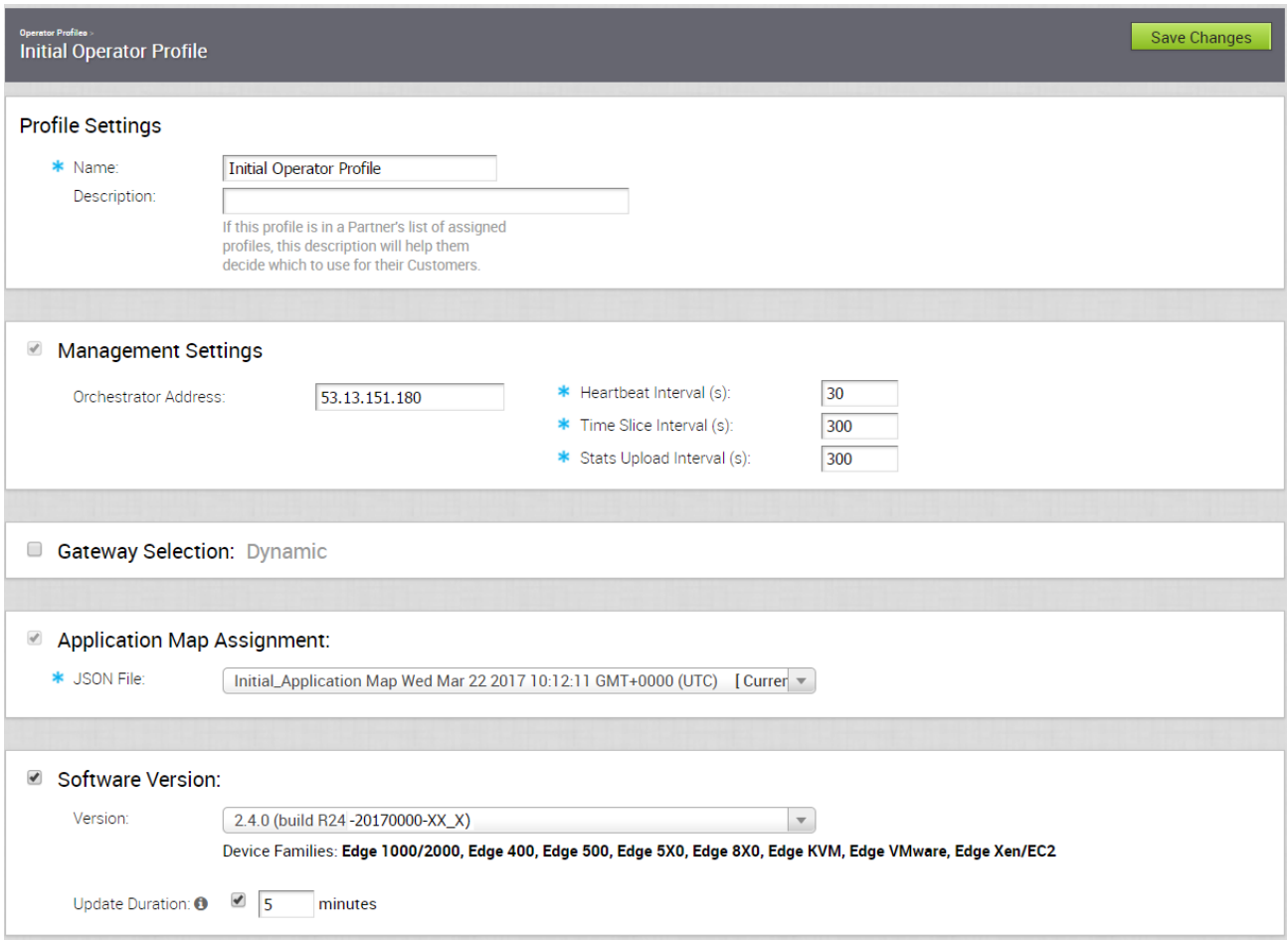
An Operator Profile is used to specify default settings for the network being managed by the VeloCloud Orchestrator. When you create a customer, you can choose a profile for that customer. An initial profile is provided when the VeloCloud Orchestrator is installed. You can add additional profiles.



Operator Profiles Screen Overview

This section describes the **Operator Profile** screen.

An Operator Profile specifies the information shown in the following example.



The following sections describe the information in the **Operator Profile** screen.

Profile Settings

The **Profile Settings** area provides text boxes for the profile name and description.

Management Settings

The **Management Settings** area specifies the primary and secondary VeloCloud Orchestrator IP addresses and management intervals.

The following sections describe the available management intervals.

Heartbeat

The Heartbeat value specifies the interval between Heartbeat messages from the VeloCloud Orchestrator to Edges. The default value is 30 seconds and should not be less than 10 seconds. If two Heartbeats to an Edge are missed, the Edge is marked as down.

Note Changing the heartbeat interval may require changing the VeloCloud Edge Offline Alert Notification Delay to avoid unnecessary alerts.

For example, if the default Heartbeat of 30 seconds is used, an Edge could miss two Heartbeats after one minute (and be marked down) but return to normal operator at the next Heartbeat. In this scenario, the Edge would be marked down for only 30 seconds. This is less than the default VeloCloud Edge Offline Alert Notification Delay of two minutes, and an alert is not sent. However, if the Heartbeat is set to five minutes, for example, anytime the Edge goes down, it will be for at least five minutes. This is more than the alert notification delay and an alert will be sent.

Timeslice

The Timeslice value specifies the interval over which monitoring data is collected for a flow.

Stats Upload

The Stats Upload value specifies the interval for uploading monitoring data. All data for each Timeslice collected during the Stats Upload Interval is uploaded.

Gateway Selection

Gateway Selection specifies the **Dynamic** or **Static** selection of Gateways. If **Gateway Selection** is not selected, the Gateway is selected dynamically and Gateways are chosen from the Gateway Pool.

The specific Gateway chosen depends on the flow type (Edge-to-Data Center, Edge-to-Edge, or Edge-to-Internet). Business Policy and Edge-to-Edge regional location can also influence Gateway selection.

At least two Gateways (and their associated secondary Gateway) should be defined in the pool so that the Gateway selection is most efficient. If **Gateway Selection** is selected, the Gateway is statically selected and you need to specify the Primary Gateway and, optionally, a Secondary Gateway. Use the **Static** option only for test/debug purposes because it specifies a specific Gateway that is used for all flow scenarios.

Application Map Assignment

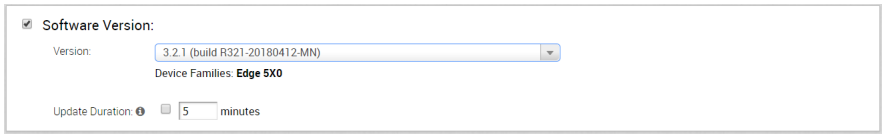
The **Application Map Assignment** area specifies the list of applications available when specifying the Business Policy.

Software Version

The **Software Version** area specifies the Edge platform and software versions for the operator profile.

Software Version

If the **Software Version** checkbox is unselected, no updates will be applied to an Edge. If the **Software Version** checkbox is selected (see image below), you can specify the software version that will be applied to your deployed Edges. After you have selected your desired software version, click the **Save Changes** button at the top, right corner of the **Operator Profile** screen. Devices with this profile will not update from their current software image.



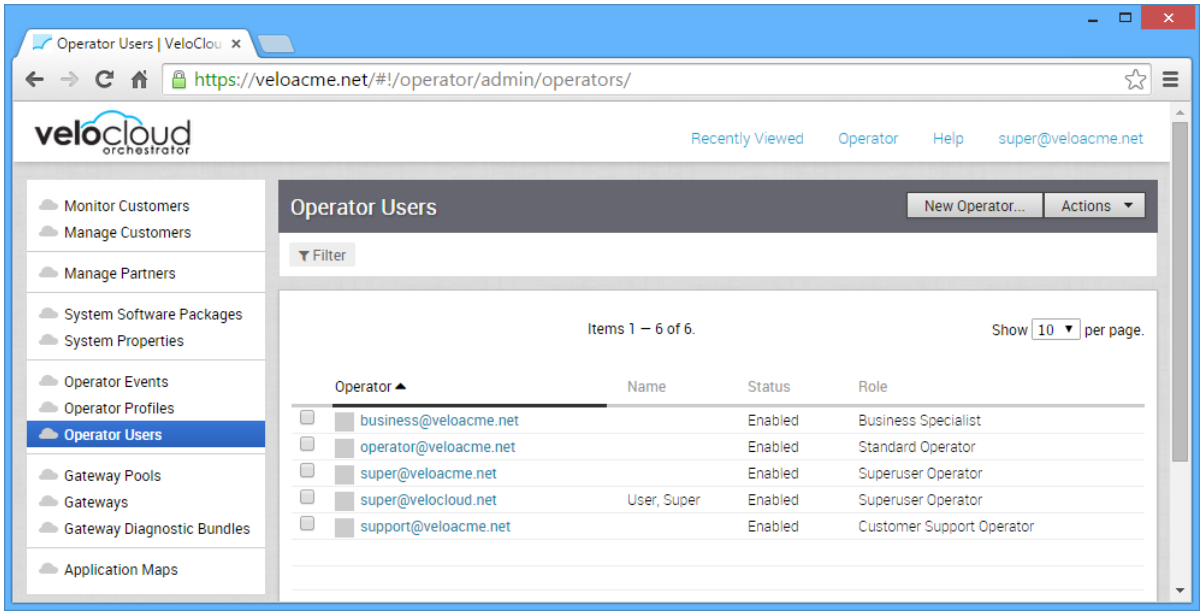
Update Duration

Update Duration defines a time interval over which all Edges receive their image update. Updates are spread evenly over this interval, reducing peak download volumes from the Orchestrator.

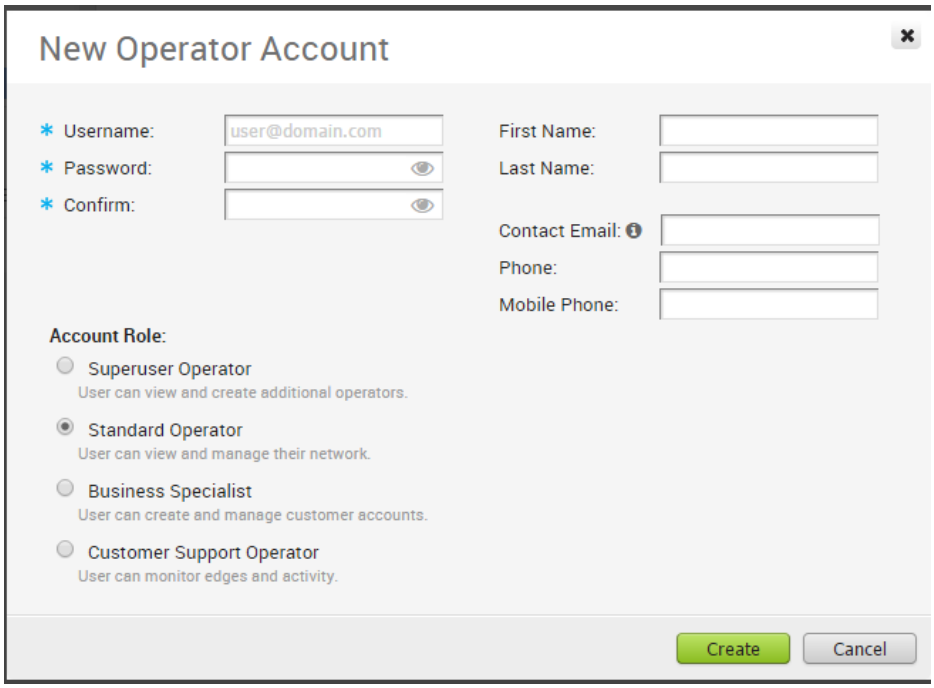
Configure Operator Users

The **Operator Users** web pages are used to create one or more operators and to view/change Operator user settings.

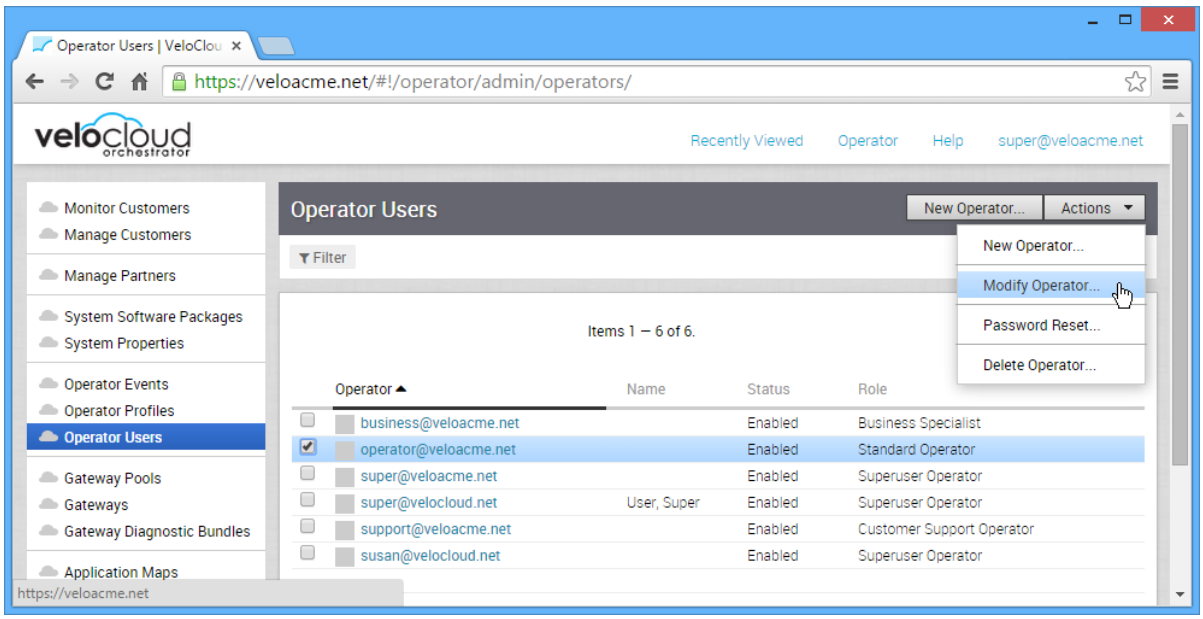
The Operators are listed when you click the **Operator Users** link.



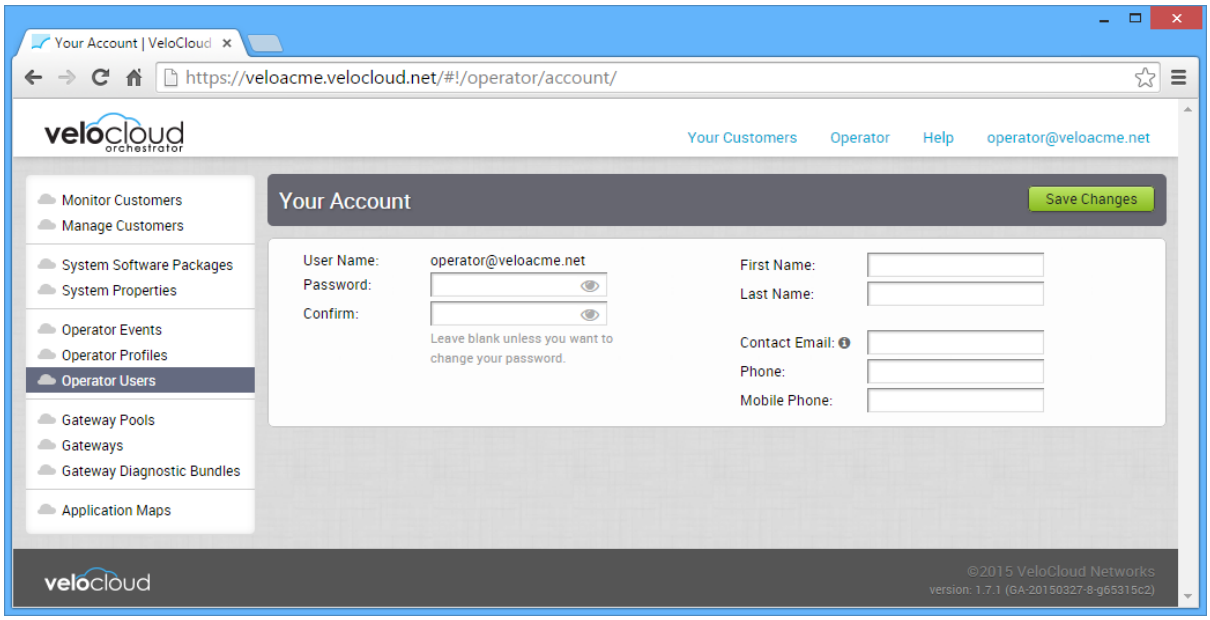
If you are logged in as an Operator that has the Superuser role, you can create additional Operators and specify their role.



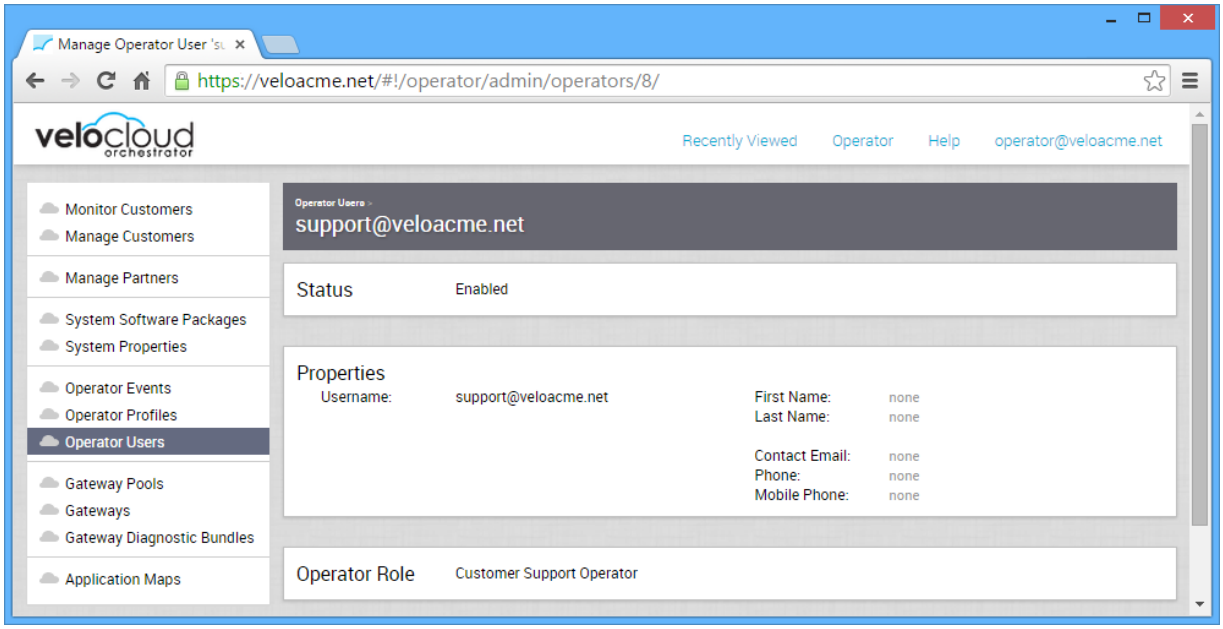
As an Operator with the Superuser role, you can modify and delete existing Operators.



If you select your Operator user name from the list of operators, you can update your password and account details.



If you select an Operator other than your own from the list of operators, you can view account details for the Operator.



Configure Orchestrator Authentication

Radius, Native, and Single Sign On (SSO) are the modes available for authentication and authorization in VeloCloud Orchestrator (VCO). Only an Operator can enable the Radius and Native modes for both Operator and Enterprise authentication. Any Operator user with super user permission can set up and configure Single Sign On (SSO) mode in VCO.

You can select your mode of choice in the **Configure Authentication** screen from the **Authentication Mode** drop down menu.

Native Mode

The Native mode of authentication is locally defined on the VCO.

Radius Authentication Mode

There are two possible deployments for the Radius Authentication Mode:

Deployment	Description
Single Radius Server	The same radius server is shared between the Operator and the Enterprise customer.
Separate Radius Servers	There is one Radius server for Operator/SP and a second one for all Enterprise Customers.

Single Sign On Mode

For the 3.3.1 release, the VeloCloud Orchestrator (VCO) supports a new type of user authentication called Single Sign On (SSO) for all Orchestrator user types: Operator, Partner, and Enterprise.

Operator users with super user permission can setup and configure SSO in VCO. For step-by-step instructions to configure SSO for Operator user, see Configure Single Sign On for Operator User.

Define System Properties for Authentication

This section describes system properties for authentication.

