

# VeloCloud Administration 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](http://www.vmware.com)

Copyright © 2021 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

# Contents

- 1** VMware SD-WAN by VeloCloud Release 3.3 11
- 2** Who Should Read This Document 14
- 3** VeloCloud Overview 15
  - Solution Components 16
  - Capabilities 16
  - Network Topologies 19
  - Branch Site Topologies 20
  - Roles and Privilege Levels 24
  - User Role Matrix 25
  - Key Concepts 28
  - Supported Modems 32
- 4** User Agreement (VCO Login Screen) 33
- 5** Log in to VCO Using SSO for Enterprise User 34
- 6** Monitor the VCO 35
  - Monitor Navigation Panel 35
  - Network Overview 35
  - Monitor Edges 38
    - Enterprise Global View 38
    - Overview Tab 39
    - QoE Tab 41
    - Transport Tab 44
    - Applications Tab 48
    - Sources Tab 50
    - Destinations Tab 51
    - Business Priority Tab 52
    - Flow Stats Rollups and Retention 53
  - Monitor Network Services 56
  - Monitor Routing 57
    - PIM Neighbors View 57
  - Monitor Alerts 58
  - Monitor Events 58
    - Auto Rollback to the Last Known “Good” Configuration 59
    - Event Types and Descriptions 60

## 7 Configuring VNFs 61

- Monitor the Edge Overview 61
- Configure a VNF Instance 62
- VNF Monitoring for an Edge 72
- VNF Events 74
- Configure VNF Alerts and Notifications 75

## 8 Configure Segments 77

## 9 Configure Network Services 79

- About Edge Clustering 80
  - How Edge Clustering Works 81
  - Configure Edge Clustering 87
- Cloud VPN Hubs & Backhaul Sites (Summary View) 89
- Configure a Non-VeloCloud Site 90
  - Configure Check Point 94
    - Step 1: Configure the Check Point CloudGuard Connect 94
    - Step 2: Configure Check Point as the Non-VeloCloud Site on the VeloCloud Orchestrator 94
  - Configure Amazon Web Services (AWS) 97
    - Obtain Amazon Web Services Configuration Details 97
    - Configure a Non-VeloCloud Site 97
  - Configure Zscaler 99
    - Step 1: Create and Configure a Non-VeloCloud Site 100
    - Step 2: Add to a Configuration Profile 101
    - Step 3: Configure Zscaler 102
    - Step 4: Configure Business Priority Rules 105
- Configuration Tasks 107
  - VPN Workflow 107
  - Configure Cloud Proxy 111
- Configure Cloud Security Services 111
  - Overview of Cloud Security Services 111
  - Configure Cloud Security Services 112
    - Add and Configure a Cloud Security Provider 113
  - Configure Cloud Security Services for Profiles 113
  - Configure Cloud Security Services for Edges 115
  - Monitor Cloud Security Services 117
    - Edges Screen 117
    - Network Services Screen 118
- Configure DNS Services 119
- Configure Netflow Settings 120



- Private Network Names 121
  - Configure Private Networks 122
  - Delete a Private Network Name 122
- Configure Authentication Services 122

## 10 Configure Profiles 124

- Create a Profile 124
- Modify a Profile 126
- Profile Overview Screen 126
- Network to Segment Migration 126
  - Edge Upgrade from 2.X to 3.X Prerequisites 127
  - Best Practices for Upgrading Edges Deployed as Hub and Spoke 127
  - Best Practices for Upgrading Edges Deployed in HA 127
  - Migrate Network to Segment 127
- Configure Local Credentials 132
  - Add Credentials 133

## 11 Configure a Profile Device 134

- Configure a Device 134
  - Assign Segments in Profile 135
  - Configure Authentication Settings 137
  - Configure DNS Settings 137
  - Configure Netflow Settings at the Profile Level 137
  - Configure Syslog Settings at Profile Level 139
  - Configure Cloud VPN 142
    - Configure Branch to VPNs 142
    - Configure Branch to VeloCloud Hubs VPN 144
    - Configure Branch to Branch VPN 145
    - Enable Branch to Branch VPN 145
    - Enable Branch to Branch VPN Isolation 145
    - Enable Dynamic Branch to Branch VPN Isolation by Profile 146
  - Configure Multicast Settings 146
    - Configure Multicast Settings at the Interface Level 148
  - Add and Configure a VLAN 150
  - Configure the Management IP Address 151
  - Configure Device Settings 152
    - Configure Interface Settings 162
  - Configure Wi-Fi Radio Settings 169
  - Configure SNMP Settings at Profile Level 169
  - Configure Visibility Mode 171
  - Assign Partner Gateways 172

- Assign Controllers 174
- Voice Quality Monitoring (VQM) 176

## 12 Cloud VPN 180

- Overview of the Cloud VPN 180
- Branch to Non-VeloCloud Site 182
  - Connect to Customer Data Center with Existing Firewall VPN Router 182
  - laas 183
  - Connect to CWS (Zscaler) 183
- Branch to VeloCloud Hubs 183
- Branch to Branch VPN 184
  - Branch to Branch VPN Isolation by Profile 184
  - Dynamic Branch to Branch 185
  - Dynamic Branch to Branch VPN Isolation by Profile 186

## 13 Configure Profile Business Policy 187

- Create Business Policy 188
  - Configure Match Source 192
  - Configure Match Destination 192
  - Configure Match Application 193
  - Configure Action Priority 194
  - Configure Action Network Service 194
  - Configure Action Link Steering 195
  - Configure Policy-based NAT 200
  - Configure Action Service Class 201
  - Overlay QoS CoS Mapping 201
  - Tunnel Shaper for Service Providers with Partner Gateway 203
- Configure Profile Firewall 204
  - Configure Firewall Rules 204
  - Create or Select a Network 210
- Provision an Edge 218
  - Overview 218
  - Enterprise Edges Screen 218
  - Provision a New Edge 220
  - Actions Drop-down Menu 222
  - Activate Edges 225
    - Activate Edges Using Zero Touch Provisioning (Tech Preview) 226
    - Activate Edges Using Email 226

## 14 Edge Overview Tab 230

- Edge Overview 230

- Edge Overview Properties 231
  - Properties Overview 231
  - Properties Area Field and Checkbox Descriptions 231
  - Initiate Edge Activation 232
  - Edge License 233
- Edge Profile 233
  - Profile Overview 234
  - Profile Drop-Down Menu 234
  - Edge-specific Overrides and Additions 235
  - Contact & Location 235
  - Change Edge Location 236
  - Change Shipping Address 236
- RMA Reactivation 236
  - Edge Reactivation Overview 236
  - RMA Reactivation Scenarios 237
  - RMA Reactivation Steps 237
  - RMA Reactivation Troubleshooting 239
- 15 Configure an Edge Device 241**
  - Configure Netflow Settings at the Edge Level 243
  - Configure Syslog Settings at Edge Level 244
  - Configure Static Route Settings 246
  - Configure ICMP Probes/Responders 247
  - Edge Cloud VPN 247
  - High Availability (HA) 247
  - Configure VLAN Settings 248
  - Configure Device Settings 248
    - Configure DHCP Server on Routed Interfaces 248
    - Enabling RADIUS on a Routed Interface 250
    - Configure Edge LAN Overrides 251
    - Configure Edge WAN Overrides 251
    - Configure Edge WAN Overlay Settings 252
    - Configure Edge WAN Settings for MPLS Private Links 256
    - Configure Edge WAN Settings for MPLS Private Links 257
    - SD-WAN Service Reachability via MPLS 259
  - Configure SNMP Settings at Edge Level 263
  - Configure Wi-Fi Radio, DNS, Authentication, and Netflow Overrides 265
    - Configure Edge Business Policy 265
    - Configure Edge Firewall 266
    - Configure Edge Activation 270
    - LAN-side NAT Rules at Edge Level 271

- 16 Site Configurations 274**
  - Data Center Configurations 275
  - Configure Branch and Hub 275
  
- 17 Configure Dynamic Routing with OSPF or BGP 287**
  - Enable OSPF 287
    - Route Filters 291
  - Enable BGP 292
  - OSPF/BGP Redistribution 297
  - Overlay Flow Control 298
    - Global Routing Preferences 298
    - Overlay Flow Control Table 299
  
- 18 Configure Alerts 301**
  - Configure SNMP Traps 301
  
- 19 Administration 303**
  - Configure System Settings 303
    - Overview of Single Sign On 303
    - Configure Single Sign On for Enterprise User 303
    - Configure Single Sign On for Identity Partners 306
      - Configure an IDP for Single Sign On 306
    - Self-service Password Reset 324
    - Configure Two-factor Authentication 327
    - Enforce PCI Compliance on VCO 328
  - Monitor Edge Licensing 329
    - Generate an Edge Licensing Report 329
  
- 20 Configure VCE High Availability 330**
  - Overview of VeloCloud Edge HA 330
  - Prerequisites 331
  - High Availability Options 331
    - HA Option 1: Standard HA 331
    - HA Option 2: Enhanced HA 335
  - Split-Brain Detection and Prevention 336
    - Split-Brain Condition 336
    - Split-Brain Detection and Prevention 336
  - Failure Scenarios 337
  - Support for BGP Over HA Link 337
  - Selection Criteria to Determine Active and Standby Status 338
  - VLAN-tagged Traffic Over HA Link 338

- Configure HA 339
  - 1. Enable High Availability (HA) 339
  - 2. Wait for VCE to Assume Active 339
  - 3. Connect the Standby VCE to the Active Edge 340
  - 4. Connect LAN and WAN Interfaces on Standby VCE 340
- HA Event Details 341

## 21 Testing and Troubleshooting 342

- Remote Diagnostics 343
- Remote Actions 346
  - Edge Remote Action Definitions 347
  - Reset Edges to Factory Settings 347
- Diagnostic Bundles 348
  - Request Packet Capture 348
  - Download Bundle 349
  - Delete Bundle 349
  - Request Diagnostic Bundle 350

## 22 VeloCloud Virtual Edge Deployment Guide 351

- Overview of Virtual Edge 351
- Deployment Prerequisites 351
- Special Considerations for VeloCloud Virtual Edge deployment 352
- Overview of cloud-init 353
- Install Virtual Edge on KVM 354
  - Considerations 355
  - Enable SR-IOV on KVM 355
  - Install a Virtual Edge on KVM 356
- Install Virtual Edge on VMware ESXi 360
  - Enable SR-IOV on VMware 360
  - Installing a Virtual Edge on VMware ESXi 362

## 23 AliCloud Virtual Edge Deployment Guide 367

- AliCloud vVCE Deployment Overview 367
- Topology A - Virtual Edge Deployment on AliCloud VPC 368
- Topology B - Virtual Edge Deployment on AliCloud Single-Arm Topology 370
- Create a Virtual Private Cloud 372
- Create a VSwitch 373
- Create a Security Group 375
- Add Security Group Rules 377
- Create Custom Route Tables and Associate VSwitches 378
- Provision an Edge on the VCO 380

- [Create a vVCE Instance on the ECS Console](#) 384
- [Create an Elastic Network Interface](#) 387
- [Create Elastic IP and Assign it to Public Interface of the Edge](#) 389
- [Bind an ENI to an Edge instance](#) 391
- [Create a LAN Instance](#) 393
- [Add a Custom Route Table Entry](#) 396
- [Create a Jump Host Instance](#) 397
- [SSH Login to Edge using EIP](#) 400
- [SSH to Private IP of the Edge from Jump Host](#) 400
- [Activate the Edge Against the VCO](#) 401

## **24** Azure Virtual WAN VCG Automation 402

- [Azure Virtual WAN VCG Automation Overview](#) 402
- [Prerequisite Azure Configuration](#) 403
  - [Register VCO Application](#) 403
  - [Assign the VCO Application to Contributor Role](#) 405
  - [Register a Resource Provider](#) 406
  - [Create a Client Secret](#) 408
- [Configure Azure Virtual WAN for Branch-to-Azure VPN Connectivity](#) 409
  - [Create a Resource Group](#) 409
  - [Create a Virtual WAN](#) 411
  - [Create a Virtual Hub](#) 412
  - [Create a Virtual Network](#) 414
  - [Create a Virtual Connection between VNet and Hub](#) 416
- [Configure VCO for Branch-to-Azure VPN Connectivity](#) 417
  - [Configure an IaaS Subscription Network Service](#) 417
  - [Configure a Microsoft Azure Non-VeloCloud Site](#) 418
    - [Associate a Non-VeloCloud Site to a Profile](#) 420
    - [Edit a VPN Site](#) 421
  - [Synchronize VPN Configuration](#) 422
  - [Delete a Non-VeloCloud Site](#) 422

## **25** VeloCloud Edge Appliance Documentation 424

# VMware SD-WAN by VeloCloud Release 3.3

1

The *VMware SD-WAN by VeloCloud Administration 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	<a href="#">Network Overview</a>
Updated	<a href="#">Overview of Single Sign On</a>
New	<a href="#">Configure VMware CSP for Single Sign On</a>
New	<a href="#">Configure Syslog Settings at Profile Level</a>
New	<a href="#">Configure Syslog Settings at Edge Level</a>
Updated	<a href="#">Configure a Device</a>
Updated	<a href="#">Chapter 9 Configure Network Services</a>
New	<a href="#">Configure Netflow Settings</a>
New	<a href="#">Configure Netflow Settings at the Profile Level</a>
New	<a href="#">Configure Netflow Settings at the Edge Level</a>
Updated	<a href="#">Chapter 15 Configure an Edge Device</a>
Updated	<a href="#">Flow Stats Rollups and Retention</a>
Updated	<a href="#">Create a Virtual Hub</a>
Updated	<a href="#">Configure Edge WAN Overlay Settings</a>
Updated	<a href="#">Configure Cloud Security Services</a>
Updated	<a href="#">Add and Configure a Cloud Security Provider</a>
Updated	<a href="#">Configure Cloud Security Services for Profiles</a>
Updated	<a href="#">Configure Cloud Security Services for Edges</a>
Updated	<a href="#">Port Forwarding Rules</a>

Status	Section
New	<a href="#">Configure a VNF Instance</a>
Updated	<a href="#">Configure VNF Alerts and Notifications</a>
New	<a href="#">LAN-side NAT Rules at Edge Level</a>
New	<a href="#">Configure SNMP Settings at Edge Level</a>
Updated	<a href="#">Enable BGP</a>
Updated	<a href="#">Enable BGP (Community Additive Support)</a>
Updated	<a href="#">Linking Steering: Overlay DSCP Configuration</a>

## What's Changed in Version 3.3.1?

Status	Section
Updated	<a href="#">Configure Cloud Security Services for Profiles</a>
Updated	<a href="#">Create Business Policy</a>
Updated	<a href="#">Configure Firewall Rules</a>
New	<a href="#">Configure Check Point</a>
Updated	<a href="#">Enable OSPF</a>
New	<a href="#">Overview of Single Sign On</a>
New	<a href="#">Configure Single Sign On for Enterprise User</a>
New	<a href="#">Chapter 5 Log in to VCO Using SSO for Enterprise User</a>
New	<a href="#">Configure an IDP for Single Sign On</a>
New	<a href="#">Azure Virtual WAN VCG Automation Overview</a>
New	<a href="#">Chapter 23 AliCloud Virtual Edge Deployment Guide</a>

## What's Changed in Version 3.3.0?

Status	Section
Updated	<a href="#">Auto Rollback to the Last Known "Good" Configuration</a>
Updated	<a href="#">Network to Segment Migration</a>
Updated	<a href="#">Split-Brain Detection and Prevention</a>
Updated	<a href="#">VLAN-tagged Traffic Over HA Link</a>



Status	Section
Updated	<a href="#">Selection Criteria to Determine Active and Standby Status</a>
Updated	<a href="#">Overview of cloud-init</a>
Updated	<a href="#">Activate Edges</a>
New	<a href="#">How Edge Clustering Works</a>
New	<a href="#">Self-service Password Reset</a>
New	<a href="#">Monitor Edge Licensing</a>
New	<a href="#">Chapter 4 User Agreement (VCO Login Screen)</a>
New	<a href="#">Flow Stats Rollups and Retention</a>
New	<a href="#">Activate Edges Using Zero Touch Provisioning (Tech Preview)</a>

## 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.

# Who Should Read This Document

# 2

This guide is written for network administrators, network analysts, and IT administrators responsible for deploying, monitoring and managing Enterprise branch network. This guide describes the settings of the core VeloCloud configurations: **Networks**, **Network Services**, **Profiles**, and **Edges** in detail.

## Prerequisites

It is assumed that you have become thoroughly familiar with the concepts described in the [Chapter 3 VeloCloud Overview](#) before proceeding with configuration steps. It is also strongly recommended that you read and perform the steps in [Activate Edges](#) to become familiar with the basic configuration and Edge activation.

## About This Guide

In this guide a hypothetical company, VeloAcme, will be used to describe the configuration for Networks, Network Services, Profiles, and Edges. This guide also provides steps to monitor, test, and troubleshoot the VeloCloud system.

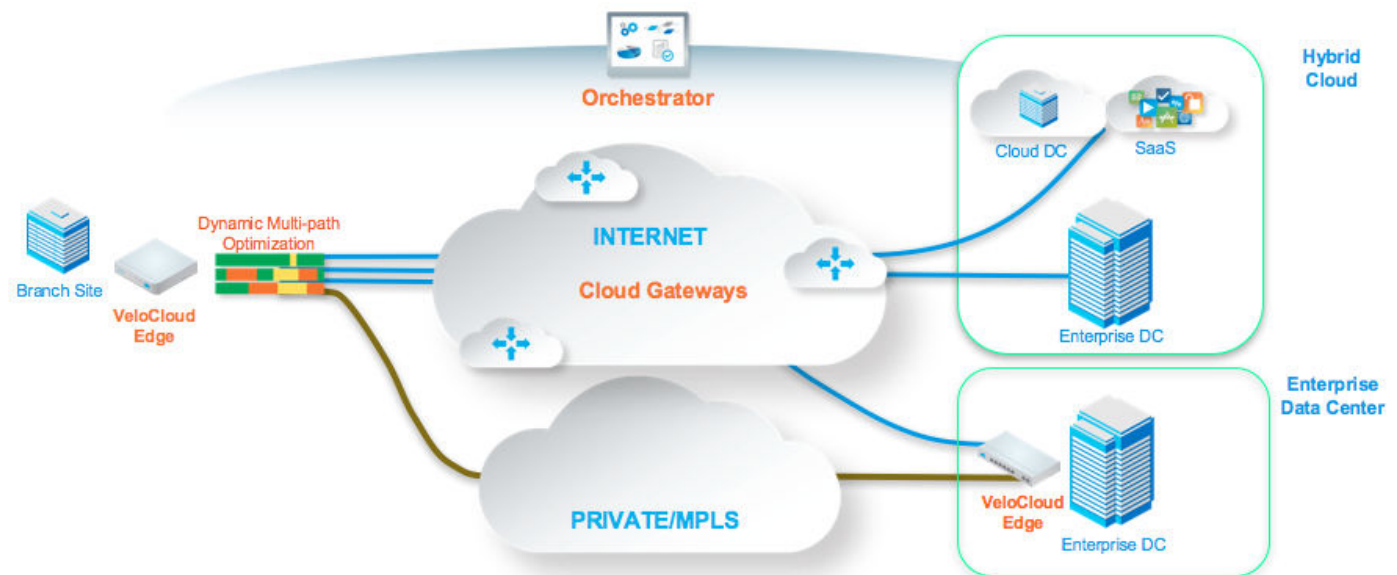
# VeloCloud Overview

# 3

This section provides an overview of VeloCloud.

Cloud-delivered Software-defined WAN from VeloCloud assures enterprise and cloud application performance over Internet and hybrid WAN while simplifying deployments and reducing costs.

VeloCloud is a cloud network service solution enabling sites to quickly deploy Enterprise grade access to legacy and cloud applications over both private networks and Internet broadband. The following figure shows the VeloCloud Software-defined WAN solution components (in orange). The components are described in more detail in the following sections.



This chapter includes the following topics:

- [Solution Components](#)
- [Capabilities](#)
- [Network Topologies](#)
- [Branch Site Topologies](#)
- [Roles and Privilege Levels](#)
- [User Role Matrix](#)
- [Key Concepts](#)

- [Supported Modems](#)

## Solution Components

This section describes VeloCloud solution components.

### VeloCloud Edge

A thin “Edge” that is zero IT touch provisioned from the cloud for secured, optimized connectivity to your apps and virtualized services. The VeloCloud Edges are zero-touch, enterprise-class devices or virtual software that provide secure and optimized connectivity to private, public and hybrid applications; compute; and virtualized services. VeloCloud Edges perform deep application recognition, application and per-packet steering, on-demand remediation performance metrics and end-to-end quality of service (QoS) in addition to hosting Virtual Network Function (VNF) services. An Edge pair can be deployed to provide High Availability (HA). Edges can be deployed in branches, large sites and data centers. All other network infrastructure is provided on-demand in the cloud.

The VeloCloud Orchestrator provides centralized enterprise-wide configuration and real-time monitoring, as well as orchestrates the data flow into and through the SDWAN overlay network. Additionally, it provides the one-click provisioning of virtual services across Edges, in centralized and regional enterprise service hubs and in the cloud.

### VeloCloud Gateways

VeloCloud’s network consists of gateways deployed at top tier network points-of-presence and cloud data centers around the world, providing SDWAN services to the doorstep of SaaS, IaaS and cloud network services, as well as access to private backbones. Multi-tenant, virtual Gateways are deployed both by VeloCloud transit and cloud service provider partners. The gateways provide the advantage of an on-demand, scalable and redundant cloud network for optimized paths to cloud destinations as well as zero-installation applications.

## Capabilities

This section describes VeloCloud capabilities.

### Dynamic Multi-path Optimization

VeloCloud Dynamic Multi-path Optimization is comprised of automatic link monitoring, dynamic link steering and on-demand remediation.

### Link Steering and Remediation

Dynamic, application aware per-packet link steering is performed automatically based on the business priority of the application, embedded knowledge of network requirements of the application, and the real-time capacity and performance of each link. On-demand mitigation of individual link degradation through forward error correction, jitter buffering and negative

acknowledgment proxy also protects the performance of priority and network sensitive applications. Both the dynamic per-packet link steering and on-demand mitigation combine to deliver robust, sub-second blocked and limited protection to improve application availability, performance and end user experience.

## Cloud VPN

Cloud VPN is a 1-click, site-to-site, VPNC-compliant, IPSec VPN to connect VeloCloud and Non-VeloCloud Sites while delivering real-time status and the health of the sites. The Cloud VPN establishes dynamic edge-to-edge communication for all branches based on service level objectives and application performance. Cloud VPN also delivers secure connectivity across all branches with PKI scalable key management. New branches join the VPN network automatically with access to all resources in other branches, enterprise data centers, and 3rd party data centers, like Amazon AWS.

## Multi-source Inbound QoS

VeloCloud classifies 2,500+ applications enabling smart control. Out-of-the-box defaults set the multi-source inbound Quality of Service (QoS) parameters for different application types with IT required only to establish application priority. Knowledge of network requirements for different application types, automatic link capacity measurements and dynamic flow monitoring enables automation of QoS configurations and bandwidth allocations.

## Firewall

VeloCloud delivers stateful and context-aware (application, user, device) integrated application aware firewall with granular control of sub-applications, support for protocol-hopping applications – such as Skype and other peer-to-peer applications (e.g., disable Skype video and chat, but allow Skype audio). The secure firewall service is user- and device OS-aware with the ability to separate voice, video, data, and compliance traffic. Policies for BYOD devices (such as Apple iOS, Android, Windows, and Mac OS) on the corporate network are easily controlled.

## Network Service Insertion

The VeloCloud Solution supports a platform to host multiple virtualized network functions to eliminate single-function appliances and reduce branch IT complexity. VeloCloud service-chains traffic from the branch to both cloud-based and enterprise regional hub services, with assured performance, security, and manageability. Branches leverage consolidated security and network services, including those from partners like Zscaler and Websense. Using a simple click-to-enable interface, services can be inserted in the cloud and on-premise with application specific policies.

## Activation

VeloCloud Edge appliances automatically authenticate, connect, and receive configuration instructions once they are connected to the Internet in a zero-touch deployment. They deliver a highly available deployment with VeloCloud Edge redundancy protocol and integrate with the existing network with support for OSPF routing protocol and benefit from dynamic learning and automation.

## Routing and Segmentation

### Overlay Flow Control

The VeloCloud Edge learns routes from adjacent routers through OSPF and BGP. It sends the learned routes to the Gateway/Controller. The Gateway/Controller acts like a route reflector and sends the learned routes to other VeloCloud SD-WAN Edges. The Overlay Flow Control (OFC) enables enterprise-wide route visibility and control for ease of programming and for full and partial overlay.

### OSPF

VeloCloud supports inbound/outbound filters to OSPF neighbors, OE1/OE2 route types, MD5 authentication. Routes learned through OSPF will be automatically redistributed to the controller hosted in the cloud or on-premise.

### BGP

VeloCloud supports inbound/outbound filters and the filter can be set to Deny, or optionally adding/changing the BGP attribute to influence the path selection, i.e. RFC 1998 community, MED, AS-Path prepend, and local preference.

## Segmentation

Network segmentation is an important feature for both enterprises and service providers. In the most basic form, segmentation provides network isolation for management and security reasons. Most common forms of segmentation are VLANs for L2 and VRFs for L3.

### Typical Use Cases for Segmentation:

- Line of Business Separation: Engineering, HR etc. for Security/Audit
- User Data Separation: Guest, PCI, Corporate traffic separation
- Enterprise uses overlapping IP addresses in different VRFs

However, the legacy approach is limited to a single box or two physically connected devices. To extend the functionality, segmentation information must be carried across the network.

VeloCloud enables end-to-end segmentation. When the packet traverses through the Edge, the Segment ID is added to the packet and is forwarded to the Hub and cloud Gateway, allowing network service isolation from the Edge to the cloud and data center. This provides the ability to group prefixes into a unique routing table, making the business policy segment aware.

## Routing

In Dynamic Routing, VeloCloud Edge learns routes from adjacent routers through OSPF or BGP. The VeloCloud Orchestrator maintains all the dynamically learned routes in a global routing table called the Overlay Flow Control. The Overlay Flow Control allows management of dynamic routes in the case of "Overlay Flow Control sync" and "change in Inbound/Outbound filtering configuration." The change in inbound filtering for a prefix from IGNORE to LEARN would fetch the prefix from the Overlay Flow Control and install into the Unified routing table.

For more information, see [Chapter 17 Configure Dynamic Routing with OSPF or BGP](#).

## Business Policy Framework

Quality of Service (QoS), resource allocations, link/path steering, and error correction are automatically applied based on business policies and application priorities. Orchestrate traffic based on transport groups defined by private and public links, policy definition, and link characteristics.

## Network Topologies

This section describes network topologies for branches and data centers.

### Branches to Private Third Party (VPN)

Customers with a private data center or cloud data center often want a way to include it in their network without having to define a tunnel from each individual branch office site to the data center. By defining the site as a non-VeloCloud site, a single tunnel will be built from the nearest VeloCloud Gateway to the customer's existing router or firewall. All the VeloCloud Edges that need to talk to the site will connect to the same VeloCloud Gateway to forward packets across the tunnel, simplifying the overall network configuration and new site bring up.



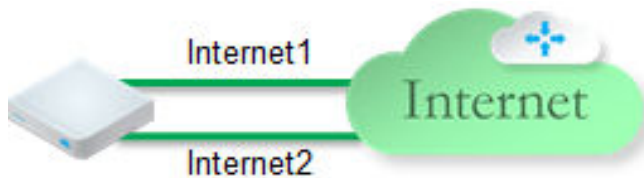
VeloCloud simplifies the branch deployment and delivers enterprise great application performance or public/private link for cloud and/or on-premise applications.

## Branch Site Topologies

The VeloCloud service defines two three different typical branch topologies designated as Bronze and Silver Bronze, Silver, and Gold. In addition, pairs of VeloCloud Edges can be configured in a High Availability (HA) configuration at a branch location.

### Bronze Site Topology

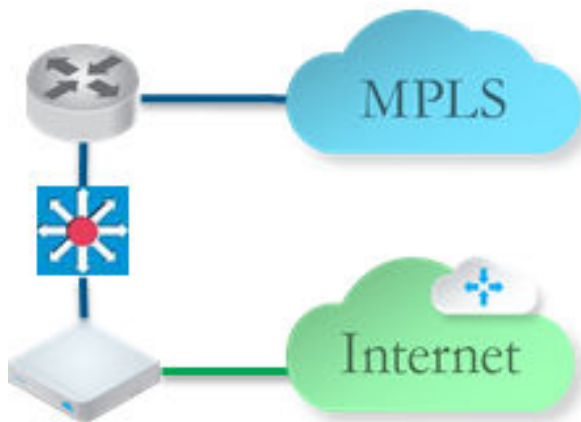
The Bronze topology represents a typical small site deployment where there are one or two WAN links connected to the public internet. In the Bronze topology, there is no MPLS connection and there is no L3 switch on the LAN-side of the VeloCloud Edge. The following figure shows an overview of the Bronze topology.



### Silver Site Topology

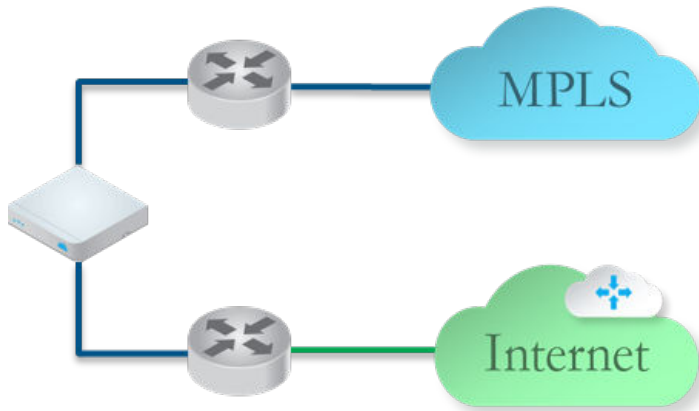
The Silver topology represents a site that also has an MPLS connection, in addition to one or more public Internet links. There are two variants of this topology.

The first variant is a single L3 switch with one or more public internet links and a MPLS link, which is terminated on a CE and is accessible through the L3 switch. In this case, the VeloCloud Edge goes between the L3 switch and Internet (replacing existing firewall/router).



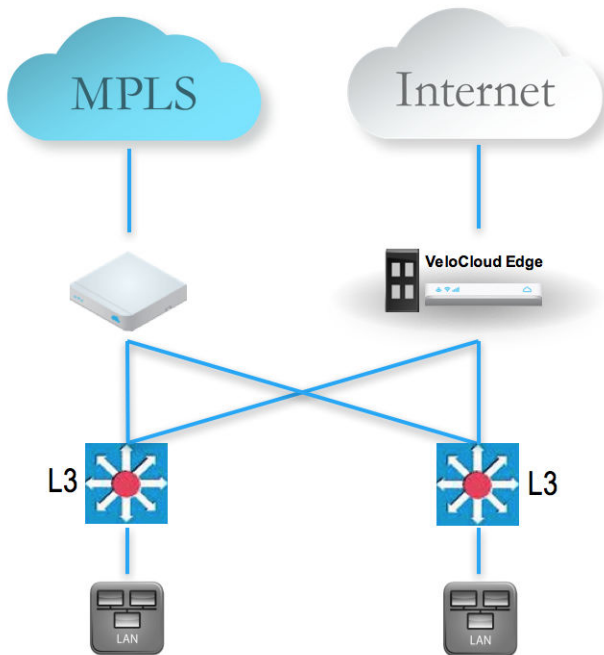
The second variant includes MPLS and Internet routers deployed using HSRP with an L2 switch on the LAN side. In this case, the VeloCloud Edge replaces the L2 switch.



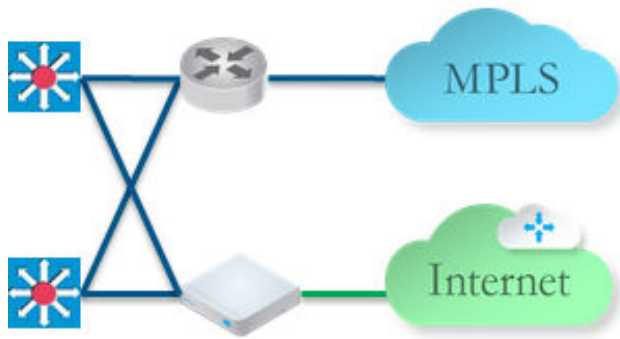


### Gold Site Topology

The Gold topology is a typical large branch site topology. The topology includes active/active L3 switches which communicate routes using OSPF or BGP, one or more public internet links and a MPLS link which is terminated on a CE router that is also talking to OSPF or BGP and is accessible through the L3 switches.

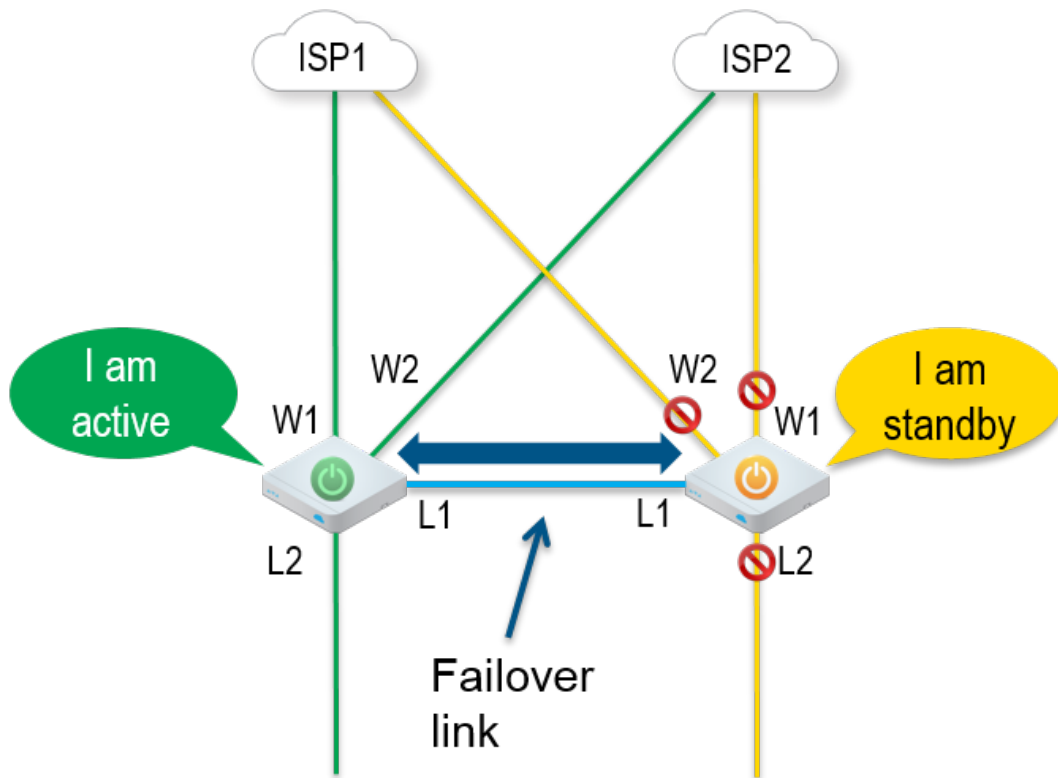


A key differentiation point here is a single WAN link is accessible via two routed interfaces. In order to support this, a virtual IP address is provisioned inside the edge (similar to a Cisco “loopback interface”) and can be advertised over OSPF , BGP, or statically routed to.



## High Availability (HA) Configuration

The following figure provides a conceptual overview of the VeloCloud High Availability configuration using two VeloCloud Edges, one active and one standby.



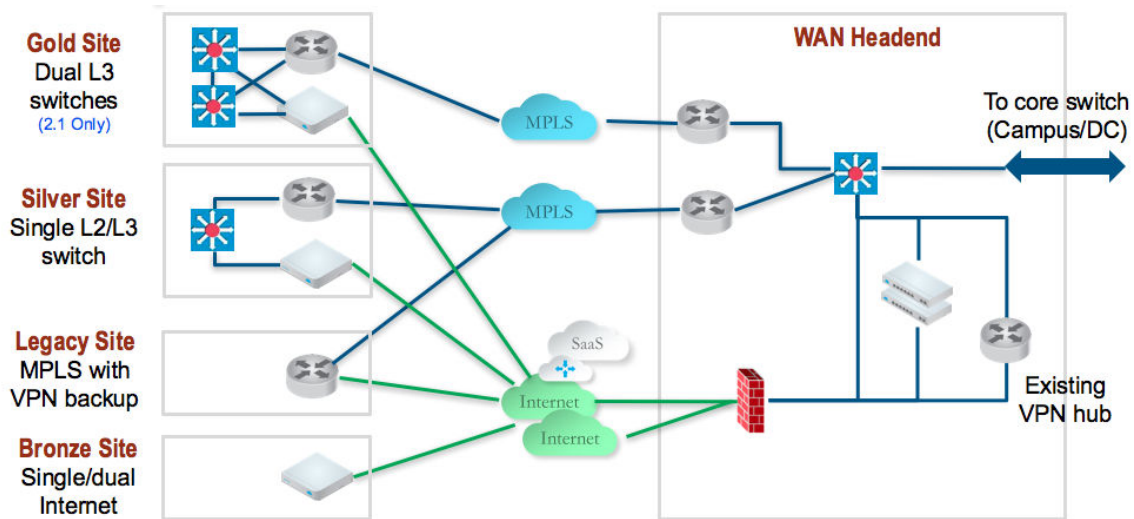
Connecting the L1 ports on each edge is used to establish a failover link. The standby VeloCloud Edge blocks all ports except the L1 port for the failover link.

## On-premise Topology

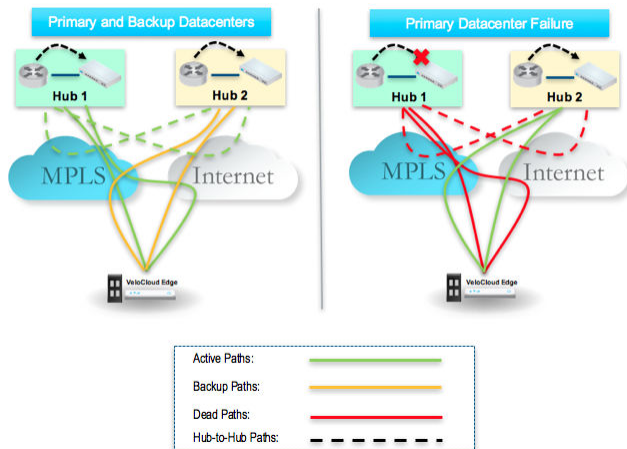
The on-premise topology consists of two hubs and multiple branches (some with VCE and some without). Each hub has hybrid WAN connectivity. There are several branch types.

**Note** The Gold Site is not currently in the scope of this release and will be added at a later time.

The MPLS network runs BGP and peers with all the CE routers. At Hub 1, Hub 2, and Silver 1 sites, the L3 switch runs OSPF or BGP with the CE router and firewall (in case of hub sites).



In some cases, there may be redundant data centers which advertise the same subnets with different costs. In this scenario, both data centers can be configured as edge-to-edge VPN hubs. Since all edges connect directly to each hub, the hubs in fact also connect directly to each other. Based on route cost, traffic is steered to the preferred active data center.



In previous versions, users could create an enterprise object using Zscaler or Palo Alto Network as a generic Non-VeloCloud Site. In 2.0, that object will now become a first-class citizen as a Non-VeloCloud Site.

VeloCloud's Cloud-Delivered SD-WAN solution combines the economics and flexibility of the hybrid WAN with the deployment speed and low maintenance of cloud-based services. It dramatically simplifies the WAN by delivering virtualized services from the cloud to branch offices. VeloCloud's customer-premise equipment, VeloCloud Edge, aggregates multiple broadband links (e.g., Cable, DSL, 4G-LTE) at the branch office, and sends the traffic to VeloCloud gateways. Using cloud-based orchestration, the service can connect the branch office to any of type of data center: enterprise, cloud, or Software-as-a-Service.

VeloCloud Edge is a compact, thin Edge device that is zero-IT-touch provisioned from the cloud for secure, optimized connectivity to applications and data. A cluster of gateways is deployed globally at top-tier cloud data centers to provide scalable and on-demand cloud network services. Working with the Edge, the cluster delivers dynamic, multi-path optimization so multiple, ordinary broadband links appear as a single, high bandwidth link. Orchestrator management provides centralized configuration, real-time monitoring, and one-click provisioning of virtual services.

## Roles and Privilege Levels

The following primary roles are defined for VeloCloud:

- IT Administrator (or Administrator)
- Site Contact at each site where a VeloCloud Edge device is deployed
- IT Operator (or Operator)
- IT Partner (or Partner)

### Administrator

The Administrator configures, monitors, and administers the VeloCloud service operation. There are three Administrator roles:

Administrator Role	Description
Enterprise Standard Admin	Can perform all configuration and monitoring tasks.
Enterprise Superuser	Can perform the same tasks as an Enterprise Standard Admin and can also create additional users with the Enterprise Standard Admin, Enterprise MSP, and Customer Support role.
Enterprise Support	Can perform configuration review and monitoring tasks but cannot view user identifiable application statistics and can only view configuration information.

**Note** An Administrator should be thoroughly familiar with networking concepts, web applications, and requirements and procedures for the Enterprise.

### Site Contact

The **Site Contact** is responsible for VeloCloud Edge physical installation and activation with the VeloCloud service. The Site Contact is a non-IT person who has the ability to receive an email and perform the instructions in the email for Edge activation.

### Operator

The Operator can perform all of the tasks that an Administrator can perform, plus additional operator-specific tasks – such as create and manage customers, Cloud Edges, and Gateways. There are four Operator roles:

Operator Role	Description
Standard Operator	Can perform all configuration and monitoring tasks.
Superuser Operator	Can view and create additional users with the Operator roles.
Business Specialist Operator	Can create and manage customer accounts.
Customer Support Operator	Can monitor Edges and activity.

An Operator should be thoroughly familiar with networking concepts, web applications, and requirements and procedures for the Enterprise.

## Partner

The **Partner** can perform all of the tasks that an Administrator can perform, along with additional Partner specific tasks – such as creating and managing customers. There are four Partner roles:

Partner Role	Description
Standard Admin	Can perform all configuration and monitoring tasks.
Superuser	Can view and create additional users with the Partner roles.
Business Specialist	Can perform configuration and monitoring tasks but cannot view user identifiable application statistics.
Customer Support	Can perform configuration review and monitoring tasks but cannot view user identifiable application statistics and can only view configuration information.

A Partner should be thoroughly familiar with networking concepts, web applications, and requirements and procedures for the Enterprise.

## User Role Matrix

This section describes feature access according to VeloCloud user roles.

**Note** The "User Role Matrix" section is new for the 3.3 release.

### Operator-level VCO Features User Role Matrix

See the table below for Operator-level user roles that have access to the VCO features. See the list below for a definition of the symbols used in the table:

- R: Read
- W: Write (Modify/Edit)
- D: Delete
- NA: No Access

VCO Feature	Operator: Superuser Operator	Operator: Standard Operator	Partner: Business Specialist	Partner: Customer Support Operator	Super User	Standard Admin	Business Specialist	Customer Support
Monitor Customers	R	R	R	R	R	R	R	R
Manage Customers	RWD	RWD	RWD	R	RWD	RWD	RWD	R
Manage Partners	RWD	RWD	RWD	R	NA	NA	NA	NA
(Managing Edge) Software Images	RWD	RWD	R	R	*See Note	*See Note	*See Note	*See Note
System Properties	RWD	R	NA	R	NA	NA	NA	NA
Operator Events	R	R	NA	R	NA	NA	NA	NA
Operator Profiles	RWD	RWD	R	R	NA	NA	NA	NA
Operator Users	RWD	R	R	R	NA	NA	NA	NA
Gateway Pools	RWD	RW	R	R	RWD	RWD	NA	R
Gateways	RWD	RWD	R	R	RW	RW	NA	R
Gateway Diagnostic Bundle	RWD	RWD	R	R	NA	NA	NA	NA
Application Maps	RWD	RWD	R	R	NA	NA	NA	NA
CA Summary	RW	R	R	R	NA	NA	NA	NA
Orchestrator Authentication	RWD	R	NA	R	NA	NA	NA	NA
Replication	RW	R	NA	R	NA	NA	NA	NA

**Note** Operator superusers have "RWD" access to certificate related configurations and standard operators have Read-only access to certificate related configurations. These users can access the certificate related configurations at **Configure > Edges** from the navigation panel.\*

**Note** Enterprise users at all levels do not have access to the Operator-level features show in the table above.

## Partner-level VCO Features User Role Matrix

See the table below for Partner-level user roles that have access to the VCO features. See the list below for a definition of the symbols used in the table:

- R: Read
- W: Write (Modify/Edit)
- D: Delete
- NA: No Access

VCO Feature	Partner: Superuser	Partner: Standard Admin	BusinessSpecialist	CustomerSupport
MonitorCustomers	R	R	R	R
Manage Customers	RWD	RWD	RWD	R
Events	R	R	NA	R
Admins	RWD	R	NA	R
Overview	R	R	R	R
Settings	RW	R	R	R
Gateway Pools	RW	RWD	NA	R
Gateways	RW	RW	NA	R

## Enterprise-level VCO Features User Role Matrix

See the table below for Enterprise-level user roles that have access to the VCO features. See the list below for a definition of the symbols used in the table:

- R: Read
- W: Write (Modify/Edit)
- D: Delete
- NA: No Access

VCO Feature	Enterprise: Super User	Enterprise: Standard Admin	Customer Support	Read Only
<b>Monitor &gt; Edges</b>	R	R	R	R
<b>Monitor &gt; Network Services</b>	R	R	R	R
<b>Monitor &gt; Routing</b>	R	R	R	NA
<b>Monitor &gt; Alerts</b>	R	R	R	NA
<b>Monitor &gt; Events</b>	R	R	R	NA

VCO Feature	Enterprise: Super User	Enterprise: Standard Admin	Customer Support	Read Only
<b>Configure &gt; Edges</b>	RWD	RWD	R	NA
<b>Configure &gt; Profiles</b>	RWD	RWD	R	NA
<b>Configure &gt; Networks</b>	RWD	RWD	R	NA
<b>Configure &gt; Segments</b>	RWD	RWD	R	NA
Configure > Overlay Flow Control	RWD	RWD	R	NA
<b>Configure &gt; Network Services</b>	RWD	RWD	R	NA
<b>Configure &gt; Alerts &amp; Notifications</b>	RW	RW	R	NA
<b>Test &amp; Troubleshoot &gt; Remote Diagnostics</b>	RW	RW	RW	NA
<b>Test &amp; Troubleshoot &gt; Remote Actions</b>	RW	RW	RW	NA
<b>Test &amp; Troubleshoot &gt; Packet Capture</b>	RW	RW	RW	NA
<b>Administration &gt; System Settings</b>	RW	RW	RW	NA
<b>Administration &gt; Administrators</b>	RW	R	R	NA

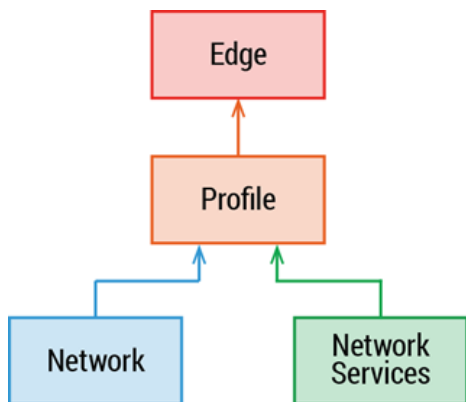
**Note** Operator-level users have complete access the VCO features shown in the preceding table.

## Key Concepts

This section describes key concepts to understand when using VeloCloud.

### Configurations

The VeloCloud service has four core configurations that have a hierarchical relationship. These configurations are created and values are entered in the VeloCloud Orchestrator.

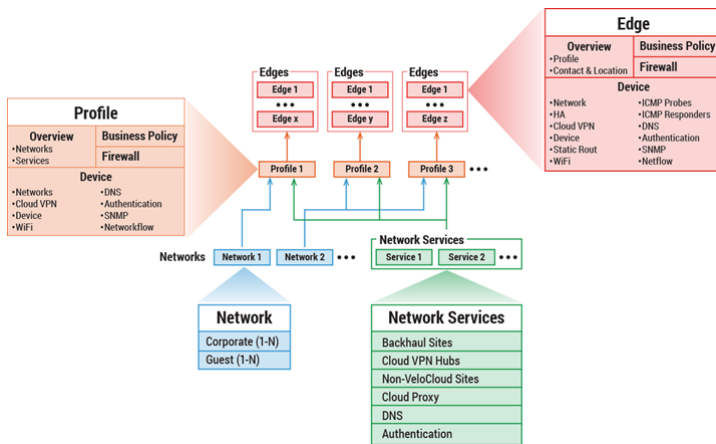




The following table provides an overview of the four configurations.

Configuration	Description
Network	Defines basic network configurations, such as addressing and VLANs. Networks can be designated as Corporate or Guest and there can be multiple definitions of each.
Network Services	Define several common services used by the VeloCloud Service, such as BackHaul Sites, Cloud VPN Hubs, Non-VeloCloud Sites, Cloud Proxy Services, DNS services, and Authentication Services.
Profile	Defines a template configuration that can be applied to multiple Edges. A Profile is configured by selecting a Network and Network Services. A profile can be applied to one or more Edge models and defines the settings for the LAN, Internet, Wireless LAN, and WAN Edge Interfaces. Profiles can also provide settings for Wi-Fi Radio, SNMP, Netflow, Business Policies and Firewall configuration.
Edge	Configurations provide a complete group of settings that can be downloaded to an Edge device. The Edge configuration is a composite of settings from a selected Profile, a selected Network, and Network Services. An Edge configuration also override settings or add ordered policies to those defined in the Profile, Network, and Network Services.

The following figure below shows a more detailed overview of the relationships between multiple Edges, Profiles, Networks, and Network Services.



Note that a single Profile can be assigned to multiple Edges. An individual Network configuration can be used in more than one Profile. Network Services configurations are used in all Profiles.

The preceding figure also gives an expanded view of the configuration settings of an Edge, Profile, Network, and Network Services, which are described in the following sections. The following sections also provide additional details for the four core configurations.

## Networks

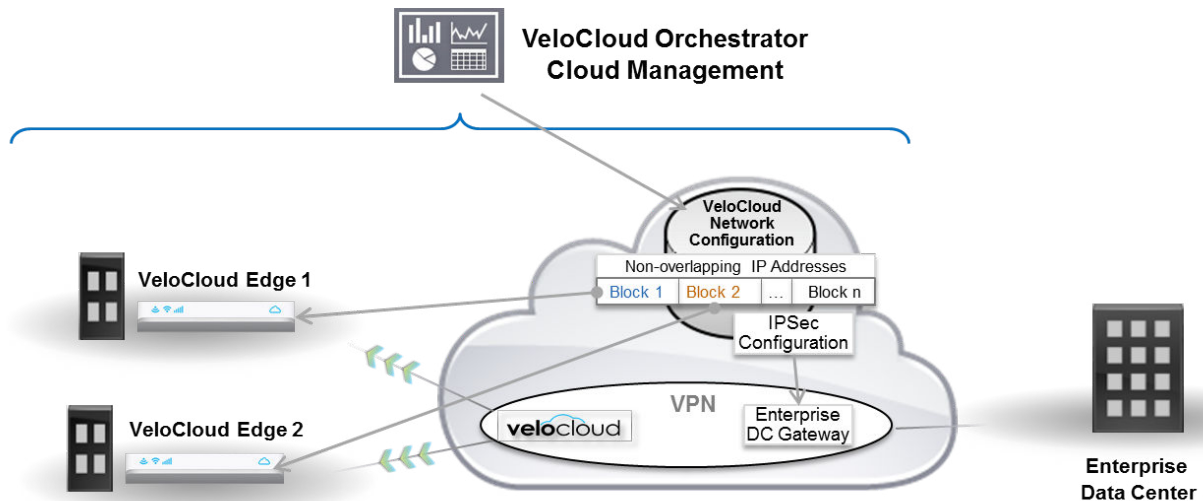
Networks are standard configurations that define network address spaces and VLAN assignments for Edges. Networks configure two network types:

- Corporate (or trusted networks)
- Guest (or untrusted networks)

Multiple Corporate and Guest Networks can be defined. VLANs can be assigned to both Corporate and Guest Networks.

- Corporate Networks can be configured with either Overlapping Addresses or Non-overlapping Addresses. With overlapping addresses, all Edges using the Network have the same address space. Overlapping addresses are associated with non-VPN configurations.
- Guest networks always use overlapping addresses.

With **non-overlapping** addresses, an address space is divided into blocks of an equal number of addresses. Non-overlapping addresses are associated with VPN configurations. The address blocks are assigned to Edges that use the Network so that each Edge has a unique set of addresses. Non-overlapping addresses are required for **Edge-to-Edge** and **Edge -to-** Non-VeloCloud Site VPN communication. The VeloCloud configuration creates the information necessary to access an Enterprise Data Center Gateway for VPN access. The following diagram shows how unique IP address blocks from a Network configuration are assigned to VeloCloud Edges. It also shows how IPSec configuration is generated by the VeloCloud Orchestrator. An administrator for the Enterprise Data Center Gateway uses the IPSec configuration information generated during Non-VeloCloud Site VPN configuration to configure the VPN tunnel to the Non-VeloCloud Site.



**Note** When using non-overlapping addressing, the VeloCloud Orchestrator automatically allocates blocks of addresses based on the maximum number of Edges you predict will use the Network configuration.

## Network Services

Network Services in VeloCloud Orchestrator allows you to define your Enterprise Network Services. These definitions can be used across all Profiles. This includes services for Authentication, Cloud Proxy, Non-VeloCloud Sites, and DNS. The possible services are defined in Network Services but are not used unless they are assigned in a Profile.

## Profiles

Profiles define a standard configuration for one or more VeloCloud Edges. A profile is a named configuration that defines a list of VLANs, Cloud VPN settings, Interface Settings (wired and wireless), and Network Services (such as DNS Settings, Authentication Settings, Cloud Proxy Settings, and VPN connections to Non-VeloCloud Sites).

Profiles provide Cloud VPN settings for Edges configured for VPN. The Cloud VPN Settings can enable/disable Edge-to-Edge and Edge-to- Non-VeloCloud Site VPN connections.

Profiles can also define rules and configuration for the VeloCloud Business Policy and Firewall settings.

## Edges

The Edge configuration includes the assignment of a Profile, from which most of the Edge configuration is derived.

Most of the settings that are defined in a Profile, Network, or Network Services can be used without modification in an Edge configuration. However, overrides or ordered policy additions can be configured for several of the Edge configuration elements to tailor an Edge for a specific scenario. This includes settings for Interfaces, Wi-Fi Radio Settings, DNS, Authentication, Business Policy, and Firewall.

Additions can also be made to an Edge configuration to augment settings not present in Profile or Network configuration. This includes Subnet Addressing, Static Route settings, and Inbound Firewall Rules (for Port Forwarding and 1:1 NAT).

## Orchestrator Configuration Workflow

VeloCloud supports multiple configuration scenarios. Here are some common scenarios:

Scenario	Description
SaaS	: Used for Edges that do not require VPN connections between Edges, to a Non-VeloCloud Site, or to a VeloCloud Site. The workflow assumes the addressing for the Corporate Network uses overlapping addressing.
Non-VeloCloud Site via VPN	Used for Edges that require a VPN connection to a Non-VeloCloud Site such as Amazon Web Services, Zscaler, Cisco ISR, or ASR 1000 Series. This workflow assumes the addressing for the Corporate Network uses non-overlapping addressing and that the Non-VeloCloud Sites are specified in the profile.
VeloCloud SiteVPN	Used for Edges that require VPN connections to a VeloCloud Site such as an Edge Hub or a Cloud VPN Hub. This workflow assumes the addressing for the Corporate Network uses non-overlapping addressing and that the VeloCloud Sites are specified in the profile.

For each scenario, there are four major steps for configuration in the VeloCloud Orchestrator:

**Step 1:** Network

**Step 2:** Network Services

**Step 3:** Profile

## Step 4: Edge

The following table provides a high-level outline of the steps required for a Quick Start configuration for each of the workflows. For Quick Start Configurations, preconfigured Network, Network Services, and Profile configurations are used. VPN configurations also require some modification of the existing VPN Profile and creating the configuration of a VeloCloud or Non-VeloCloud Site. The final step is to create a new Edge and activate it. Additional details (including screen captures) can be found in the [Activate Edges](#) section.

Quick Start Configuration Steps	SaaS	Non-VeloCloud Site Site VPN	VeloCloud Site VPN
Step 1: Network	Select Quick Start Internet Network	Select Quick Start VPN Network	Select Quick Start VPN Network
Step 2: Network Service	Use pre-configured Network Services	Use pre-configured Network Services	Use pre-configured Network Services
Step 3: Profile	Select Quick Start Internet Profile	Select Quick Start VPN Profile Enable Cloud VPN - Configure Non-VeloCloud Sites	Select Quick Start VPN Profile Enable Cloud VPN- Configure VeloCloud Sites
Step 4: Edge	Add New Edge and Activate Edge	Add New Edge and Activate Edge	Add New Edge and Activate Edge

## Supported Modems

This section describes how to get a list of supported modems.

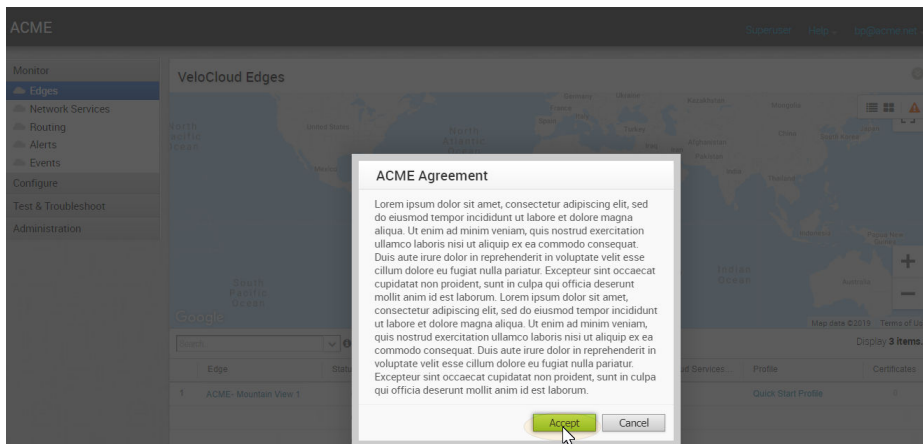
For a detailed list of our supported modems, go to <http://velocloud.com/get-started/supported-modems>

# User Agreement (VCO Login Screen)

# 4

An Enterprise Superuser or Partner Superuser might see a user agreement upon logging into the VCO. The user must accept the agreement before gaining access to the VCO. If the user does not accept the agreement, he or she will be automatically logged out of the VCO.

**Note** The "User Agreement (VCO Login Screen)" section is new for the 3.3 release.



# Log in to VCO Using SSO for Enterprise User

# 5

Describes how to log in to VeloCloud Orchestrator (VCO) using Single Sign On (SSO) as an Enterprise user.

To login into VCO using SSO as an Enterprise user:

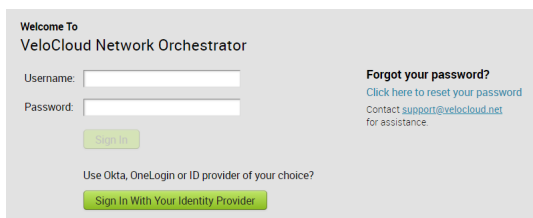
## Prerequisites

- Ensure you have configured SSO authentication in VCO. For more information, see [Configure Single Sign On for Enterprise 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 VCO application as Enterprise user.

The **VeloCloud Network Orchestrator** screen appears.



Welcome To  
VeloCloud Network Orchestrator

Username:

Password:

[Forgot your password?](#)  
Click here to reset your password  
Contact [support@velocloud.net](mailto:support@velocloud.net)  
for assistance.

Use Okta, OneLogin or ID provider of your choice?

- 2 Click **Sign In With Your Identity Provider**.
- 3 In the **Enter your Organization Domain** text box, enter the domain name used for the SSO configuration and click **Sign In**.

The IDP configured for SSO will authenticate the user and redirect the user to the configured VCO URL.

---

**Note** Once the users log in to the VCO using SSO, they will not be allowed to login again as native users.

---

# Monitor the VCO

# 6

The VeloCloud Orchestrator provides monitoring functionality that enables you to observe various performance and operational characteristics of VeloCloud Edges. Monitoring functionality is accessible in **Monitor** area of the navigation panel.

This chapter includes the following topics:

- [Monitor Navigation Panel](#)
- [Network Overview](#)
- [Monitor Edges](#)
- [Monitor Network Services](#)
- [Monitor Routing](#)
- [Monitor Alerts](#)
- [Monitor Events](#)

## Monitor Navigation Panel

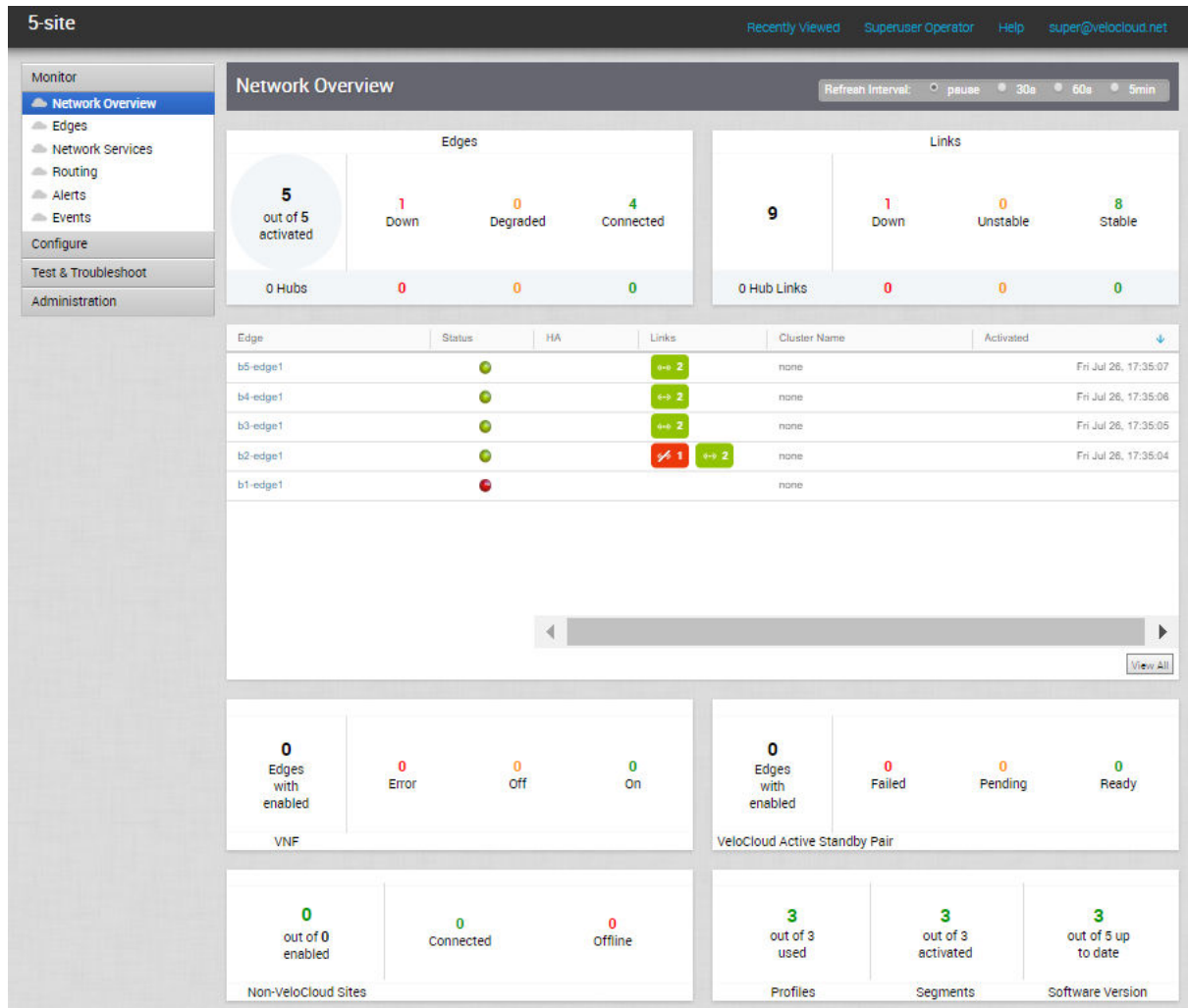
The following monitoring capabilities are displayed under **Monitor** in the navigation panel.

- [Network Overview](#)
- [Monitor Edges](#)
- [Monitor Network Services](#)
- [Monitor Routing](#)
- [Monitor Alerts](#)
- [Monitor Events](#)

## Network Overview

The Network Overview feature helps to monitor networks by checking the Edge and Link (activated Edge) status summary. Clicking **Monitor > Network Overview** in the navigation panel opens the **Network Overview** screen, which provides a visual summary about the enterprises

running VeloCloud edge devices, Non-VeloCloud sites, profiles, segments, software versions, and their system configuration time and run time statuses.



The following table describes the connection status types and definitions for the Edge, Edge Hub, Link, and Hub Link:

Color	Meaning
Green	Connected
Amber	Degraded
Red	Down

The **Network Overview** screen presents the overall summary information about a network in three dashboard sections:

- VeloCloud Edge statistics - Includes the following information about the Edges and Links:
  - Total number of Edges



- Total number of Edge Hubs
- Total number of Links
- Total number of Hub Links
- Count of Edges/Edge Hubs (Connected, Degraded, and Down)
- Count of Link/Hub Links (Stable, Unstable, and Down)
- Summary dashboard table - Includes a table that displays top ten Edges, or Edge Hubs, or Links, or Hub Links sorted by last contact time, based on the selected filter criteria in the VeloCloud Edge statistics section.
- Non-Edge statistics - Includes the following non-edge related information:
  - Total number of Virtual Network Functions (VNFs)-enabled Edges
  - Count of VNFs-enabled Edges (Error, On, and Off)
  - Total number of VeloCloud Active Standby Pair-enabled Edges
  - Count of VeloCloud Active Standby Pair-enabled Edges (Failed, Pending, and Ready)
  - Total number of enabled Non-VeloCloud Sites (NVS)
  - Count of NVS (Connected and Offline)
  - Count of used Profiles out of the total number of Profiles configured for the Enterprise.
  - Count of activated Segments out of the total number of Segments configured for the Enterprise.
  - Count of Edges with up-to-date Software version out of the total number of Edges configured for the Enterprise.

---

**Note** The minimum supported edge version is 2.4.0. You can change the target edge version against which the edges will be compared by using the system property `product.edge.version.minimumSupported`.

---

You can also get detailed information on a specific item in the **Network Overview** screen by clicking the link on the respective item or metric. For example, clicking the **Edge** link in the summary dashboard table takes you to the Edge detail dashboard for the selected Edge.

You can configure the refresh time interval for the information displayed in the Network Overview dashboard screen to one of the following options:

- **pause**
- **30s**
- **60s**
- **5min**

## Monitor Edges

By clicking **Edges** under **Monitor** in the navigation panel, you can monitor your Edge WAN links and get usage data via network sources and traffic destinations.

The **Edges** monitoring screen includes the following tabs (with the **Overview** tab as the initial display screen):

- [Overview Tab](#)
- [QoE Tab](#)
- [Transport Tab](#)
- [Applications Tab](#)
- [Sources Tab](#)
- [Destinations Tab](#)
- [Business Priority Tab](#)

The following sections describe the tab pages listed above that can be accessed via **Monitor > Edges**.

### Enterprise Global View

Clicking **Monitor > Edges** in the navigation panel opens the VeloCloud Edge Enterprise Global View screen, which provides a visual overview of all the branches and their connection status.

The following list describes the Edge connection status types and definitions:

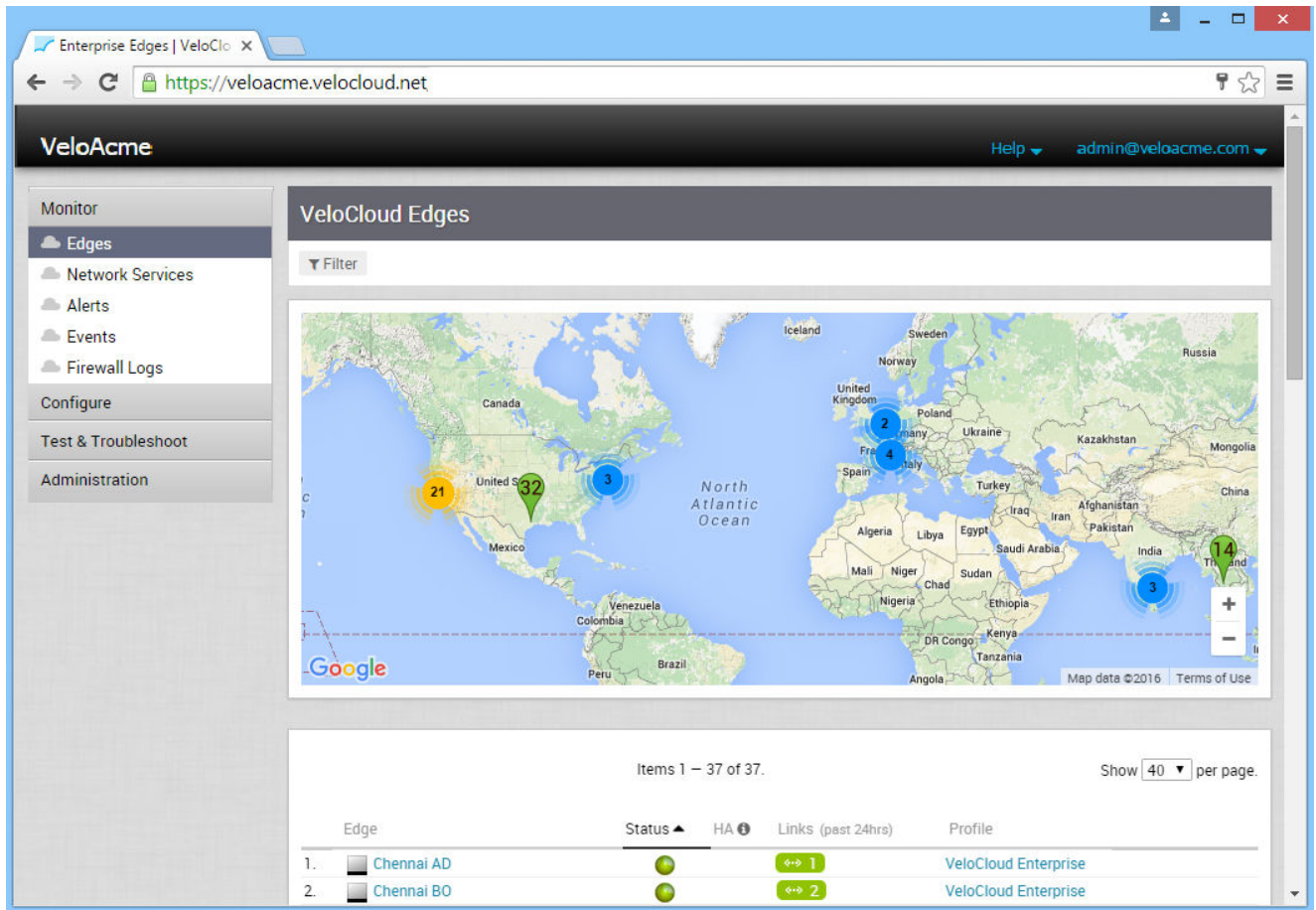
Color	Meaning
Green	Connected
Amber	Degraded
Blue	Never Activated
Red	Offline

The numbers on the map represent the number of Edges in that location as shown in the image below. Click the number(s) on the map to open a pop-up that displays the name of the Edge and its location.

---

**Note** You can **Filter** your map view by Name, Serial Number, IP Address, Status, Software Version, Software Build, Profile, or Operator Profile.

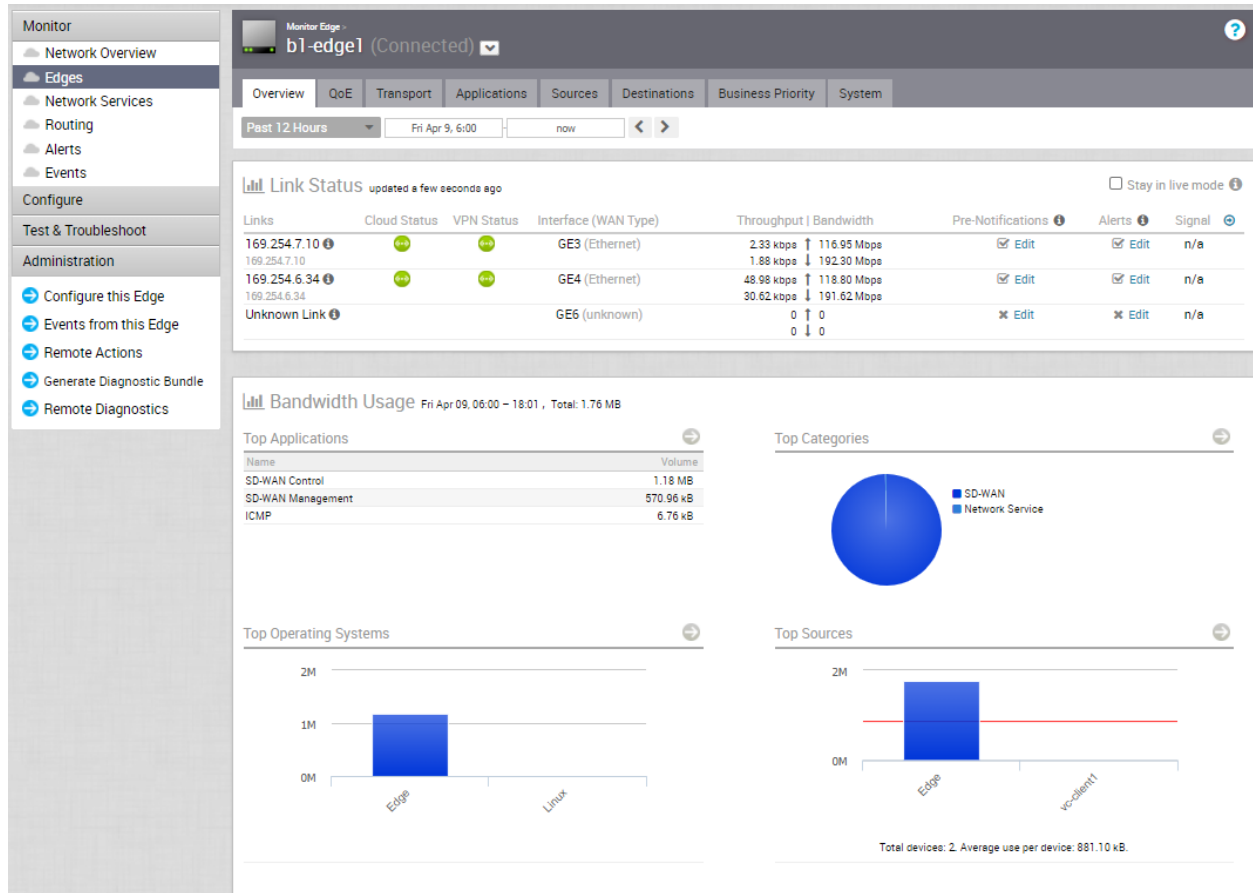
---



## Overview Tab

The Overview tab of an Edge in the monitoring dashboard displays the details of WAN links along with bandwidth consumption and network usage.