You must first define system properties for the VCO to communicate with the Radius server. To define a system property, go to the **System Properties** screen, and click the **New System Property** button.

The four system properties that must be defined for Radius authentication are listed below. See the images below for dialog examples of System Properties 1 and 2.

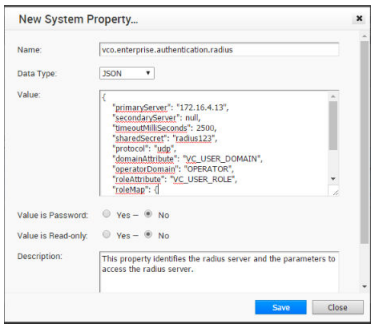
Property #1: `vco.enterprise.authentication.radius`

Property #2: `vco.enterprise.authentication.mode`

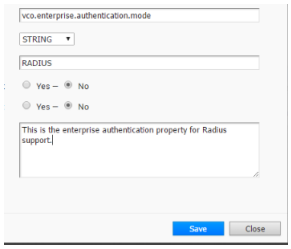
Property #3: `vco.operator.authentication.radius`

Property #4: `vco.operator.authentication.mode`

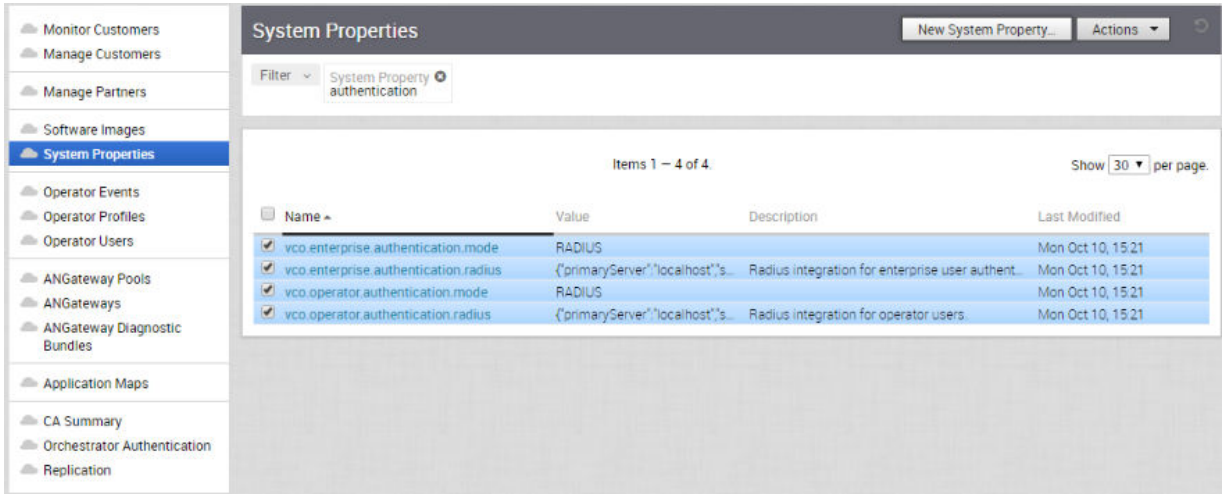
System Property #1 Dialog Example for Enterprise authentication



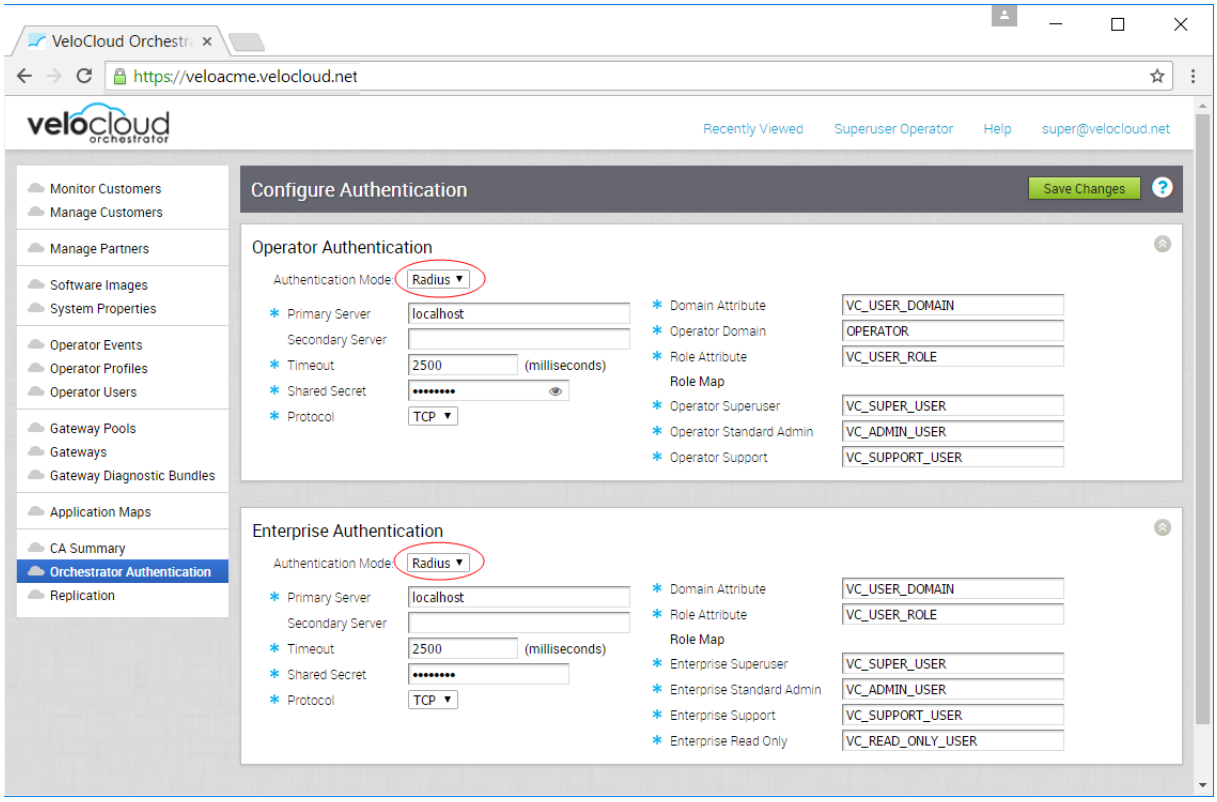
System Property #2 Dialog Example for Enterprise authentication



The following image shows an example of fully configured system properties.



After the system properties have been defined, you can configure the Operator and the Enterprise authentication on the VCO. From the **Orchestrator Authentication** screen, choose **Radius** as the authentication mode.



Configure Operator Single Sign On

For the 3.3.1 release, Single Sign On (SSO) mode is newly added in **Orchestrator Authentication** screen.

Overview of Single Sign On

For the 3.3.1 release, the VeloCloud Orchestrator (VCO) 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 VCO users to log in to the VCO with one set of login credentials to access multiple applications. Integrating the SSO service with VCO improves the security of user authentication for VCO users and enables VCO 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 VeloCloud Orchestrator (VCO). To setup SSO authentication for Operator user, perform the steps on this procedure.

To configure single sign on for an Operator user:

Prerequisites

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

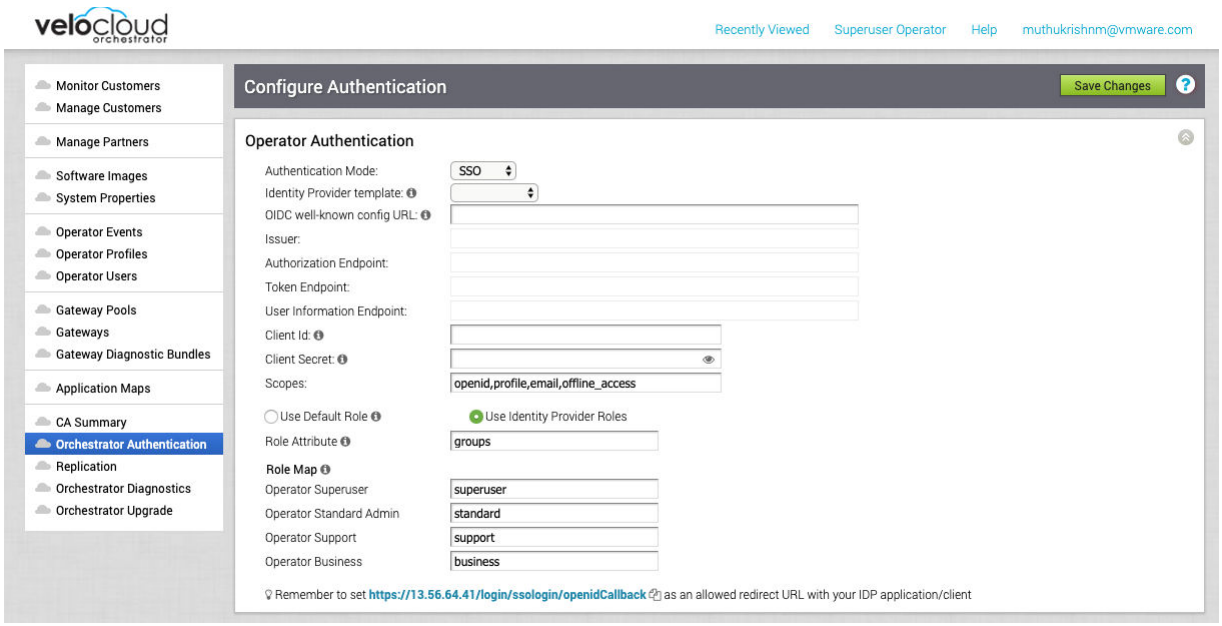
Note SSO integration at the Operator management level of a VMware hosted VeloCloud Gateway is reserved for the VMware SD-WAN TechOPS operators. Partners with Operator level access of a hosted orchestrator do not have the option to integrate to an SSO service.

Procedure

1 Log in to the VCO application as Operator super user.

2 Click **Orchestrator Authentication**.

The **Configure Authentication** screen appears.



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 VCO 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 VCO, select one of the options:

- **Use Default Role** – Uses the role set up in the VCO, by default. The supported roles are: Operator Superuser, Operator Standard Admin, Operator Support, and Operator Business.
- **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 VCO 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 VCO 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 VCO test call back, a successful validation message appears.

Results

The SSO authentication setup is complete in VCO.

What to do next

Chapter 4 Log in to the SD-WAN Orchestrator Using SSO for Operator User

Configure Gateways and Gateway Pools

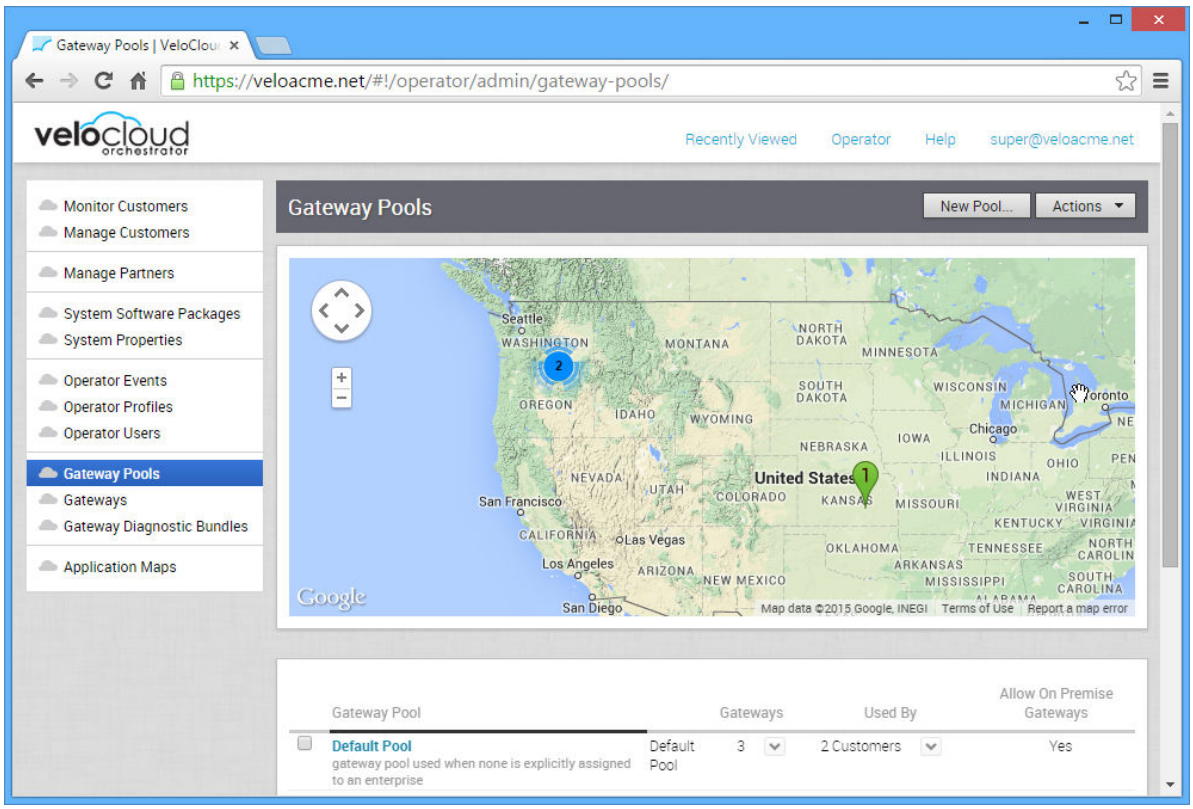
10

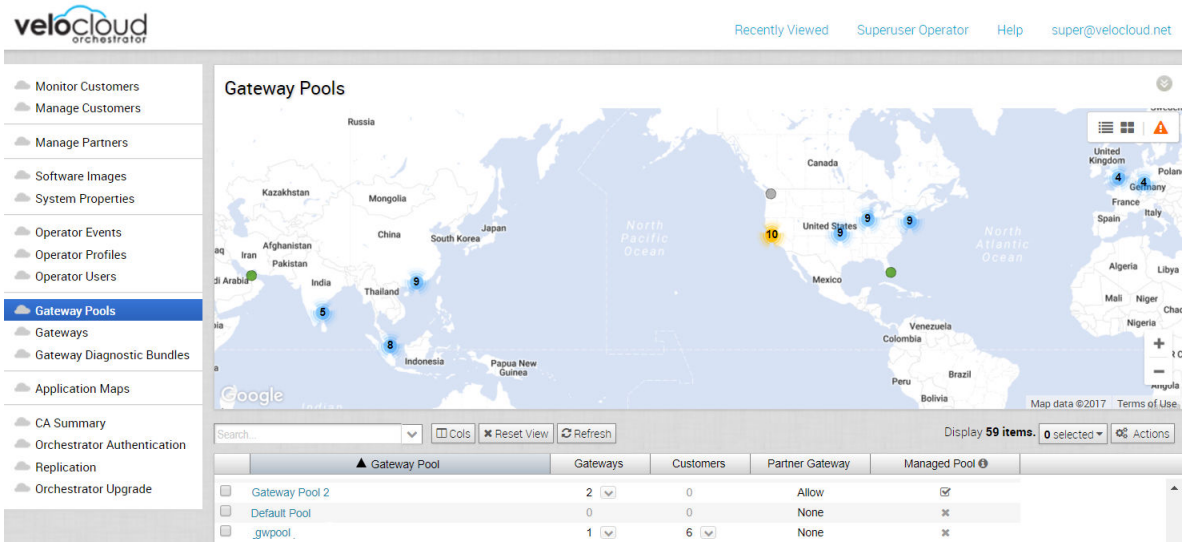
VeloCloud's network consists of multiple service Gateways deployed at top tier network and cloud data centers around the world, providing scalability, redundancy and on-demand flexibility. The Gateways provide the advantage of cloud-delivered services and optimized paths to all applications, branches and data centers. Service providers can also deploy their own On-Premise Gateways in their private cloud infrastructure.

This chapter includes the following topics:

Gateway Pools

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





Managed Pool Column

Check marks in the **Managed Pool** column that are associated with Gateway Pools represent Gateway Pools that Partners can edit and manage. If a Gateway Pool has an “x” associated with it, Partners have just ‘read-only’ access to that Gateway Pool.

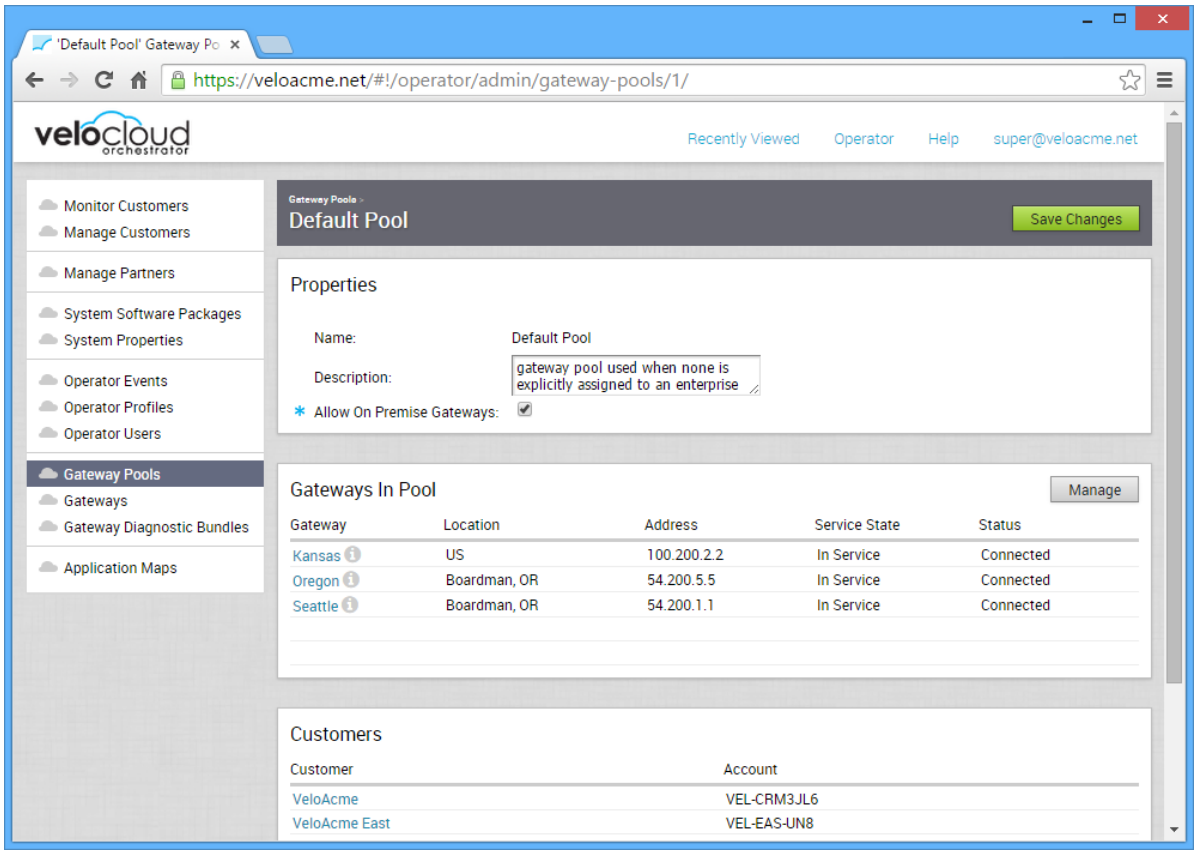
Note If an Operator checks the **Grant Gateway Management Access** checkbox, Gateway Pools assigned to a Partner will display under the **Managed Pool** column with a check mark associated with it.

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.

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 VeloCloud Gateway can function as a standard Gateway that provides VeloCloud 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.



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 VCO Partner Portal:

1 From the VCO 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).

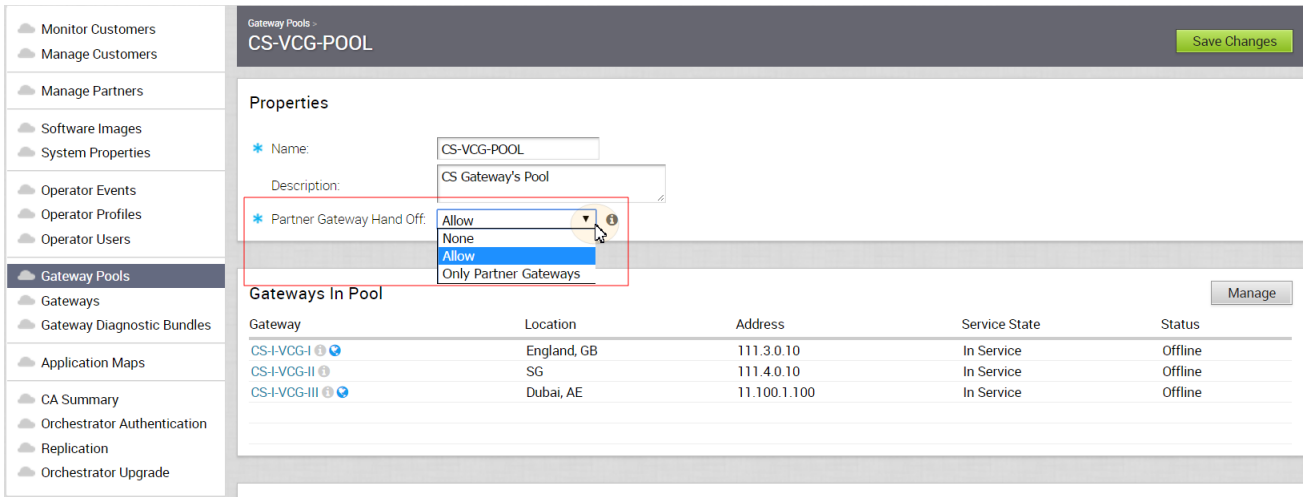
> **Note** In the above steps, you are creating Partner specific Gateways; therefore, any Gateways or Gateway Pools you create will only be associated with this Partner.

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 he or she can delete it.

Partner Gateway Hand Off

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



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.

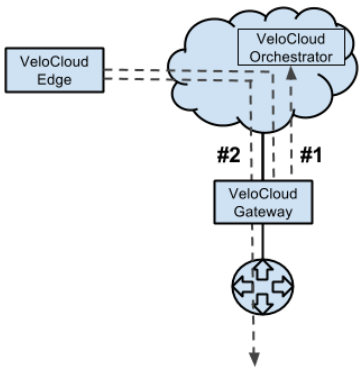
Overview of Partner Gateways

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

Consider the following figure, in which 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 VeloCloud Orchestrator in the public cloud, and there must be a path to reach the cloud. The VeloCloud Gateway can selectively NAT certain traffic (such as the IP address of a VeloCloud Orchestrator, or the subnets used to reach a public DNS servers) even though it is operating in VLAN/VRF mode.

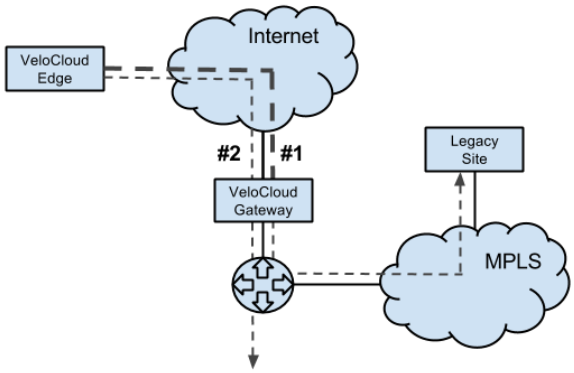


- #1 - VCO traffic is routed via IP address(es) to NAT
- #2 - Corporate Traffic is routed via subnet(s) to VLAN/VRF

Gateway Configuration Use Case #2

Additionally, it is a common use case 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 VeloCloud. For this use case, it is necessary to specify traffic by subnet on the Partner VeloCloud Gateway. Each subnet can also be configured to encrypt network traffic.

The diagram below shows an example in which only the traffic to legacy sites is encrypted. If the VeloCloud 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 would be to add the private subnet for your legacy sites and mark it as encrypted.

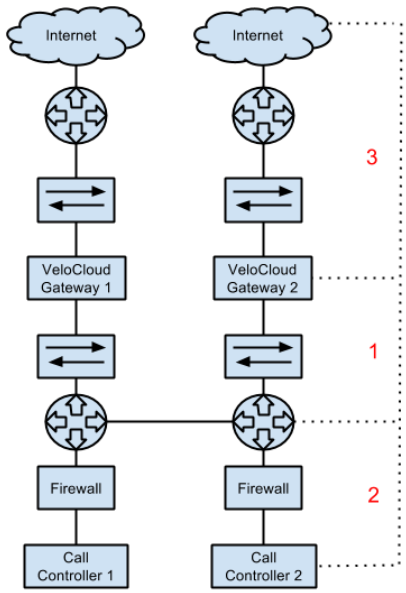


- #1 - Subnet (e.g. 10.0.0.0/8) defined for Legacy Sites and marked for encryption. Traffic is transmitted between VeloCloud Edge and VeloCloud Gateway over the IPsec tunnel.
- #2 - Remaining traffic is sent unencrypted to the VeloCloud Edge, and then to its final destination.

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.

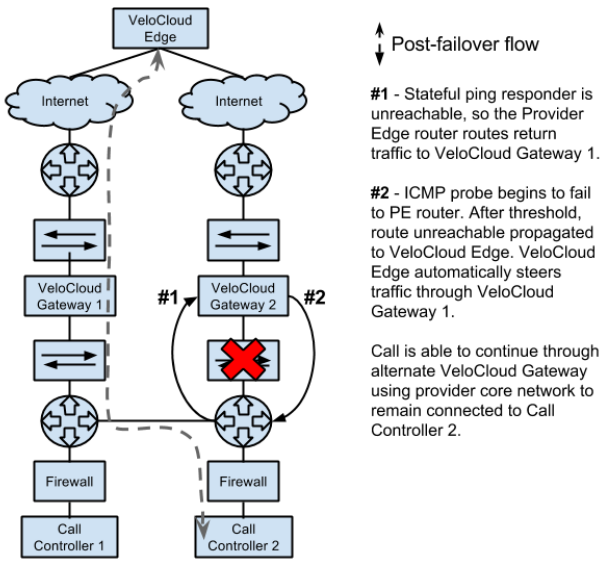
Consider the following Gateway topology:



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 VeloCloud Gateway, or from the VeloCloud Gateway to the Provider Edge router.
2	Call Controller	The VeloCloud Gateway should be able to ping the Provider Edge router or Call Controller to verify connectivity.
3	WAN	The VeloCloud 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 VeloCloud Gateway and Provider Edge router and describes the activity that occurs.



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 VeloCloud Gateway topology diagram, the VeloCloud 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 VeloCloud 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 VeloCloud 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 VeloCloud Edges connect to the primary VeloCloud Gateway. The primary VeloCloud Gateway marks routes as reachable.

2 The Primary VeloCloud Gateway fails to receive a reply for three successive probes (~6 seconds).

3 The Primary VeloCloud Gateway marks routes as unreachable and communicates this to all connected Edges.

4 Edges begin routing traffic via the alternate VeloCloud Gateway.

5 Connectivity is restored and the primary VeloCloud Gateway receives three successive replies from probes.

6 The Primary VeloCloud Gateway marks routes as reachable and communicates this to all connected Edges.

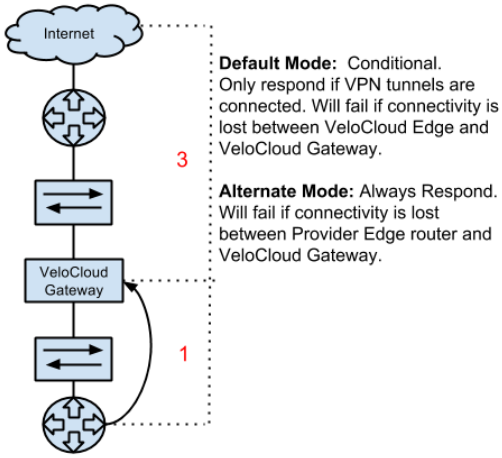
7 Edges route traffic back through the primary VeloCloud Gateway.

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 VeloCloud 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 VeloCloud 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 VeloCloud 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 VeloCloud Gateway only respond if VPN tunnels are connected - this is similar to the behavior with BGP (no clients connected means no client routes).



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.

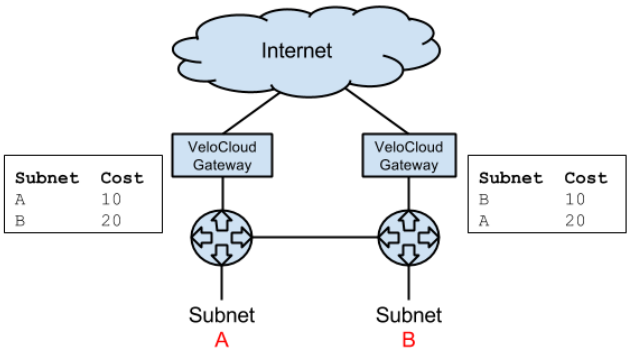
- Reverse flow is not supported in the NAT hand-off mode.

Active/Backup Subnets

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

Subnets on a Partner Gateway

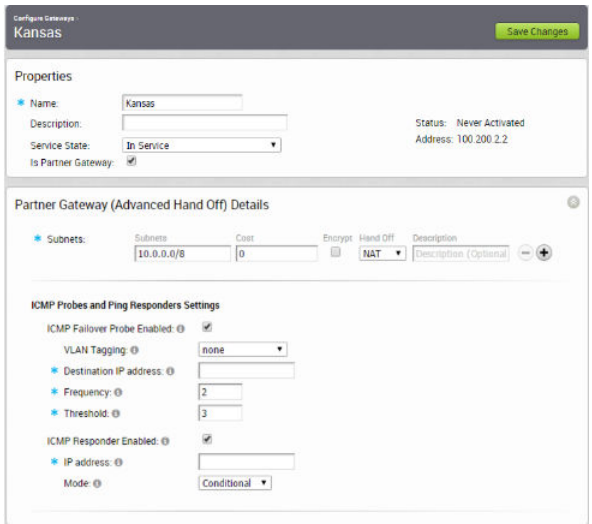
Subnets configured on a Partner Gateway are input as subnets and optional descriptions. A `Cost` field is included to allow for weighting between routes. Lower-cost routes are preferred over higher-cost routes. The following figure shows `Cost` settings per subnet.



Partner Gateway Configuration and Use

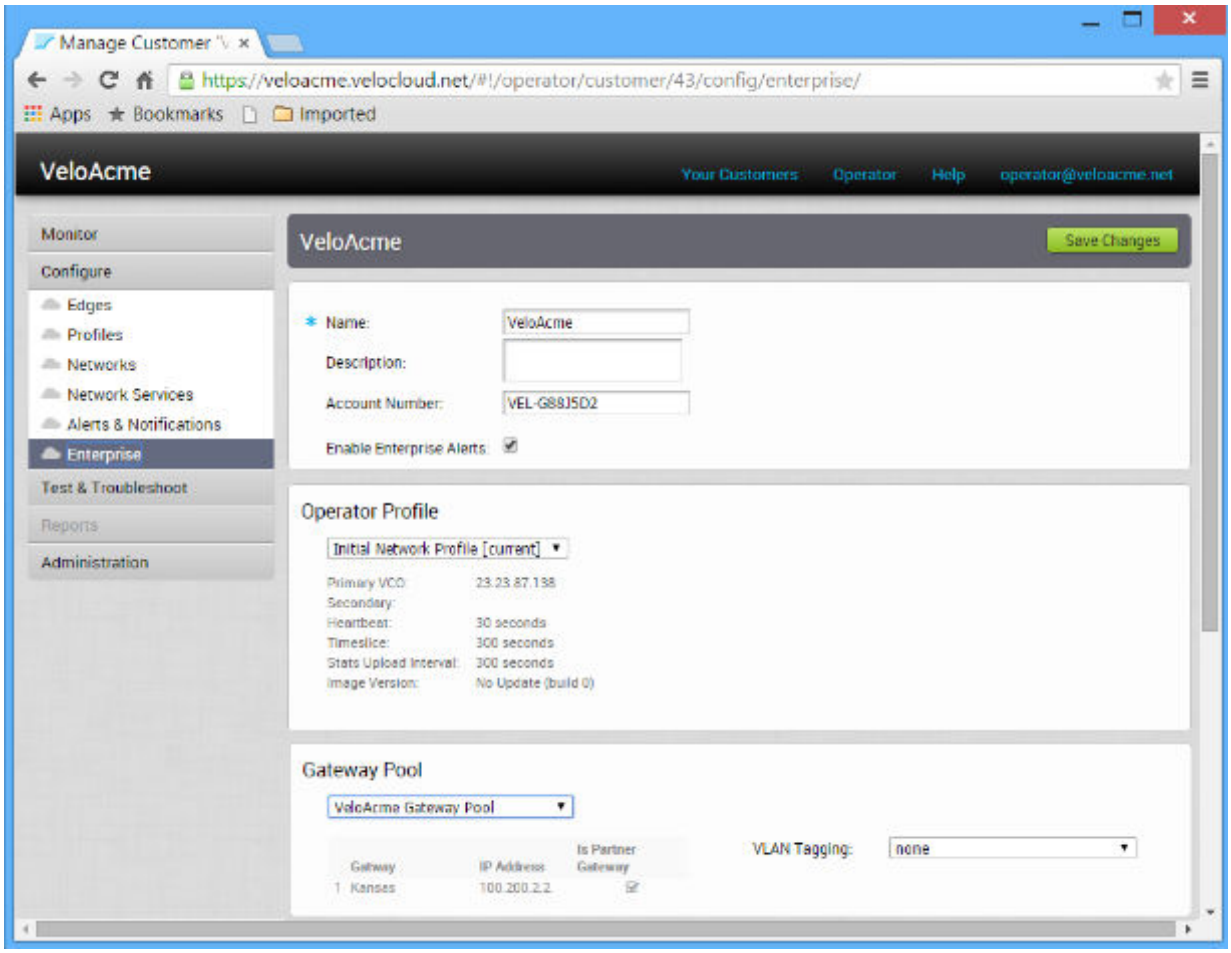
If the **Is Partner Gateway** option is selected for a Gateway, additional configuration is required:

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.



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.

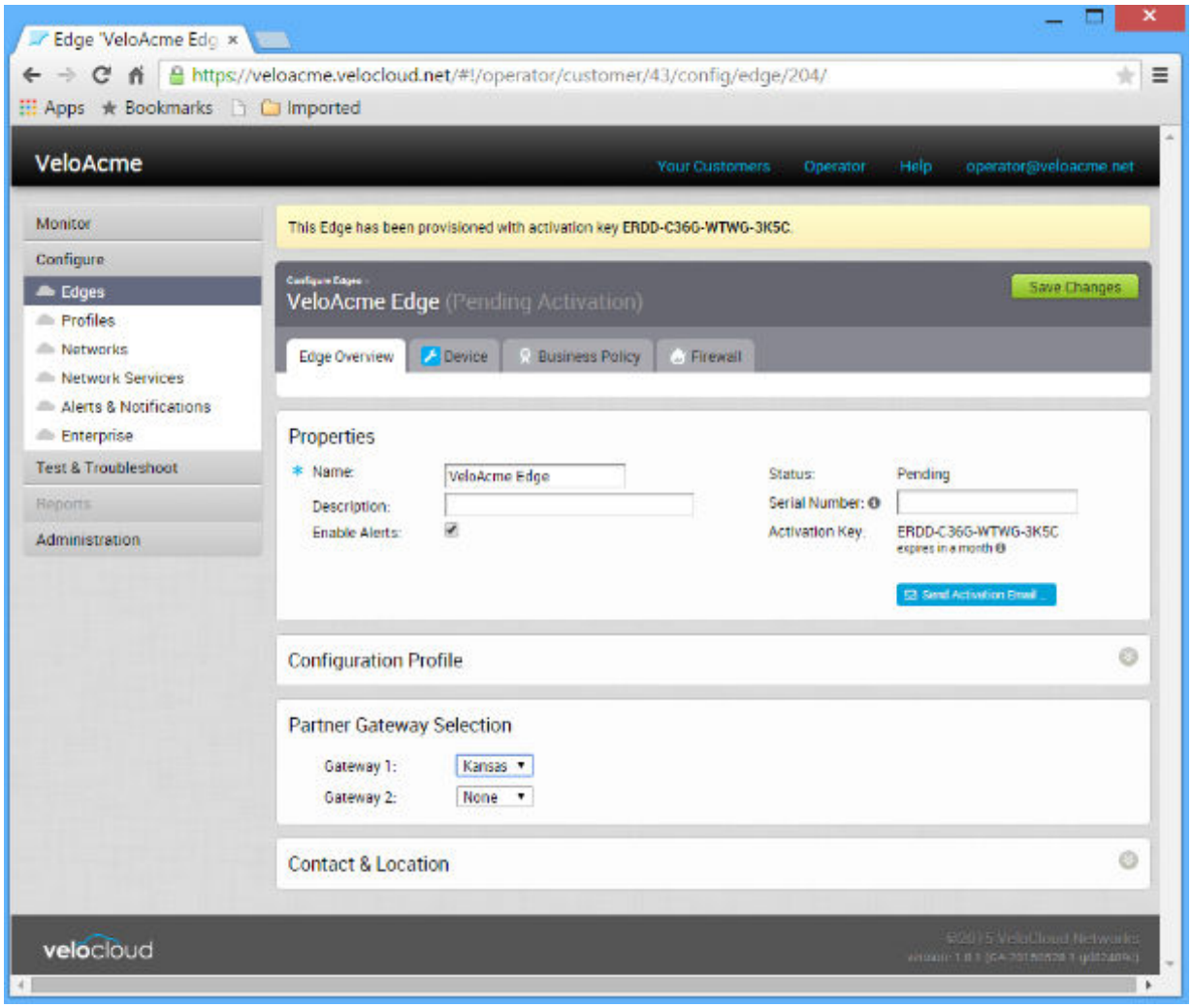
2 For each Customer that uses Partner Gateways, select a Gateway Pool that contains the Partner Gateway by selecting a customer, then choosing **Configure -> Enterprise**.



You can also choose VLAN tagging for the pool.

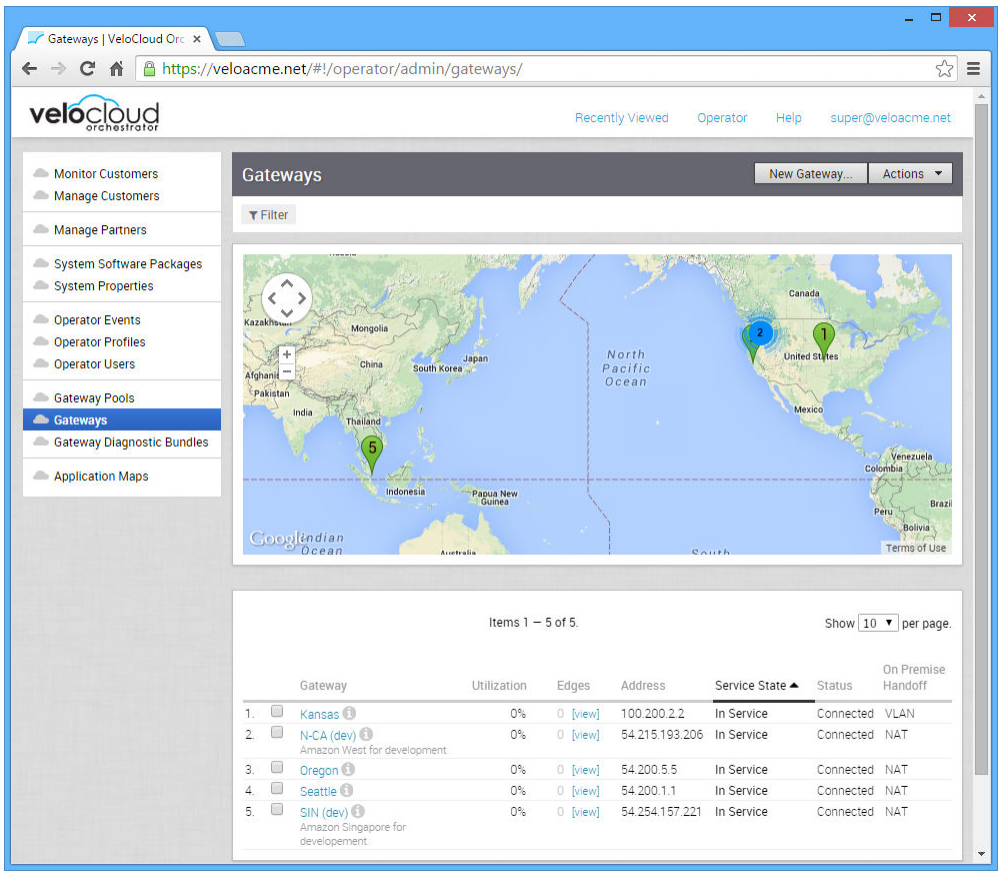
3 If you want to make the Partner Gateway VRF-aware and enable BGP, then go to **Configure > Customer** in the **Gateway Pool** screen. See Configure Gateway BGP for more configuration details.

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**.