The **Overview** tab displays the details of links with status and the bandwidth consumption.



You can choose to view the Edge information live by selecting the **Stay in live mode** checkbox. When this mode is enabled, live monitoring of the Edge happens and the data in the page is updated whenever there is a change. The live mode is automatically moved to offline mode after a period of time to reduce the network load.

The Links Status section displays the following details:

Option	Description
Links	The Interface and WAN links of the selected Edge
Cloud Status	Connectivity status of the Link to the Gateway.
VPN Status	Connectivity status of the Link IPsec tunnel to the Gateway.
Interface (WAN Type)	The Interface connected to the Link.
Throughput	Total bytes in a given direction divided by the total time. The total time is the periodicity of statistics uploaded from the Edge. By default, the periodicity in the Orchestrator is 5 minutes.
Bandwidth	The maximum rate of data transfer across a given path. Displays both the upstream and downstream bandwidth details.

Option	Description
Pre-Notifications	Allows to enable or disable the alerts sent to the Operator. Click <b>Edit</b> to modify the notification settings.
Alerts	Allows to enable or disable the alerts sent to the Enterprise Customer. Click <b>Edit</b> to modify the notification settings.
Signal	Information on signal strength.
Latency	Time taken for a packet to get across the network, from source to destination. Displays both the upstream and downstream Latency details.
Jitter	Variation in the delay of received packets caused by network congestion or route changes. Displays both the upstream and downstream Jitter details.
Packet loss	Packet loss happens when one or more packets fail to reach the intended destination. A lost packet is calculated when a path sequence number is missed and does not arrive within the re-sequencing window. A “very late” packet is counted as a lost packet.

The **Bandwidth Usage** section displays graphical representation of bandwidth and network usage of the following: Applications, Categories, Operating Systems, and Sources of the Edges. Click the Arrow in each panel to navigate to the corresponding tab and view more details.

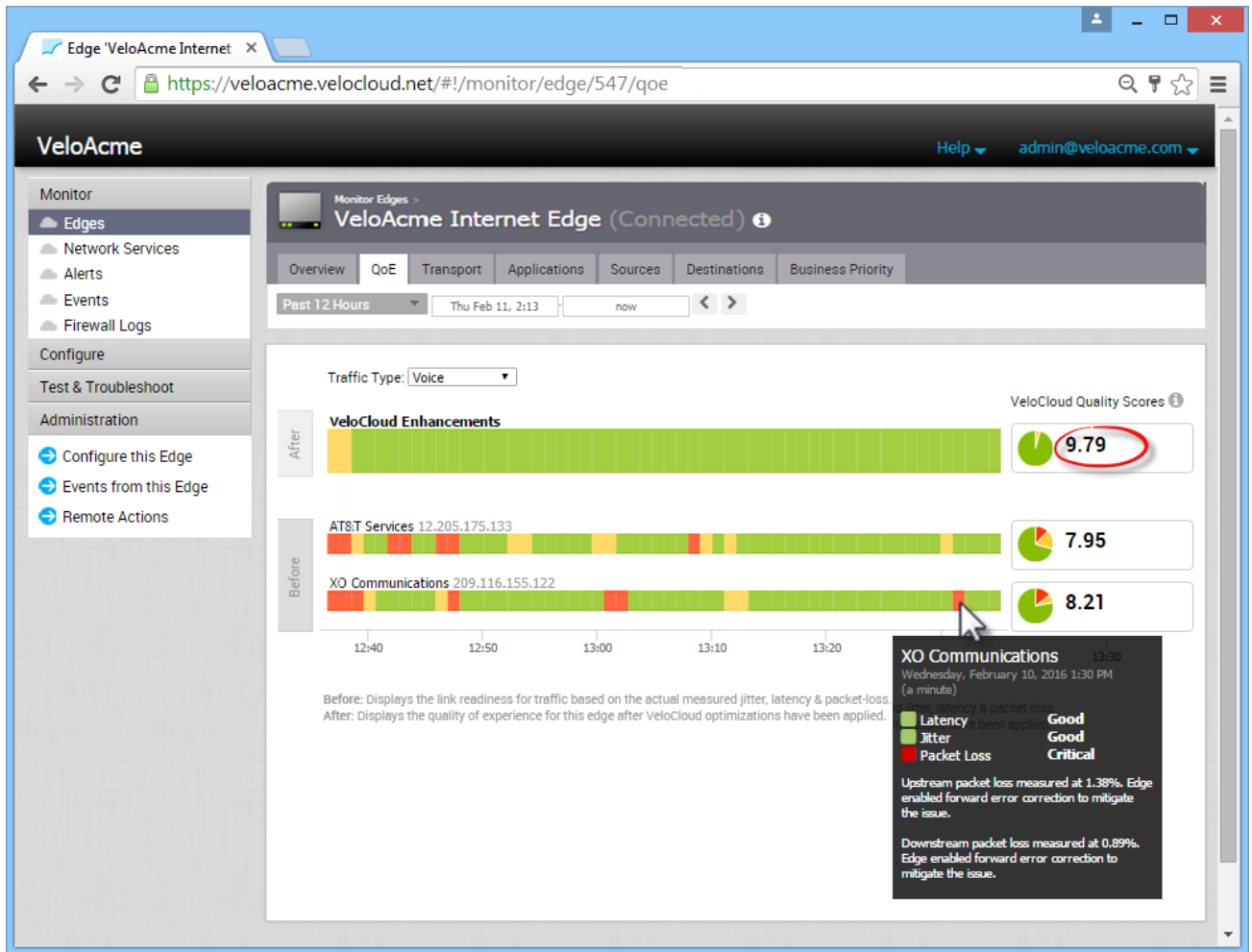
Hover the mouse on the graphs to view more details.

## QoE Tab

The VeloCloud **Quality of Experience (QoE)** tab shows the VeloCloud Quality Score (VQS) for different applications. The VQS rates an application's quality of experience that a network can deliver for a period of time. See sections below for more information.

## Traffic Type

There are three different traffic types that you can monitor (Voice, Video, and Transactional) in the **QoE** tab. You can hover over a WAN network link, or the aggregate link provided by the VeloCloud to display a summary of Latency, Jitter, and Packet Loss (see image below).



## VeloCloud Quality Score

The VeloCloud Quality Score (VQS) rates an application's quality of experience that a network can deliver for a given time frame. Some examples of applications are: video, voice, and transactional. QoE rating options are shown in the table below.

Rating Color	Rating Option	Definition
Green	Good	All metrics are better than the objective thresholds. Application SLA met/exceeded.
Yellow	Fair	Some or all metrics are between the objective and maximum values. Application SLA is partially met.
Red	Poor	Some or all metrics have reached or exceeded the maximum value. Application SLA is not met.

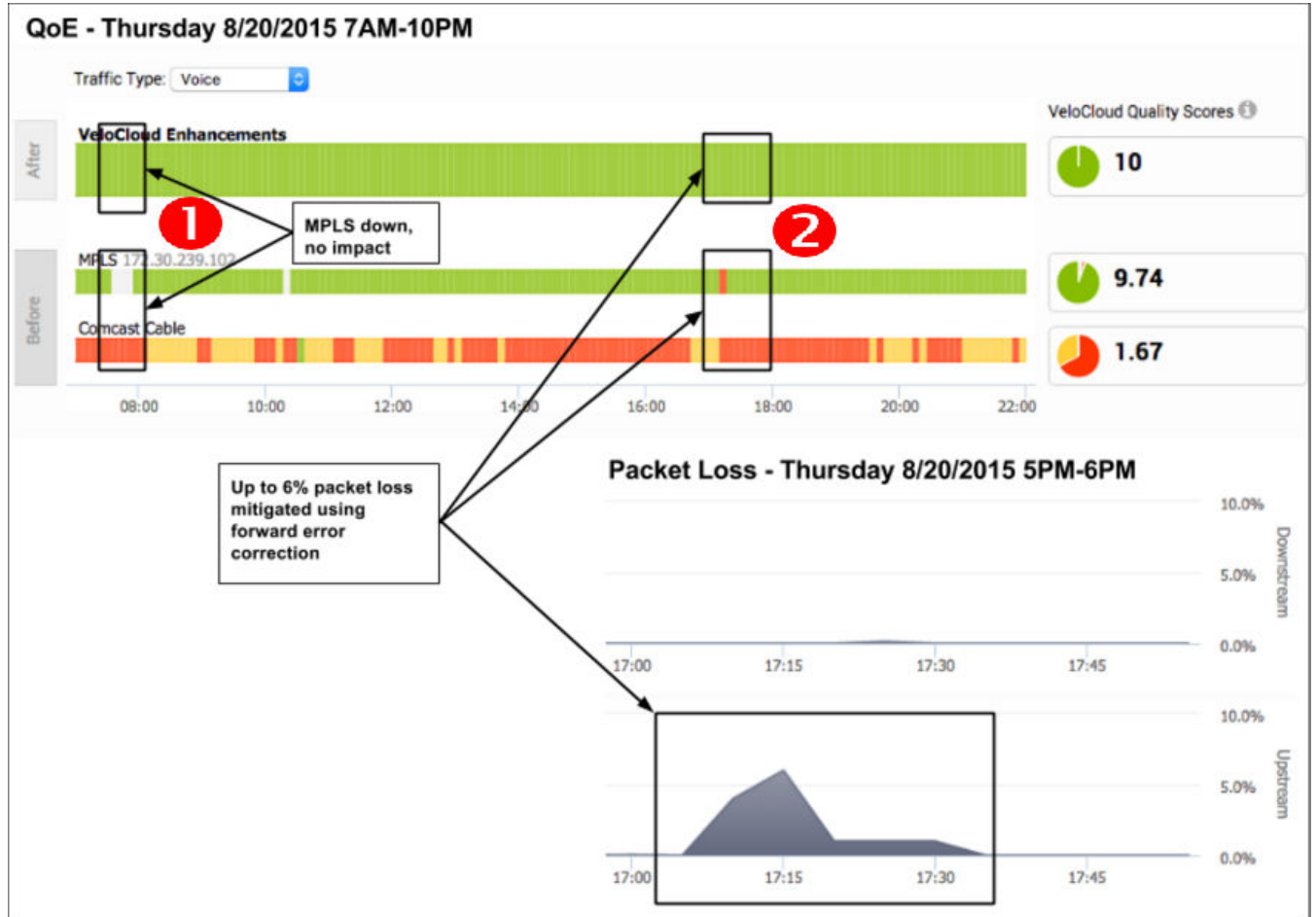
## QoE Example

The two QoE example images below show three before and after voice traffic scenario problems and how VeloCloud solved them. See the table below for more information. (The red numbers in the images below represent the scenario numbers in the table below).

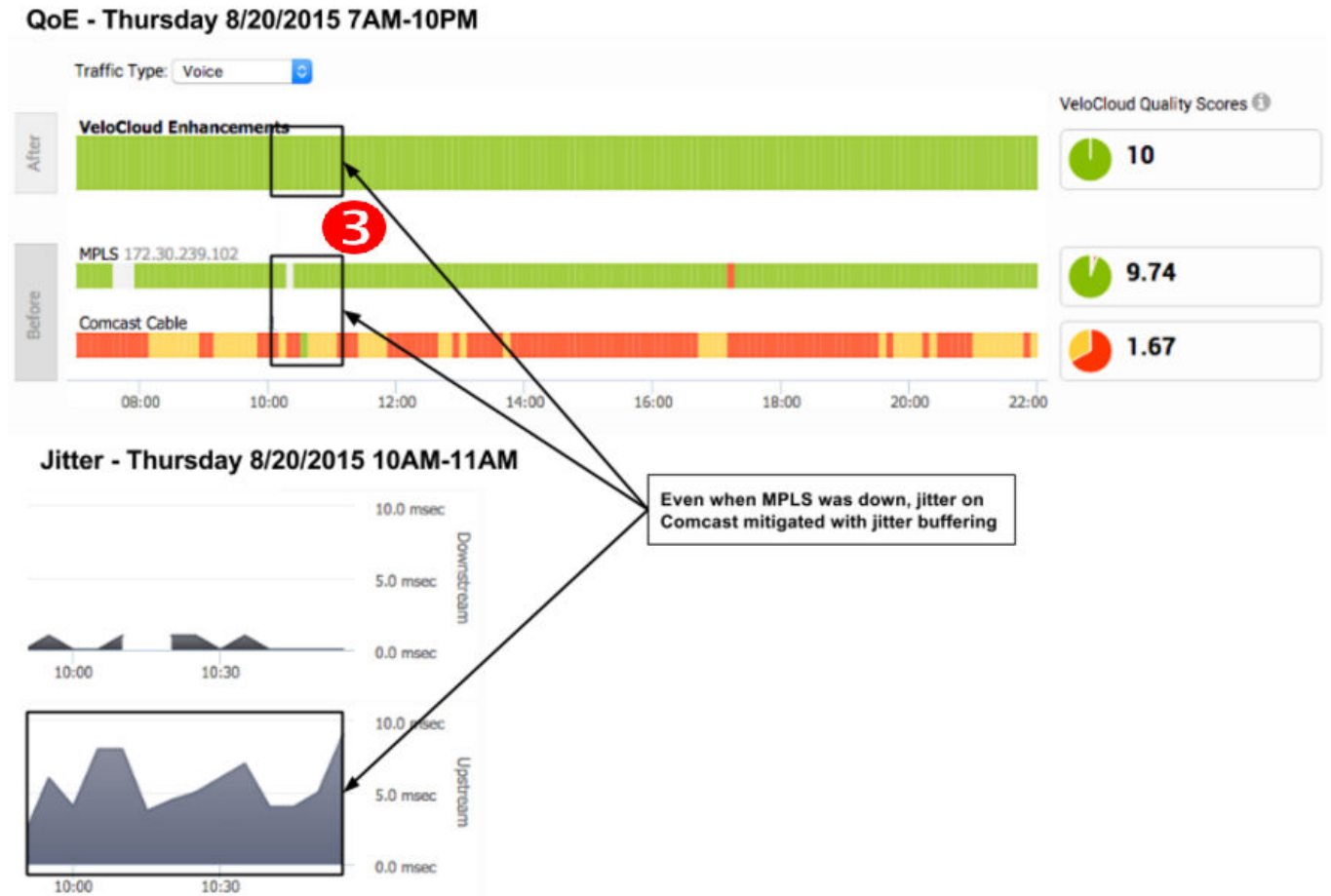
## QoE Example Table

Scenario	Issue	VeloCloud Solution
1	MPLS is down	Link steering
2	Packet loss	Forward error correction
3	MPLS is down; Jitter on Comcast	Link steering and jitter buffering

### Scenario 1 and 2: Link Steering and Forward Error Correction Solution Example



### Scenario 3: Link Steering and Jitter Buffering Solution Example



### Transport Tab

The Edge **Transport** tab provides an overview of the bandwidth used across all of the WAN links. You can hover over the line graph and view Sent and Received data in a pop-up window.

For any point in time, you can view which Link or Transport Group was used for the traffic and how much data was sent. See the sections below for a description of the major areas of the **Transport** tab.





## Links

When you click the **Transport** tab, **Links** is the default display screen (as shown in the image above). The **Links** screen displays Sent and Received data for your links. Any links associated with an Edge are displayed in a numbered list at the bottom of the screen under the Link column, along with their Interface (WAN Type) and Total Bytes. See image above.

The **Links** screen appears:

- Status for Cloud and VPN ( **green**: connected, **red**: disabled, **gray**: unavailable)
- Link Info (you can access this pop-up window by clicking the down arrow next to **Interface WAN Type**)
- Applications (click the gray arrow underneath the **Application** column)

**Note** You can also access the **Links** screen at anytime by clicking the **Links** button.

## Links Stats Menu

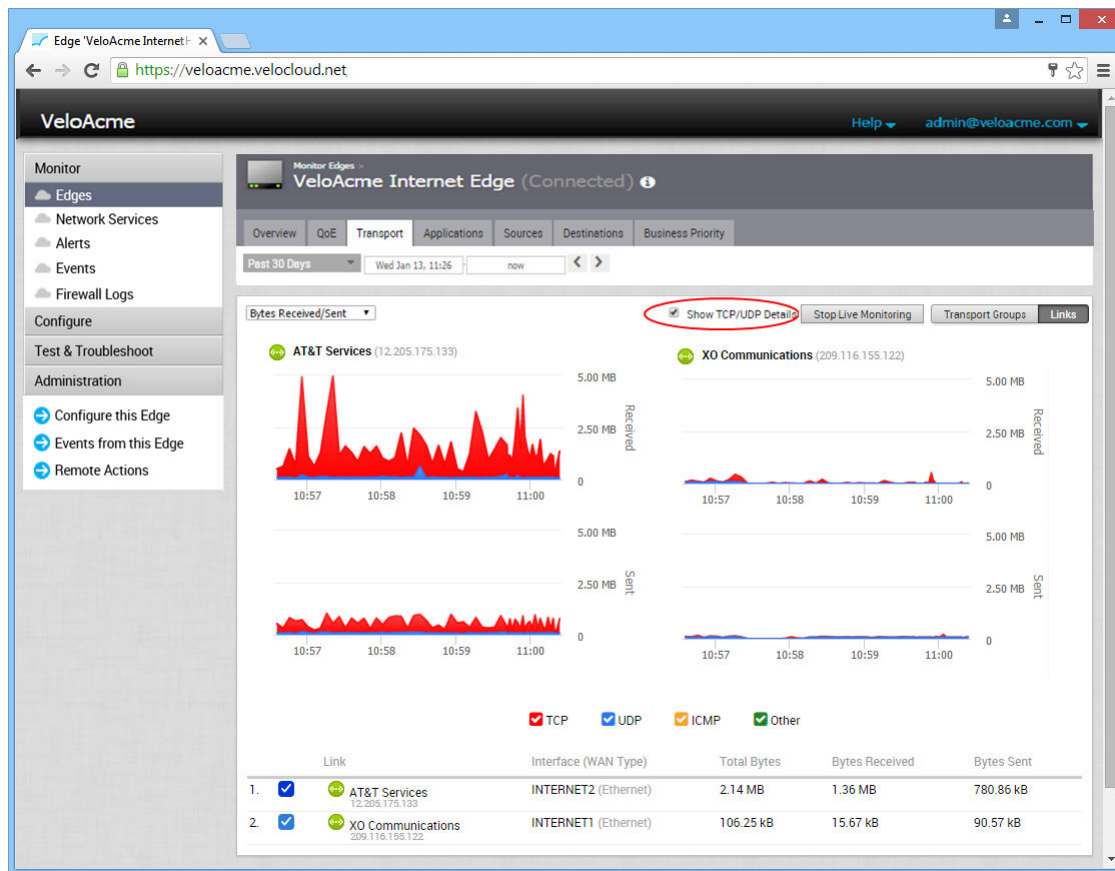
The **Links Stats** menu is located next to the Scale Y-Axis checkbox at the top left side of the **Transport** tab screen (as shown in the image above). Descriptions for the options listed in the **Links Stats** drop-down menu are described in the following table.

Link Stat Item	Definition
Bandwidth	This parameter denotes the desired bandwidth allocation in Mbps for each flow. Based on these parameters, the total capacity is allocated in proportion to the bandwidth values of various flows.
Jitter	Jitter is calculated using the RFC 3550 Formula for calculating jitter that is used by RTP.
Latency	For each packet, the latency is measured by subtracting the network send time (packet is time stamped immediately before being sent) from the network receive time (packet is time stamped immediately after being received).
Packet Loss	A lost packet is calculated when a path sequence number is missed and doesn't arrive within the re-sequencing window. A "very late" packet is counted as a lost packet in this regard.

## Live Monitoring

Live monitoring is useful for conducting active testing and calculating Average Throughput. It is also beneficial for troubleshooting security compliance and for seeing how traffic policies are being leveraged in real time.

To monitor live traffic for Links and Transport Groups click the **Start Live Monitoring** button. When the **Live Monitoring** screen appears, select the **Show TCP/UDP Details** checkbox to view protocol level link usage details.



## Transport Groups

Transport Groups are links grouped into one of the following categories:

- Public Wired
- Private Wired
- Public Wireless

Transport Groups enable box-by-box configuration and business policy abstraction. A single plan can be applied across different hardware agnostic types. When you click the **Transport Groups** button, the above items are displayed in a numbered list in the **Transport Group** area at the bottom of the **Transport** screen.

You can also click the **Transport Group** link to view the data for that group. See the section below (*Viewing Links in a Transport Group*) for information about the **Transport Groups** dialog box.

### View Links in a Transport Group

In addition to viewing Transport Group data (within the line graph), you can also view the specific links in your Transport Group.

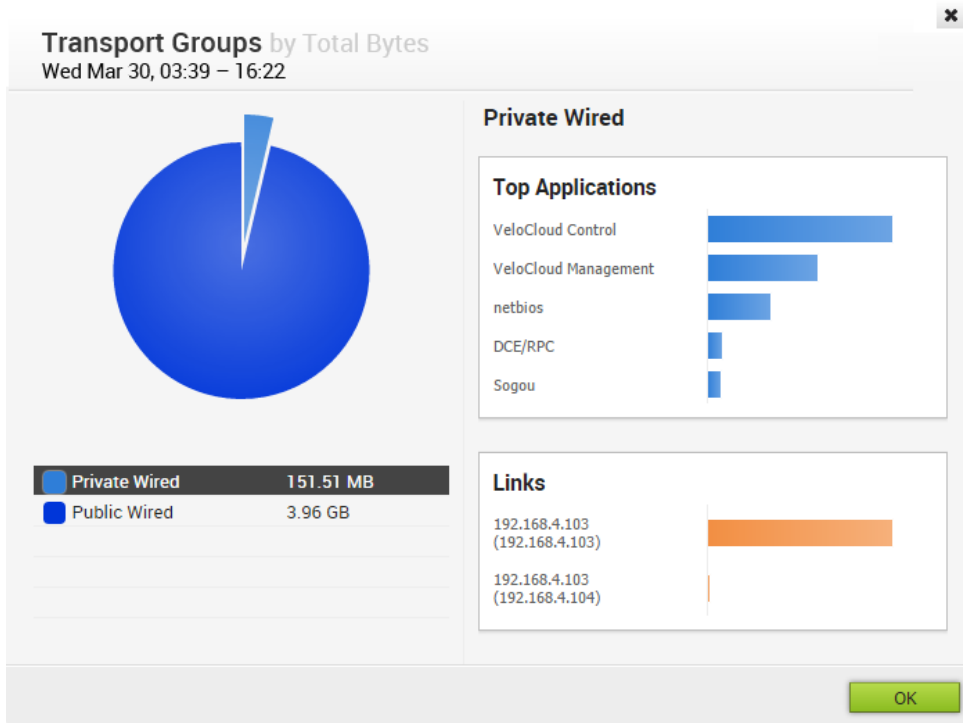
To view links in a Transport Group:

- 1 Click the **Transport Groups** button.

Transport Groups are displayed in a numbered list at the bottom of the **Transport** tab.

- 2 Click a **Transport Group** link (Public Wired, Private Wired, or Public Wireless).

The **Transport Groups** dialog box appears.



- Click a Transport Group from the Pie chart to display the top applications and links within a Transport Group. (You can also toggle between Transport Groups by clicking the Transport Group categories displayed below the Pie chart).
- Click **OK** to exit the dialog box.

## Applications Tab

The Edge **Applications** tab displays network usage information about your applications or your application categories. The following section provide information about the **Applications** and **Categories** areas.

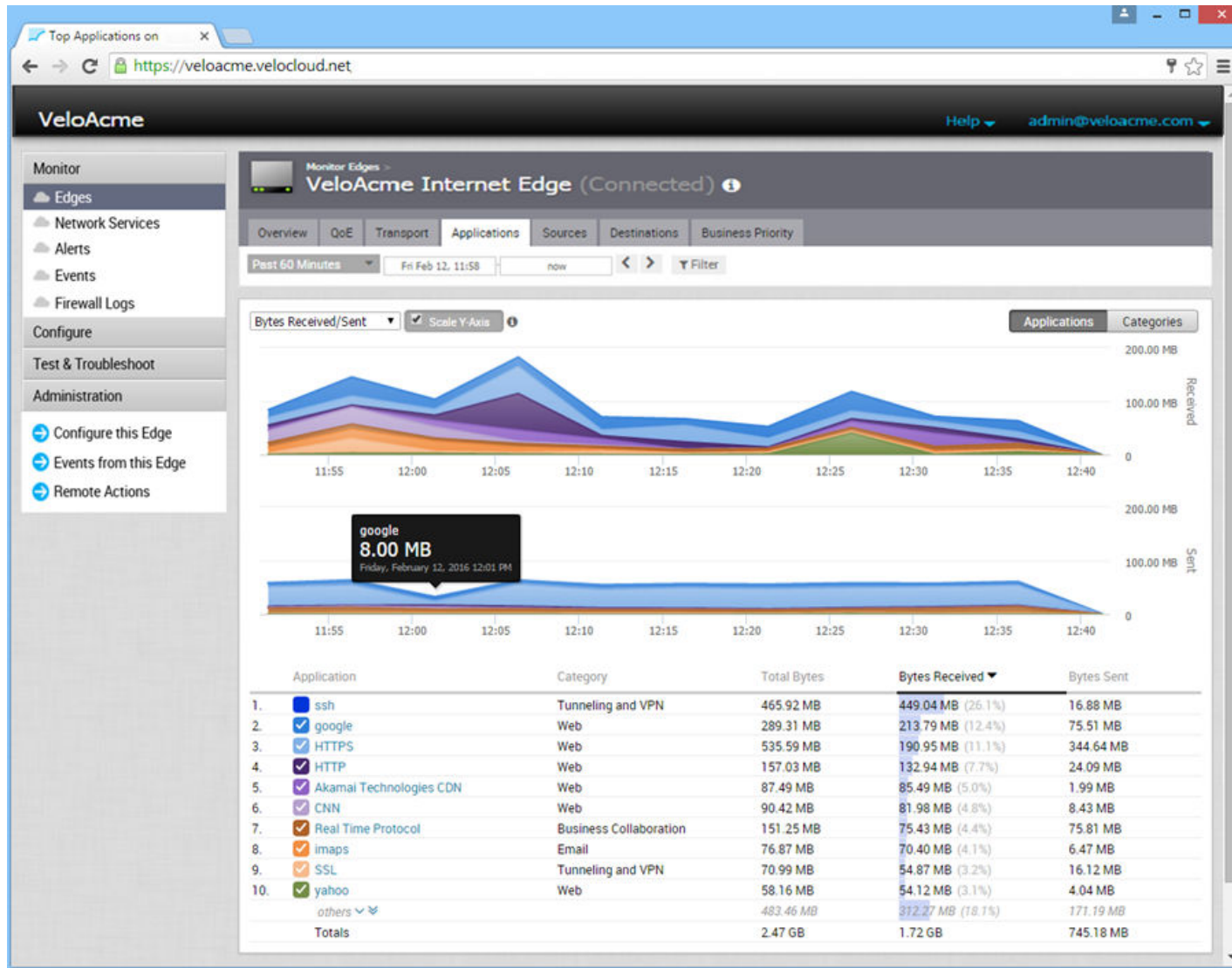
### Network Usage

Network usage data is displayed as one or two graphs (depending upon the type of data you choose) with an option to scale the Y-axis. You can hover over a segment of the graph to display network usage data for that segment. You can also choose which type of data is displayed from the **Data** drop-down menu (Bytes Received/Sent, Total Bytes, Total Packets, or Packets Received/Sent).

**Note** Network usage data for the **Applications** tab is displayed over a historical period of time.

### Top Applications

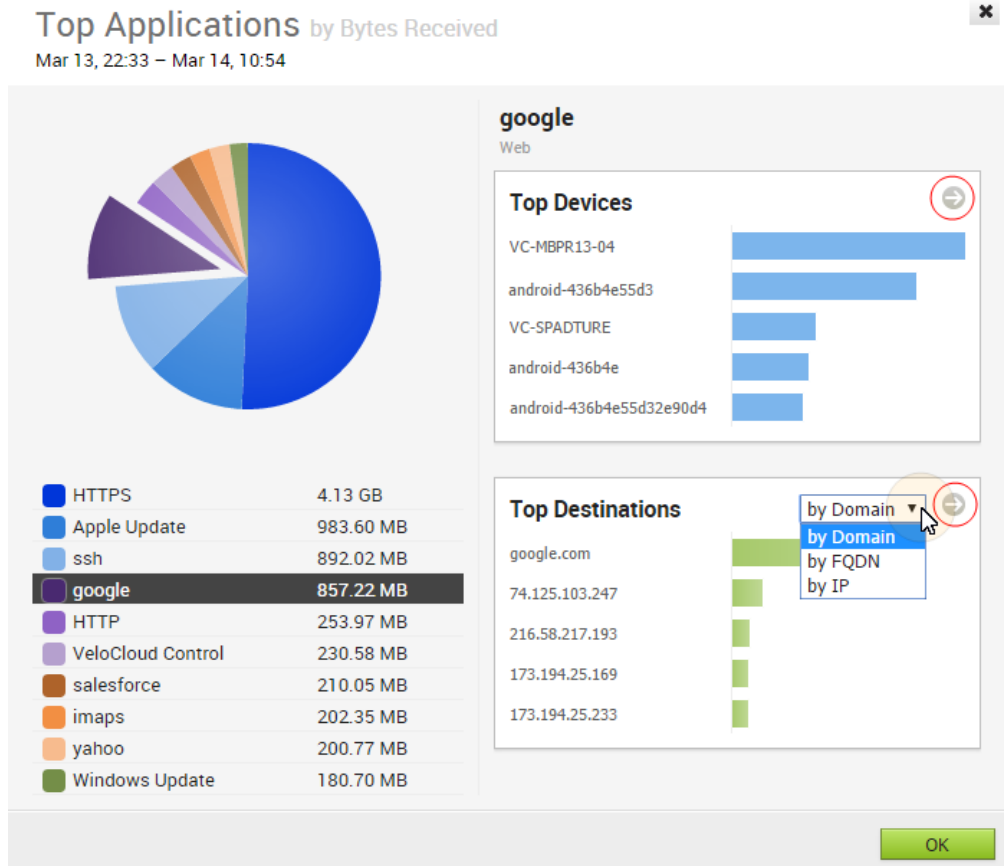
When you click the **Applications** button (located on the upper, right side of the screen), a list of your applications display at the bottom of the screen (as shown in the image below) in the **Applications** column.



To display specific application data in the graphs, select or unselect the checkboxes next to the applications in the **Applications** column. You can also click an application in the **Applications** column to open a dialog box, which displays all applications in a Pie chart. (See image below).

In the **Top Applications** dialog box (as shown in the image below), you can:

- Click an application name (or its color-coded slice of the Pie chart) to view its Transport Groups, Top Operating Systems, and Top Destinations.
- Click the arrow next to the **Top Devices** area to open the **Sources** tab.
- Choose an option from the drop-down menu in the **Top Destinations** section (by Domain, by FQDN, or by IP).
- Click the arrow (top, right corner) of the **Top Destinations** area to open the **Destinations** tab.



## Top Categories

When you click the **Categories** button, two **Category** columns display at the bottom of the screen. The first **Category** column lists your top categories. Click a category from this column to open the **Top Categories** dialog box.

The **Top Categories** dialog box includes similar features and functionality as the **Top Applications** dialog box with a couple of exceptions, instead of Transport Groups, the **Top Categories** dialog displays Top Applications in the top, right area of the dialog. Also, when you click the arrow in the **Top Applications** area, the **Applications** tab opens displaying usage data for all the applications in that category.

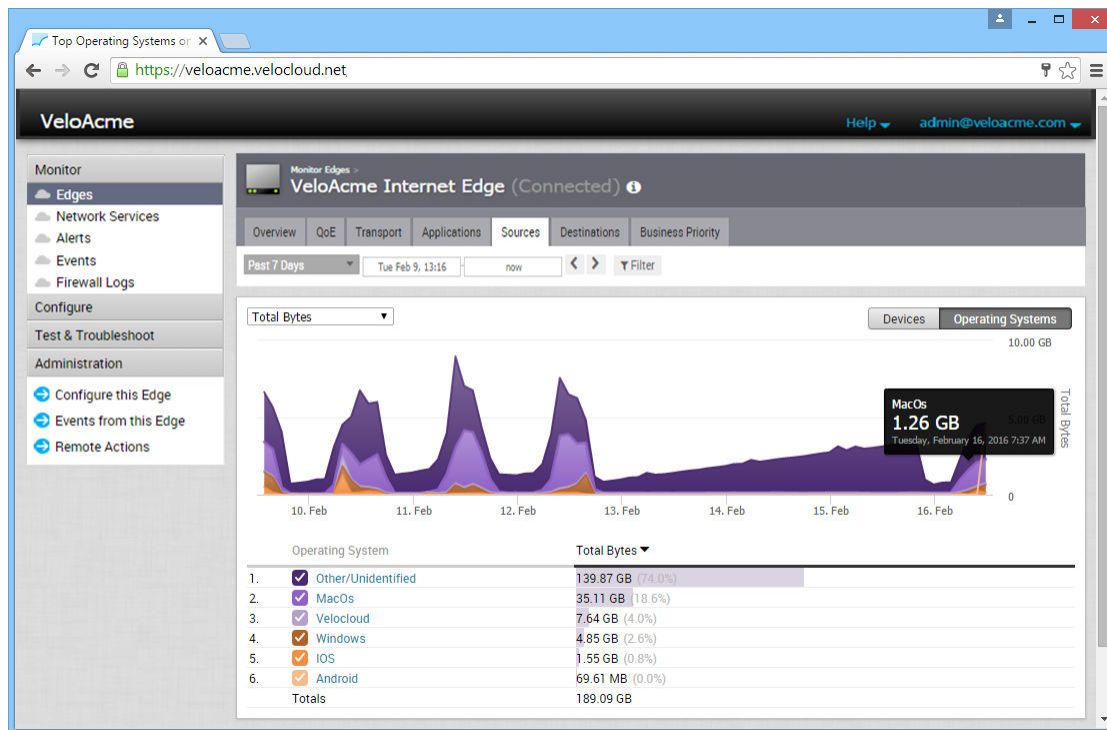
## Sources Tab

The Edge **Sources** tab screen displays network usage data (operating system, device type) over a historical period of time.

The data is displayed as two line graphs. You can change the data that is displayed in the graphs from the **Data** drop-down menu (Bytes Received/Sent, Total Bytes, Total Packets, or Packets Received/Sent). You can also hover over a segment of the graph to display the source and its associated network usage.

In the **Sources** tab screen (below image), you can:

- View the operating systems of your applications and destinations in the **Operating Systems** column (located at the bottom of the screen).
- Use **Filter** to display operating systems based on **Application**, **Category**, type of **Operating System**, and **Destination**.
- Click an operating system from the **Operating System** column to open the **Top Operating Systems** dialog box.
- Go to the **Applications** tab by clicking the gray arrow next to the **Top Applications** area of the **Top Operating Systems** dialog box.
- Go to the **Destinations** tab by clicking the gray arrow next to the **Top Destinations** area of the **Top Operating Systems** dialog box.

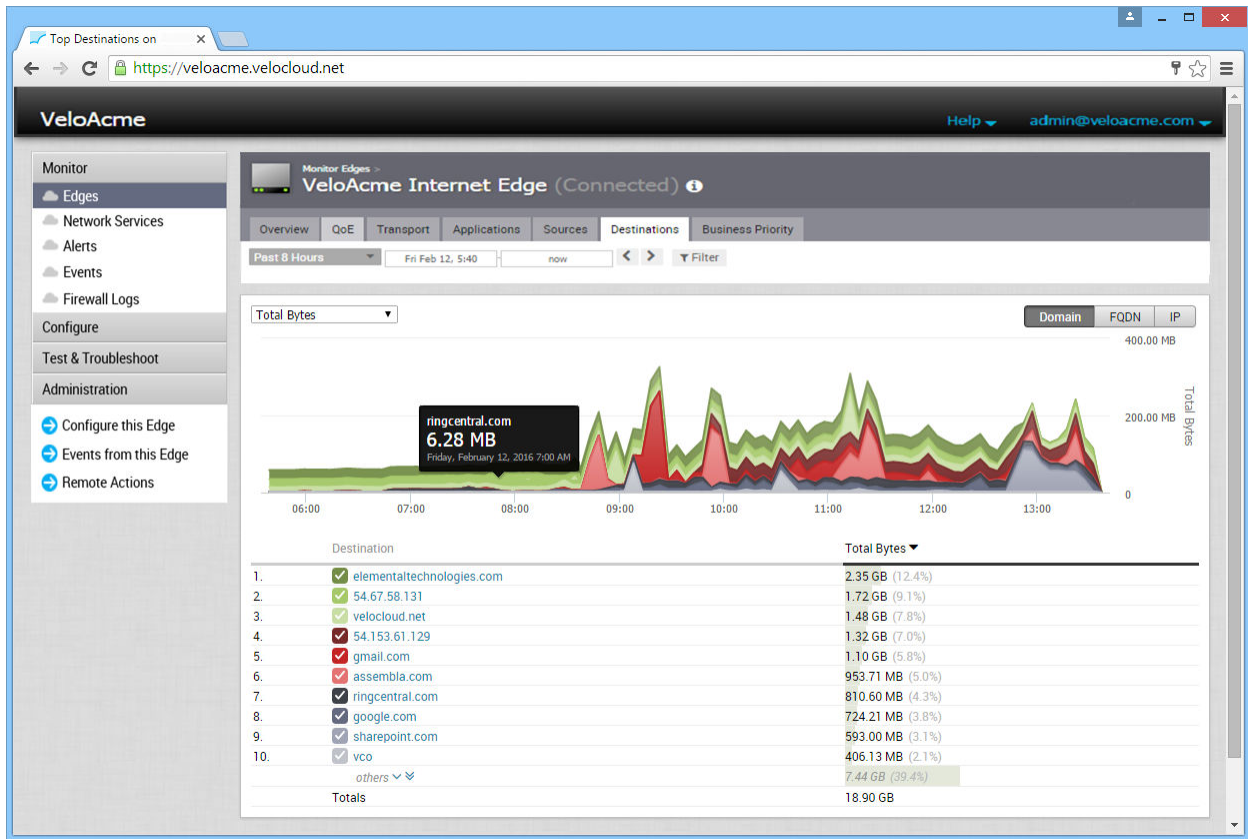


## Destinations Tab

The Edge **Destinations** tab displays network usage as two line graphs (over a historical period of time) by the destination of the network traffic. If you hover over a segment of the graph, the destination and its associated network usage appears.

There are three display buttons (Domain, FQDN, and IP) located on the right side of the screen. Click one of the display buttons to update destinations by type in the **Destination** column.

For each display button (Domain, FQDN, and IP), the **Top Destinations** dialog box appears by type when you click a destination from the Destination column. You can open the **Applications** and **Sources** tabs from the **Top Destinations** dialog box. Click the gray arrows next to the **Top Applications** and **Top Operating** areas of the dialog boxes (respectively) to open these tabs.

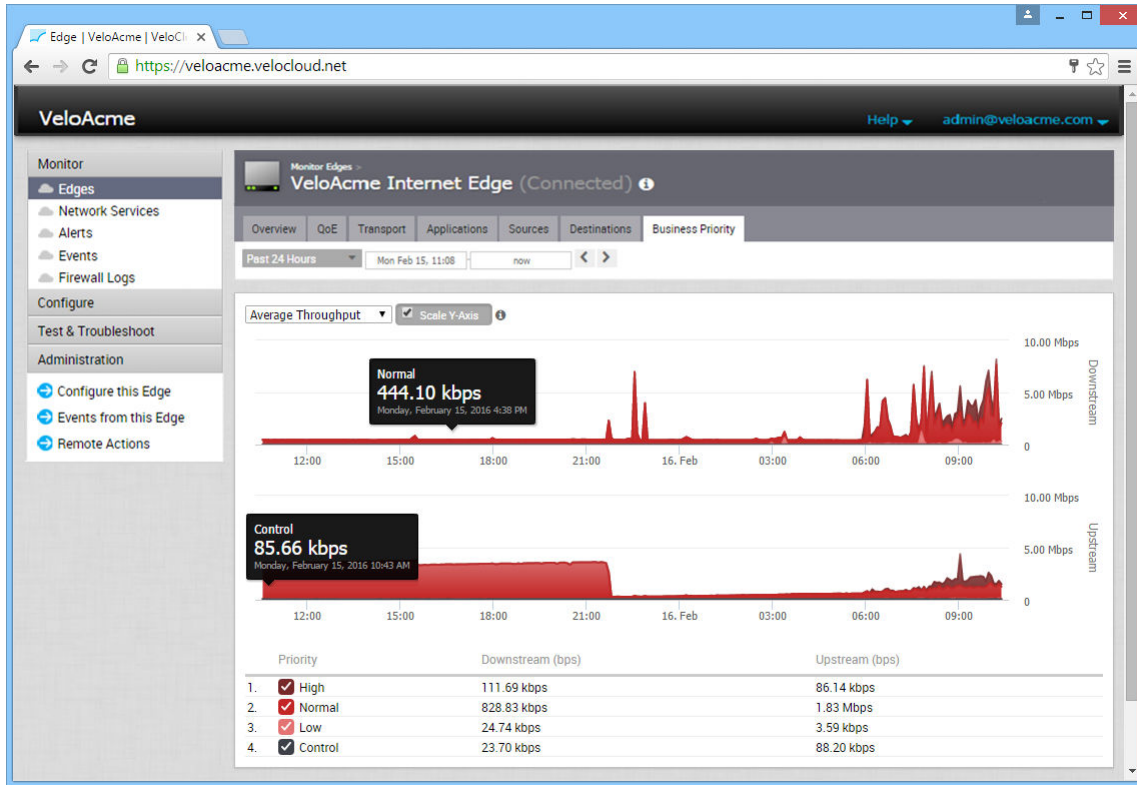


## Business Priority Tab

The Edge **Business Priority** tab displays the priority (High, Normal, Low) of the network traffic over a historical period of time.

If you mouse over a segment of the graph, the Business Policy characteristics and its associated network usage appears.





## Flow Stats Rollups and Retention

In 3.3.0 release, the VeloCloud Orchestrator (VCO) stores only flow statistics with high resolution to provide visibility and troubleshooting capability. In 3.3.2 release, VCO supports retention of flow stats for upto one year by rolling up flow stats for every edge on a daily basis. Currently, the daily flow stats rollups is supported only for on-prem customers.

### Aggregating Flow Statistics

The VCO currently aggregates flow statistics from a higher resolution (every 5 minutes) to a ready-to-use form at a low resolution (every 24 hours). The following tables summarize the flow stats rollup and retention support information.

Table 6-1. Flow Stats Rollup Support

Resolution	Rollup Pre 3.3.0	Rollup Post 3.3.0	Rollup Post 3.3.2
High	5 minutes	5 minutes	5 minutes
Medium	2 hours	Deprecated	Not Supported
Low	8 hours	Deprecated	24 hours

Table 6-2. Flow Stats Retention Support

Resolution	Retention Pre 3.3.0	Retention Post 3.3.0 for OnPrem	Retention Post 3.3.0 for Hosted	Retention Post 3.3.2 for OnPrem	Retention Post 3.3.2 for Hosted
High	6-10 weeks	14 days (Default), 31 days (Maximum)	14 days	14 days	14 days
Medium	10 -14 weeks	Deprecated	Deprecated	Deprecated	Deprecated
Low	Upto 1 year	Deprecated	Deprecated	Upto 1 year	Deprecated

## Frequently Asked Questions

- How to enable flow stats daily rollups post a 3.3.2 upgrade?

To enable flow stats daily rollups, set the `flowStats.daily.rollup.enabled` system property to `true`.

- What is the maximum number of flows that are rolled up per edge per day?

By default, a maximum of one million flows are rolled up per edge per day. This averages out to approximately 3500 flows per 5-minute push. You can modify the number of flows that are rolled up per edge per day, by using the `flowStats.daily.rollup.flowLimit` system property.

- Are hub flows rolled up?

By default, rolling up of hub flows is disabled. You can enable hub flows by using the `flowStats.daily.rollup.edgeFlowLimit` system property, which takes a key-value pair of `<edgeId>:<numFlows>`. You can view high resolution hub flows upto 15 days only.

- Is the flow stats retention policy configurable?

The retention policy for rolled up stats is configurable on the VCO using the `retentionWeeks.flowStats.daily` system property. The rolled-up flow stats retention can be configured to persist anywhere between 1 and 52 weeks.

- Will the UI be able to query flowstats for more than 15 days after enabling rollups?

No. Rolling up flowstats for longer retention is separated from actually being able to query those flowstats. You can set the number of days you want to query the flows by using the `session.options.maxFlowstatsRetentionDays` system property.

- Will there be side effects from a data perspective after turning on this feature?

Although, no side effects are observed on aggregated results, time-series graphs on the VCO UI would have a loss in fidelity due to displaying of rolled up series stats.

- What are the side effects from a system load perspective?

Since rolling up daily flowstats aggregates results from the full resolution table and stores it separately, the system load (CPU/load average) is bound to increase due to the additional processing required by MySQL for aggregating the results.

- What would be the impact to storage requirements for on-premise deployments?

Since rolling up daily flowstats aggregates results from the high resolution table and stores it separately, VeloCloud anticipates the need for the on-premise customers to plan their storage requirements to accommodate rolled up stats. On an average, rolled up flows will consume 1/8th of the space required for high resolution stats; however, this is strongly dependent on the uniqueness of daily flows sent by the edge. In any case, the storage space consumption growth of rolled up flows will be at a much lower rate than the high resolution statistics. For customers that start off with smaller volume drive, VeloCloud recommends using logical volumes so the storage capacity can be grown as the Edges increase.

## Changing the Retention Period

High resolution flow stats retention can be configured to persist anywhere between 1 and 31 days. With the 3.3.0 release, the configuration granularity of the high-resolution flow stats retention has been changed from months to days. Operators can change the retention period by creating a system property. To create a system property to change the retention period, follow the steps below.

- 1 From the VCO navigation panel, click **System Properties**.
- 2 In the **System Properties** screen, click the **New System Properties** button.
- 3 In the **New System Property** dialog box:
  - a In the **Name** text field, type `retention.flowstats.days`.
  - b In the **Data Type** drop-down menu, choose **Number**.
  - c In the **Value** text field, enter the retention period in days.

The screenshot shows a dialog box titled "New System Property...". It contains the following fields and options:

- Name:** A text input field containing the text "retention.flowstats.days".
- Data Type:** A dropdown menu with "NUMBER" selected.
- Value:** A text input field containing the number "7".
- Value is Password:** Two radio buttons, "Yes" and "No", with "No" selected.
- Value is Read-only:** Two radio buttons, "Yes" and "No", with "No" selected.
- Description:** A text area containing the text "Changes the retention period of flow statistics".

At the bottom right of the dialog, there are two buttons: "Save" (highlighted in green) and "Close".

- 4 Click **Save**.

# Monitor Network Services

Network Services (located under **Monitor** in the navigation panel), displays the status of the VPN tunnels to Non-VeloCloud Sites.

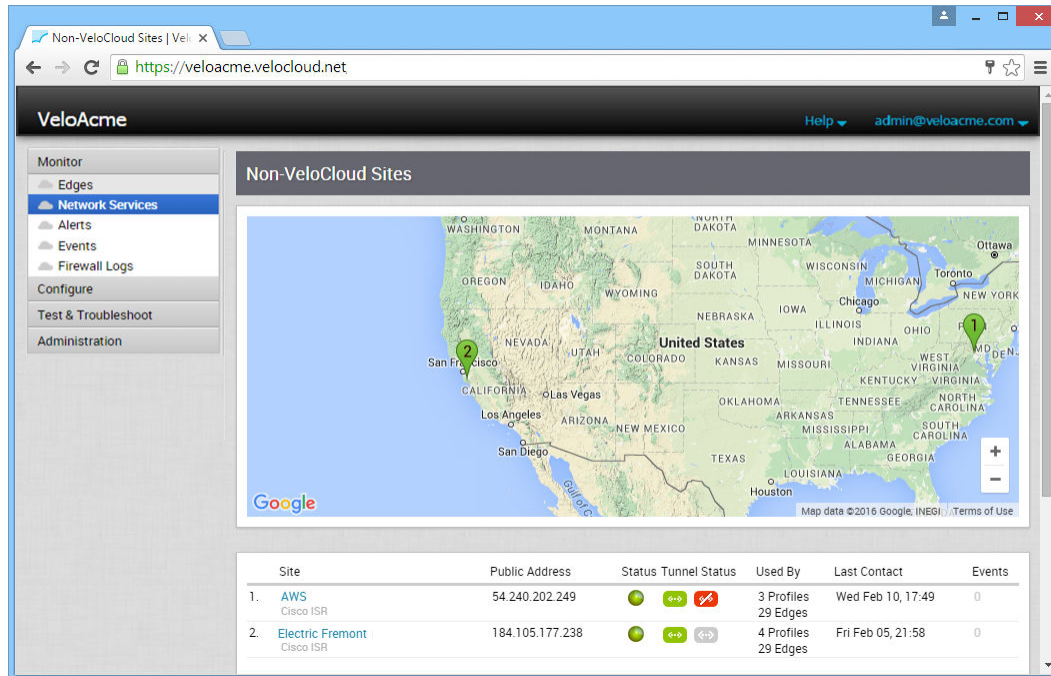
You can click a Non-VeloCloud Site from the **Site** column to open a dialog box to change information about your site.

Types of Non-VeloCloud Sites include:

- IaaS: AWS
- CWS: Zscaler
- Non-VeloCloud Site: Palo Alto, Sonic Wall
- Non VeloCloud Hub

The Non-VeloCloud Site screen displays the Status and the Tunnel Status. Types of status results are listed below:

Color	Meaning
Green	Connected
Red	Offline/ Disconnected
Gray	Not Enabled



# Monitor Routing

The Routing feature ( **Monitor > Routing > Multicast** tab) displays Multicast Group and Multicast Edge information.

The screenshot shows the Velocloud interface with the 'Monitor' sidebar on the left. The 'Routing' section is active, and the 'Multicast' tab is selected. The main area displays a table of Multicast Groups:

Segment	Multicast Group	Source Address	RP	Multicast Edges	Created	Last Update
Global Segment	225.1.1.1	*	3.3.3.3	2 Edges	23 days ago	4 days ago
Global Segment	225.1.1.1	10.7.0.25	3.3.3.3	1 Edge		23 days ago
Global Segment	224.1.1.1	10.2.0.25	NA	1 Edge		4 days ago

A tooltip is visible over the '2 Edges' cell, listing 'EDGE-2' and 'EDGE7'. Below the table, the 'Multicast Group Details' for 'Global Segment / 225.1.1.1 / \*' are shown, displaying a table of Multicast Edges:

	Multicast Edges	Upstream	Downstream
1	EDGE-2 <a href="#">View PIM Neighbors</a>	GE6	GE6 br-network1
2	EDGE7 <a href="#">View PIM Neighbors</a>	EDGE-3	br-network1 EDGE-3

## PIM Neighbors View

The following figure shows the PIM neighbors of the selected Edge (per segment), the interface where the PIM neighbor was discovered, the neighbor IP address, and time stamps.

The screenshot shows a window titled 'Multicast PIM Neighbors: EDGE7'. It contains a search bar and a table with the following data:

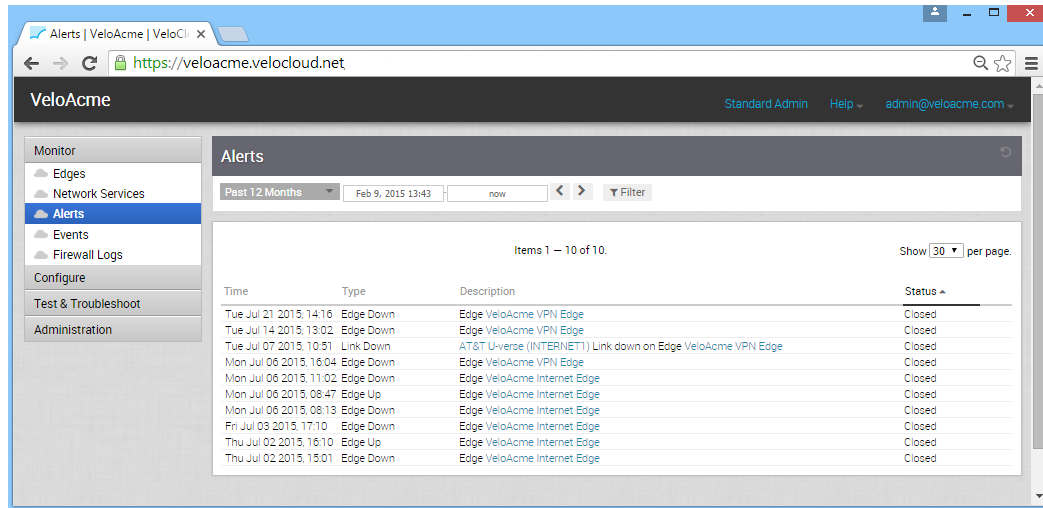
Segment	Edge Name	Interface	Address	Created	Last Update
1 Global Segment	EDGE-3		10.3.0.1	Sat Apr 07, 00:53:08	23 days ago

A 'Close' button is located at the bottom right of the window.

## Monitor Alerts

VeloCloud Orchestrator provides an alert function to notify one or more Enterprise Administrators (or other support users) when a problem occurs. You can access this functionality by clicking **Alerts** under **Monitor** in the navigation panel.

You can send Alerts when a VeloCloud Edge goes offline or comes back online, a WAN link goes down, a VPN tunnel goes down, or when an Edge HA failover occurs. A delay for sending the alert after it is detected can be entered for each of the alert types. You can configure alerts in **Configure > Alerts and Notifications**.

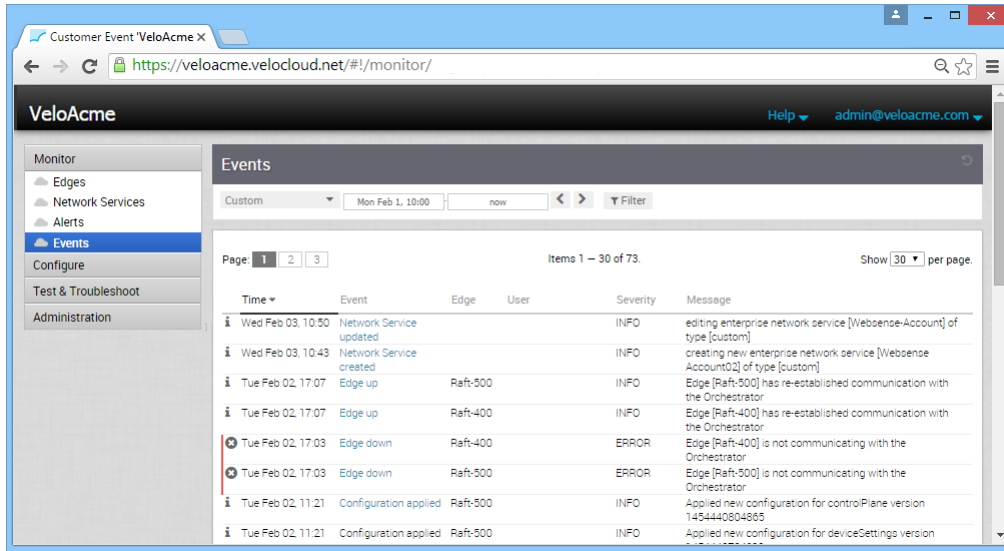


**Note** If you are logged in using a user ID that has Customer Support privileges, you will only be able to view VeloCloud Orchestrator objects. You will not be able to create new objects or configure/update existing ones.

## Monitor Events

The **Events** screen (located under **Monitor** in the navigation panel) displays the events that have been generated by the Orchestrator. These events can help you determine the operational status of the VeloCloud system.

You can click an **Event** link (under the **Event** column) to get more details.



The Events feature is useful for obtaining the following information:

- Audit trail of user activity [filter by user]
- Historical record of activity at a given site [filter by site]
- Record of outages and significant network events [filter by event]
- Analysis of degraded ISP performance [filter by time period]

## Auto Rollback to the Last Known “Good” Configuration

If an Administrator changes device configurations that cause the Edge to disconnect from the Orchestrator, the Administrator will get an “Edge Down” alert. Once the Edge detects that it cannot reach the VCO, it will rollback to the last known configuration and generate an event on the Orchestrator titled, “bad configuration.”

---

**Note** The "Auto Rollback to Last Known "Good" Configuration" section is new for the 3.3.0 release.

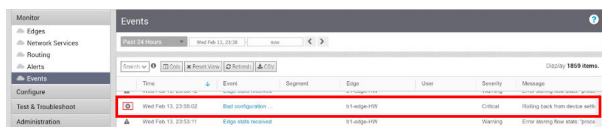
---

The rollback time, which is the time necessary to detect a bad configuration and apply the previous known “good” configuration for a standalone Edge is between 5-6 minutes. For HA Edges, the rollback time is between 10-12 minutes.

---

**Note** This feature rolls back only Edge-level device settings. If the configuration is pushed from the Profile that causes multiple Edges to go offline from the Orchestrator, the Edges will log “Bad Configuration” events and roll back to the last known good configuration individually. **IMPORTANT:** The Administrator is responsible for fixing the Profile accordingly. the Profile configuration will not roll back automatically.

---



## Event Types and Descriptions

The following table describes well-known events.

Event Type	Description
Bad Configuration	Rolling back device settings to the last known settings. See section titled, “ <a href="#">Auto Rollback to the Last Known “Good” Configuration</a> for more information.
Profile Updated	Admin user has updated profile or Edge configuration.
Configuration Applied	New configuration has been applied to an Edge.
Edge Provisioned	An Edge has been created on the VCO (but not yet activated).
Edge Activation	An Edge has been activated.
Link Up / Link Down	A link has come up or gone down.
Edge Up / Edge Down	An Edge has come up or gone down.
User Login	An admin user has logged into the VCO.
User Created	An admin user has been created.



# Configuring VNFs

# 7

The VeloCloud SD-WAN solution supports the following third-party firewalls, Palo Alto Networks, Fortinet, and Check Point CloudGuard Edge VNF. See the links below to successfully deploy and forward traffic through VNF on the VMware SD-WAN Edge.

This chapter includes the following topics:

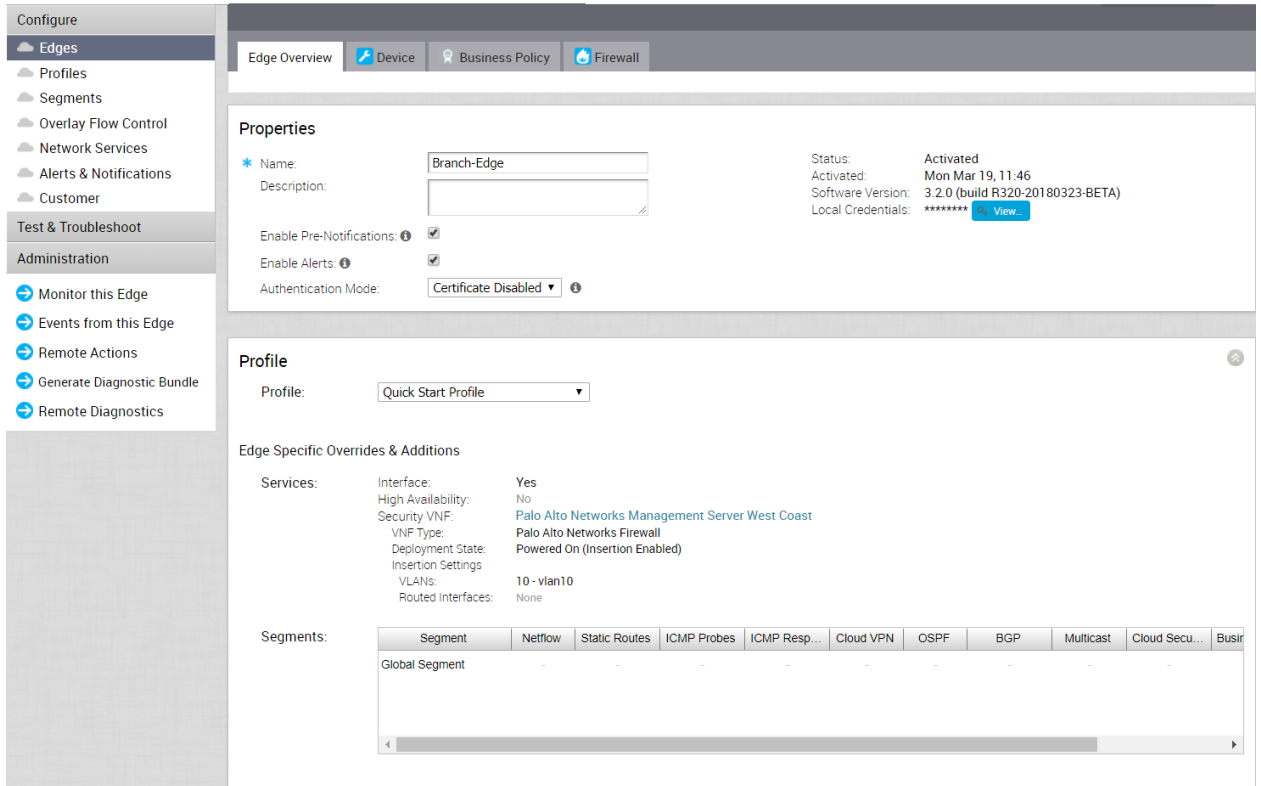
- [Monitor the Edge Overview](#)
- [Configure a VNF Instance](#)
- [VNF Monitoring for an Edge](#)
- [VNF Events](#)
- [Configure VNF Alerts and Notifications](#)

## Monitor the Edge Overview

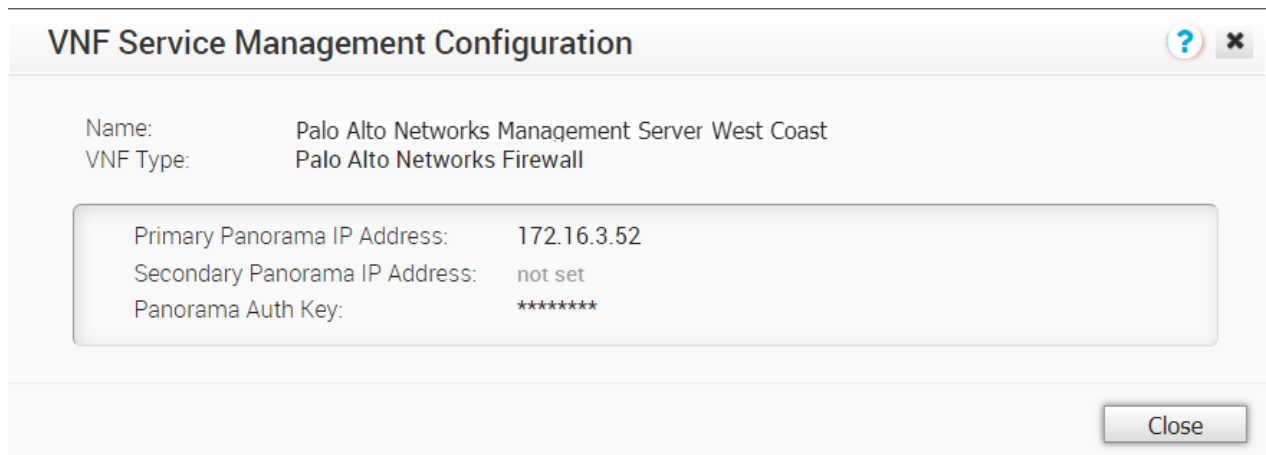
This section describes how to get an overview of a configured Edge.

To see an overview of a configured Edge:

- 1 Go to **Configure > Edges > Edge Overview** tab from the VCO navigation panel.
- 2 In the **Profile** area, select your profile from the **Profile** drop-down menu.
- 3 In the **Services** section of the **Profile** area, note the Security VNF's type, deployment state, and insertion settings, as shown in the following example.



Clicking the **Security VNF** link opens the network service **VNF Management Configuration** dialog so that you can view more information about your VNF.



## Configure a VNF Instance

The VMware SD-WAN by VeloCloud solution supports the following third-party firewalls, Palo Alto Networks VM-series, Fortinet FortiGate VNF, and Check Point CloudGuard Edge VNF. See the sections below to successfully deploy and forward traffic through VNF on the VMware SD-WAN Edge.

## Before you begin:

- You must have an activated SD-WAN Edge 520V or 840.
- You must have a SD-WAN Orchestrator version 3.3.2 or later.
- You must be running an SD-WAN Edge software version 3.3.2 or later.
- You must have VNF Manager add on license.

## About this task:

The procedures in this section provide steps on how to configure a VNF instance via the SD-WAN orchestrator. This task requires additional steps from outside of the orchestrator from the third-party firewall you've chosen. Please refer to the appropriate deployment guides for these additional steps

---

**Note** Only Operator Superusers and Standard Operators can enable Edge NFV and Security VNFs. Business Specialist Operators and Support Operators must contact their Operators to request access. If you do not have access, your Operator must enable this feature to configure VNFs. If you have Operator access, see "Step 1: Enable Edge NFV and Edge VNF" in the Procedure section below.

---

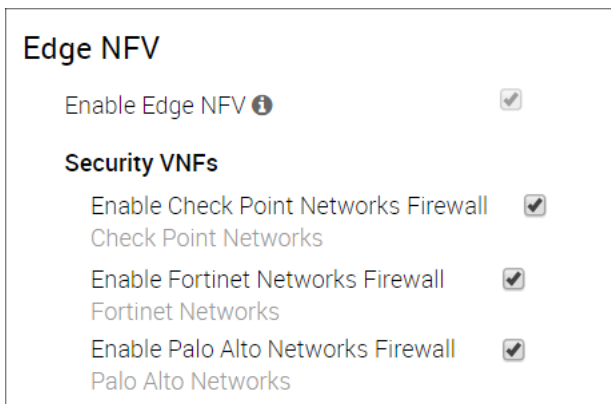
## Procedure to Configure a VNF Instance:

### Step 1: Enable Edge NFV and Edge VNF

- 1 If you have the necessary Operator access, go to **Configure** > **Customer** in the navigation panel of the VCO.

The **Customer Configuration** screen appears.

- 2 In the **Edge NFV** area, check the **Enable Edge NFV** checkbox (image below).
- 3 In the **Security VNFs** area, enable the applicable security VNFs: **Enable Check Point Networks Firewall**, **Enable Fortinet Networks Firewall**, or **Enable Palo Alto Networks Firewall**.



After you enable **Edge NFV** and choose a **Security VNF**, the **Enable Edge NFV** checkbox becomes disabled because there is now a network service associated with it.

- 4 Click the **Save Changes** button.

## Step 2: Define a VNF Instance

- 1 From the VeloCloud Orchestrator, go to **Configure > Network Services**.

The **Services** screen appears.

- 2 In the **VNFs** area, click the **New** button.

The **VNF Service Management Configuration** dialog box appears.

- 3 In the **VNF Service Management Configuration** dialog box complete the following:

- a Type in a name in the appropriate text box for the VNF service instance.
- b From the **VNF Type** drop-down menu, choose one of the following for the VNF Type: Check Point Firewall, Fortinet Firewall, or Palo Alto Networks Firewall.

**Note** The **VNF Service Management Configuration** dialog box will require different information depending upon which VNF type you choose. If you chose Palo Alto Networks Firewall, see Step 3c. If you chose Check Point Firewall, see step 3d. If you chose Fortinet Firewall, see step 3e. Follow the appropriate steps below to determine what types of information is required in the **VNF Management Configuration** dialog box.

- c If you've chosen Palo Alto Networks Firewall as the VNF type, enter in the following in the **VNF Management Configuration** dialog box as described in the steps below:

The screenshot shows a dialog box titled "VNF Service Management Configuration" with a help icon and a close button. It contains the following fields:

- Name:** Palo Alto Networks Management Server West Coast
- VNF Type:** Palo Alto Networks Firewall
- Primary Panorama IP Address:** 172.16.3.52
- Secondary Panorama IP Address:** (empty)
- Panorama Auth Key:** (masked with dots)

At the bottom right, there are two buttons: "Save Changes" (highlighted in green) and "Cancel".

- 1 Type in a **Primary Panorama IP Address** and a **Secondary Panorama IP Address**, if necessary.
- 2 Type in the **Panorama Auth Key** in the appropriate text box. The customer must configure the Auth Key password on Panorama. VNF uses the Auth Key to login and communicate with Panorama.
- 3 Click **Save Changes**.

The **VNFs** area updates, displaying the newly created VNF configuration.

VNFs			New...	Delete...
Name	Type	Used By		
<input type="checkbox"/> Palo Alto Networks Management Server West Coast	Palo Alto Networks Firewall	1 Edge		

4 Define VNF Licenses for Palo Alto Networks. (These licenses will be applied to one or more VNF configured Edges).

- In the **VNF Licenses** area, click the **New** button (from the **Configure > Network Services** screen).
- In the **VNF License Configuration** dialog box complete the following steps below:
  - Type in a name in the appropriate textbox.
  - In the **VNF Type** drop-down menu, choose the only available option, **Palo Alto Networks Firewall**.
  - Type in the **License Server API Key** in the appropriate textbox. The customer gets this key from their Palo Alto Networks account. The VCO uses this key to communicate with Palo Alto Networks license server.
  - Type in the Authorization Code in the **Auth Code** textbox. The customer must purchase the Auth Code from Palo Alto Networks). See image below.

- Click the **Test** button to validate the configuration.
- If your configuration is valid, a confirmation indicator will display next to the **Test** button.
- If the configuration is not valid, an invalid message icon will display next to the **Test** button.

- Click **Save Changes**. The customer can now apply one or more of these licenses to VNF configured Edges.

The **VNF Licenses** area updates as shown in the image below.

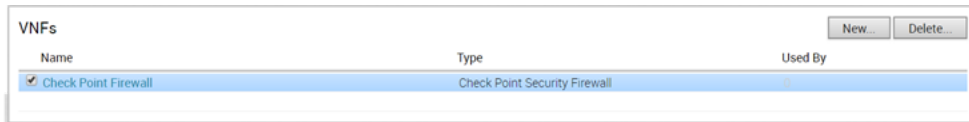
VNF Licenses			New...	Delete...
Name	Type	Used By		
<input type="checkbox"/> VM-50 License	Palo Alto Networks Firewall	1 Edge		

- Proceed to Step 3: Configure Edge-specific Settings on the VNF.
- d If you've chosen Check Point Firewall as the VNF type, enter the following in the **VNF Service Management Configuration** dialog box as described below. (See image below).

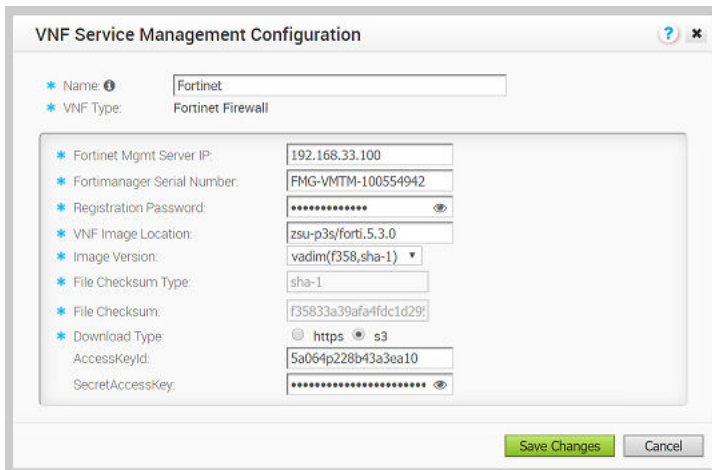
- 1 Type in a name in the appropriate text box for your VNF service instance.
- 2 From the **VNF Type** drop-down menu, choose **Check Point Firewall**.
- 3 Type in the **Primary Check Point Mgmt Server IP** in the appropriate text box. This is the Check Point Smart Console IP address that the Check Point CloudGuard Edge will connect to.
- 4 Type in the **SIC Key for Mgmt Server Access** in the appropriate text box. This is the password used to register the VNF to the Check Point Smart Console.
- 5 Type in the **VNF Image Location** in the appropriate text box. This is the image location where the SD-WAN Orchestrator will download the VNF image.
- 6 From the **Image Version** drop-down menu, select a version of the Check Point VNF image.
- 7 **File Checksum Type** autopopulated field – Specifies the method used to validate the VNF image. This field is automatically populated after you choose an image version from the above step.
- 8 **File Checksum** autopopulated field – Specifies the checksum used to validate the VNF image. This field is automatically populated after you choose an image version from the previous step.

- 9 **Download Type** radio buttons – Specify where the image is available by choosing one of the following options, s3 or https. NOTE: When you select https, enter the username and password in the appropriate text field. When you select s3, enter the AccessKeyId and SecretAccessKey in the appropriate text field.
- 10 Click the **Save Changes** button.

The VNFs area updates displaying the newly created VNF configuration (see image below)



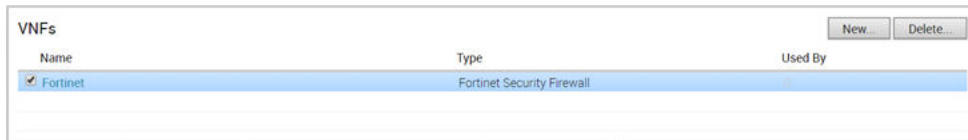
- 11 Proceed to Step 3: Configure Edge-specific Settings on the VNF.
- e If you’ve chosen Fortinet Firewall as the VNF type, follow the steps below in the **VNF Service Management Configuration** dialog box (see image below).



- 1 Type in a name in the appropriate text box for your VNF service instance.
- 2 Choose the **VNF type Fortinet Firewall** from the drop-down menu.
- 3 Type in the **Fortinet Mgmt Server IP** in the appropriate text box. This is the IP address of the FortiManager for the FortiGate to connect to.
- 4 Type in the **Registration Password**. This is the password used to register the VNF to the FortiManager.
- 5 Type in the **VNF Image Location**. This is the image location for the SD- WAN Orchestrator to download the VNF image.
- 6 From the **Image Version** drop-down menu, select a version of the Fortinet VNF image.
- 7 **File Checksum Type** text box– Specifies the method used to validate the VNF image. This field is automatically populated after you choose an image version from the previous step.

- 8 **File Checksum** text box – Specifies the checksum used to validate the VNF image. This field is automatically populated after you choose an image version from the previous step.
- 9 Download Type radio buttons – Specify where the image is available by choosing one of the following options, s3 or https. NOTE: When you select https, enter the username and password in the appropriate text field. When you select s3, enter the AccessKeyid and SecretAccessKey in the appropriate text field.
- 10 Click the **Save Changes** button.

The **VNFs** area updates displaying the newly created VNF configuration (see image below).