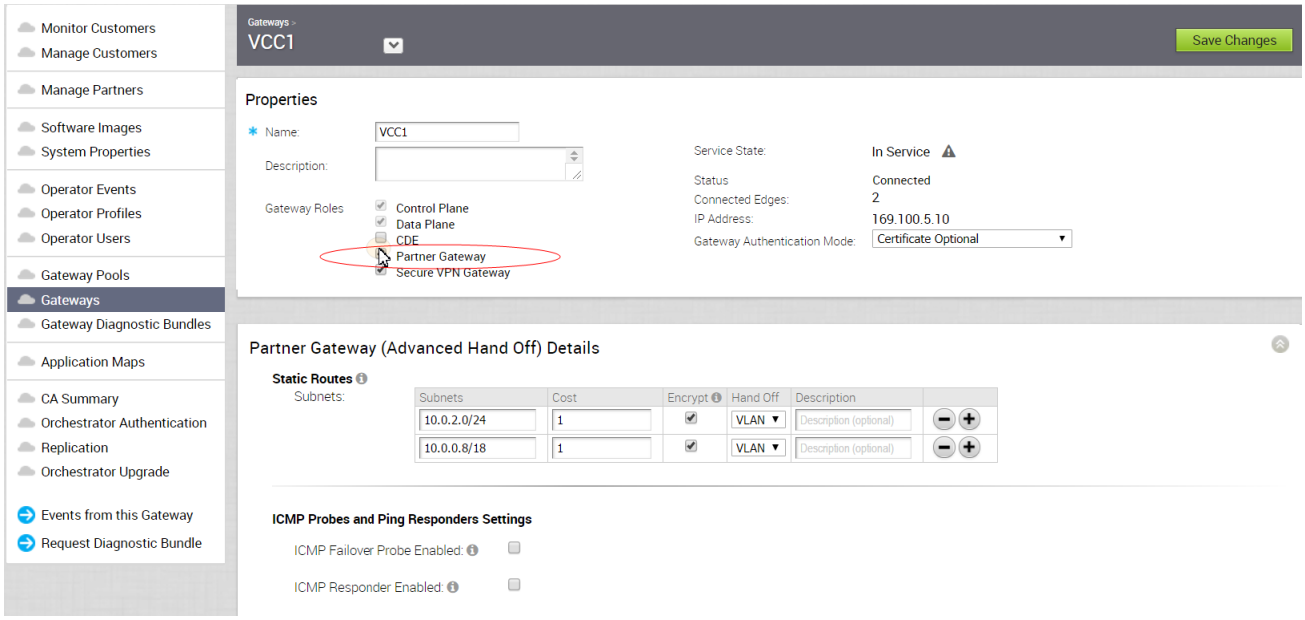
Gateways Page

If you click the **Gateways** link, all gateways managed by the VeloCloud 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.



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 VCG to establish an IPSec tunnel to a non-VeloCloud site).



- Static Routes: Specify the subnets or routes that the VCG should advertise to the VeloCloud Edge, along with the handoff mode and whether or not to encrypt the traffic. This is global per VCG 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 VCE 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 VCG. With BGP support on the Partner Gateway, using ICMP probe for failover and route convergence is no longer required.

- ICMP Failover Probe: The VeloCloud Gateway can use ICMP probe to check for the reachability of a particular IP. It can notify the VeloCloud Edge to failover to the secondary Gateway if the VeloCloud Gateway detects that the particular IP is not reachable.
- ICMP Responder Enabled: This will allow the VeloCloud Gateway to respond to the ICMP probe from the next hop router when its tunnels are up.
- Mode=Conditional: The VCG will respond to the ICMP request only when its service is up and when at least one tunnel is up.
- Mode=Always: The VCG 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.

In the **Customer Configuration** screen, Operators can enable BGP on Partner Gateways. Enterprise Admins will not have visibility or access to enable BGP. For information on BGP for VeloCloud Edge (VCE), refer to *Configure Dynamic Routing with OSPF or BGP* in the Admin Guide.

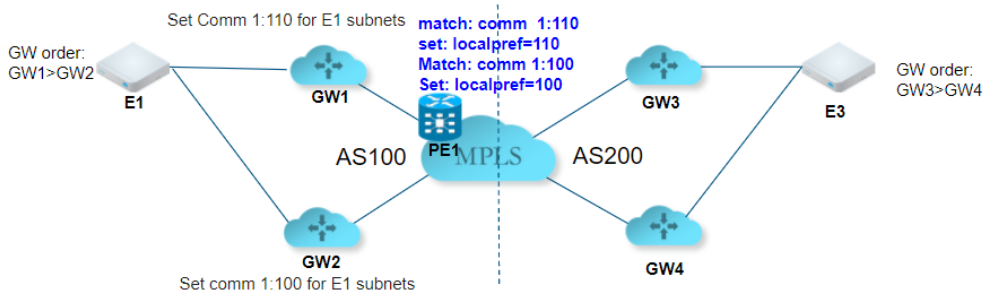
Note We support 4-Byte ASN BGP:- As the ASN of the VCE itself- Peer to a neighbor with 4-Byte ASN- Accept 4-Byte ASNs in route advertisements

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, VeloCloud 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.

Local IP Address

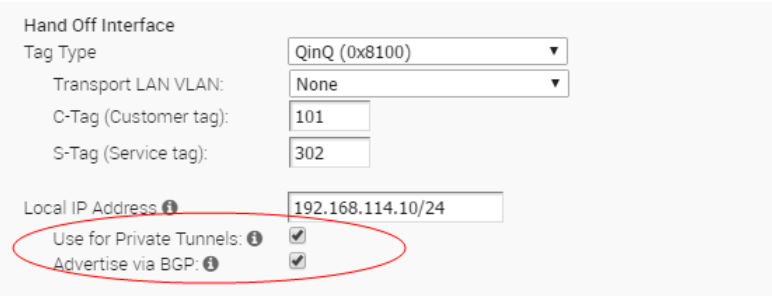
This section describes the local IP address.

Use for Private Tunnels

Operators can choose to have private WAN links connect to the private IP address of a Partner Gateway. If private WAN connectivity is enabled on a Gateway, the VCO will audit to ensure that the local IP address is unique for each Gateway within a customer.

Advertise via BGP

The Operator can choose to automatically advertise the private WAN IP of a Partner Gateway via BGP. The connectivity will be provided via the existing local IP address defined in the Partner Gateway configuration.

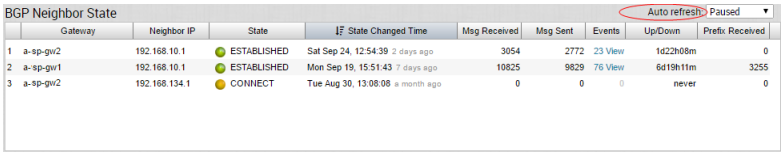


Monitoring

To view configured Gateways:

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

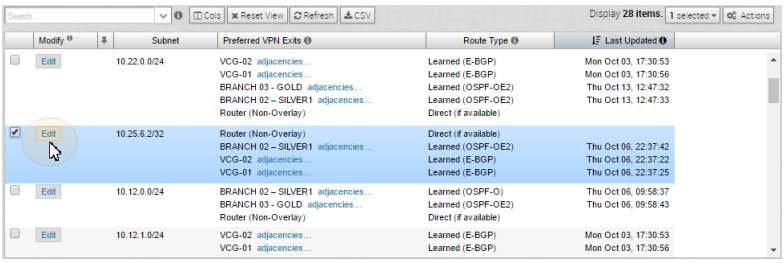
2 In the **Network Services** screen, scroll down to the **BGP Neighbor State** area to view your configured Gateways.



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.

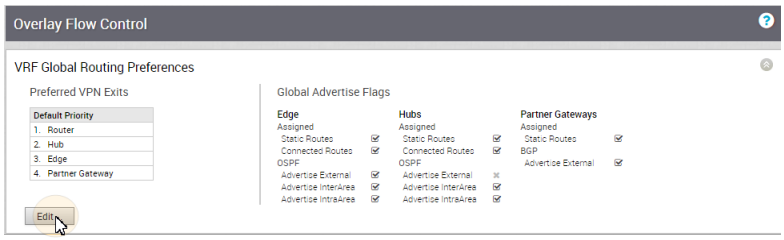


Column Name	Description
Modify	Access to edit the Global Configs.
Subnet	The network that this route corresponds to, along with a list of Edges that learned this route.
Route Type	Types include: BGP, OSPF-O, OSPF-OE2, Static, and Connected.
Preferred VPN Exits	The order of the VPN exit.
Last Updated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

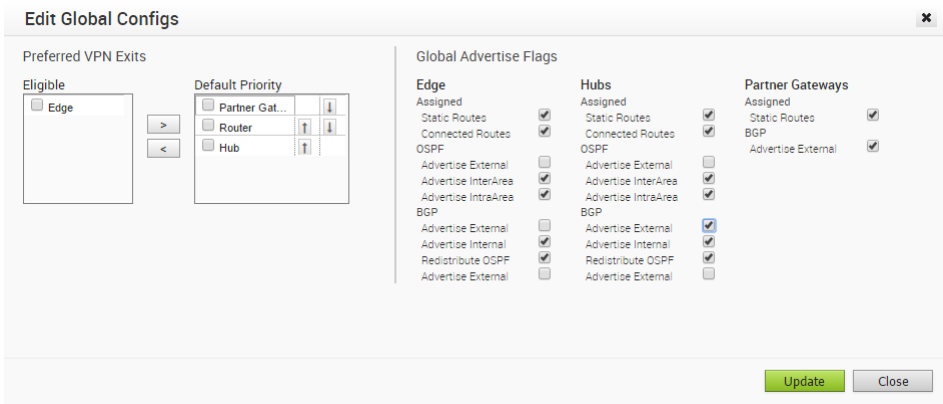
Edit Global Configs

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.



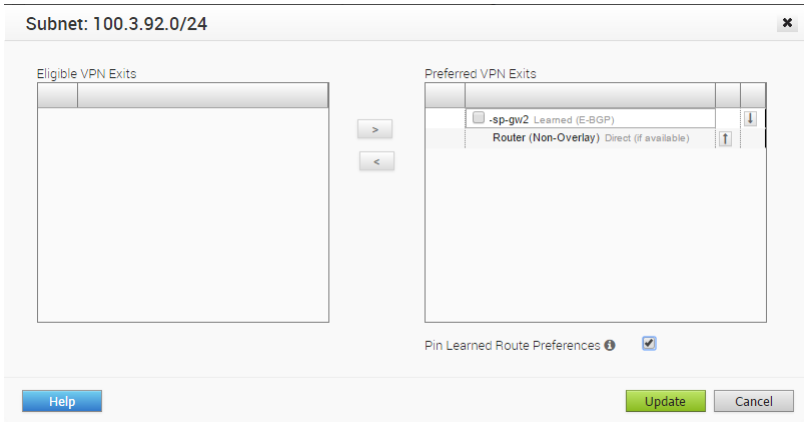
2 In the **Edit Global Configs** dialog box, edit the **Global Advertise Flags** area.



Edit Subnet

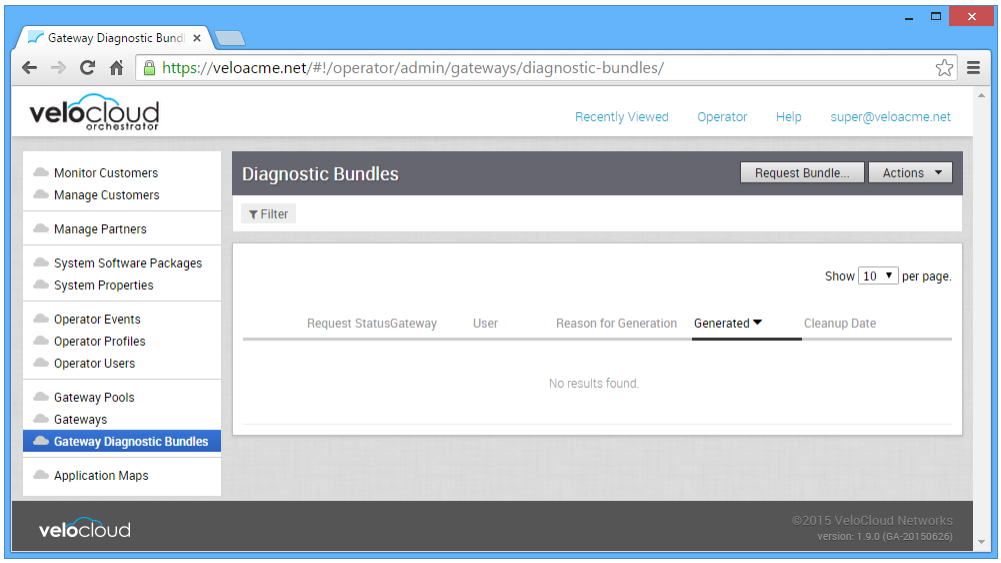
As an additional option, you can change the order of the VPN exit by editing the Subnet.

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



Manage Gateway Diagnostic Bundles

Diagnostic Bundles are used by VeloCloud Support Engineers to troubleshoot VeloCloud operation. The **Gateway Diagnostic Bundles** web page displays any diagnostic bundles that have been requested and allows you to request new bundles. Once a bundle is created, it can be downloaded or deleted when it is no longer needed.



Configure Application Maps

11

The **Application Maps** section has been updated for the 3.3.0 release.

This chapter includes the following topics:

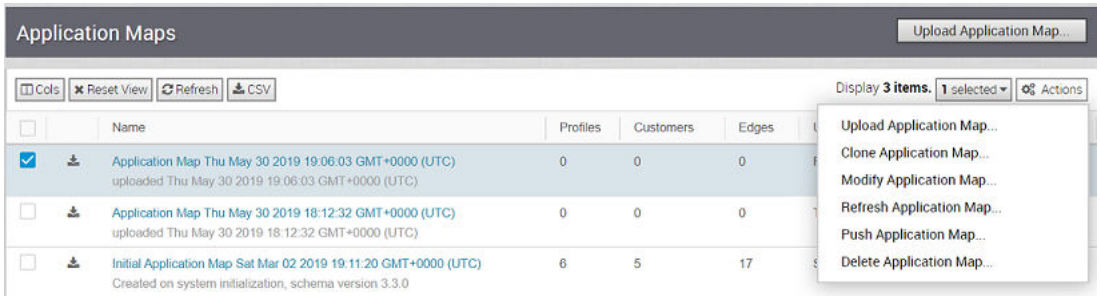
Overview of Application Maps

The **Application Maps** screen allows the uploading of files that define the applications that can be selected for Business Rules.

After an application map is uploaded, it can be specified for use in an Operator Profile. You can upload a map in one of two ways:

- Click the **Upload Application Map** button.
- Click the **Actions** button to display the drop-down menu, and then click **Upload Application Map**.

After uploading an application map, you can clone, modify, refresh the application definitions in an application map, push the updated definitions to associated Edges, or delete the application map. These options are available in the **Actions** drop-down menu.



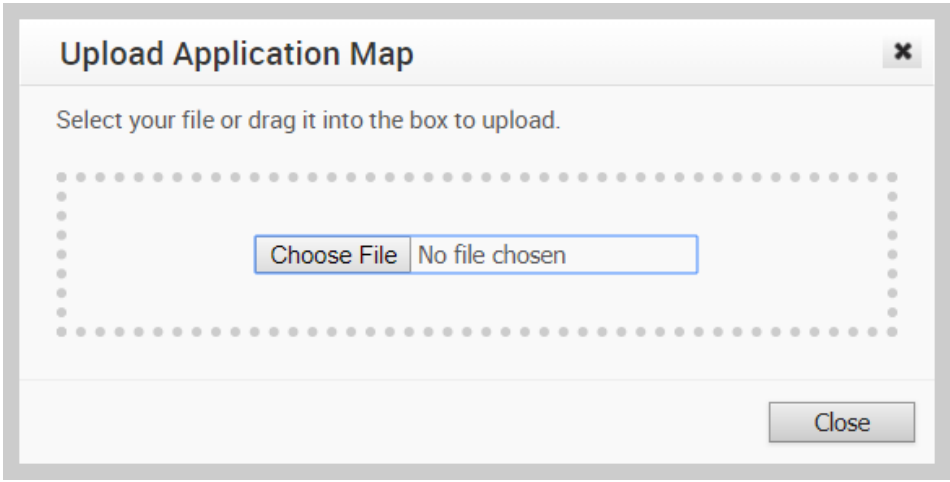
Upload an Application Map

Application maps

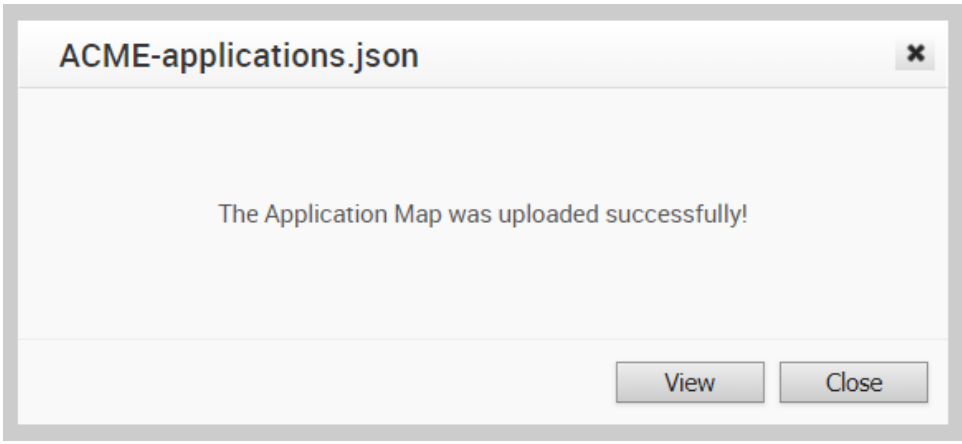
1 Click **Application Maps** from the navigation panel.

2 Click the **Upload Application Map** button. Alternatively, from the **Actions** button, choose **Upload Application Map**.

3 In the **Upload Application Map** dialog, click **Choose File** to select your file or drag it into the box.



After validating the contents, the file uploads successfully.



4 Click **View** to change the name or description of the file. The view also displays the Size and the Number of profiles. If you make changes to any of the fields in the dialog box, click the **Submit** button. Otherwise, click the **Close** button.

Your application map uploads and displays in the **Application Maps** screen.

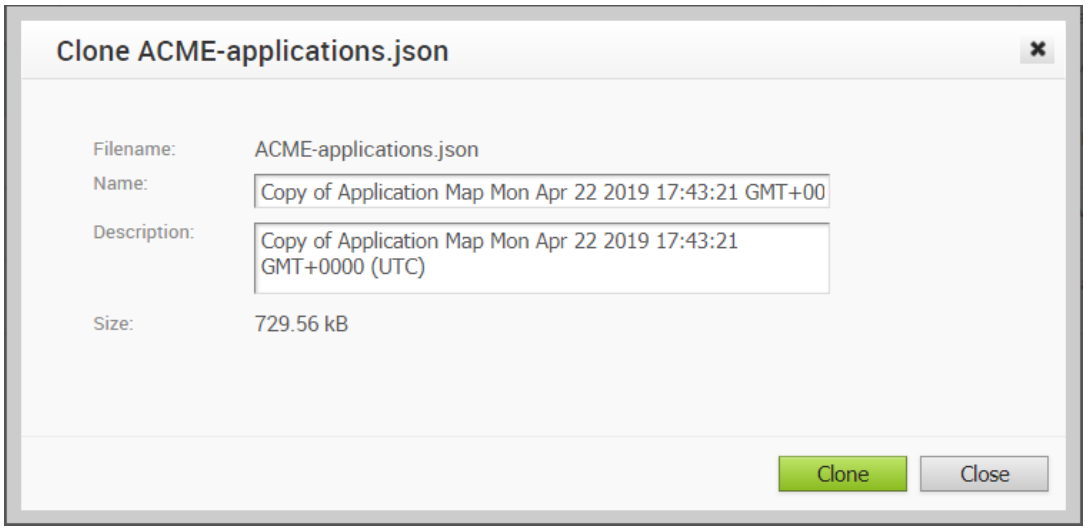
Clone an Application Map

You can create an application map by cloning an existing application map:

1 Select the application map you want to clone.

2 Choose **Clone Application Map** from the **Actions** drop-down menu.

3 In the **Clone Application Map** dialog box, enter a new name and description for the application map.



4 Click **Clone**.

Modify an Application Map

To modify an application map:

1 From the navigation panel, click **Application Maps**.

2 From the **Application Map** screen, click the link to an application map, to open the **Application Map Editor** dialog box. You can also open the **Application Map Editor** by selecting an application map and choosing **Modify Application Map** from the **Actions** menu.

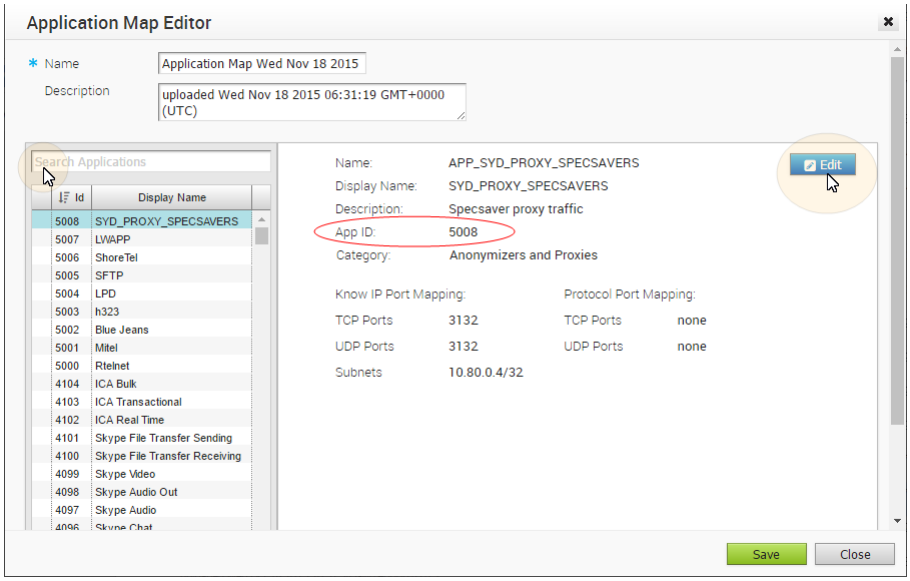
3 The **Application Map Editor** dialog box displays the list of application definitions available in the applcation map.

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

4 Click **Add New** to add a definition to the list.

5 Click **Remove** to delete a definition from the list.

6 Click **Edit** to modify the details of the selected definition. You can update the Name, Display Name, Description, Category, and Ports.



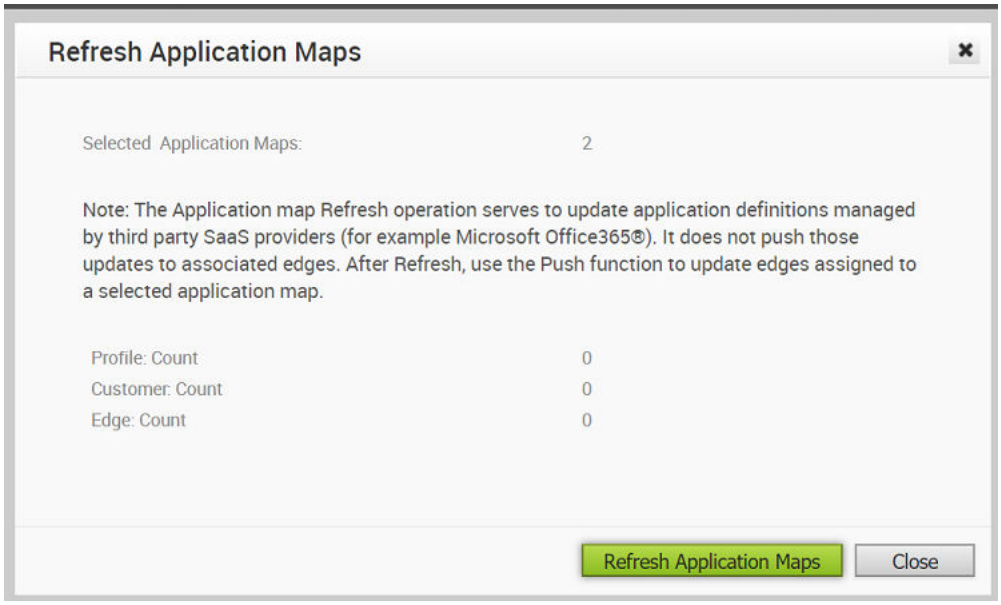
7 Click **Save** to commit your changes.

Refresh Application Map

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

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

- In the **Application Maps** page, select the Application maps that you want to refresh and then click **Actions > Refresh Application Map**.
- The **Refresh Application Maps** page opens, which lists the number of operator profiles, customers, and Edges associated with the selected Application maps.
- Click **Refresh Application Maps** to refresh the selected Application maps.



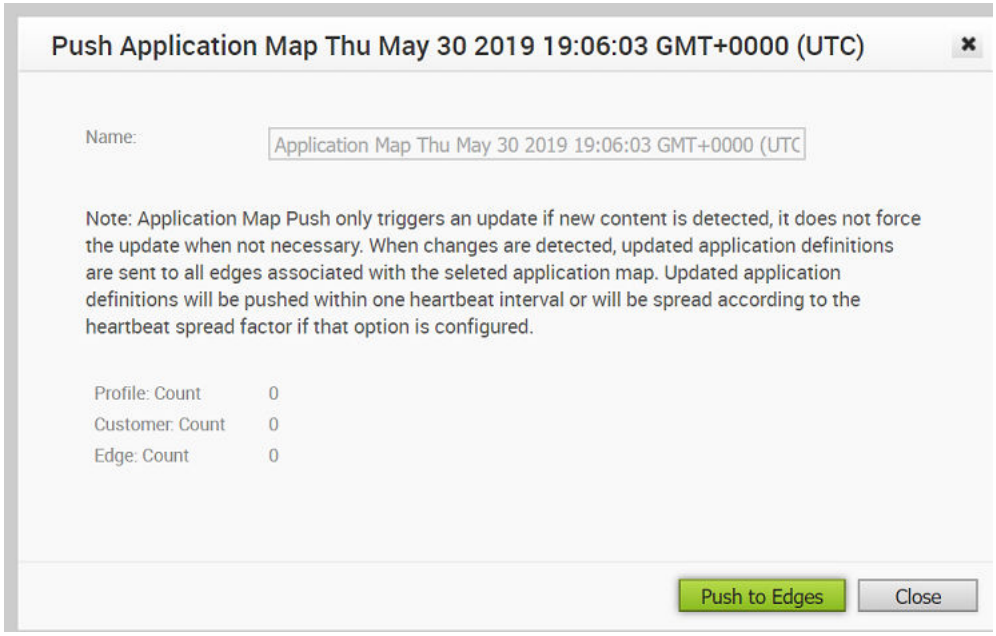
Note You can only update the Application definitions in the Application Maps using the Refresh option. If you want to update the associated Edges with the latest definitions, then use the Push Application Map option.

Push Application Map

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

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

- In the **Application Maps** page, select the Application map that you want to push to the associated Edges and then click **Actions > Push Application Map**.
- The **Push Application Map** page opens, which lists the number of operator profiles, customers, and Edges associated with the selected Application map.
- Click **Push to Edges** to update the 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.

Delete an Application Map

This section describes how to delete an application map.

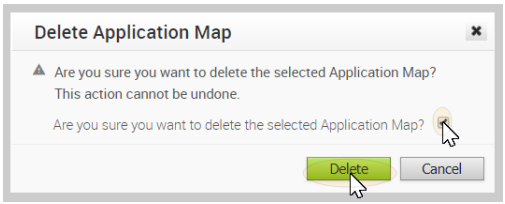
To delete an application map:

1 Select the application map you want to delete.

2 Choose **Delete Application Map** from the **Actions** button drop-down menu.

Note You cannot undo the action to delete an application map.

3 Read the warning in the **Delete Application Map** dialog box, and then click the **Are you sure you want to delete the selected application map?** checkbox to confirm deletion.



4 Click the **Delete** button to delete the application map.

Manage User Agreements

12

The "User Agreements" section is new for the 3.3.0 release.

This chapter includes the following topics:

Overview of End User License Agreements

Operator Superusers can now create and manage end user license agreements.

Note Only an Operator Superuser can create an end user license agreement. Only an Enterprise Superuser or Partner Superuser can accept a license agreement, depending on the system property settings. For more information, see *End user License Agreement System Properties*.

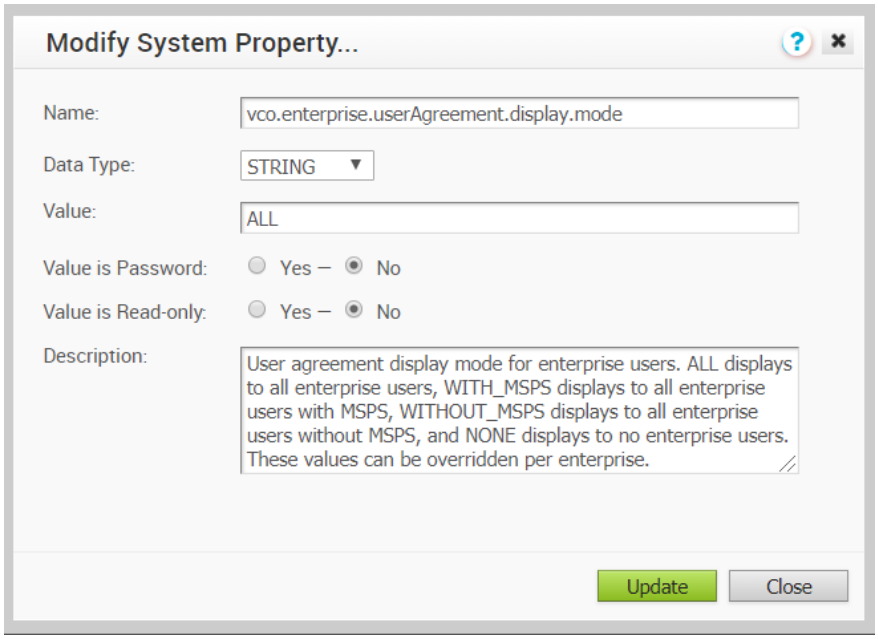
User Agreement System Properties

This section describes user agreement system properties.

The following two system properties must be enabled to allow Operators to create and manage user agreements.

- `session.options.enableUserAgreements`: Set this system property to **True**. This property enables the user agreement functionality.
- `vco.enterprise.userAgreement.display.mode`: This property displays the user agreement to the superusers specified in the `Value` text field. Set the `Value` text field to one of the following:
  - **NONE** (the default)

- **ALL** - includes Enterprise Superusers and Partner Superusers
- **WITH_MSPS**
- **WITHOUT_MSPS**



Create a User Agreement

Only Operator Superusers can create a new user agreement. The Operator Superuser can create multiple agreements, but only one agreement can be active at a time.

To create a user agreement:

1 Click the **User Agreement** link from the navigation panel of the VCO.

2 In the **User Agreements** screen, click the **New User Agreement** button.

3 In the **User Agreement** dialog box:

a Type in the name of the customer who will see the agreement.

Note Only an Enterprise Superuser or Partner Superuser (based on system property settings) can accept the agreement. See the User Agreement System Properties section for more information.

b The **Enabled** checkbox is selected by default. Note the following important information about the **Enabled** checkbox:

- Because the **Enabled** checkbox is selected by default, all agreements you create will also be enabled by default. Although all agreements can be enabled, only one agreement can be **ACTIVE** at a time. Therefore, it is advisable to unselect the **Enabled** checkbox until you are ready to activate an agreement.

- If you want to activate a different agreement, you must first disable the current agreement by unselect the **Enabled** checkbox. If multiple agreements are also enabled, go to **Update** (from the **Actions** drop-down menu) and unselect the **Enabled** checkbox.

  Note Enable only the agreement you want to activate.

c In the **Effective Start Date** field, click the **Calendar** icon to select a start date to indicate when you want the agreement activated. If this field is not specified, it will be activated immediately after the agreement is created.

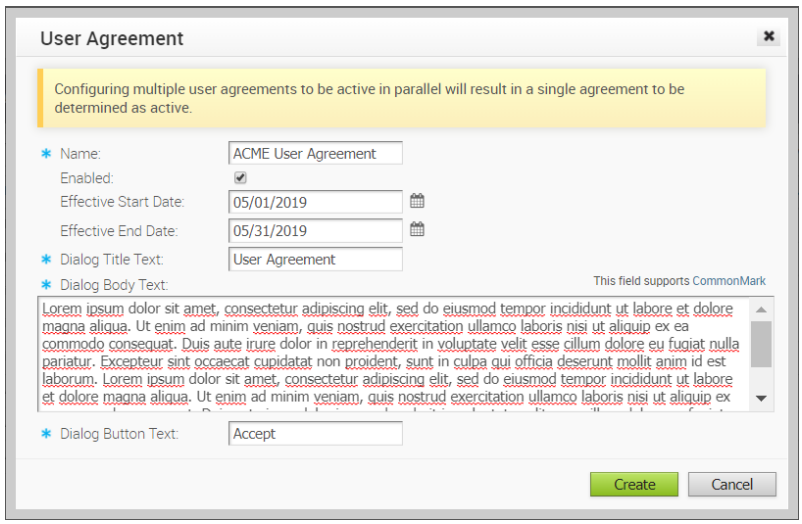
d In the **Effective End Date** field, click the **Calendar** icon to indicate when the user agreement will be inactive.

e In the **Dialog Title Text** field, enter a title or heading for the user agreement. (This represents the title of the user agreement and will be displayed to the customer).

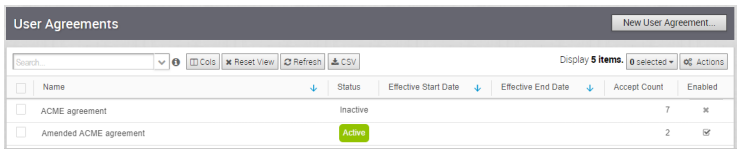
f In the **Dialog Body Text** field, enter the user agreement text. (Not only will this content be visible to the customer, this is the actual agreement the customer will be accepting.

g In the **Dialog Button Text** field, enter the name of the button the customer will click to accept the agreement (e.g. Agree, OK, etc.).

h Click **Create**.



After the agreement has been created, it populates in the **User Agreements** screen. The **Active** button indicates which agreement is active among multiple agreements.



The Enterprise Superuser or Partner Superuser will see the agreement upon logging into the VCO. He or she must accept the agreement before accessing it. If the user does not accept the agreement, he or she will be automatically logged out.

To determine which customers have accepted the agreement, Operators can generate a user agreement acceptance report. See *Export Acceptance Report* for more information.

After a customer accepts the user agreement, note the following:

- After a customer accepts the agreement, the Operator will see the following updates to the **User Agreements** screen: the Status column changes from 'Inactive' to 'Active', and the Accept Count column updates to indicate the number of customers who have accepted the agreement.
- Accepted user agreements are archived and cannot be deleted by the Operator Superuser.
- Only one user agreement can be active at a time.

Clone a User Agreement

Operator Superusers can clone existing user agreements.

To clone a user agreement:

1 Click the **User Agreement** link from the navigation panel of the VCO.

2 Select the user agreement to be cloned by clicking the checkbox next to the user agreement name.

3 In the **User Agreements** screen, click the **Actions** button and choose **Clone**.

The cloned user agreement is created with the name of the original user agreement with the word "copy" next to it and is populated in the **User Agreements** screen.

Operator Superusers can make changes to the cloned agreement by selecting the cloned agreement, then click the **Actions** button and choose **Update**. See "*Update New User Agreement*" for more information.

Update a User Agreement

After a new user agreement has been created, only the agreement name and the Effective Start and End dates can be changed. The **Enabled** checkbox can be enabled or disabled as well.

To update a user agreement:

1 Select the User Agreement.

2 From the **Actions** button drop-down menu, choose **Update**.

Activate a Different Agreement

In order to activate a different agreement, you must deactivate/disable the current agreement by unselecting the **Enabled** checkbox.

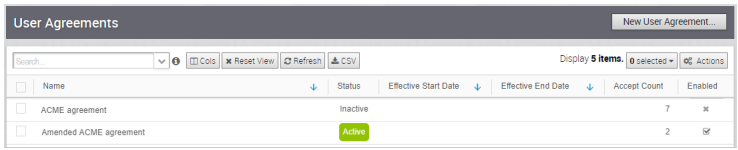
To activate a different agreement:

1 Select the agreement.

2 Click the **Actions** button and choose **Update**.

3 In the **User Agreement** dialog, unselect the **Enabled** checkbox.

4 If other agreements are enabled, follow steps 1-3 above. Enable only the agreement you want to be ACTIVE.



Delete a User Agreement

An Operator Superuser can delete a user agreement if a user has not accepted it. Therefore, the **Accept Count** will be zero.

To delete an inactive user agreement:

1 Click the **User Agreement** link from the navigation panel of the VCO.

2 Select the user agreement to be deleted by selecting the checkbox next to the user agreement name.

3 In the **User Agreements** screen, click the **Delete** button.

> **Note** Deleting an inactive user agreement cannot be undone.

4 Click **OK** in the dialog box to answer the question, **Are you sure you want to delete the selected item?**

Export an Acceptance Report

Operator Superusers can generate an Excel spreadsheet report of all customers who have accepted user agreements.

To generate an Excel spreadsheet report:

1 Click the **User Agreement** link from the navigation panel of the VCO.

2 In the **User Agreements** screen, click the **Actions** button and choose **Export Acceptance Report**.

3 In the **CSV Export** dialog box, enter a name for the report in the **File Name** field.

4 Click the **Export to CSV** button.

An Excel spreadsheet of all customers who have accepted the user agreement downloads.

Manage Edge Licensing

13

Standard Administrator Superusers, Standard Administrators, Business Specialists, and Customer Support users can monitor and generate a report displaying the license types that have been assigned to them by either their Partner or Operator. From the list of license types, users must assign license types to their Edges.

Note The *Edge Licensing* section is new for the 3.3.0 release.

This chapter includes the following topics:

Overview of Edge Licensing

Superuser Operators, Standard Admin Operators and Business Specialists can assign and manage license types to Partner and Enterprise customers.

Note Customer Support Operators cannot assign license types, but they can manage and upgrade existing license types.

Edge License Type Attributes

The Edge license type consists of the following attributes:

Attribute	Description
Bandwidth	■ **10M** ■ **30M** ■ **50M** ■ **100M** ■ **200M** ■ **500M** ■ **1G** ■ **2G** ■ **5G** ■ **10G**
Editions (from lowest level to highest level)	■ **Standard** ■ **Enterprise** ■ **Premium**
Region	■ **North America** ■ **Europe** ■ **APJC** ■ **Middle East** ■ **LATAM** ■ **APJC**
Term	■ **1 Year** ■ **3 Year** ■ **5 Year**

Superuser Operators, Standard Admin Operators, and Business Specialists can assign license types to Partners and Enterprise customers from a catalog of 270 license types. The above-mentioned users will get access to the catalog of 270 license types automatically during a VCO installation or when upgrading to the 3.3.0 release. These license types will be displayed in the **Edge Licensing** screen. To use the Edge License feature, the above-mentioned users must enable the Edge License system property. For more information, see Enable Edge Licensing.

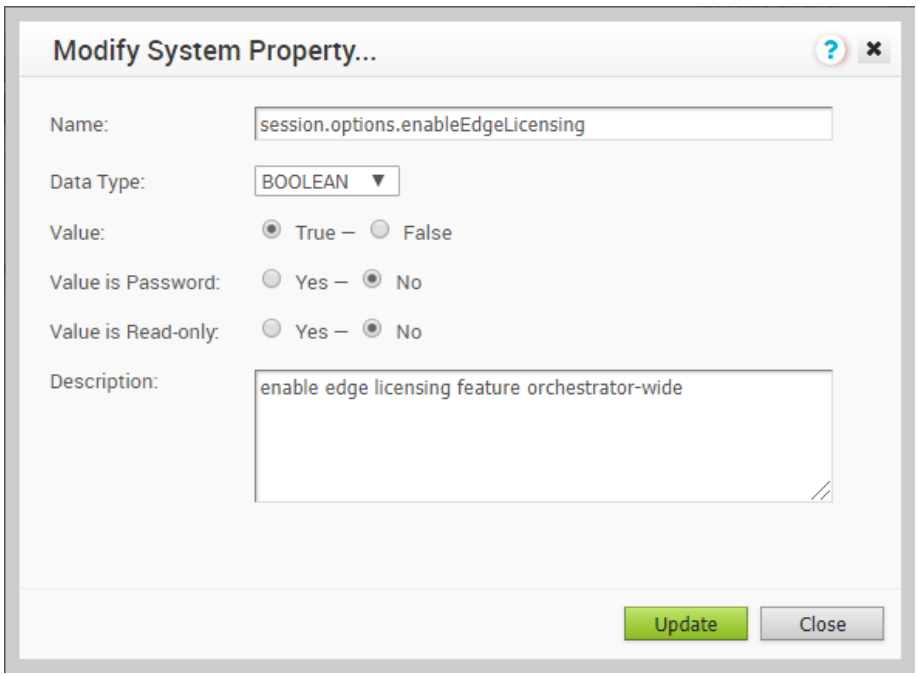
Note Assigning a license type to an Edge does NOT change or limit the functionality of the Edge in anyway. The Edge License feature does NOT enforce license types onto the Edge, but merely introduces the ability to attach license types. The intent is to ensure license types can be attached to Edges and reported when necessary.