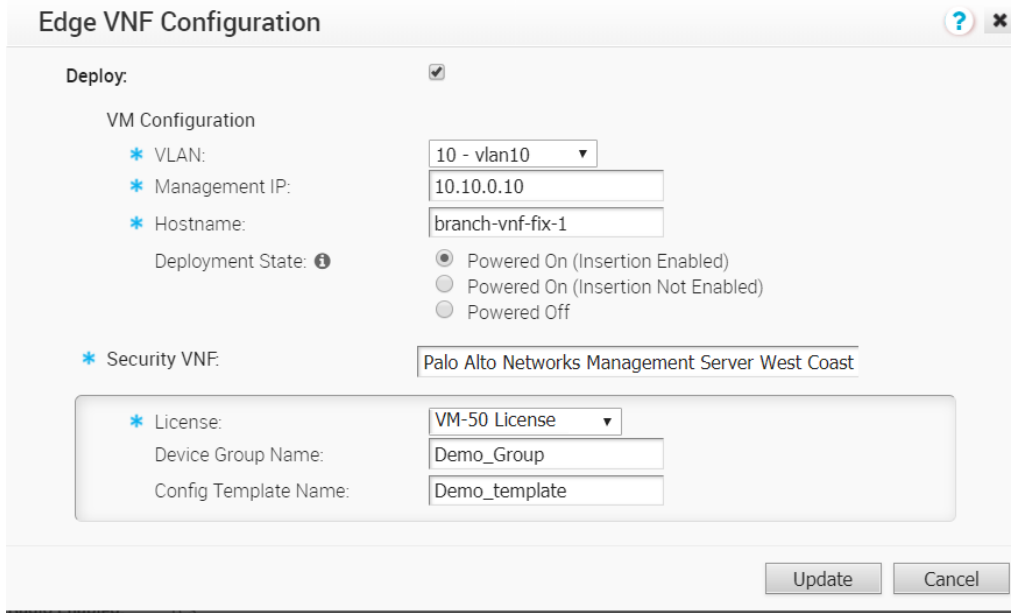
VNFs			New	Delete...
Name	Type	Used By		
<input checked="" type="checkbox"/> Fortinet	Fortinet Security Firewall			

- 11 Proceed to Step 3: Configure Edge-specific Settings on the VNF.

### Step 3: Configure Edge-specific Settings on the VNF

- 1 From the VCO navigation panel, go to **Configure > Edges > Devices** tab.
- 2 Choose an Edge on the **Edges** screen.
- 3 Click the **Device** tab.
- 4 In the **Device** tab screen, scroll down to the **Security VNF** area, click the **Edit** button.  
The **Edge VNF Configuration** dialog box displays.
- 5 In the Edge VNF Configuration dialog, check the Deploy checkbox (image below).
- 6 In the **Edge VNF Configuration** dialog box, check the **Deploy** checkbox.





- 7 In the **VM Configuration** area of the **Edge VNF Configuration** dialog box complete the following:
  - a Choose a **VLAN** from the drop-down menu. (This VLAN will be used for the VNF management).
  - b Type in the **Management IP**. Note that when the VNF is created, it will automatically specify the IP address of the VLAN interface as a default Gateway.
  - c Type in the **Hostname** in the appropriate text box.
  - d Choose a **Deployment State**. The type of deployment state will be determined based on what type of predefined “Security VNF” network service as described below.
    - If you choose Fortinet or Checkpoint as a security VNF, choose from one of the following two **Deployment States**: Image Downloaded and Powered On or Image Downloaded and Powered Off. (See the table below for a description of these states).
    - If you choose PaloAlto Networks as a security VNF, choose from one of the following two **Deployment States**: Powered On or Powered Off. (See the table below for more information about these states).

State	Definition
Powered On	After building the firewall VNF on the Edge, power it up.
Powered Off	After building the firewall VNF on the Edge, keep it powered down.

**Note** Traffic only transits the VNF when it is in the “Powered On” state, which requires that at least one VLAN or routed interface be configured for VNF insertion. Do not select ‘Powered Off’ if you intend to send traffic through the VNF.

- e In the **Security VNF** drop-down menu, choose one of the following: a predefined VNF network service or a new network service (if you choose the later option, the **Network Service VNF Configuration** dialog box opens so you can create a new VNF service).
- **If you choose Palo Alto as your Security VNF:**
    - Choose a license from the **License** drop-down menu.
    - Type in the **Device Group Name** and the **Config Template Name** in the appropriate textboxes. (The Device Group Name and the Config Template Name are pre-configured on the Panorama server).
    - Click the **Update** button.

The **Security VNF** panel updates.

Security VNF		Security VNF:	
VM Configuration <span style="float: right;">Edit</span> Deployment State: <span style="color: red;">ⓘ</span> Powered On (Insertion Enabled)		Palo Alto Networks Management Server West Coast Palo Alto Networks Firewall	
VLAN:	10 - vlan10	License:	VM-50 License
Management IP:	10.10.0.10	Device Group Name:	Demo_Group
Hostname:	branch-vnf-fix-1	Config Template Name:	Demo_template

- **If you choose Fortinet as your Security VNF:**
  - Choose an **Inspection** mode. (Proxy mode is selected by default).
  - Drag the license file into the **License** box located at the bottom of the screen.

Click the **Update** button.

The **Security VNF** panel updates.
- **If you choose Check Point as your Security VNF:**
  - Choose Check Point from the **Security VNF** drop-down menu.
  - Click the **Update** button.

The **Security VNF** panel updates.

## Step 4: Insert VNF into the Dataplane

The VNF can be inserted to both the VLAN as well as routed interface. If you choose to use routed interface, make sure the trusted source is checked and disabled WAN overlay on that interface.

- 1 If you are not in the **Device** tab screen for a VeloCloud Edge, go to **Configure > Edges** in the navigation panel of the VCO.  
The **VeloCloud Edges** screen appears.
- 2 Select an Edge and click the **Device** icon associated with the selected Edge located the Device column.
- 3 Scroll down to the **Configure VLAN** area.
- 4 Click the applicable VLAN **Edit** link.

- In the **VLAN** dialog box, click the **VPN Insertion** checkbox to insert the VNF into VLAN. This step redirects traffic from a specific VLAN into the VNF.

The screenshot shows the 'VLAN' configuration dialog box. The 'VNF Insertion' checkbox is checked and highlighted with a mouse cursor. Other fields include VLAN Name (Corporate), VLAN Id (1), Edge LAN IP Address (10.0.0.1), Cidr Prefix (24), Network (10.0.0.0), and Multicast settings (IGMP, PIM, PIM SM). The DHCP section is also visible, showing Type (Enabled), DHCP Start (10.0.0.13), Num. Addresses (242), and Lease Time (1 day). The OSPF section shows 'Enabled' with a note 'OSPF not enabled'. Buttons for 'Add VLAN' and 'Cancel' are at the bottom right.

The screenshot shows the 'Configure VLAN' table with the following data:

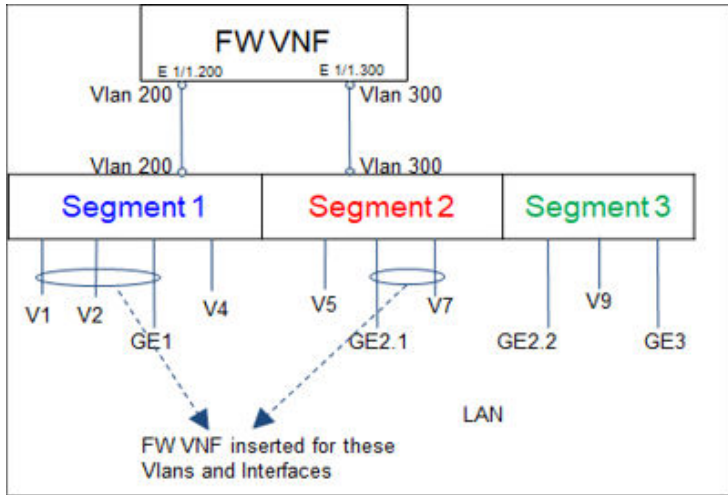
Action	VLAN	Network	IP Address	DHCP	Segment	IGMP	PIM	VNF Insertion
Edit   Del	1 - Corporate			Enabled (242)	Global Segment			<input checked="" type="checkbox"/>

- Insert the VNF into Layer 3 interfaces or sub-interfaces. This step redirects traffic from specific Layer 3 interfaces or subinterfaces into the VNF.

## (Optional) Step 5: Define Mapping between Segments and Service VLANs

This step is applicable if multiple traffic segments must be redirected to the VNF.

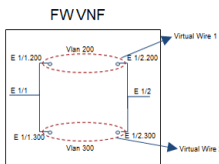
As shown in the following figure, the segment in which the VNF is inserted is assigned a unique VLAN ID. The FW policy on the VNF is defined using these VLAN IDs. Traffic from VLANs and interfaces within these segments is tagged with the VLAN ID allocated for that particular segment.



The following figure zooms into the **FW VNF** area of the preceding figure.

Note the following about Firewall VNF (The image below pertains to Palo Alto Networks only):

- One Virtual Wire per Vlan ID
- Sub-interface pairs should be created on Panorama per Virtual Wire
- FW policies are associated with the Virtual Wire
- Overlapping addresses can be used in separate Virtual Wires



**To define mapping between segments and service VLANs (Step 3), complete the following substeps:**

- 1 Go to **Configure > Segments**.
- 2 For available segments, type in Service VLANs for each segment.



- 3 Click **Save Changes**.

## VNF Monitoring for an Edge

This section describes VNF monitoring for an Edge.

There are two ways to monitor a VNF on the Edge:


- Monitor VNF and VM Status per Edge
- View All the VNF Network Services Configured for the Customer

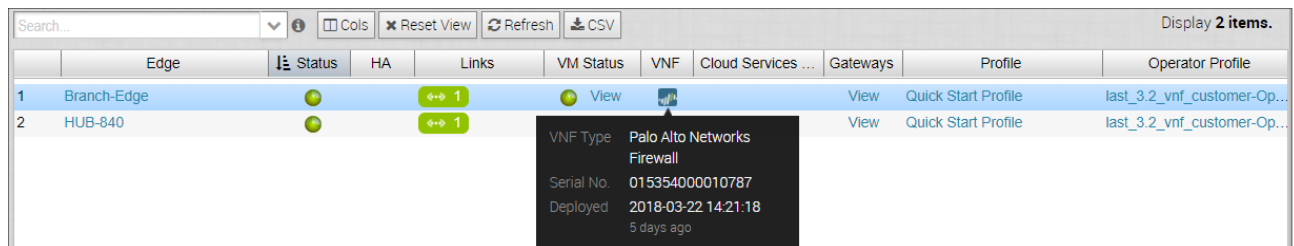
## Monitor VNF and VM Status per Edge

You can monitor the VNF status on the Edges from the VCO at **Monitor > Edges**. VNF Monitoring displays VNF and VM states and deployment information.

You can monitor the VNF status of the Edges from the VeloCloud Orchestrator at **Monitor > Edges**. VNF Monitoring can be classified in two categories

- VNF VM related event/metrics
- VNF application related events/metrics

In the **Edge Monitoring** table, you can check the VNF status for an Edge. Hover over the  icon in the **VNF** column to view additional information about your VNF (type, serial number, and when it was deployed).



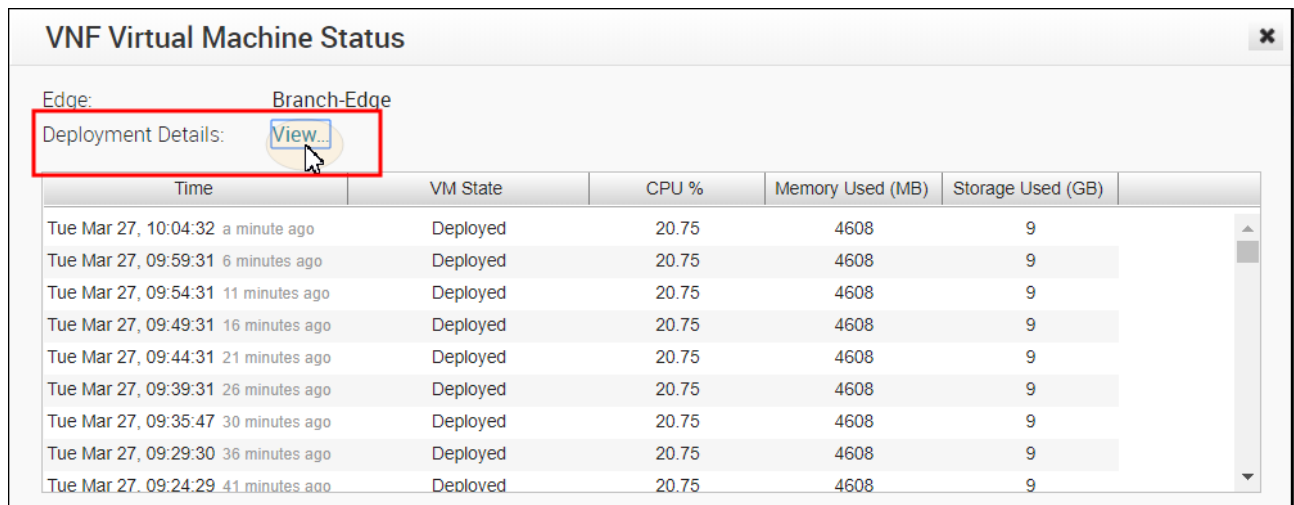
Edge	Status	HA	Links	VM Status	VNF	Cloud Services ...	Gateways	Profile	Operator Profile
1 Branch-Edge							<a href="#">View</a>	<a href="#">Quick Start Profile</a>	<a href="#">last_3.2_vnf_customer-Op...</a>
2 HUB-840							<a href="#">View</a>	<a href="#">Quick Start Profile</a>	<a href="#">last_3.2_vnf_customer-Op...</a>

VNF Type: Palo Alto Networks Firewall

Serial No.: 015354000010787

Deployed: 2018-03-22 14:21:18  
5 days ago

Click the **VM Status** link to open the **VNF Virtual Machine Status** dialog box, where you can view the deployment status for the Edge. To view deployment details, click the **Deployment Details View** link.



**VNF Virtual Machine Status** ✕

Edge: Branch-Edge

Deployment Details: [View...](#)

Time	VM State	CPU %	Memory Used (MB)	Storage Used (GB)
Tue Mar 27, 10:04:32 a minute ago	Deployed	20.75	4608	9
Tue Mar 27, 09:59:31 6 minutes ago	Deployed	20.75	4608	9
Tue Mar 27, 09:54:31 11 minutes ago	Deployed	20.75	4608	9
Tue Mar 27, 09:49:31 16 minutes ago	Deployed	20.75	4608	9
Tue Mar 27, 09:44:31 21 minutes ago	Deployed	20.75	4608	9
Tue Mar 27, 09:39:31 26 minutes ago	Deployed	20.75	4608	9
Tue Mar 27, 09:35:47 30 minutes ago	Deployed	20.75	4608	9
Tue Mar 27, 09:29:30 36 minutes ago	Deployed	20.75	4608	9
Tue Mar 27, 09:24:29 41 minutes ago	Deployed	20.75	4608	9

## View All the VNF Network Services Configured for the Customer

You can view all the VNF network services configured for the customer from the VCO at **Monitoring > Network Services**.

Edge VNFs			
	Service	Used By	Edge VM Status
1	new_vnf Palo Alto Networks Firewall	1 Edge <a href="#">View</a>	Powered On (Insertion Enabled) 1 Edge

## VNF Events

VNF Events are categorized into the following categories:

### Edge VNF Virtual Machine Deployment

- VNF\_VM\_DEPLOYED
- VNF\_VM\_POWERED\_ON
- VNF\_VM\_POWERED\_OFF
- VNF\_VM\_DELETED
- VNF\_VM\_ERROR

### Edge VNF Insertion

- VNF\_INSERTION\_ENABLED
- VNF\_INSERTION\_DISABLED

Events							
Time	Event	Segment	Edge	User	Severity	Message	
Mon Mar 26, 13:34:26	Profile updated		Branch-Edge	super@velocloud.net	Info	profile [Edge Specific Profile] edit m	
Mon Mar 26, 13:34:09	VNF_INSERTION_EV...		Branch-Edge		Alert	VNF insertion ENABLED	
Mon Mar 26, 13:34:09	Configuration applied		Branch-Edge		Info	Applied new configuration for device 1522096466551	
Mon Mar 26, 13:34:09	Configuration applied		Branch-Edge		Info	Applied new configuration for contr 1522096487789	
Mon Mar 26, 13:33:47	Network Service upda...				Info	editing enterprise network service [E 1521241836416] of type [securityVr	
Mon Mar 26, 13:32:54	Profile updated		Branch-Edge	super@velocloud.net	Info	profile [Edge Specific Profile] edit m	
Mon Mar 26, 13:32:54	Network Service upda...			super@velocloud.net	Info	editing enterprise network service [E 1521241836416] of type [securityVr	
Mon Mar 26, 13:32:39	VNF_INSERTION_EV...		Branch-Edge		Alert	VNF insertion DISABLED	
Mon Mar 26, 13:32:38	Configuration applied		Branch-Edge		Info	Applied new configuration for device 1522096374454	

	Time	Event	Segment	Edge	User	Severity	Message
i	Fri Mar 30, 12:06:53	VNF_VM_EVENT		Branch-Edge		Info	QEMU event
i	Fri Mar 30, 11:53:26	Link alive		HUB-840		Info	Link GE3 is no longer DEAD
i	Fri Mar 30, 11:53:02	Profile updated		HUB-840	super@velocloud.net	Info	profile [Edge Specific Profile] edit m
i	Fri Mar 30, 11:52:28	Edge Interface Up		HUB-840		Info	Interface GE3 is up
i	Fri Mar 30, 11:52:26	Configuration applied		HUB-840		Info	Applied new configuration for contrc 1522435987007
i	Fri Mar 30, 11:52:26	Edge Interface Down		HUB-840		Info	Interface GE3 is down
i	Fri Mar 30, 11:52:26	Configuration applied		HUB-840		Info	Applied new configuration for device 1522435982247
i	Thu Mar 29, 14:58:48	Profile updated		Branch-Edge	super@velocloud.net	Info	profile [Edge Specific Profile] edit m
i	Thu Mar 29, 14:58:08	Configuration applied		Branch-Edge		Info	Applied new configuration for contrc 1522360729025
i	Thu Mar 29, 14:58:08	Configuration applied		Branch-Edge		Info	Applied new configuration for device 1522360728073
i	Thu Mar 29, 12:06:53	VNF_VM_EVENT		Branch-Edge		Info	QEMU event
i	Wed Mar 28, 12:06:52	VNF_VM_EVENT		Branch-Edge		Info	QEMU event
i	Wed Mar 28, 06:12:23	New client device seen		HUB-840		Notice	New or updated client device 00:50:172.16.3.38, segId 0, hostname 6-si HOST, os Ubuntu/Debian 5/Knoppix
i	Tue Mar 27, 12:06:52	VNF_VM_EVENT		Branch-Edge		Info	QEMU event
i	Tue Mar 27, 11:45:18	New client device seen		Branch-Edge		Notice	New or updated client device 00:0c:10.10.0.249, segId 0, hostname ubu 5/Knoppix 6

## Configure VNF Alerts and Notifications

To receive alerts and notifications regarding VNF events, go to **Configure > Alerts & Notifications > Alert Configuration** screen.

**Note** For VNF configuration, there are two types of notifications:

- Choose the **Edge VNF Virtual Machine Deployment** notification to receive an alert when an Edge virtual machine deployment state changes.
- Choose the **Edge VNF Insertion** notification to receive an alert when an Edge VNF deployment state changes.

Select Alerts	Alert Type	Notification Delay
<input type="checkbox"/>	Edge Down ⓘ	3 minutes
<input type="checkbox"/>	Edge Up ⓘ	1 minutes
<input type="checkbox"/>	Link Down ⓘ	3 minutes
<input type="checkbox"/>	Link Up ⓘ	1 minutes
<input type="checkbox"/>	VPN Tunnel Down ⓘ	3 minutes
<input type="checkbox"/>	Edge HA Failover ⓘ	1 minutes
<input type="checkbox"/>	Edge VNF Virtual Machine Deployment ⓘ	0 minutes
<input type="checkbox"/>	Edge VNF Insertion ⓘ	0 minutes
<input type="checkbox"/>	Edge CSS tunnel up ⓘ	3 minutes
<input type="checkbox"/>	Edge CSS tunnel down ⓘ	3 minutes
<input type="checkbox"/>	Edge VNF Image Download Event ⓘ	0 minutes

See table below for a description of each alert.

Alert Type	Description
Edge Down	Receive an alert when an Edge is no longer visible in the Orchestrator. Receiving this alert might indicate an Edge device failure or a failure of network connectivity. You can disable alerts for a specific Edge on the <b>Edge Overview</b> screen.
Edge Up	Receive an alert when an Edge transitions from the offline to the online state. You can disable alerts for a specific Edge on the <b>Edge Overview</b> screen.
Link Down	Receive an alert when a WAN Link is disconnected from the Edge or when the Link cannot communicate with the VeloCloud service. You can disable alerts for a specific Link on the Edge <b>Device</b> screen.
Link Up	Receive an alert when a WAN Link returns to a normal functioning state. You can disable alerts for a specific Link on the Edge <b>Device</b> screen.
VPN Tunnel Down	Receive an alert when the IPSec tunnel configured from the VeloCloud service to your VPN Gateway cannot be established or if the tunnel is dropped and cannot be re-established.
Edge HA Failover	Receive an alert when an HA Edge fails-over to its standby.
Edge VNF Virtual Machine Deployment	Receive an alert when an Edge VNF virtual machine deployment state changes.
Edge VNF Insertion	Receive an alert when an Edge VNF deployment state changes.
Edge VNF Image Download Event	Receive an alert when an Edge VNF image download state changes.
Edge CSS Tunnel Up	Receive an alert when the Edge Cloud Security Service Tunnel is up.
Edge CSS Tunnel Down	Receive an alert when the Edge Cloud Security Service Tunnel is down.

### To set alerts:

- 1 In the **Select Alerts** area, select the type of alert you want to receive.
- 2 No need to the number of Notification Delay minutes for each type because the **Notification Delay** value is not valid for VNF alerts.
- 3 If applicable, type in **Customers, Email Addresses, Phone Numbers**, and **SNMP Traps** in the appropriate textboxes.
- 4 Click the **Save Changes** button.



# Configure Segments



In the VeloCloud segment-aware topology, different VPN profiles can be enabled for each segment. For example, Guest traffic can be backhauled to remote data center firewall services: Voice media can flow direct from Branch-to-Branch based on dynamic tunnels, and the PCI segment can backhaul traffic to the data center to exit out of the PCI network.

You can create segments in the **Segments** window ( **Configure > Segments** in the navigation panel).

There are two types of segments:

- Regular
- CDE (Cardholder Data Environment). The CDE type is for customers who require PCI and want to leverage the VeloCloud SD-WAN PCI certification.

Beginning with the 3.1 release, VeloCloud provides PCI certified VeloCloud SD-WAN service. For customers who have PCI certified VeloCloud SD-WAN, they must create a segment for PCI traffic and assign the type as CDE. VeloCloud hosted Orchestrator and Controller will be aware of the PCI segment and in the PCI scope. Gateways (marked as non-CDE Gateways) will not be aware or transmit PCI traffic and will be out of PCI scope.



**Note** For information about the Service VLAN column in the Segments screen, see Step 3 "Define Mapping between Segments and Service VLANs (Optional)" in [Chapter 7 Configuring VNFs](#).

The following table describes the fields displayed in the **Segments** screen.

<b>Field</b>	<b>Description</b>
<b>Segment Name</b>	Name of segment (up to 256 characters).
<b>Description</b>	Description of segment (up to 256 characters).
<b>Type</b>	Regular or CDE.
<b>Delegate To Partner</b>	By default, this is selected. If unselected, the Partner cannot change configs within the segment, including the interface assignment.
<b>Delegate To Customer</b>	By default, this is selected. If unselected, the Customer cannot change configs within the segment, including the interface assignment.

# Configure Network Services

# 9

This section describes how to configure network services.

---

**Note** If you are logged in using a user ID that has Customer Support privileges, you will only be able to view VeloCloud Orchestrator objects. You will not be able to create new objects or configure/update existing ones.

---

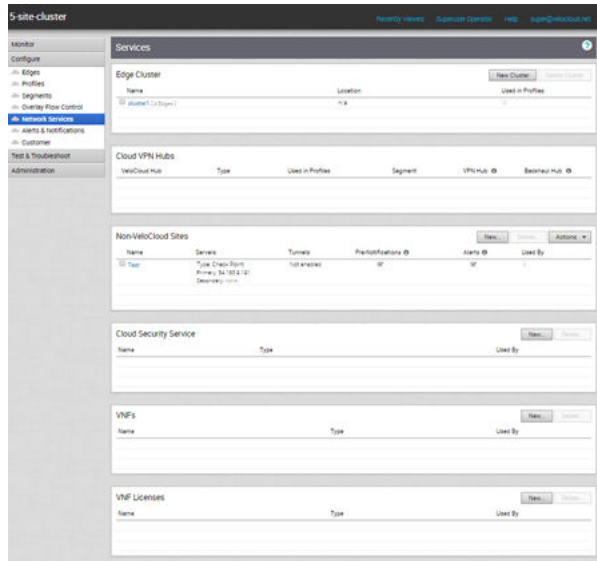
You can configure the following Network Services:

- Edge Cluster
- Cloud VPN Hubs
- Non-VeloCloud Sites
- Cloud Security Service
- VNFs
- VNF Licenses
- DNS Services
- Netflow Settings
- Private Network Names
- Authentication Services

---

**Note** Configuring Network Services are optional and can be configured in any order.

---



This chapter includes the following topics:

- [About Edge Clustering](#)
- [Cloud VPN Hubs & Backhaul Sites \(Summary View\)](#)
- [Configure a Non-VeloCloud Site](#)
- [Configure Cloud Security Services](#)
- [Configure DNS Services](#)
- [Configure Netflow Settings](#)
- [Private Network Names](#)
- [Configure Authentication Services](#)

## About Edge Clustering

The size of a single VMware SD-WAN VPN Network with an VMware SD-WAN Hub is constrained by the scale of the individual Hub. For large networks containing thousands of remote sites, it would be preferable for both scalability and risk mitigation to use multiple Hubs to handle the Edges. However, it is impractical to mandate that the customer manage individual separate Hubs to achieve this. Clustering allows multiple Hubs to be leveraged while providing the simplicity of managing those Hubs as one common entity with built-in resiliency.

SD-WAN Edge Clustering addresses the issue of SD-WAN Hub scale because it can be used to easily expand the tunnel capacity of the Hub dynamically by creating a logical cluster of Edges. Edge Clustering also provides resiliency via the Active/Active High Availability (HA) topology that a cluster of SD-WAN Edges would provide. A cluster is functionally treated as an individual Hub from the perspective of other Edges.

The Hubs in a VMware SD-WAN Cluster can be either physical or Virtual Edges. If they are virtual, they may exist on a single hypervisor or across multiple hypervisors.

Each Edge in a cluster periodically reports usage and load stats to the SD-WAN Gateway. The load value is calculated based on Edge CPU and memory utilization along with the number of tunnels connected to the Hub as a percentage of the Edge model's tunnel capacity. The Hubs within the cluster do not directly communicate nor exchange state information. Typically, Edge Clusters are deployed as Hubs in data centers.

---

**Note** Theoretically, Edge Clustering could be used to horizontally scale other vectors, such as throughput. However, the current Edge Clustering implementation has been specifically designed and tested to scale at tunnel capacity only.

---

## How Edge Clustering Works

This section provides an in-depth overview of how the SD-WAN Edge Clustering functionality works.

The following are important concepts that describe the SD-WAN Edge Clustering functionality:

- Edge Clustering can be used on Hubs as follows:
  - To allow greater tunnel capacity for a Hub than an individual Edge serving as a Hub can provide.
  - To distribute the remote Spoke Edges among multiple Hubs and reduce the impact of any incident that may occur.
- Cluster Score is a mathematical calculation of the overall utilization of the system as follows:

The three measured utilization factors are CPU usage, memory usage, and tunnel capacity.

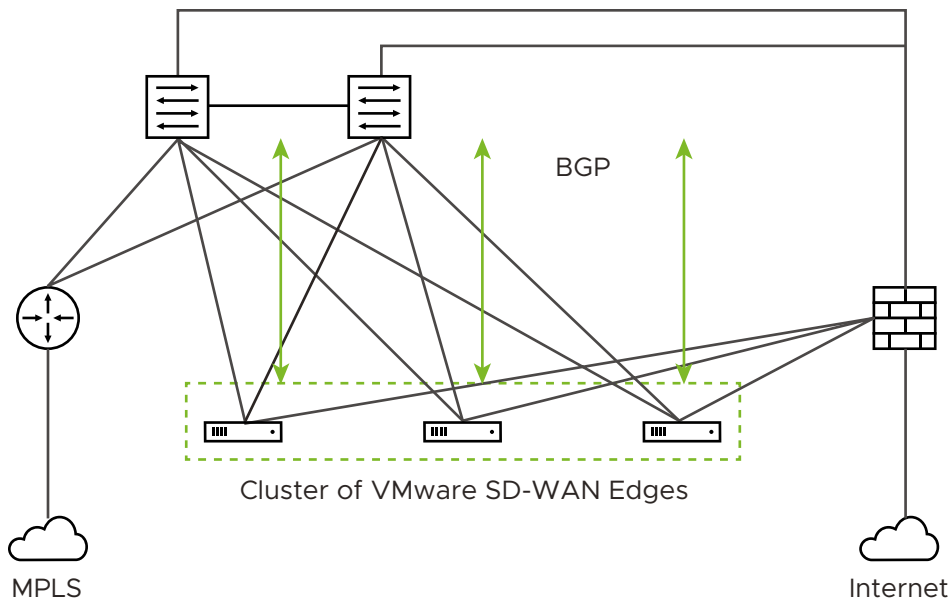
  - Each measure of utilization is treated as a percentage out of a maximum of 100%.
  - Tunnel capacity is based on the rated capacity for a given hardware model or Virtual Edge configuration.
  - All three utilization percentages are averaged to arrive at an integer-based Cluster Score (1-100).
  - While throughput is not directly considered, CPU and memory usage indirectly reflect throughput and flow volume on a given Hub.
  - For example, on an Edge 2000:
    - CPU usage = 20%
    - Memory usage = 30%
    - Connected Tunnels = 600 (out of a capacity of 6000) = 10%
    - Cluster Score:  $(20 + 30 + 10)/3 = 20$
- A Cluster Score greater than 70 is considered "over capacity."

- A “logical ID” is a 128-bit UUID that uniquely identifies an element inside the VMware SD-WAN Network.
  - For instance, each Edge is represented by a logical ID and each Cluster is represented by a logical ID.
  - While the user is providing the Edge and Cluster names, the logical IDs are guaranteed to be unique and are used for internal identification of elements.
- By default, the load is evenly distributed among Hubs. Hence, it is necessary that all Edges that are part of a cluster must be of the same model and capacity.

Each cluster member will have its own IP addressing for the WAN and LAN Interfaces. All the VMware SD-WAN Edges in the hub cluster are required to run a dynamic routing protocol, like eBGP, with the Layer 3 devices on the LAN side with a unique Autonomous System Number (ASN) for each cluster member. Dynamic routing on the clusters LAN side ensures that traffic from the DC to a particular Spoke site is routed through the appropriate Edge Cluster member.

### How are Edge Clusters tracked by the VMware SD-WAN Gateway?

Once a Hub is added to a VMware SD-WAN Cluster, the Hub will tear down and rebuild tunnels to all of its assigned Gateways and indicate to each Gateway that the Hub has been assigned to a Cluster and provide a Cluster logical ID.



For the Cluster, the SD-WAN Gateway tracks:

- The logical ID
- The name
- Whether Auto Rebalance is enabled
- A list of Hub objects for members of the Cluster

For each Hub object in the Cluster, the Gateway tracks:

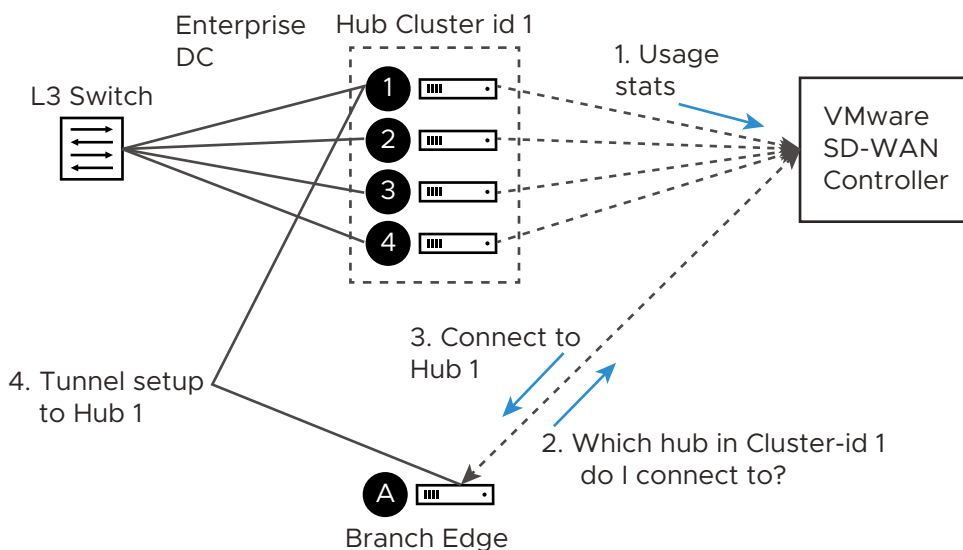
- The logical ID
- The name
- A set of statistics, updated every 30 seconds via a periodic message sent from the Hub to each assigned Gateway, including:
  - Current CPU usage of the Hub
  - Current memory usage of the Hub
  - Current tunnel count on the Hub
  - Current BGP route count on the Hub
- The current computed Cluster Score based on the formula provided above.

A Hub is removed from the list of Hub objects when the Gateway has not received any packets from the Hub Edge for more than seven seconds.

### How are Edges assigned to a specific Hub in a Cluster?

In a traditional Hub and Spoke topology, the SD-WAN Orchestrator provides the Edge with the logical ID of the Hub to which it must be connected. The Edge asks its assigned Gateways for connectivity information for that Hub logical ID—i.e. IP addresses and ports, which the Edge will use to connect to that Hub.

From the Edge’s perspective, this behavior is identical when connecting to a Cluster. The Orchestrator informs the Edge that the logical ID of the Hub it should connect to is the Cluster logical ID rather than the individual Hub logical ID. The Edge follows the same procedure of sending a Hub connection request to the Gateways and expects connectivity information in response.



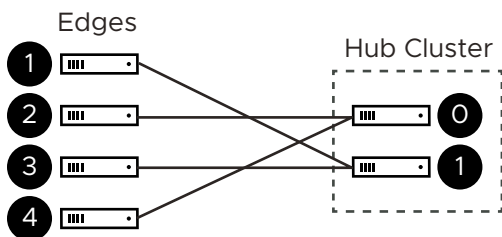
There are two divergences from basic Hub behavior at this point:

- **Divergence Number One:** The Gateway must choose which Hub to assign.
- **Divergence Number Two:** Due to Divergence Number One, the Edge may get different assignments from its different Gateways.

Divergence Number One was originally addressed by using the Cluster Score to assign the least loaded Hub in a Cluster to an Edge. While in practice this is logical, in the real world, it turned out to be a less than ideal solution because a typical reassignment event can involve hundreds or even thousands of Edges and the Cluster Score is only updated every 30 seconds. In other words, if Hub 1 has a Cluster Score of 20 and Hub 2 has a Cluster Score of 21, for 30 seconds all Edges would choose Hub 1, at which point it may be overloaded and trigger further reassignments.

Instead, the Gateway first attempts a fair mathematical distribution disregarding the Cluster Score. The Edge logical IDs, which were generated by a secure random-number generator on the Orchestrator, will (given enough Edges) have an even distribution of values. That means that using the logical ID, a fair share distribution can be calculated.

- Edge logical ID **modulo** the number of Hubs in Cluster = Assigned Hub index
- For example:
  - Four Edges that have logical IDs ending in 1, 2, 3, 4
  - Cluster with 2 Hubs
  - $1 \% 2 = 1$ ,  $2 \% 2 = 0$ ,  $3 \% 2 = 1$ ,  $4 \% 2 = 0$  (Note: "%" is used to indicate the modulo operator)
  - Edges 2 and 4 are assigned Hub Index 0
  - Edges 1 and 3 are assigned Hub Index 1



This is more consistent than a round-robin type assignment because it means that Edges will tend to be assigned the same Hub each time, which makes assignment and troubleshooting more predictive.

---

**Note** When a Hub restarts (e.g. due to maintenance or failure), it will be disconnected from the Gateway and removed from the Cluster. This means that Edges will always be evenly distributed following all Edges restarting (due to the above described logic), but will be unevenly distributed following any Hub event that causes it to lose connectivity.

---



## What happens when a Hub exceeds its maximum allowed tunnel capacity?

The Edge assignment logic will attempt to evenly distribute the Edges between all available Hubs. However, after an event (like restart) on the Hub, the Edge distribution will no longer be even.

---

**Note** Generally, the Gateway tries at initial assignment to evenly distributed Edges among Hubs, an uneven distribution is not considered an invalid state. If the assignments are uneven but no individual Hub exceeds 70% tunnel capacity, the assignment is considered valid.

---

Due to such an event on the Hub (or adding additional Edges to the network), Clusters might reach a point where an individual Hub has exceeded 70% of its permitted tunnel capacity. If this happens, and at least one other Hub is at less than 70% tunnel capacity, then fair share redistribution is performed automatically regardless of whether rebalancing is enabled on the Orchestrator. Most Edges will retain their existing assignment due to the predictive mathematical assignment using logical IDs, and the Edges that have been assigned to other Hubs due to failovers or previous utilization rebalancing will be rebalanced to ensure the Cluster is returned to an even distribution automatically.

## What happens when a Hub exceeds its maximum allowed Cluster Score?

Unlike tunnel percentage (a direct measure of capacity), which can be acted upon immediately, the Cluster Score is only updated every 30 seconds and the Gateway cannot automatically calculate what the adjusted Cluster Score will be after making an Edge reassignment. In the Cluster configuration, an Auto Rebalance parameter is provided to indicate whether the Gateway should dynamically attempt to shift the Edge load for each Hub as needed.

If Auto Rebalance is deactivated and a Hub exceeds a 70 Cluster Score (but not 70% tunnel capacity), then no action is taken.

If Auto Rebalance is enabled and one or more Hubs exceed a 70 Cluster Score, the Gateway will reassign one Edge per minute to the Hub with the lowest current Cluster Score until all Hubs are below 70 or there are no more reassignments possible.

---

**Note** Auto Rebalance is deactivated by default.

---

## What happens when two VMware SD-WAN Gateways give different Hub assignments?

As is the nature of a distributed control plane, each Gateway is making an individual determination of the Cluster assignment. In most cases, Gateways will use the same mathematical formula and thus arrive at the same assignment for all Edges. However, in cases like Cluster Score-based rebalancing this cannot be assured.

If an Edge is not currently connected to a Hub in a Cluster, it will accept the assignment from any Gateway that responds. This ensures that Edges are never left unassigned in a scenario where some Gateways are down and others are up.

If an Edge is connected to a Hub in a Cluster and it gets a message indicating it should choose an alternate Hub, this message is processed in order of “Gateway Preference.” For instance, if the Super Gateway is connected, the Edge will only accept reassignments from the Super Gateway. Conflicting assignments requested by other Gateways will be ignored. Similarly, if the Super Gateway is not connected, the Edge would only accept reassignments from the Alternate Super Gateway. For Partner Gateways (where no Super Gateways exist), the Gateway Preference is based on the order of configured Partner Gateways for that specific Edge.

### **What happens when a VMware SD-WAN Gateway goes down?**

When a SD-WAN Gateway goes down, Edges may be reassigned if the most preferred Gateway was the one that went down, and the next most preferred Gateway provided a different assignment. For instance, the Super Gateway assigned Hub A to this Edge while the Alternate Super Gateway assigned Hub B to the same Edge.

The Super Gateway going down will trigger the Edge to fail over to Hub B, since the Alternate Super Gateway is now the most preferred Gateway for connectivity information.

When the Super Gateway recovers, the Edge will again request a Hub assignment from this Gateway. In order to prevent the Edge switching back to Hub A again in the scenario above, the Hub assignment request includes the currently assigned Hub (if there is one). When the Gateway processes the assignment request, if the Edge is currently assigned a Hub in the Cluster and that Hub has a Cluster Score less than 70, the Gateway updates its local assignment to match the existing assignment without going through its assignment logic. This ensures that the Super Gateway, on recovery, will assign the currently connected Hub and prevent a gratuitous failover for its assigned Edges.

### **What happens if a Hub in a Cluster loses its dynamic routes?**

As noted above, the Hubs report to the SD-WAN Gateway the number of dynamic routes they have learned via BGP every 30 seconds. If routes are lost for only one Hub in a Cluster, either because they are erroneously retracted or the BGP neighborhood fails, the SD-WAN Gateway will failover Spoke Edges to another Hub in the Cluster that has an intact routing table.

As the updates are sent every 30 seconds, the route count is based on the moment in time when the update is sent to the SD-WAN Gateway. The SD-WAN Gateway rebalancing logic occurs every 60 seconds, meaning that users can expect failover to take 30-60 seconds in the unlikely event of total loss of a LAN-side BGP neighbor. To ensure that all Hubs have a chance to update the Gateways again following such an event, rebalancing is limited to a maximum of once per 120 seconds. This means that users can expect failover to take 120 seconds for a second successive failure.

### **How to configure Routing on Cluster Hubs?**

As the Gateway can instruct the spokes to connect to any member Hub of the Cluster, the routing configuration should be mirrored on all the Hubs. For example, if the spokes have to reach a BGP prefix 192.168.2.1 behind the Hubs, all the Hubs in the cluster should advertise 192.168.2.1 with the exact same route attributes.

BGP uplink community tags should be used in the cluster deployment. Configure the cluster nodes to set the uplink community tag when redistributing routes to BGP peers.

### What happens if a Hub in a Cluster fails?

The SD-WAN Gateway will wait for tunnels to be declared dead (7 seconds) before failing over Spoke Edges. This means that users can expect failover to take 7-10 seconds (depending on RTT) when an SD-WAN Hub or all its associated WAN links fail.

## Configure Edge Clustering

To configure Edge clusters:

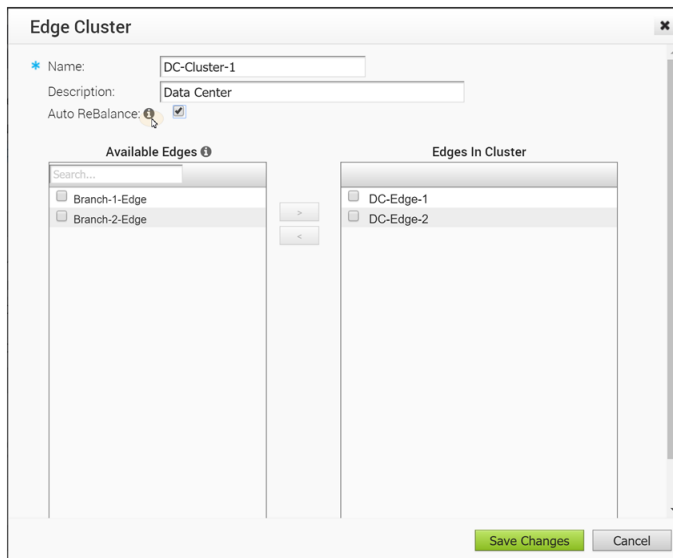
- 1 To access the **Edge Cluster** area, go to **Configure > Network Services**.

Edge Cluster			New Cluster	Delete Cluster
Name	Location	Used in Profiles		
<input type="checkbox"/> East Coast DC Cluster [ 3 Edges ]	n.a.	1 Profile 1 Edge		

- 2 If necessary, add a new cluster:
  - a From the **Edge Cluster** area, click the **New Cluster** button.
  - b In the **Edge Cluster** dialog box, enter the name and description in the appropriate text boxes. (See image below).
  - c If required, select the **Auto Rebalance** checkbox.

**Note** As stated in the **Auto Rebalance** tool tip in the VCO: If this option is enabled, when an individual Edge in a Hub cluster exceeds 70% aggregate utilization, we will rebalance spokes at the rate of one spoke per minute until utilization is reduced by 70%. This rebalancing will cause VPN tunnels to disconnect and may cause up to 6-10 seconds of downtime to prevent overloading of individual Hubs. If all in a Hub cluster exceed 70%, no

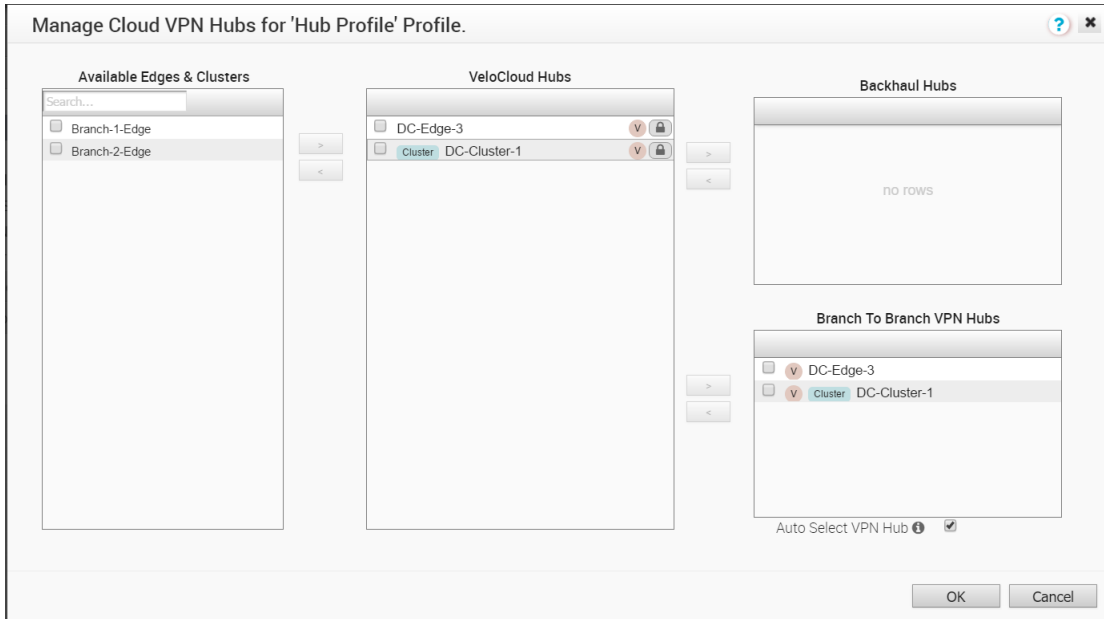
rebalancing will be performed.



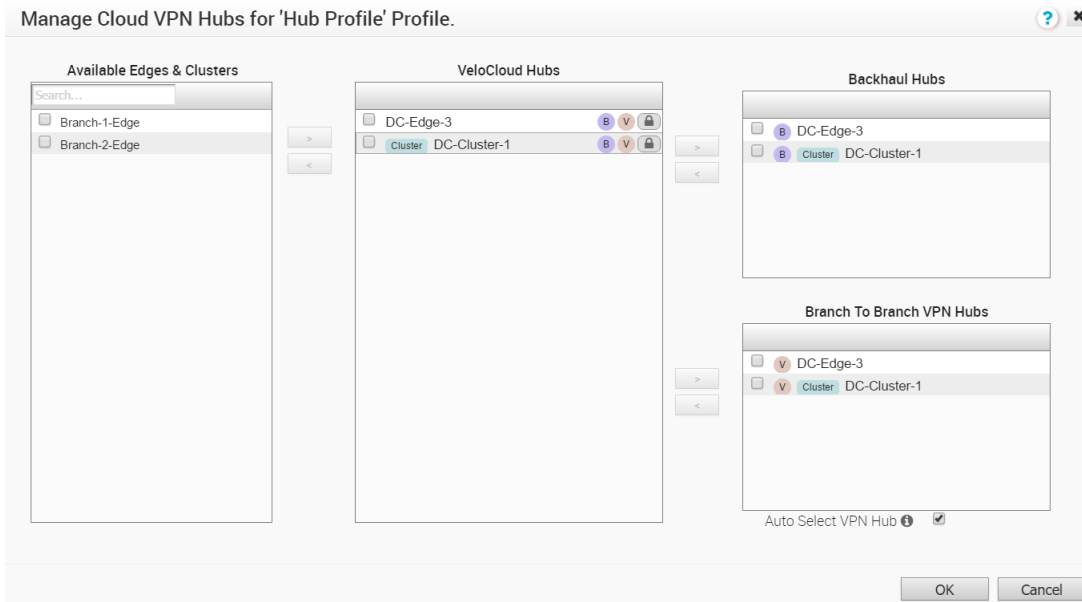
- d In the **Available Edges** section, select an Edge and (using the arrow) move it to the **Edges In Cluster** section.
- e Click **Save Changes**.

**Note** Edges used as a Hub or in Hub Clusters, or configured as an Active Standby HA pair are not displayed in the **Available Edges** list area.

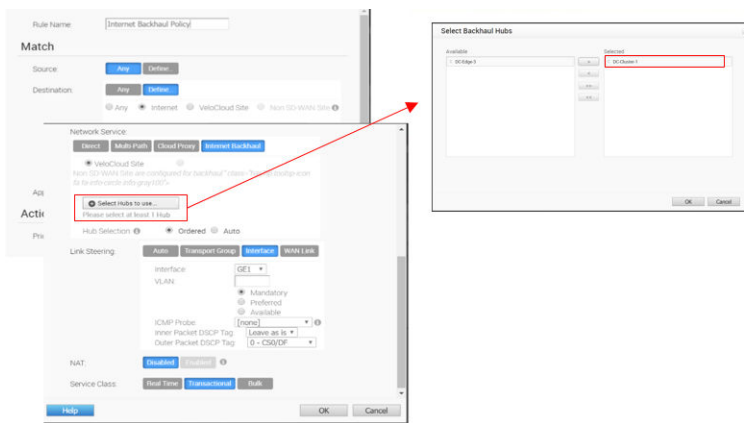
- 3 An Edge Cluster and an individual Edge can be simultaneously configured as Hubs in a branch profile. Once Edges are assigned to a Cluster, they cannot be assigned as individual Hubs. Choose an Edge Cluster as a Hub in the Branch Profile.



- Branch to Branch VPN using Hubs functions the same regardless of whether the Hubs are Clusters or individual Edges. In order to configure Branch to Branch VPN using Hubs that are also Edge Clusters, you can select a Hub from the **VeloCloud Hubs** area and move it to the **Branch to Branch VPN Hubs** area.



- Hub Clusters can also be configured as Internet Backhaul Hubs in the business policy configuration by selecting a Hub from the **VeloCloud Hubs** area and move it to **Backhaul Hubs** area ( **Business Policy Match** dialog) and above ( **Backhaul Hubs** area).



**Note** It is mandatory to run a dynamic routing protocol, like eBGP, on the LAN side of the clusters.

## Cloud VPN Hubs & Backhaul Sites (Summary View)

The Cloud VPN Hubs and Backhaul Sites are Read Only. You cannot configure them from this screen. Hub roles from different profiles appear as a summary view only.

Cloud VPN Edge Hubs				
VeloCloud Hub	Location	Used in Profiles	VPN Hub ⓘ	Backhaul Hub ⓘ
XEN12-DATACENTER-I	US, DC, Washington	BRANCHES	✘	✘
XEN12-DATACENTER-II	US, TX	BRANCHES	✘	✘

## Configure a Non-VeloCloud Site

VeloCloud supports the following Non-VeloCloud Site configurations:

- Check Point
- Cisco ASA
- Cisco ISR
- Generic IKEv2 Router (Route Based VPN)
- Microsoft Azure Virtual Hub
- Palo Alto
- SonicWALL
- Zscaler
- Generic IKEv1 Router (Route Based VPN)
- Generic Firewall (Policy Based VPN)

---

**Note** VeloCloud now supports both Generic IKEv1 Router (Route Based VPN) and Generic IKEv2 Router (Route Based VPN) Non-VeloCloud Site Configurations.

---

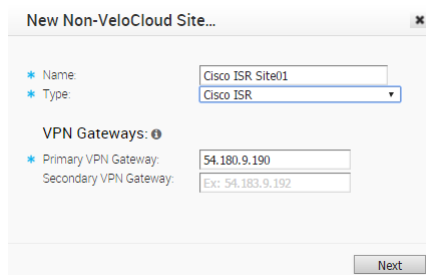
### Cisco ISR

Cisco ISR is one of the more common third party configurations. Instructions on how to configure with Cisco ISR in the VeloCloud Orchestrator are listed below.

To configure via Cisco ISR:

- 1 Go to **Configure > Network Services**.
- 2 In the **Non-VeloCloud Sites** area, click the **New** button.

The New Non-VeloCloud Site dialog box appears.



- 3 In the **New Non-VeloCloud Site** dialog box:
  - a Enter the name of your site.
  - b Select **Cisco ISR** from the **Type** drop-down menu.
  - c Type in the Primary VPN Gateway (and the Secondary VPN Gateway if necessary).
- 4 Click **Next**.

Your Non-VeloCloud Site is created, and a dialog box for your Non-VeloCloud Site appears. (See image below).

**Cisco ISR Site01**

\* Name: Cisco ISR Site01  
 Type: Cisco ISR  
 Enable Tunnel(s):

Primary VPN Gateway:  
 \* Public IP: 54.180.9.190  
 Tunnel Settings:  
 PSK: [masked]  
 Encryption: AES 128  
 DH Group: 2  
 PFS: disabled

Secondary VPN Gateway: Add

Redundant VeloCloud Cloud VPN:

Site Subnets

Subnet	Description	Advertise
10.0.3.0/27	(optional)	<input checked="" type="checkbox"/>

Source NAT IP: 10.0.5.2

Buttons: Help, Advanced, View IKE/IPSec Template, Save Changes, Close

- 5 In the dialog box for your Non-VeloCloud Site:
  - a Click the **Advanced** button located at the bottom of the dialog box.
  - b If not already selected, check the **Enable Tunnel(s)** checkbox.
  - c The VeloCloud Orchestrator generates a PSK by default. If you want to use your own PSK, type it in the **PSK** text box.
  - d Type in the Subnet and description for your site.
  - e To add a Secondary VPN Gateway click the **Add** button.
  - f To provide an optimal Source NAT IP to translate the source IP address, type the IP in the **Source NAP IP** text box.
  - g Click **Save Changes**.

---

**Note** The **View IKE/IPSec Template** button shows a sample configuration of the PSK and IP details that would be useful to configure a Non-VeloCloud Site.

---

## Cisco ASA

Cisco ASA is another common third party configuration. Instructions on how to configure with Cisco ASA in the VeloCloud Orchestrator are listed below.

To configure via Cisco ASA:

- 1 Go to **Configure > Network Services**.
- 2 In the **Non-VeloCloud Sites** area, click the **New** button.

The **New** Non-VeloCloud Site dialog box appears.

- 3 In the **New Non-VeloCloud Site** dialog box:
  - a Enter the name of your site.
  - b Select **Cisco ASA** from the **Type** drop-down menu.
  - c Type in the Primary VPN Gateway (and Secondary if necessary).
- 4 Click **Next**.

Your Non-VeloCloud Site is created, and a dialog box for your Non-VeloCloud Site appears.



### Cisco ASA Site01 ✕

\* Name:

Type: Cisco ASA

Enable Tunnel(s):

Primary VPN Gateway:

\* Public IP:

Tunnel Settings: ⓘ

PSK:

Encryption: AES 128 ▾

DH Group: 2 ▾

PFS: disabled ▾

Secondary VPN Gateway: ✕

Secondary VPN Gateways are not supported for Cisco ASA. This is a limitation of the Cisco ASA VPN.

Redundant VeloCloud Cloud VPN: ⓘ

Help

Advanced

View IKE/IPSec Template

Save Changes

Close

**Site Subnets**

Subnet	Description	Advertise		
10.0.2.0/24	Cisco ASA Site01	<input checked="" type="checkbox"/>	-	+

**Custom Source Subnets:** ⓘ

Subnet	Description	Advertise		
Ex: 10.0.2.0/24	(optional)	<input checked="" type="checkbox"/>	-	+

Source NAT IP: ⓘ

- 5 In the dialog box for your Non-VeloCloud Site:
  - a Click the **Advanced** button located at the bottom of the dialog box.
  - b If not already selected, select the **Enable Tunnel(s)** checkbox.
  - c The VeloCloud Orchestrator generates a PSK by default. If you want to use your own PSK, type it in the **PSK** text box.
  - d To add a Secondary VPN Gateway, click the **Add** button.
  - e Type in the Subnet and description for your site. (Type in Custom Source Subnets if necessary).
  - f To provide an optimal Source NAT IP if to translate the source IP address, type the IP in the **Source NAP IP** text box.
  - g Click **Save Changes**.

---

**Note** The **View IKE/IPSec Template** button shows a sample configuration of the PSK and IP details that would be useful to configure a Non-VeloCloud Site.

---

## Microsoft Azure Virtual Hub

Microsoft Azure Virtual Hub is one of the more common third party configurations. For instructions on how to configure a Non-VeloCloud Site (NVS) of type Microsoft Azure Virtual Hub in VeloCloud Orchestrator, see [Configure a Microsoft Azure Non-VeloCloud Site](#).

## Configure Check Point

The VeloCloud Gateway connects to the Check Point CloudGuard service using IKEv1/IPsec. There are two steps to configure Check Point: Configuring the Checkpoint CloudGuard service and Configuring Checkpoint on the VeloCloud Orchestrator. You will perform the first step on the Check Point Infinity Portal and the second step on the VeloCloud Orchestrator.

**Click the links for the following sections below to complete the instructions to configure Check Point.**

Step 1: [Step 1: Configure the Check Point CloudGuard Connect](#)

Step 2: [Step 2: Configure Check Point as the Non-VeloCloud Site on the VeloCloud Orchestrator](#)

### Prerequisites

You must have an active Check Point account and login credentials to access Check Point's Infinity Portal.

### Step 1: Configure the Check Point CloudGuard Connect

Step 1 instructions on how to configure the Check Point CloudGuard Service.

You must have an active Check Point account and login credentials to access Check Point's Infinity Portal.

### Procedure

- 1 To configure the Check Point CloudGuard service, login to Check Point's Infinity Portal at (<https://portal.checkpoint.com/>).
- 2 Once logged in, create a site at Check Point's Infinity Portal via the following link: <https://sc1.checkpoint.com/documents/integrations/VeloCloud/check-point-VeloCloud-integration.html>

After you create a site at Check Point's Infinity Portal, you're ready to complete Step 2: [Step 2: Configure Check Point as the Non-VeloCloud Site on the VeloCloud Orchestrator](#)

### Step 2: Configure Check Point as the Non-VeloCloud Site on the VeloCloud Orchestrator

After you create a site at Check Point's Infinity Portal, complete step two instructions on how to configure Check Point as the Non-VeloCloud Site on the VeloCloud Orchestrator.

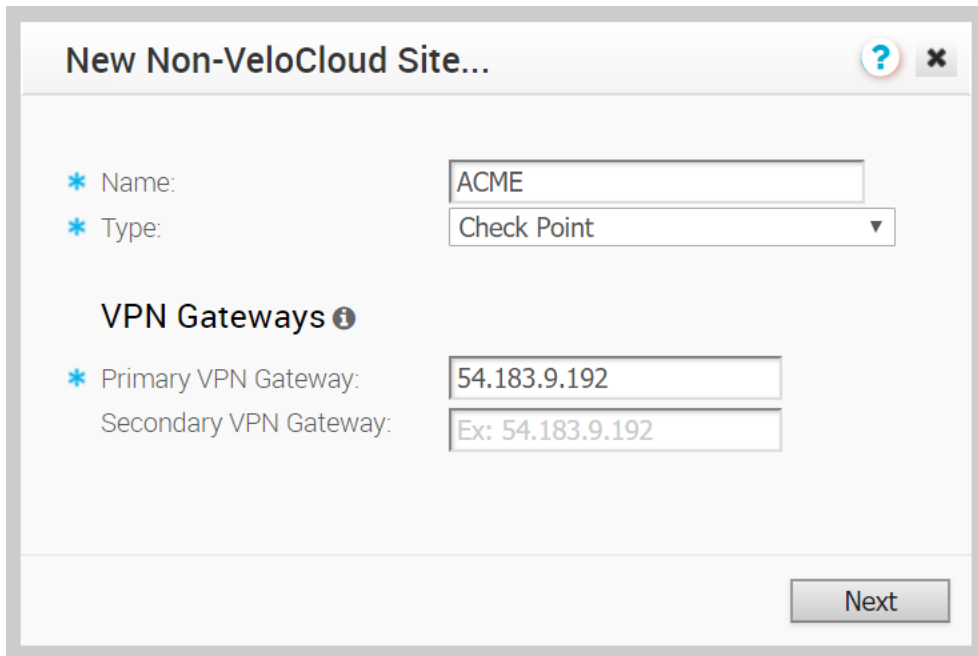
After you create a site at Check Point's Infinity Portal, complete the steps below:

### Procedure

- 1 From the VeloCloud Orchestrator, go to **Configure > Network Services**

- 2 In the **Non-VeloCloud Sites** area, click the **New** button.

The **New Non-VeloCloud Site** dialog box appears.



**New Non-VeloCloud Site...**

\* Name:

\* Type:

**VPN Gateways** ⓘ

\* Primary VPN Gateway:

Secondary VPN Gateway:

Next

- 3 Complete the following sub steps in the **New Non-VeloCloud Site** dialog box:
  - a Enter the Name of your site.
  - b Select Check Point from the **Type** drop-down menu.

- c Type in the Primary VPN Gateway (and the Secondary VPN Gateway if necessary).
- d Click **Next**.

A dialog box for your Non-VeloCloud Site appears. (image below).

**Note** To configure tunnel settings to the Non-VeloCloud site's Primary VPN Gateway, click the Advanced button located at the bottom of the dialog box. Any changes made to Encryption, DH Group, or PFS will also be applied to the redundant tunnel configuration. After saving your changes, update the site's primary VPN Gateway device. Click on the "View IKE/IPSec Template" button for details.

- 4 In the Primary VPN Gateway area, of the dialog box of your Non-VeloCloud Site (image above):
  - a **PSK text box:** Enter the Pre-Shared Key that was configured on the Check Point infinity portal. Do not configure redundant IPsec tunnels (keep the checkbox for **Redundant VeloCloud Cloud VPN** unchecked).
  - b **Encryption drop-down menu:** The Encryption should be set to the same algorithm that was configured on the checkpoint infinity portal.
  - c **DH Group:** The DH group should be set to the same value that was configured on the checkpoint infinity portal.
  - d For the purposes of this specific Check Point configuration, choose **disabled** from PFS drop-down menu.
- 5 To add a Secondary VPN Gateway click the **Add** button. Clicking the **Save Changes** button will immediately create the Secondary VPN Gateway for this site and provision a VeloCloud VPN tunnel to this Gateway.
- 6 As mentioned in Step 4a above, leave the **Redundant VeloCloud Cloud VPN** checkbox unchecked.

- 7 For the purposes of the Check Point configuration, choose **Default** from the Local Auth Id drop-down menu.
- 8 For the purposes of the Check Point configuration, check the **Disable Site Subnets** checkbox.
- 9 Click **Save Changes**.
- 10 Check the **Enable Tunnel(s)** checkbox once you are ready to initiate the tunnel from the VeloCloud Gateway to the Check Point CloudGuard VPN gateways.

## Configure Amazon Web Services (AWS)

This section describes Amazon Web Services (AWS) configuration.

The Amazon Web Services (AWS) configuration consists of two major steps (with multiple steps within each one).

- 1 Obtain Public IP, Inside IP, and PSK details from the Amazon Web Services website.
- 2 Enter the details you obtained from the AWS website into the “Non-VeloCloud Network Service” in the VeloCloud Orchestrator.

To configure using Amazon Web Services, complete the instructions in the following section.

### Obtain Amazon Web Services Configuration Details

This section describes how to obtain Amazon Web Services configuration details.

When using Amazon Web Services for your configurations, refer to the instructions in Amazon's documentation (Amazon Virtual Private Cloud Network Administrator Guide), which can be found at: <http://awsdocs.s3.amazonaws.com/VPC/latest/vpc-nag.pdf>. Reference the following section, "Example: Generic Customer Gateway without Border Gateway" on page 79 for specific configuration instructions .

- 1 From Amazon's Web Services, create VPC and VPN Connections. (See section above for the link on how to access the Amazon Web Services to complete this step).
- 2 Make note of the VeloCloud gateways associated with the enterprise account in the VeloCloud Orchestrator that might be needed to create a virtual private gateway in the Amazon Web Services.
- 3 Make a note of the Public IP, Inside IP and PSK details associated with the Virtual Private Gateway. You will enter this information in the VeloCloud Orchestrator when you create a Non-VeloCloud Site.

### Configure a Non-VeloCloud Site

Once you obtain Public IP, Inside IP, and PSK information from the Amazon Web Services website, you can configure a Non-VeloCloud Site.

To configure a Non-VeloCloud Site:

- 1 Go to **Configure > Network Services**.
- 2 In the **Non-VeloCloud Sites** area, click the **New** button.

The **New** Non-VeloCloud Site dialog box appears.

- 3 In the **New Non-VeloCloud Site** dialog box:
  - a Enter the name of your site.
  - b Select **Generic Router (Route Based VPN)** from the **Type** drop-down menu.
  - c Type in the Primary VPN Gateway (and the Secondary VPN Gateway if necessary).
  - d Click **Next**.

Your Non-VeloCloud Site is created, and a dialog box for your Non-VeloCloud Site appears.

- 4 In the dialog box for your Non-VeloCloud Site:
  - a Click the **Advanced** button located at the bottom of the dialog.
  - b If not already selected, select the **Enable Tunnel(s)** checkbox.
  - c Type in the Site Subnet(s) and description. (Enter the network which is behind the VPN firewall / router and can be exposed to branches for access).
  - d To provide an optimal Source NAT IP to translate the source IP address, type the IP in the **Source NAT IP** text box.
  - e Add the PSK details and the Public IP you obtained from the Amazon Web Services site.
  - f Select the **Redundant VeloCloud Cloud VPN** checkbox to establish redundant tunnels on a second gateway. This functionality establishes a redundant tunnel from a redundant VeloCloud Gateway to the Non-VeloCloud Site.
  - g Click **Save Changes**.


---

**Note** The **View IKE/IPSec Template** button shows a sample configuration of the PSK and IP details that would be useful to configure a Non-VeloCloud Site.

---

**Amazon Site01**

\* Name: Amazon Site01  
 Type: Generic Router (Route Based VPN)  
 Enable Tunnel(s):

Primary VPN Gateway:  
 \* Public IP: 54.184.9.194  
 Tunnel Settings:  
 PSK: .....   
 Encryption: AES 128  
 DH Group: 2  
 PFS: 2

Secondary VPN Gateway: Add

Redundant VeloCloud Cloud VPN:

**Site Subnets**


Subnet	Description	Advertise
172.15.0.0/15	Amazon01-Subnet-1	<input type="checkbox"/> - +
172.24.0.0/16	Amazon01-Subnet-1	<input type="checkbox"/> - +

Disable Site Subnets

Source NAT IP: 10.0.2.5

Authentication: None

Buttons: Help, Advanced, View IKE/IPSec Template, Save Changes, Close

**Note** You can click the  symbol next to the PSK to change to a visible display.

For more information about VeloCloud Orchestrator Network Services documentation, go to [Chapter 9 Configure Network Services](#).

## Configure Zscaler

The Zscaler configuration includes four major steps. You must perform all four steps to complete this configuration.

The first three major steps include setting up a VPN IPsec tunnel gateway between VeloCloud and Zscaler, and the last step requires that you set up business rules. Complete the following configuration steps:

- 1 Create and Configure a Non-VeloCloud Site.
- 2 Add a Non-VeloCloud Site to the Configuration Profile.
- 3 Zscaler Configuration: Create an account, add V'PN credentials, add a location.
- 4 Configure Business Priority Rules.

**Note** You will perform Step 1, Step 2, and Step 4 in the VeloCloud Orchestrator. You will perform Step 3 at the Zscaler site.

## Step 1: Create and Configure a Non-VeloCloud Site

To create and configure a non-VeloCloud site:

- 1 From the navigation panel in the VCO, go to **Configure > Network Services**.

The **Services** screen appears.

- 2 In the **Non-VeloCloud Sites** area, click the **New** button.

The **New** Non-VeloCloud Site dialog box appears.



**New Non-VeloCloud Site...**

\* Name: Zscaler Site01

\* Type: Zscaler

**VPN Gateways:** ⓘ

\* Primary VPN Gateway: 54.183.9.193

Secondary VPN Gateway: Ex: 54.183.9.192

Next

- 3 In the **New Non-VeloCloud Site** dialog box:

- a Enter the name of your site.
- b Select **Zscaler** from the **Type** drop-down menu.
- c Type in the Primary VPN Gateway (and Secondary if necessary).
- d Click **Next**.

Your Non-VeloCloud Site is created, and a dialog box for your Non-VeloCloud Site appears.



**Zscaler West Coast Site**

\* Name: Zscaler West Coast Site  
 Type: Zscaler  
 Enable Tunnel(s):

Primary VPN Gateway:  
 \* Public IP: 54.183.9.193  
 Tunnel Settings:  
 PSK: [Redacted]

Source NAT IP: Ex: 10.0.2.5  
 Authentication: User FQDN  
 velocloud01@velocloud.net


Secondary VPN Gateway: Add

Redundant VeloCloud Cloud VPN:

Buttons: Help, Advanced, View IKE/IPSec Template, Save Changes, Close

- 4 In the dialog box for your Non-VeloCloud Site:
  - a Click the **Advanced** button located at the bottom of the dialog box.
  - b If not already selected, select the **Enable Tunnel(s)** checkbox.
  - c Select the **Disable Site Subnets** checkbox.
  - d In the **Authentication** drop-down menu, choose **User FQDN** and type in the domain address.
  - e Copy the **User FQDN** domain address and the **PSK**. (You will need this information when you set up your VPN Credentials in your Zscaler account).

---


**Note** You can click the  symbol next to the PSK to change the PSK information to a visible display.

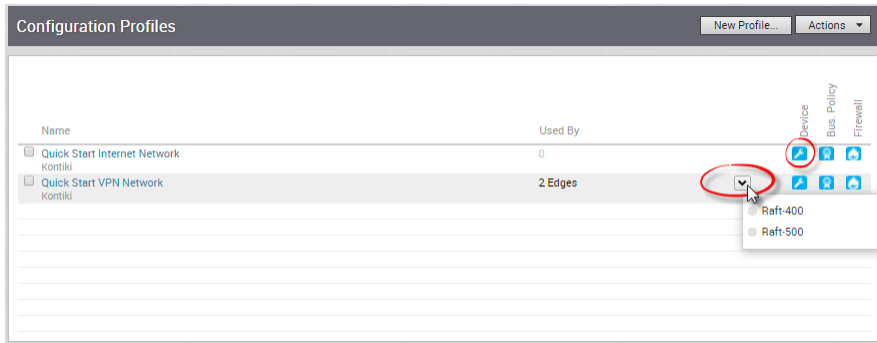
---

- f Click **Save Changes**.

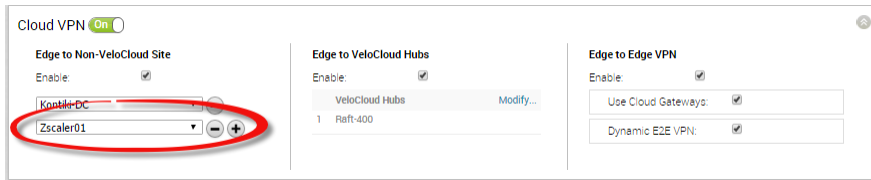
## Step 2: Add to a Configuration Profile

To add to a configuration profile:

- 1 From the navigation panel in the VCO, go to **Configure > Profiles**.
- 2 In the **Configure Profiles** screen, click the **Devices** icon  to the right of your profile. (For multiple Edges, use the drop-down menu to select your Edge, then click the **Device** tab).



- 3 From the **Cloud VPN** area, click the **+** symbol, and choose your Non-VeloCloud Site from the drop-down menu.




---

**Note** You can also create a new Non-VeloCloud Site from the Cloud VPN area. After you click the **+** symbol, choose **New Non-VeloCloud Site ...** from the drop-down menu.

---

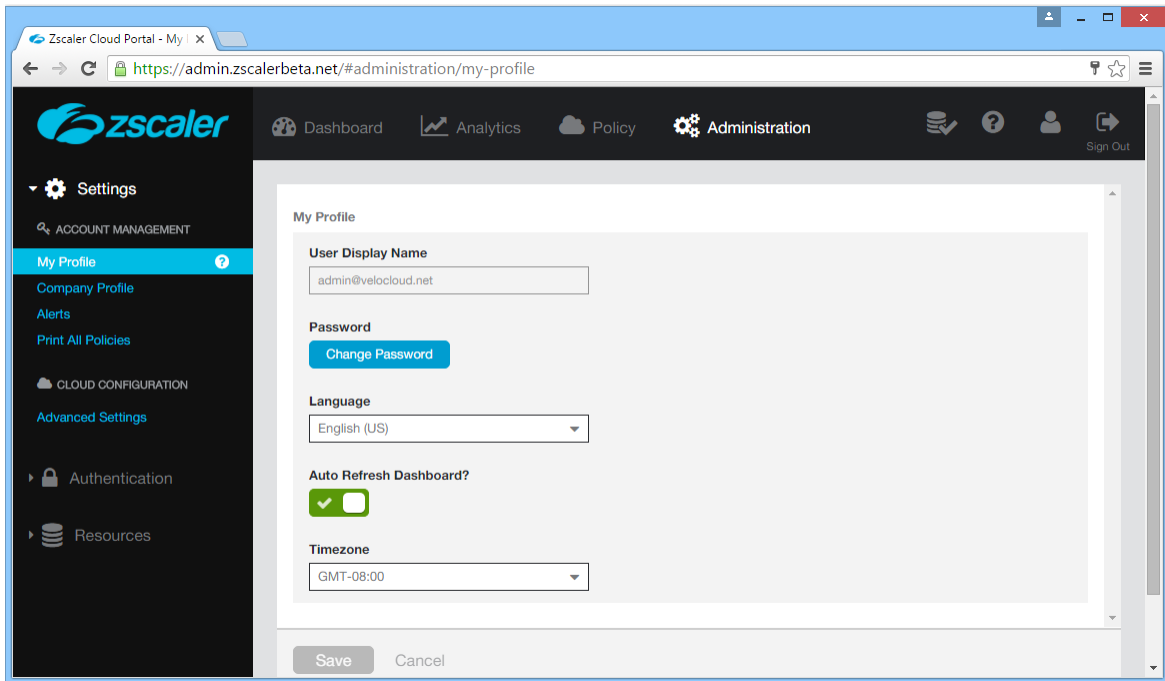
- 4 Click **Save Changes**.

### Step 3: Configure Zscaler

This section describes Zscaler configuration.

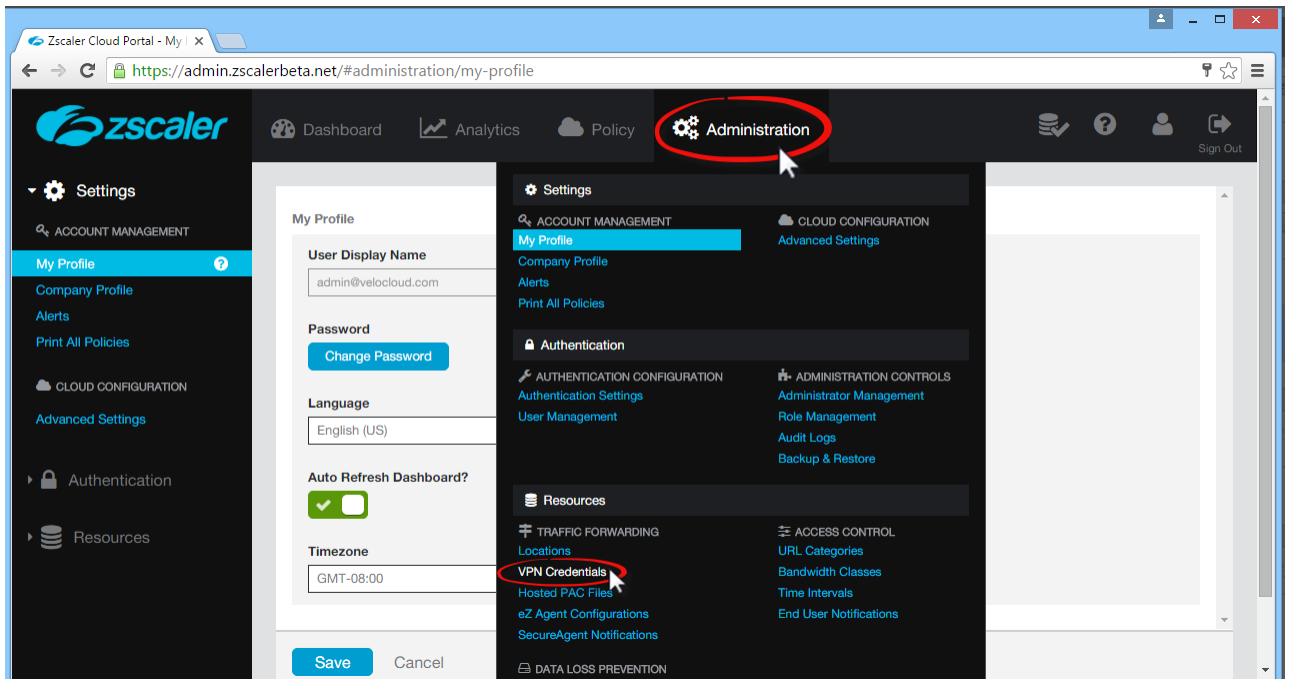
Complete the following these steps on the Zscaler website. From there, you will create a Zscaler account, add VPN credentials, and add a location.

- 1 From the Zscaler website, create a Zscaler web security account.

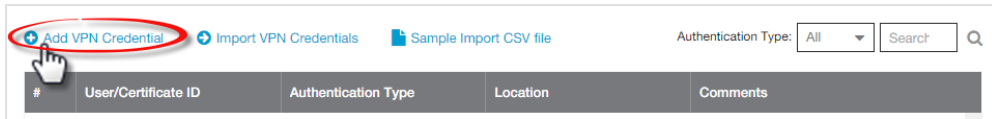


2 Set up your VPN Credentials:

- a At the top of the Zscaler screen, hover over the **Administration** option to display the drop down menu. (See image below).
- b Under **Resources**, click **VPN Credentials**.

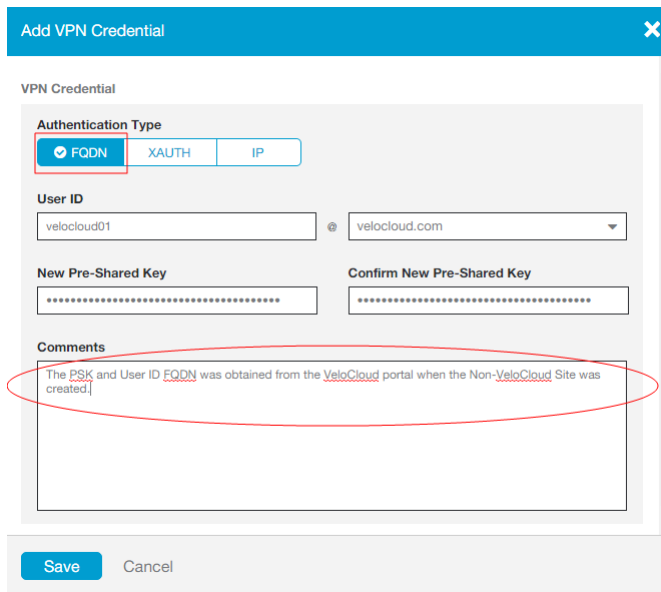


- c Click **Add VPN Credentials** at the top left corner.



d From the **Add VPN Credential** dialog box:

- 1 Choose **FQDN** as the Authentication Type.
- 2 Type the User ID and Pre-Shared Key (PSK). You obtained this information from your Non-VeloCloud Site's dialog box from the VCO.
- 3 If necessary, type in any comments in the **Comments** section.




4 Click **Save**.

3 Assign a location:

- a At the top of the Zscaler screen, hover over the **Administration** option to display the drop-down menu.
- b Under **Resources**, click **Locations**.
- c Click **Add Location** at the top left corner.
- d In the **Add Location** dialog box (see image below):
  - 1 Complete the text boxes in the Location area (Name, Country, State/Province, Time Zone).
  - 2 Choose **None** from the **Public IP Addresses** drop-down menu.
  - 3 In the **VPN Credentials** drop-down menu, select the credential you just created. (See image below).
  - 4 Click **Done**.
  - 5 Click **Save**.

## Step 4: Configure Business Priority Rules

To define the business policy in your VCO to determine web security screening:

- 1 From the navigation panel in the VCO, go to **Configure > Edges**.
- 2 In the **VeloCloud Edges** screen, click the **Bus. Policy** icon  for your Edge.
- 3 Click the **New Rule** button.
  - a In the **Rule** dialog box:
    - 1 Type in a name for the rule in the **Rule Name** textbox.
    - 2 In the **Destination** area of the **Match** section, choose your options. (Example options are shown below):
      - a Click the **Define** button.
      - b Choose **Internet**.
      - c Choose **TCP** from the **Protocol** drop-down menu.
      - d Type your port in the **Ports** text box. The image below shows an example using the port 80 option. VeloCloud recommends using port 80 or port 443. See note at the end of this section for more information.

- 3 In the **Action** area, choose your options. (Example options are shown below):
  - a For **Priority**, choose **Normal**.
  - b For **Network Service**, click **Internet Backhaul** and choose your Non-VeloCloud Site from the drop down menu.
  - c For **Link Steering**, choose an option (for example, **by Service Group**).
  - d For **Service Class**, choose **Transactional**.
- b Click **OK**.

The screenshot shows a configuration window for a rule named "Zscaler 80". The window is divided into several sections:

- Match:**
  - Source: **Any** (selected), Define...
  - Destination: **Any** (selected), Define...
    - Radio buttons:  Any,  Internet,  VeloCloud Site,  Non-VeloCloud Site
    - IP Address:
    - Hostname:
    - Protocol:
    - Ports:
- Application: **Any** (selected), Define...

- Action:**
- Priority:  High,  Normal,  Low
- Rate Limit
- Network Service: **Direct**, **Internet Multi-Path**, **Cloud Proxy**, **Internet Backhaul** (selected)
  - Radio buttons:  VeloCloud Site,  Non-VeloCloud Site
  - Site:
- Link Steering: **by Service Group** (selected), by Interface, by WAN Link
  - Service Group:
  - Radio buttons:  Mandatory,  Preferred,  Available
- Service Class:  Real Time,  Transactional,  Bulk

Buttons: OK, Cancel

**Note** VeloCloud recommends business policy rules to Backhaul web traffic, specifically port 80 and 443. You can send all Internet traffic to Backhaul Zscaler. An image example using port 443 is shown below.

Rule Name:

### Match

Source:

Destination:

Any
  Internet
  VeloCloud Site
  Non-VeloCloud Site

IP Address:

Hostname <sup>i</sup>:

Protocol:

Ports:

Application:

### Action

Priority:

Rate Limit

Network Service:    i

VeloCloud Site
  Non-VeloCloud Site

Site:

Link Steering:   i

Service Group: 

- Mandatory
- Preferred
- Available

Service Class:

## Configuration Tasks

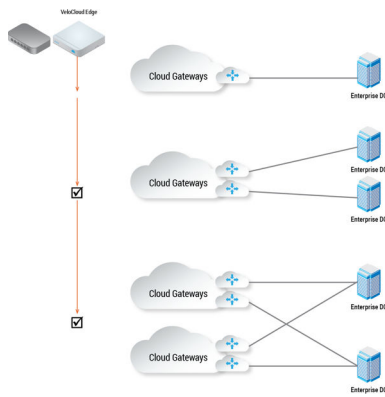
This section describes configuration tasks for NVS.

### VPN Workflow

This is an optional service that allows you to create VPN tunnel configurations to access one or more Non-VeloCloud Sites. The VeloCloud provides the configuration required to create the tunnel(s) – including creating IKE IPsec configuration and generating a pre-shared key.

#### Overview

The following figure shows an overview of the VPN tunnels that can be created between the VeloCloud and a Non-VeloCloud Site.



**Note** It is required that an IP address be specified for a Primary VPN Gateway at the Non-VeloCloud Site. The IP address is used to form a Primary VPN Tunnel between a VeloCloud Gateway and the Primary VPN Gateway.

Optionally, an IP address can be specified for a Secondary VPN Gateway to form a Secondary VPN Tunnel between a VeloCloud Gateway and the Secondary VPN Gateway. Using Advanced Settings, Redundant VPN Tunnels can be specified for any VPN tunnels you create.

### Add Non-VeloCloud Site VPN Gateway

Enter a Name and chose a gateway Type (Cisco ASA, Cisco ISR, Palo Alto, SonicWall, or Generic). Specify the IP address for the Primary VPN Gateway and, optionally, specify an IP address for a Secondary VPN Gateway.

## New Non-VeloCloud Site ✕

\* Name:

\* Type:

**VPN Gateways:** ⓘ

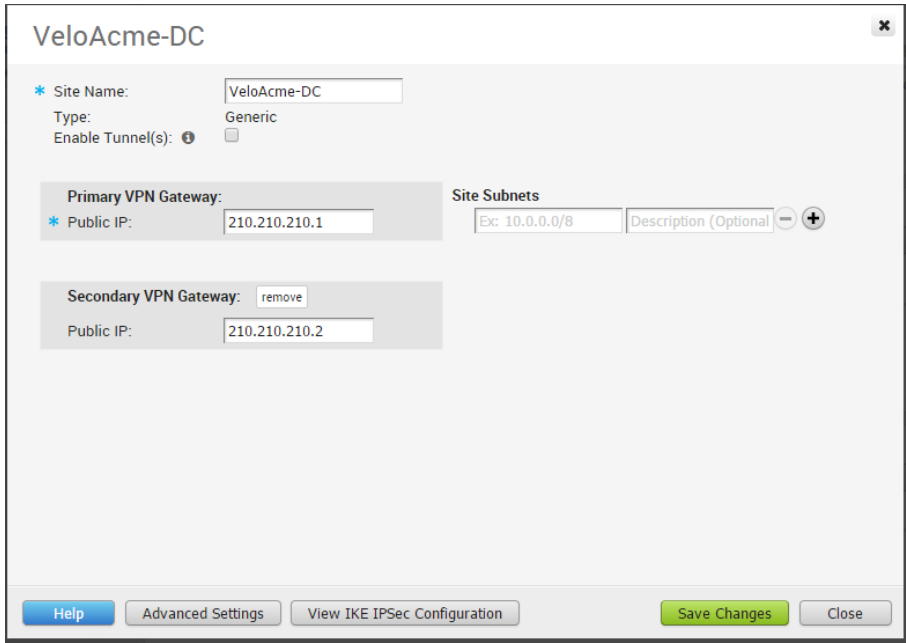
\* Primary VPN Gateway IP:

Secondary VPN Gateway IP:

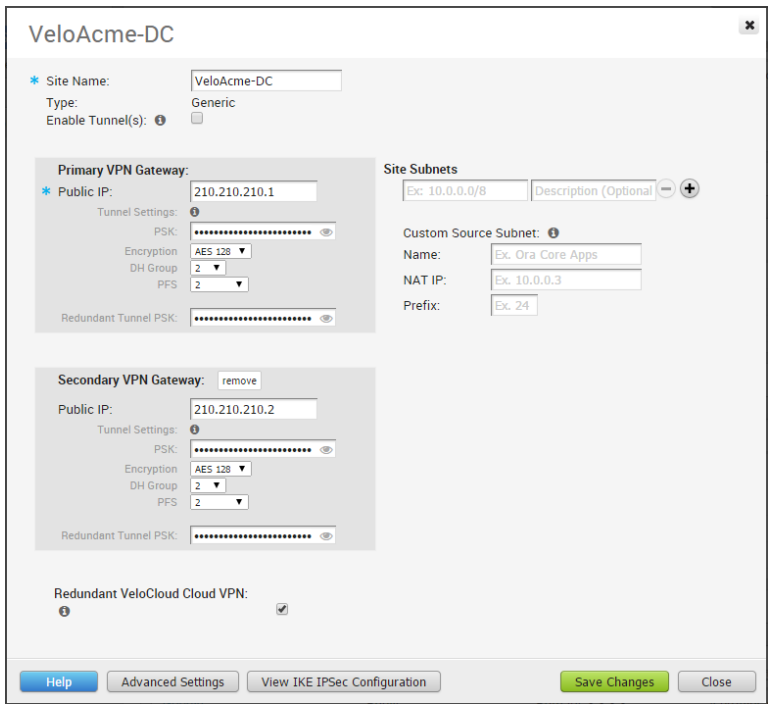
### Configure Non-VeloCloud Site Subnets

Once you have created a Non-VeloCloud Site configuration, you can add subnets using the following dialog box.



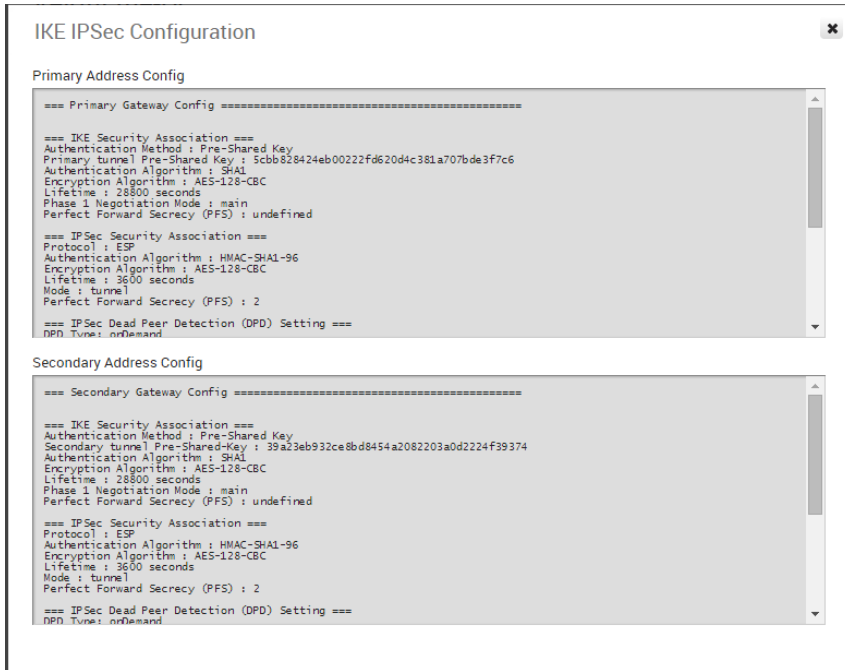


Click the **Advanced Settings** button to enter additional subnet parameters, VPN Gateway parameters, and to add Redundant VPN tunnel(s).



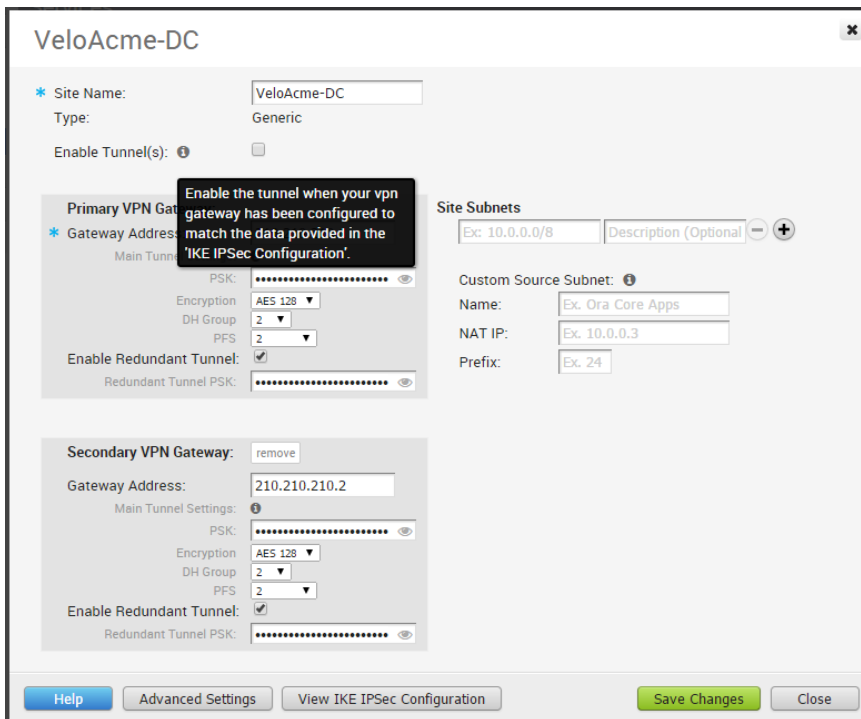
**View IKE IPsec Configuration, Configure Non-VeloCloud Site Gateway**

If you click the View IKE IPsec Configuration button, the information needed to configure the Non-VeloCloud Site Gateway appears. The Gateway administrator should use this information to configure the Gateway VPN tunnel(s).



### Enable IPSec Tunnel

The Non-VeloCloud Site VPN tunnel is initially disabled. You must enable the tunnel(s) after the Non-VeloCloud Site Gateway has been configured and before first use of the Edge-to-Non-VeloCloud Site VPN.



## Configure Cloud Proxy

This is an optional service that allows you to create a cloud proxy configuration for Cloud Web Security. The service can be a Websense Web Proxy or a Generic Web Proxy.

To create a cloud proxy:

- 1 In the **New Cloud Proxy** dialog box, specify a Service Name and select a Service type.

- 2 Specify settings for the selected Service Type.

- 3 Click **Save Changes**.

## Configure Cloud Security Services

Cloud Security Service is a cloud-hosted security offering (such as firewalls, URL filtering, etc.) that protects an Enterprise's branch and/or data center. The following sections describe how to define and configure a cloud security service instance and how to establish a secure tunnel directly from the Edge to the cloud security service.

### Overview of Cloud Security Services

This section provides an overview of Cloud Security Services.

Currently, the connectivity from a branch Edge to a cloud service or a Non-VeloCloud site is established through the VeloCloud Gateway. In this model, the VeloCloud Gateway aggregates traffic from multiple branch Edges and securely forwards the traffic to the Non-VeloCloud site.

You can also configure the branch Edge to establish a tunnel direct to the cloud service pop. This option has the following advantages:

- You can save link bandwidth costs by offloading non-enterprise traffic to the internet.
- By redirecting the Internet traffic to a cloud security service, you can ensure that the branch sites are protected from malicious traffic.
- Simplified configuration.

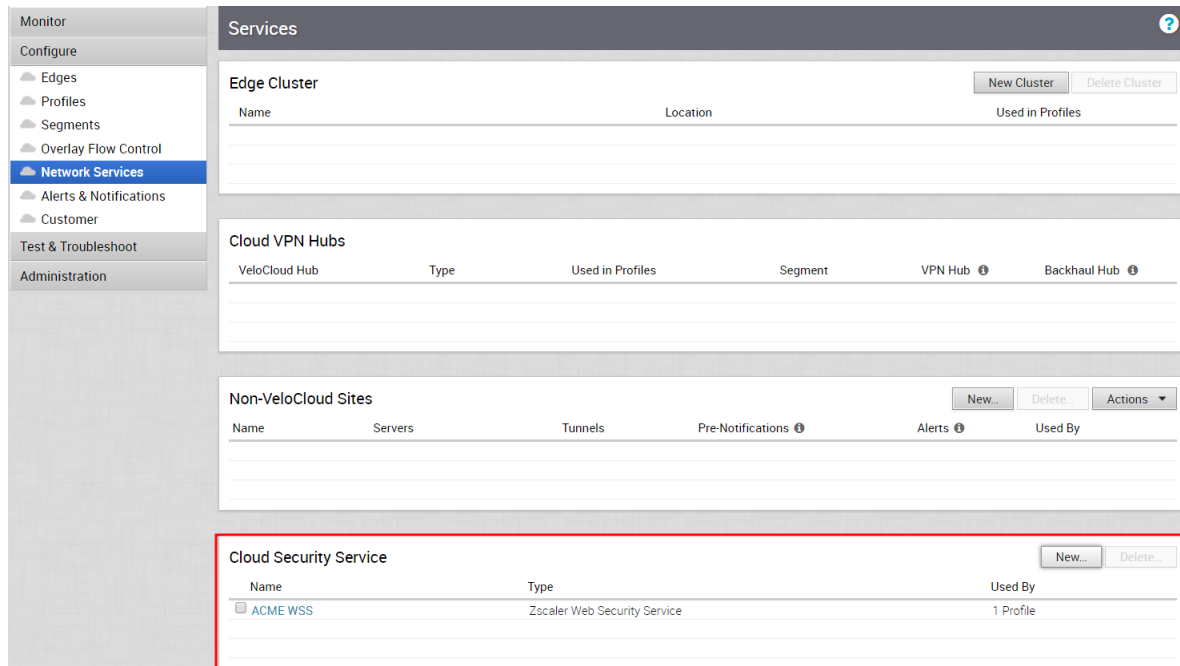
This document describes how to define and configure a cloud security service instance and establish a secure tunnel directly from the Edge to the cloud security service. The configuration is divided into three parts:

- [Configure Cloud Security Services](#)
- [Configure Cloud Security Services for Profiles](#)
- [Configure Cloud Security Services for Edges](#)

## Configure Cloud Security Services

You can configure the cloud security services from the Network Services window.

In the Enterprise portal, navigate to **Configure > Network Services**. For establishing a secured tunnel to cloud security service sites from the Edge, you can define the service instance in the **Cloud Security Service** area.



## Add and Configure a Cloud Security Provider

The cloud security service establishes a secure tunnel from an Edge to the cloud security service sites. This ensures secured traffic flow to the cloud security services.

- 1 In the Customer panel, click **Configure > Network Services**.
- 2 In the **Cloud Security Service** panel, click **New**.
- 3 In the **New Cloud Security Provider** dialog box, select the **Service Type** for the cloud service.
- 4 Enter a descriptive name next to **Service Name**.
- 5 Enter the IP Address for **Primary Point-of-Presence/Server** and **Secondary Point-of-Presence/Server**.

---

**Note** If you have selected **Zscaler Cloud Security Service** as Service Type and planning to assign a GRE tunnel, it is recommended to enter only IP address as Point-of-Presence and not the hostname, as GRE does not support hostnames.

---

- 6 To save your configuration, click **Add**.

---

**Note** You must configure the tunnel attributes for each Edge. See the [Configure Cloud Security Services for Edges](#) section.

---

## Configure Cloud Security Services for Profiles

You must enable cloud security to establish a secured tunnel from an Edge to cloud security service sites. This enables the secured traffic being redirected to third party cloud security sites.

Before you begin:

- Ensure that you have access permission to configure network services.
- Ensure that your SD-WAN Orchestrator has version 3.3.x or above.
- You should have Cloud security service gateway endpoint IPs and FQDN credentials configured in the third party CSS.

- 1 In the Enterprise portal, click **Configure > Profiles**.
- 2 Click the Device Icon next to a profile, or click the link to the profile, and then click the **Device** tab.

- 3 In the **Cloud Security** section, switch the dial from the **Off** position to the **On** position.
- 4 Configure the following settings:



Option	Description
Cloud Security Service	Select a cloud security service from the drop-down menu. You can also click <b>New Cloud Security Service</b> from the drop-down to create a new service type.
Tunneling Protocol	This option is available only for Zscaler cloud security service. Choose either IPsec or GRE. By default, IPsec is selected.
Hash	Select the Hash function as SHA 1 or SHA 256 from the drop-down. By default, SHA 1 is selected.  <b>Note</b> VeloCloud does not support MD5 and it is recommended not to choose MD5 as the Hash function.
Encryption	Select the Encryption algorithm as AES 128 or AES 256 from the drop-down. By default, None is selected.
Key Exchange Protocol	This option is not available for Symantec cloud security service.  Select the key exchange method as IKEv1 or IKEv2. By default, IKEv2 is selected.

- 5 Click **Save Changes**.

When you enable Cloud Security Service and configure the settings in a profile, the setting is automatically applied to the Edges that are associated with the profile. If required, you can override the configuration for a specific Edge. See [Configure Cloud Security Services for Edges](#).

For the profiles created with cloud security service enabled and configured prior to 3.3.1 release, you can choose to redirect the traffic as follows:

- Redirect only web traffic to Cloud Security Service
- Redirect all internet bound traffic to Cloud Security Service
- Redirect traffic based on Business Policy Settings – This option is available only from release 3.3.1. If you choose this option, then the other two options are no longer available.

---

**Note** For the new profiles that you create for release 3.3.1 or later, by default, the traffic is redirected as per the Business Policy settings.

---

You can create a rule in the business policy to redirect the traffic to cloud security service.

- 1 In the **Business Policy** tab of the profile, create a new rule by clicking **New Rule** or, from the **Actions** drop-down menu, choose **New**.

The **Configure Rule** dialog box appears.

- 2 Enter a unique name for the **Rule Name**.
- 3 In the **Action** area, click the **Internet Backhaul** button and choose **Cloud Security Service**.

The screenshot shows the 'Configure Rule' dialog box with the following configuration:

- Rule Name:** Velo\_Zscaler\_Rule
- Match:**
  - Source: Any
  - Destination: Any
  - Application: Any
  - IP Address: Ex: 10.0.2.0
  - CIDR prefix: 24
  - Hostname: Ex: domain.com
  - Protocol: (dropdown)
  - Ports: Ex: 2224-2226
- Action:**
  - Priority: Normal
  - Rate Limit: (checkbox)
  - Network Service: Internet Backhaul
    - Backhaul Hubs
    - Non-VeloCloud Site
    - Cloud Security Service (Velo\_Zscaler\_CSS)
  - Link Steering: Auto
    - Inner Packet DSCP Tag: Leave as is
    - Outer Packet DSCP Tag: 0 - CS0/DF
  - NAT: Disabled
  - Service Class: Transactional

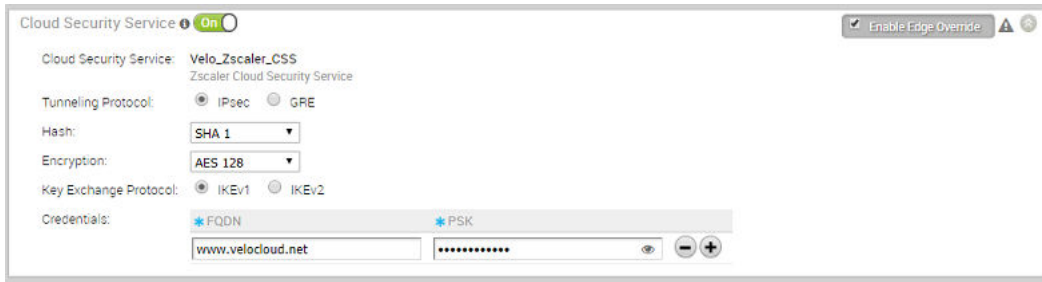
- 4 Click **OK**.

The new rule appears in the **Business Policy** screen.

## Configure Cloud Security Services for Edges

When you have assigned a profile to an Edge, the device automatically inherits the cloud security service associated with the profile. You can override the settings to modify the attributes for each Edge.

- 1 In the Enterprise portal, click **Configure > Edges**.
- 2 In the **Cloud Security Service** section, the cloud security service parameters of the associated profile are displayed. Select **Enable Edge Override**, to modify the attributes. For more information on the attributes, see [Configure Cloud Security Services for Profiles](#).



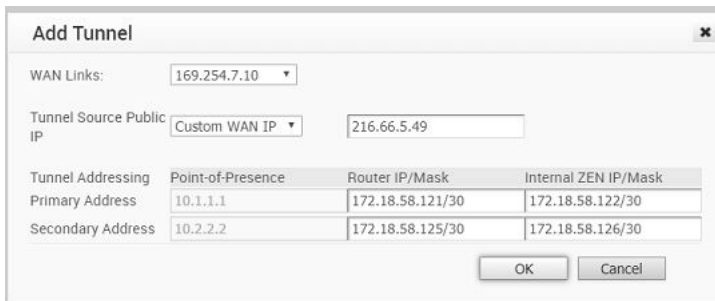
Apart from the existing attributes, you can configure the following additional parameters for an Edge:

- **FQDN** – Enter the Fully Qualified Domain Name for an IPsec protocol.
- **PSK** – Enter the Pre-shared Key for an IPsec protocol.

**Note** The above options are not available for Symantec cloud security service.

If you choose the GRE tunneling protocol for Zscaler cloud security service, add the GRE tunnel parameters.

- 1 Click **Add Tunnel**.
- 2 In the **Add Tunnel** window, configure the following:



Option	Description
WAN Links	Select the WAN interface to be used as source by the GRE tunnel.
Tunnel Source Public IP	Choose the IP address to be used as a public IP address by the Tunnel. You can either choose the WAN Link IP or Custom WAN IP. If you choose Custom WAN IP, enter the IP address to be used as public IP.
Primary Router IP/Mask	Enter the primary IP address of Router.
Secondary Router IP/Mask	Enter the secondary IP address of Router.



Option	Description
Primary ZEN IP/Mask	Enter the primary IP address of Internal Zscaler Public Service Edge.
Secondary ZEN IP/Mask	Enter the secondary IP address of Internal Zscaler Public Service Edge.

---

**Note** The Router IP/Mask and ZEN IP/Mask are provided by Zscaler.

---

3 Click **OK** and the tunnel details are displayed in the Cloud Security Services section.

Click **Save Changes** in the **Edges** window to save the modified settings.

For the profiles created with cloud security service enabled and configured prior to 3.3.1 release, you can choose to redirect the traffic as follows:

- Redirect only web traffic to Cloud Security Service
- Redirect all internet bound traffic to Cloud Security Service
- Redirect traffic based on Business Policy Settings – This option is available only from release 3.3.1. If you choose this option, then the other two options are no longer available.

---

**Note** For the new profiles that you create for release 3.3.1 or later, by default, the traffic is redirected as per the Business Policy settings.

---

You can create a rule in the business policy to associate the cloud security service.

1 In the **Business Policy** tab of the Edge, create a new rule by clicking **New Rule** or, from the **Actions** drop-down menu, choose **New Rule**.

The **Configure Rule** dialog box appears.

2 Enter a unique name for the **Rule Name**.

3 In the **Action** area, click the **Internet Backhaul** button and choose **Cloud Security Service**.

4 Click **OK**.

The new rule appears in the **Business Policy** screen.

## Monitor Cloud Security Services

There are two places you can monitor cloud security services from the VCO navigation panel, the **Edges** screen ( **Monitor > Edges**) and the **Network Services** screen ( **Monitor > Network Services**) screens. The following sections provide more information.

### Edges Screen

To monitor your cloud services from the **Edges** screen, go to **Monitor > Edges**. This view displays the number of tunnels that are up and the number of tunnels that are down.

Edge	Status	HA	Link	Gateways	Profile	Operator Profile	Certificates	Soft
1 Edge-1	<span style="color: green;">●</span>	<span style="color: green;">●</span>	<span style="color: green;">↔ 1</span>	<a href="#">View</a>	Spoke		1 <a href="#">View</a>	3
2 Edge-2	<span style="color: green;">●</span>	<span style="color: green;">●</span>	<span style="color: green;">↔ 2</span>	<a href="#">View</a>	Spoke		4 <a href="#">View</a>	3

**Up Tunnels**

vpn1  
Zscaler Web Security Service  
199.168.148.13 ● Up  
2  
199.168.148.13 ● Up  
2

## Network Services Screen

To monitor your cloud security services from the **Network Services** screen, go to **Monitor > Network Services > Cloud Security Tunnel State**.

Monitor

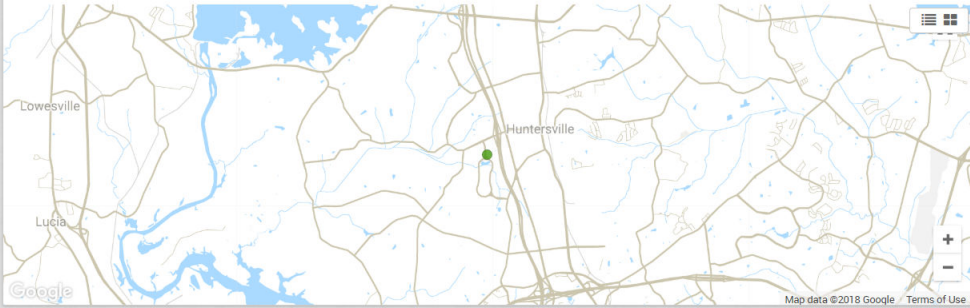
- Edges
- Network Services
- Routing
- Alerts
- Events
- Firewall Logs

Configure

Test & Troubleshoot

Administration

### Network Services



**Cloud Security Service Sites**

	Name	Public IP	Status	Edge Status	State Changed Time	Events
1	vpn1	199.168.148.132 104.129.194.39	<span style="color: green;">●</span>	<span style="color: green;">↔ 9</span>	Tue Apr 24, 14:30:42 a day ago	501 <a href="#">View</a>
2	Zscaler URL	sunnyvale1-vpn... was1-vpn.zscal...	<span style="color: green;">●</span>	<span style="color: green;">↔ 6</span>	Tue Apr 03, 01:43:55 22 days ago	1004 V...

The Edge Status column in the Cloud Security Tunnel State area displays how many Edges are fully connected and disconnected.

### Status Column

The **Status** column shows the overall connectivity state of the specific Cloud Security Service. If all Edges are fully connected, the color of the icon will be green. If some Edges are connected, while some are disconnected, the color of the icon will be yellow. If all Edges are disconnected, the color of the icon will be red.

### Events

To view the Events for the Cloud Security Service, click the **Events** link in the **Cloud Security Service Sites** area.

Events

dialogs.CloudSecurityProviderDialog.provider: Zscaler URL  
 dialogs.CloudSecurityProviderDialog.provider: UIPlugins.zscalerWebSecurityService.title

	Edge	Identifier	Public IP	State	State Changed Time
1	Edge-4	kr1@velocloud.net	sunnyvale1-vpn...	UP	Tue Apr 03, 01:43:55 22
2	Edge-4	kr1@velocloud.net	was1-vpn.zscaler...	UP	Tue Apr 03, 01:43:55 22
3	Edge-4	kr1@velocloud.net	was1-vpn.zscaler...	UP	Tue Apr 03, 01:43:50 22
4	Edge-4	kr1@velocloud.net	sunnyvale1-vpn...	UP	Tue Apr 03, 01:43:50 22
5	Edge-4	kr1@velocloud.net	was1-vpn.zscaler...	UP	Tue Apr 03, 01:43:50 22
6	Edge-4	kr1@velocloud.net	was1-vpn.zscaler...	DOWN	Tue Apr 03, 01:43:45 22

Close

## Configure DNS Services

This is an optional service that allows you to create a configuration for DNS.

The DNS Service can be for a public DNS service or a private DNS service provided by your company. A **Primary Server** and **Backup Server** can be specified. The service is preconfigured to use Google and Open DNS servers.

The following figure shows a sample configuration for a Public DNS.

New DNS Service

Public DNS Private DNS

**Server Details:**

- \* Service Name:
- \* Primary Server:
- Backup Server:

Save Changes Cancel

For a private service, you can also specify one or more **Private Domains**.

New DNS Service

Public DNS Private DNS

**Server Details:**

- \* Service Name:
- \* Primary Server:
- Backup Server:

**Private Domains:**

- +

Save Changes Cancel

## Configure Netflow Settings

In an Enterprise network, Netflow monitors traffic flowing through VeloCloud Edges (VCEs) and exports Internet Protocol Flow Information eXport (IPFIX) information directly from VCEs to one or more Netflow collectors. The VCO allows you to configure Netflow collectors and filters as network services at the profile, edge, and segment level. You can configure a maximum of two collectors per segment and eight collectors per profile and edge. Also, you can configure a maximum of 16 filters per collector.

### Procedure

- 1 From the VeloCloud Orchestrator, go to **Configure > Network Services**.

The **Services** page appears.

- 2 To configure a collector, go to the **Netflow Settings** area and click the **New** button at the right side of the Collector table. The **Add New Collector** dialog box appears.
  - a In the **Collector Name** text box, enter a unique name for the collector.
  - b In the **Collector IP** text box, enter the IP address of the collector.
  - c In the **Collector Port** text box, enter the port ID of the collector.
  - d Click **Save Changes**.

Under **Network Services**, the newly added collector appears in the Collector table.

- 3 VCO allows filtering of traffic flow records by source IP, destination IP, and application ID associated with the flow. To configure a filter, go to the **Netflow Settings** area and click the **New** button at the right side of the Filter table. The **Add New Filter** dialog box appears.

The screenshot shows the 'Add New Filter' dialog box with the following configuration:

- Filter Name:** Allow\_ICMP
- Match:**
  - Source:** IP Address (0.0.0.0/1)
  - Destination:** Any
  - Application:** Any
- Action:** Allow

- In the **Filter Name** text box, enter a unique name for the filter.
- Under the **Match** area, click **Define** to define per collector filtering rules to match by source IP or destination IP or application associated with the flow, or click **Any** to use any of the source IP or destination IP or application associated with the flow as the match criteria for Netflow filtering.
- Under the **Action** area, select either **Allow** or **Deny** as the filter action for the traffic flow, and click **OK**.

Under **Network Services**, the newly added filter appears in the Filter table.

## Results

At the profile and edge level, the configured collectors and filters appears as a list under the **Netflow Settings** area in the **Device** tab.

- While configuring a profile or edge, you can either select a collector and filter from the available list or add a new collector and a filter. For steps, see [Configure Netflow Settings at the Profile Level](#).
- To override Netflow settings at the Edge level, see [Configure Netflow Settings at the Edge Level](#).

## Private Network Names

You can define multiple private networks and assign them to individual private WAN overlays.

## Configure Private Networks

To configure private networks:

- 1 From the VCO navigation panel, go to **Configure > Network Services**.
- 2 In the **Private Network Names** area, click the **New** button.
- 3 In **New Private Network Name** dialog box, enter a unique name in the appropriate text box.

- 4 Click **Save Changes**.

The private network name appears in the **Private Network Name** area.

Name	Used By
<input type="checkbox"/> MPLS A	0
<input type="checkbox"/> MPLS B	0

## Delete a Private Network Name

Only private network names that are not used by an Edge device can be deleted.

To delete a private network name not used by an Edge device:

- 1 Select the name by clicking the name's checkbox, and then click the **Delete** button.
- 2 In the **Confirm Deletion dialog box**, click **OK**.

You can select private link tags when you define a User Defined Overlay. See section titled, "*Select a Private Network Name*."

## Configure Authentication Services


Authentication Services is an optional configuration. If your organization uses a service for authentication or accounting, you can create a Network Service that specifies the IP address and ports for the service. This is a part of the 802.1x configuration process, which is configured in the profile.

The following figure shows an example configuration.

### New Radius Service ✕

\* Service Name:

\* Server Address:

\* Shared Secret:  

\* Authentication Port:

Accounting Port:

# Configure Profiles

# 10

Profiles provide a composite of the configurations created in Networks and Network Services. It also adds configuration for Business Policy and Firewall rules.

---

**Note** If you are logged in using a user ID that has Customer Support privileges, you will only be able to view VeloCloud Orchestrator objects. You will not be able to create new objects or configure/update existing ones.

---

Profiles have four tab pages: **Profile Overview**, **Device**, **Business Policy**, and **Firewall**.

This chapter includes the following topics:

- [Create a Profile](#)
- [Modify a Profile](#)
- [Profile Overview Screen](#)
- [Network to Segment Migration](#)
- [Configure Local Credentials](#)

## Create a Profile

After a new installation, the VeloCloud Orchestrator has the following predefined Profiles: Internet Profile, VPN Profile, and as of the 3.0 release, Segment-based profiles.

---

**Note** With the Segmentation feature introduced in the 3.0 release, Edges running the software prior to 3.0 could have a Network-based Configuration or a Segmentation-based Configuration. **\*\*Because of this transition, you must migrate/convert the Network-based profile to the Segment-based profile.**

---

The following steps are typically followed when creating a new Profile:

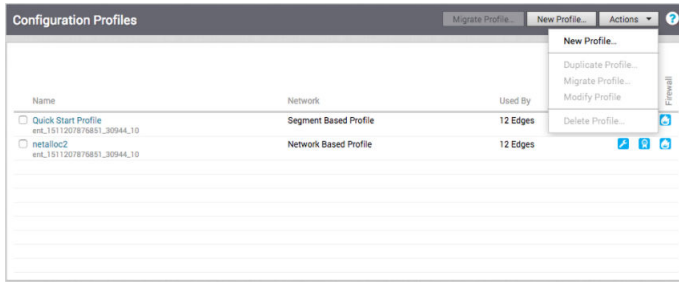
- 1 Create a Profile
- 2 Configure Device
  - a Select Network
  - b Assign Authentication/DNS
  - c Configure Interface Settings



- 3 Enable Cloud VPN
- 4 Configure Business Policy
- 5 Configure Firewall
- 6 Review Profile Overview

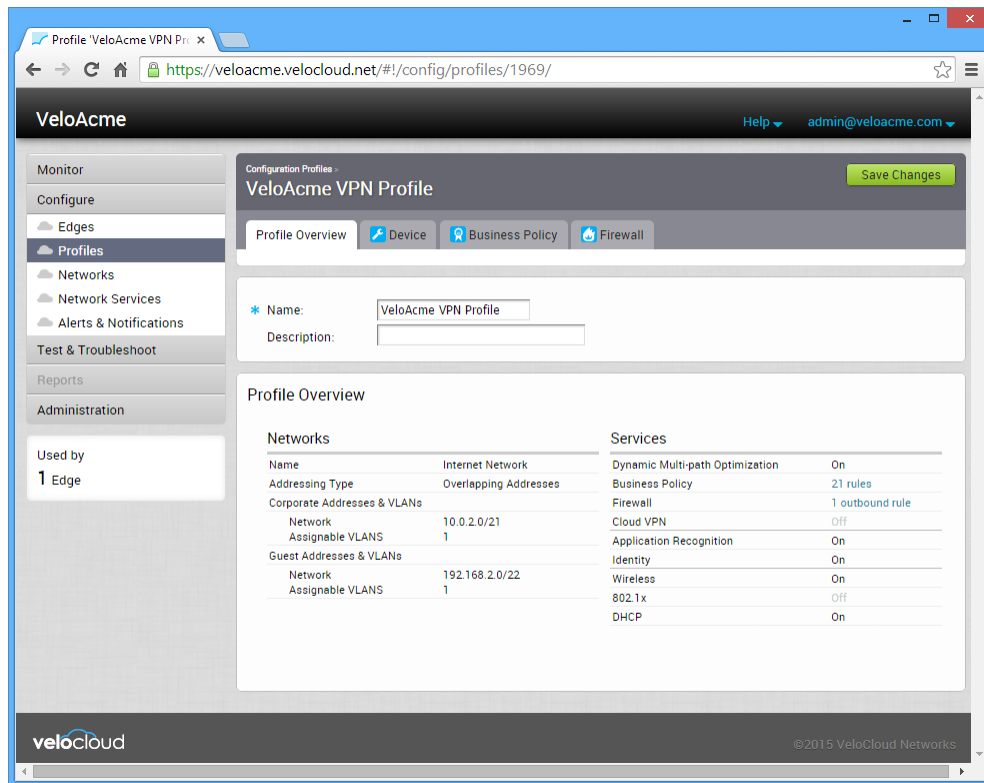
To create a new Profile:

- 1 Go to Configure ->Profiles, and click the **New Profile** button.



- 2 In the **New Profile** dialog, enter a Profile Name and Description in the appropriate textboxes.
- 3 Click the **Create** button.

The **Profile Overview** tab page refreshes. See the **Profile Overview Screen** section below for more information.



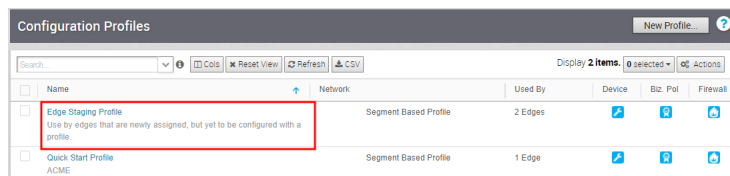
## Modify a Profile

Enterprise Admins can also manually assign a profile to an Edge.

**Note** Content for "Change a Profile" is new for the 3.3.0 release.

One scenario in which this is necessary is for Edge Staging Profiles. In this case, the Edge gets activated against the staging profile by default due to push activation. Enterprise Admins must manually assign a final production profile to the Edge. See *Provision an Edge* in *Assign a Profile (Change a Profile)* for instructions on how to manually assign Profiles.

**Note** Push activation is tech preview for the 3.3.0 release. For more information, see section titled *Push Activation*.



Name	Network	Used By	Device	Biz. Pol.	Firewall
Edge Staging Profile <small>Use by edges that are newly assigned, but yet to be configured with a profile.</small>	Segment Based Profile	2 Edges	[Device Icon]	[Biz. Pol. Icon]	[Firewall Icon]
Quick Start Profile <small>ACME</small>	Segment Based Profile	1 Edge	[Device Icon]	[Biz. Pol. Icon]	[Firewall Icon]

## Profile Overview Screen

The **Profile Overview** screen provides a quick summary of all Networks and Services that are defined in the profile.

The overview is divided into two categories:

Category	Description
Networks	Has the name of the Network configuration used, the type of addressing, and the Network addresses and VLANs assigned to the Corporate and Guest networks.
Services	Has a summary of the services provided by the VeloCloud system.

After all settings have been entered for the Profile Device, Business Policy, and Firewall tab screens, the **Profile Overview** screen should reflect the configurations you have performed.

## Network to Segment Migration

In the 3.2 release, the Profile Migration feature was introduced to help simplify the workflow to upgrade Edges from Network-based Profiles to Segment-based Profiles. This document provides the workflow and details on how to upgrade a 2.X Edge with a Network-based Profile to 3.X with a Segment-based profile.

## Edge Upgrade from 2.X to 3.X Prerequisites

To upgrade from version 2.X to 3.X, the following prerequisites are required for the Edge:

- Upgrading to 3.X is supported from versions 2.4 and 2.5.
- Make sure the VCO and VCG are the same version or a higher version than the Edge.

## Best Practices for Upgrading Edges Deployed as Hub and Spoke

While performing upgrades for Edges deployed in Hub and Spoke configurations:

- The Edges configured as a Hub should be upgraded to 3.X before upgrading the Edges configured as Spokes.
- Tunnel formation will not occur if the Hub is in a 3.X based profile and all the Spokes are running in a 2.X based profile.
- In order to overcome the above-mentioned restriction, each Spoke profile should have at least one Spoke running in the 3.2.1 based profile.

## Best Practices for Upgrading Edges Deployed in HA

There are no restrictions for upgrading Edges configured in HA. Normal software steps are applicable.

## Migrate Network to Segment

This section describes network to segment migration.

### Before You Begin

Prior to upgrading an Edge, make sure the VCO and VCG are the same version or a higher version than the Edge.

---

**Note** Because 3.X Edges only understand Segment-based Profiles, the 3.2 image update will get pushed out to the Edge only if the Edge has a Segmented Profile assigned. Once a Segment-based Profile is assigned to an Edge, it cannot be reassigned to a Network-based Profile. The transition from a Network-based Profile to a Segment-based Profile is supported, but a Segment-based Profile to a Network-based Profile is not supported.

---

### Step 1: Enable Segmentation

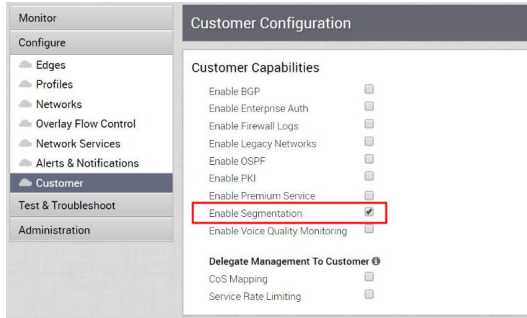
Segmentation must be enabled prior to migrating a profile. Enterprise and Partner level users must contact their Operator to ensure this feature is enabled.

Operators must enable segmentation before a profile can be migrated. Enterprise and Partner level users do not have access to this feature.

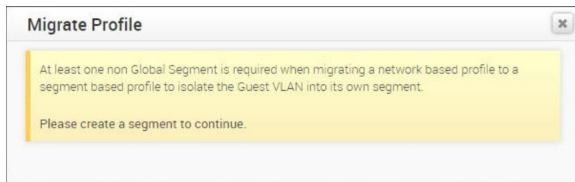
To enable Segmentation:

- 1 Select **Configure -> Customer** from the VCO navigation panel.

- From the **Customer Configuration** screen, select the **Enable Segmentation** checkbox located under **Customer Capabilities**.



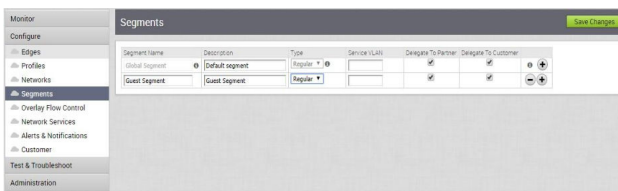
**Note** If you attempt to migrate a profile without segmentation enabled, the following error message appears.



## Step 2: Create a Non-global Segment for Allocating a Guest Network

Because guest networks are created by default in a Network-based profile, you must create a non-global segment to map the guest networks to a separate segment during migration.

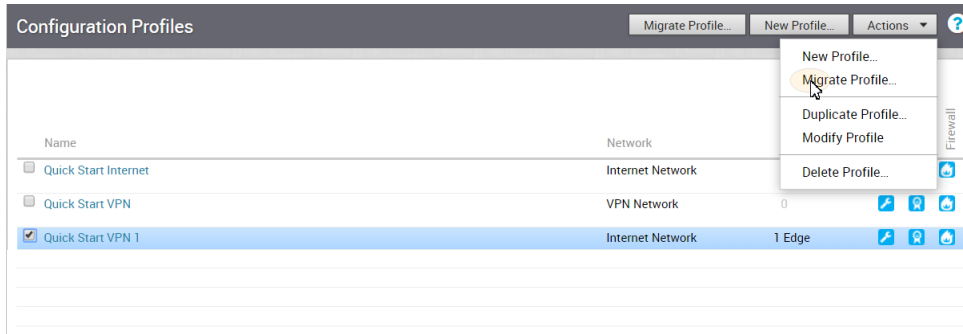
- From the VeloCloud Orchestrator, go to **Configure > Segments**. The **Segments** screen appears. Note that the Global Segment cannot be deleted.



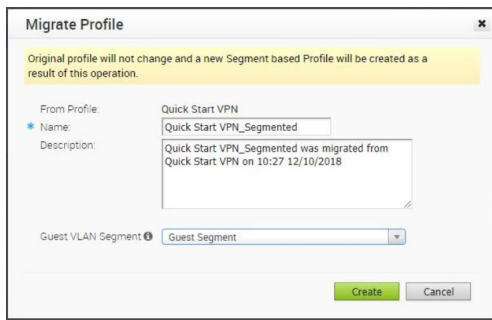
- Click the Add symbol **+** to create a new segment.
- Click **Save Changes**.

## Step 3: Create a Migrated Profile from a Network Profile

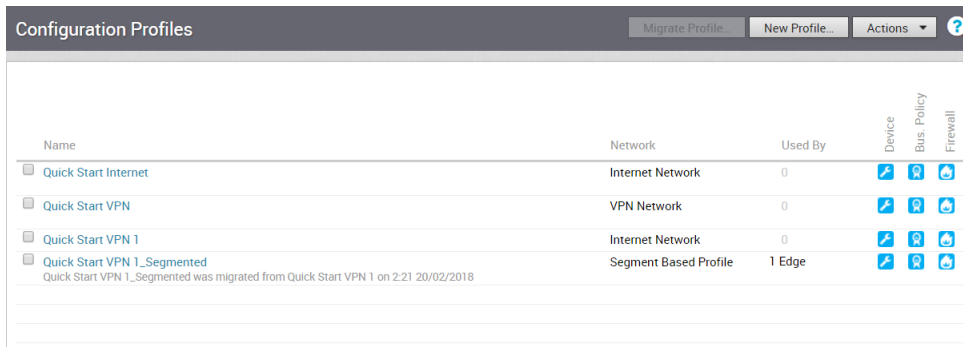
- From the VCO navigation panel, go to **Configure > Profiles**.
- Select a Network-based Profile by selecting the checkbox next to the name of the configuration profile.
- From the **Actions** drop-down menu, choose **Migrate Profile**.



- 4 In the **Migrate Profile** dialog box, type in a name and description for the profile.
- 5 Select the segment to which the Guest Network will be mapped (refer to Step 4). The corporate segment configuration will be migrated to the Global Segment.
- 6 Click the **Create** button.



A new Segment-based Profile is created with the same settings in the Global Segment as the old Network-based Profile. See image below. Please note that no Edges are assigned to this Profile.



### Step 4 Assign Migrated Profile to Edges (See IMPORTANT NOTE Below)

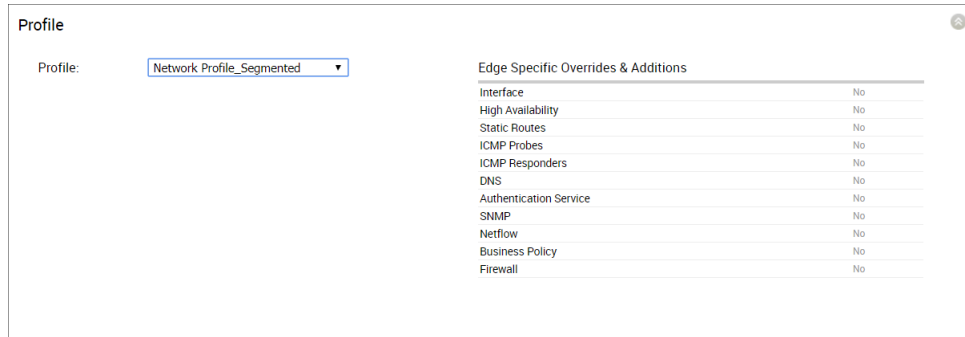
During this step, no configuration updates will be pushed out to the Edge while the Edge reported software image is < 3.0. Edges in this state are essentially ‘configuration frozen’ until a 3.X image is provisioned to them.

To assign a segment-based profile to a network-based Edge:

- 1 Go to **Configure > Edges** in the navigation panel of the VCO.

- 2 In the **VeloCloud Edges** screen, select the Edge you want to assign a Segment Profile to.
- 3 In the **Edge Overview** tab, go to the **Profile** area.
- 4 From the **Profile** drop-down menu, choose a **Segment Based Profile** (see image below).

The segment-based profile will be applied only after the Edge is upgraded to 3.2.X.



**Note** There are two additional steps to migrate a profile, 'Create a New Operator Profile with a 3.2 Edge Image' and 'Assign the Segment-based Operator Profile to the Edges.' Enterprise Admin users at all levels do not have access to these additional steps and must contact their Operator. Their Operator must create a new Operator Profile with a 3.X Image and assign the Operator profile to the Enterprise usage. After assigning the 3.X based Operator profile and segmented profile, the Edge will receive a software image update. Contact your Operator for more information.

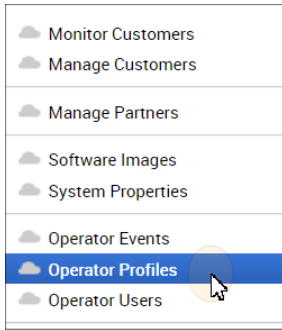
**Note** The next step, "Create a New Operator Profile with a 3.2 Edge Image" is an Operator-level only step that must be completed before a profile can be migrated. Partners do not have access to the features for this step and must contact their Operators.

## Step 5: Create a New Operator Profile with a 3.2 Edge Image (Operator-level Only Step)

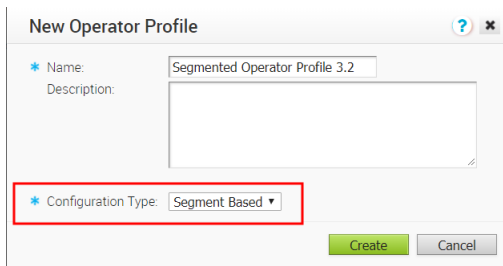
Operators must create a new Operator profile with a 3.2 Edge image before a profile can be migrated. Enterprise and Partner level users do not have access to the features in this step.

Step 5 is an Operator-level only step. Your Operator must create a new Operator Profile with a 3.2 Edge Image.

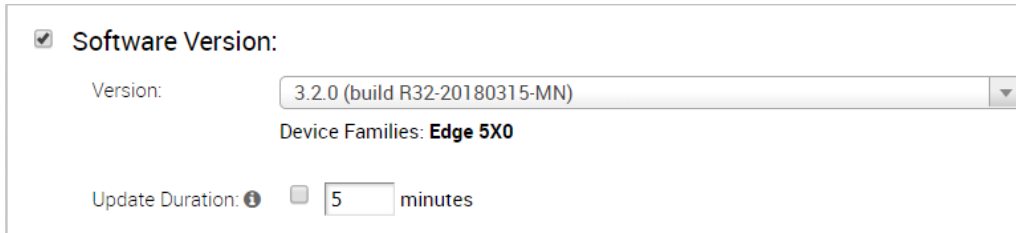
- 1 From the VCO, choose **Operator Profiles**. See image below.



- 2 From the **Operator Profile** screen, click the **New Profile** button.
- 3 In the **New Operator Profile** dialog box:
  - a Type in a Name and Description for the profile.
  - b In the **Configuration Type** drop-down menu, choose **Segment Based**.
  - c Click the **Create** button.



- 4 In the newly created **Operator Profile** screen, go to the **Software Version** area.
- 5 In the **Software Version** area, choose a software version from the **Version** drop-down menu. (See image below).



- 6 Click the **Save Changes** button at the top of the VCO screen.

### Step 6: Assign the Segment-based Operator Profile to the Edges

**An Important Note has been added to this step for the 3.3.0 software release (see note below).**

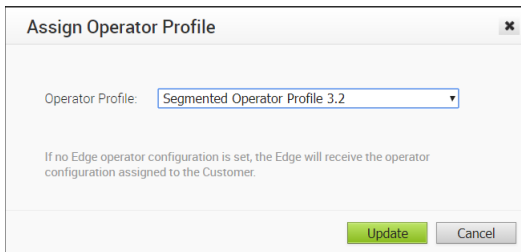
**Note** Operators and Partners can assign software images, but Enterprise Admins at all levels do not have access to this feature.

The Edge with the Segmented Profile will receive a software image update via the Operator Profile. This can be accomplished either by switching the Operator Profile for the customer or assigning a new Operator Profile to selected Edges. The steps below describe how to assign a new Operator Profile to a selected Edge.

**Note** It is recommended that you perform the profile assignment to one Edge first and validate that the Edge is working correctly before you proceed to the other Edges. The first Edge that you assign a profile to will be classified as a Hub (because Hubs must be migrated before spokes).

#### To Assign a new Operator Profile:

- 1 From the VCO navigation panel, go to **Configure > Edges**.
- 2 In the **VeloCloud Edges** screen, select the Edge(s) you want to assign an Operator Profile to.
- 3 From the **Actions** drop-down menu, choose **Assign Operator Profile** or **Assign Software Image**. (NOTE: Only Operator Superusers will see **Assign Operator Profile** from the **Actions** drop-down menu, all other users with access to this feature will see **Assign Software Image** from the **Actions** drop-down menu).
- 4 From the appropriate dialog box ( **Assign Operator Profile** dialog box or **Assign Software Image** dialog box), choose the Segment-based Operator Profile that was created in Step 3. ( **NOTE:** If necessary, assign the Operator Profile to a Customer or Partner).
- 5 Click the **Update** button.

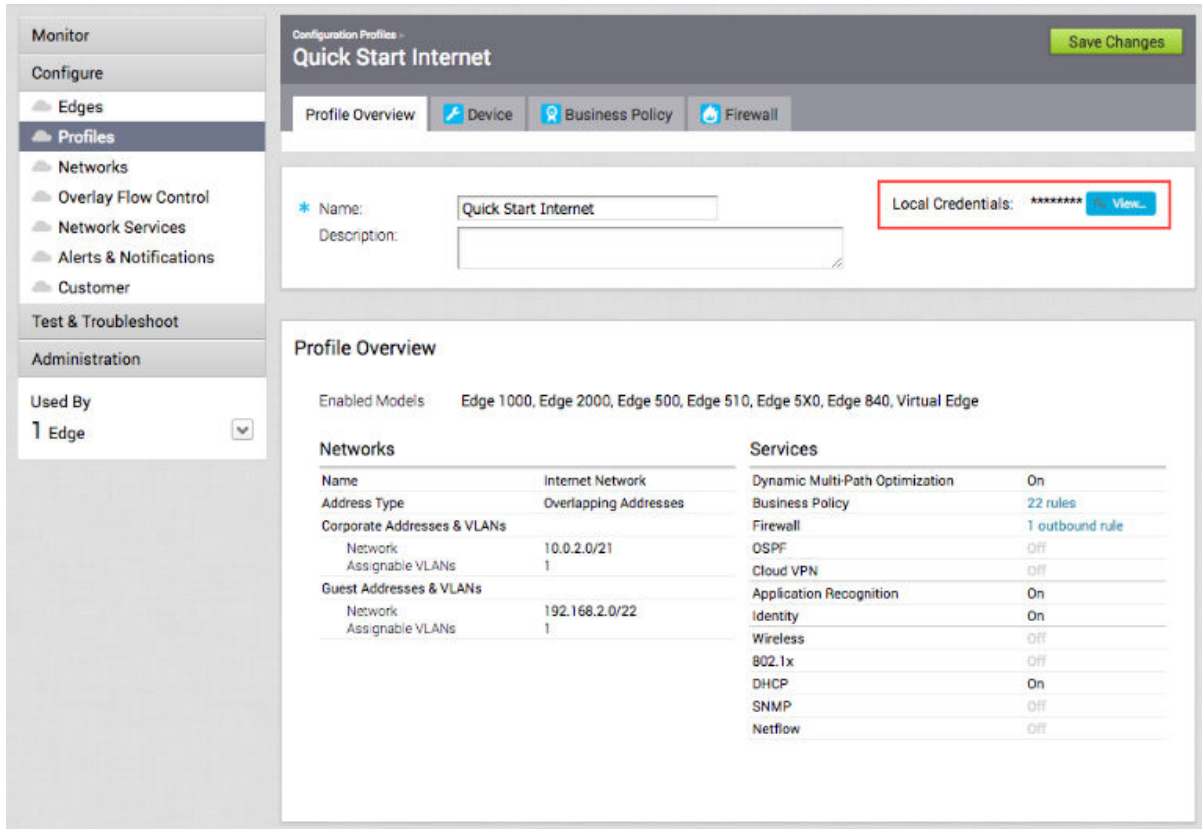


After this operation, Edge(s) will receive the 3.2 software image update, and after the image update process is complete, Edge(s) will begin communicating with the VCO.

## Configure Local Credentials

You can change the local credentials at the Profile level from the **Configure > Profiles > Profile Overview** tab. When the credentials are updated, they will be sent to all Edges that use the Profile as an Edge action.

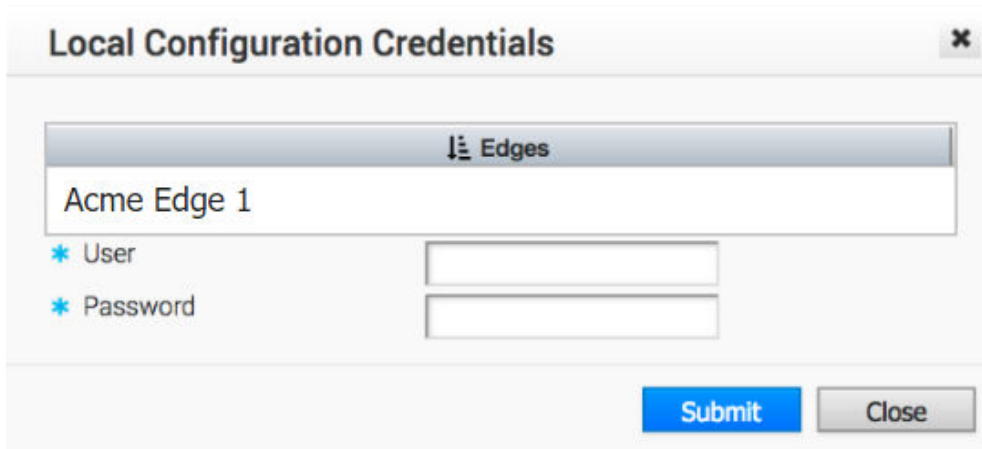




## Add Credentials

This section describes how to add credentials.

Click the **View button** to open the **Local Configuration Credentials** dialog box. Type in a **User** name and a **Password**, and then click the **Submit** button.



# Configure a Profile Device

# 11

This section describes how to configure a profile device.

---

**Note** If you are logged in using a user ID with Customer Support privileges, you will only be able to view VeloCloud Orchestrator objects. You will not be able to create new objects or configure/update existing ones.

---

VeloCloud provides device settings using the **Device** tab ( **Configure > Profiles > Device Tab**) in a profile. The **Device Settings** tab is used to assign segments, create VLANs, configure interfaces, configure DNS settings, Configure Authentication Settings. For more information about Segmentation, see [Chapter 8 Configure Segments](#).

This chapter includes the following topics:

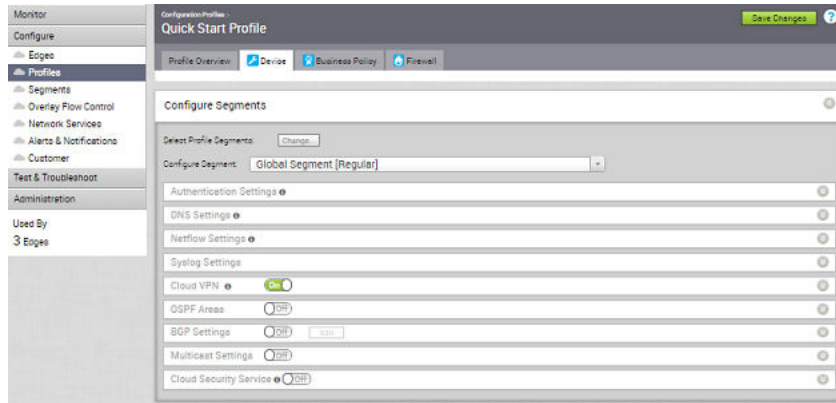
- [Configure a Device](#)

## Configure a Device

Device configuration allows you to assign segments to a Profile and configure Interfaces to be associated with a Profile.

For segment aware profiles, there are two sections on the UI:

Configuration Type	Description
Segment-aware configurations	<b>Configure Segments</b> area of the <b>Device</b> tab screen. Customers can choose the segment from the drop-down menu, select the segment, and then the configuration for that segment will display in the <b>Configure Segments</b> area.
Common configurations	The lower part of the <b>Device</b> tab screen. Features and configurations that apply to multiple segments, which include VLAN configs, Device Settings, Wifi and Multi-source QoS.



You can perform the following steps for Device Configuration:

## Segment-aware Configurations

- Authentication Settings
- DNS Settings
- Netflow Settings
- Syslog Settings
- Cloud VPN
- OSPF Areas
- BGP Settings
- Multicast Settings
- Cloud Security Service

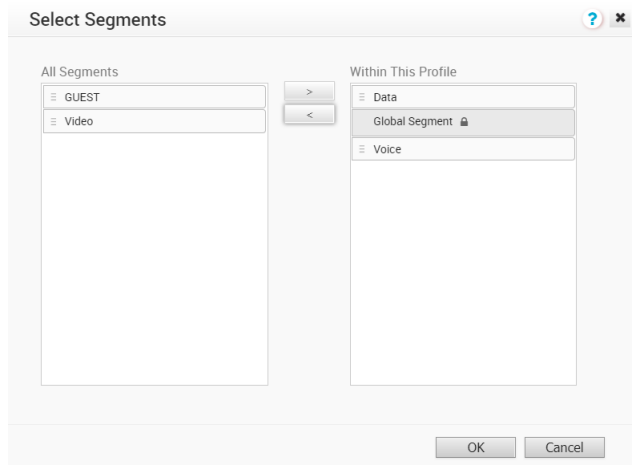
## Common Configurations:

- VLAN
- Device Settings
- Wi-Fi Radio Settings
- Multi-Source QoS
- SNMP Settings
- NTP Servers
- Visibility Mode

## Assign Segments in Profile

After creating a Profile, you can select Profile Segments by clicking the **Change** button in the image **Configure Segments** window.

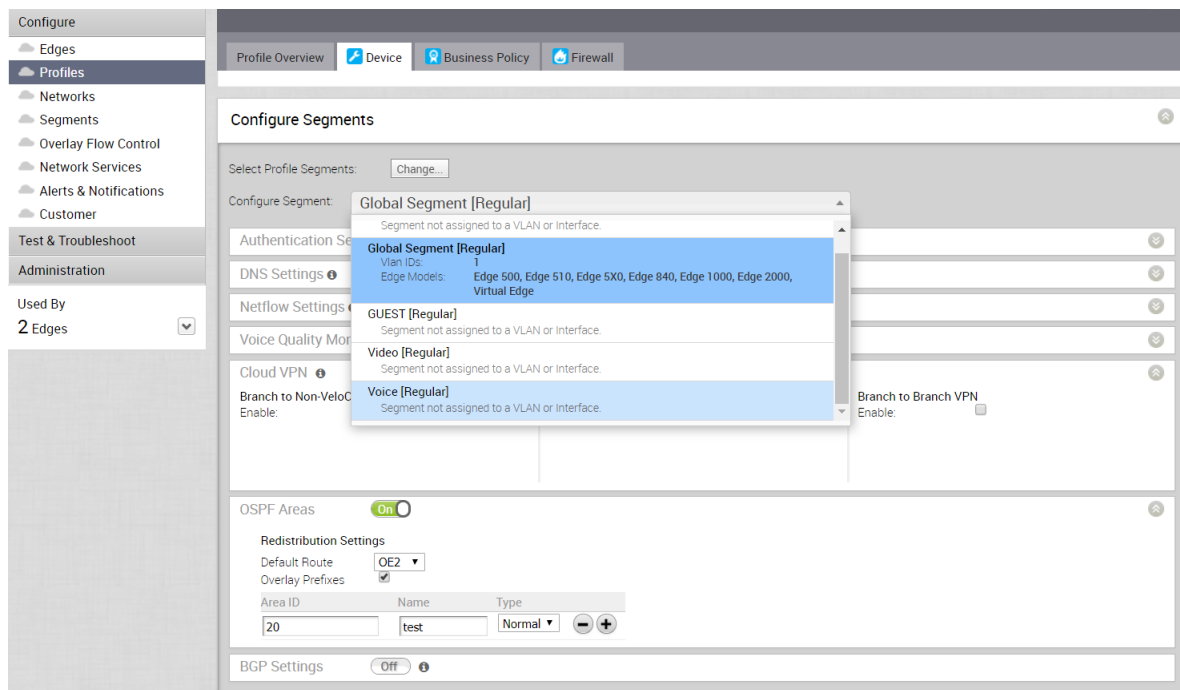
Clicking the **Change** button opens the **Select Segments** dialog box.



In this dialog box, you can select the Segments that you want to include in your profile. Segments with a lock symbol next to them indicate that the Segment is in use within a profile, and it cannot be removed. Segments available for use will be displayed on the left side of the dialog under **All Segments**.

After you have selected a Segment, you can configure your Segment through the **Configure Segment** drop-down menu. All Segments available for configuration are listed in the **Configure Segment** drop-down menu. If a Segment is assigned to a VLAN or interface, it will display the VLAN ID and the Edge models associated with it.

When you choose a Segment to configure from the **Configure Segment** drop-down menu, depending upon the Segment's options, the settings associated that Segment display in the **Configure Segments** area.



## Configure Authentication Settings

The **Device Authentication Settings** allow you to specify which Network Services DNS Service to use.



The screenshot shows a configuration box titled "Authentication Settings". Inside the box, there is a label "RADIUS Servers:" followed by a dropdown menu. The dropdown menu is currently set to "VeloAcme-radius".

## Configure DNS Settings

The **DNS Settings** allow you to specify which Network Services DNS Service will be used.



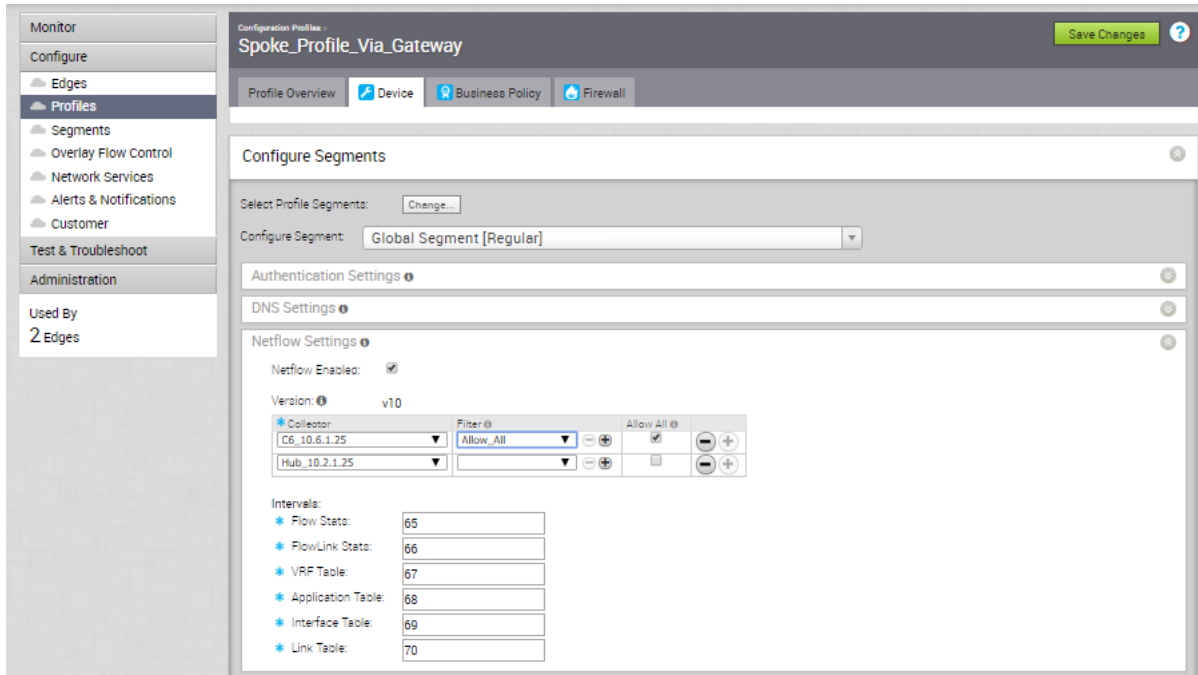
The screenshot shows a configuration box titled "DNS Settings". Inside the box, there is a label "Public DNS:" followed by a dropdown menu. The dropdown menu is currently set to "VeloAcmeDNS".

## Configure Netflow Settings at the Profile Level

As an enterprise Administrator, you can configure Netflow settings at the Profile level by performing the steps on this procedure.