Considerations When Assigning Edge License Types

Scenario	Considerations
Mixing License Types	■ Standard License Type: No mixing of license types ■ Enterprise License Type: Can mix with the Premium license type ■ Premium License Type: Can mix with the Enterprise license type
Upgrading an Edge License Type	■ A Standard license type can be upgraded to an Enterprise or Premium license type ■ An Enterprise license type can be upgraded to a Premium license type
Downgrading an Edge License Type	■ License types cannot be downgraded. ■ Once a higher edition license type is assigned, it cannot be downgraded to a lower edition.

Enable Edge Licensing

To enable Edge Licensing, set the following Edge Licensing system property (`session.options.enableEdgeLicensing`) to **True**, and then click the **Update** button.

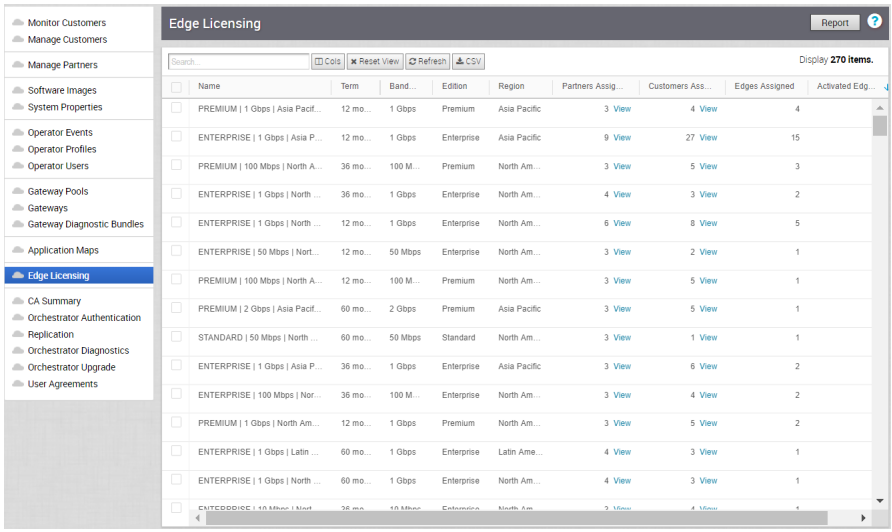


To disable the Edge Licensing feature, set the value to **False**. However, VeloCloud recommends that the Edge Licensing feature be always enabled.

Edge Licensing Screen

The **Edge Licensing** screen provides an inventory view of the number of Partners, Enterprises, and Edges a license type has been assigned to.

Superuser Operators, Standard Admin Operators, Business Specialists, and Customer Support Operators can generate a report to get information about Edge status, activation date, assigned license types, and other information. See *Generate an Edge License Report* for more information.



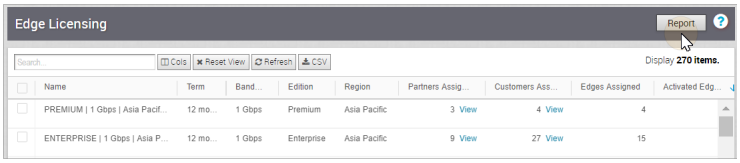
Generate an Edge Licensing Report

Operator Superusers, Standard Operators, Business Specialists, and Customer Support Operators can generate a report about Edges and their license types.

To generate an Edge Licensing Report:

1 From the Orchestrator navigation panel, click **Edge Licensing**.

2 From the **Edge Licensing** screen, click the **Report** button.



The Excel spreadsheet report automatically downloads. See sample output below.

Operators can assign license types to Partners, so those license types can be assigned to Customers (Enterprises) of the Partners. For information about assigning license types to Partners, see *Create a Partner*. For information about assigning license types to Enterprise Customers, see *Create a Customer*.

Upgrade VCO with DR Deployment

14

This section is new for the 3.3.0 release.

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 VCO" 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.

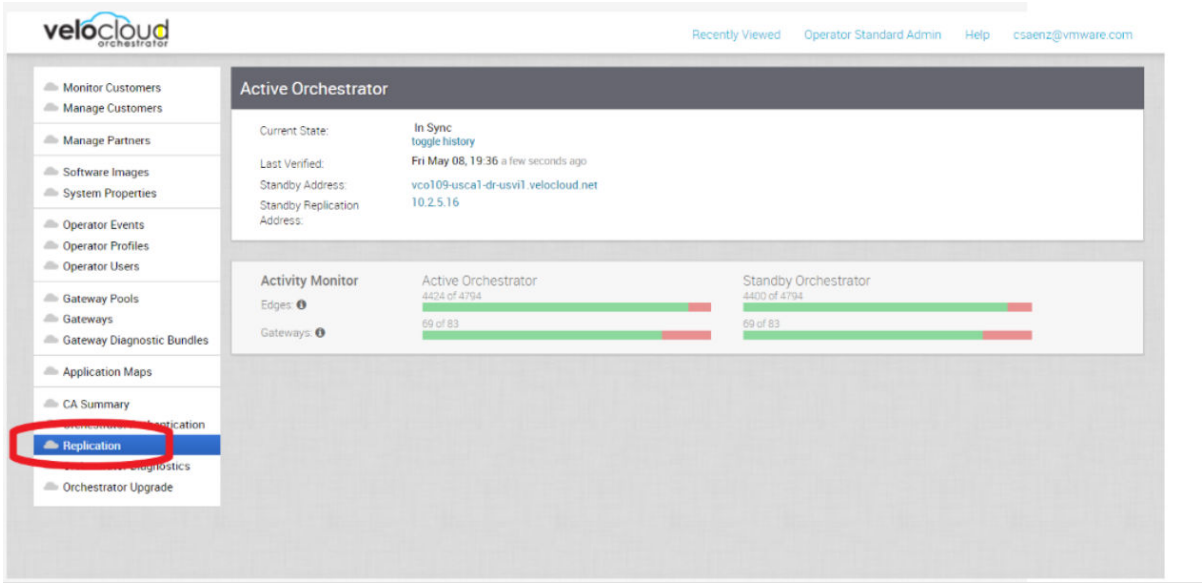
To upgrade SD-WAN Orchestrator:

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.



- 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').

  - LVM layout
    - pvdisplay -v
    - vgdisplay -v
    - lvdisplay -v
    - df -h
    - cat /etc/fstab
  - Memory information
    - free -m
    - cat /proc/meminfo

        - ps -ef
        - top -b -n 2
    - CPU Information
        - cat /proc/cpuinfo
    - 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.

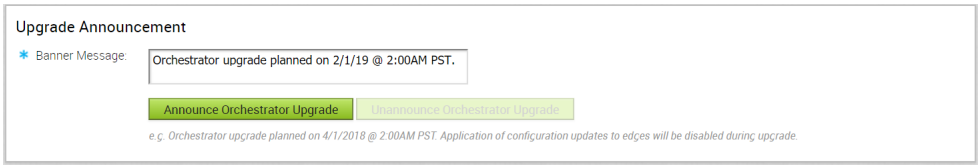
Step 2: Send Upgrade Announcement

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:

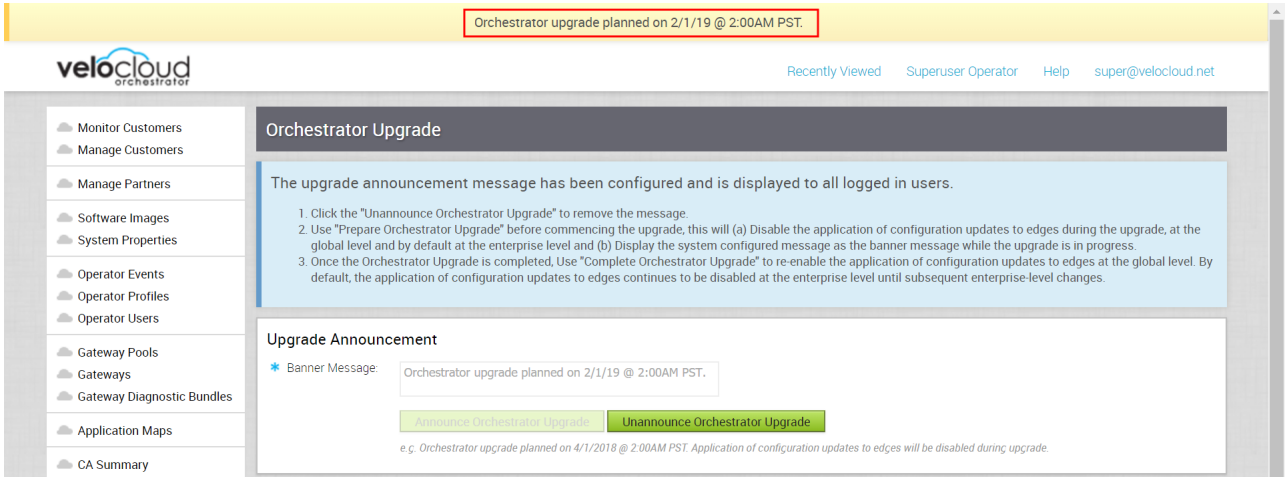
1 From the SD-WAN Orchestrator, select **Orchestrator Upgrade** from the navigation panel.

2 In the **Upgrade Announcement** area, type in your message in the **Banner Message** text box.



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.



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 VCO.

VCO Disaster Recovery

This section describes how to set up and upgrade disaster recovery in the VCO.

Set Up DR in the VCO

To set up disaster recovery in the VCO:

1 Install a new VCO whose version matches the version of the VCO that is currently the Active VCO.

2 Set the following properties on the Active and Standby VCO, if necessary.

- `vco.disasterRecovery.transientErrorToleranceSecs` to a non-zero value (Defaults to 900 seconds in version 3.3, zero in earlier versions). This prevents any transient errors from resulting in a Edge/Gatewaymanagement plane update.
- `vco.disasterRecovery.mysqlExpireLogsDays` (Defaults to 1 day). This is the amount of time the Active VCO 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 *VeloCloud 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 VCO Disaster Recovery 15

This section describes disaster recovery for VeloCloud Orchestrator.

This chapter includes the following topics:

VCO DR Overview

The VeloCloud Orchestrator (VCO) Disaster Recovery (DR) feature prevents the loss of stored data and resumes VCO services in the event of system or network failure.

VCO DR involves setting up an active/standby VCO 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 VeloCloud sales team for support.

Active/Standby Pair

In a VCO DR deployment, two identical VCO 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 VCOs, and while they receive configuration changes only from the active VCO, 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.

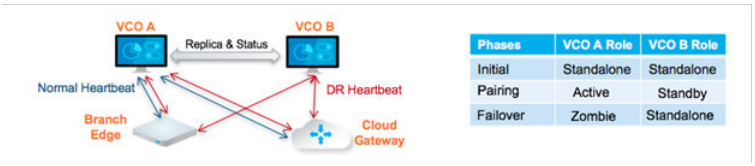
DR States

From the view of an operator, and of the edges and gateways, a VCO has one of four DR states:

DR State	Description
Standalone	No DR configured.
Active	DR configured, acting as the primary VCO server.
Standby	DR configured, acting as an inactive replica VCO 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 VCO are redirected to the promoted server.



Phases	VCO A Role	VCO B Role
Initial	Standalone	Standalone
Pairing	Active	Standby
Failover	Zombie	Standalone

Set Up VCO Replication

Two installed VCO instances are required to initiate replication.

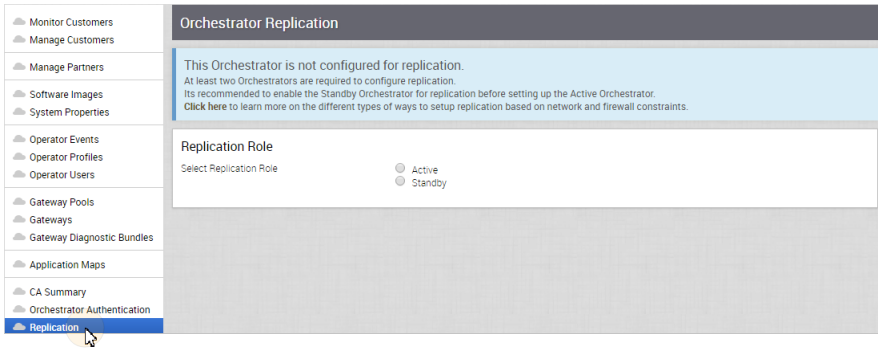
- The selected standby is put into a `STANDBY_CANDIDATE` state, enabling it to be configured by the active server.
- The active server is then given the address and credentials of the standby and it enters the `ACTIVE_CONFIGURING` state.

When a `STANDBY_CONFIG_RQST` is made from active to standby, the two servers synchronize through the state transitions shown below.

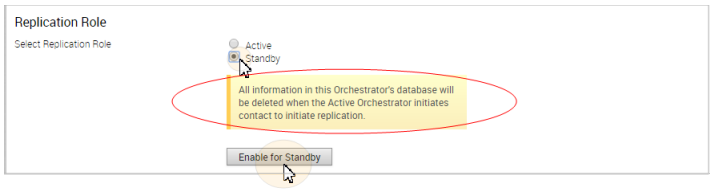
Set Up the Standby Orchestrator

To set up VCO replication (using the first of two VCOs):

1 Click **Replication** from the Navigation panel to display the **Orchestrator Replication** screen.

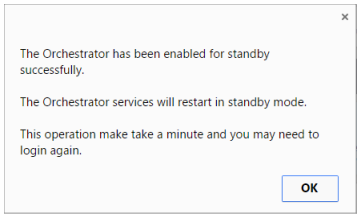


2 Enable the Standby Orchestrator by selecting the **Standby (Replication Role)** radio button.

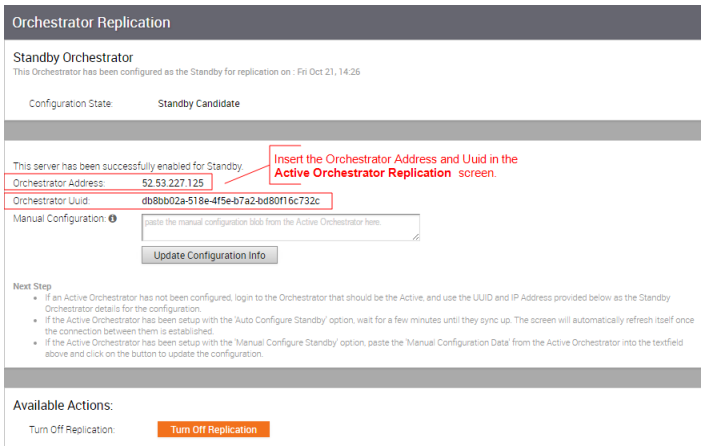


3 Click the **Enable for Standby** button.

The **Orchestrator Success** dialog box appears, indicating that the Orchestrator has been enabled for Standby, and that the Orchestrator will restart in Standby mode.



4 Click **OK**.



After the Standby Orchestrator has been configured for replication, configure the Active Orchestrator according to the instructions below.

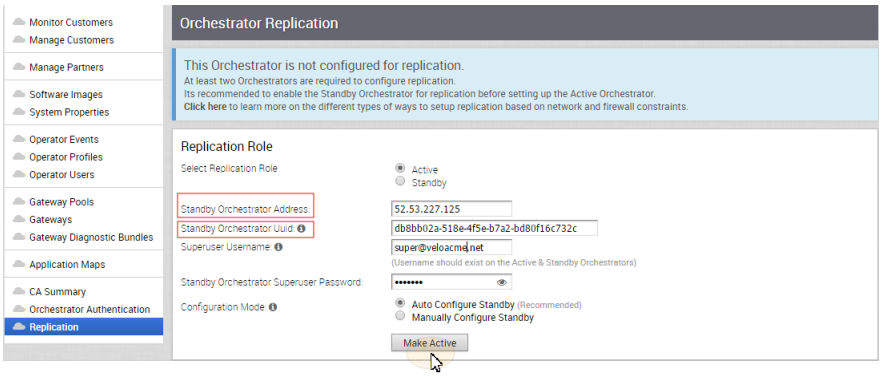
Set Up the Active Orchestrator

To configure the second VCO 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.

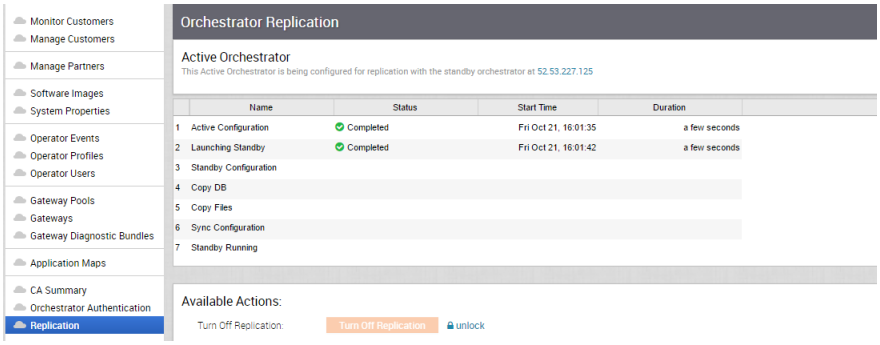


4 Type in the username and password for the Orchestrator Superuser to be used for replication.

Note This Superuser should already exist on both systems.

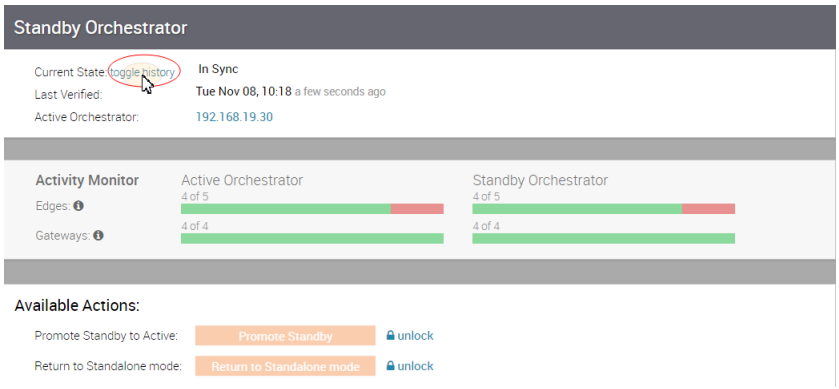
5 Click the **Make Active** button.

The **Active Orchestrator** screen displays showing a status of the current state.

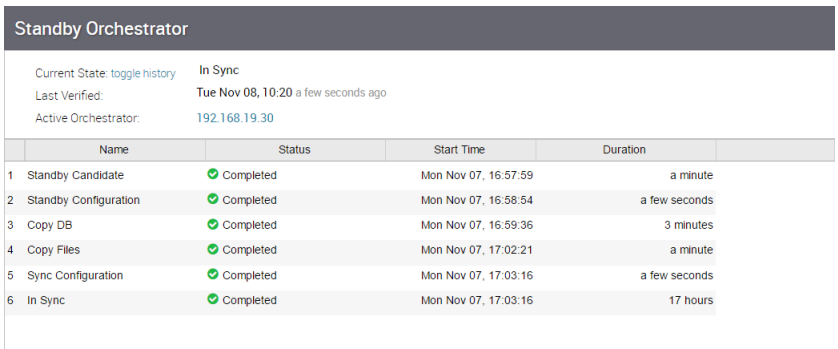


When configuration is complete, both Orchestrators (Standby and Active) will be in sync.

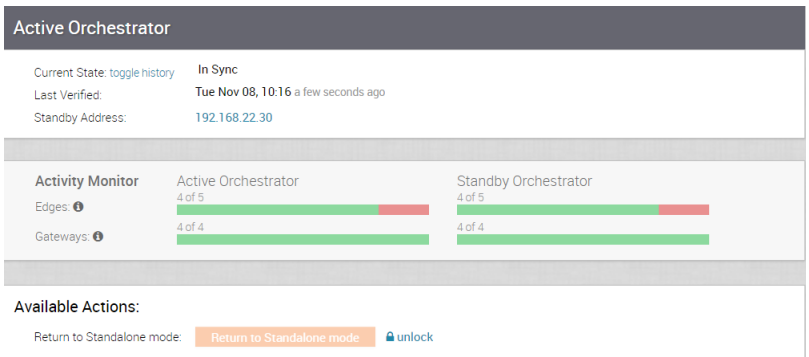
Standby Orchestrator in Sync



You can click the **toggle history** link to view the status of each state.



Active Orchestrator in Sync



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

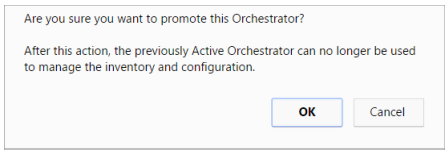
This section describes how to promote a Standby Orchestrator.