### Procedure

- 1 From the VeloCloud Orchestrator, go to **Configure > Profiles**.  
The **Configuration Profiles** page appears.
- 2 Select a profile you want to configure Netflow settings and click the icon under the **Device** column.  
The Device Setting page for the selected profile appears.



3 From the **Configure Segment** drop-down menu, select a profile segment to configure Netflow settings.

4 Go to the **Netflow Settings** area and configure the following details.

a Select the **Netflow Enabled** checkbox.

VCO supports IP Flow Information Export (IPFIX) protocol version 10.

b From the **Collector** drop-down menu, select an existing Netflow collector to export IPFIX information directly from VCEs, or click **New Collector** to configure a new Netflow collector.

For more information about how to add a new collector, see [Configure Netflow Settings](#).

**Note** You can configure a maximum of two collectors per segment and eight collectors per profile by clicking the **+** button. When the number of configured collectors reaches the maximum allowable limit, the **+** button will be disabled.

c From the **Filter** drop-down menu, select an existing Netflow filter for the traffic flows from VCEs, or click **New Filter** to configure a new Netflow filter.

For more information about how to add a new filter, see [Configure Netflow Settings](#).

**Note** You can configure a maximum of 16 filters per collector by clicking the **+** button. However, the 'Allow All' filtering rule is added implicitly at the end of the defined filter list, per collector.

- d Enable the **Allow All** checkbox corresponding to a collector to allow all segment flows to that collector.
- e Under **Intervals**, configure the following Netflow export intervals:
  - **Flow Stats** - Export interval for flow stats template. By default netflow records of this template is exported every 60 seconds. The allowable export interval range is from 60 seconds to 300 seconds.
  - **FlowLink Stats** - Export interval for flow link stats template. By default netflow records of this template is exported every 60 seconds. The allowable export interval range is from 60 seconds to 300 seconds.
  - **VRF Table** - Export interval for VRF option template. The default export interval is 300 seconds. The allowable export interval range is from 60 seconds to 300 seconds.
  - **Application Table** - Export interval for Application option template. The default export interval is 300 seconds. The allowable export interval range is from 60 seconds to 300 seconds.
  - **Interface Table** - Export interval for Interface option template. The default export interval is 300 seconds. The allowable export interval range is from 60 seconds to 300 seconds.
  - **Link Table** - Export interval for Link option template. The default export interval is 300 seconds. The allowable export interval range is from 60 seconds to 300 seconds.

---

**Note** In an Enterprise, you can configure the Netflow intervals for each template only on the Global segment. The configured Netflow export interval is applicable for all collectors of all segments on an edge.

---

- 5 Click **Save Changes**.

## Configure Syslog Settings at Profile Level

In an Enterprise network, VeloCloud Orchestrator (VCO) supports collection of VCO bound events originating from enterprise VeloCloud Edges (VCEs) to one or more centralized remote Syslog collectors (Servers), in the native Syslog format. For the Syslog collector to receive VCO bound events from the configured edges in an Enterprise, at the profile level, configure Syslog collector details per segment in the VCO by performing the steps on this procedure.

### Prerequisites

- Ensure that Cloud VPN (branch-to-branch VPN settings) is configured for the VCE (from where the VCO bound events are originating) to establish a path between the VCE and the Syslog collectors. For more information, see [Configure Cloud VPN](#).

### Procedure

- 1 From the VeloCloud Orchestrator, go to **Configure > Profiles**.

The **Configuration Profiles** page appears.

- 2 Select a profile you want to configure Syslog settings and click the icon under the **Device** column.

The Device Setting page for the selected profile appears.

- 3 From the **Configure Segment** drop-down menu, select a profile segment to configure syslog settings. By default, **Global Segment [Regular]** is selected.
- 4 Go to the **Syslog Settings** area and configure the following details.
  - a From the **Facility Code** drop-down menu, select a Syslog standard value that maps to how your Syslog server uses the facility field to manage messages for all the events from VCEs. The allowed values are from **local0** through **local7**.

---

**Note** The **Facility Code** field is configurable only for the **Global Segment**, even if the Syslog settings is enabled or not for the profile. The other segments will inherit the facility code value from the Global segment.

---

- b Select the **Syslog Enabled** checkbox.
- c In the **IP** text box, enter the destination IP address of the Syslog collector.
- d From the **Protocol** drop-down menu, select either **TCP** or **UDP** as the Syslog protocol.
- e In the **Port** text box, enter the port number of the Syslog collector. The default value is 514.
- f As Edge interfaces are not available at the Profile level, the **Source Interface** field is set to **Auto**. The Edge automatically selects an interface with 'Advertise' field set as the source interface.
- g From the **Roles** drop-down menu, select **EDGE EVENT**.
- h From the **Syslog Level** drop-down menu, select the Syslog severity level that need to be configured. For example, If **CRITICAL** is configured, the VCE will send all the events which are set as either critical or alert or emergency.

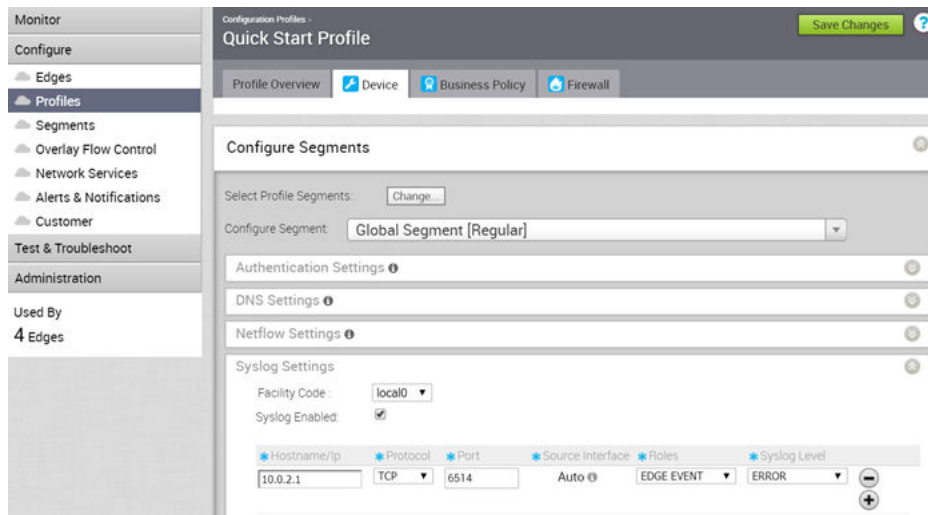
The allowed Syslog severity levels are:

- **EMERGENCY**
- **ALERT**
- **CRITICAL**
- **ERROR**
- **WARNING**
- **NOTICE**
- **INFO**
- **DEBUG**



- Click the + button to add another Syslog collector.

**Note** You can configure a maximum of two Syslog collectors per segment and 10 Syslog collectors per Edge. When the number of configured collectors reaches the maximum allowable limit, the + button will be disabled.



**Note** By configuring the Syslog setting for the Edges, only remote syslog for VCO bound events from Edges will be received at the Syslog collector. If you want the VCO auto-generated local events to be received at the Syslog collector, you must configure Syslog at the VCO level by using the `log.syslog.backend` and `log.syslog.upload` system properties.

### Example: IETF Syslog Format

The following is a sample syslog message in IETF format.

```
<%PRI%>1 %TIMESTAMP:::date-rfc3339% %HOSTNAME% %APP-NAME% %PROCID% %MSGID% %STRUCTURED-DATA% %msg%\n
```

The following is a sample syslog message.

```
<163>1 2019-06-16T09:17:15.003Z b1-edge1 Edged 1312 ID47 'Interface GE3 is up'
```

The message has the following parts:

- Priority - Facility \* 8 + Severity (local4 & critical) - 163
- Version - Syslog version - 1
- Date - Date in YYYY-MM-DD format - 2019-06-16
- Time - Time in UTC - 09:17:15.003Z (3 ms into next second)
- Host Name - b1-edge1
- Application Name - Edged [Mgd for mgd generated events]
- Process ID - 1312

- Message ID - type of message (String)
- Message - Event message in UTF-8

## Configure Cloud VPN

If a Network with a non-overlapping address is assigned to a Profile, it is assumed for a VPN configuration and the Cloud VPN section will be available.

**Note** Cloud VPN should be configured per Segment.

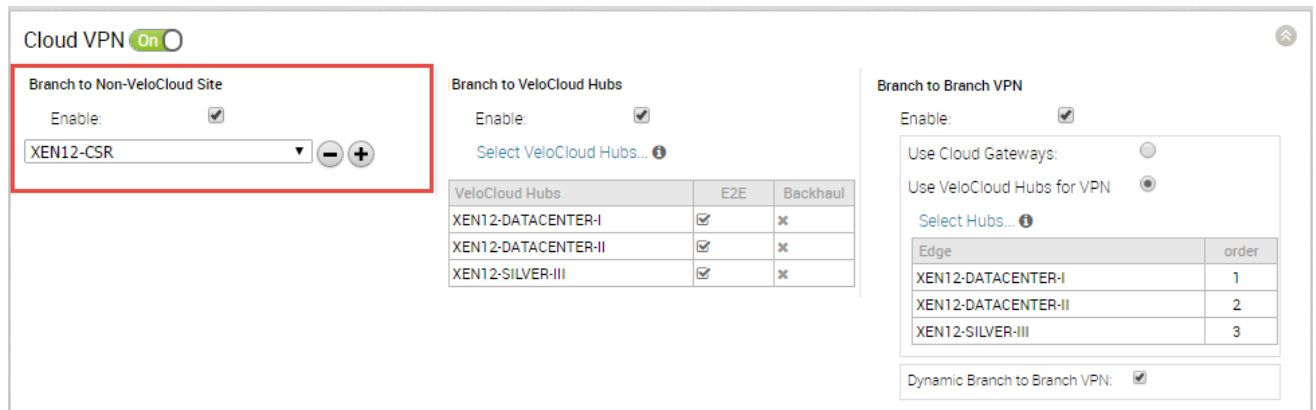
When Cloud VPN on the **Profile Device** tab is enabled, you can configure three different Cloud VPN types:

- [Branch to Non-VeloCloud Site](#)
- [Branch to VeloCloud Hubs](#)
- [Branch to Branch VPN](#)

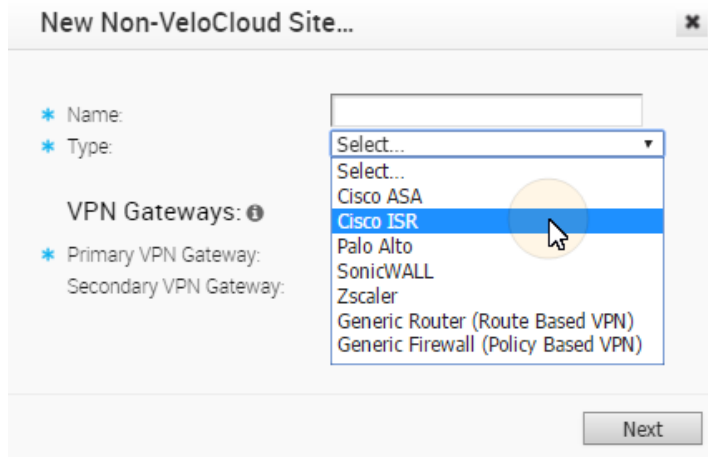
## Configure Branch to VPNs

This section describes how to configure branch to VPNs.

You can configure Branch to Non-VeloCloud Sites by selecting the **Enable** checkbox (see the highlighted area in the screen capture below). You can also choose one or more Non-VeloCloud Sites by selecting the **Enable** check box, and then selecting Non-VeloCloud Site from the drop-down menu. You can click the **+** (plus) button to add additional Non-VeloCloud Sites.

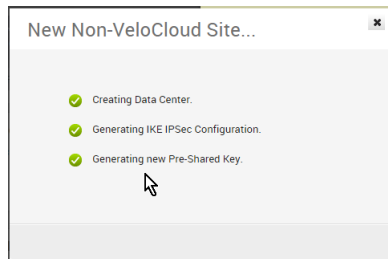


You can also create VPN connections by selecting the **New** Non-VeloCloud Site from the drop-down menu. Select a **Type** for the Non-VeloCloud Site. The Non-VeloCloud Site **Type** options (as shown in the image below) are Cisco ASA, Cisco ISR, Palo Alto, SonicWall, Zscaler, Generic Router (Route Based VPN), and Generic Firewall (Policy Based VPN). In the example below, Cisco ISR is chosen. In this example, you can enter a **Primary VPN** gateway, and a **Secondary VPN** gateway option is available. Enter the required parameters (**Name**, **Type**, **Primary Gateway**, and **Secondary Gateway**) for the Non-VeloCloud Site you selected, then click **Next**.

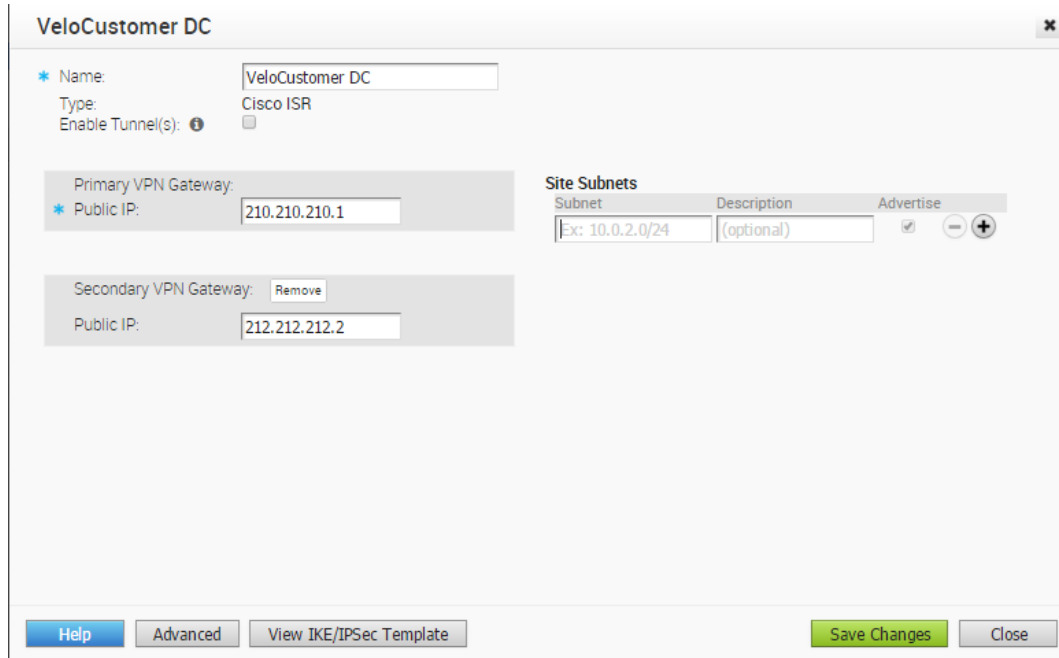


**Note** Cisco ASA does not support a secondary gateway. This is a limitation of the Cisco ASA VPN.

A status appears for the creation of the new Non-VeloCloud Site.



A final dialog box for completing the configuration of the Non-VeloCloud Site appears.



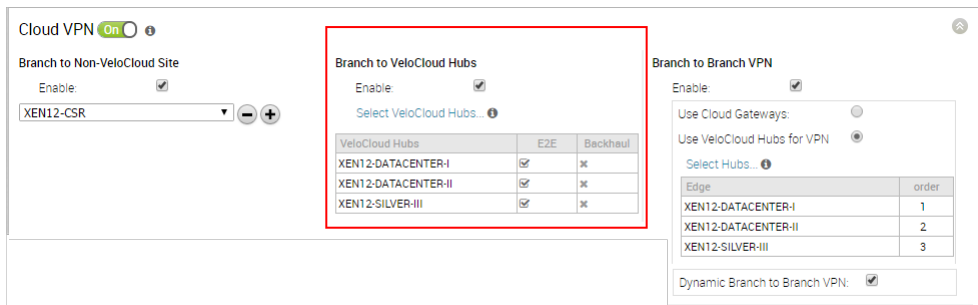
**Note** The Branch to Non-VeloCloud Site VPN should not be enabled until after the gateway for the Enterprise Data Center is configured by the Enterprise Data Center Administrator and the Data Center VPN Tunnel is enabled.

### Configure Branch to VeloCloud Hubs VPN

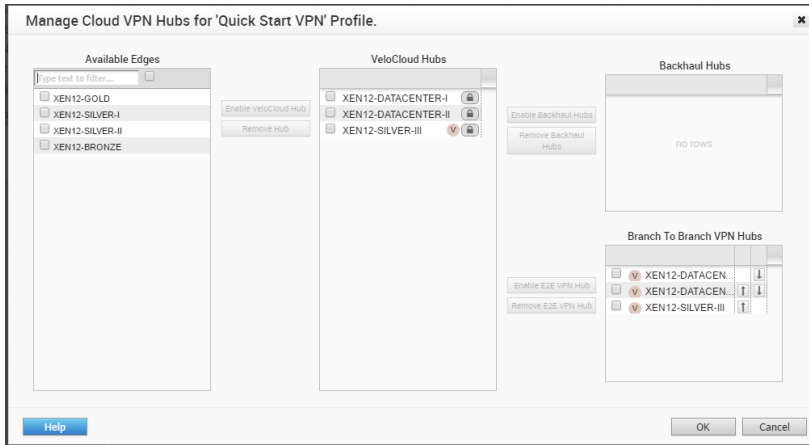
This section describes how to configure the Branch to VeloCloud Hubs VPN.

To configure Branch to VeloCloud Hubs:

- 1 Select the **Enable** checkbox (see the highlighted area in the screen capture below).
- 2 Click the **Select VeloCloud Hubs** link.



The following dialog appears for you to select the select the VeloCloud Hubs that can be used for VPN tunnels between the Branch using this profile and the selected VeloCloud Hub.



## Configure Branch to Branch VPN

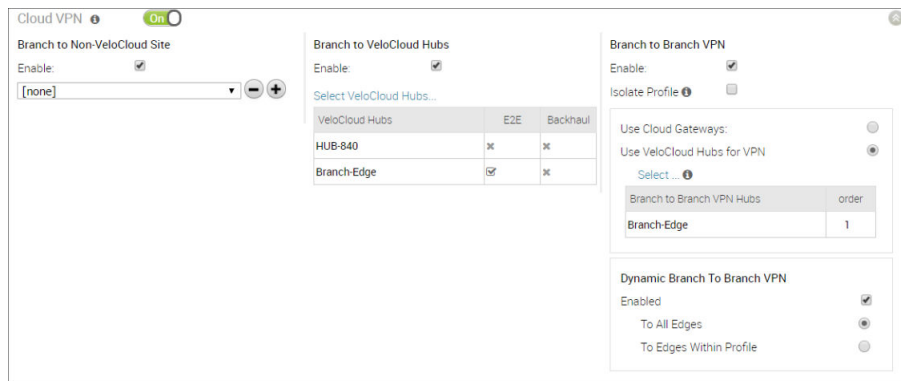
This section describes how to configure branch-to-branch VPN.

### Enable Branch to Branch VPN

You can configure Branch to Branch VPN by selecting the **Enable** checkbox.

Branch to Branch VPN supports two configurations for establishing a VPN connection between branches:

Configuration	Description
Using a VeloCloud Gateway	In this option, the closest gateway is used to establish VPN connections between Edges. The VeloCloud Gateway may have traffic from other users.
Using a VeloCloud Hub	In this option, one or more Edges are selected to act as hubs that can establish VPN connections between branches. The hub will be your asset and will only have your corporate data on it, improving overall security.

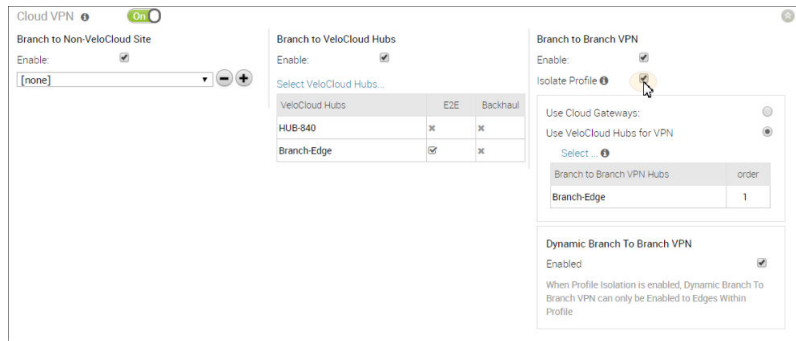


### Enable Branch to Branch VPN Isolation

Configure Branch to Branch VPN Isolation by selecting the **Isolate Profile** checkbox.

When the Isolate Profile checkbox is selected, the Edges within the profile will not learn routes from other Edges outside this profile via the SD-WAN Overlay.

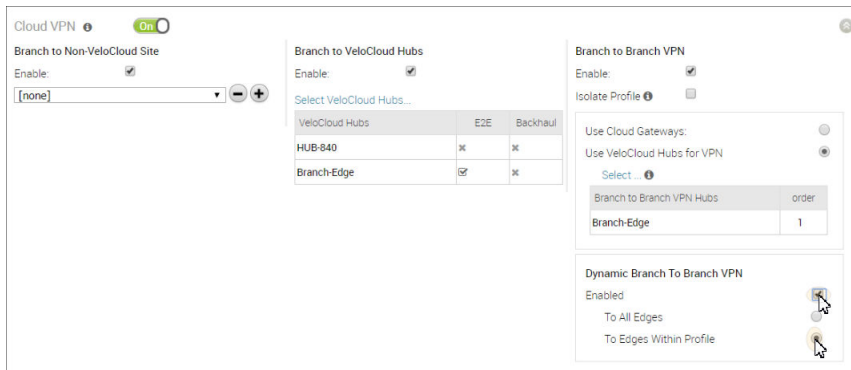
**Note** For topology and use cases, see [Branch to Branch VPN](#).



## Enable Dynamic Branch to Branch VPN Isolation by Profile

To configure Dynamic Branch to Branch VPN Isolation by profile:

- 1 Make sure the **Isolate Profile** checkbox is unselected.
- 2 Enable Branch to Branch VPN by selecting the **Enabled** checkbox.



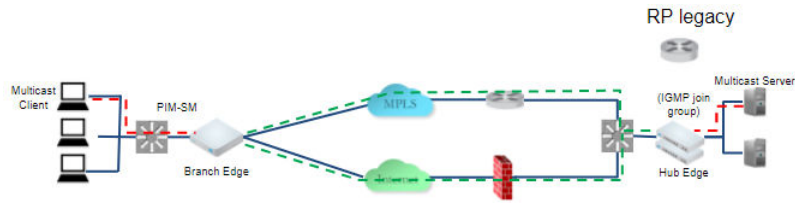
- 3 Select the **To Edges Within Profile** checkbox.

**Note** For topology and use cases, see [Dynamic Branch to Branch VPN Isolation by Profile](#).

## Configure Multicast Settings

Multicast provides an efficient way to send data to an interested set of receivers to only one copy of data from the source, by letting the intermediate multicast-routers in the network replicate packets to reach multiple receivers based on a group subscription.

Multicast clients (aka receivers) use the Internet Group Management Protocol (IGMP) to propagate membership information from hosts to Multicast enabled routers and PIM to propagate group membership information to Multicast servers via Multicast routers.



Multicast support includes:

- Multicast support on both overlay and underlay
- Protocol-Independent Multicast - Sparse Mode (PIM-SM) on VCE
- Internet Group Management Protocol (IGMP) version 2 on VCE
- Static Rendezvous Point (RP) configuration, where RP is enabled on a 3rd party router.

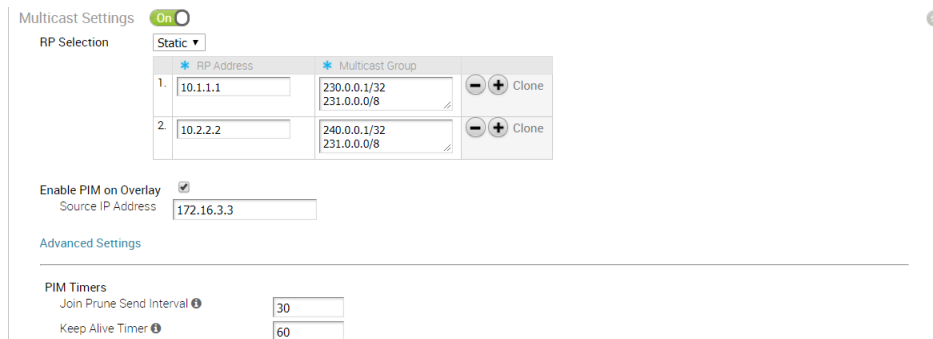
### Configure Multicast Globally

There are two steps to enable and configure Multicast (globally and at the interface level), in which both can be overridden at the Edge Level. The steps below provide instructions on how to enable the Multicast globally.

To configure Multicast globally:

- 1 From **Configure > Profile > Devices**, go to the **Multicast Settings** area.
- 2 If the **Multicast Settings** button is in the **Off** position, click the **Off** button to turn **On** Multicast Settings.

The RP Selection is set to **Static** by default.



- 3 In the appropriate textboxes for the RP Selection, type in the RP Address and Multicast Group. (See the table below for a description of **RP Address** and **Multicast Group** ).
- 4 If applicable, select the **Enable PIM on Overlay** checkbox and enter the IP Source Address.
- 5 Set **Advanced Settings**, if necessary. Refer to the table that follows for a description of each setting. In the appropriate text boxes, enter PIM Timers for **Join Prune Send Interval** (default 60 seconds) and **Keep Alive Timer** (default 60 seconds).

### Multicast Settings

The following table describes Multicast settings.

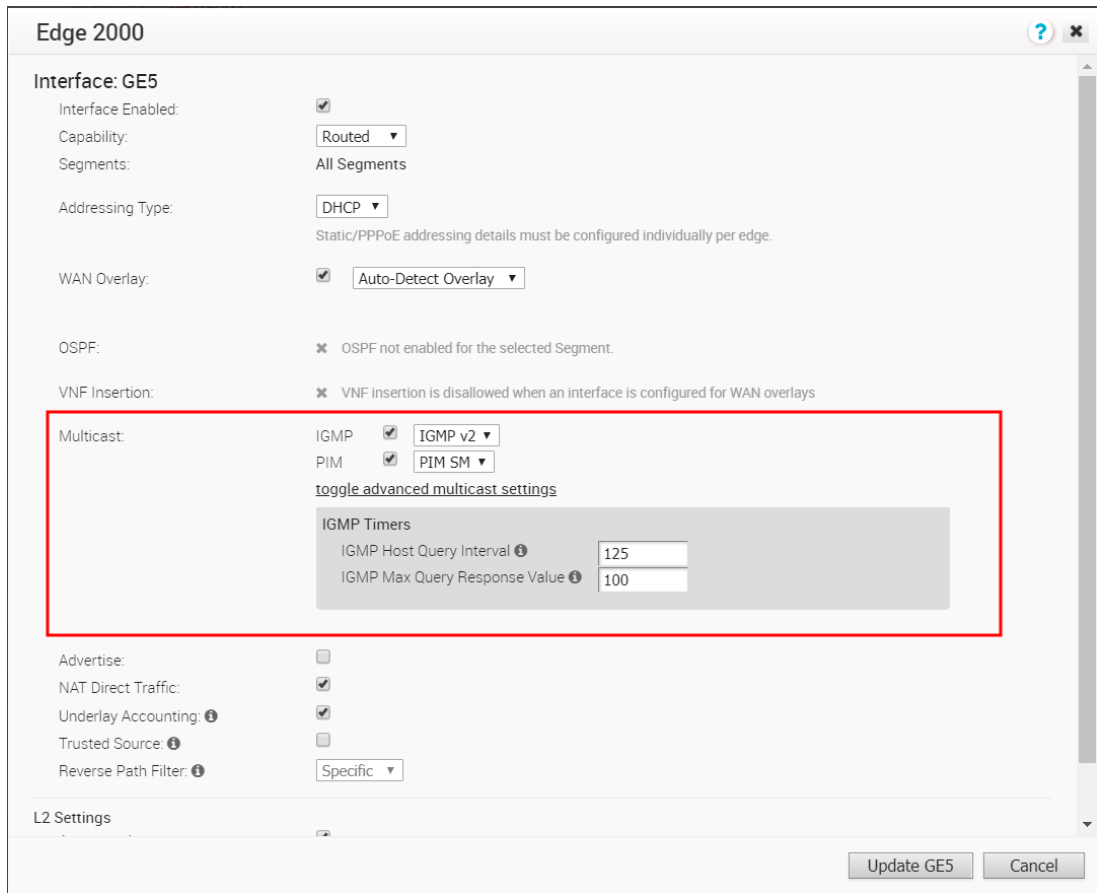
Multicast Setting	Description
<b>RP Selection</b>	Configure RP for multicast groups. <b>Static RP</b> is the default and supported mechanism in 3.2 release.
<b>Enable PIM on Overlay</b>	Enable PIM peering on SD-WAN Overlay, for example when enabled on both branch VCE and hub VCE. Branch VCE and hub VCE will form a PIM peer. By default, the source IP address for the overlays is derived from one of the multicast-enabled underlay interfaces and it is recommended to leave the default. Users can optionally change the source IP by specifying <b>Source IP Address</b> , which will be a virtual address and will be advertised over the overlay automatically.
PIM Timers	
<b>Join Prune Send Interval</b>	The Join Prune Interval Timer. Default value is 60 seconds.
<b>Keep Alive Timer</b>	PIM keep alive timer. Default value is 60 seconds.

## Configure Multicast Settings at the Interface Level

To enable and configure Multicast at the Interface level:

- 1 From the **Configure Profiles Device** tab screen, choose a target Edge model and go the Interfaces Settings area and select the interface you want to enable Multicast.
- 2 Click the **Edit** button to open the **Interface Settings** dialog box for the Edge you configured.
- 3 In the **Interface** dialog box of the Edge model:
  - a Select the **Interface Enabled** checkbox to display the settings for the dialog.
  - b In the **Capability** drop-down menu, choose **Routed** to be able to use the Multicast settings.
  - c In the **Addressing Type** drop-down menu, choose either DHCP, PPPoE, or Static.
  - d If applicable, select the **WAN Overlay** checkbox.
  - e If applicable, select the **OSPF** checkbox.
  - f In the **Multicast** section:
    - 1 If applicable, select the **IGMP** checkbox and select the only available option IGMP v2.
    - 2 If applicable, select the **PIM** checkbox and select the only available option PIM SM.
    - 3 Click the '**toggle advanced multicast settings**' link to set IGMP Timers, as shown in the image below.





- IGMP Host Query Interval: The default is 125 seconds and the range is 1-1800.
  - IGMP Max Query Response Value: The default is 100 deciseconds and the range is 10-250.
- g If applicable, select the following checkboxes: Advertise, NAT Direct Traffic, Underlay Accounting, and Trusted Source.
  - h In the **Reverse Path Filter** drop-down menu, make a selection ( **Disabled**, **Specific**, **Loose**). **NOTE:** The user can only set the Reverse Path Filter when the trusted zone is checked. When the trusted zone is unchecked, the value will default to **Specific** as shown in the image above.
  - i In the **L2 Settings** area, if applicable, select the **Autonegotiate** checkbox. If so, enter the MTU in the textbox.
  - j If Autonegotiate is unselected, enter the **Speed**, **Duplex**, and **MTU** in the appropriate checkboxes.
  - k Click **Update** for the Edge model.

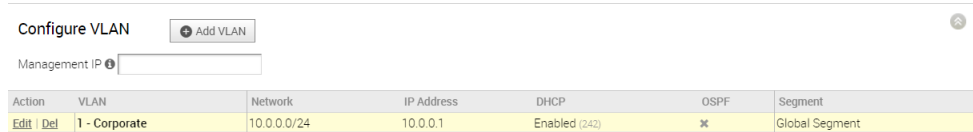
The following table describes the IGMP Timers.

IGMP Timers	Description
IGMP Host Query Interval	IGMP host query interval, default value is 60 sec.
IGMP Max Query Response Value	IGMP max query response value, default value is 10 sec.

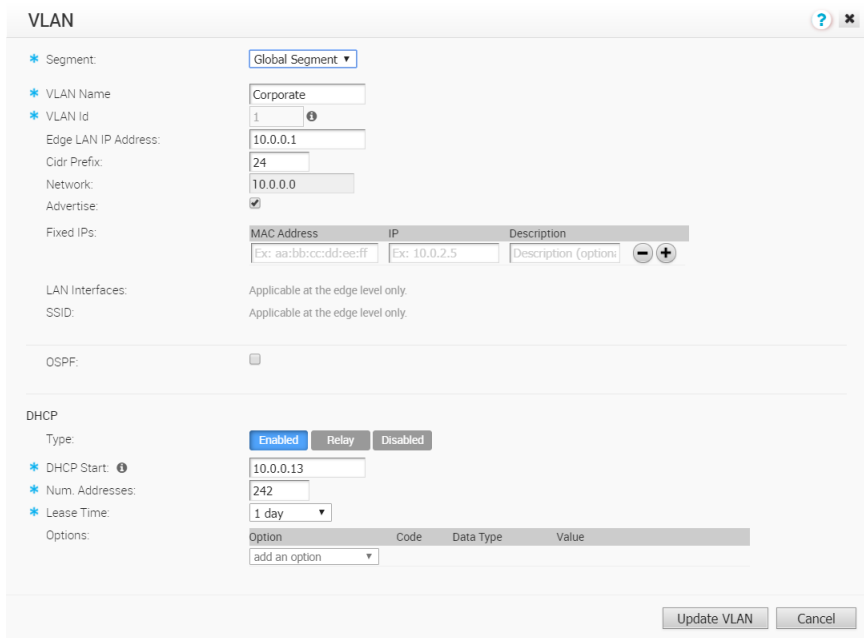
**Note** Go to **Monitor > Routing > Multicast** tab, to view Multicast routing information. See [Monitor Routing](#) for more information.

## Add and Configure a VLAN

To add and configure a VLAN:



- 1 From the **Configure VLAN** area, click the **Add VLAN** button.
- 2 In the **VLAN** dialog box, choose a Segment from the **Segment** drop-down menu.



- 3 Enter the following information in the appropriate text boxes: **VLAN Name**, **VLAN ID**, **Edge LAN IP Address**, **Cidr**, and **Network**.
- 4 If applicable, select the **Advertise** checkbox.
- 5 Enter any Fixed IPs in **Fixed IPs** text boxes.
- 6 Select the **OSPF** checkbox, if applicable.
- 7 In the **DHCP** area, choose the type (**Enabled**, **Relay**, or **Disabled**).

8 Depending upon the DHCP type you have selected, enter in the appropriate information.

## Configure the Management IP Address

You can configure the Management IP address at the Profile-level and choose to override it at the Edge-level.

The following are the various scenarios when you can use the Management IP address:

- It is used to source the management traffic from Edges to Orchestrator. In this scenario, you can either use the default Management IP address (192.168.1.1) or an IP address of your choice that you configure at the Profile-level so that all Edges attached to the Profile use the same IP address to source the traffic to the Orchestrator.

---

**Note** You can choose to ignore the Management IP configuration, if you have NAT Direct enabled on the WAN ports or if the traffic from the Edges is routed to the Orchestrator through a Gateway.

---

- If you choose to configure services such as DNS, NTP, Netflow, BGP and so on, you must override the Management IP address configuration at the Edge-level so that each Edge has a unique IP address that can be used as the source address for these services.
- It is also used as the destination IP address for diagnostic tests when configured at the Edge-level.

To configure the Management IP address for a Profile:

- 1 In the Enterprise portal, go to **Configure > Profiles**.
- 2 Either click the Device icon next to the Profile for which you want to configure the Management IP address, or click the link to the Profile, and then go to the **Device** tab.
- 3 In the **Device** page, scroll down to the **Management IP** section, and enter the required Management IP address.
- 4 Click **Save Changes**.

You can choose to override the Management IP address configuration for an Edge:

- 1 In the Enterprise portal, go to **Configure > Edges**.
- 2 Either click the Device icon next to the Edge for which you want to override the Management IP address configuration, or click the link to the Edge, and then go to the **Device** tab.
- 3 In the **Device** page, scroll down to the **Management IP** section, and select the **Enable Edge Override** check box.
- 4 Enter the required Management IP address.
- 5 Click **Save Changes**.

## Configure Device Settings

Device Settings allows you configure the Interface Settings for one or more Edge models in a profile.

Depending on the Edge Model, each interface can be a Switch Port (LAN) interface or a Routed (WAN) Interface. Depending on the Branch Model, a connection port is a dedicated LAN or WAN port, or ports can be configured to be either a LAN or WAN port. Branch ports can be Ethernet or SFP ports. Some Edge models may also support wireless LAN interfaces.

It is assumed that a single public WAN link is attached to a single interface that only serves WAN traffic. If no WAN link is configured for a routed interface that is WAN capable, it is assumed that a single public WAN link should be automatically discovered. If one is discovered, it will be reported to the VeloCloud Orchestrator. This auto-discovered WAN link can then be modified via the VeloCloud Orchestrator and the new configuration pushed back to the branch.

---

### Note

- If the routed Interface is enabled with the WAN overlay and attached with a WAN link, then the interface will be available for all Segments.
  - If an interface is configured as PPPoE, it will only support a single auto-discovered WAN link. Additional links can not be assigned to the interface.
- 

If the link should not or cannot be auto-discovered, it must be explicitly configured. There are multiple supported configurations in which auto-discovery will not be possible, including:

- Private WAN links
- Multiple WAN links on a single interface. Example: A Datacenter Hub with 2 MPLS connections
- A single WAN link reachable over multiple interfaces. Example: for an active-active HA topology

Links that are auto-discovered are always public links. User-defined links can be public or private, and will have different configuration options based on which type is selected.

---

**Note** Even for auto-discovered links, overriding the parameters that are automatically detected -- such as service provider and bandwidth -- can be overridden by the Edge configuration.

---

### Public WAN Links

Public WAN links are any traditional link providing access to the public internet such as Cable, DSL, etc. No peer configuration is required for public WAN links. They will automatically connect to the VeloCloud Gateway, which will handle the dissemination of information needed for peer connectivity.

## Private (MPLS) WAN Links

Private WAN links belong to a private network and can only connect to other WAN links within the same private network. Because there can be multiple MPLS networks, within a single enterprise, for example, the user must identify which links belong to which network. The VeloCloud Gateway will use this information to distribute connectivity information for the WAN links.

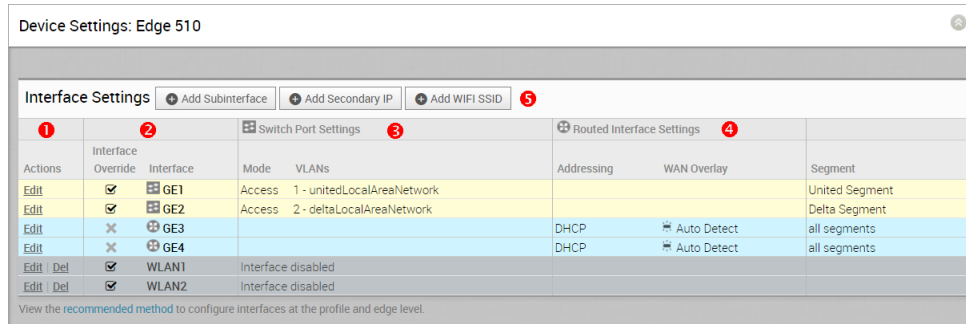
You may choose to treat MPLS links as a single link. However, to differentiate between different MPLS classes of service, multiple WAN links can be defined that map to different MPLS classes of service by assigning each WAN link a different DSCP tag.

Additionally, you may decide to define a static SLA for a private WAN link. This will eliminate the need for peers to exchange path statistics and reduce the bandwidth consumption on a link. Since probe interval influences how quickly the device can fail over, it's not clear whether a static SLA definition should reduce the probe interval automatically.

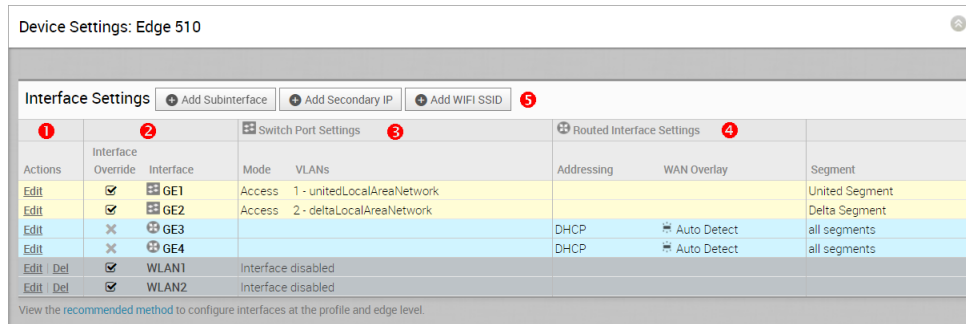
## Device Settings

The following screen captures illustrate the top-level user interface for the VeloCloud Edge 500 and the VeloCloud Edge 1000. The following table describes the major features of the UI (the numbers in the table correspond to the numbers in the subsequent screen captures).

1	Actions you can perform on the network interface, such as Edit or <b>Delete</b> .
2	The Interface name. This name matches the Edge port label on the Edge device or is predetermined for wireless LANs.
3	The list of Switch Ports with a summary of some of their settings (such as Access or Trunk mode and the VLANs for the interface). Switch Ports are highlighted with a light yellow background.
4	The list of Routed Interfaces with a summary of their settings (such as the addressing type and if the interface was auto-detected or has an Auto Detected or User Defined WAN overlay). Routed Interfaces are highlighted with a light blue background.
5	The list of Wireless Interfaces (if available on the Edge device). You can add additional wireless networks by clicking the <b>Add Wi-Fi SSID</b> button. Wireless Interfaces are highlighted with a light gray background.
5	<ul style="list-style-type: none"> <li>■ You can add additional wireless networks by clicking the <b>Add Wi-Fi SSID</b> button. Wireless Interfaces are highlighted with a light gray background.</li> <li>■ You can add sub interfaces by clicking the <b>Add Sub Interfaces</b> button. Sub interfaces are displayed with "SIF" next to the interface.</li> <li>■ You can add secondary IPs by clicking the <b>Add Secondary IP</b> button. Secondary IPs are displayed with "SIP" next to the interface.</li> </ul>



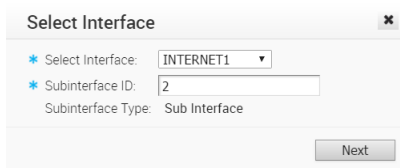
## Sub Interfaces and Secondary IPs



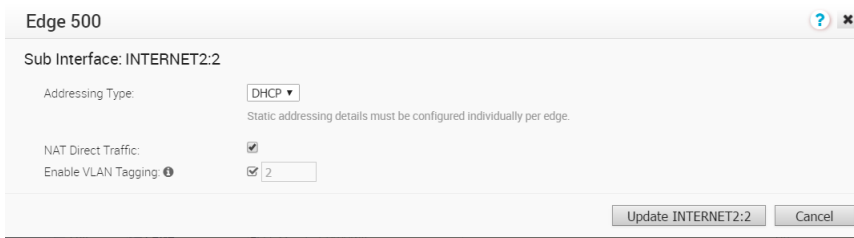
## Adding a Sub Interface

When you add a sub interface to a routed interface, the sub interface gets a subset of the configuration options provided to the parent interface.

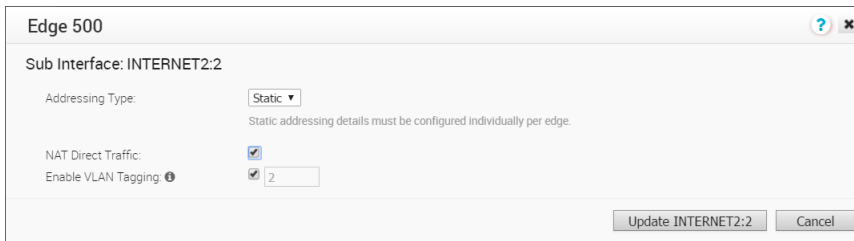
- 1 Click the **Add Sub Interface** button.
- 2 Select an Interface from the drop-down menu and the **Sub Interface ID** in the text box as shown in the **Select Interface** dialog below.



- 3 Click **Next**.
- 4 In the **Sub Interface** dialog box, choose your Addressing Type ( **DHCP** or **Static**).
  - a If you choose the Addressing Type **DHCP**, the **Enable VLAN Tagging** checkbox is selected by default and the Sub Interface ID you chose in the previous dialog displays in the text box.



- b If you choose the Addressing Type **Static**, you have the option of enabling VLAN by selecting the **Enable VLAN Tagging** check box. The Sub Interface ID you chose in the previous dialog displays in the text box.



- 5 Check **NAT Direct Traffic** checkbox if necessary.
- 6 Click the **Update** button.

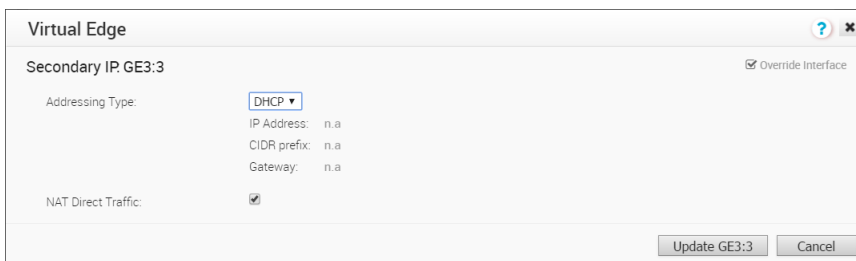
The **Interface** column refreshes, showing the newly created sub interface.

### Adding a Secondary IP Address

- 1 Click the **Add Secondary IP** button.
- 2 Select an Interface from the drop-down menu and the **Sub Interface ID** in the text box as shown in the **Select Interface** dialog below. Note the Sub Interface type is Secondary IP.



- 3 Click **Next**.
- 4 In the **Secondary IP** dialog box, choose your Addressing Type ( **DHCP** or **Static**).



- 5 In the **Secondary IP** dialog box, choose your Addressing Type ( **DHCP** or **Static**).
- 6 Click the **Update** button.

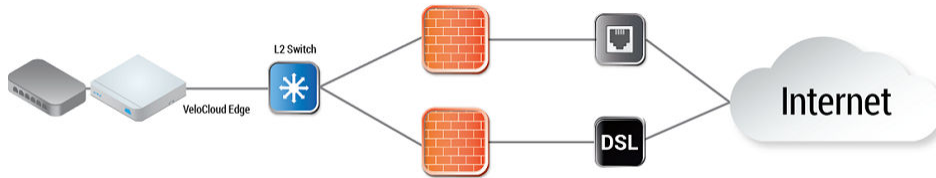
The **Interface** column refreshes, showing the newly created Secondary IP (see the **Interface Settings** image below).

Interface Settings							
		Switch Port Settings			Routed Interface Settings		
Actions	Interface Override	Interface	Mode	VLANs	Addressing	WAN Overlay	OSPF
Edit	<input checked="" type="checkbox"/>	GE1	Access	1 - Corporate			off
Edit	<input checked="" type="checkbox"/>	GE2			DHCP	Auto Detect	off
Edit	<input checked="" type="checkbox"/>	GE3			DHCP	Auto Detect	off
Edit Del	<input checked="" type="checkbox"/>	GE3:3 SIP			DHCP	n.a	n.a
Edit	<input checked="" type="checkbox"/>	GE4			Static	User Defined	on. Area: 1
					CIDR: 192.168.200.2/24 Gateway: 192.168.200.1		

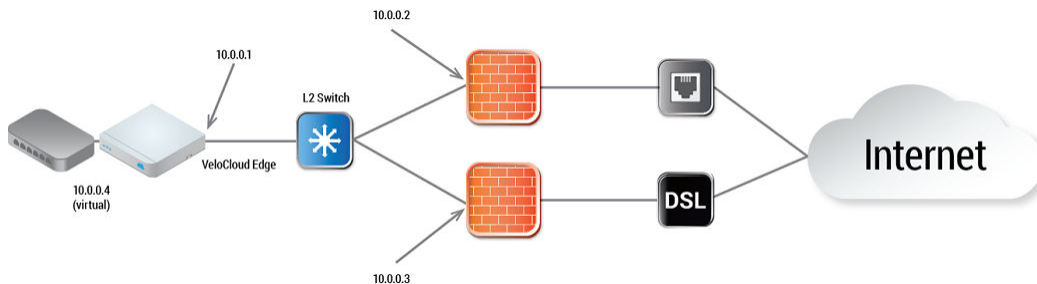
### User-defined WAN Overlay Use Cases

The scenarios wherein this configuration is useful are outlined first, followed by a specification of the configuration itself.

- Use Case 1: Two WAN links connected to an L2 Switch** Consider the traditional data center topology where the VCE is connected to an L2 switch in the DMZ that is connected to multiple firewalls, each connected to a different upstream WAN link.



In this topology, the VeloCloud interface has likely been configured with FW1 as the next hop. However, in order to use the DSL link, it must be provisioned with an alternate next hop to which packets should be forwarded, because FW1 cannot reach the DSL. When defining the DSL link, the user must configure a custom next hop IP address as the IP address of FW2 to ensure that packets can reach the DSL modem. Additionally, the user must configure a custom source IP address for this WAN link to allow the edge to identify return interfaces. The final configuration becomes similar to the following figure:



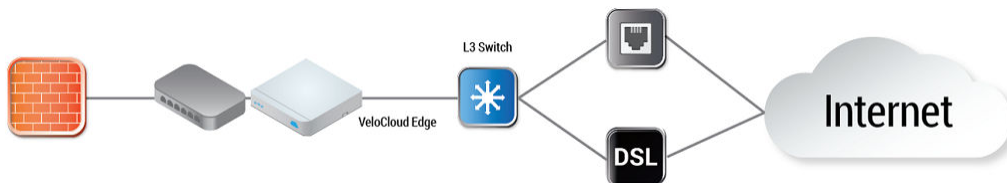
The following paragraph describes how the final configuration is defined.

- The interface is defined with IP address 10.0.0.1 and next hop 10.0.0.2. Because more than one WAN link is attached to the interface, the links are set to “user defined.”



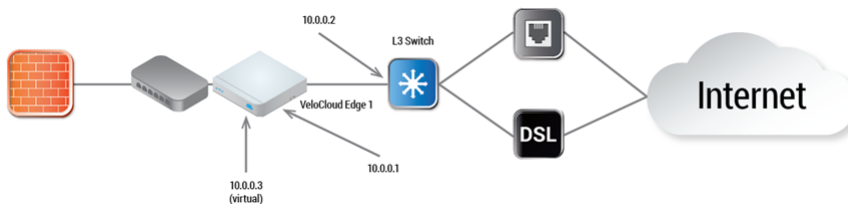
- The Cable link is defined and inherits the IP address of 10.0.0.1 and next hop of 10.0.0.2. No changes are required. When a packet needs to be sent out the cable link, it is sourced from 10.0.0.1 and forwarded to the device that responds to ARP for 10.0.0.2 (FW1). Return packets are destined for 10.0.0.1 and identified as having arrived on the cable link.
- The DSL link is defined, and because it is the second WAN link, the VCO flags the IP address and next hop as mandatory configuration items. The user specifies a custom virtual IP (e.g. 10.0.0.4) for the source IP and 10.0.0.3 for the next hop. When a packet needs to be sent out the DSL link, it is sourced from 10.0.0.4 and forwarded to the device that responds to the ARP for 10.0.0.3 (FW2). Return packets are destined for 10.0.0.4 and identified as having arrived on the DSL link.

- 2 **Case 2: Two WAN links connected to an L3 switch/router:** Alternatively, the upstream device may be an L3 switch or a router. In this case, the next hop device is the same (the switch) for both WAN links, rather than different (the firewalls) in the previous example. Often this is leveraged when the firewall sits on the LAN side of the VCE.



In this topology, policy-based routing will be used to steer packets to the appropriate WAN link. This steering may be performed by the IP address or by the VLAN tag, so we support both options.

Steering by IP: If the L3 device is capable of policy-based routing by source IP address, then both devices may reside on the same VLAN. In this case, the only configuration required is a custom source IP to differentiate the devices.

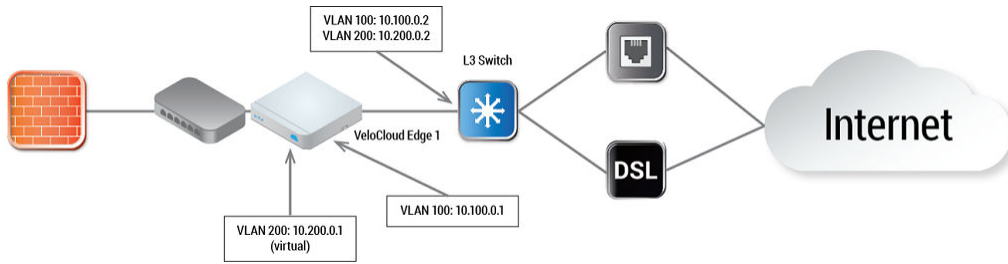


The following paragraph describes how the final configuration is defined.

- The interface is defined with IP address 10.0.0.1 and next hop 10.0.0.2. Because more than one WAN link is attached to the interface, the links are set to “user defined.”
- The Cable link is defined and inherits the IP address of 10.0.0.1 and next hop of 10.0.0.2. No changes are required. When a packet needs to be sent out the cable link, it is sourced from 10.0.0.1 and forwarded to the device that responds to ARP for 10.0.0.2 (L3 Switch). Return packets are destined for 10.0.0.1 and identified as having arrived on the cable link.
- The DSL link is defined, and because it is the second WAN link, the VCO flags the IP address and next hop as mandatory configuration items. The user specifies a custom

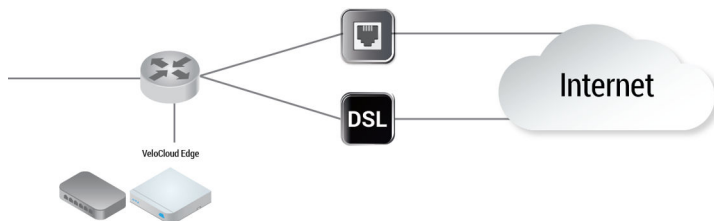
virtual IP (for example, 10.0.0.3) for the source IP and the same 10.0.0.2 for the next hop. When a packet needs to be sent out the DSL link, it is sourced from 10.0.0.3 and forwarded to the device that responds to the ARP for 10.0.0.2 (L3 Switch). Return packets are destined for 10.0.0.3 and identified as having arrived on the DSL link.

Steering by VLAN: If the L3 device is not capable of source routing, or if for some other reason the user chooses to assign separate VLANs to the cable and DSL links, this must be configured.



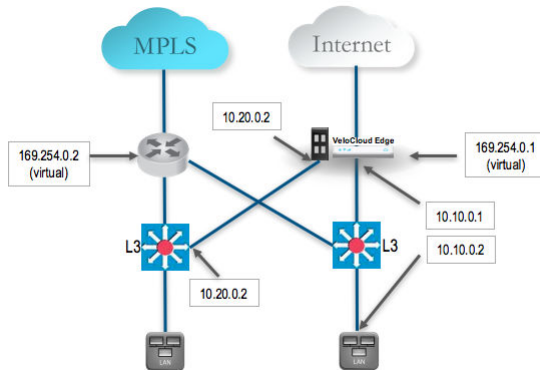
- The interface is defined with IP address 10.100.0.1 and next hop 10.100.0.2 on VLAN 100. Because more than one WAN link is attached to the interface, the links are set to “user defined.”
- The Cable link is defined and inherits VLAN 100 as well as the IP address of 10.100.0.1 and next hop of 10.100.0.2. No changes are required. When a packet needs to be sent out the cable link, it is sourced from 10.100.0.1, tagged with VLAN 100 and forwarded to the device that responds to ARP for 10.100.0.2 on VLAN 100 (L3 Switch). Return packets are destined for 10.100.0.1/VLAN 100 and identified as having arrived on the cable link.
- The DSL link is defined, and because it is the second WAN link the VCO flags the IP address and next hop as mandatory configuration items. The user specifies a custom VLAN ID (200) as well as virtual IP (e.g. 10.200.0.1) for the source IP and the 10.200.0.2 for the next hop. When a packet needs to be sent out the DSL link, it is sourced from 10.200.0.1, tagged with VLAN 200 and forwarded to the device that responds to the ARP for 10.200.0.2 on VLAN 200 (L3 Switch). Return packets are destined for 10.200.0.1/VLAN 200 and identified as having arrived on the DSL link.

3 **Case 3: One-arm Deployments:** One-arm deployments end up being very similar to other L3 deployments.



Again, the VCE shares the same next hop for both WAN links. Policy-based routing can be done to ensure that traffic is forwarded to the appropriate destination as defined above. Alternately, the source IP and VLAN for the WAN link objects in the VeloCloud may be the same as the VLAN of the cable and DSL links to make the routing automatic.

- 4 **Case 4: One WAN link reachable over multiple interfaces:** Consider the traditional gold site topology where the MPLS is reachable via two alternate paths. In this case, we must define a custom source IP address and next hop that can be shared regardless of which interface is being used to communicate.



- GE1 is defined with IP address 10.10.0.1 and next hop 10.10.0.2
- GE2 is defined with IP address 10.20.0.1 and next hop 10.20.0.2
- The MPLS is defined and set as reachable via either interface. This makes the source IP and next hop IP address mandatory with no defaults.
- The source IP and destination are defined, which can be used for communication irrespective of the interface being used. When a packet needs to be sent out the MPLS link, it is sourced from 169.254.0.1, tagged with the configured VLAN and forwarded to the device that responds to ARP for 169.254.0.2 on the configured VLAN (CE Router). Return packets are destined for 169.254.0.1 and identified as having arrived on the MPLS link.

---

**Note** If OSPF or BGP is not enabled, you may need to configure a transit VLAN that is the same on both switches to enable reachability of this virtual IP.

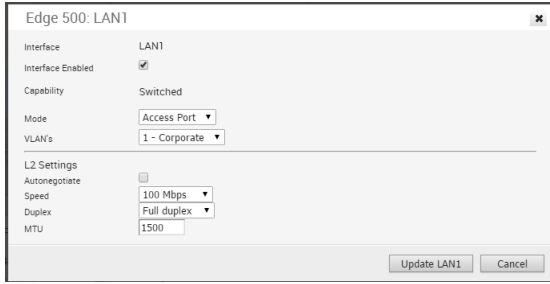
---

## Interface Configuration

Clicking the **Edit** link presents a dialog for updating the settings for a specific interface. The following sections provide a short description for the various dialogs that are presented for the Edge model and interface types.

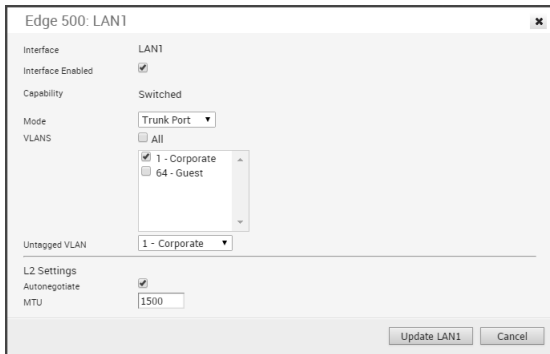
### Edge 500 LAN Access

The following shows the parameters for an Edge 500 LAN interface configured as an Access Port. You can choose a VLAN for the port and select L2 Settings for Autonegotiate (selected by default), Speed, Duplex type, and MTU size (default 1500).



## Edge 500 LAN Trunk

The following shows the parameters for an Edge 500 LAN interface configured as a Trunk Port. You can choose VLANs for the port, how Untagged VLAN data is handled (routed to a specific VLAN or Dropped) and select L2 Settings for Autonegotiate (selected by default), Speed, Duplex type, and MTU size (default 1500).



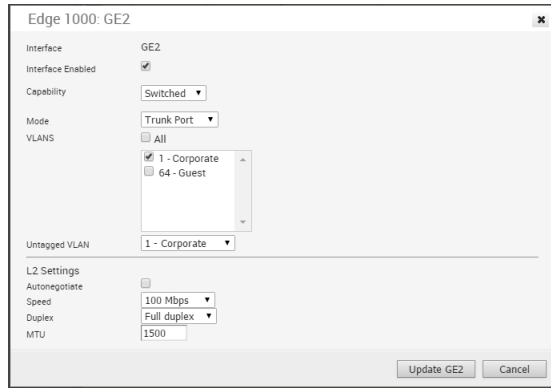
## Edge 1000 LAN Access

The following shows the parameters for an Edge 1000 LAN interface configured as a Switched Access Port. You can choose a VLAN for the port and select L2 Settings for Autonegotiate (selected by default), Speed, Duplex type, and MTU size (default 1500).



## Edge 1000 LAN Trunk

The following shows the parameters for an Edge 1000 LAN interface configured as a Trunk Port. You can choose VLANs for the port, how Untagged VLAN data is handled (routed to a specific VLAN or Dropped) and select L2 Settings for Autonegotiate (selected by default), Speed, Duplex type, and MTU size (default 1500).



Edge 1000: GE2

Interface: GE2

Interface Enabled:

Capability: Switched

Mode: Trunk Port

VLANs:  All,  1 - Corporate,  64 - Guest

Untagged VLAN: 1 - Corporate

L2 Settings

Autonegotiate:

Speed: 100 Mbps

Duplex: Full duplex

MTU: 1500

Update GE2 Cancel

## Edge 500 WAN

The following shows the parameters for an Edge 500 WAN interface with Capability= Routed. You can choose Addressing Type (DHCP, PPPoE, or static), a WAN Overlay (Auto-detect or User Defined), enable OSPF, enable NAT Direct Traffic, and select L2 Settings for Autonegotiate (selected by default), Speed, Duplex type, and MTU size (default 1500).

---

**Note** The port can also be configured as a Switched interface.

---



Edge 500: INTERNET1

Interface: INTERNET1

Interface Enabled:

Capability: Routed

Addressing Type: DHCP

WAN Overlay:  Auto-Detect Overlay

OSPF:  OSPF Not Enabled

NAT Direct Traffic:

L2 Settings

Autonegotiate:

MTU: 1500

Update INTERNET1 Cancel

## Edge 1000 WAN

The following shows the parameters for an Edge 1000 WAN interface with Capability= **Routed**. You can choose Addressing Type (DHCP, PPPoE, or static), a WAN Overlay (Auto-detect or User Defined), enable OSPF, enable NAT Direct Traffic, and select L2 Settings for Autonegotiate (selected by default), Speed, Duplex type, and MTU size (default 1500).

---

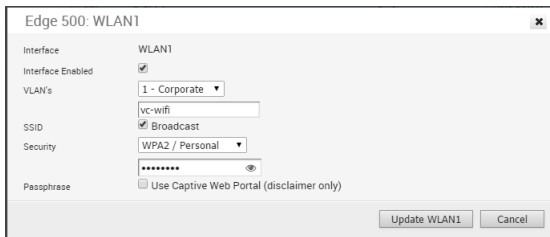
**Note** The port can also be configured as a Switched interface.

---



## Edge 500 WLAN

Initially, two Wi-Fi networks are defined for the VeloCloud Edge 500; one as a Corporate network and one as a Guest network that is initially disabled. Additional wireless networks can be defined, each with a specific VLAN, SSID, and security configuration.



## Security for Wi-Fi Connections

Security for your Wi-Fi connections can be one of three types:

Type	Description
Open	No security is enforced.
WPA2 / Personal	A password is used to authenticate a user.
WPA2 / Enterprise	A Radius server is used to authenticate a user. In this scenario, a Radius Server must be configured in Network Services and the Radius Server must be selected in the <b>Profile Authentication Settings</b> on the <b>Device</b> page. The default settings for Security can also be overridden on the <b>Edge Device</b> page.

## Configure Interface Settings

You can configure the Interface settings for each Edge model. Each Interface on an Edge can be a Switch Port (LAN) or a Routed (WAN) Interface.

The Interface Settings options vary based on the Edge model. For more information on different Edge models and deployments, see [Configure Device Settings](#).

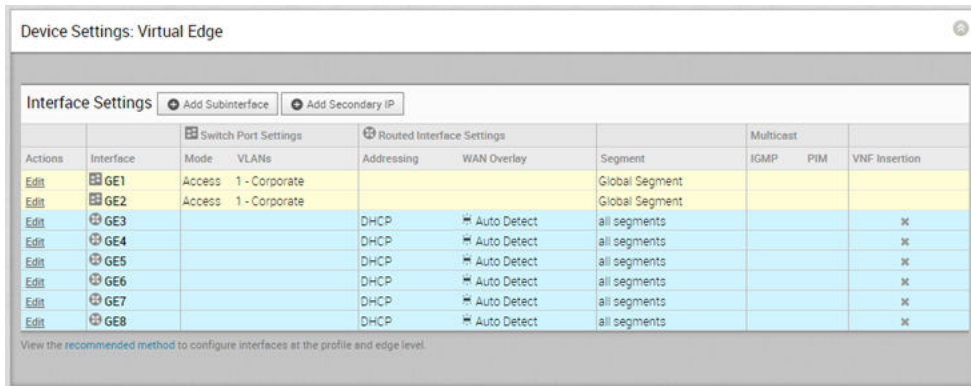
### Procedure

- 1 In the Enterprise portal, click **Configure > Profiles**.

- 2 Click the Device Icon next to a profile, or click the link to the profile, and then click the **Device** tab.
- 3 Scroll down to the **Device Settings** section, which displays the existing Edge models in the Enterprise.



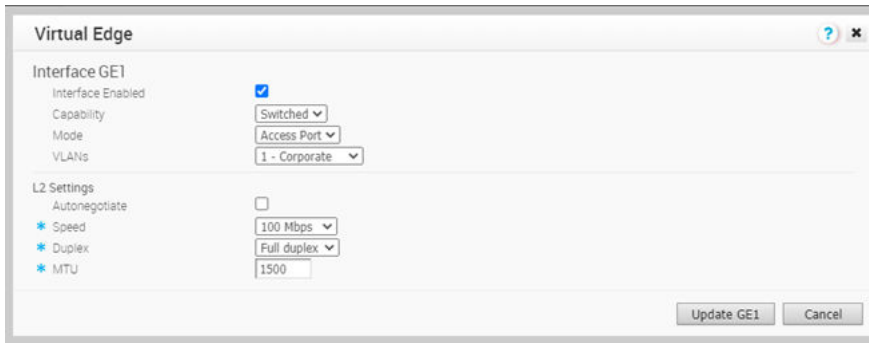
- 4 Click the DOWN arrow next to an Edge model to view the **Interface Settings** for the Edge.



The **Interface Settings** section displays the existing interfaces available in the selected Edge model.

- 5 Click the **Edit** option for an Interface to view and modify the settings.

6 The following image shows the Switch Port settings of an Interface.



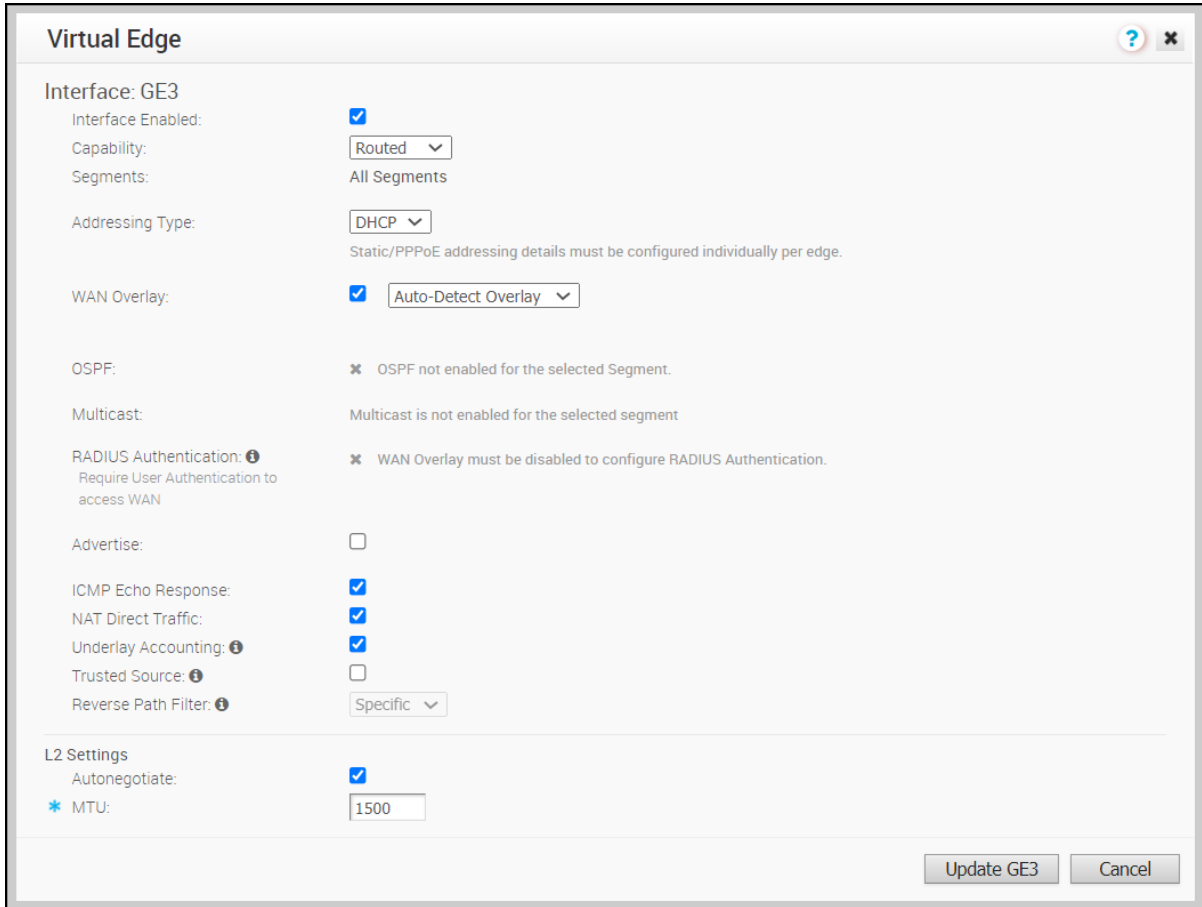
You can modify the existing settings as follows:

Option	Description
Interface Enabled	This option is enabled by default. If required, you can disable the Interface. When disabled, the Interface is not available for any communication.
Capability	For a Switch Port, the option <b>Switched</b> is selected by default. You can choose to convert the port to a routed Interface by selecting the option <b>Routed</b> from the drop-down list.
Mode	Select the mode of the port as Access or Trunk port.
VLANs	For an Access port, select an existing VLAN from the drop-down list. For a Trunk port, you can select multiple VLANs and select an untagged VLAN.
<b>L2 Settings</b>	
Autonegotiate	This option is enabled by default. When enabled, Auto negotiation allows the port to communicate with the device on the other end of the link to determine the optimal duplex mode and speed for the connection.
Speed	This option is available only when <b>Autonegotiate</b> is disabled. Select the speed that the port has to communicate with other links. By default, 100 Mbps is selected.
Duplex	This option is available only when <b>Autonegotiate</b> is disabled. Select the mode of the connection as Full duplex or Half duplex. By default, Full duplex is selected.
MTU	The default MTU size for frames received and sent on all switch interfaces is 1500 bytes. You can change the MTU size for an Interface.

Click **Update** to save the settings.



7 The following image shows the Routed Interface settings.



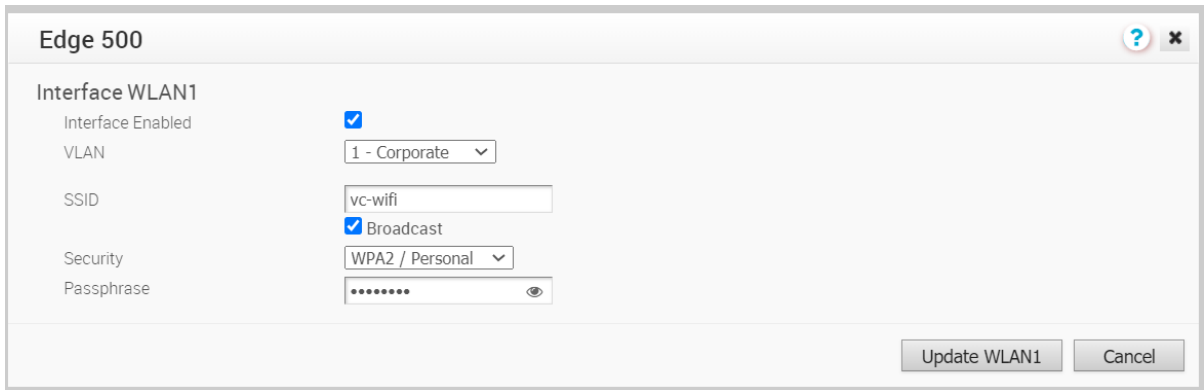
You can modify the existing settings as follows:

Option	Description
Interface Enabled	This option is enabled by default. If required, you can disable the Interface. When disabled, the Interface is not available for any communication.
Capability	For a Routed Interface, the option <b>Routed</b> is selected by default. You can choose to convert the Interface to a Switch Port by selecting the option <b>Switched</b> from the drop-down list.
Segments	By default, the configuration settings are applicable to all the segments.
Addressing Type	By default, DHCP is selected, which assigns an IP address dynamically. If you select Static or PPPoE, you should configure the addressing details for each Edge.
WAN Overlay	By default, this option is enabled with Auto-Detect Overlay. You can choose the User Defined Overlay and configure the Overlay settings. For more information, see <a href="#">Configure Edge WAN Overlay Settings</a> .

Option	Description
OSPF	This option is enabled only when you have configured OSPF for the Profile. Select the checkbox and choose an OSPF from the drop-down list. Click <b>toggle advance ospf settings</b> to configure the Interface settings for the selected OSPF. For more information on OSPF settings, see <a href="#">Enable OSPF</a> .
VNF Insertion	You must disable WAN Overlay and enable Trusted Source to allow VNF insertion. When you insert the VNF into Layer 3 interfaces or sub-interfaces, the system redirects traffic from the Layer 3 interfaces or subinterfaces to the VNF.
Multicast	This option is enabled only when you have configured multicast settings for the Profile. You can configure the multicast settings for the selected Interface. For more information, see <a href="#">Configure Multicast Settings at the Interface Level</a> .
RADIUS Authentication	You must disable WAN Overlay to configure RADIUS Authentication. Select the checkbox to enable RADIUS Authentication on the Interface and add the MAC addresses that should not be forwarded to RADIUS for re-authentication. For more information, see <a href="#">Enabling RADIUS on a Routed Interface</a> .
Advertise	Select the checkbox to advertise the Interface to other branches in the network.
ICMP Echo Response	Select the checkbox to enable the Interface to respond to ICMP echo messages. You can disable this option for the Interface, for security purposes.
NAT Direct Traffic	Select the checkbox to apply NAT to the network traffic sent from the Interface.
Underlay Accounting	This option is enabled by default. If a private WAN overlay is defined on the Interface, all underlay traffic traversing the interface will be counted against the measured rate of the WAN link to prevent over-subscription. If you do not want this behavior (for example, while using one-arm deployments), disable the option.
Trusted Source	Select the checkbox to set the Interface as a trusted source.