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.

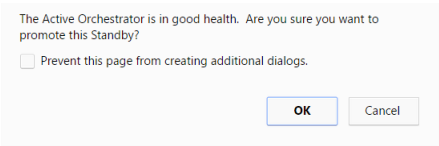
The following dialog box appears, indicating that when you promote your Standby Orchestrator, administrators will no longer be able to manage the VCO using the previously Active Orchestrator.



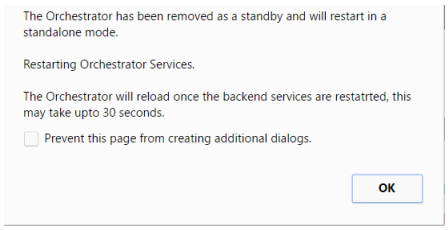
3 Click the **OK** button to promote the Standby Orchestrator.

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.

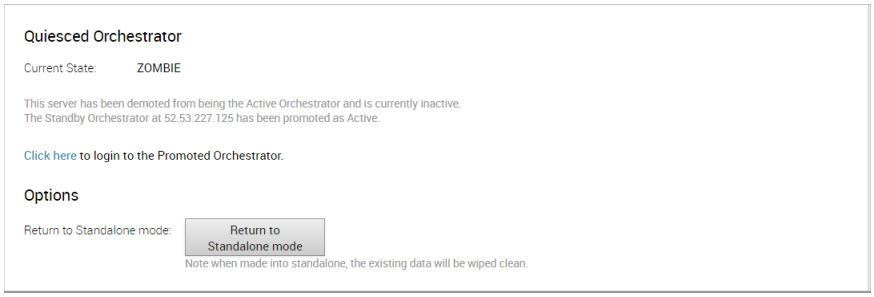


A final dialog box appears indicating that the Orchestrator is no longer a Standby and will restart in Standby mode.



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.



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.

Troubleshooting VCO 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 VeloCloud log.

Recoverable Failures

The following errors are recoverable failures that can occur after VCO DR reaches an in sync state. If the problem causing these failures is corrected, VCO 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 VCO DR. VCO 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

Configure Single Sign On for Identity Partners

16

The Identity Partner (IDP) Configuration for Single Sign On (SSO) is newly added for the 3.3.1 release.

This chapter includes the following topics:

Configure an IDP for Single Sign On

To enable Single Sign On (SSO) for VeloCloud Orchestrator (VCO), you must configure an Identity Partner (IDP) with details of VCO. 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 VCO 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.

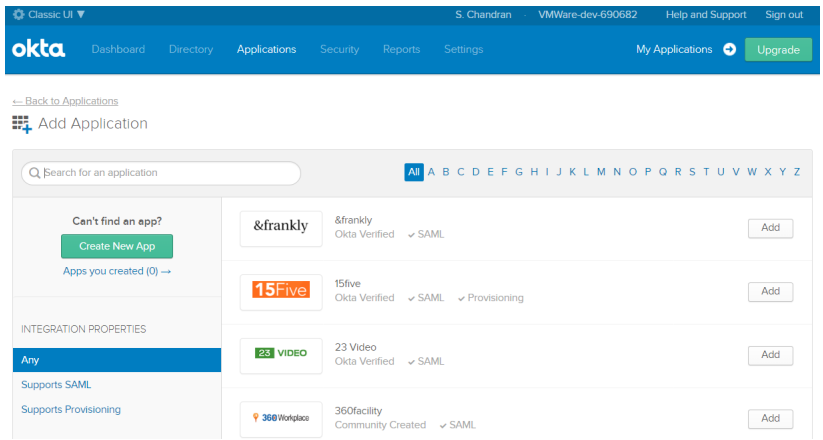
The **Okta** home screen appears.

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.



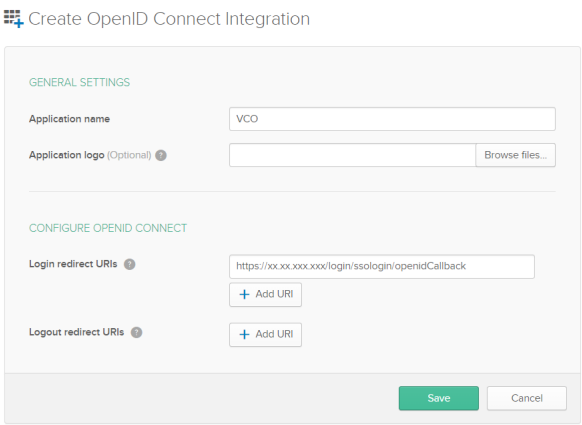
b Click **Create New App**.

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.



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

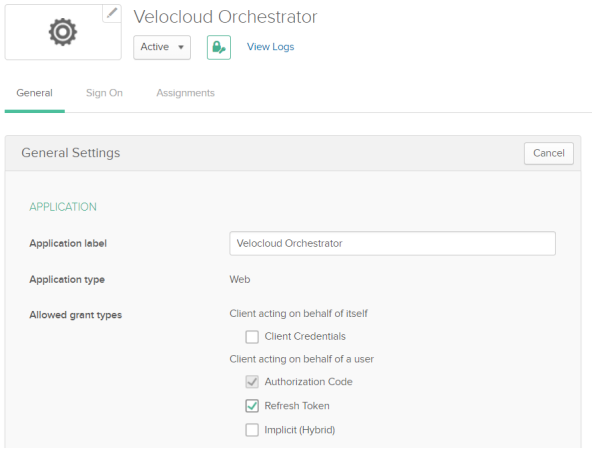
f Under the **CONFIGURE OPENID CONNECT** area, in the **Login redirect URIs** text box, enter the redirect URL that your VCO application uses as the callback endpoint.

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

g Click **Save**.

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 VCO.



i Click the **Sign On** tab and under the **OpenID Connect ID Token** area, click **Edit**.

j In the **Groups claim filter** area, set the filter for the user groups and click **Save**.

The application is setup in IDP. You can assign groups and users to your VCO application.

3 To assign groups and users to your VCO application:

a Go to **Application** > **Applications** and click on your VCO 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 VCO application and click **Done**.

Results

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

What to do next

Configure Single Sign On in VCO.

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.

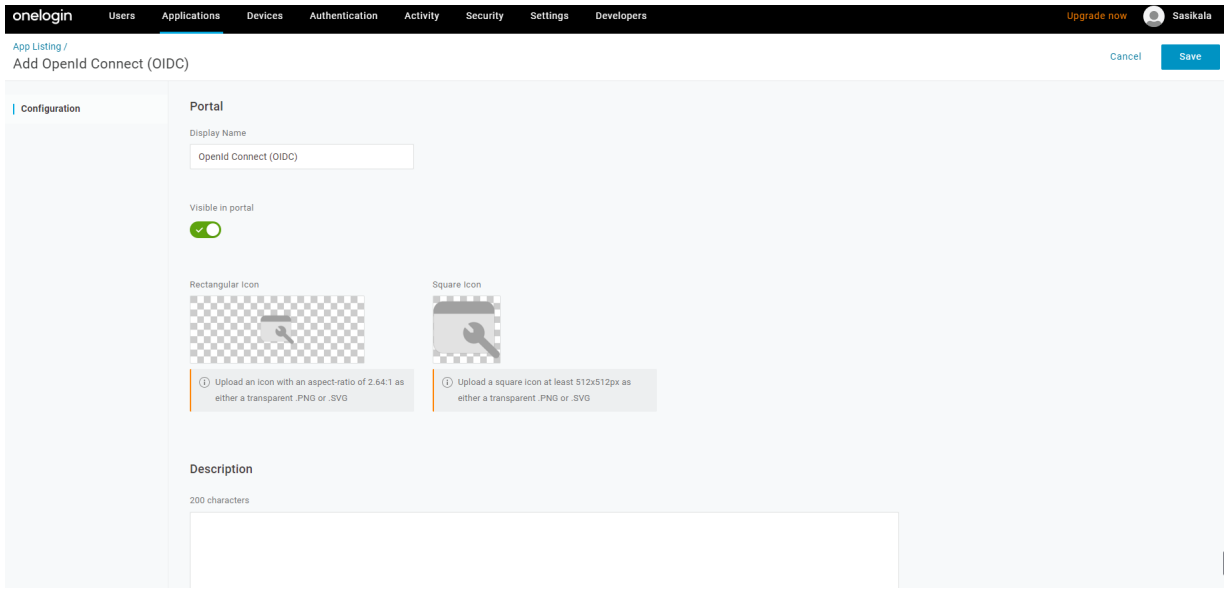
The **OneLogin** home screen appears.

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.

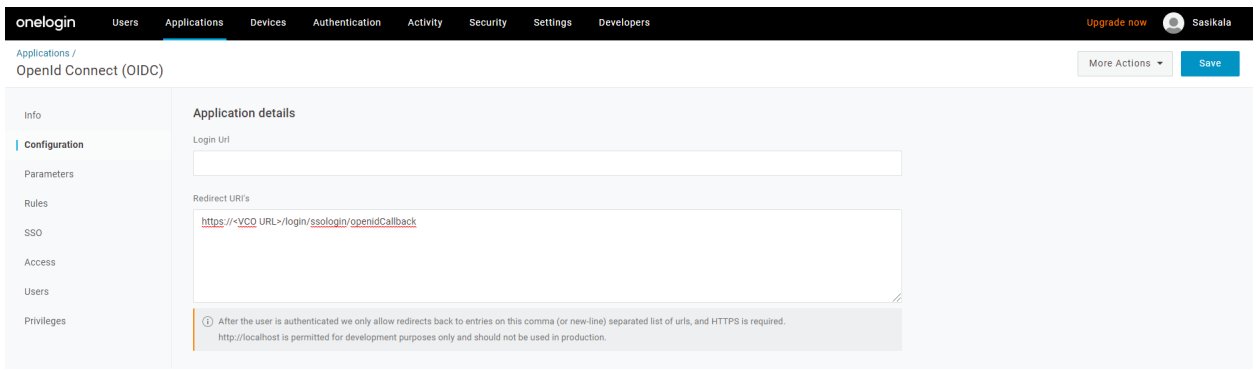
The **Add OpenId Connect (OIDC)** screen appears.



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

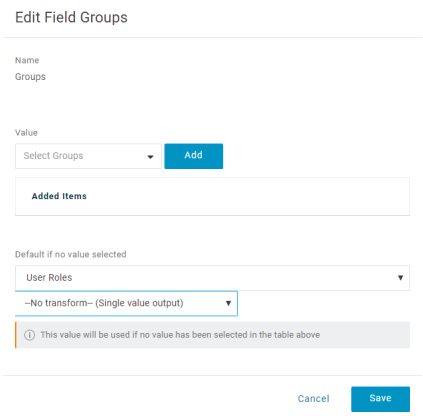
d On the **Configuration** tab, enter the redirect URI that VCO uses as the callback endpoint and click **Save**.

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



e On the **Parameters** tab, under **OpenId Connect (OIDC)**, double click **Groups**.

The **Edit Field Groups** popup appears.

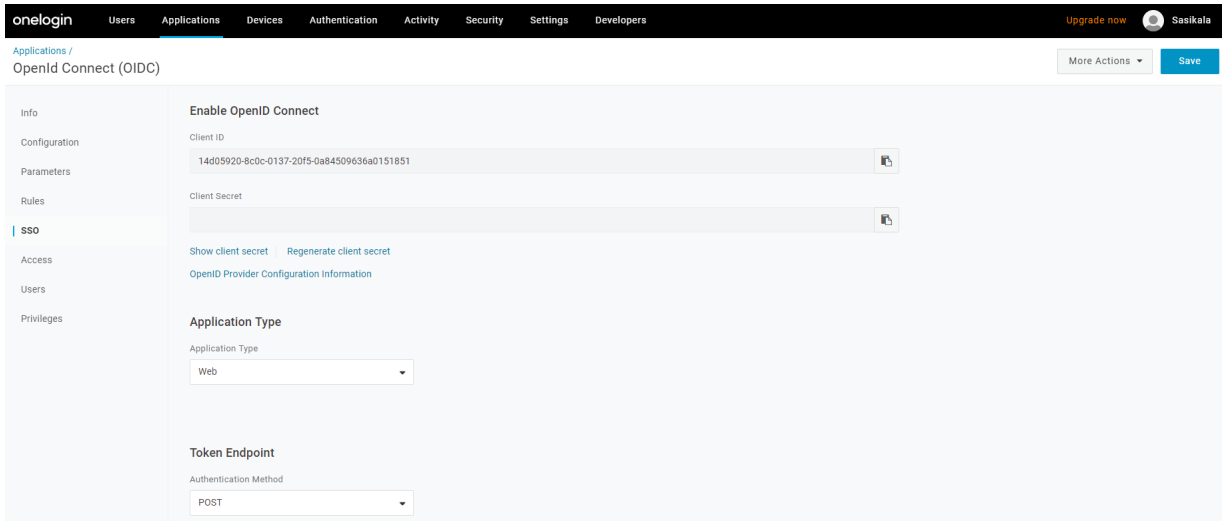


f Configure User Roles with value “--No transform--(Single value output)” to be sent in groups attribute and click **Save**.

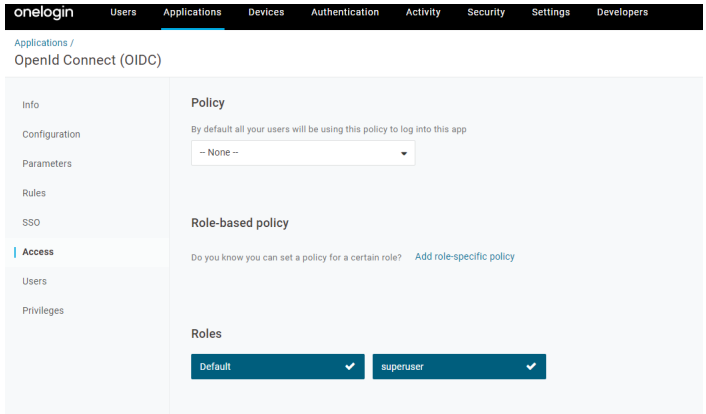
g On the **SSO** tab, from the **Application Type** drop-down menu, select **Web**.

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

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



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



3 To add roles and users to your VCO 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 VCO.

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, VeloCloud Orchestrator (VCO) supports PingOne as the Identity Partner (IDP); however, any PingIdentity product supporting OIDC can be easily configured.

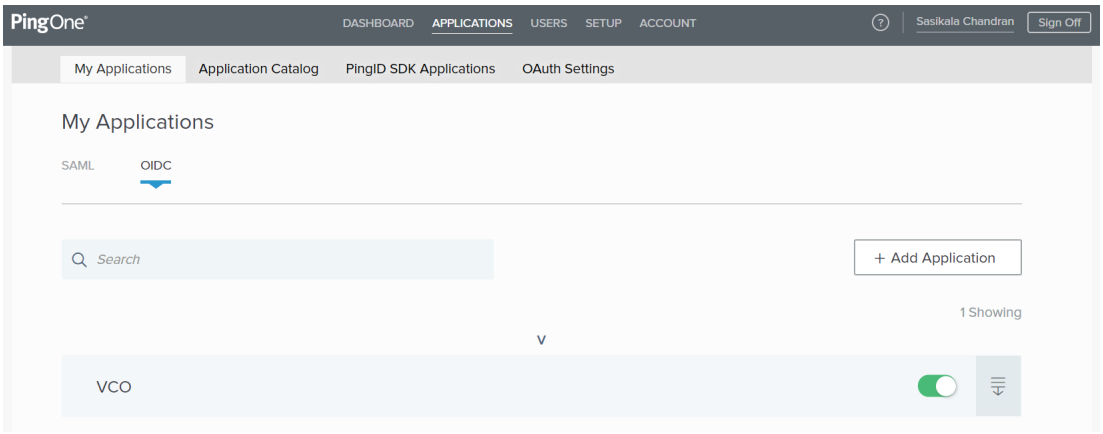
Procedure

1 Log in to your PingOne account as an Admin user.

The **PingOne** home screen appears.

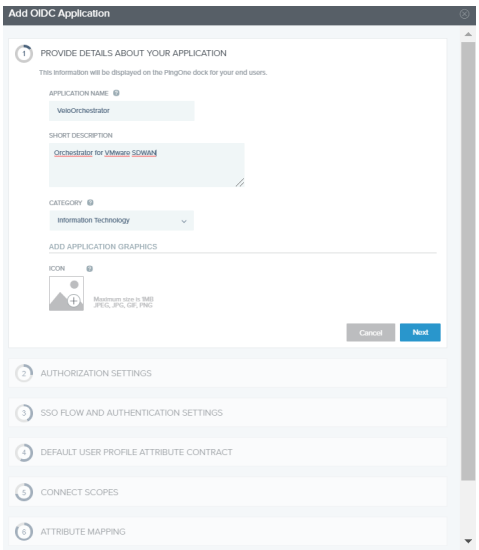
2 To create a new application:

a In the upper navigation bar, click **Applications**.



b On the **My Applications** tab, select **OIDC** and then click **Add Application**.

The **Add OIDC Application** pop-up window appears.



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

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

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

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

In the VCO application, at the bottom of the **Configure Authentication** screen, you can find the redirect URL link. Ideally, the VCO redirect URL will be in this format: https://<VCO 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 VCO application during authentication and click **Next**.

i Under **Attribute Mapping**, map your identity repository attributes to the claims available to your VCO 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 VCO 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 VCO.

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.

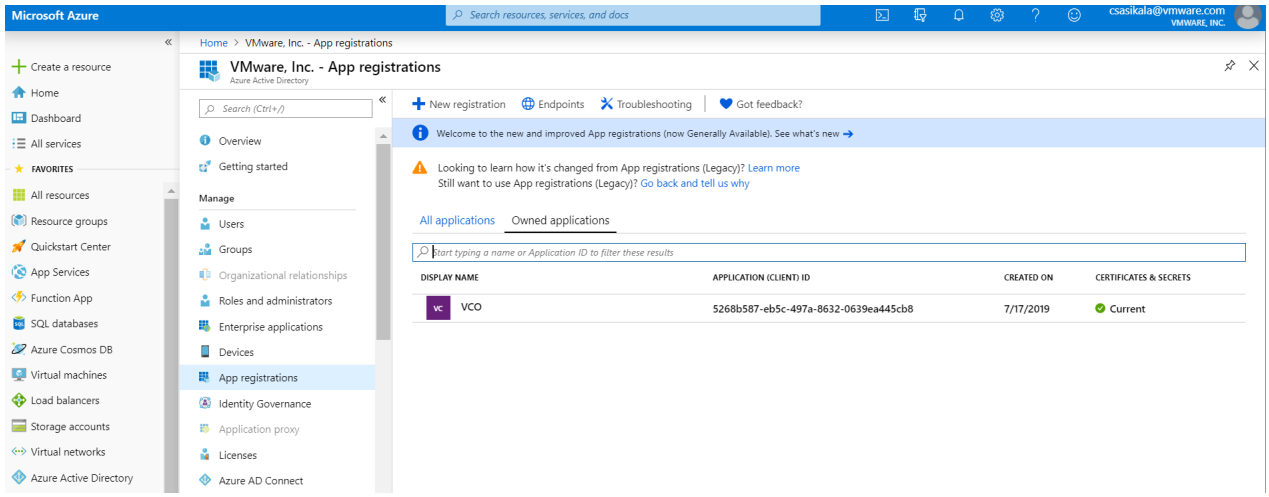
Procedure

1. Log in to your Microsoft Azure account as an Admin user.

   The **Microsoft Azure** home screen appears.

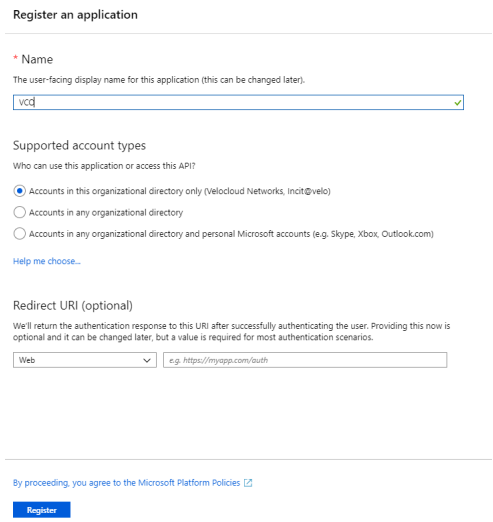
2 To create a new application:

a Search and select the **Azure Active Directory** service.



b Go to **App registration** > **New registration**.

The **Register an application** screen appears.



c In the **Name** field, enter the name for your VeloCloud Orchestrator (VCO) application.

d In the **Redirect URL** field, enter the redirect URL that your VCO application uses as the callback endpoint.