Option	Description
Reverse Path Forwarding	<p>You can choose an option for Reverse Path Forwarding only when you have enabled Trusted Source. This option allows traffic on the interface only if return traffic can be forwarded on the same interface. This helps to prevent traffic from unknown sources (malicious traffic) on an enterprise network. If the incoming source is unknown, then the packet is dropped at ingress without creating flows. Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> <li>■ <b>Disabled</b> – Allows incoming traffic even if there is no matching route in the route table.</li> <li>■ <b>Specific</b> – This option is selected by default. The incoming traffic should match a specific return route on the incoming interface. If a specific match is not found, then the incoming packet is dropped. This is a commonly used mode on interfaces configured with public overlays and NAT.</li> <li>■ <b>Loose</b> – The incoming traffic should match any route(Connected/Static/Routed) in the routing table. This allows asymmetrical routing and is commonly used on interfaces that are configured without next hop.</li> </ul>
VLAN	Enter a VLAN ID for the Interface to support VLAN tagging over the port. This option is not available if you have chosen the <b>Addressing Type</b> as DHCP.
<b>L2 Settings</b>	
Autonegotiate	This option is enabled by default. When enabled, Auto negotiation allows the port to communicate with the device on the other end of the link to determine the optimal duplex mode and speed for the connection.
Speed	This option is available only when <b>Autonegotiate</b> is disabled. Select the speed that the port has to communicate with other links. By default, 100 Mbps is selected.
Duplex	This option is available only when <b>Autonegotiate</b> is disabled. Select the mode of the connection as Full duplex or Half duplex. By default, Full duplex is selected.
MTU	The default MTU size for frames received and sent on all routed interfaces is 1500 bytes. You can change the MTU size for an Interface.

8 Some of the Edge models support Wireless LAN. The following image shows WLAN Interface settings.



You can modify the settings as follows:

Option	Description
Interface Enabled	This option is enabled by default. If required, you can disable the Interface. When disabled, the Interface is not available for any communication.
VLAN	Choose the VLAN to be used by the Interface.
SSID	Enter the wireless network name. Select the <b>Broadcast</b> checkbox to broadcast the SSID name to the surrounding devices.
Security	Select the type of security for the Wi-Fi connection, from the drop-down list. The following options are available: <ul style="list-style-type: none"> <li>■ <b>Open</b> – No security is enforced.</li> <li>■ <b>WPA2 / Personal</b> – A password is required for authentication. Enter the password in the <b>Passphrase</b> field.</li> <li>■ <b>WPA2 / Enterprise</b> – A RADIUS server is used for authentication. You should have already configured a RADIUS server and selected it for the Profile and Edge.  To configure a RADIUS server, see <a href="#">Configure Authentication Services</a>.  To select the RADIUS server for a Profile, see <a href="#">Configure Authentication Settings</a>.</li> </ul>

### What to do next

When you configure the Interface Settings for a Profile, the settings are automatically applied to the Edges that are associated with the profile. If required, you can override the configuration for a specific Edge as follows:

- 1 In the Enterprise portal, click **Configure > Edges**.

- 2 Click the Device Icon next to an Edge, or click the link to an Edge and then click the **Device** tab.
- 3 In the **Device** tab, scroll down to the **Interface Settings** section, which displays the interfaces available in the selected Edge.
- 4 Click the **Edit** option for an Interface to view and modify the settings.
- 5 Select the **Override Interface** checkbox to modify the configuration settings for the selected Interface.

## Configure Wi-Fi Radio Settings

The **Wi-Fi radio Settings** determine whether the Wi-Fi radio is enabled, selects the **Country** where the Edge is located, selects the **Band** of the Wi-Fi radio, and the **Channel** used by the Wi-Fi network. If a specific **Country** is selected, a specific Wi-Fi channel can be selected.

## Configure SNMP Settings at Profile Level

SNMP is a commonly used protocol for network monitoring and MIB is a database associated with SNMP to manage entities. SNMP can be enabled by selecting the desired SNMP version as described in the steps below.

### Before you begin:

- To download the VeloCloud Edge MIB: go to the **Remote Diagnostic** screen (**Test & Troubleshooting > Remote Diagnostics**) and run MIB for VeloCloud Edge. Copy and paste results onto your local machine.
- Install all MIBs required by VELOCLOUD-EDGE-MIB on the client host, including SNMPv2-SMI, SNMPv2-CONF, SNMPv2-TC, INET-ADDRESS-MIB, IF-MIB, UUID-TC-MIB, and VELOCLOUD-MIB. All the above-mentioned MIBs, except VELOCLOUD-MIB, can be found online. For VELOCLOUD-MIB, check the VeloCloud website.

### Supported MIBs

- SNMP MIB-2 System
- SNMP MIB-2 Interfaces
- VELOCLOUD-EDGE-MIB
- HOST-RESOURCES-MIB, from RFC 1514

**Procedure to Configure SNMP Settings at Profile Level:**

- 1 Obtain the VELOCLOUD-EDGE-MIB from **Remote Diagnostic**.
- 2 Install all MIBs required by VELOCLOUD-EDGE-MIB. (See "Before you begin" for more information.
- 3 From the navigation panel, go to **Configure > Profiles**.

The **Configuration Profiles** screen appears.

- 4 Select a profile you want to configure SNMP settings for, and click the **Device** icon under the Device column.

The **Configuration Profiles** screen for the selected Profile appears.

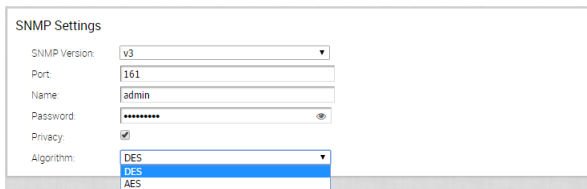
- 5 Scroll down to the **SNMP Settings** area. You can choose between two versions, v2c or v3.
- 6 For a SNMP v2c Config follow the steps below:

- a Check the **v2c** checkbox.
- b Type in a Port in the **Port** textbox. The default setting is 161.
- c In the **Community** textbox, type in a word or sequence of numbers that will act as a 'password' that will allow you access to the SNMP agent.
- d For Allowed IPs:
  - Check the **Any** checkbox to allow any IP to access the SNMP agent.
  - To restrict access to the SNMP agent, uncheck the **Any** checkbox and enter the IP address(es) that will be allowed access to the SNMP agent.



- 7 For a SNMP v3 Config, which provides added security support follow the steps below:

- a Type in a port in the **Port** textbox. 161 is the default setting.
- b Type in a user name and password in the appropriate textboxes.
- c Check the **Privacy** checkbox if you want your packet transfer encrypted.
- d If you have checked the **Privacy** checkbox, choose DES or AES from the **Algorithm** drop-down menu.



- 8 Configure Firewall Settings. After you have configured SNMP Settings, go to Firewall settings (**Configure > Profiles > Firewall**) to configure the Firewall settings that will enable your SNMP settings.

---

**Note** SNMP interface monitoring is supported on DPDK enabled interfaces for 3.3.0 and later releases.

---

## Configure Visibility Mode

This section describes how to configure Visibility mode.

### About Visibility Mode

Even though tracking by MAC Address is ideal (providing a global unique identifier), there's a lack of visibility when an L3 switch is located between the client and the Edge because the switch MAC is known to the Edge, not the device MAC. Therefore, two tracking modes (MAC Address and now IP Address) are available. When tracking by MAC address is not possible, IP address will be used instead.



### Choosing Visibility Mode

To choose a **Visibility Mode**, go to **Configure > Profile > Devices** tab. Select one of the following:

- **Visibility by MAC address**
- **Visibility by IP address**

### Considerations for Using Visibility Mode

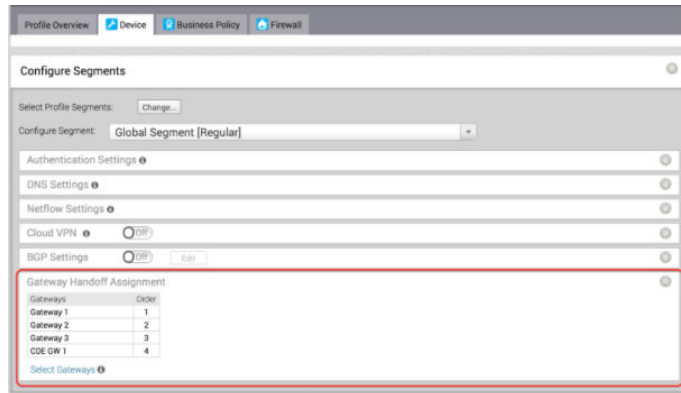
Keep in mind the following when choosing a Visibility mode:

- If **Visibility by MAC address** is selected:
  - Clients are behind L2 SW
  - Client MAC, IP and Hostname (if applicable) will appear
  - Stats are collected based on MAC
- If **Visibility by IP address** is selected:
  - Clients are behind L3 SW
  - SW MAC, Client IP and Hostname (if applicable) will appear
  - Stats are collected based on IP

## Assign Partner Gateways

In order for customers to be able to use partner gateways, your Operator must select the **Enable Partner Handoff** check box for the Gateway to enable this feature. If this feature is available to you, will see the **Partner Gateway Assignment** area in the **Configure > Profiles > Device** tab screen.

**Note** The Partner Gateway Assignment feature has been enhanced to also support segment-based configurations. Multiple Partner Gateways can be configured on the Profile level and/or overridden on the Edge level.

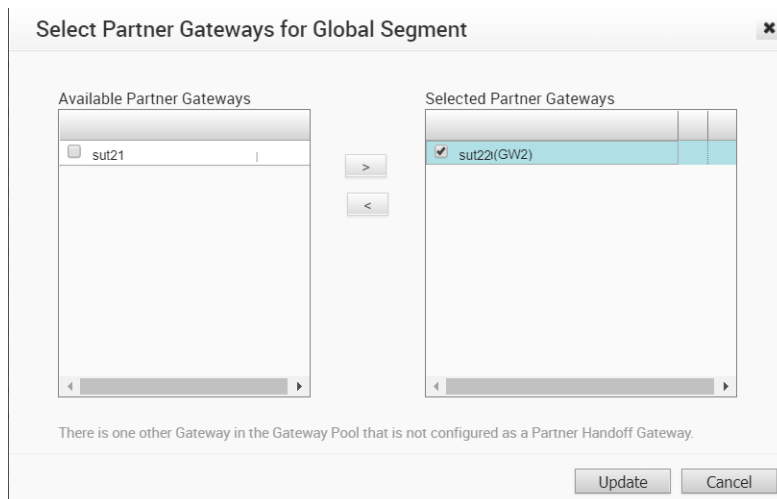


### Select Gateways

To complete this section, you must have this feature enabled. See your Operator for more information.

If there are no Gateways listed in the **Gateway Handoff Assignment** area:

- 1 Click the **Select Gateways** link to select Partner Gateways.
- 2 In the **Select Partner Gateways for Global Segment** dialog box, select an available Partner Gateway from the **Available Partner Gateway** area and move it (using the appropriate arrow) to the **Selected Partner Gateway** area.





Note that only Gateways configured as a Partner Handoff Gateway will be visible in the **Available Partner Gateways** area. If there are other Gateways not configured as a Partner Handoff Gateway, the following message will appear in the dialog box: **There is one other Gateway in the Gateway Pool that is not configured as a Partner Handoff Gateway.**

## Selecting CDE Gateways

In normal scenarios, the PCI traffic runs between customer branch and the Data Center where the PCI traffic is handoff to the PCI network and the Gateways are out of PCI scope. (The Operator can configure the Gateway to exclude PCI Segment by unchecking the CDE role).

In certain scenarios where Gateways can have a handoff to the PCI network and in the PCI scope, the Operator can enable CDE role for the Partner Gateways and these Gateways (CDE Gateways) will be available for the user to assign in the PCI Segments (CDE Type).

To complete this section, you must have this feature enabled. See your Operator for more information.

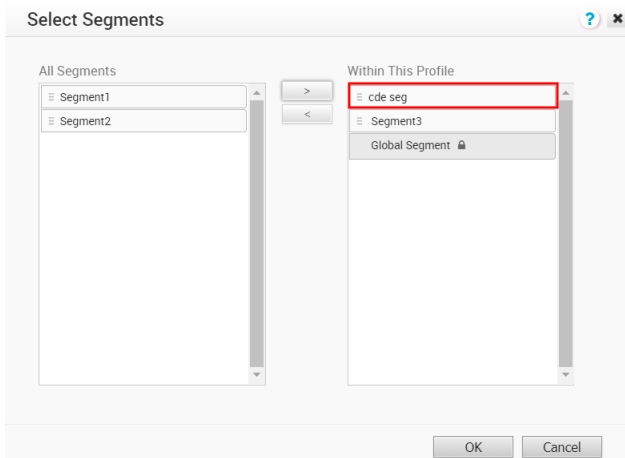
## Assign a CDE Gateway

To assign a CDE Gateway:

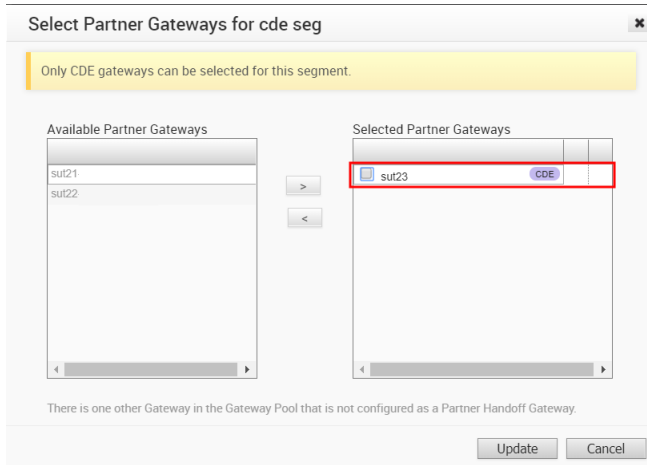
- 1 From the **Configure Segments** window, click the **Select Profile Segments Change** button.



- 2 In the **Select Segments** dialog box, move the available CDE segment from the **Available Segments** area (using the appropriate arrow) to the **Within This Profile** area.



- 3 In the **Gateway Handoff Assignment** area, click the **Select Gateways** link.
- 4 In the **Select Partner Gateways for cde seg** dialog box, select an available CDE Partner Gateway (from the **Available Partner Gateways** area) and move it to the **Selected Partner Gateways** area.



5 Click the **Update** button.

The **Gateway Handoff Assignment** area refreshes with the selected Gateways.

---

**Note** As indicated in the **Select Partner Gateways for cde seg** dialog box, only CDE gateways can be selected for the segment.

---

### Considerations When Assigning Partner Gateways:

Consider the following notes when assigning Partner Gateways:

- Partner Gateways can be assigned at the Profile or Edge level.
- More than two Partner Gateways can be assigned to an Edge (up to 16).
- Partner Gateways can be assigned per Segment.

---

**Note** If you do not see the **Gateway Handoff Assignment** area displayed in the **Configure Segments** window, contact your Operator to enable this feature.

---

## Assign Controllers

The VeloCloud Gateway is enabled for supporting both the data and control plane. In the 3.2 release, VeloCloud introduces a Controller-only feature (Controller Gateway Assignment).

There are multiple use cases which require the VeloCloud Gateway to operate as a Controller only (that is, to remove the data plane capabilities). Additionally, this will enable the Gateway to scale differently, as resources typically dedicated for packet processing can be shifted to support control plane processing. This will enable, for instance, a higher number of concurrent tunnels to be supported on a Controller than on a traditional Gateway. See the following section for a typical use case.

## Use Case: Dynamic Branch-to-Branch via Different Partner Gateways

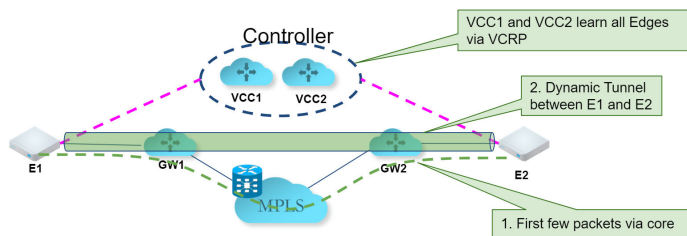
In this scenario, Edge 1 (E1) and Edge 2 (E2) as shown in the image belong to the same enterprise in the Orchestrator. However, they connect to different Partner Gateways (typically due to being in different regions). Therefore, Dynamic Branch-to-Branch is not possible between E1 and E2, but by leveraging the Controller, this is possible.

### Initial Traffic Flow

As shown in the image below, when E1 and E2 attempt to communicate directly, the traffic flow begins by traversing the private network as it would in previous versions of the code. Simultaneously, the Edges will also notify the Controller that they are communicating and request a direct connection.

### Dynamic Tunnel

The Controller signals to the Edges to create the dynamic tunnel by providing E1 connectivity information to E2 and vice versa. The traffic flow moves seamlessly to the new dynamic tunnel if and when it is established.



### Configuring a Gateway as a Controller

In order for customers to be able to use partner gateways, your Operator must select the **Enable Partner Handoff** check box for the Gateway to enable this feature. If this feature is available to you, you will see the **Controller Assignment** area in the **Configure > Profiles > Device** tab screen.

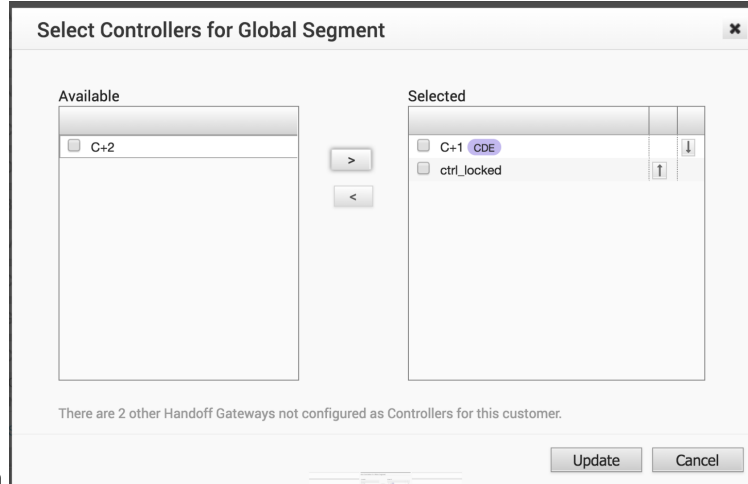
**Note** At least one Gateway in the Gateway Pool should be a "Controller Only" Gateway.

- 1 Go to **Configure > Profiles > Device** tab in the VCO.
- 2 Scroll down to the **Controller Assignment** area.



- 3 In the **Controller Assignment** area, click the **Select Gateways** link.

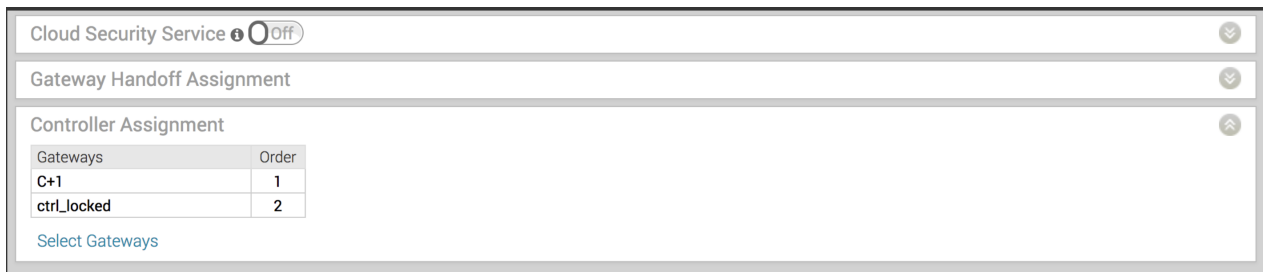
- In the **Select Controllers for Global Segment** dialog, move controllers from the **Available**



area to the **Selected** area.

- Click **Update**.

The **Controller Assignment** area refreshes.



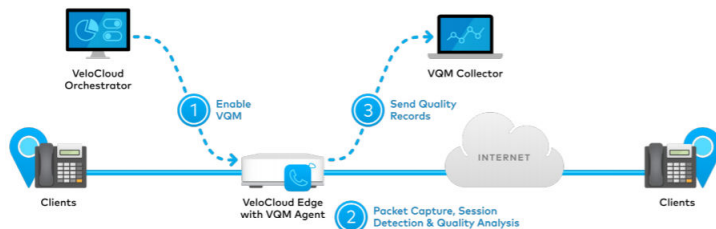
## Voice Quality Monitoring (VQM)

When enabled in the VeloCloud Orchestrator, VeloCloud Voice Quality Monitoring (VQM) diagnoses, monitors, and troubleshoots network issues that impact voice communications.

**Note** The Voice Quality Monitoring (VQM) feature will be deprecated in future releases.

VQM supports 80+ Voice Codecs and provides listening and conversational call quality metrics in both R-Factor and MOS (mean opinion score) formats as well as detailed diagnostic information.

These report metrics provide a high-level health overview of the network and specific details of each call session, which get sent to a RFC6035 compliant VQM Collector (e.g. Oracle Palladion, Telchemy SQMediator, etc.). If there are multiple reports sent from a single call session, the VQM collector will correlate these reports into a single coherent quality record.



## Enabling Voice Quality Monitoring

To enable Voice Quality Monitoring (VQM):

- 1 Go to **Configure > Edges > Device** tab.
- 2 Scroll down to the **Voice Quality Monitoring Settings** area. (See image below).



- 3 Check the **Enabled** checkbox to enable VQM.
- 4 From the **Protocol** drop-down menu, select the Protocol.
- 5 In the **Collectors** text box, type in the IP Address and Port number of the location where you would like to receive the Voice Quality metric reports. To add multiple IP Addresses and Ports, click the "+" symbol. To delete a Collector, click the "-" symbol.
- 6 If applicable, check the **Enable Edge Override** checkbox. Hover over the symbol of the "triangle exclamation point" to view the pop up message (as displayed in the image above).

## Supported RFC6035 Report Metrics

The table below lists the supported RFC6035 report metrics.

Category	RFC 6035 Metrics
Call and User Info	LocalGroup, RemoteGroup, CallID, LocalID, RemoteID, OrigID, LocalAddr, RemoteAddr
Call Config Info	PayloadType, SampleRate, PacketLossConcealment, JitterBufferNominal, JitterBufferMax, JitterBufferAdaptive, SampleRate
Listening Quality	MOS-LQ, ListeningQualityR, SignalLevel, NoiseLevel
Conversational Quality	MOS-CQ, ConversationalQualityR, RoundTripDelay, EndSystemDelay, ResidualEchoReturnLoss
IP Network Health	NetworkPacketLoss, JitterBufferDiscardRate, InterarrivalJitter, MeanAbsoluteJitter, BurstLossDensity, BurstDuration, GapLossDensity, GapDuration

**Note** Refer to RFC 6035 for detailed description of the metrics.

## Supported VOIP Codecs

The following VOIP codecs are supported.

- G.711 A-law /  $\mu$ -law
- G.723.1
- G.723.1 Annex C

- G.728
- G.729
- G.729A/AB
- G.729E
- G.726
- G.722 with PLC App. 3
- MS RTAudio
- IS-54
- iLBC
- Broadvoice16
- Broadvoice32
- AMBE2Plus
- GSM 06.10/06.20/06.30
- QCELP8K
- QCELP13K
- EVRC-A
- EVRC-B
- AMR-NB
- AMR-WB/G.722.2
- AMR-WB+
- SMV
- Siren7/G.722.1
- Siren14/G.722.1C
- Siren14/G.722.1C with LPR
- Siren22 (32, 48 and 64 kbit/s)
- Siren22 with LPR
- G.729 + GIPS NetEQ,
- iLBC + GIPS NetEQ
- GIPS Enhanced G.711  $\mu$ -law
- GIPS Enhanced G.711 A-law
- GIPS iPCM-WB
- Speex Narrowband

- Speex Wideband
- Lucent/elemedia SX7300
- Lucent/elemedia SX9600
- Japanese PDC

This section describes the Cloud VPN.

This chapter includes the following topics:

- [Overview of the Cloud VPN](#)
- [Branch to Non-VeloCloud Site](#)
- [Branch to VeloCloud Hubs](#)
- [Branch to Branch VPN](#)

## Overview of the Cloud VPN

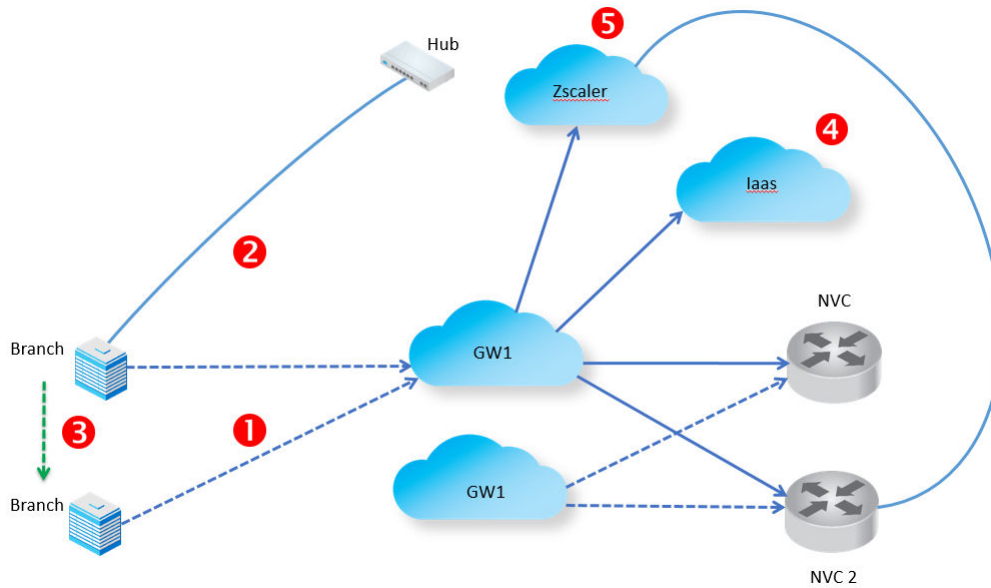
The Cloud VPN enables a VPNC-compliant IPsec VPN that connects VeloCloud and Non-VeloCloud Sites. It also indicates the health of the sites (up or down status) and delivers real-time status of the sites.

Cloud VPN supports the following traffic flows:

- Branch to Non-VeloCloud Site
- Branch to VeloCloud Hub
- Branch to Branch VPN

The following figure represents all three branches of the Cloud VPN. The numbers in the image represent each branch and correspond to the descriptions in the table that follows.

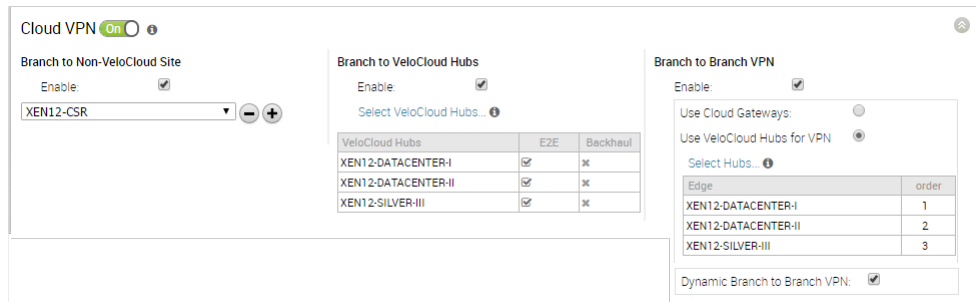




**Number (from above image) Description**

<b>1</b>	Non-VeloCloud Site
<b>2</b>	Branch to VeloCloud Hub
<b>3</b>	Branch to Branch VPN
<b>4</b>	Branch to Non-VeloCloud Site
<b>5</b>	Branch to Non-VeloCloud Site

You can access the 1-click Cloud VPN feature in the VeloCloud Orchestrator (VCO) from **Configure > Profiles > Device Tab** in the **Cloud VPN** area.



**Note** For configuration information for each branch, see the [Chapter 11 Configure a Profile Device](#) section.

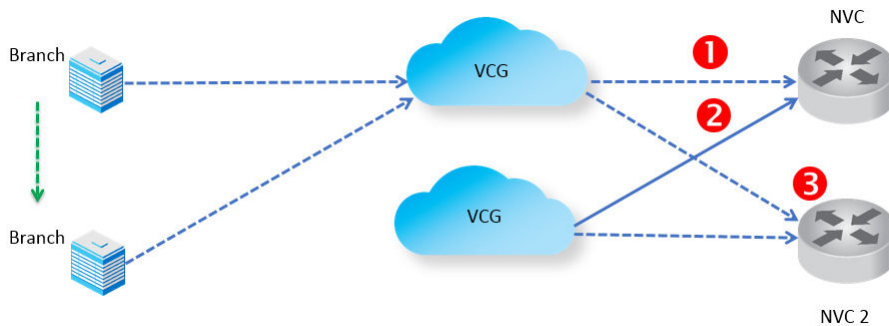
## Branch to Non-VeloCloud Site

This section describes the Branch to Non-VeloCloud site.

### Connect to Customer Data Center with Existing Firewall VPN Router

A VPN connection between the VeloCloud Gateway and the data center firewall (any VPN router) provides connectivity between branches (with VeloCloud Edges installed) and Non-VeloCloud Sites, resulting in ease of insertion, in other words, no customer Data Center installation is required.

The following figure shows a VPN configuration:



Number (from above image)	Description
1	Primary tunnel
2	Redundant tunnel
3	Secondary VPN Gateway

VeloCloud supports VPN connectivity to the following third-party firewalls:

- Cisco ASA
- Cisco ISR
- PaloAlto
- SonicWall
- Generic Router (Router Based VPN)
- Generic Firewall (Policy Based VPN)

For information on how to configure a Branch to Non-VeloCloud Site see [Configure a Non-VeloCloud Site](#).

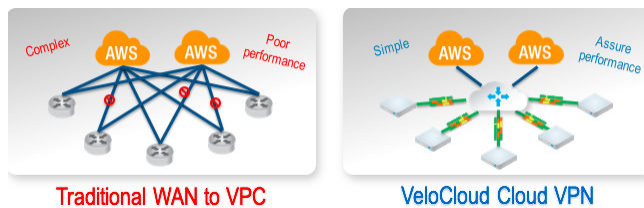
## laas

When configuring with Amazon Web Services (AWS), use the Generic Firewall (Policy Based VPN) option in the Non-VeloCloud Site dialog box.

Configuring with a third party can benefit you in the following ways:

- Eliminates mesh
- Cost
- Performance

As shown in the following figure, VeloCloud Cloud VPN is simple to set up (global networks of VeloCloud Gateways eliminates mesh tunnel requirement to VPCs), has a centralized policy to control branch VPC access, assures performance, and secures connectivity as compared to traditional WAN to VPC.



For information on how to configure using Amazon Web Services (AWS), see the [Configure Amazon Web Services \(AWS\)](#) section.

## Connect to CWS (Zscaler)

Zscaler Web Security provides security, visibility, and control. Delivered in the cloud, Zscaler provides web security with features that include threat protection, real-time analytics, and forensics.

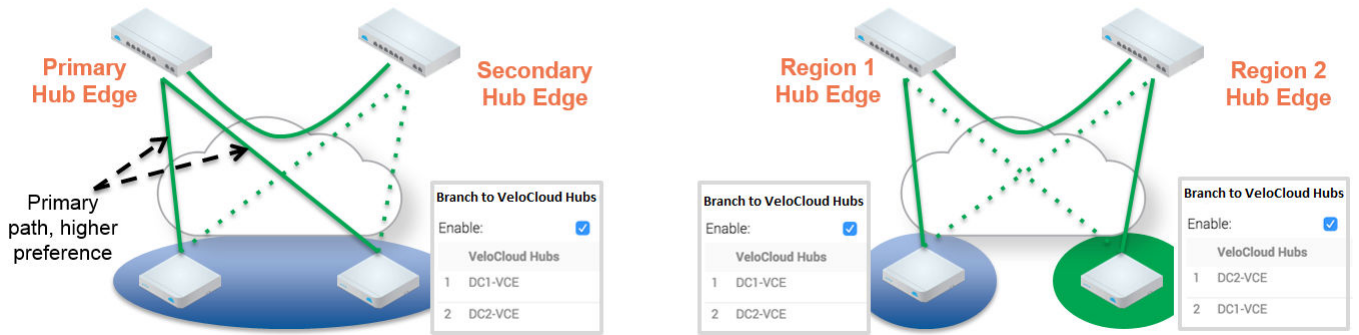
Configuring using Zscaler provides the following benefits:

- **Performance:** Direct to Zscaler (Zscaler via Gateway)
- **Managing proxy is complex:** Enables simple click policy aware Zscaler

## Branch to VeloCloud Hubs

The VeloCloud Hub is an Edge deployed in Data Centers for branches to access Data Center resources. You must set up your VeloCloud Hub in the VeloCloud Orchestrator (VCO). The VCO notifies all the VeloCloud Edges (VCEs) about the Hubs, and the VCEs build secure overlay multi-path tunnel to the Hubs.

The following figure shows how both Active-Standby and Active-Active are supported.



For information on how to configure a Branch to VeloCloud Hub, see "Configure Cloud VPN" in the [Chapter 9 Configure Network Services](#) section.

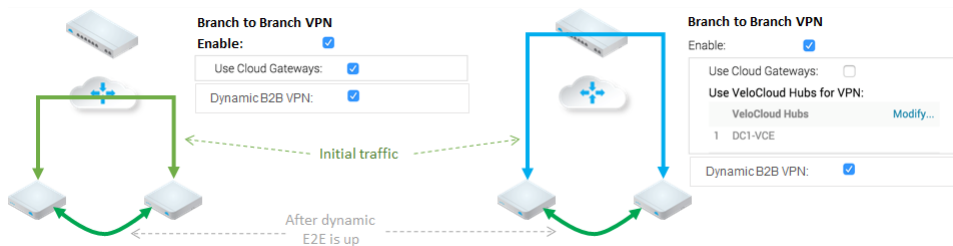
## Branch to Branch VPN

Branch to Branch VPN supports configurations for establishing a VPN connection between branches for improved performance and scalability.

Branch to Branch VPN supports two configurations:

- Cloud Gateways
- VeloCloud Hubs for VPN

The following figure shows Branch to Branch traffic flows for both Cloud Gateway and a VeloCloud Hub.



You can also enable Dynamic Branch to Branch VPN for both Cloud Gateways and Hubs.

## Branch to Branch VPN Isolation by Profile

For hosted SD-WAN customers, there is always a common controller that connects to all the branch Edges, so that Edges have routes to connect to all other Edges. If customers want to prevent branch edges from learning routes or connecting to each other over the SD-WAN overlay, isolation needs to be enabled.

## When Profile Isolation is Enabled

When the Profile Isolation feature is enabled for a profile, the Edges within that profile will only learn:

- Routes to other Edges within its own profile as well as the underlay routes behind those Edges
- Routes to the assigned Hubs as well as underlay routes learned by the Hub

---

**Note** When the Profile Isolation feature is enabled for a profile, the Edges within that profile will not learn routes of other Edges outside of that profile.

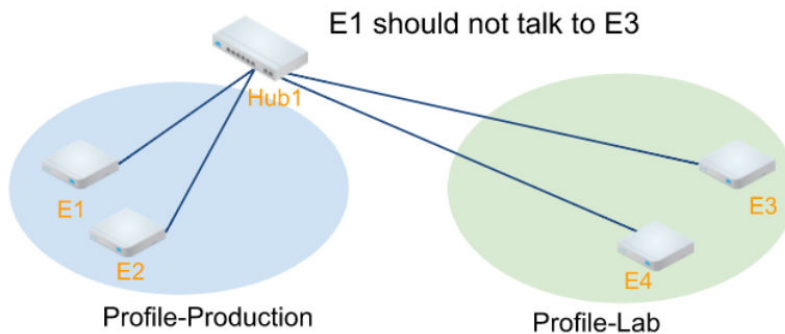
---

### Considerations When Enabling VPN Isolation:

- There is no communication between profiles
- Simplified route controls between regions
- Dynamic B2B within a profile can still be turned on/off

### VPN Isolation by Profile Example

The following figure shows two isolated environments for production and lab. Edges within the profile-production should not have routes to Edges within profile-lab, but they all need to connect to the Hub to reach common services. In this case, the **Profile Isolation** checkbox should be checked for both profiles.




---

**Note** For configuration information, see [Enable Branch to Branch VPN Isolation](#).

---

## Dynamic Branch to Branch

When you enable Dynamic Branch to Branch VPN, the first packet goes through the Cloud Gateway (or the Hub). If the initiating Edge determines that traffic can be routed through a secure overlay multi-path tunnel, and if Dynamic Branch to Branch VPN is enabled, then a direct tunnel is created between the branches.

Once the tunnel is established, traffic begins to flow over the secure overlay multi-path tunnel between the branches. After 180 seconds of traffic silence (forward or reverse from either side of the branches), the initiating edge tears down the tunnel.

## Dynamic Branch to Branch VPN Isolation by Profile

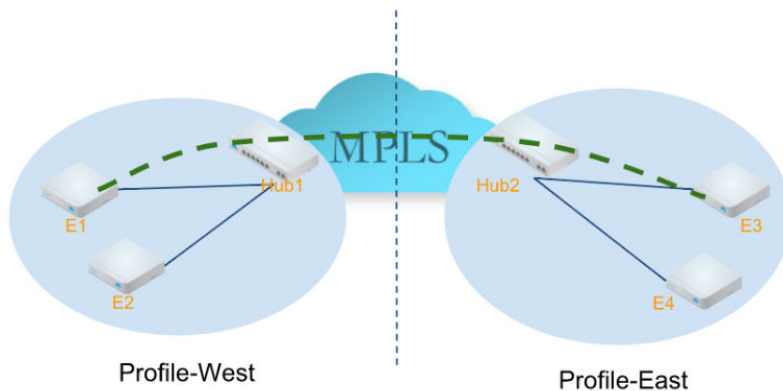
Dynamic Branch to Branch can further be configured to be within the profile only or across different profiles. In some scenarios, you may want to enable Dynamic Branch to Branch within certain regions/domains, but not between regions/domains.

### Considerations when Enabling Dynamic branch to branch VPN Isolation by Profile

- Enforcing Edge to Edge via MPLS Core
- Disable Dynamic Edge to Edge Cross Profiles
- Enable Dynamic Edge to Edge within Profiles

### Example of Dynamic Branch to Branch VPN Isolation by Profile

For example, shown in the diagram below, there are branches in east and west region with a regional Hub for each region. To avoid mid-mile issue, you want to leverage MPLS underlay routing when there are traffic across regions. At the same time, edges within same region should still be able to establish dynamic tunnels. For east region profile and west region profile, you can enable Dynamic Branch to Branch VPN “within profile.” When this is configured, when E1 need to route to E3, it will take the path of E1 overlay to Hub1 and route via MPLS underlay to Hub2 then overlay to E3.




---

**Note** For configuration information, see [Enable Dynamic Branch to Branch VPN Isolation by Profile](#).

---

# Configure Profile Business Policy

# 13

The VeloCloud provides an enhanced Quality of Service feature called Business Policy. This feature is defined using the **Business Policy** tab in a Profile (or at the Edge override level).

---

**Note** If you are logged in using a user ID that has Customer Support privileges, you will only be able to view VeloCloud Orchestrator objects. You will not be able to create new objects or configure/update existing ones.

---

Based on the business policy configuration, the VeloCloud examines the traffic being used, identifies the Application behavior, the business service objective required for a given app (High, Med, or Low), and the Edge WAN Link conditions. Based on this, the Business Policy optimizes Application behavior driving queuing, bandwidth utilization, link steering, and the mitigation of network errors.

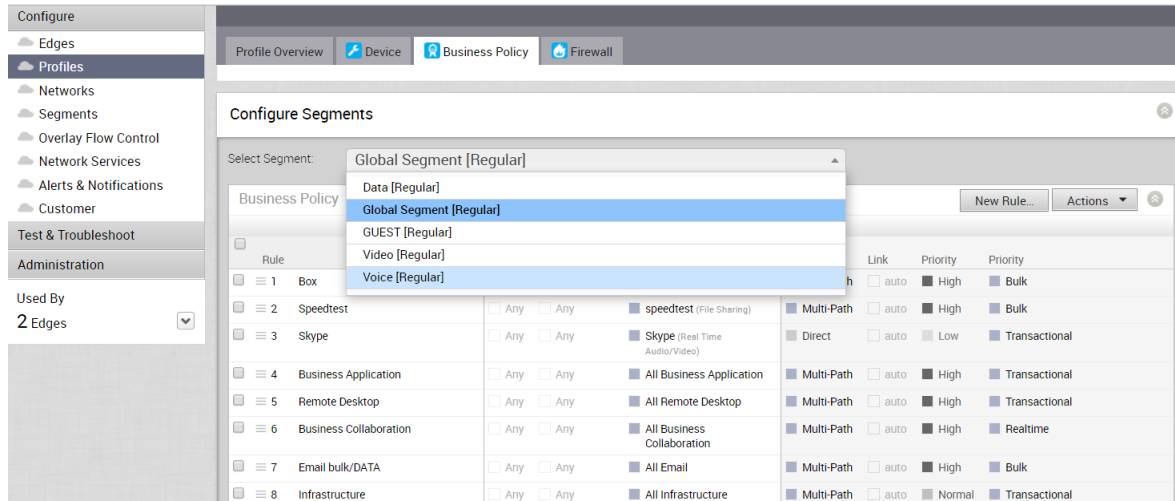
The screen capture below shows some of the Business Policy rules. A number of rules are predefined and you can add your own rules to customize your network operation. Rules are listed in order of highest precedence. Network traffic is managed by identifying its characteristics then matching the characteristics to the rule with the highest precedence.

As shown in the image below, Business Policy Rules are now Segment aware. All Segments available for configuration are listed in the **Configure Segment** drop-down menu.

When you choose a Segment to configure from the **Configure Segment** drop-down menu, the settings and options associated with that Segment appear in the **Configure Segments** area.

**Global Segment [Regular]** is the default segment.

For more information about Segmentation, see [Chapter 8 Configure Segments](#) and [Chapter 11 Configure a Profile Device](#).



**Note** You can move your configured rules up or down in the list of rules to establish precedence by hovering over the numeric value at the left side of the rule and moving the rule up or down. If you hover over the right side of a rule, click the **– (minus) sign** next to the rule to remove it from the list or the **+ (plus) sign** to add a new rule.

This chapter includes the following topics:

- [Create Business Policy](#)
- [Configure Profile Firewall](#)
- [Provision an Edge](#)

## Create Business Policy

Operators, Partners, and Admins of all levels can create a business policy.

**Before you begin:** Know the IP Addresses of your devices and understand the implications of setting a wildcard mask.

**About this task:** New for the 3.3.1 release, there are three IP Address options available: **CIDR Prefix**, **Subnet Mask**, and **Wildcard Mask**.

To create a business policy:

- 1 Click the **New Rule** button to add a Business Policy rule.  
The **Configure Rule** dialog box appears.
- 2 In the **Match** area of the **Configure Rule** dialog box, there are three sections to configure traffic:
  - **Source**
  - **Destination**
  - **Application**

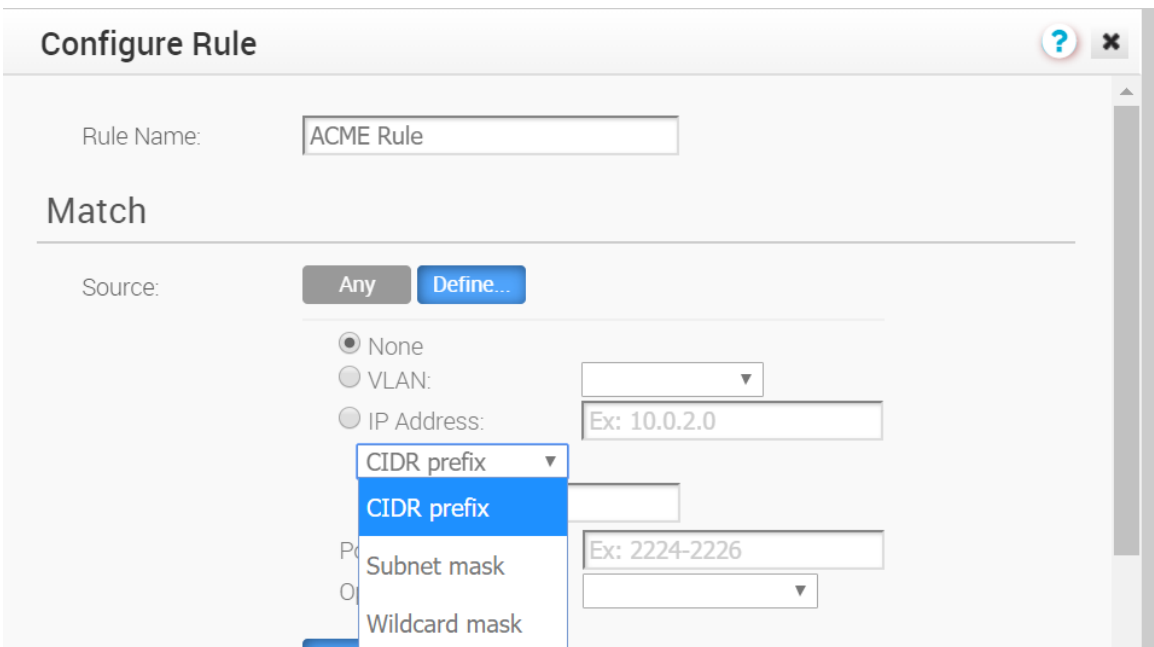


See the steps below to configure the **Source** section of the **Match** area.

- 3 In the **Source** section, click the **Define** button if you want to narrow the source traffic to a specific VLAN, an IP Address, or an Operating System. By default, the **Any** button is selected.
- 4 If you click the **Define** button, complete the appropriate options in the sub steps below.

- a **None**: Selected by default.
- b **VLAN**: Click the **VLAN** radio button and choose the appropriate VLAN from the drop-down menu.
- c **IP Address**: Click the **IP Address** radio button and type in the IP Address, and then choose one of the three options from the drop-down menu (CIDR prefix, Subnet mask, or Wildcard mask). See image below. Wildcard mask and subnet mask are new for the 3.3.1 release. See the table below for a description of each of these options.

Option	Description
<b>CIDR prefix</b>	Choose this option if you want the network defined as a CIDR value (for example: 172.10.0.0 / 16).
<b>Subnet mask</b>	Choose this option if you want the network defined based on a Subnet mask (for example, 172.10.0.0 255.255.0.0).
<b>Wildcard mask</b>	Choose the Wildcard mask option if you want the ability to narrow the enforcement of a policy to a set of devices across different IP subnets that share a matching host IP address value. The Wildcard mask matches an IP or a set of IP addresses based on the inverted Subnet mask. A '0' within the binary value of the mask means the value is fixed and a 1 within the binary value of the mask means the value is wild (can be 1 or 0). For example, a Wildcard mask of 0.0.0.255 (binary equivalent = 00000000.00000000.00000000.11111111) with an IP Address of 172.0.0, the first three octets are fixed values and the last octet is a variable value. Note: After you set up this rule using a Wildcard mask, you are narrowing the number of clients this rule applies to.



- d **Ports**: Type in the ports in the appropriate text box.

- e **Operating System:** From the drop-down menu, choose the Operating System of the Client device.
- 5 In the **Destination** section, you can assign additional parameters to identify the traffic destination as shown in the sub steps below:
- a Define your traffic destination by clicking one of the following radio buttons (**Any**, **Internet**, **VeloCloud Edge**, or **Non-VeloCloud Site**). See [Configure Match Destination](#) for a description of these traffic destinations. NOTE: Branch to Branch Cloud VPN must be enabled before you can define your traffic destination .
  - b Type in the IP Address in the appropriate text box and specify an IP Address option: **CIDR Prefix**, **Wildcard mask**, and **Subnet mask**. (Wildcard mask and Subnet mask are new for the 3.3.1 release).

Option	Description
<b>CIDR prefix</b>	Choose this option if you want the network defined as a CIDR value (for example: 172.10.0.0 / 16).
<b>Subnet mask</b>	Choose this option if you want the network defined based on a Subnet mask (for example, 172.10.0.0 255.255.0.0).
<b>Wildcard Mask</b>	Choose the Wildcard mask option if you want the ability to narrow the enforcement of a policy to a set of devices across different IP subnets that share a matching host IP address value. The Wildcard mask matches an IP or a set of IP addresses based on the inverted Subnet mask. A '0' within the binary value of the mask means the value is fixed and a 1 within the binary value of the mask means the value is wild (can be 1 or 0). For example, a Wildcard mask of 0.0.0.255 (binary equivalent = 00000000.00000000.00000000.11111111) with an IP Address of 172.0.0, the first three octets are fixed values and the last octet is a variable value.

**Note** After you set up this rule using a Wildcard mask, you are narrowing the number of clients this rule applies to.

- c **Enter a Hostname:** Use this field to match the entire hostname or a portion of the hostname. For example, "salesforce" will match traffic to "www.salesforce.com."
  - d **Protocol:** A protocol is a set of rules and standards that define a language devices use to communicate. Choose a protocol from the drop-down menu (**GRE**, **ICMP**, **TCP**, or **UDP**).
  - e **Ports:** A port is an address on a single machine you can tie to a specific piece of software. Enter the appropriate port number in the Port textbox.
- 6 Choose the applications from the **Application** section:
- a Click the **Define** button if you want to choose specific applications. By default, the **Any** button is selected.
  - b From the **Browse** list, select an application category. A list of specific applications display on the right side of the **Browse** list. Scroll down the list and select the specific application you want to define.
  - c Choose a DSCP from the drop-down menu.

7 In the **Actions** area, complete the following sub-steps below:

- a **Priority:** Designate the priority of the rule (**High**, **Normal**, or **Low**). Click the **Rate Limit** checkbox to set limits for inbound and outbound traffic directions.
- b **Network Service:** Choose one of the options (**Direct**, **Multi-Path**, or **Internet Backhaul**). With the **Direct** option, traffic is sent to the destination directly, bypassing the VeloCloud Gateway. The Internet Backhaul option can only be used on Internet rules. For information about these options see the section titled, [Configure Action Network Service](#).
- c **Link Steering:** Choose one of the following options from the table below. (For information about DSCP, DSCP marking for both Underlay and Overlay traffic, see [Link Steering: DSCP Marking for Underlay and Overlay Traffic](#)).

Option	Description
<b>Auto</b>	By default, all applications are put in automatic Link Steering mode. When an application is in the automatic Link Steering mode, the DMPO automatically chooses the best links based on the application type and automatically enables on-demand remediation when necessary. For more information about this topic, see <a href="#">Link Selection: Auto</a> . Enter an Inner Packet DSCP Tag from the drop-down menu and an Outer Packet DSCP Tag from the drop-down menu.
<b>Transport Group</b>	A transport group is a bundle of WAN links grouped together by similar characteristics and functionality. For a description of the Transport Group options below, see <a href="#">Link Steering by Transport Group</a> . Choose <b>Public Wired</b> , <b>Public Wireless</b> , or <b>Private Wired</b> from the drop-down menu. Choose one of the following radio buttons: <b>Mandatory</b> , <b>Preferred</b> , or <b>Available</b> . Choose the Inner and Outer Packet DSP Tag from the appropriate drop-down menus.
<b>Interface</b>	Complete the following options for the Interface below. For more information, see section titled, <a href="#">Link Steering by Interface</a> . <ul style="list-style-type: none"> <li>■ Choose an Interface from the drop-down menu.</li> <li>■ Type in the VLAN in the text box.</li> </ul> <p><b>Note</b> VLAN cannot be specified when using the Multi-Path network service.</p> <ul style="list-style-type: none"> <li>■ Choose one of the following radio buttons: Mandatory, Preferred, Available. If you choose the Preferred option, the <b>Error Correct Before Steering</b> checkbox appears. If you unselect this checkbox, the application will steer before Error Correction occurs.</li> <li>■ <b>ICMP Probe:</b> If applicable, choose an ICMP Probe from the drop-down menu.</li> <li>■ Choose Inner and Outer Packet DSCP Tags from the appropriate drop-down menus.</li> </ul>
<b>WAN Link</b>	For this option, the interface configuration is separate and distinct from the WAN link configuration. You will be able to select a WAN link that was either manually configured or auto-discovered. Select a WAN link from the drop-down menu. For more information, see <a href="#">WAN Link Drop Down Menu</a> .

- d **NAT:** Disable or Enable NAT. For more information, see section titled, [Configure Policy-based NAT](#).
  - e **Service Class:** Choose a Service Class option. The Service Class parameter can be set to Real-time (time sensitive traffic), Transactional, or Bulk. This option is only for a custom application. VeloCloud Apps/Categories fall in one of these categories.
- 8 Click **OK** to configure your rule. The business policy rule will be created successfully.

Reference: [Overlay QoS CoS Mapping](#)

## Configure Match Source

This section describes the **Match Source**, **Destination**, and **Application** selections in more detail. For each of the Match selections, **Any** is used to designate any traffic from a source, destination, or application.

If the Match Source **Define** option is chosen, the source traffic can be narrowed to a specific VLAN, an IP Address, a Port, an Operating System or any combination of selections.

## Configure Match Destination

If the **Match Destination Define** option is chosen, specify additional parameters to identify traffic destination.

The destination can be first narrowed to a type (**Any**, **Internet**, **Edge**, or Non-VeloCloud Site). See the table below for a description of the above-mentioned traffic destinations.

Option	Description
<b>Any</b>	All traffic regardless of destination or routing.
<b>Internet</b>	Traffic that is designated to be sent out to the Internet and not inside the network.
<b>VeloCloud Edge</b>	Traffic designated for another site in the network. Sites such as these would use a VeloCloud Edge.
<b>Non-VeloCloud Site</b>	Sites that do not use a VeloCloud Edge, but that have a route inside the network. A Non-VeloCloud Site is configured in <b>Configure &gt; Network Services</b> .

The destination can then be further defined by specifying an **IP Address**, **Hostname**, **Protocol** (GRE, ICMP, TCP, or UDP), and a port.

**Match Destination** options are particularly useful if the same traffic match pattern needs to be assigned different QoS values depending on the route taken. As an example, you may want to assign a higher priority to traffic destined to a VeloCloud Site versus regular cloud-based internet traffic. This can be easily achieved using the Destination configuration value.

Destination:

Any Define...

Any
  Internet
  Edge
  Non-VeloCloud Site

IP Address

Hostname

Protocol

Ports

## Configure Match Application

If the **Match Application Define** option is chosen, applications can be chosen first by category then by specific application. In addition, a DSCP value can be specified to match traffic coming in with a preset DSCP/TOS tag.

Application:

Any Define...

Browse List

Any Application  
 Anonymizers and Proxies  
**Authentication**  
 Business Application  
 Business

Idaps  
 PPP CHAP  
 PPP PAP  
 radius  
 tacacs\_plus

DSCP

- 46 - EF
- 44 - VA
- 10 - AF11
- 12 - AF12
- 14 - AF13
- 18 - AF21
- 20 - AF22
- 22 - AF23
- 26 - AF31
- 28 - AF32
- 30 - AF33
- 34 - AF41
- 36 - AF42
- 38 - AF43

The following sections describe the **Action Priority**, **Network Service**, **Link Steering**, NAT, and **Service class** selections in more detail.

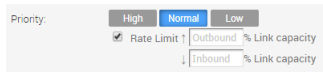
---

**Note** Depending on your **Match** choices, some Actions may not be available. For example, if **All Applications** is chosen, **Network Service** and **Link Actions** are grayed out and are not available for selection. In a similar manner, if a **Destination** of type **Internet** or an **Application** of type **Routeable Apps** is chosen for a VPN profile, an additional **Network Service** option, **Internet Backhaul**, becomes available.

---

## Configure Action Priority

The Action **Priority** parameter allows traffic to be categorized as **High**, **Normal**, or **Low**. A percentage **Rate Limit** can also be applied in both the **Outbound** and **Inbound** direction.



## Configure Action Network Service

While creating or updating a Business Policy rule and action, you can set the **Network Service** to **Direct**, **Multi-Path**, and **Internet Backhaul**.

### Direct

Sends the traffic out of the WAN circuit directly to the destination, bypassing the VeloCloud Gateway. NAT is applied to the traffic if the **NAT Direct Traffic** checkbox is enabled on the **Interface Settings** under the **Device** tab.

### Multi-Path

Sends the traffic from one VeloCloud Edge to another Edge.

### Internet Backhaul

While configuring the business policy rule match criteria, if you define the **Destination** as **Internet**, then the **Internet Backhaul** network service will be enabled.

---

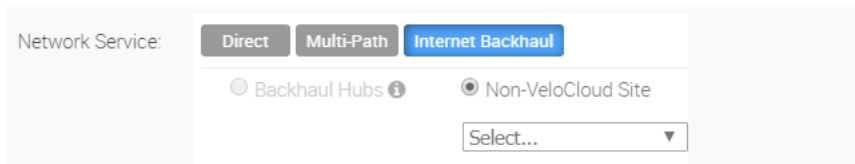
**Note** The **Internet Backhaul** Network Service will only apply to Internet traffic (WAN traffic destined to network prefixes that do not match a known local route or VPN route).

---

When the **Internet Backhaul** is selected, you need to select one of the following:

- **Backhaul Hubs**
- **Non-VeloCloud Site**
- **Cloud Security Service**

You should be able to configure multiple VeloCloud Sites for backhaul to support the redundancy that is inherently built into the Non-VeloCloud Site connection, but keep a consistent behavior of service unavailability leading to traffic being dropped.



If Conditional Backhaul is enabled at the profile level, then it will apply for all Business Policies configured for that profile. You can disable conditional backhaul for selected policies to exclude select traffic (Direct and Multi-Path) from this behavior by selecting the **Disable Conditional Backhaul** checkbox in the **Action** area of the **Configure Rule** screen for the selected business policy.

## Configure Action Link Steering

In the Business Policy, there are four link steering modes: **Auto**, **Transport Group**, **WAN Link**, and **Interfaces**.

**Note** More details about Public/Private WAN links, interface configuration, and user defined options are available in the relevant sections are available at the following links.

### Link Selection: Auto

By default, all applications are given the automatic Link steering mode. This means the DMPO automatically picks the best links based on the application type and automatically enables on-demand remediation when necessary. There are four possible combinations of Link Steering and On-demand Remediation for Internet applications. As mentioned earlier, traffic within the Enterprise (VPN) always goes through the DMPO tunnels, hence it always receives the benefits of on-demand remediation.

Scenario	Expected DMPO Behavior
At least one link satisfies the SLA for the application.	Pick the best available link.
Single link with packet loss exceeding the SLA for the application.	Enable FEC for the real-time applications sent on this link.
Two links with loss on only one link.	Enable FEC on both links.
Multiple links with loss on multiple links.	Enable FEC on two best links.
Two links but one link appears unstable, i.e. missing three consecutive heartbeats.	Mark link un-usable and steer the flow to the next best available link.
Both Jitter and Loss on both links.	<p>Enable FEC on both links and enable Jitter buffer on the receiving side. Jitter buffer is enabled when Jitter is greater than 7 ms for voice and greater than 5 ms for video.</p> <p>The sending DMPO endpoint notifies the receiving DMPO endpoint to enable Jitter buffer. The receiving DMPO endpoint will buffer up to 10 packets or 200 ms of traffic, whichever happens first. The receiving DMPO endpoint uses the original time stamp embedded in the DMPO header to calculate the flow rate to use in de-jitter buffer. If the flow is not sent at a constant rate, the Jitter buffering is disabled.</p>

## Link Steering by Transport Group

A Transport Group represents WAN links bundled together based on similar characteristics and functionality. Defining a Transport Group allows business abstraction so that a similar policy can apply across different Hardware types.

Different locations may have different WAN transports (e.g. WAN carrier name, WAN interface name); DMPO uses the concept of Transport Group to abstract the underlying WAN carriers and interfaces from the Business Policy configuration. The Business Policy configuration can specify the transport group (public wired, public wireless, private wired, etc.) in the steering policy so that the same Business Policy configuration can be applied across different device types or locations, which may have completely different WAN carriers and WAN interfaces. When the DMPO performs the WAN link discovery, it also assigns the transport group to the WAN link. This is the most desirable option for specifying the links in the Business Policy because it eliminates the need for IT administrators to know the type of physical connectivity or the WAN carrier.

If you choose the **Preferred** option, the **Error Correct Before Steering** checkbox displays.

If you select the **Error Correct Before Steering** checkbox, the Loss% variable textbox displays. When you define a loss percentage (4% for example), the Edge will continue to use the selected link or transport group and apply error correction until loss reaches 4%, which is when it will steer traffic to another path. (See image below). When the **Error Correct Before Steering** checkbox is unchecked, the Edge will start steering traffic away if the loss for the link exceed the application SLA - i.e. Real-time application SLA is 0.3% by default. If you disable this checkbox, the application will steer before Error Correction occurs.

The screenshot shows the configuration interface for Network Service. Under 'Network Service', 'Multi-Path' is selected. Under 'Link Steering', 'Transport Group' is selected. The 'Transport Group' dropdown is set to 'Public Wired'. The 'Preferred' radio button is selected. The 'Error Correct Before Steering' checkbox is checked and highlighted with a red box. Below it, the 'Loss (%)' field is set to 4.00. Other options include 'Mandatory', 'Available', 'Inner Packet DSCP Tag' (Leave as is), and 'Outer Packet DSCP Tag' (0 - CS0/DF).

---

**Note** This option is allowed at both the Edge Override level and Profile level.

---



## Link Steering by Interface

For this option, the link steering is tied to a physical interface. Link steering by interface will be used primarily for routing purposes. However, even though it logically should only be used for routing traffic directly from the VeloCloud Site, if the rule specified has a Network Service requiring Internet Multi-path benefits, it will pick a single WAN link connected to the interface.

If you choose the **Preferred** option, the **Error Correct Before Steering** checkbox displays. If you check the box is checked, an additional Loss% variable will become available. When the option is disabled, the Edge will start steering traffic away if the loss for the link exceed the application SLA - i.e. Real-Time application SLA is 0.3% by default. When “Error Correct Before Steering” is applied and Loss percentage defined, let’s say if it’s 4% in this example, the Edge will continue to use the selected link or transport group and apply error correction until loss reaches 4%, which is when it will steer traffic to another path. If you disable this checkbox, the application will steer before Error Correction occurs.

---

**Note** This option is only allowed at the Edge override level. This will ensure that the link options provided always match the VeloCloud Edge hardware model.

---

Link Steering: **Auto** Transport Group **Interface** WAN Link

Interface: INTERNET1

VLAN:

Mandatory  
 Preferred  
 Available

ICMP Probe: [none]

Inner Packet DSCP Tag: 46 - EF

Outer Packet DSCP Tag: 0 - CS0/DF

## WAN Link

For this option, the interface configuration is separate and distinct from the WAN link configuration. You will be able to select a WAN link that was either manually configured or auto-discovered.

## WAN Link Drop Down Menu

You can define policy rules based on specific private links. If you have created private network names and assigned them to individual private WAN overlays, these private link names will display in the **WAN Link** drop-down menu.

For information on how to define multiple private network names and assign them to individual private WAN overlays, see [Private Network Names](#) and *Selecting a Private Name Link*.

If you choose the **Preferred** option, the **Error Correct Before Steering** checkbox displays. If you disable this checkbox, the application will steer before Error Correction occurs.

---

**Note** This option is only allowed at the Edge override level.

---

Link Steering: **Auto** **Transport Group** **Interface** **WAN Link**

WAN Link: e-commerce

Mandatory  
 Preferred  
 Available

Inner Packet DSCP Tag: Leave as is

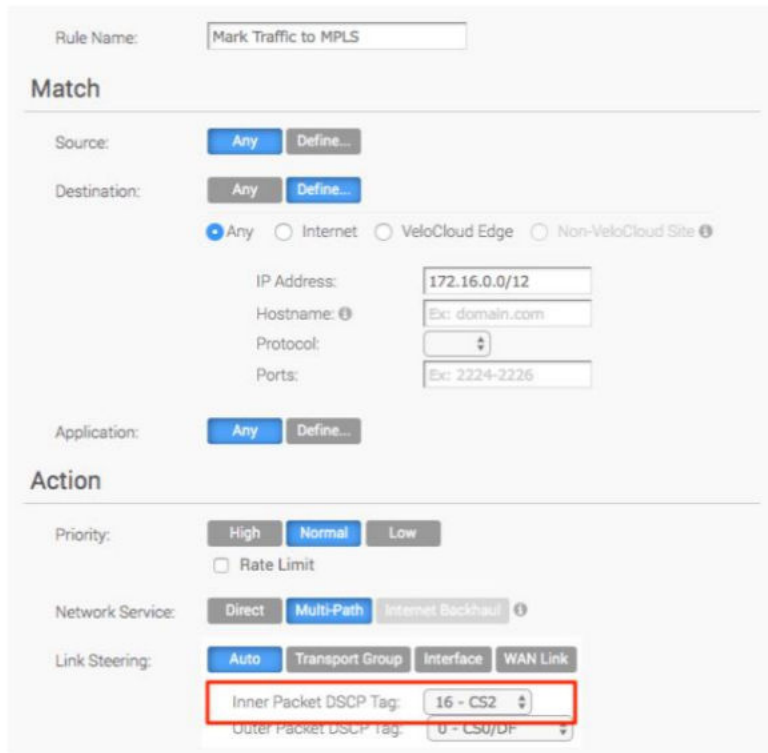
Outer Packet DSCP Tag: 0 - CS0/DF

For the **by Interface** and **by WAN Link** choices, you must select one of the following options:

Option	Description
Mandatory	Indicates that traffic will be sent over the WAN link or link Service-group specified. If the link specified (or all links within the chosen service group) is inactive <b>or</b> if a Multi-path gateway route is unavailable, the corresponding packet will be dropped.
Preferred	Indicates that traffic should preferably be sent over the WAN link or link Service-group specified. If the link specified (or all links within the chosen service group) is inactive, or if the Multi-path gateway route chosen is unstable, or if the link Service Level Objective (SLO) is not being met, the corresponding packet will be steered on the next best available link. If the preferred link becomes available again, traffic will be steered back to the preferred link.
Available	Indicates that traffic should preferably be sent over the WAN link or link Service-group specified as long as it is available (irrespective of link SLO). If the link specified (or all links within chosen service group) are not available, or if the selected Multi-path gateway route is unavailable, the corresponding packet will be steered to the next best available link. If the preferred link becomes available again, traffic will be steered back to the available link.

### Link Steering: DSCP Marking for Underlay and Overlay Traffic Overview

In the 3.3.0 release, VeloCloud supports DSCP remarking of packets forwarded by the Edge to the Underlay. The VMware SD-WAN Edge can re-mark underlay traffic forwarded on a WAN link as long as “Underlay Accounting” is enabled on the interface. DSCP re-marking is enabled in the Business Policy configuration in the Link Steering area. (See section titled, [Create Business Policy](#) for more information). In the example image shown below (assuming the Edge is connected to MPLS with both underlay and overlay traffic forwarded MPLS), if the traffic matches the network prefix 172.16.0.0/12, the Edge will re-mark the underlay packets with a DSCP value of 16 or CS2 and ignore the “Outer Packet DSCP Tag” field. For overlay traffic sent toward MPLS matching the same business policy, the DSCP value for the outer header will be set to the “Outer Packet DSCP tag.”

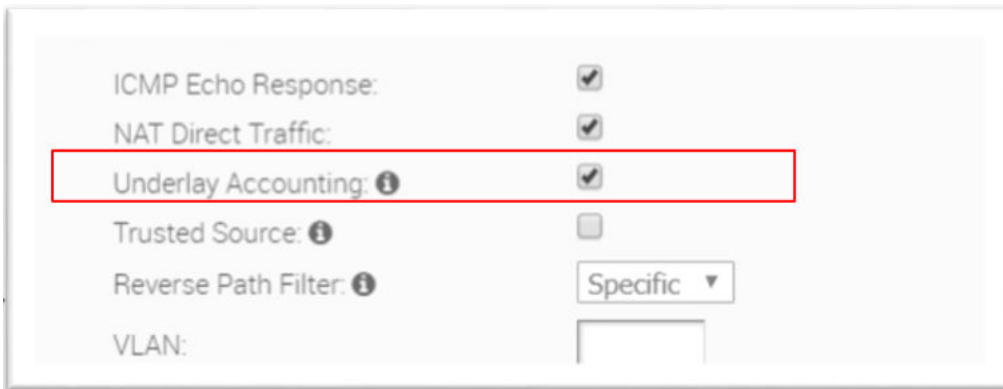


### Link Steering: DSCP Marking for Underlay Traffic Use Case

Edges that are connected to MPLS normally mark DSCP on the packet before sending to the PE for the SP to treat the packet according to the SLA. “Underlay Accounting” must be enabled on the WAN interface for DSCP marking on Underlay traffic via Business Policy to take effect.

### Linking Steering: Underlay DSCP Configuration

- 1 Verify that “Underlay Accounting” is enabled for WAN Overlay by default in the VCO (**Configure > Edge Devices > Device Settings** area). See image below.



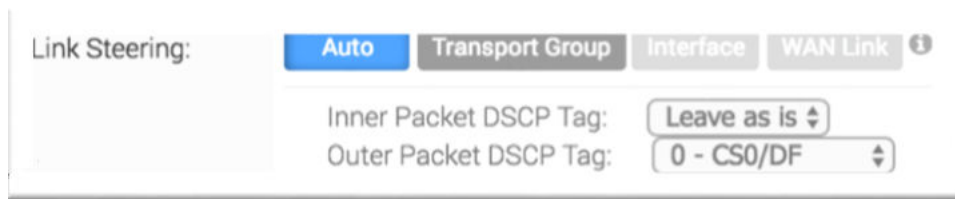
- 2 From the VCO, go to **Configure > Edges > Business Policy**.
- 3 From the **Business Policy** screen, click an existing rule or click the **New Rule** button to create a new rule.

- 4 In the **Action** section, go to the **Link Steering** area.
- 5 Click one of the following as applicable: Auto, Transport Group, Interface, or WAN Link.
- 6 Configure **Match** criteria for the underlay traffic and config “Inner Packet DSCP Tag.” See image below.



### Linking Steering: Overlay DSCP Configuration

- 1 Verify that “Underlay Accounting” is enabled for WAN Overlay by default in the VCO (**Configure**> **Edge Devices** > **Device Settings** area). See image above.
- 2 From the VCO, go to **Configure** > **Edges** > **Business Policy**.
- 3 From the **Business Policy** screen, click an existing rule or click the **New Rule** button to create a new rule.
- 4 In the **Action** section, go to the **Link Steering** area.
- 5 Click one of the following as applicable: Auto, Transport Group, Interface, or WAN Link.
- 6 Configure **Match** criteria for the Overlay traffic and config “Inner Packet DSCP Tag” and “Outer Packet DSCP Tag.” See image below.



### Configure Policy-based NAT

You can configure Policy-based NAT for both Source and Destination. The NAT can be applied to either Non-VeloCloud Site traffic or Internet traffic using Multi-path. When configuring NAT, you must define which traffic to NAT and the action you want to perform. There are two types of NAT configuration: Many to One and One-to-One.

### Accessing NAT

You can access the NAT feature from **Configure** > **Profiles** > **Business Policy tab**, then click the **New Rule** button. The NAT feature is located under the **Action** area.

## Many-to-One NAT Configuration

In this configuration, you can NAT the traffic's source or destination IP originated from the hosts behind the edge to a different unique source or destination IP address. For example, the user can source NAT all the flows destined to a host or server in the Data Center, which is behind the Partner Gateway with a unique IP address, even though they are originated from different hosts behind an Edge.

The following figure shows an example of the Many to One configuration. In this example, all the traffic originating from the hosts that are connected to VLAN **100 - Corporate 2** (behind the Edge destined to an Internet host or a host behind the DC) will get source NAT with the IP address 72.4.3.1.

Many to One NAT

Source NAT all traffic coming thru Vlan100 to 72.4.3.1

Match

Source:

Any Define...

None

VLAN: 100 - Corporate 2

IP Address: Ex: 10.0.2.0/24

Ports: Ex: 2224-2226

Operating System:

NAT:

Disabled Enabled

Source NAT IP: 72.4.3.1

Destination NAT IP:

## One-to-One NAT Configuration

In this configuration, the Branch Edge will NAT a single local IP address of a host or server to another global IP address. If the host in the Non-VeloCloud Site or Data Center sends traffic to the global IP address (configured as the Source NAT IP address in the One-to-One NAT configuration), the VeloCloud Gateway will forward that traffic to the local IP address of the host or server in the Branch.

## Configure Action Service Class

The Service Class parameter can be set to **Real Time** (time-sensitive traffic), **Transactional**, or **Bulk**. This option is only for a custom application. VeloCloud Apps/Categories belong to one of these categories.

Service Class: Real Time Transactional Bulk

## Overlay QoS CoS Mapping

A Traffic Class is defined with a combination of Priority (High, Normal, or Low) and Service Class (Real-Time, Transactional, or Bulk) resulting into a 3x3 matrix with nine Traffic Classes. You can map Application/Category and scheduler weight onto these Traffic Classes. All applications within a Traffic Class will be applied with the aggregate QoS treatment, including Scheduling and Policing.

All applications in a given Traffic Class have a guaranteed minimum aggregate bandwidth during congestion based on scheduler weight (or percentage of bandwidth). When there is no congestion, the applications are allowed into the maximum aggregated bandwidth. A Policer can be applied to cap the bandwidth for all the applications in a given Traffic Class. See the image below for a default of the Application/Category and Traffic Class Mapping.

	HIGH	NORMAL	LOW
REAL-TIME	Business Collaboration	Audio/Video	
TRANSACTIONAL	Remote Desktop, Business App	Infrastructure, Administration, Management, Network Services, Firewalling	IM, Web, PaaS, SaaS, Media, Social
BULK	Email	File Sharing	Storage Backup, POP

The Business Policy contains the out-of-the-box Smart Defaults functionality that maps more than 2,500 applications to Traffic Classes. You can use application-aware QoS without having to define policy. Each Traffic Class is assigned a default weight in the Scheduler, and these parameters can be changed in the Business Policy. Below are the default values for the 3x3 matrix with nine Traffic Classes. See the image below for default of the Weight and Traffic Class Mapping.

	HIGH	NORMAL	LOW
REAL-TIME	35	15	1
TRANSACTIONAL	20	7	1
BULK	15	5	1

### Example:

In this example, a customer has 90 Mbps Internet link and 10 Mbps MPLS on the Edge and the aggregate Bandwidth is 100 Mbps. Based on the default weight and Traffic Class mapping above, all applications that map to Business Collaboration will have a guaranteed bandwidth of 35 Mbps, and all applications that map to Email will have a guaranteed bandwidth of 15 Mbps. Note that business policies can be defined for an entire category like Business Collaborations, applications (e.g. Skype for Business), and more granular sub-applications (e.g. Skype File Transfer, Skype Audio, and Skype Video).

### Configure Overlay QoS CoS Mapping

**Note** The SD-WAN Traffic Class and Weight Mapping feature is editable only if it is enabled by your Operator. To gain access to this feature, see your Operator for more information.

#### To enable Overlay QoS CoS Mapping:

- 1 Go to **Configure > Profiles**.
- 2 Click the link of the appropriate configuration profile.

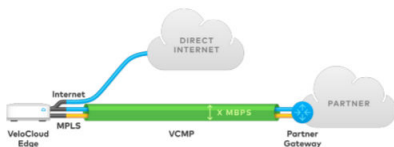
- 3 Click the **Business Policy** tab.
- 4 In the **SD-WAN Traffic Class and Weight Mapping** area, type in numerical values for **Real Time**, **Transactional**, and/or **Bulk** as necessary.
- 5 Check the **Policing** checkbox for a Service Class if necessary.

Service Class / Priority	High	Policing	Normal	Policing	Low	Policing
Real Time	35	<input checked="" type="checkbox"/>	15	<input type="checkbox"/>	1	<input type="checkbox"/>
Transactional	20	<input type="checkbox"/>	7	<input type="checkbox"/>	1	<input type="checkbox"/>
Bulk	15	<input type="checkbox"/>	5	<input type="checkbox"/>	1	<input type="checkbox"/>

## Tunnel Shaper for Service Providers with Partner Gateway

This section describes the Tunnel Shaper for Service Providers with the Partner Gateway.

Service Providers may offer SD-WAN services at a lower capacity compared to the aggregated capacity of WAN links at the local branch. For example, customers may have purchased a broadband link from another vendor and SP offering SD-WAN services, and hosting VeloCloud Partner Gateway has no control over the underlay broadband link. In such situations, in order to ensure that the SD-WAN service capacity is being honored and to avoid congestion towards Partner Gateway, a Service Provider can enable the DMPO Tunnel Shaper between the tunnel and the Partner Gateway.



### Tunnel Shaper Example:

As shown in the diagram above, the VCE has dual links, 20 Mbps Internet and 20 Mbps MPLS, with 35 Mbps SD-WAN service from SP. To ensure that the traffic towards Partner Gateway doesn't exceed 35 Mbps (displayed as "X" in the image above), a Service Provider can place a Tunnel Shaper on the DMPO tunnel.

## Configure Rate-Limit Tunnel Traffic


**Note** The Rate-Limit Tunnel Traffic feature is editable only if it is enabled by your Operator. To gain access to this feature, see your Operator for more information.

### To enable Rate-Limit Tunnel Traffic:

- 1 Go to **Configure > Profiles** from the navigation panel.
- 2 Click the link of the appropriate configuration profile.

- 3 Click the **Business Policy** tab.
- 4 In the **SD-WAN Overlay Rate Limit** area, check the **Rate-Limit Tunnel Traffic** check box. (See image below).
- 5 Select either the **Percent** or **Rate (Mbps)** radial buttons.
- 6 In the **Limit** text box, type in a numerical limit to the Tunnel Traffic.
- 7 Click the **Save Changes** button located on the top, right corner of the VCO screen.

**SD-WAN Overlay Rate Limit**

Rate-Limit Tunnel Traffic:  

Percent (%):

Rate (Mbps):

Limit:

## Configure Profile Firewall

VeloCloud provides multiple types of firewall configuration. Firewall configuration is defined using the Firewall tab in a Profile. Firewall configuration is for inbound and outbound firewalls and to define direct Edge access.

---

**Note** If you are logged in using a user ID that has Customer Support privileges, you will only be able to view VeloCloud Orchestrator objects. You will not be able to create new objects or configure/update existing ones.

---

## Configure Firewall Rules

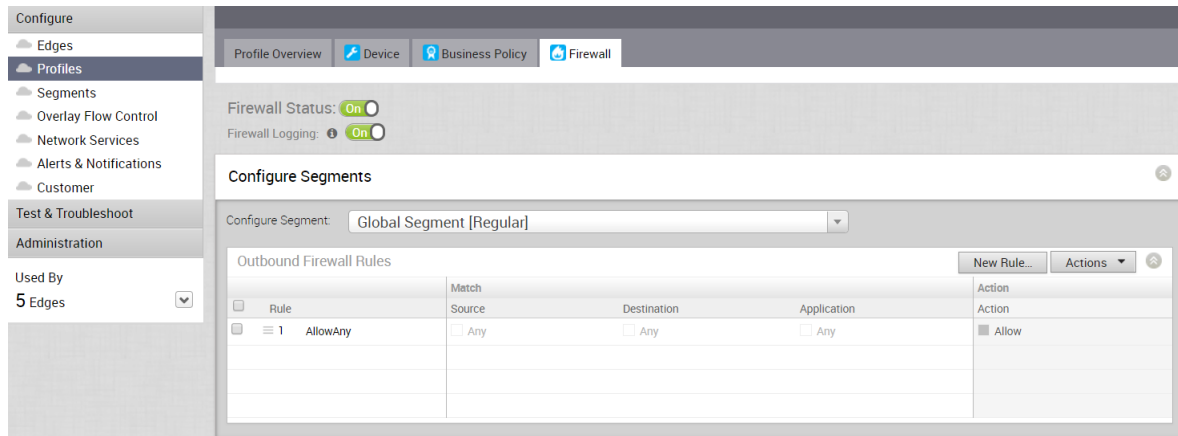
Firewall rules are used to configure Allow or Deny Access Control List (ACL) rules. The rules are used to determine what traffic is allowed between VLANs or out from the LAN to the Internet. The rules can be based on applications, application categories, source IP address/port, destination IP address/port, DSCP tags or protocol.

Network traffic is managed by identifying its characteristics then matching the characteristics to the rule with the highest precedence. The following screen capture shows the initial definition of firewall rules. Note that Firewall function can be disabled using the Firewall Status switch.

Firewall Profiles are Segment aware. All Segments available for configuration are listed in the Configure Segment drop-down menu.

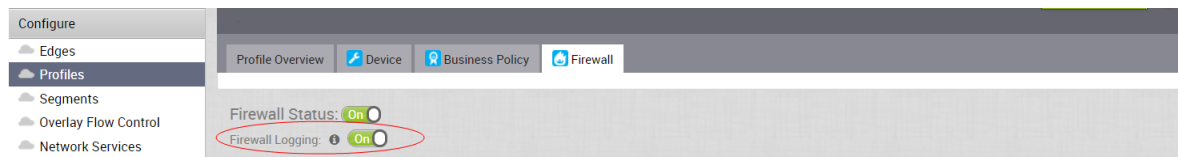
When you choose a Segment to configure from the **Configure Segment** drop-down menu, the settings and options associated with that Segment appear in the **Configure Segments** area. **Global Segment [Regular]** is the default Segment.





For more information about Segmentation, see [Chapter 8 Configure Segments](#) and [Chapter 11 Configure a Profile Device](#).

The Firewall Logging feature must be enabled to log individual firewall logging events.



**Note** An Operator must enable Firewall logging in order for an Enterprise user to enable or disable it.

For the 3.3.1 release, there are three new IP Address options available: **CIDR Prefix**, **Wildcard Mask**, and **Subnet Mask**.

To create a Firewall rule:

- 1 Click the **New Rule** button to create a new Firewall rule.  
The **Configure Rule** dialog box appears. From this dialog box, you can select **Source**, **Destination**, and **Application** characteristics to match. Given a match, the Firewall action defined in the rule will be applied.
- 2 In the **Match** area of the **Configure Rule** dialog box, there are three sections to configure the traffic: **Source**, **Destination**, and **Application**. See the steps below to configure the **Source** section of the **Match** area.
- 3 In the **Source** section, click the **Define** button if you want to narrow the source traffic to a specific VLAN, an IP Address, or MAC Address, as described in the steps that follow.
- 4 By default, the **Any** button is selected. If you click the **Define** button, complete the appropriate options in the sub steps below.
  - a **None**: Selected by default.
  - b **VLAN**: Click the VLAN radio button and choose the appropriate VLAN from the drop-down menu.

- c **IP Address:** Click the IP Address radio button and type in the IP Address and choose one of the three options from the drop-down menu.

---

**Note** **Wildcard Mask** and **Subnet Mask** are new for the 3.3.1 release.

---

Option	Description
<b>CIDR prefix</b>	Choose this option if you want the network defined as a CIDR value (for example: 172.10.0.0 / 16).
<b>Subnet mask</b>	Choose this option if you want the network defined based on a Subnet mask (for example, 172.10.0.0 255.255.0.0).
<b>Wildcard Mask</b>	Choose the Wildcard mask option if you want the ability to narrow the enforcement of a policy to a set of devices across different IP subnets that share a matching host IP address value. The Wildcard mask matches an IP or a set of IP addresses based on the inverted Subnet mask. A '0' within the binary value of the mask means the value is fixed and a 1 within the binary value of the mask means the value is wild (can be 1 or 0). For example, a Wildcard mask of 0.0.0.255 (binary equivalent = 00000000.00000000.00000000.11111111) with an IP Address of 172.0.0, the first three octets are fixed values and the last octet is a variable value.

---

**Note** After you set up this rule using a Wildcard mask, you are narrowing the number of clients this rule applies to.

---

- d **MAC Address:** Type in the MAC Address in the appropriate text box.
  - e **Ports:** Type in the ports in the appropriate text box.
- 5 In the **Destination** section, you can assign additional parameters to identify the traffic destination, as described in the following sub-steps:
- a Define your traffic destination by clicking one of the following radio buttons (**Any**, **Internet**, **VeloCloud Edge**, or **Non-VeloCloud Site**).

- b Type in the IP Address in the appropriate text box and specify an IP Address option: **CIDR Prefix**, **Wildcard Mask**, and **Subnet Mask**.

---

**Note** **Wildcard Mask** and **Subnet Mask** are new for the 3.3.1 release.

---

Option	Description
<b>CIDR prefix</b>	Choose this option if you want the network defined as a CIDR value (for example: 172.10.0.0 / 16).
<b>Subnet mask</b>	Choose this option if you want the network defined based on a Subnet mask (for example, 172.10.0.0 255.255.0.0).
<b>Wildcard Mask</b>	Choose the Wildcard mask option if you want the ability to narrow the enforcement of a policy to a set of devices across different IP subnets that share a matching host IP address value. The Wildcard mask matches an IP or a set of IP addresses based on the inverted Subnet mask. A '0' within the binary value of the mask means the value is fixed and a 1 within the binary value of the mask means the value is wild (can be 1 or 0). For example, a Wildcard mask of 0.0.0.255 (binary equivalent = 00000000.00000000.00000000.11111111) with an IP Address of 172.0.0, the first three octets are fixed values and the last octet is a variable value.

---

**Note** After you set up this rule using a Wildcard mask, you are narrowing the number of clients this rule applies to.

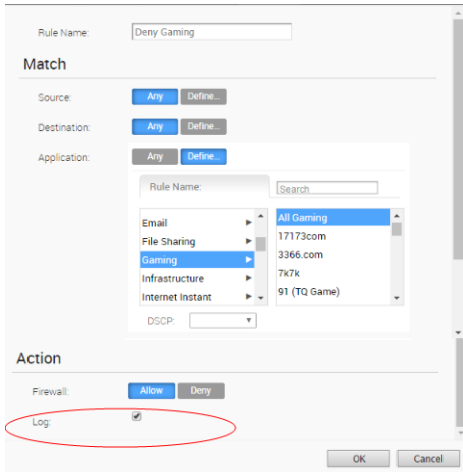
---

- c **Protocol:** Type in the Protocol in the appropriate text box.
- d **Ports:** Type in the ports in the appropriate text box.
- 6 Choose the applications to apply the Firewall rule in Application section:
- Click the **Define** button if you want to choose specific applications. By default, the **Any** button is selected.
  - From the Browse List, select an application category. A list of specific applications display on the right side of the Browse list. Scroll down the list and select the specific application you want to define.
  - Choose a DSCP from the drop-down menu.
- 7 In the **Actions** area, click Allow or Deny the firewall rule.
- 8 Click **OK** to create the Firewall rule.

The **Profile Firewall** page allows you to define **Outbound Firewall Rules** and **Edge Access**. Inbound rules must be defined at each Edge.

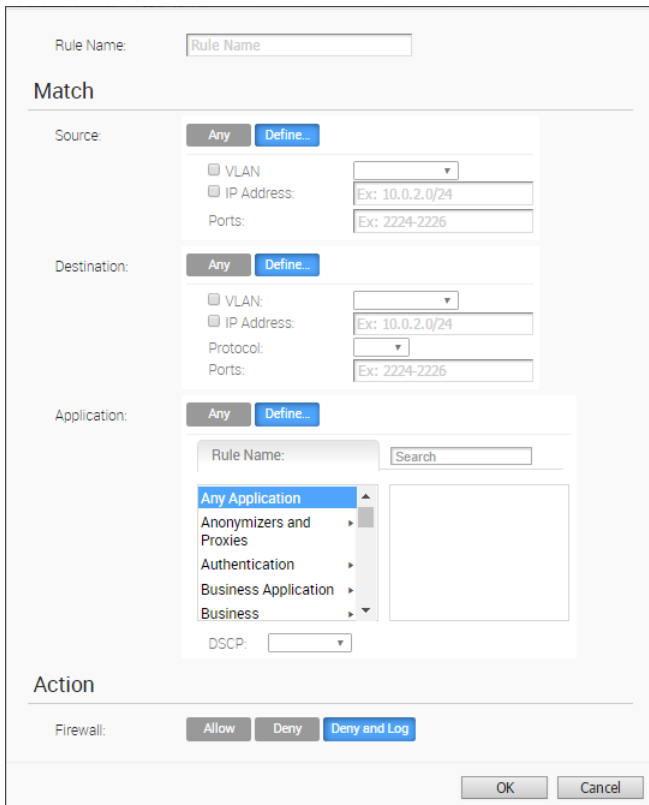
## Outbound Firewall Rules

Click **New Rule** to add a new Firewall rule. The following dialog box appears. Using the dialog box, you can select Source, Destination, and Application characteristics to match. Given a match, the Firewall action defined in the rule will be applied.



**Note** When a **Deny** action is detected by the firewall, an Event is generated. The event can be seen in the list of events using **Monitor -> Events**. When a **Deny and Log** action is detected, the Firewall logs the event locally.

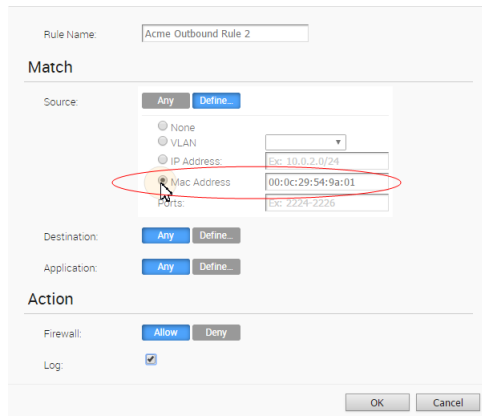
The following screen capture shows expanded options for Source, Destination, and Application. You can use the parameters to finely select where you want the Firewall rule to be applied.



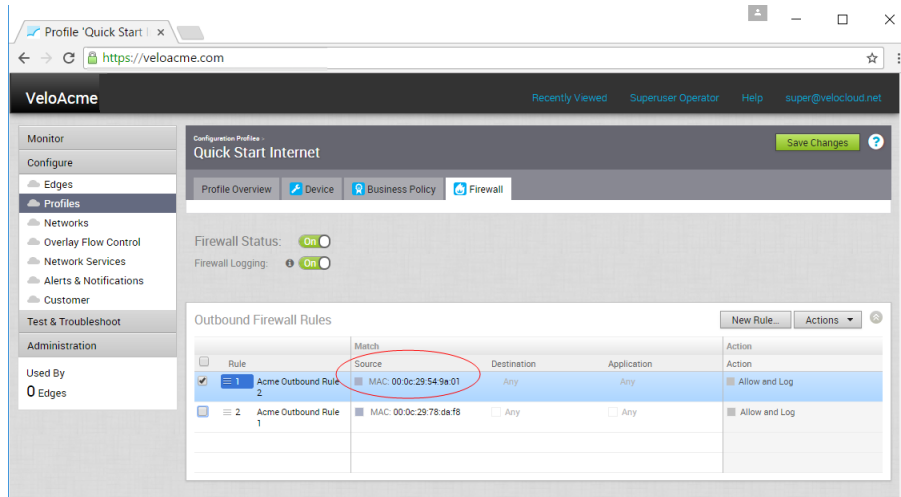
## Mac Address Filtering

Mac Address Filtering is another **Source** option available in the **Match** area of the dialog box shown below. You can use the Mac Address feature when you want a filtering rule to apply to a specific client no matter what subnet the client is associated with. (The filtering rule is independent of the client's subnet).

To enable this filter, choose the **Mac Address** radio button, type in the Mac address, and click the **OK** button.



The **Outbound Firewall Rules** area updates as shown below.



## Edge Access

Edge Access behavior can be defined on the **Firewall** page. Accessing an Edge by remotely accessing the Edge Local UI or accessing the Edge via SNMP can be set to **Deny All**, **Allow All**, or **Allow for specific IP addresses**. Accessing an Edge by Support Access can be set to **Deny All** or **Allow for specific IP addresses**. A Local Web UI Port Number can also be specified.

For security reasons, please keep Support Access and the Local Web UI disabled.

**Note** All access is disabled by default.

## Create or Select a Network

This section describes how to create or select a network.

---

**Note** If you are logged in using a user ID that has Customer Support privileges, you will only be able to view VeloCloud Orchestrator objects. You will not be able to create new objects or configure/update existing ones.

---

**Note** This tab is not used for the Segmentation feature.

---

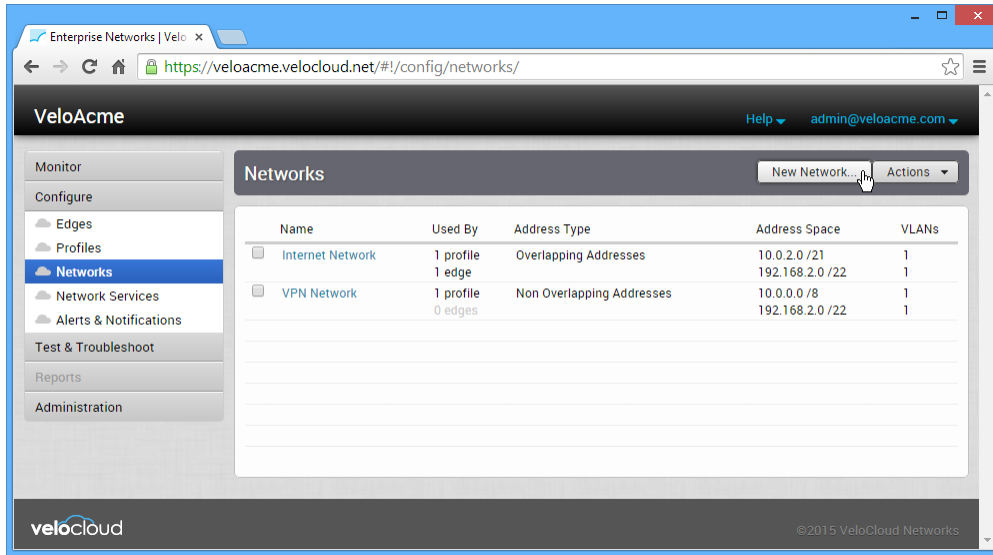
### Steps Overview

The following steps are required for a Network configuration:

- 1 Create a new Network or select an existing Network
- 2 Configure Corporate Networks
  - a Configure Address Space
  - b Configure VLANs
- 3 Configure Guest Networks
  - a Configure Address Space
  - b Configure VLANs

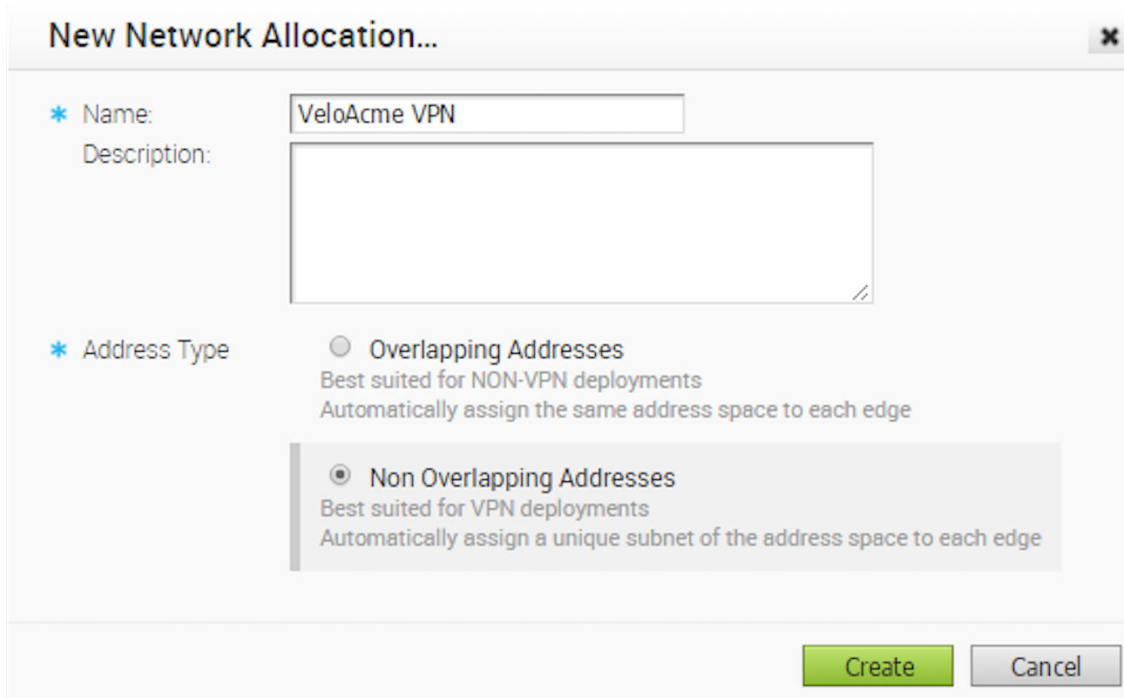
### Create Network or Select Existing Network

If you are creating a new Network, on the **Networks** page, click **New Network**. As an alternative, you can select a predefined Network by clicking the name of the predefined Network. After a new installation, the VeloCloud Orchestrator has two predefined Networks: Internet Network and VPN Network.



If you are creating a new Network, the **New Network Allocation** dialog is displayed (see the image below). In the **New Network Allocation** dialog, specify a Name, Description, and choose an addressing type.

Although the Address Type can be either Overlapping Addresses (where every VeloCloud Edge has the same address space) or Non Overlapping Addressing (where each VeloCloud Edge has a unique address block), we mandate Non Overlapping. For this example, we will call our new Network, VeloAcme VPN.



## Overlapping Addresses

In order to enable branches with Overlapping IP to reach the common server in the hub or data center, or to enable data center users to reach servers in Overlapping IP branches, NAT on the Edge must be configured. You can define NAT for a single source local IP to map to one VPN IP address, or for a block of IP addresses to a block of VPN addresses with same prefix length.

There are two steps you must complete:

- 1 Enable VPN via NAT in the Overlapping Address Network setup.
- 2 *Configure NAT on the Edge level.*

See instructions below to configure Overlapping IP for VPN.

## Configure Overlapping IP for VPN

To configure overlapping IP for VPN:

- 1 Enable VPN via NAT in Overlapping Address Network setup.
  - a Go to **Configure > Networks** from the Navigation Panel.
  - b Click the **New Network** button.
  - c In the **New Network Allocation** dialog box:
    - 1 Type the network name in the **Name** textbox.
    - 2 If there is a description, type it in the **Description** textbox.
    - 3 In the **Address Type** area, choose the **Overlapping Addresses** dial.
    - 4 Click the **Create** button.

The screenshot shows a dialog box titled "New Network Allocation...". It has a "Name" field with the text "Acme" and a "Description" field which is empty. Below these fields is the "Address Type" section, which contains two radio button options. The first option, "Overlapping Addresses", is selected and has the text "Best suited for NON-VPN deployments" and "Automatically assign the same address space to each edge" below it. The second option, "Non Overlapping Addresses", is not selected and has the text "Best suited for VPN deployments" and "Automatically assign a unique subnet of the address space to each edge" below it. At the bottom of the dialog box are two buttons: "Create" and "Cancel".

- d Click the newly created network link in the **Network** screen.
- e In the **Networks** screen, click the **Allow VPN Via NAT** checkbox if NAT on the Edge is required. See image below.
- f Click the **Save Changes** button.



Networks - Acme Save Changes

\* Name:

Description:

Address Type: **Overlapping Addresses**  
Best suited for NON-VPN deployments  
Automatically assign the same address space to each edge

Allow VPN Via NAT:

2 In the **Corporate Networks** area, create a new VLAN or update an existing VLAN.

Corporate Networks (addresses and VLANs)

\* Address Space:

Max VLANs:

Name	VLAN ID	DHCP Type	Static Addresses	DHCP Addresses	DHCP Options
Corporate	1	Enabled	10	244	0

New... Delete

- a If you are updating an existing VLAN, click the link of the VLAN to open the **Corporate** dialog box.
- b If you are creating a new VLAN, click the **New** button in the **VLANs** area to open the **New VLAN** dialog box. (From the **New VLAN** dialog box, enter the **VLAN Name** and **VLAN ID**).
- c Click the **Add VLAN** button.
- d Whether you update an existing VLAN or you are creating a new VLAN, enter the Subnet in the **Subnet** textbox.

New VLAN...

VLAN

\* VLAN Name:

\* VLAN ID:

Subnet:

DHCP

Type:  Enabled  Relay  Disabled

Static Addresses:

Lease Time:

Option	Code	Data Type	Value
add an option			

Add VLAN Cancel

3 If the **Allow VPN via NAT** is checked, define NAT on the Edge level (1:1 or use VPN IP Subnet blockpool). See section titled, *Configure Edge Device*.

## Non-Overlapping Addressing

The summary of the new Network where non-overlapping addressing is shown in the following screen capture. In this Network definition, every edge will have a unique network address space. VeloAcme will also have some Edges that require communication between Edges using a VPN tunnel. This requires that each connection across all of the Edges must have a unique IP address.

## VeloCloud Site VPN

### Configure Corporate Network

**Note** Initially, one Corporate Network is defined. Additional Corporate networks can be defined by clicking on the '+' symbol to the right of the network.

Perform the follow steps for your VPN Corporate Network.

### Configure Address Space

Enter the address space for the Corporate Network.

### SaaS

The following screen capture shows a screen capture for a Corporate Network that uses overlapping addressing. Enter the address space that the Corporate Network will occupy on all Edges.

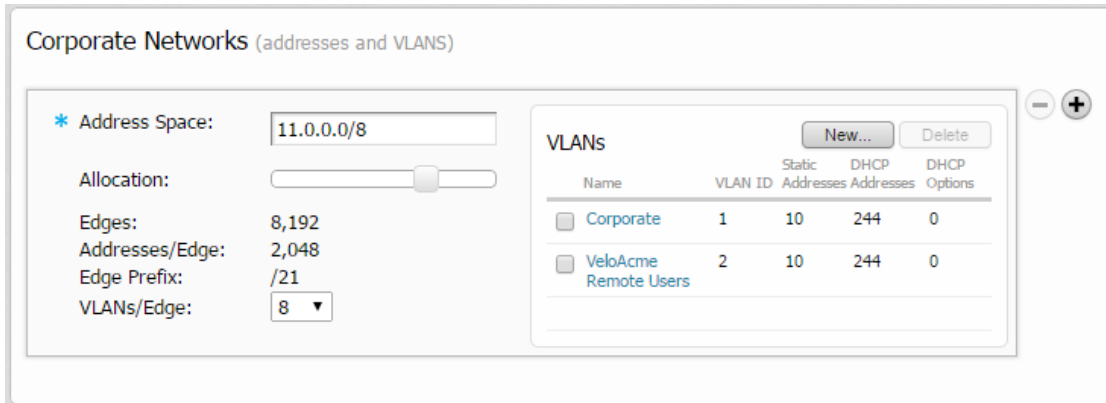
The screenshot displays the 'Corporate Networks (addresses and VLANS)' configuration page. On the left, the 'Address Space' is set to '10.0.2.0/21' and 'Max VLANs' is set to '8'. On the right, a table lists the configured VLANs.

Name	VLAN ID	Static Addresses	DHCP Addresses	DHCP Options
<input type="checkbox"/> Corporate	1	10	244	0

**Note** Although SaaS can use either but for VPN we mandate Non-Overlapping.

### Non-VeloCloud Site via VPN

The following screen capture shows a screen capture for a Corporate Network that uses overlapping addressing. The address space was decided in the previous step when you create the network space and will be distributed across the number of Edges chosen using the Allocation slider. You can specify the number of Edges, the Addresses/Edge, and the Edge Prefix. The Allocation slider help you choose these values by calculating the values when all addresses are assigned across the number of Edges. This is the built-in IPAM IP address management for Edges to allocate LAN side subnet behind the Edge.



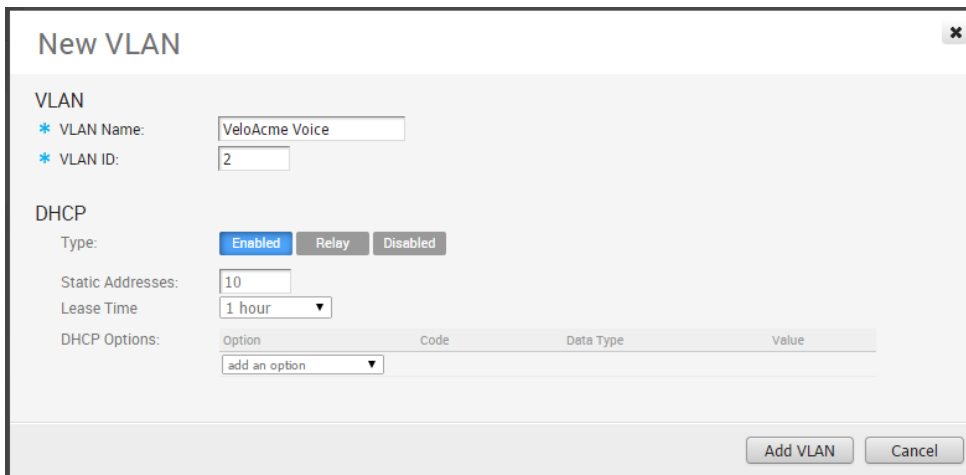
**Note** Once a Network is assigned to an Edge, it is not possible to change the Address Space Allocation.

**Note** The number of Edges is the maximum number of Edges that will ever be deployed using this Network. The Addresses/Edge defines the size of the address space for each Edge.

### Configure VLANs

You can define as many VLANs as you like for the Corporate Network, but the Max VLANs value specifies the maximum number you can specify for use in a Profile or Edge.

Click the New button to create a new VLAN. The dialog below is presented. You can configure the VLAN Name, VLAN ID, and the DHCP configuration (see the screen capture below).



The following screen captures shows some examples for configuring DHCP options. Choose one of the following types:

Type	Description
Enabled	The Edge is the DHCP server
Relay	The DHCP is at a remote location
Disabled	The DHCP is incapacitated

When choosing **Enabled**, you can add one or more DHCP options where you specify predefined options or add custom options. The following screen capture shows an example configuration with one predefined and one custom DHCP option.

**New VLAN**

VLAN

\* VLAN Name:

\* VLAN ID:

DHCP

Type: **Enabled** Relay Disabled

Static Addresses:

Lease Time:

Option	Code	Data Type	Value
TFTP Server (66)	66	Host	tftp.eloacme.com
HTTP Proxy	252	Text	proxy.eloacme.com
add an option			

Add VLAN Cancel

If you choose the DHCP type of Relay, you can specify the IP address of one or more Relay Agents (see the screen capture below).

**New VLAN**

VLAN

\* VLAN Name:

\* VLAN ID:

DHCP

Type: Enabled **Relay** Disabled

Relay Agent Ip:

Add VLAN Cancel

If the DHCP type of Disabled is chosen, IP addresses are not provided by DHCP for this VLAN.

**New VLAN**

VLAN

\* VLAN Name:

\* VLAN ID:

DHCP

Type:

Click Add VLAN to complete the VLAN creation.

## Configure Guest Networks

**Note** Initially, one Guest Network is defined. Additional Guest networks can be defined by clicking on the '+' symbol to the right of the network.

The Guest Network is an untrusted network that always uses an overlapping address space. It is completely segmented and on separate VRF as compared to corporate network. The **Guest Network** section (see screen capture below) defines the Address Space. You can define as many VLANs as you like for the Guest Network, but the Max VLANs value specifies the maximum number you can use in a Profile or Edge.

**Guest Networks** (addresses and VLANs)

\* Address Space:

Max VLANs:

VLANs		<input type="button" value="New..."/>		<input type="button" value="Delete"/>	
Name	VLAN ID	Static Addresses	DHCP Addresses	DHCP Options	
<input type="checkbox"/> Guest	64	10	52	0	

## Configure Address Space

Enter the address space that the Guest Network will occupy on all Edges.

## Configure VLANs

You can define as many VLANs as you like for the Guest Network, but the Max VLANs value specifies the maximum number you can use in a Profile or Edge. For VeloAcme, we used the default VLAN, Guest.

Our VeloAcme Network definitions are now complete and ready to be incorporated into our Profile and Edge Definitions.

## Provision an Edge

This section describes how to provision an Edge.

---

**Note** Content for Provision an Edge has been updated for the 3.3.0 release.

---

### Overview

Enterprise Admins can provision a single Edge or multiple Edges, such as assigning a Profile configuration to an Edge or changing other Edge specific parameters. You must create a configuration for every Edge you will deploy to a specific site. This section describes what an Enterprise Admin can provision.

### Enterprise Edges Screen

The Enterprise Edges Configuration screen lists all the provisioned Edges in the Enterprise network that you can make changes to. You can also create an Edge from this screen.

The *Enterprise Edges Identification* table below provides details for each field and button displayed on this screen.

Edge	Certificates	Profile	Operator Profile	HA	Device	Biz Pol	Firewall	Alerts	Oper...	Softwar...
ACME- Mountain View 1		Quick Start Profile	sa-profile							3.2.0








---

**Note** If you are logged in using a user ID that has Customer Support privileges, you will only be able to view VeloCloud Orchestrator objects. You will not be able to create new objects or configure/update existing ones.

---

### Enterprise Edges Screen Identification Table

Most of the column headers have a sorting feature that lists items in the column in alphabetical order, numerical order, or by type. (The Device, Biz Policy, Firewall, Alerts, and Operator Alerts columns do not have this feature). Click the column headers that have this feature to sort the list.

Columns/ Checkboxes/ Buttons	Description
<b>Edge Column</b>	Displays the name of the Edge. Click the <b>Edge</b> column header to sort the Edge list in alphabetical order. The Edge name is also a link; click the link to open the <a href="#">Chapter 14 Edge Overview Tab</a> screen. Select the checkbox next to the name of the Edge to select the Edge.
<b>Certificates Column</b>	Displays an Edge's current and expired certificates. Click the <b>View link</b> next to the number of certificates for more information.
<b>Profile Column</b>	Lists the Profile assigned to the Edge. The Profile name is also a link; clicking the link opens the <a href="#">Profile Overview Screen</a> Tab screen. NOTE: If an Edge Staging Profile is displayed due to <i>push activation</i> , this profile is used by a newly assigned Edge, but has not been configured with a production Profile. Enterprise Admins must manually assign a Profile to these Edges. See section titled, <i>Assign a Profile (Change a Profile)</i> for instructions on how to manually assign a profile to an Edge.
<b>Operator Profile Column</b>	This column is visible to only Operators. The Operator Profile is the template assigned to the customer the moment the customer is created by the Operators. It includes the software image, application maps, Gateway selection, and the management settings of the Edge. Operator-level Admins can change the Operator Profile for specific Edges. Enterprise Admins have read-only access. The Operator Profile name is also a link; clicking the link opens the <i>Operator Profiles</i> screen.
<b>HA Checkbox</b>	Selecting the <b>HA</b> checkbox enables the VeloCloud Active Standby HA option.
<b>Device Column</b>	Displays a blue  icon if Edge specific configurations have been configured. Displays a gray  icon to indicate that all settings (if any) have been inherited from the Profile. To navigate to the <b>Device</b> settings screen, click the icon in the <b>Device</b> column, and then click the <b>Device</b> tab.
<b>Biz Policy Column</b>	Displays a blue  icon if Business Policy rules have been configured. Displays a gray  icon to indicate that all rules (if any) have been inherited from the Profile. To navigate to the <b>Business Policy</b> screen, click the icon in the <b>Biz Policy</b> column and then click the <b>Business Policy</b> tab.
<b>Firewall Column</b>	Displays a blue  icon if Firewall rules have been configured. Displays a gray  icon to indicate that all rules (if any) have been inherited from the Profile.  Displays a red line across the icon  if the Firewall is disabled. When the Firewall is disabled, it indicates that it has been turned off in an Edge's profile configuration. To turn the Firewall on, go the profile configuration ( <b>Configure &gt; Profiles &gt; Firewall</b> tab).  To navigate to the <b>Firewall</b> screen, click the icon in the <b>Firewall</b> column and then click the <b>Firewall</b> tab.
<b>Alerts Checkbox</b>	If Customer alerts are enabled for the Edge, the <b>Alerts</b> checkbox will be checked in this column. Click the name of the Edge in the <b>Edge</b> column to open the <a href="#">Chapter 14 Edge Overview Tab</a> to enable or disable Customer alerts.
<b>Operator Alerts Checkbox</b>	If Operator alerts are enabled for the Edge, the <b>Operator Alerts</b> checkbox will be checked in this column. Click the name of the Edge in the <b>Edge</b> column to open the <a href="#">Chapter 14 Edge Overview Tab</a> to enable or disable Operator alerts.
<b>Software Version Column</b>	The software version of the Edge will display in this column.
<b>Factory Software Version Column</b>	When the Edge is shipped from the factory, it is shipped with a default software version.
<b>Build Number Column</b>	Displays the build number of an activated Edge.

Columns/ Checkboxes/ Buttons	Description
<b>Model Column</b>	Displays the model type of the Edge.
<b>Serial Number Column</b>	Displays the serial number of the Edge. Assigning a serial number to an Edge is optional. If a serial number is not assigned to the Edge, this field will be blank.
<b>Created Column</b>	Displays the date and time the Edge was provisioned.
<b>Activated Column</b>	Displays the date and time the Edge was activated.
<b>Last Contact Column</b>	The last date and time the Edge communicated with the VCO.
<b>Column (Cols) button</b>	Click the <b>Cols</b> button to select the options you want to display in the Enterprise Edges list (See image above).
<b>Reset View Button</b>	Resets the Enterprise Edges list to the default view. (This removes filters and resets any options that were selected from the <b>Cols</b> button drop-down menu to the default view).
<b>Refresh Button</b>	Refreshes the Enterprise Edges list with current data from the server.
<b>CSV Button</b>	To export the content displayed in the Enterprise Edges list, click the <b>CSV</b> button.
<b>Selected Button</b>	Indicates how many Edges are selected from the <b>Edge</b> column. Click the <b>Selected</b> button to select all or deselect all of the Edges listed in the <b>Edge</b> column.
<b>Actions Button</b>	Lists the following actions you can perform on a selected Edge: <ul style="list-style-type: none"> <li>■ <i>New Edge</i></li> <li>■ <i>Local Credentials</i></li> <li>■ <i>Delete Edge</i></li> <li>■ <i>Assign Profile</i></li> <li>■ <i>Assign Operator Profile</i></li> <li>■ <i>Update Pre-notifications</i></li> <li>■ <i>Edge Licensing</i></li> <li>■ <i>Update Customer Alerts</i></li> <li>■ <i>Rebalance Gateways</i></li> </ul> <p><b>Note</b> Assign Operator Profile and Rebalance Gateways are Operator-level only features.</p>
<b>New Edge Button</b>	Opens the <b>Provision New Edge</b> dialog to provision a new Edge. See section, <i>Provision a New Edge</i> for more information.
<b>Help Button</b>	Access the online help for this feature by clicking the <b>Question Mark</b> icon.

## Provision a New Edge

This section describes the first steps to provision a new Edge configuration using a Profile.

**Note** This "Provision a New Edge" section below has been updated for the 3.3 release.



To provision an Edge:

- 1 In the **VeloCloud Edges** screen, click the **New Edge** button, located on the top, right corner of the VCO.
- 2 In the **Provision New Edge** dialog box, type a unique name for the Edge in the **Name** text field (see image below).

The screenshot shows the 'Provision New Edge' dialog box with the following details:

- Name:** ACME- Mountain View 1
- Model:** Edge 5X0
- Profile:** Quick Start Profile
- Authentication:** Certificate Optional
- Edge License:** ENTERPRISE | 1 Gbps | Asia Pac
- High Availability:**
- Serial Number:** VC00000990 (Optional. If specified, the activated Edge device must have this serial number.)
- Contact Name:** Jane Doe
- Contact Email:** jane@acme.net
- Location:** (with a globe icon and a 'Set Location...' link)

- 3 From the **Model** drop-down menu, select the model of the Edge you are creating.
- 4 Assign a profile to the Edge by choosing a profile from the **Profile** drop-down menu.
  - If an Edge Staging Profile is displayed as an option due to push activation, this profile is used by a newly assigned Edge, but has not been configured with a production Profile.
  - If a customer has a Network-based Operator Profile, then the customer can only provision Network-based Edges. In addition, if a customer has a Segment-based Operator Profile, then the customer can only provision Segment-based Edges. (For more information about Profile migration see, [Network to Segment Migration](#). For more information about how to create a new profile, see the [Chapter 10 Configure Profiles](#) section titled, [Create a Profile](#)).
- 5 Apply a certificate to the Edge from the **Authentication** drop-down menu. Options are as follows: Certificate Disabled, Certificate Optional, and Certificate Required (if a valid certificate is available). For more information about each of these certificates, see **Authentication**, in the [Properties Area Field and Checkbox Descriptions](#) table.
- 6 Choose an Edge license from the **Edge License** drop-down menu. For more information about Edge Licensing, see *Edge Licensing*.
- 7 To apply High Availability (HA), select the **High Availability** checkbox. (Edges can be installed as a single standalone device or paired with another Edge to provide High Availability (HA) support. For more information about HA, see the [High Availability Options](#) section).
- 8 As an optional step, enter the serial number of the Edge in the **Serial Number** text field. If specified, the serial number must match the serial number of the Edge that will be activated.
- 9 Type in the name and email address of the site contact for the Edge.
- 10 Click the **Set Location** link to enter the location of the Edge. See [Contact & Location](#) in the [Monitor the Edge Overview](#) section for more information.

- Click the **Create** button to Provision the Edge. The Edge gets provisioned with an activation key.

**Note** The activation key expires in one month if the Edge device is not activated against it. For information on how to activate an Edge see the [Configure Edge Activation](#) section in the *Edge Activation Quick Start Guide*.

After you click the **Create** button, the **Edge Overview** screen appears showing the Edge activation key at the top of the screen. To see an overview of the Edge you just created, or to make any changes to it, see the [Chapter 14 Edge Overview Tab](#) section.

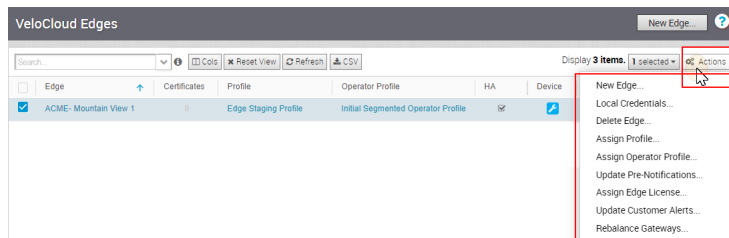
After you have Provisioned the Edge, you can select the Edge from the **VeloCloud Edges** window, click the **Actions** button to open the drop-down menu, and perform relevant options on the selected Edge. See the section below for a description of all the options in the **Actions** drop-down menu.

## Actions Drop-down Menu

This section describes the **Actions** drop-down menu.

### Overview

After you select an Edge from the Enterprise Edges Configuration screen ( **Configure > Edges** from the VCO), the following actions can be taken from the **Actions** drop-down menu.

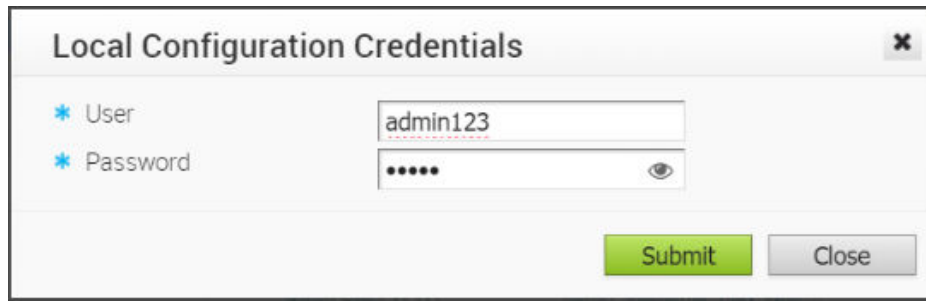


### New Edge

You can create a new Edge by either clicking the **Create Edge** button or by choosing **New Edge** from the **Actions** drop-down menu. See the [Provision a New Edge](#) section in this document for information on how to Provision a new Edge.

### Local Credentials

You can assign local configuration credentials by selecting an Edge and choosing **Local Credentials** from the **Actions** drop-down menu. In the **Local Configuration Credentials** dialog, type the User and Password in the appropriate fields. The default credentials are username: admin password: admin123 (case sensitive). Then, click the **Submit** button.



**Local Configuration Credentials** [X]

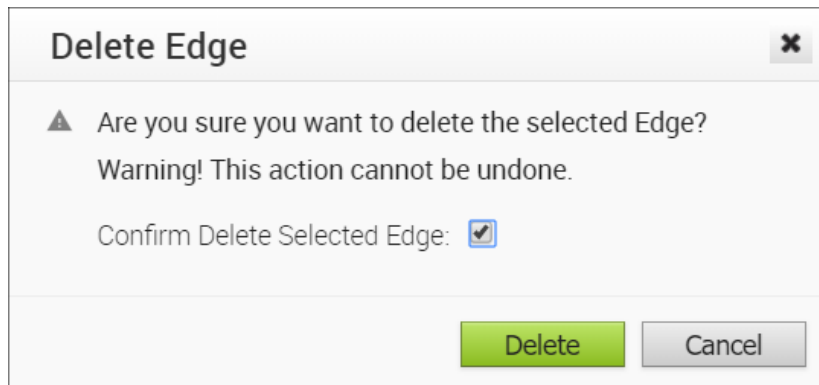
\* User:

\* Password:  [Eye icon]

Submit Close

## Delete an Edge

Once you delete an Edge the action cannot be undone. If you're sure you want to delete an Edge, select the Edge you want to delete, and then choose **Delete Edge** from the **Actions** drop-down menu. In the **Delete Edge** dialog, make note of the warning message that deleting an Edge cannot be undone, click the **Confirm Delete Selected Edge** checkbox, and then click the **Delete** button.



**Delete Edge** [X]

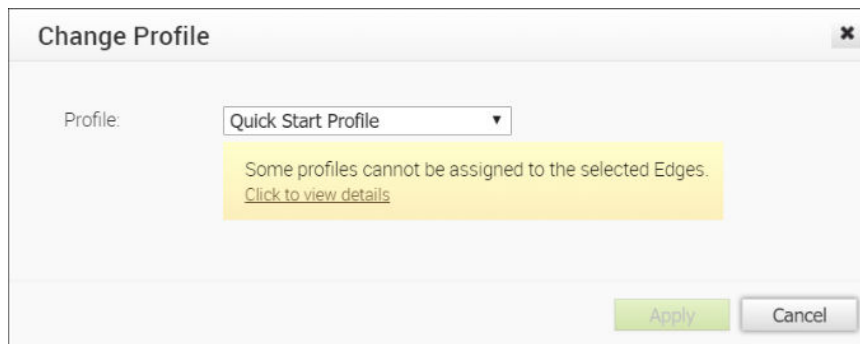
⚠ Are you sure you want to delete the selected Edge?  
Warning! This action cannot be undone.

Confirm Delete Selected Edge:

Delete Cancel

## Assign a Profile (Change a Profile)

You can change an Edge's profile by selecting a profile and choosing **Assign a Profile** from the **Actions** drop-down menu. If applicable, a message will display in the dialog indicating that some profiles cannot be assigned to the selected Edge. (See image below). Click the link, **Click to view details**, for the reason the profile cannot be assigned to the selected Edge.



**Change Profile** [X]

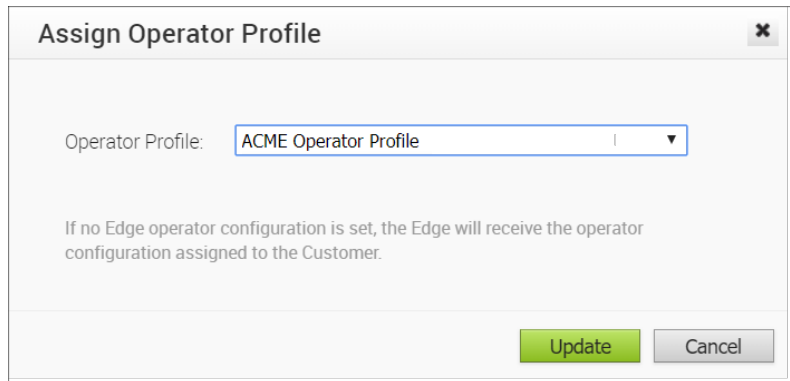
Profile:  ▼

Some profiles cannot be assigned to the selected Edges.  
[Click to view details](#)

Apply Cancel

## Assign Operator Profile

The **Assign Operator Profile** dialog enables Operators to change the Operator Profile. **(NOTE: This feature is an Operator-level only feature. It is not visible to Standard Admins).**



The dialog box titled "Assign Operator Profile" has a close button (X) in the top right corner. It contains a label "Operator Profile:" followed by a dropdown menu showing "ACME Operator Profile". Below this is a note: "If no Edge operator configuration is set, the Edge will receive the operator configuration assigned to the Customer." At the bottom right, there are two buttons: "Update" (highlighted in green) and "Cancel" (disabled).

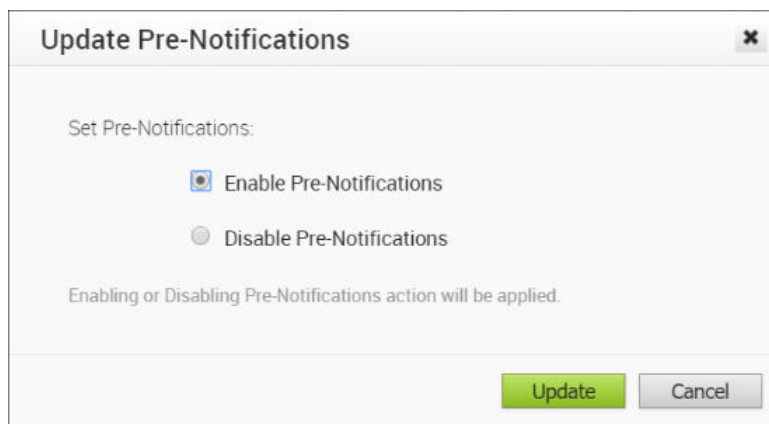
---

**Note** If no Edge operator configuration is set, the Edge will receive the operator configuration assigned to the Customer.

---

## Update Pre-notifications

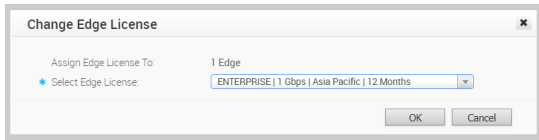
To set Edge device alerts for Operators, select an Edge, and then choose **Update Pre-Notifications** from the **Actions** drop-down menu. In the **Update Pre-Notifications** dialog, select the **Enable Pre-Notifications** radio button, and then click **Update**. **NOTE:** In order for an Operator to receive alert messages, alerts and notifications must be selected and enabled via email, SMS, or SNMP Traps at **Configure > Alerts and Notifications**. You can change this pre-notification setting by selecting the Edge, and then going to the **Properties** area at **Configure > Edges** to enable or disable the alert.



The dialog box titled "Update Pre-Notifications" has a close button (X) in the top right corner. It contains the label "Set Pre-Notifications:" followed by two radio buttons: "Enable Pre-Notifications" (which is selected) and "Disable Pre-Notifications". Below this is a note: "Enabling or Disabling Pre-Notifications action will be applied." At the bottom right, there are two buttons: "Update" (highlighted in green) and "Cancel" (disabled).

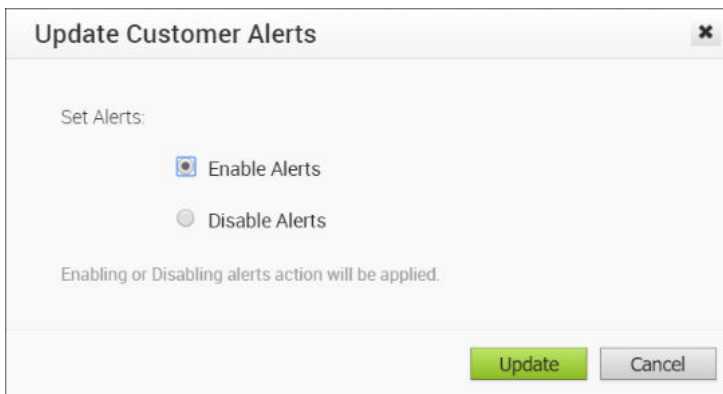
## Assign Edge License

Superuser Administrators and Standard Administrators can assign a license type to an Edge from the **Actions** drop-down menu, by choosing **Assign Edge License**. See section [Monitor Edge Licensing](#) for more information. (This feature is new for the 3.3.0 release).



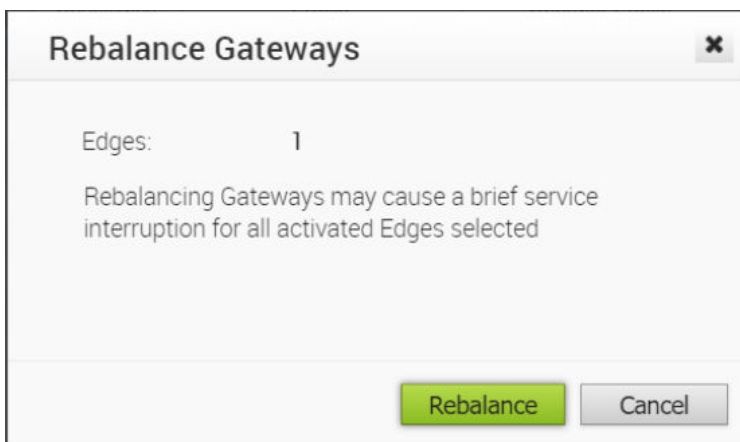
## Update Customer Alerts

To set Edge device alerts for customers, select an Edge, and then choose **Update Customer Alerts** from the **Actions** drop-down menu. In the **Update Customer Alerts** dialog, select the **Enable Alerts** radio button, and then click the **Update** button. NOTE: In order for a customer to receive alert messages, alerts and notifications must be selected and enabled via email, SMS, or SNMP Traps at **Configure > Alerts and Notifications**. You can change this alert setting by selecting the Edge, and then going to the **Properties** area at **Configure > Edges** to enable or disable the alert.



## Rebalance Gateways

Rebalance Gateways is an Operator-level only feature to help rebalance VeloCloud hosted Gateways across the Enterprise Edges. (This feature is not visible to Standard Admins).



## Activate Edges

The VeloCloud SD-WAN solution supports two methods of VCE deployment and activation: Email and Zero Touch Provisioning

	Email (Office Admin Activates)	Zero Touch Provisioning (Central NOC Activates)
No IT Visit Required	✓	✓
No Pre-staging Required	✓	✓
No Security Risk if Box Is Lost	✓	✓
No Site-by-site Link Profile Needed	✓	✓
No Device Tracking Needed	✓	
Requires Email to Office Admin	✓	
Requires Knowledge of Device to Site	✓	✓

## Activate Edges Using Zero Touch Provisioning (Tech Preview)

In this method, the VCE is activated without the requirement for an office admin to click an activation link.

Following are some scenarios that require you to activate your Edges using the Zero Touch Provisioning method:

- When a Service Provider outsources the physical installation of devices at a site—in most instances, just to connect cables and power. The person who installs the device may neither be an employee of the end customer nor of the Service Provider.
- When the person at the remote site is unable to connect a laptop/tablet/ phone to the VCE, and therefore cannot use an email or cannot click an activation code/URL.

For details about how to activate your Edges using the Zero Touch Provisioning method, contact [VeloCloud Customer Support](#).

## Activate Edges Using Email

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

Complete the following tasks to activate your Edges using the Email method:

- 1 Send an Activation Email.

The administrator initiates the activation process by sending an activation procedure email to the person that will install the Edge, typically a Site Contact.

- 2 Activate the Edge Device.

The individual following the instructions in the activation procedure email will activate the Edge device.

Complete the following instructions to complete the activation process.

## Step 1: Send an Activation Email

The process of activating the Edge begins with the initiation of an activation procedure email that is sent to the Site Contact by the IT Admin.

To send the activation procedure email:

- 1 Go to **Configure > Edges** from the Orchestrator.
- 2 Select the Edge you want to activate. The **Edge Overview Tab** window appears.
- 3 As an optional step, in the **Properties** area, enter the serial number of the Edge that will be activated in the **Serial Number** text field. Serial numbers are case sensitive, so make sure that “VC” is capitalized.

---

**Note** This step is optional. However, if specified, the serial number must match the activated Edge.

---

- 4 Click the **Send Activation Email** button to send the activation email to the Site Contact. For a detailed description of the fields and checkboxes featured in the **Properties** area, see the [Properties Area Field and Checkbox Descriptions](#) in the [Chapter 14 Edge Overview Tab](#).

The screenshot shows the 'Properties' section of the Edge Overview Tab. It contains the following elements:

- Name:** A text field containing 'ACME: Mountain View 1'.
- Description:** An empty text field.
- Status:** A label indicating 'Pending'.
- Serial Number:** A text field containing '00-VC00000480'. Below it, a note states: 'Optional. If specified, the activated Edge device must have this serial number.'
- Activation Key:** A text field containing 'UNF4-C4HS-LLKS-R4J8'. Below it, a note states: 'expires in a month'.
- Enable Pre-Notifications:** A checkbox that is checked.
- Enable Alerts:** A checkbox that is checked.
- Authentication Mode:** A dropdown menu set to 'Certificate Required'.
- Send Activation Email:** A blue button at the bottom right.

- 5 The **Send Activation Email** pop-up window appears. It describes the steps for the Site Contact to complete to activate the Edge device.

**Send Activation Email**

Edge: ACME- Mountain View 1  
 Recipients: Site Contact

\* From: support@velocloud.net  
 \* To: jdoe@acme.com  
 CC:   
 \* Subject: Edge Activation  
 \* Message Body:

Hi,  
 To activate your VeloCloud Edge, please follow these steps:

1. Connect your device to power and any Internet cables or USB modems.
2. Find and connect to the Wi-Fi network that looks like "velocloud-" followed by 3 more letters/numbers (e.g. "velocloud-01c"), and use "vcsecret" as the password. If your device does not have Wi-Fi, connect to it using an Ethernet cable.
3. Click the following link to activate your edge

[http://192.168.2.1/?activation\\_key=UNF4-C4HS-LLKS-R4J8&custom\\_vco=34.232.58.228](http://192.168.2.1/?activation_key=UNF4-C4HS-LLKS-R4J8&custom_vco=34.232.58.228)

If you experience any difficulty, please contact your IT admin.

**Send** **Close**

- 6 Click the **Send** button to send the activation procedure email to the Site Contact.

## Step 2: Activate an Edge Device

The Site Contact performs the steps outlined in the Edge activation procedure email.

In general, the Site Contact completes the following steps:

- 1 Connect your Edge device to power and insert any Internet cables or USB modems.
- 2 Find and connect to the Wi-Fi network that looks like `velocloud-` followed by three more letters/numbers (for example, `velocloud-01c`) with the password `vcsecret`.
- 3 Click the hyperlink in the email to activate the Edge.

---

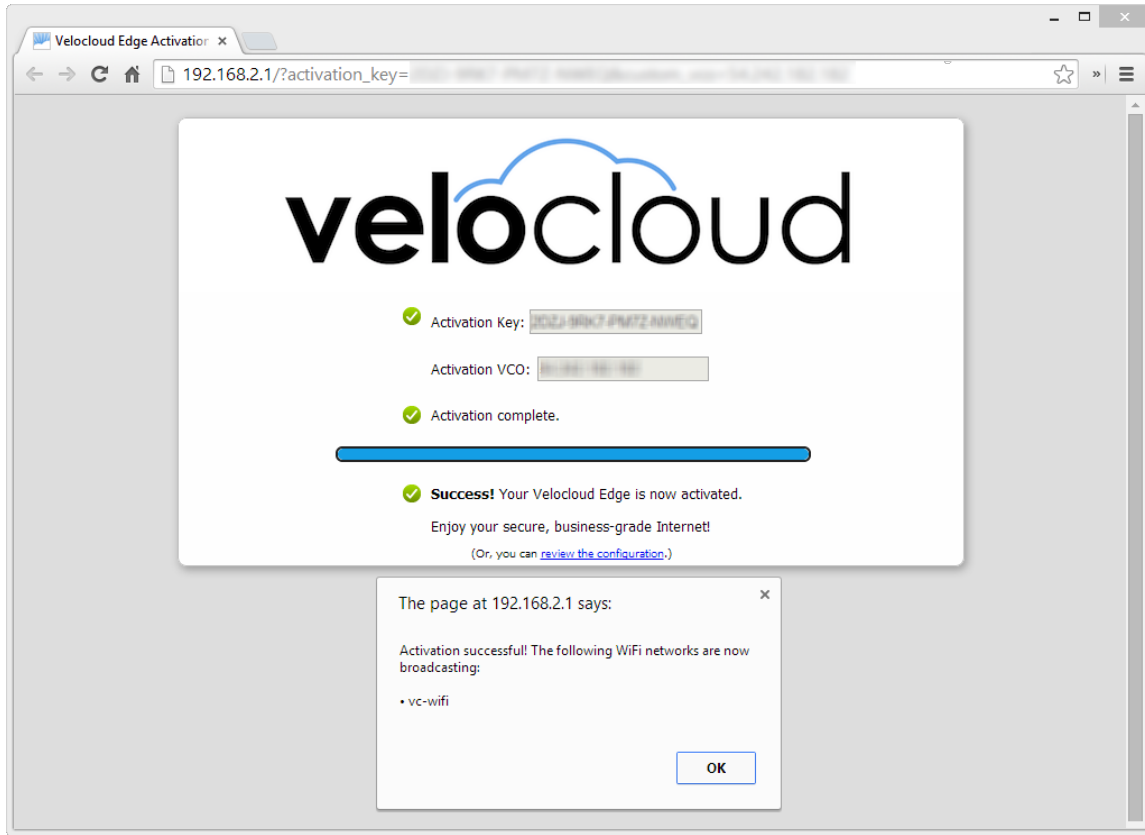
**Note** Refer the Wi-Fi SSID from the box. The default Wi-Fi is `vc-wifi`.

---

The Edge activation email might provide specific instructions for connecting WAN cables and USB modems, connecting devices to the LAN connections, and connecting additional networking devices to the Edge. It might also provide instructions for using one or more Wi-Fi connections.

During the Edge activation, the activation status screen appears.





The Edge will download the configuration and software from the VCO. The Edge will be activated successfully and will be ready for service. Once an Edge has been activated, it will be “useable” for routing network traffic. In addition, more advanced functions such as monitoring, testing, and troubleshooting will be enabled.

# Edge Overview Tab

# 14

This section describes the Edge Overview tab.

---

**Note** Content for Edge Overview Tab has been updated for the 3.3 release.

---

This chapter includes the following topics:

- [Edge Overview](#)
- [Edge Overview Properties](#)
- [Edge Profile](#)
- [RMA Reactivation](#)

## Edge Overview

The **Edge Overview** tab provides an overview of a selected Edge, which includes properties, status, profile configurations, and contact information.

In this tab, you can send an Edge activation email, make changes to certain properties, assign a different profile to a selected Edge, update Edge contact and location information, or request an Edge RMA reactivation. To access the **Edge Overview Tab**:

- 1 Go to **Configure > Edges** on the navigation panel of VCO.
- 2 In the **Enterprise Edges** screen, select and click an Edge to open the **Edge Overview Tab**.

You can perform the following tasks (as well as other tasks) on the **Edge Overview Tab**:

- To enable alerts for a specific Edge, or send an Edge activation email, see the [Edge Overview Properties](#) section.
- To see an overview of the Edge overrides from a specific profile, or if you need to change to a different profile, see the [Edge Profile](#) section.
- To change the contact, location, or the shipping address of an Edge, see the [Contact & Location](#) section.
- To replace an Edge that has malfunctioned, see the [RMA Reactivation](#) section.
- To assign a License to an Edge, see the [Edge License](#) section.

The following sections provide detailed descriptions of each area of the **Edge Overview Tab**.

## Edge Overview Properties

This section describes properties.

### Properties Overview

In the **Properties** area, you can initiate the Edge activation process by sending an Edge activation email, and you can also view and change certain properties of a selected Edge. The Edge status, activation date, and software version also display in this area.

See the [Properties Area Field and Checkbox Descriptions](#) for a description of all fields and checkboxes featured in the **Properties** area. See the [Initiate Edge Activation](#) section for information on how to send an Edge activation email.

The image below represents an activated Edge.

### Properties Area Field and Checkbox Descriptions

This section describes the Properties Area Field and Checkbox.

Field/Checkbox	Description
<b>Name</b>	Displays the unique name of the Edge at the customer level. If you change the name of the Edge, remember to click the <b>Save Changes</b> button.
<b>Description</b>	Enables you to provide information about the Edge. If you make updates to the Edge description, remember to click the <b>Save Changes</b> button. <b>Note</b> This is the only location where a description of the Edge is displayed.
<b>Enable Pre-Notifications</b> checkbox	This checkbox is enabled by default after the Edge has been provisioned. For Operators to receive alerts, the <b>Enable Pre-Notifications</b> checkbox must be checked, and alerts must be selected and enabled via email, SMS, or SNMP Traps at <b>Configure &gt; Alerts &amp; Notifications</b> . In addition to receiving an email, SMS, or SNMP Trap, Alerts can also be viewed on the <b>Alerts</b> screen at <b>Monitor &gt; Alerts</b> . Uncheck this checkbox to disable alert notifications for Operators for the selected Edge.
<b>Enable Alerts</b> checkbox	This checkbox is enabled by default after the Edge has been provisioned. For Customers to receive Edge Device alerts, the <b>Enable Alerts</b> checkbox must be checked, and alerts must be selected and enabled via email, SMS, or SNMP Traps at <b>Configure &gt; Alerts &amp; Notifications</b> . In addition to receiving an email, SMS, or SNMP Trap, Alerts can also be viewed on the <b>Alerts</b> screen at <b>Monitor &gt; Alerts</b> . Uncheck this checkbox to disable alerts for the selected Edge.

Field/Checkbox	Description
<b>Authentication Mode</b>	<p>There are three options for the Authentication Mode (Certificate Disabled, Certificate Optional, and Certificate Required).</p> <ul style="list-style-type: none"> <li>■ <b>Certificate Disabled (default):</b> If Certificate Disabled is selected as an option, the Edge will use a pre-shared key mode of authentication.</li> <li>■ <b>Certificate Optional:</b> If Certificate Optional is selected as an option, the Edge will use either the PKI certificate or the Pre-shared key (depending upon which certificate the other Edge or Gateway is using).</li> </ul> <p><b>Note</b> The Operator must enable PKI at Configure &gt; Customer.</p> <ul style="list-style-type: none"> <li>■ <b>Certificate Required:</b> Once the Edge obtains a valid certificate, Certificate Required becomes available as an option in the drop-down menu. If the Certificate Required option is selected, the Edge will use the PKI certificate as the mode of authentication.</li> </ul> <p><b>Note</b> The Operator must enable PKI at <b>Configure &gt; Customer</b>.</p>
<b>License</b>	The <b>License</b> drop-down menu displays available license types that can be assigned to an Edge.
<b>View Certificate</b>	If the Edge has a valid certificate, the <b>View</b> link displays. Click the <b>View</b> link to view, export, or revoke the certificate.
<b>Status</b>	<p>Displays the following status options: Pending, Activated, and Reactivation Pending.</p> <ul style="list-style-type: none"> <li>■ <b>Pending:</b> The Edge has not been activated.</li> <li>■ <b>Activated:</b> The Edge has been activated.</li> <li>■ <b>Reactivation Pending:</b> If the <b>Request Reactivation</b> button is clicked, the status will change to Reactivation Pending. This status update does not change the Edge's function, it only indicates that a new or replacement Edge can be activated with the existing configuration.</li> </ul>
<b>Activated</b>	Displays the date and time the Edge was activated.
<b>Software Version</b>	Displays the software version and build number of the Edge.
<b>Local Credentials</b>	Displays the credentials for the local UI. The default credentials are username: admin password: admin123 (case sensitive). <b>Click the View</b> button to change the credentials.
<b>Serial Number</b>	If the Edge is in the Pending state, the <b>Serial Number</b> text field displays. Entering the serial number is optional, but if specified, the serial number must match the serial number of the Edge that will be activated.
<b>Activation Key</b>	<p>If the Edge is in the Pending state, the Edge Activation Key displays. The activation key is only valid for one month. After one month, the key will expire, and a warning message will display underneath the activation key. You can generate a new key by clicking the <b>Generate New Activation Key</b> button located below the warning message.</p> <p>See the <i>Expired RMA Activation Key</i> section for more information.</p>
<b>Send Activation Email</b>	When the <b>Send Activation Email</b> button is clicked, an email with activation instructions is sent to the Site Contact.

## Initiate Edge Activation

This section describes how to initiate Edge activation.

Once the Edge configuration is saved, an activation key is assigned. In the **Properties** area, click the **Send Activation Email** button to initiate the Edge activation process. Clicking the **Send Activation Email** button does not activate the Edge; it only initiates the activation process by sending an email to the Site Contact with instructions on how to activate the Edge device.

The following image represents an unactivated Edge.

The screenshot shows the 'Properties' section of a configuration interface. On the left, there are fields for Name (ACME-Mountain View 1), Description, and checkboxes for 'Enable Pre-Notifications' and 'Enable Alerts', both of which are checked. Below these are 'Authentication Mode' (Certificate Optional) and 'License' (ENTERPRISE 11 Gbps | Asia Pacific | 12 Months). On the right, the Status is 'Pending', the Serial Number is 'E1-V330000000', and the Activation Key is 'BTKW-S4H6-LJDTY-P3ZT expires in 10 days'. A blue 'Send Activation Email' button is located at the bottom right.

After clicking the **Send Activation Email** button, a pop-up window displays the email that will be sent to the Site Contact. Instructions are provided in the email for the Site Contact to connect and activate the Edge hardware. For more information on how to activate an Edge, see the *Edge Activation Quick Start Guide* in the online help. For information about Pull Activation and Push Activation, see *Zero Touch Provisioning*.

**Note** The image above represents an Edge that has not been activated. Notice that the Edge status is in the Pending state and displays the **Serial Number** text field, the Activation Key, and the **Send Activation Email** button). See the [Properties Area Field and Checkbox Descriptions](#) table for a description of each of these fields.

## Edge License

This section describes the Edge License.

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

Standard Administrator Superusers and Standard Administrators can assign and monitor Edge license types that have been assigned to them. See [Monitor Edge Licensing](#) for additional information, including how to generate a report that provides a list of Edges and their license types.

To assign a license type to an Edge, choose a license type from the **License** drop-down menu located at the bottom of the **Properties** area of the **Edge Overview** Tab.

This is an identical screenshot to the one above, showing the 'Properties' section of a configuration interface for an Edge device. The Name is 'ACME-Mountain View 1', Status is 'Pending', Serial Number is 'E1-V330000000', and Activation Key is 'BTKW-S4H6-LJDTY-P3ZT expires in 10 days'. A blue 'Send Activation Email' button is at the bottom right.

## Edge Profile

This section describes an Edge Profile.

## Profile Overview

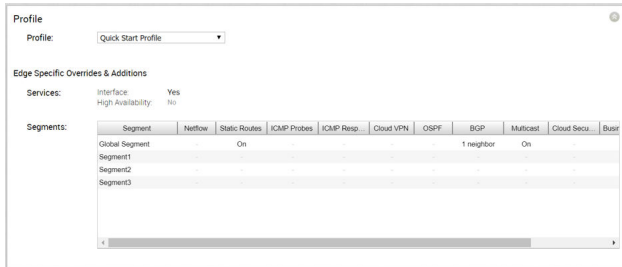
The profile is the “template” from which the Edge configuration is derived.

When switching to a different profile on the Edge, all relevant configurations will be changed except for any Edge override configurations. Overwritten configurations are displayed in the **Profile** area.

---

**Note** Edge overwritten configurations will not be changed when switching to a different profile.

---




---

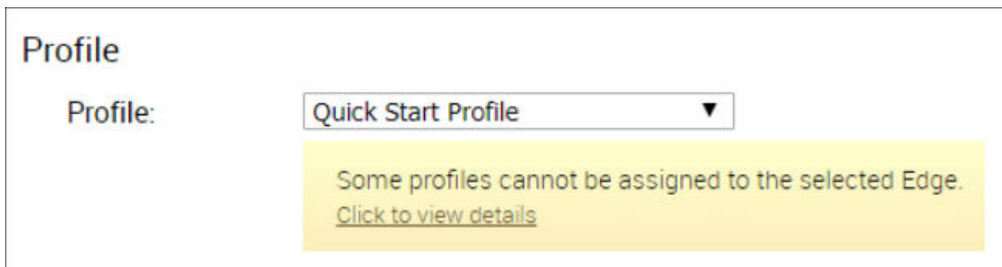
**Note** If an Edge Staging Profile is displayed as an option due to push activation, it is a newly assigned Edge that has not been configured by a production Profile. Enterprise Admins must manually assign a Profile to those Edges by choosing a new profile from the **Profile** drop-down menu.

---

## Profile Drop-Down Menu

The **Profile** drop-down menu displays a list of profiles that can be assigned to a specific Edge.

However, based on system validations, some profiles cannot be assigned to the selected Edge. In these instances (as shown in the image below), click the **Click to view details** link for the reason the profile cannot be assigned to the selected Edge.



See the Important Note in the *Profile Overview* section above for information about Edge Staging Profiles.

## Operator Profile Selection

The following table provides a customer-assigned Operator Profile and an Edge-assigned Enterprise Profile compatibility matrix. Refer to this matrix when switching profiles.

### Operator Profile Selection Matrix

Customer Operator Profile Type	Current Edge Enterprise Profile	Selected Edge Enterprise Profile	Result
Segment-based	Segment-based	Segment-based	No Change
Network-based	Network-based	Network-based	No Change
Segment-based	Network-based	Segment-based	The Edge configuration will be converted to a Segment-based configuration. However, it will not be delivered to the Edge until the Edge software image is updated to a version $\geq$ 3.0.
Network-based	Network-based	Segment-based	The Edge configuration will be converted to a Segment-based configuration. However, it will not be delivered to the Edge until the Edge software image is updated to $\geq$ 3.0.
Segment-based	Network-based	Network-based	The Edge will not receive the image update.
Network-based	Segment-based	Segment-based	The Edge will not receive the image update.

See the following sections related to the Profile drop-down menu for more information:

- [Create a Profile](#)
- [Network to Segment Migration](#)

## Edge-specific Overrides and Additions

This section describes how Service and Segment configurations can be overridden at the Edge level.

Edge overrides are the changes to the inherited profile configurations at the Edge level. Edge additions are configurations that are not included in the profile, but they are added to the selected Edge. A summary of all Edge overrides and additions are displayed in the **Profile** area (see the image in the *Profile Profile Overview* section).

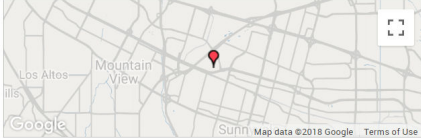
## Contact & Location

This section describes the **Contact & Location** area.

The **Contact & Location** area displays the Edge contact information and location. If you make changes to the Contact Name, Contact Email, or Contact Phone fields, remember to click the **Save Changes** button located on the top, right corner of the VCO.

**Contact & Location**

\* Contact Name:   
 \* Contact Email:   
 Contact Phone:   
 Location: 295 N Bernardo Ave,  
 Mountain View, CA 94043,  
 US  
 Lat,Lng: 37.3870566, -122.04981600000002  
[Update Location...](#)



Shipping Address  Same as above

## Change Edge Location

This section describes how to change the Edge location.