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

e Click **Register**.

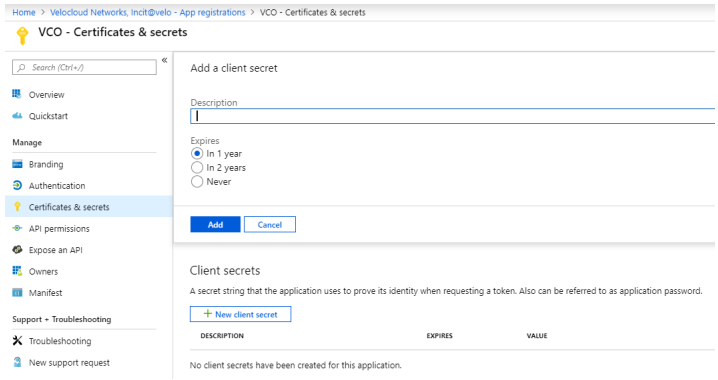
Your VCO application will be registered and displayed in the **All applications** and **Owned applications** tabs. Make sure to note down the Client ID/Application ID to be used during the SSO configuration in VCO.

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

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

h Go to **Certificates & secrets** > **New client secret**.

The **Add a client secret** screen appears.

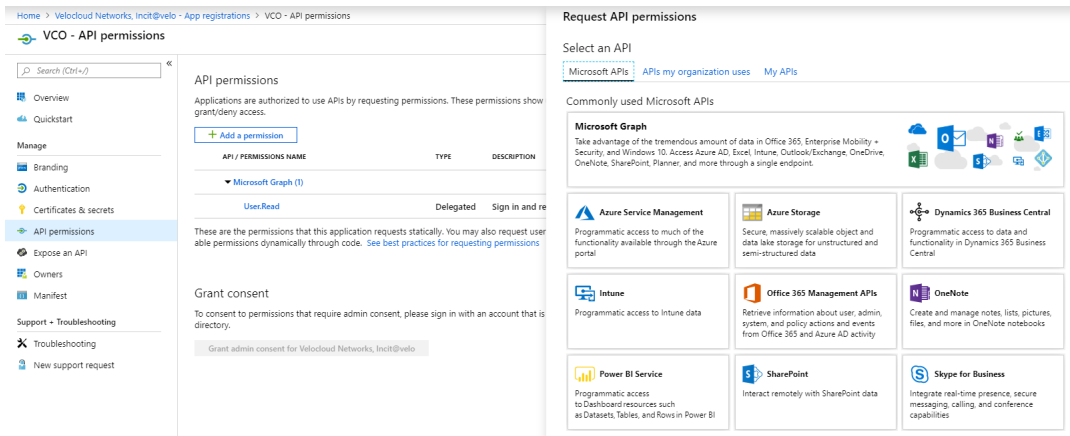


i Provide details such as description and expiry value for the secret and click **Add**.

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

j To configure permissions for your VCO application, click on your VCO application and go to **API permissions** > **Add a permission**.

The **Request API permissions** screen appears.



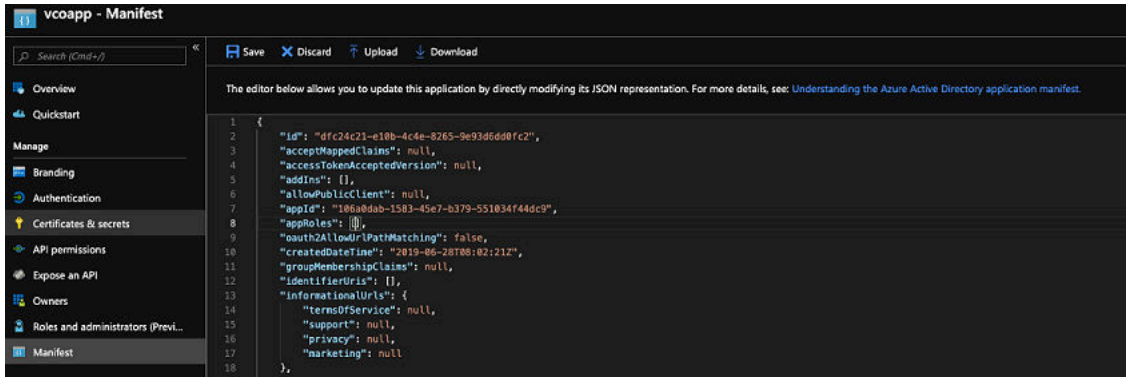
k Click **Microsoft Graph** and select **Application permissions** as the type of permission for your application.

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

m Click **Add permissions**.

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

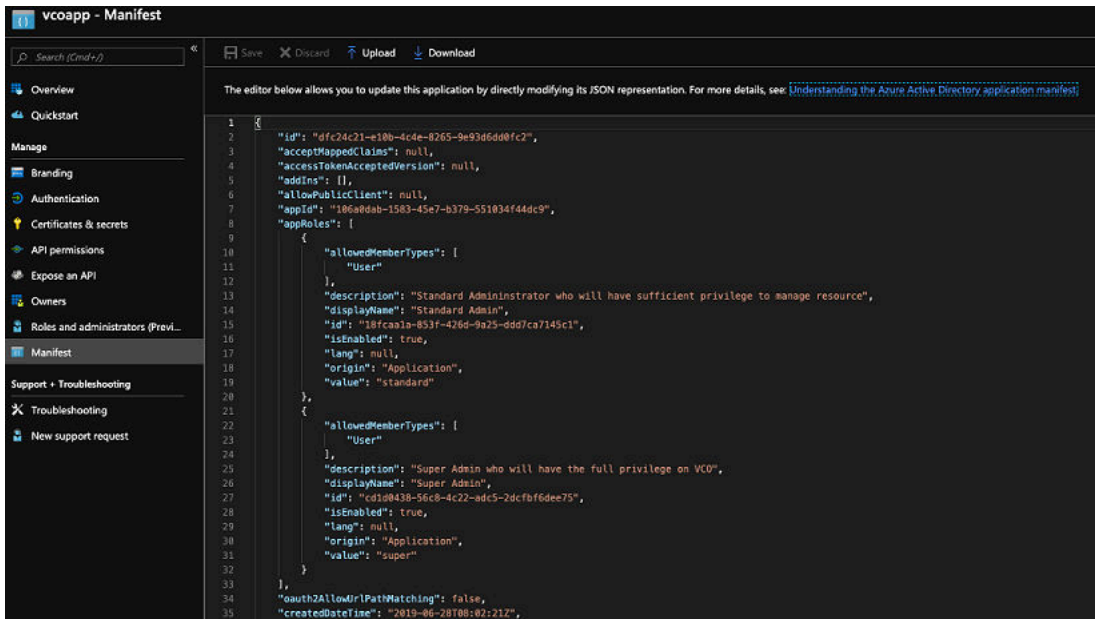
A web-based manifest editor opens, allowing you to edit the manifest within the portal. Optionally, you can select **Download** to edit the manifest locally, and then use **Upload** to reapply it to your application.



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

Sample role objects

```
{
            "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": "superuser"
        }
```



Note Make sure to set `id` to a newly generated GUID value.

3 To assign groups and users to your VCO application:

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

b Search and select your VCO 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 VCO.

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 SD-WAN Support Provider for receiving a Service invitation URL link to register your VCO 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.

   Your 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 VCO.

   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 VCO application as Super Admin user and configure SSO using the received 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 VCO, 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 VCO 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 VCO, select either **Use Default Role** or **Use Identity Provider Roles**.

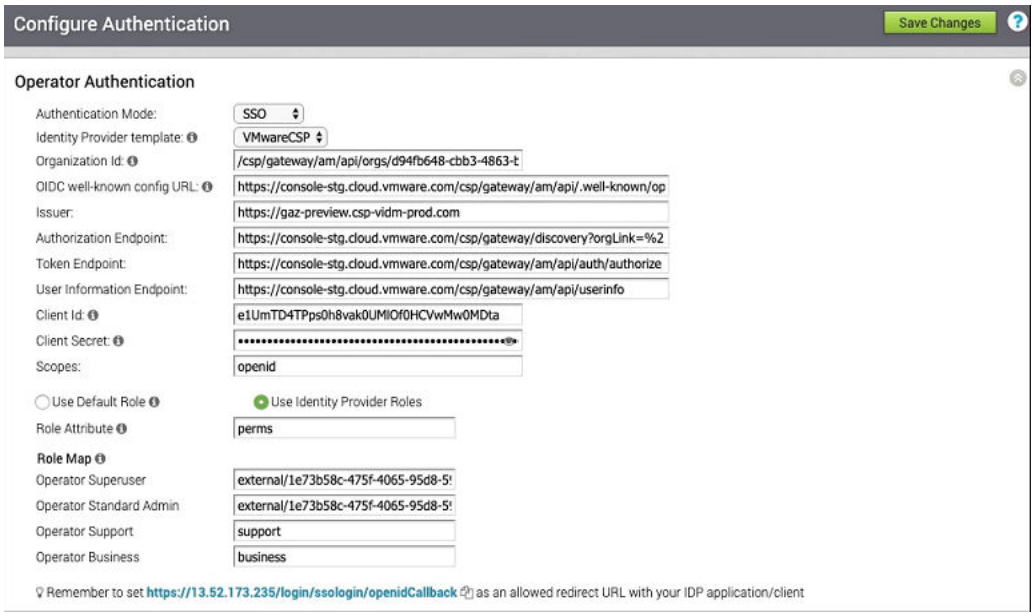
j On selecting the **Use Identity Provider Roles** option, in the **Role Attribute** text box, enter the name of the attribute set in the VMware CSP to return roles.

k In the **Role Map** area, map the VMwareCSP-provided roles to each of the VCO 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.



The user is navigated to the VMware CSP website and allowed to enter the credentials. On IDP verification and successful redirect to VCO test call back, a successful validation message will be displayed.

Results

You have completed integrating VCO application in VMware CSP for SSO and can access the VCO 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 Manage Users.

Troubleshooting VCO

17

This section describes VCO troubleshooting.

This chapter includes the following topics:

Orchestrator Diagnostics

This section describes Orchestrator Diagnostics.

Note The "Orchestrator Diagnostics" section is new for the 3.3.0 release.

VCO Diagnostics Overview

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

Diagnostics Bundle Tab

Users can request and download a diagnostic bundle in the **Diagnostics Bundle** tab.

Columns in the Diagnostics Bundle Tab

The Orchestrator Diagnostics table grid includes the following columns:

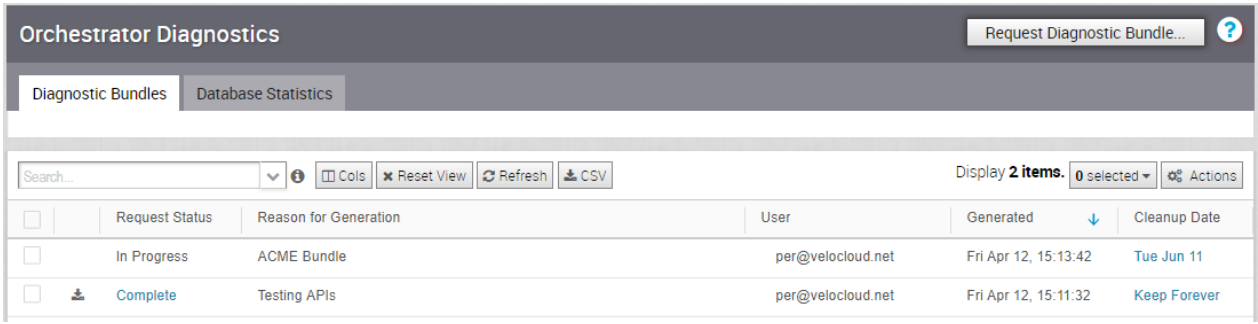
Column Name	Description
Request Status	There are two types of status requests: ■ **Complete** ■ **In Progress** If a bundle has not completed the download, the **In Progress** status appears.
Reason for Generation	The specific reason given for generating a diagnostic bundle. Click the **Request Diagnostic Bundle** button to include a description of the bundle.
User	The individual logged into the VCO.

Column Name	Description
Generated	The date and time when the diagnostic bundle request was sent.
Cleanup Date	The default **Cleanup Date** is three months after the generated date, when the bundle will be automatically deleted. If you need to extend the Cleanup date period, click the **Cleanup Date** link located under the **Cleanup Date** column. For more information, see *Updating Cleanup Date*.

Request a Diagnostic Bundle

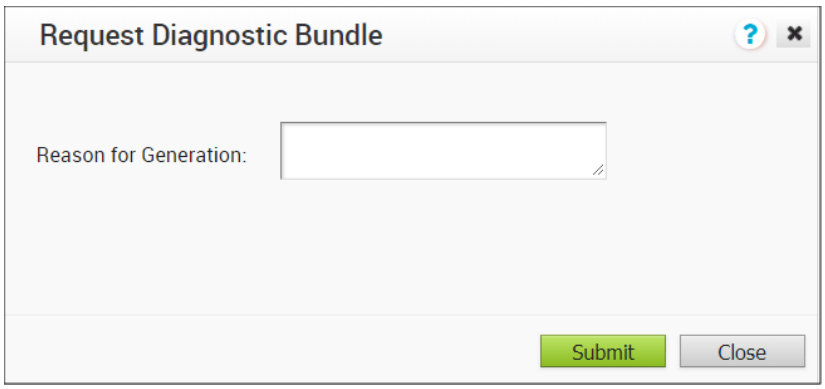
To request a diagnostic bundle:

1 From the VCO navigation panel, click **Orchestrator Diagnostics** .



2 From the **Request Diagnostic Bundle** tab, click the **Request Dialog Bundle** button.

3 In the **Request Diagnostic Bundle** dialog, enter the reason for the request in the appropriate area.



4 Click **Submit**. The bundle request you created displays in the grid area of the **Diagnostic Bundle** screen with an **In Progress** status.

5 Refresh your screen to check the status of diagnostic bundle request. When the bundle is ready for download, a **Complete** status appears.

Download a Diagnostic Bundle

To download a diagnostic bundle:

1 Select a diagnostic bundle you want to download.

2 Click the **Actions** button, and choose **Download Diagnostic Bundle**. You can also click the **Complete** link to download the diagnostics bundle.

The diagnostics bundle downloads.

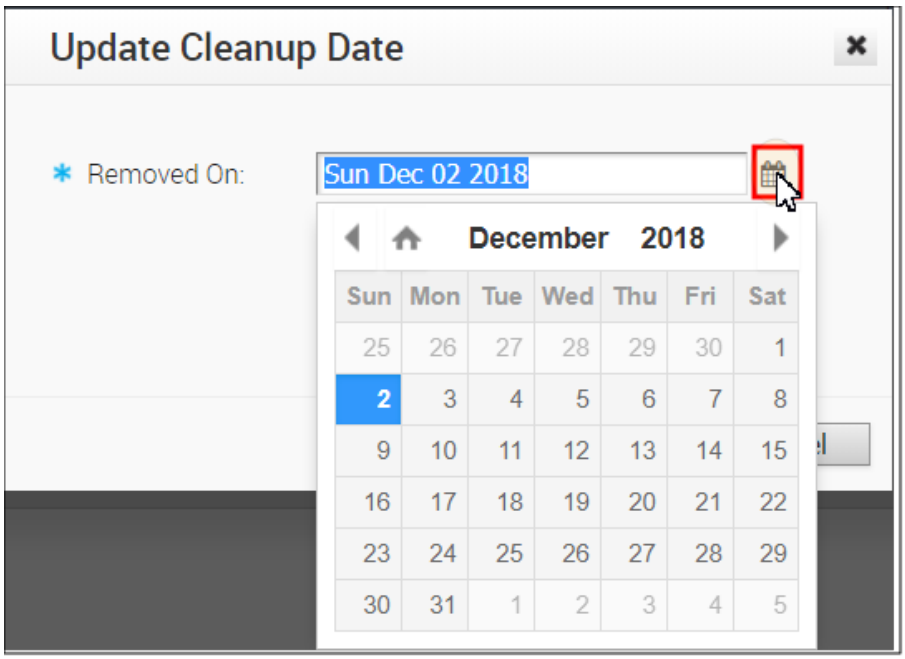
Update the Cleanup Date

The Cleanup date represents the date when the generated bundle will be automatically deleted, which by default is three months after the Generated date. You can change the Cleanup date or choose to keep the bundle indefinitely.

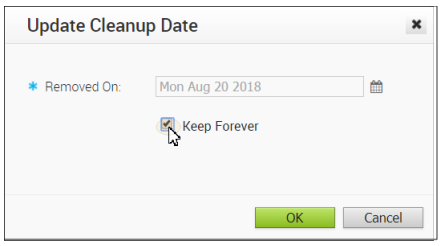
To update the Cleanup date:

1 From the **Clean up Date** column, click the **Cleanup Date** link of your chosen Diagnostic Bundle.

2 From the **Update Cleanup Date** dialog, click the **Calendar** icon to change the date.

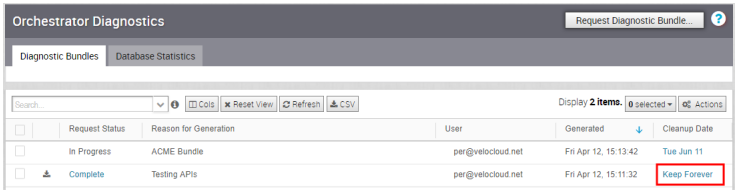


3 You can also choose to keep the bundle indefinitely by checking the **Keep Forever** checkbox.



4 Click **OK**.

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

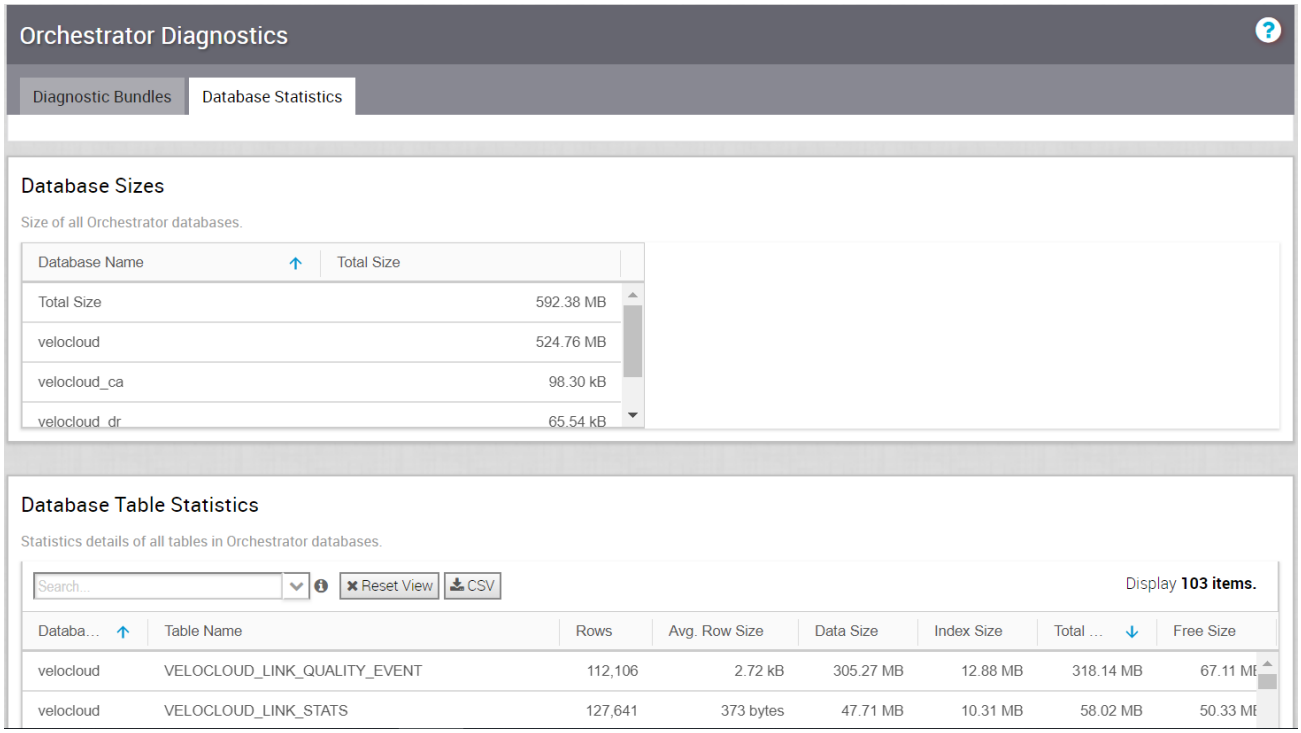


Database Statistics Tab

The **Database Statistics** tab provides a read-only access view of some of the information from a diagnostic bundle.

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

The **Database Statistics** tab displays the following information:



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