To change the Edge address:

- 1 Click the **Update Location** link.
- 2 In the **Set Edge Location** pop-up window, update the location using either the **Search Address** feature (selected by default) or by typing the address manually.
- 3 If you choose to type the address manually, click the **Manual Address Entry** button, and type either the address or type the Latitude and Longitude.
- 4 If you choose to type the address, click the **Update Lat,Lng From Address** button.
- 5 If you choose to type the Latitude and Longitude, click the **Update Address From Lat,Lng** button.
- 6 Click **OK** when complete.

## Change Shipping Address

This section describes how to change the shipping address.

If the shipping address is different from the Edge location, unselect the **Same as above** checkbox for the shipping address, then type in the shipping contact in the appropriate text field.

To change the Edge shipping location:

- 1 Click the **Set Location** link.
- 2 In the **Edge Shipping Location** pop-up window, update the shipping location using either the **Search Address** feature (selected by default) or by typing the address manually.
- 3 If you choose to type the address manually, click the **Manual Address Entry** button, type the address, and then click the **Update Location on Map** button.
- 4 Click **OK**.

## RMA Reactivation

This section describes RMA reactivation.

### Edge Reactivation Overview

If an Edge hardware malfunction occurs, or if you need to upgrade your Edge device, an Edge RMA reactivation is required.



See the [RMA Reactivation Steps](#) section for detailed instructions on how to activate the replacement Edge device. See the RMA Reactivation Scenarios section below for scenarios that require an Edge RMA reactivation.

## RMA Reactivation Scenarios

There are several scenarios that require an Edge RMA reactivation. This section describes two of the most common scenarios.

### Replace an Edge Due to a Malfunction

A typical scenario that requires an Edge RMA reactivation occurs when a malfunctioned Edge of the same model needs replacing. For example, a customer needs to replace a 520 Edge model with another 520 Edge model. The detailed [RMA Reactivation Steps](#) below describe the complete process for this scenario.

### Upgrade an Edge Hardware Model

Another common scenario that requires an Edge RMA reactivation is when a customer wants to replace an Edge with a different model. Usually this is due to a scaling issue in which a customer has outgrown the capacity of the current Edge. To avoid an activation failure in this scenario, it is important to remember to complete Step 8 (select the RMA model that will replace the old model from the RMA Model drop-down menu) and Step 9 (click the **Update** button) of the RMA Reactivation Steps below.

## RMA Reactivation Steps

This section describes the steps to complete RMA reactivation.

To complete the RMA reactivation process:

- 1 From the Orchestrator, go to **Configure > Edges**.
- 2 Select the Edge you want to reactivate.
- 3 In the **Edge Overview Tab**, scroll down to the bottom of the screen to the **RMA Reactivation** area. Expand the area by clicking the gray arrow located on the upper, right side.
- 4 Click the **Request Reactivation** button. This step generates a new activation key and places the Edge status in Reactivation Pending mode.

---

**Note** The reactivation key is only valid for one month from the time when the reactivation request was made.

---



- 5 If you need to cancel the activation request for any reason, click the **Cancel Reactivation Request** button. The Edge status changes from **Reactivation Pending** to **Activated**.
- 6 If the activation key has expired (the key is valid for one month), you will need to generate a new activation key. For more information, see *Expired RMA Activation Key*.

- 7 As an optional step, you can enter the serial number of the Edge that will be activated in the RMA Serial Number text field. Serial numbers are case sensitive, so make sure “VC” is capitalized.

---

**Note** Activation will fail if the serial number doesn’t match the Edge that will be activated.

---

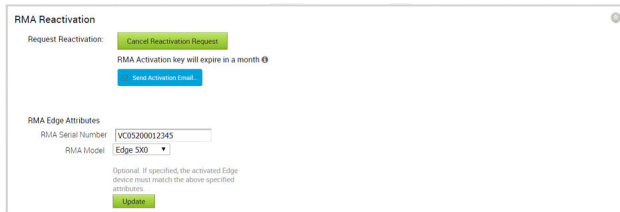
- 8 The **RMA Model** drop-down menu displays the selected Edge by default. If you are reactivating a different Edge model, select the Edge model that will be activated from the **RMA Model** drop-down menu.

---

**Note** Activation will fail if the selected Edge model doesn’t match the Edge that will be activated.

---

- 9 If you entered a serial number or chose a model from the RMA Model drop-down menu, click the **Update** button.



- 10 Click the **Send Activation Email** button. The **Send Activation Email** pop-up window appears.

**Send Activation Email**

Edge: ACME- Mountain View 1  
 Recipients: Site Contact

\* From: support@velocloud.net  
 \* To: jdoe@acme.com  
 CC:   
 \* Subject: Edge Activation  
 \* Message Body:

Hi,  
 To activate your VeloCloud Edge, please follow these steps:

1. Connect your device to power and any Internet cables or USB modems.
2. Find and connect to the Wi-Fi network that looks like "velocloud-" followed by 3 more letters/numbers (e.g. "velocloud-01c"), and use "vcsecret" as the password. If your device does not have Wi-Fi, connect to it using an Ethernet cable.
3. Click the following link to activate your edge

[http://192.168.2.1/?activation\\_key=UNF4-C4HS-LLKS-R4J8&custom\\_vco=34.232.58.228](http://192.168.2.1/?activation_key=UNF4-C4HS-LLKS-R4J8&custom_vco=34.232.58.228)

If you experience any difficulty, please contact your IT admin.

**Send** **Close**

- 11 Click the **Send** button to send the activation procedure email to the Site Contact. This email will include the same information displayed in the **Send Activation Email** pop-up window. The remaining instructions provide steps for activating the replacement Edge device.
- 12 Disconnect the old Edge from the power and network.
- 13 Connect the new Edge to the power and network. Make sure the Edge is connected to the Internet.
- 14 Follow the activation procedures you received via email.

---

**Note** Be sure to click the activation link in the email to activate the Edge.

---

The Edge will download the configuration and software from the VCO. The new Edge will be activated successfully and will be ready for service.

## RMA Reactivation Troubleshooting

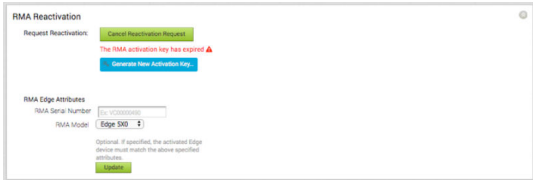
Trying to activate an Edge using an expired RMA Activation key is a common issue. Use these instructions to generate a new activation key after it has expired.

## Expired RMA Activation Key

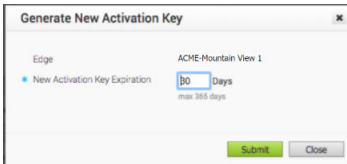
The RMA Activation Key is valid for one month from the time the reactivation request was made. If the RMA Activation Key has expired, a warning message displays in the RMA Reactivation area of the VCO. You can either cancel the reactivation request (by clicking the **Cancel Reactivation Request** button) or generate a new key. Follow the instructions below to generate a new key after the one-month expiration date.

To generate a new RMA Activation Key after the one-month expiration date:

- 1 Click the **Generate New Activation Key** button.



- 2 In the **Generate New Activation Key** dialog box, specify the number of days you would like the key to be active.



- 3 Click **Submit**.
- 4 Follow the *RMA Reactivation Steps* to complete the RMA reactivation process.

# Configure an Edge Device

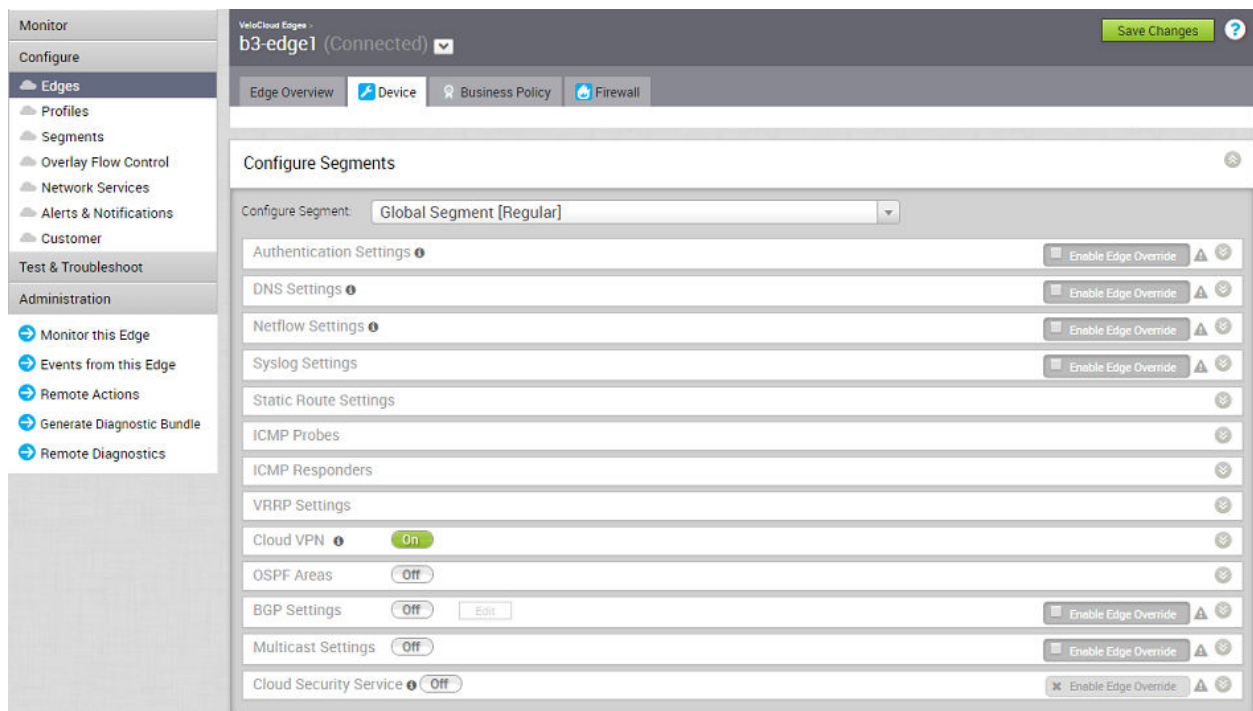
# 15

Configuration overrides can be made to some settings that were assigned to an Edge. In most cases, an override must first be enabled then changes can be made.

Overrides can be made to Interfaces, DNS, and Authentication. In addition override rules can be added to existing Business Policy and Firewall rules. Override rules have precedence over all other rules defined for Business Policy or Firewall.

**Note** Edge overrides enable Edge specific edits to the displayed settings, and discontinue further automatic updates from the configuration Profile. You can simply disable the override and go back to automatic updates any time.

The sections below describe the areas in the **Configure > Edges > Device** tab screen.



Some areas are Segment-aware.

## Segment-aware Configurations:

- Authentication Settings
- DNS Settings
- Netflow Settings
- Syslog Settings
- Static Route Settings
- ICMP Probes
- ICMP Responders
- VRRP Settings
- Cloud VPN
- OSPF Areas
- BGP Settings
- Multicast Settings
- Cloud Security Service

## Common Configurations:

- High Availability
- VLAN
- Device Settings
- WAN Settings
- Multi-Source QoS
- SNMP Settings
- NTP Servers
- Visibility Mode

---

**Note** For information about OSPF and BGP, see the [Chapter 17 Configure Dynamic Routing with OSPF or BGP](#) section.

---

This chapter includes the following topics:

- [Configure Netflow Settings at the Edge Level](#)
- [Configure Syslog Settings at Edge Level](#)
- [Configure Static Route Settings](#)
- [Configure ICMP Probes/Responders](#)

- [Edge Cloud VPN](#)
- [High Availability \(HA\)](#)
- [Configure VLAN Settings](#)
- [Configure Device Settings](#)
- [Configure SNMP Settings at Edge Level](#)
- [Configure Wi-Fi Radio, DNS, Authentication, and Netflow Overrides](#)

## Configure Netflow Settings at the Edge Level

As an enterprise Administrator, at the Edge level, you can override the Netflow settings specified in the Profile by selecting the **Enable Edge Override** checkbox. To override Netflow settings per Edge, perform the steps on this procedure.

### Procedure

- 1 From the VeloCloud Orchestrator, go to **Configure > Edges**.

The **VeloCloud Edges** page appears.

- 2 Select an Edge you want to override Netflow settings and click the icon under the **Device** column.

The Device Setting page for the selected Edge appears.

- 3 From the **Configure Segment** drop-down menu, select a profile segment to configure Netflow settings.

- 4 Go to the **Netflow Settings** area and select the **Enable Edge Override** checkbox.

At the edge level, the **Observation ID** field is auto-populated with 8 bits segment ID and 24 bits edge ID and it cannot be edited. The Observation ID is unique to an Exporting Process per segment per enterprise.

- 5 Follow the Step 4 in [Configure Netflow Settings at the Profile Level](#) to override the collector, filter, and Netflow export interval information specified in the Profile.
- 6 From the **Source Interface** drop-down menu, select an Edge interface configured in the segment as the source interface, to choose the source IP for the NetFlow packets.

---

**Note** Make sure you select an Edge interface with 'Advertise' field set as the source interface. If **none** is selected, the Management interface IP is set as the source interface for the Global segment and the Edge automatically selects an interface with 'Advertise' field set as the source interface for all other segments.

---

- 7 Click **Save Changes**.

## Configure Syslog Settings at Edge Level

In an Enterprise network, VeloCloud Orchestrator (VCO) supports collection of VCO bound events originating from enterprise VeloCloud Edges (VCEs) to one or more centralized remote syslog collectors (Servers), in native syslog format. At the Edge level, you can override the syslog settings specified in the Profile by selecting the **Enable Edge Override** checkbox.

To override the Syslog settings at the Edge level, perform the following steps.

### Prerequisites

- Ensure that Cloud VPN (branch-to-branch VPN settings) is configured for the VCE (from where the VCO bound events are originating) to establish a path between the VCE and the Syslog collectors. For more information, see [Configure Cloud VPN](#).

### Procedure

- 1 From the VeloCloud Orchestrator, go to **Configure > Edges**.  
The **VeloCloud Edges** page appears.
- 2 Select an Edge you want to override Syslog settings and click the icon under the **Device** column.  
The Device Setting page for the selected Edge appears.
- 3 From the **Configure Segment** drop-down menu, select a profile segment to configure syslog settings. By default, **Global Segment [Regular]** is selected.
- 4 Go to the **Syslog Settings** area and select the **Enable Edge Override** checkbox to override the syslog settings specified in the Profile associated with the Edge.



5 Click the expand icon and configure the following details.

- a From the **Facility Code** drop-down menu, select a Syslog standard value that maps to how your Syslog server uses the facility field to manage messages for all the events from VCEs. The allowed values are from **local0** through **local7**.

---

**Note** The **Facility Code** field is configurable only for the **Global Segment**, even if the Syslog settings is enabled or not for the Edge. The other segments will inherit the facility code value from the Global segment.

---

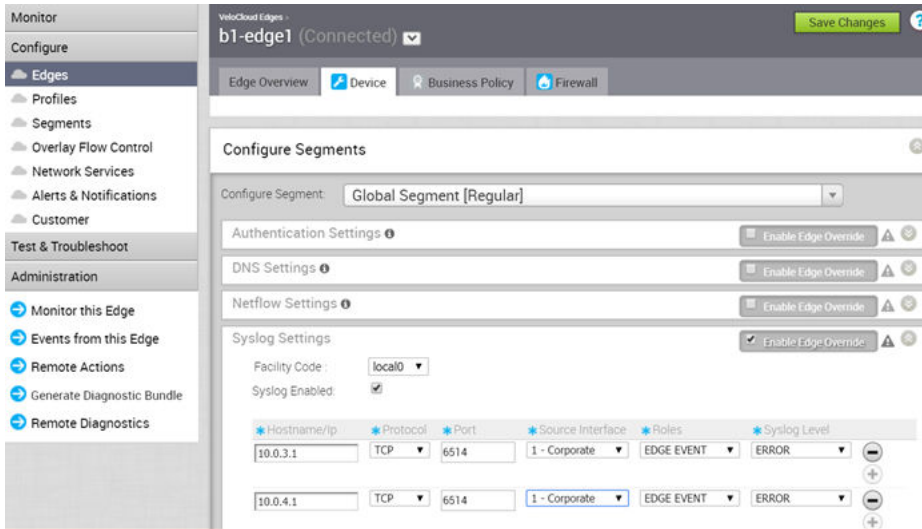
- b Select the **Syslog Enabled** checkbox.
- c In the **IP** text box, enter the destination IP address of the Syslog collector.
- d From the **Protocol** drop-down menu, select either **TCP** or **UDP** as the Syslog protocol.
- e In the **Port** text box, enter the port number of the Syslog collector. The default value is 514.
- f From the **Source Interface** drop-down menu, select one of the Edge interface configured in the segment as the source interface.
- g From the **Roles** drop-down menu, select **EDGE EVENT**.
- h From the **Syslog Level** drop-down menu, select the Syslog severity level that need to be configured. For example, If **CRITICAL** is configured, the VCE will send all the events which are set as either critical or alert or emergency.

The allowed Syslog severity levels are:

- **EMERGENCY**
- **ALERT**
- **CRITICAL**
- **ERROR**
- **WARNING**
- **NOTICE**
- **INFO**
- **DEBUG**

6 Click the + button to add another Syslog collector.

You can configure a maximum of two Syslog collectors per segment and 10 Syslog collectors per Edge. When the number of configured collectors reaches the maximum allowable limit, the + button will be disabled.



**Note** By configuring the Syslog setting for the Edges, only remote syslog for VCO bound events from Edges will be received at the Syslog collector. If you want the VCO auto-generated local events to be received at the Syslog collector, you must configure Syslog at the VCO level by using the `log.syslog.backend` and `log.syslog.upload` system properties.

## Configure Static Route Settings

**Static Route Settings** are useful for special cases in which static routes are needed for existing network attached devices (such as printers). You can add additional Static Route Settings (plus '+' icon) or delete Static Route Settings (minus '-' icon) located to the right of the dialog box.

For details about the settings in the dialog box, refer to the table that follows.

* Subnet	Source IP	* Next Hop	* Interface	VLAN	* Cost	Preferred	Advertise	ICMP Probe	Description
52.1.1.0/24	n/a	176.253.2.33	GE4		10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	[none]	Description (Optional)
32.1.1.0/24	n/a	10.23.0.166	[not applicable]		10	<input type="checkbox"/>	<input type="checkbox"/>	[none]	Description (Optional)

To specify the Static Route Settings:

- 1 Enter the subnet for the route.
- 2 Enter the IP address for the route.
- 3 Select the WAN interface where the Static Route will be bound.
- 4 Select the **Broadcast** checkbox to advertise this route over VPN and allow other Edges in the network to have access to this resource.
- 5 Optionally, add a description for the route.

## Configure ICMP Probes/Responders

ICMP handlers may be needed to enable integration with an external router that is performing dynamic routing functionality and needs stateful information about route reachability via VeloCloud. The **Device Settings** area provides sections for specifying ICMP Probes and Responders.

ICMP Probes can be specified settings for Name, VLAN Tagging (none, 802.1q, 802.1ad, QinQ (0x8100), or QinQ (0x9100)), C-Tags, S-Tags, Source/Destination/Next Hop IPs, Frequency to send ping requests, and Threshold the value for number of missed pings that will cause route to be marked unreachable.

ICMP Responders can be specified settings for **Name**, **IP Address**, and **Mode** ( **Conditional** or **Always**).

- **Always:** Edge always responds to ICMP Probes.
- **Conditional:** Edge only responds to ICMP Probes when the SD-WAN Overlay is up.

The screenshot shows two configuration panels. The top panel, titled "ICMP Probes", includes fields for Name, VLAN Tagging (set to "none"), C-Tag, S-Tag, Source IP, Destination IP, Next Hop IP, Frequency, and Threshold. The bottom panel, titled "ICMP Responders", includes fields for Name, IP Address, and Mode (set to "Conditional"). Both panels have "Clone" buttons.

## Edge Cloud VPN

The Edge Cloud VPN settings are inherited from the Profile selected for the Edge and can be reviewed in the Edge **Device** tab. Changes to Cloud VPN settings can be made only in the associated Profile.

The screenshot shows the "Cloud VPN" configuration interface, which is currently "On". It features three main sections: "Branch to Non-VeloCloud Site" (Enabled, with a dropdown set to "VeloAcme-DC"), "Branch to VeloCloud Hubs" (Disabled), and "Branch to Branch VPN" (Enabled). The "Branch to Branch VPN" section includes sub-options: "Use Cloud Gateways" (Enabled), "Use VeloCloud Hubs for VPN" (Disabled), and "Dynamic Branch to Branch VPN" (Enabled).

## High Availability (HA)

Enable High Availability (HA) for the Edge here.

The screenshot shows the "High Availability" configuration interface. It includes a "Type" section with four radio button options: "None" (selected), "VeloCloud Active Standby Pair", "VeloCloud Cluster", and "Non VeloCloud VRRP Pair".

For more

information about the setup and configuration of HA, see *HA Configuration*.

## Configure VLAN Settings

The **VLAN** dialog box displays settings that can be chosen for your LAN interfaces.

**VLAN**

Segment: United Segment  Enable Edge Override

VLAN Name: unitedLocalAreaNetwork

VLAN Id: 1

Edge LAN IP Address: 10.54.0.7

Cidr Prefix: 24

Network: 10.54.0.0

Advertise:

Fixed IPs:

MAC Address	IP	Description
Ex: aa:bb:cc:dd:ee:ff	Ex: 10.0.2.5	Description (option)

LAN Interfaces: **GE1**

SSID: There are no Wi-Fi SSIDs configured on this VLAN.

**DHCP**  Enable Edge Override

Type: Enabled

DHCP Start: 10.54.0.0

Num. Addresses: 7

Lease Time: 1 day

DHCP Options: not set

**OSPF**  Enable Edge Override

Enabled:  OSPF not enabled for the selected Segment.

Update VLAN Cancel

The Edge LAN IP address, the Edge Management IP address, and CIDR Prefix. You can also specify Fixed IP addresses tied to specific MAC Addresses. The list of LAN interfaces and the SSID of any Wi-Fi interfaces that are configured for this VLAN are listed. Finally, a block for configuring DHCP is shown. DHCP can be Enabled (where a start address, the number of addresses, the lease time, and optional parameters are entered), the address of one or more relay agents can be enabled, or DHCP can be disabled.

## Configure Device Settings

The Edge **Device Settings** screen provides the ability to do the following tasks:

- Set VLAN Settings
- Override Syslog Settings
- Override Profile Interface Settings
- Add a User Defined WAN Overlay
- Configure NAT for overlapping Network

### Configure DHCP Server on Routed Interfaces

You can configure DHCP server on a Routed Interface in an Edge.

To configure DHCP Server settings:

- 1 In the Enterprise portal, click **Configure > Edges**.

- 2 Click the Device Icon next to an Edge, or click the link to the Edge, and then click the **Device** tab.
- 3 Scroll down to the **Device Settings** section and click the DOWN arrow to view the **Interface Settings** for the Edge.
- 4 The **Interface Settings** section displays the existing interfaces available in the Edge.
- 5 Click the **Edit** option for the Routed interface that you want to configure DHCP settings.

The screenshot shows the configuration window for Interface: GE3. The settings are as follows:

- Interface: GE3** (Override Interface checked)
- Interface Enabled:
- Capability: Routed (dropdown)
- Segments: All Segments
- Addressing Type: Static (dropdown)
- IP Address: 169.254.7.10
- CIDR prefix: 29
- Gateway: 169.254.7.9
- WAN Overlay:  Auto-Detect Overlay (dropdown) unlock
- OSPF:  OSPF not enabled for the selected Segment.
- Multicast: Multicast is not enabled for the selected segment
- RADIUS Authentication:  Require User Authentication to access WAN. Note: WAN Overlay must be disabled to configure RADIUS Authentication.
- Advertise:
- ICMP Echo Response:
- NAT Direct Traffic:
- Underlay Accounting:
- Trusted Source:
- Reverse Path Filter: Specific (dropdown)
- VLAN: (empty field)
- L2 Settings**
- Autonegotiate:
- MTU: 1500
- DHCP Server**
- Type: Enabled (selected), Relay, Disabled
- DHCP Start: 169.254.7.10
- Num. Addresses: 6
- Lease Time: 1 hour (dropdown)
- Options: add an option (dropdown)

Buttons at the bottom: Update GE3, Cancel

- 6 In the **Interface** window, select the **Addressing Type** as **Static** and enter the IP addresses for the Edge Interface and the Gateway.
- 7 In the **DHCP Server** section, choose one of the following DHCP settings:
  - **Enabled** – Enables DHCP with the Edge as the DHCP server. Configure the following details:
    - **DHCP Start** – Enter a valid IP address available within the subnet.
    - **Num. Addresses** – Enter the number of IP addresses available on a subnet in the DHCP Server.
    - **Lease Time** – Select the period of time from the drop-down list. This is the duration the VLAN is allowed to use an IP address dynamically assigned by the DHCP Server.

- **Options** – Add pre-defined or custom DHCP options from the drop-down list. The DHCP option is a network service passed to the clients from the DHCP server. For a custom option, enter the code, data type, and value.
- **Relay** – Enables DHCP with the DHCP Relay Agent installed at a remote location. If you choose this option, configure the following:
  - **Relay Agent IP(s)** – Specify the IP address of Relay Agent. Click the Plus(+) Icon to add more IP addresses.
- **Disabled** – Disables DHCP.

For more information on other options in the **Interface Settings** window, see [Configure Interface Settings](#).

## Enabling RADIUS on a Routed Interface

RADIUS can be enabled on any interface that can be configured as a routed interface. See the section below for step-by-step instructions.

### Requirements

- A RADIUS server must be configured and added to the Edge. This is performed on the **Configure -> Network Services** screen in the VMware SD-WAN Orchestrator.
- RADIUS may be enabled on any interface that can be configured as a routed interface. This includes the interfaces for any Edge model, except for the LAN 1-8 ports on Edge models 500/520/540.

---

**Note** RADIUS enabled interfaces do not use DPDK.

---

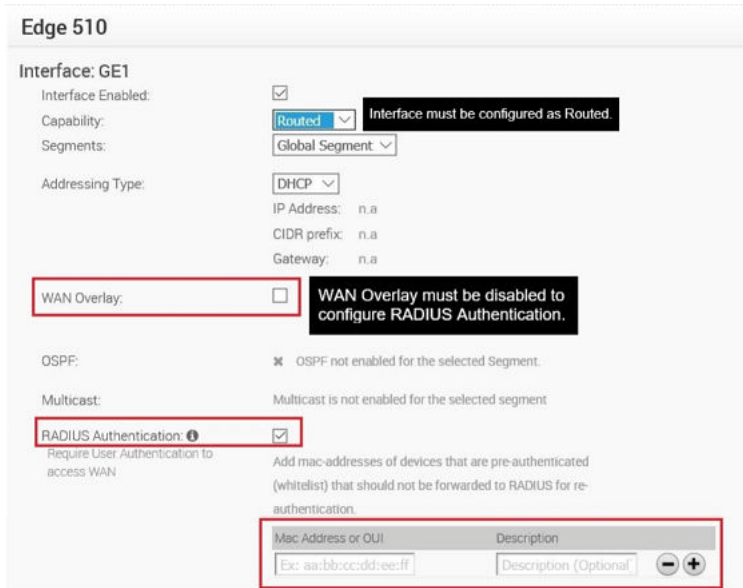
### Enabling RADIUS on a Routed Interface

- 1 Go to **Configure->Device** on the VMware SD-WAN Orchestrator, click **Edit** for the interface you want to enable RADIUS authentication.
- 2 Configure the Capability parameter as **Routed**.
- 3 Disable the **WAN Overlay** by unchecking the box.
- 4 Enable **RADIUS Authentication** by checking that box.
- 5 Configure the allowed list of devices that are pre-authenticated and should not be forwarded to RADIUS for re-authentication. You can add devices by individual MAC addresses (e.g. 8c:ae:4c:fd:67:d5) and by OUI (Organizationally Unique Identifier [e.g. 8c:ae:4c:00:00:00]).

---

**Note** The interface will use the server that has already been assigned to the Edge (i.e. two interfaces cannot use two different RADIUS servers).

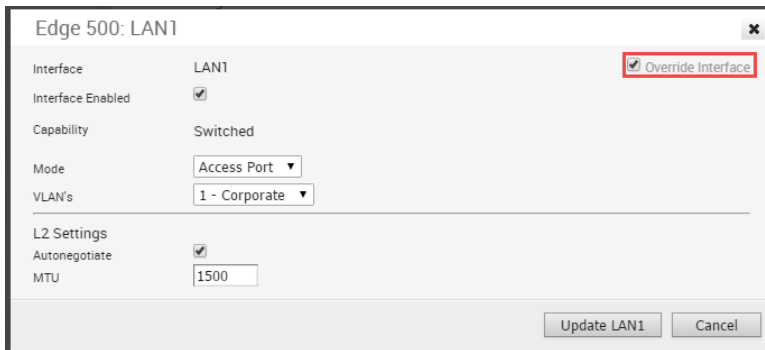
---



## Configure Edge LAN Overrides

The LAN settings specified in the Profile can be overridden by selecting the **Override Interface** check box.

See [Chapter 11 Configure a Profile Device](#) for LAN interface configuration parameters.



## Configure Edge WAN Overrides

The WAN settings specified in the Profile can be overridden by selecting the **Override Interface** checkbox.

See [Chapter 11 Configure a Profile Device](#) for LAN interface configuration parameters.



## Configure Edge WAN Overlay Settings

Edge WAN settings enable you to add or modify the user-defined WAN Overlay network. You can also modify the auto-detected WAN Overlay settings. You can assign the configured WAN interfaces to a WAN link.

In the Enterprise portal, navigate to **Configure > Edges**.

Either click the Device Icon next to an Edge or click the link to the Edge and click the **Device** tab.

You can configure the WAN overlay properties in the **WAN Settings**.

For the auto-detected WAN Overlay networks, click the **Edit** option to modify the settings.

For the user-defined WAN Overlay networks, click **Add User Defined WAN Overlay** to create new Overlay settings or click **Edit** for an existing network to modify the settings.



### Virtual Edge: Corporate

#### User Defined WAN Overlay

Link Type: Private

Name: Corporate

SD-WAN Service Reachable:

Public SD-WAN Addresses:

Address
10.81.117.193
169.254.10.2
169.254.10.10

Public IP Address: n. a.

Pre-Notification Alerts:

Alerts:

Interfaces: GE5

update selection

#### Optional Configuration

Source IP Address: 10.1.1.1

Next-Hop IP Address: 10.1.2.1

Custom VLAN:  101

802.1P Setting:  001

#### Advanced Settings

Bandwidth Measurement: Measure Bandwidth (Slow Start)

Dynamic Bandwidth Adjustment:

Link Mode: Active

MTU: 1500

Overhead Bytes: 0

Private Network Name: Test

#### Private Link Configuration

Configure Static SLA:

Configure Class of Service:

Strict IP Precedence:

Class Of Service	DSCP Tags	Bandwidth (%)	Policing	Default Class	
CoS 1	CS5, EF	60	<input checked="" type="checkbox"/>	<input type="radio"/>	- +
CoS 2	AF41, CS4	20	<input type="checkbox"/>	<input type="radio"/>	- +
CoS 3	AF21, CS2	20	<input type="checkbox"/>	<input checked="" type="radio"/>	- +

Advanced
Update Link
Cancel

**Table 15-1. WAN Overlay Settings**

Option	Description
Link Type (Available only for user-defined Overlay)	You can deploy the WAN Overlay as a public or private link. Choose the relevant link type from the drop-down.
Name	Enter a descriptive name for the public or private link
SD-WAN Service Reachable (Available only for user-defined Overlay and a Private link)	<p>VeloCloud supports private WAN deployments with a hosted VeloCloud service for customers with hybrid environments who deploy in sites with only a private WAN link.</p> <p>In a site with no public overlays, the private WAN can be used as the primary means of communication with the VeloCloud service, by enabling the SD-WAN Service Reachable option.</p> <p>When you select the checkbox, the list of public SD-WAN IP addresses is displayed, which would be advertised across the private network to allow the operation without public WAN overlays.</p>

Table 15-1. WAN Overlay Settings (continued)

Option	Description
Public IP Address	Displays the IP address learned from the Interface associated with the WAN Overlay being edited or created.
Pre-Notification Alerts	Select the checkbox to enable pre-notification alerts. Ensure that you have enabled the Link alerts in the <b>Configure &gt; Alerts &amp; Notifications</b> screen to receive the alerts.
Alerts	Select the checkbox to enable alerts. Ensure that you have enabled the Link alerts in the <b>Configure &gt; Alerts &amp; Notifications</b> screen to receive the alerts.
Interfaces	Select one or more routed interfaces from the <b>update selection</b> drop-down. The list consists of Routed Interfaces with the WAN Overlay set to <b>User Defined Overlay</b> . This option binds the current user-defined overlay with the routed interface that you select. <b>Note</b> The <b>update selection</b> option is available only for user-defined WAN Overlay.
Source IP Address (Available only for user-defined Overlay)	Enter the IP address of the routed interface. This is the raw socket source IP address used for VCMP tunnel packets that originate from the Interface selected in the <b>Interfaces</b> drop-down, to which the User Defined Overlay is bounded. Source IP address does not have to be pre-configured anywhere but must be routable to and from the Interface this User Defined Overlay is bounded.
Next-Hop IP Address (Available only for user-defined Overlay)	Enter the next hop IP address to which the packets, which come from the raw socket source IP address specified in the <b>Source IP Address</b> field, should be routed.
Custom VLAN (Available only for user-defined Overlay)	Select the checkbox to enable custom VLAN and enter the VLAN ID. The range is 2 to 4094. This option applies the VLAN tag to the packets originated from the Source IP Address of a VCMP tunnel from the interface selected in the <b>Interfaces</b> drop-down.
802.1P Setting (Available only for user-defined Overlay)	To configure the 802.1P setting, the System Property <b>session.options.enable8021PConfiguration</b> must be set to True. By default, this value is False. If this option is not available for you, contact your Operator to enable the setting. You can select this checkbox, only when you have already selected the Custom VLAN checkbox. Select the checkbox to enable the 802.1P setting and enter the priority value as a 3-digit binary number. The range is from 000 to 111 and default is 000.

Click **Advanced** to configure the following settings:

Option	Description
Bandwidth Measurement	<p>Choose a method to measure the bandwidth from the following options:</p> <ul style="list-style-type: none"> <li>■ <b>Measure Bandwidth (Slow Start):</b> When measuring the default bandwidth reports incorrect results, it may be due to ISP throttling. To overcome this behavior, choose this option for a sustained slow burst of UDP traffic followed by a larger burst.</li> <li>■ <b>Measure Bandwidth (Burst Mode):</b> Choose this option to perform short bursts of UDP traffic to an SD-WAN Gateway for public links or to the peer for private links, to assess the bandwidth of the link.</li> <li>■ <b>Do Not Measure (define manually):</b> Choose this option to configure the bandwidth manually. This is recommended for the Hubs.</li> </ul>
Upstream Bandwidth	Enter the upstream bandwidth in Mbps. This option is available only when you choose Do Not Measure (define manually).
Downstream Bandwidth	Enter the downstream bandwidth in Mbps. This option is available only when you choose Do Not Measure (define manually).
Dynamic Bandwidth Adjustment	Select the checkbox to track congestion and packet loss in WAN and to adjust the bandwidth as required. It is recommended to enable this option for wireless links.
Use as Backup Only	<p>Select the checkbox to use the Overlay WAN as a backup, when other Overlay networks are down or not available. The Overlay WAN is displayed in the Monitoring page as a backup link. Click <b>Monitor &gt; Edges</b> to view the status of the Edge.</p> <hr/> <p><b>Note</b> If the Edge is used as a hub or is part of a cluster, then do not choose this option.</p>
MTU	<p>Enter a value for the maximum transmission unit (MTU). The range is 576 to 1500 bytes.</p> <hr/> <p><b>Note</b> It is recommended to use the MTU size from 1300 bytes and above. The optimum size is 1500 bytes.</p>
Overhead Bytes	<p>Enter a value for the Overhead bandwidth in bytes. This is an option to indicate the additional L2 framing overhead that exists in the WAN path.</p> <p>When you configure the Overhead Bytes, the bytes are additionally accounted for by the QoS scheduler for each packet, in addition to the actual packet length. This ensures that the link bandwidth is not oversubscribed due to any upstream L2-framing overhead.</p>
Private Network Name (Available only for user-defined Overlay and a Private link)	Choose the private network name from the drop-down list. You can also click <b>New Private Network Name</b> from the list and enter a name for a new network.

Option	Description
UDP Hole Punching (Available only for a Public link)	Select the checkbox to enable UDP hole punching for the Overlay network.
Type (Available only for a Public link)	Choose whether the link is Wired or Wireless, from the drop-down.
Configure Static SLA (Available only for user-defined Overlay and a Private link)	Select the checkbox to configure the static SLA and enter the values for Latency, Jitter, and Loss.
Configure Class of Service (Available only for user-defined Overlay and a Private link)	<p>Select the checkbox to configure the class of service and enter appropriate values for the following:</p> <ul style="list-style-type: none"> <li>■ <b>Class of Service:</b> Enter a descriptive name for the class of service.</li> <li>■ <b>DSCP Tags:</b> Click <b>Set</b> to select the DSCP tags to be used in the class of service.</li> <li>■ <b>Bandwidth:</b> Enter a value for the bandwidth.</li> <li>■ <b>Policing:</b> Select the checkbox to enable the class-based policing.</li> <li>■ <b>Default Class:</b> Click to set the corresponding class of service as default.</li> </ul> <p>Click the Plus icon (+) to add more rows and the Minus icon (-) to remove a row. For more information on class of service, see <a href="#">Configure Edge WAN Settings for MPLS Private Links</a>.</p>

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

## Configure Edge WAN Settings for MPLS Private Links

You can differentiate traffic within a private WAN link by defining multiple Classes of Service (CoS). The following example is a simple scenario in which a percentage of the bandwidth (10Mbps) is assigned to three Classes of Services.

### Edge WAN Settings for MPLS Private Links Example

In this simple example, the user has 10Mbps bandwidth available. They want to send some traffic to voice, some traffic to PCI data, and all other data to be designated as default traffic. The types of traffic (CoS) will be defined by the user via Differentiated Services Code Point (DSCP) Tag(s), as shown in the table below.

**Note** The **DSCP Tags** are user defined.

Table: MPLS CoS Example

Class of Service	Description	DSCP Tags	Policing	Static SLA			
					Bandwidth (Percentage)	Latency	Jitter
CoS1	Voice	CS5, EF	✓	60	10ms	4ms	0.005%

<b>CoS2</b>	Video	AF41, CS4	20	15ms	4ms	0.05%
<b>CoS3</b>	File Transfer	AF21, CS2	20	15ms	4ms	0.1%
Link Characteristics				15ms	4ms	0.1%

Therefore, according to the above table, the voice on a MPLS CoS would be identified as DSCP tag CS5, EF, Video on a MPLS CoS would be identified as AF41, CS4, and the file transfer on a MPLS CoS would be identified as DSCP tag AF21, CS2. See the **Private Link Configuration** image below for an example.

Private Link Configuration

Configure Static SLA:

Configure Class of Service:

Class Of Service	DSCP Tags	Bandwidth (%)	Policing	Default Class	
CoS 1	CS5, EF	60	<input checked="" type="checkbox"/>	<input type="radio"/>	[-] [+]
CoS 2	AF41, CS4	20	<input type="checkbox"/>	<input type="radio"/>	[-] [+]
CoS 3	AF21, CS2	20	<input type="checkbox"/>	<input checked="" type="radio"/>	[-] [+]

### Policing MPLS CoS

For a private link that has CoS agreement with a MPLS provider, a Service Provider will guarantee a different SLA for each CoS on a MPLS Link. The DMPO can treat each CoS as a different link and can take granular application aware decisions for a private link with CoS agreements. A Policer can be defined for a MPLS CoS underlay to ensure that the Service Provider committed bandwidth SLAs are being honored by the customer.

## Configure Edge WAN Settings for MPLS Private Links

To assign CoS to a user-defined private WAN link:

**Note** For more information, see [Configure Edge WAN Settings for MPLS Private Links](#) and *Edge WAN Settings for Private Links Example*.

- 1 Click **Edges** under **Configure** in the navigation panel of the VCO.
- 2 In the VeloCloud **Edges** screen, you have two options to access the **Device Settings** tab:
  - a **First Option:** Click an Edge's link to open the **Edge Overview** screen, and then click the **Device Settings** tab.
  - b **Second Option:** From the VeloCloud **Edges** screen, click an Edge's **Device Settings** icon.
- 3 In the **Actions** section of the **WAN Settings** area, click the **Edit** link for a Private link. See image below.

WAN Settings							
Add User Defined WAN Overlay							
Actions	Type	Name	Interfaces	Link Type	Public IP	Pre-Notifications	Alerts
<a href="#">Edit</a>   <a href="#">Del</a>	Auto Detect	AT&T Services	INTERNET1	Public Wired	12.205.175.221	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<a href="#">Edit</a>   <a href="#">Del</a>	User Defined	Private Link ...	INTERNET2	Private Wired	192.168.2.2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

- In the **Private Link...** dialog, click the **Advanced** button to open the **Private Link Configuration** area.
- In the **Private Link Configuration** area, click the **Configure Class of Service** checkbox. See image below.

**Private Link Configuration**

Configure Static SLA:

Configure Class of Service:

Class Of Service	DSCP Tags	Bandwidth (%)	Policing	Default Class	
<input type="text"/>	<a href="#">Set...</a>	100	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="button" value="-"/> <input type="button" value="+"/>

- In the **Class of Service** text box, type in a Class of Service to differentiate the types of traffic (e.g. Voice). Click the **Plus** symbol to add another row.
- Click the **Set** link to open the **DSCP Tags** dialog to assign a DSCP tag for the Class of Service you created.
- In the **DSCP Tags** dialog, select a DSCP tag from the **Available DSCP Tags** list area, and then click the appropriate arrow to move the tag to the **Selected DSCP Tags** area. See the image below.

**Note** You can select multiple DSCP Tags to assign to a single CoS.

- Click **Submit**.

**DSCP Tags** ✕

<p>Available DSCP Tags</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> AF11</li> <li><input type="checkbox"/> AF12</li> <li><input type="checkbox"/> AF13</li> <li><input type="checkbox"/> AF21</li> <li><input type="checkbox"/> AF22</li> <li><input type="checkbox"/> AF23</li> <li><input type="checkbox"/> AF31</li> <li><input type="checkbox"/> AF32</li> <li><input type="checkbox"/> AF33</li> <li><input type="checkbox"/> AF41</li> </ul>	<input type="button" value="&gt;"/> <input type="button" value="&lt;"/> <input type="button" value="&gt;&gt;"/> <input type="button" value="&lt;&lt;"/>	<p>Selected DSCP Tags</p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> EF</li> </ul>
---	--	--

- 10 In the **Bandwidth (%)** column, type in the traffic percentages you want to designate for each of the Class of Services. All of the values in the **Bandwidth** column must equal 100%. See image below.
- 11 If applicable, check the **Default Class** radial button.
- 12 If applicable, check the **Policing** checkbox. For more information, see section title, *Edge WAN Settings for MPLS Private Links Example* for more information about Policing.

Private Link Configuration

Configure Static SLA:

Configure Class of Service:

Class Of Service	DSCP Tags	Bandwidth (%)	Policing	Default Class	
CoS 1	CS5, EF	60	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="button" value="-"/> <input type="button" value="+"/> <input type="button" value="-"/> <input type="button" value="+"/>
CoS 2	AF41, CS4	20	<input type="checkbox"/>	<input type="radio"/>	<input type="button" value="-"/> <input type="button" value="+"/> <input type="button" value="-"/> <input type="button" value="+"/>
CoS 3	AF21, CS2	20	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="button" value="-"/> <input type="button" value="+"/> <input type="button" value="-"/> <input type="button" value="+"/>

- 13 Click the **Update Link** button.

## SD-WAN Service Reachability via MPLS

An Edge with only Private MPLS links can reach the Orchestrator and Gateways located in public cloud, by using the SD-WAN Service Reachable option.

In a site with no direct public internet access, the SD-WAN Service Reachable option allows the private WAN to be used for private site-to-site VCMP tunnels and as a path to communicate with an internet hosted VeloCloud service.

For hybrid environments that have MPLS-only links or require failover to MPLS links, you can enable the SD-WAN Service Reachable option.

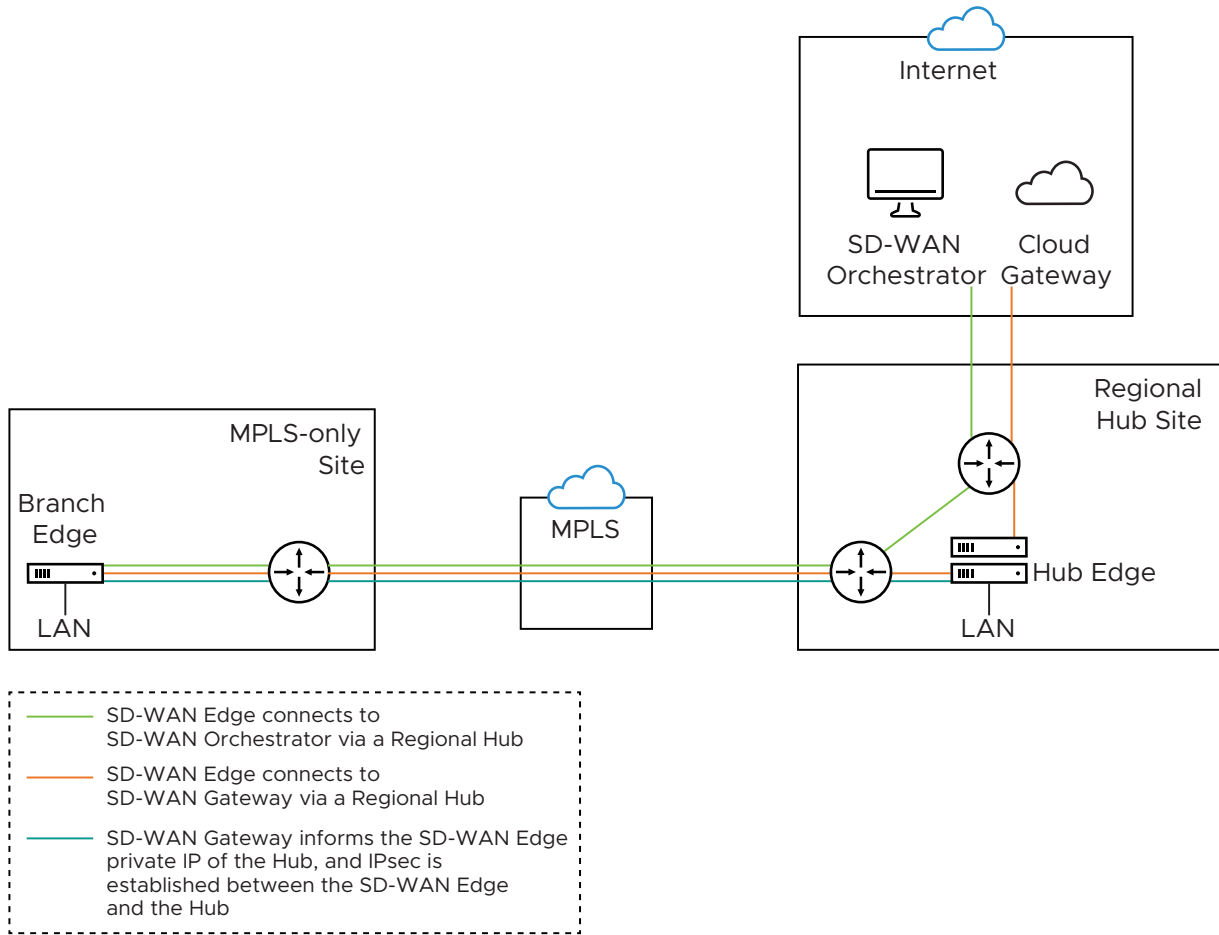
### MPLS-only Sites

VeloCloud supports private WAN deployments with a hosted VeloCloud service for customers with hybrid environments who deploy in sites with only a private WAN link.

In a site with no public overlays, the private WAN can be used as the primary means of communication with the VeloCloud service, including the following:

- Enabled SD-WAN service reachability through private link
- Enabled NTP override using private NTP servers

The following image shows a Regional Hub with Internet connection and SD-WAN Edge with only MPLS connection.

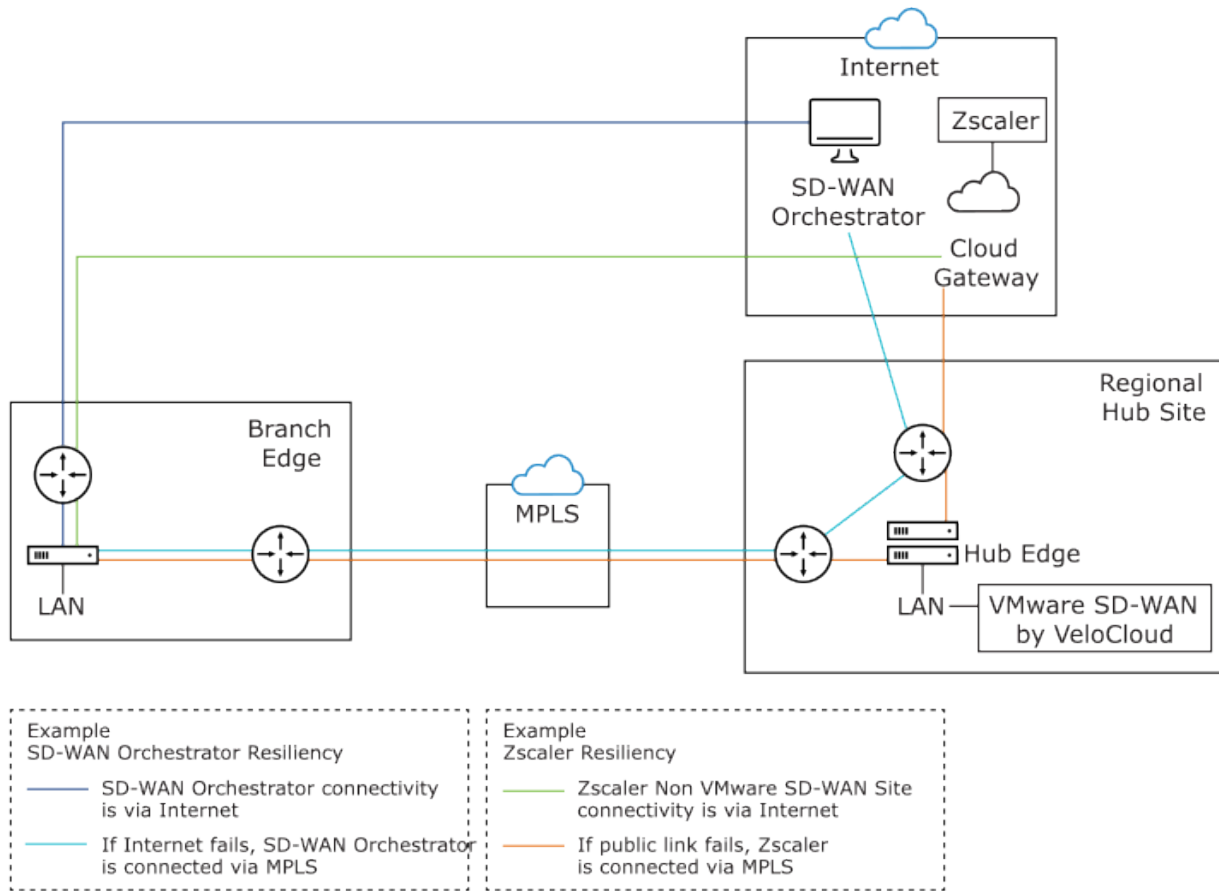


The traffic from the SD-WAN Edge with MPLS-only links is routed to the Orchestrator and Gateway through a Regional Hub, which is able to break out to the public cloud. SD-WAN Service Reachable option allows the Edge to remain online and manageable from the Orchestrator, and allows public internet connectivity through the Gateway irrespective of whether or not there is public link connectivity.

### Dynamic Failover via MPLS

If all the public Internet links fail, you can failover critical Internet traffic to a private WAN link. The following image illustrates Resiliency of SD-WAN Orchestrator and Non-VeloCloud Site, Zscaler.





- **Orchestrator Resiliency** – The Orchestrator connects to the Internet. If the Internet fails, the Orchestrator will connect through MPLS. The Orchestrator connection is established using the IP Address which is advertised over MPLS. The connectivity leverages the public Internet link in the Regional Hub.
- **Zscaler Resiliency** – The Zscaler connectivity is established through Internet. If the public link fails, then Zscaler connects through MPLS.

### Configure SD-WAN Service Reachable

- 1 In the Enterprise portal, click **Configure > Edges**.
- 2 In the Edges page, either click the device Icon next to an Edge or click the link to the Edge and click the **Device** tab.
- 3 Scroll down to **Interface Settings** and **Edit** the Interface connected to the MPLS link.
- 4 In the **Interface** window, select the **User Defined Overlay** checkbox.

**Virtual Edge**

**Interface GE6** Override Interface

Interface Enabled

Capability ↓ Routed

Segments All Segments

Addressing Type ↓ Static

IP Address 172.16.1.10

CIDR prefix 29

Gateway 172.16.1.11

WAN Overlay  ↓ User Defined Overlay

OSPF  OSPF not enabled for the selected Segment.

VNF Insertion  VNF insertion is disallowed when an interface is configured for WAN overlays

Multicast Multicast is not enabled for the selected segment

RADIUS Authentication  Require User Authentication to access WAN   
  WAN Overlay must be disabled to configure RADIUS Authentication.

Advertise

ICMP Echo Response

NAT Direct Traffic

Underlay Accounting

Trusted Source

Reverse Path Forwarding ↓ Specific

VLAN

**L2 Settings**

Autonegotiate

\* MTU 1500

**DHCP Server**

Type Enabled Relay Disabled

Update GE6 Cancel

The **SD-WAN Service Reachable** is available only for a **User Defined Overlay** network.

- 5 In the **WAN Settings** section, **Edit** the Interface enabled with **User Defined Overlay**.
- 6 In the **User Defined WAN Overlay** window, select the **SD-WAN Service Reachable** checkbox to deploy sites which only have a private WAN link and/or enable the capability to failover critical Internet traffic to a private WAN link.

**Virtual Edge: GE6\_Private**

**User Defined WAN Overlay**

Link Type ↓ Private

Name GE6\_Private

SD-WAN Service Reachable

Public SD-WAN Addresses

Address
169.254.8.2
169.254.10.2
169.254.10.10

Public IP Address n. a.

Pre-Notification Alerts

Alerts

Interfaces  GE6

update selection ↓

**Optional Configuration**

Source IP Address 1.2.3.4

Next-Hop IP Address 1.2.3.4

Custom VLAN

Advanced Update Link Cancel

When you select the **SD-WAN Service Reachable** checkbox, a list of public IP addresses of SD-WAN Gateways and SD-WAN Orchestrator is displayed, which may need to be advertised across the private network, if a default route has not been already advertised across the same private network from the firewall.

- 7 Configure other options as required and click **Update Link** to save the settings.

For more information on other options in the **WAN Overlay** window, see [Configure Edge WAN Overlay Settings](#).

## Configure SNMP Settings at Edge Level

SNMP is a commonly used protocol for network monitoring and MIB is a database associated with SNMP to manage entities. SNMP can be enabled by selecting the desired SNMP version as described in the steps below. At the Edge Level, you can override the SNMP settings specified in the Profile by selecting the **Enable Edge Override** checkbox.

---

**Note** Edges do not generate SNMP traps. If there is a failure at the Edge level, the Edge reports the failure in the form of events to Orchestrator, which in turn generates traps based on the alerts configured for the received events.

---

### Before you begin:

- The VeloCloud Edge MIB is new for the 3.3.2 release. To download the VeloCloud Edge MIB: go to the **Remote Diagnostic** screen (**Test & Troubleshooting > Remote Diagnostics**) and run MIB for VeloCloud Edge. Copy and paste results onto your local machine.
- Install all MIBs required by VELOCLOUD-EDGE-MIB on the client host, including SNMPv2-SMI, SNMPv2-CONF, SNMPv2-TC, INET-ADDRESS-MIB, IF-MIB, UUID-TC-MIB, and VELOCLOUD-MIB. All the above-mentioned MIBs, except VELOCLOUD-MIB, can be found online. For VELOCLOUD-MIB, please check VeloCloud website.

**About this task:** At the Edge level, you can override the SNMP settings specified in the Profile by selecting the **Enable Edge Override** checkbox. The Edge Override option enables Edge specific edits to the displayed settings, and discontinues further automatic updates from the configuration profile for this module. For ongoing consistency and ease of updates, it is recommended to set configurations at the Profile rather than Edge exception level.

### Supported MIBs

- SNMP MIB-2 System
- SNMP MIB-2 Interfaces
- VELOCLOUD-EDGE-MIB (new for the 3.3.2 release)
- HOST-RESOURCES-MIB, from RFC 1514

### Procedure to Configure SNMP Settings at Edge Level:

- 1 Obtain the VELOCLOUD-EDGE-MIB on the Remote Diagnostic screen of the VeloCloud Orchestrator. (See "Before you begin" for more information).

2 Install all MIBs required by VELOCLOUD-EDGE-MIB. (See "Before you begin" for more information.)

3 From the VeloCloud Orchestrator, go to **Configure > Edges**.

The **VeloCloud Edges** screen appears.

4 Select an Edge you want to configure SNMP settings for, and click the **Device** icon under the Device column.

The **Configuration Edges** screen for the selected Edge appears.

5 Scroll down to the **SNMP Settings** area and check the **Enable Edge Override** checkbox. You can choose between two versions, v2c or v3.



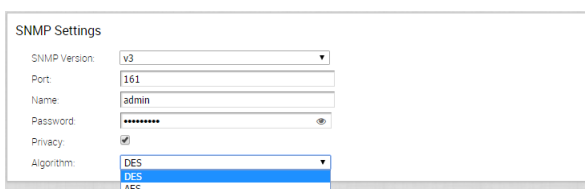
6 For a SNMP v2c config follow the steps below:

- a Check the **v2c** checkbox.
- b Type in a Port in the **Port** textbox. The default setting is 161.
- c In the **Community** textbox, type in a word or sequence of numbers that will act as a 'password' that will allow you access to the SNMP agent.
- d For Allowed IPs:
  - Check the **Any** checkbox to allow any IP to access the SNMP agent.
  - To restrict access to the SNMP agent, uncheck the **Any** checkbox and enter the IP address(es) that will be allowed access to the SNMP agent.



7 For a SNMP v3 config, which provides added security support follow the steps below:

- a Type in a port in the **Port** textbox. 161 is the default setting.
- b Type in a user name and password in the appropriate textboxes.
- c Check the **Privacy** checkbox if you want your packet transfer encrypted.
- d If you've checked the **Privacy** checkbox, choose DES or AES from the **Algorithm** drop-down menu.



- Configure Firewall Settings. After you have configured SNMP Settings, go to Firewall settings (**Configure > Profiles > Firewall**) to configure the Firewall settings that will enable your SNMP settings.

## Configure Wi-Fi Radio, DNS, Authentication, and Netflow Overrides

The **Overrides of Profile** settings for Wi-Fi Radio, DNS, Authentication, and Netflow settings can be specified by selecting the **Enable Edge Override** option for the appropriate block.

Details about each of these options can be found at [Chapter 11 Configure a Profile Device](#).

On the Edge **Device** tab, you can review any detected WAN connections after a device has been activated. The status of WAN interfaces for an Edge appear in the **Link Status** area of the **Overview** tab. Two status examples are shown in the figures below. The status will display as **Backup: Active** and/or **Backup: Standby**.

Links	Cloud Status	Interface (WAN Type)	Throug
AT&T U-verse Backup <b>Active</b> 108.65.77.184	<span style="color: green;">●</span>	INTERNET2 (Ethernet)	39.76 kI 48.22 kI
AT&T U-verse 108.214.98.136	<span style="color: red;">●</span>	INTERNET1 (Ethernet)	

Links	Cloud Status	Interface (WAN Type)	Throughput   Capacity
AT&T U-verse Backup Standby	<span style="color: gray;">●</span>	INTERNET2 (Ethernet)	0 ↑ 559.00 kbps 0 ↓ 3.54 Mbps
AT&T U-verse 108.214.98.136	<span style="color: green;">●</span>	INTERNET1 (Ethernet)	52.83 kbps ↑ 496.00 kbps 68.58 kbps ↓ 4.03 Mbps

## Configure Edge Business Policy

This section describes how to configure the Edge Business Policy.

### Configure Edge Business Policy

The Edge Firewall primarily uses rules from the assigned Profile. Overriding Profile Business Policy rules at the Edge is an optional step.

### Business Policy Override Rules

At the Edge, Business Policy Rules from the assigned Profile can be overridden using the Edge Business Policy dialog shown below. Any Business Policy override match value that is the same as any Profile Business Policy rule, will override that Profile rule. You can create override rules in the same way as you create Profile rules (see [Chapter 13 Configure Profile Business Policy](#)).

As shown in the image below, Business Policy is Segment aware. All Segments available for configuration are listed in the **Configure Segment** drop-down menu.

When you choose a Segment to configure from the **Configure Segment** drop down, the settings and options associated with that Segment display in the **Configure Segments** area. **Global Segment [Regular]** is the default Segment.

For more information about Segmentation, see [Chapter 8 Configure Segments](#) and *Configure Edge Device*.

The screenshot displays the 'Configure Segments' interface. At the top, there are tabs for 'Edge Overview', 'Device', 'Business Policy', and 'Firewall'. Below this, the 'Configure Segments' section is active, showing a 'Select Segment' dropdown set to 'Global Segment [Regular]'. A 'Business Policy' section contains a table of rules. The table has columns for 'Rule', 'Match' (Source, Destination, Application), and 'Action' (Network Service, Link, Priority, Priority). Rules 1-3 are highlighted in blue, indicating they are selected. Rules 4-23 are listed below, with their respective match and action configurations.

Rule	Source	Destination	Application	Network Service	Link	Priority	Priority
1 data_transfer	Any	Protocol: ICMP	Any	Multi-Path	auto	Normal	Transactional
2 Voip_control	Any	Any	sip (Business Collaboration)	Multi-Path	auto	High	Realtime
3 VOIP_traffic	Any	Any	Real Time Protocol (Business Collaboration)	Multi-Path	auto	High	Realtime
4 Box	Any	Any	Box.net (File Sharing)	Multi-Path	auto	High	Bulk
5 Speedtest	Any	Any	speedtest (File Sharing)	Multi-Path	auto	High	Bulk
6 Skype	Any	Any	Skype (Real Time Audio/Video)	Direct	auto	Low	Transactional
7 Business Application	Any	Any	All Business Application	Multi-Path	auto	High	Transactional
8 Remote Desktop	Any	Any	All Remote Desktop	Multi-Path	auto	High	Transactional
9 Business Collaboration	Any	Any	All Business Collaboration	Multi-Path	auto	High	Realtime
10 Email bulk/DATA	Any	Any	All Email	Multi-Path	auto	High	Bulk
11 Infrastructure	Any	Any	All Infrastructure	Multi-Path	auto	Normal	Transactional
12 Web	Any	Any	All Web	Multi-Path	auto	Normal	Transactional
13 Authentication	Any	Any	All Authentication	Multi-Path	auto	Normal	Transactional
14 Management	Any	Any	All Management	Multi-Path	auto	Normal	Transactional
15 Network Service	Any	Any	All Network Service	Multi-Path	auto	Normal	Transactional
16 Tunneling and VPN	Any	Any	All Tunneling and VPN	Multi-Path	auto	Normal	Transactional
17 Audio/Video	Any	Any	All Real Time Audio/Video	Multi-Path	auto	High	Realtime
18 File Sharing	Any	Any	All File Sharing	Multi-Path	auto	Normal	Bulk
19 Internet Instant Messaging	Any	Any	All Internet Instant Messaging	Direct	auto	Low	Transactional
20 Anonymizers And Proxies	Any	Any	All Anonymizers and Proxies	Direct	auto	Low	Transactional
21 Gaming	Any	Any	All Gaming	Direct	auto	Low	Transactional
22 Media	Any	Any	All Media	Direct	auto	Low	Transactional
23 Social Networking	Any	Any	All Social Networking	Direct	auto	Low	Transactional

\* Business policy rules applied from the assigned Profile of this Edge. Quick start test profile

SD-WAN Traffic Class and Weight Mapping Enable Edge Override

## Configure Edge Firewall

The Edge Firewall primarily uses rules from the assigned Profile. Overriding Profile Firewall rules at the Edge level is an optional step.

## Configure Edge Firewall

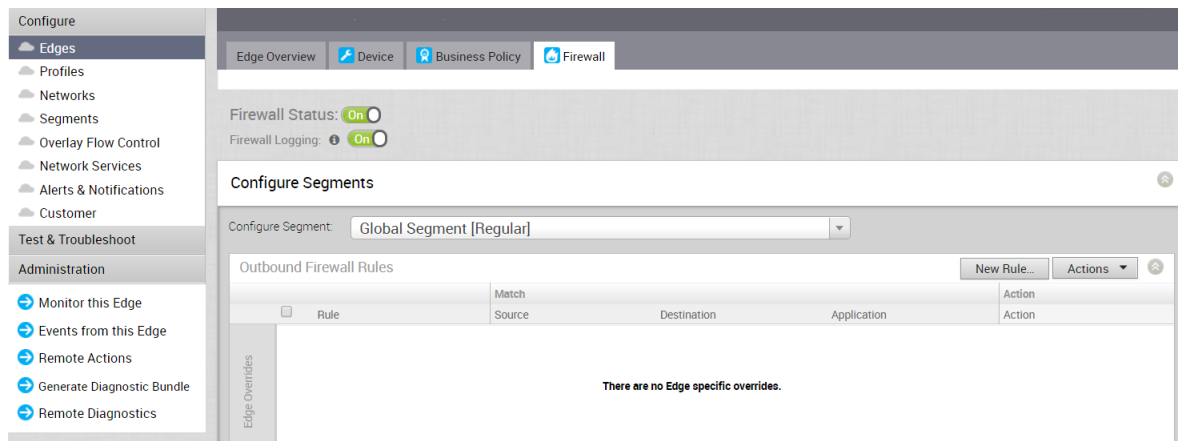
The Edge Firewall primarily uses rules from the assigned Profile. Overriding Profile Firewall rules at the Edge is an optional step.

### Outbound Firewall Rules

At the Edge, Firewall Rules from the assigned Profile can be overridden using the **Edge Firewall** dialog shown below. Any Firewall override match value that is the same as any Profile Firewall rule, will override that Profile rule. You can create override rules in the same way as you create Profile rules (see [Configure Profile Firewall](#)).

Firewall Profiles are Segment aware. All Segments available for configuration are listed in the **Configure Segment** drop-down menu. When you choose a Segment to configure from the **Configure Segments** drop-down menu, the settings and options associated with that Segment appear in the **Configure Segments** area. **Global Segment [Regular]** is the default Segment.

For more information about Segmentation, see [Chapter 8 Configure Segments](#) and *Configure Edge Device*.



### Inbound Firewall Rules

**Note** Inbound Firewall Rules are configured at the Edge Level and are Segment aware.

Inbound firewall rules gives Internet clients access to servers connected to an Edge LAN interface. Access can be made available through either Port Forwarding Rules or 1:1 NAT (Network Address Translation) rules.

### Port Forwarding Rules

Port forwarding rules enable you to configure rules to redirect traffic from a specific WAN port to a device (LAN IP/ LAN Port) within the local subnet. Optionally, you can also restrict the inbound traffic by an IP or a subnet. For the 3.3.2 release, the Inbound port forwarding rule can be configured with the Outside IP (which is on the same subnet of the WAN IP). See the example below.

## Example

If the WAN IP is 169.254.6.45, port forwarding rules can be as follows:

- If the source IP is 88.88.88.88 (from Internet), and it tries to reach 169.254.6.46 port 8888, it will port forward to 192.168.10.10 / port 80.
- If source IP is 99.99.99.99, and it tries to reach 169.254.6.46 port 8888 (same as above), it will port forward to 192.168.20.10 / port 80.

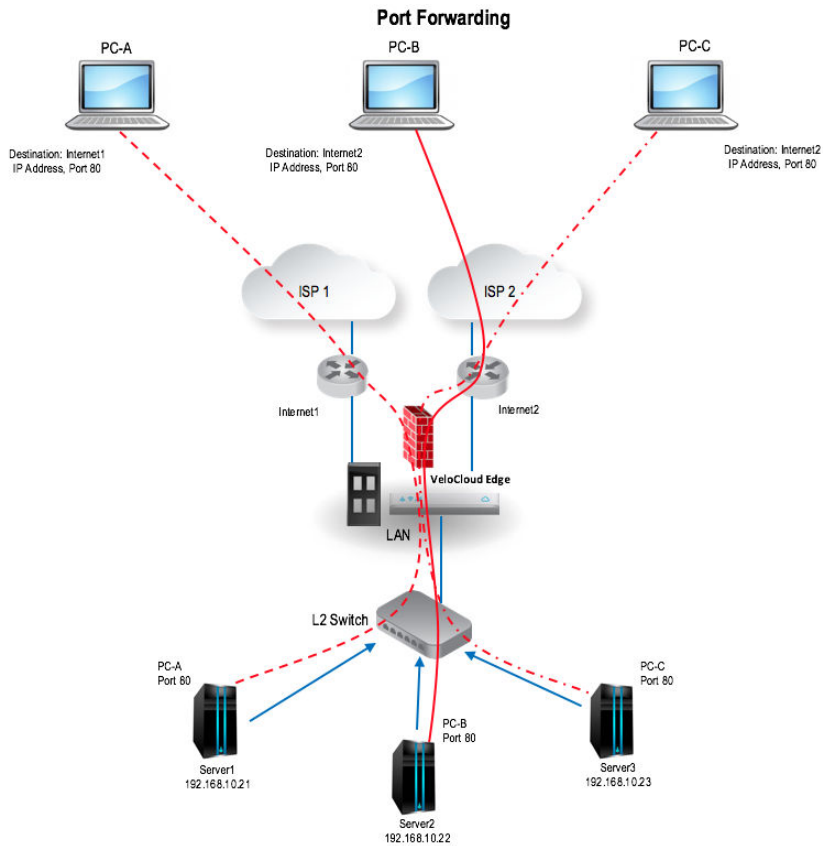
### Procedure:

- 1 Enter a name (optional) in the **Name** text field.
- 2 Enter the protocol to be forwarded, TCP or UDP.
- 3 Select the Interface for the Inbound traffic.
- 4 Enter the Outside IP address in the appropriate text box. For more information, see the 'Port Forwarding Rules' section above.
- 5 Enter the WAN port number. (To configure a range of ports, separate the first port and last port with a dash, e.g. "20-25").
- 6 Enter the LAN IP and the Port where the request will be forwarded.
- 7 From the **Segment** drop-down menu, select a segment the LAN IP will belong to.
- 8 In the appropriate text field, enter the Inbound Traffic (Remote IP Address/subnet) that will be allowed to be forwarded to an internal server. Leave the **Remote IP Address/subnet** text field blank to allow "any" traffic.

Name	Protocol	Interface	Outside IP	WAN Port(s)	LAN IP	LAN Port	Segment	Remote IP/Subnet
Server 1	TCP	GE1	10.0.2.5	80	192.168.10.21	80	Global Segment	0.0.0.0/0.0.0.0
Server 2	TCP	GE2	10.0.2.5	25	192.168.10.22	80	Global Segment	0.0.0.0/0.0.0.0

The following figure shows an illustration overview of the port forwarding configuration.





## 1:1 NAT Settings

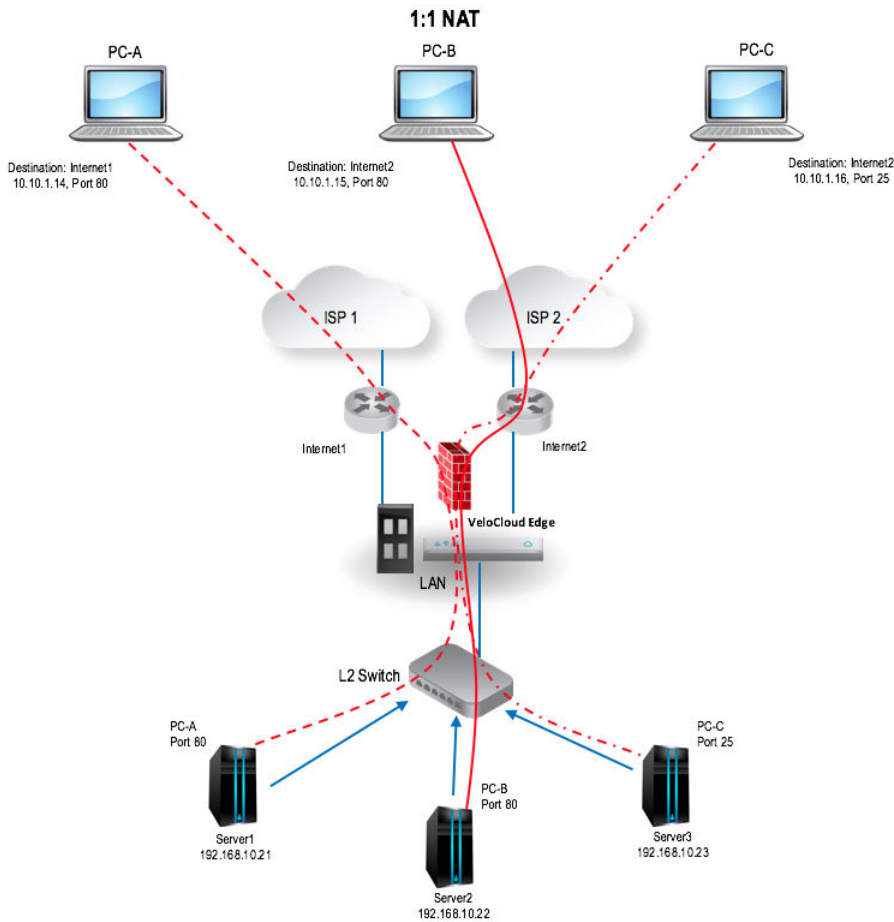
These are used to map an Outside IP address supported by the VeloCloud Edge to a server connected to an Edge LAN interface (for example, a web server or a mail server). It can also translate outside IP addresses in different subnets than the WAN interface address if the ISP routes traffic for the subnet towards the VeloCloud Edge. Each mapping is between one IP address outside the firewall for a specific WAN interface and one LAN IP address inside the firewall. Within each mapping, you can specify which ports will be forwarded to the inside IP address. The '+' icon on the right can be used to add additional 1:1 NAT settings.

### To configure the mapping:

- 1 Optionally, enter a name for the mapping.
- 2 Enter the Outside IP (LAN) address.
- 3 Select the WAN interface where the Outside IP address will be bound.
- 4 Enter the Inside (LAN) IP address.
- 5 From the **Segment** drop-down menu, select a segment the LAN IP will belong to.
- 6 Select if Outbound traffic should also be allowed to pass over the firewall connection by checking the **Outbound Traffic** checkbox.
- 7 Enter the Allowed Traffic Source (Protocol, Ports, Remote IP/Subnet) for the mapping.



The following figure shows an overview view of the 1:1 NAT configuration.



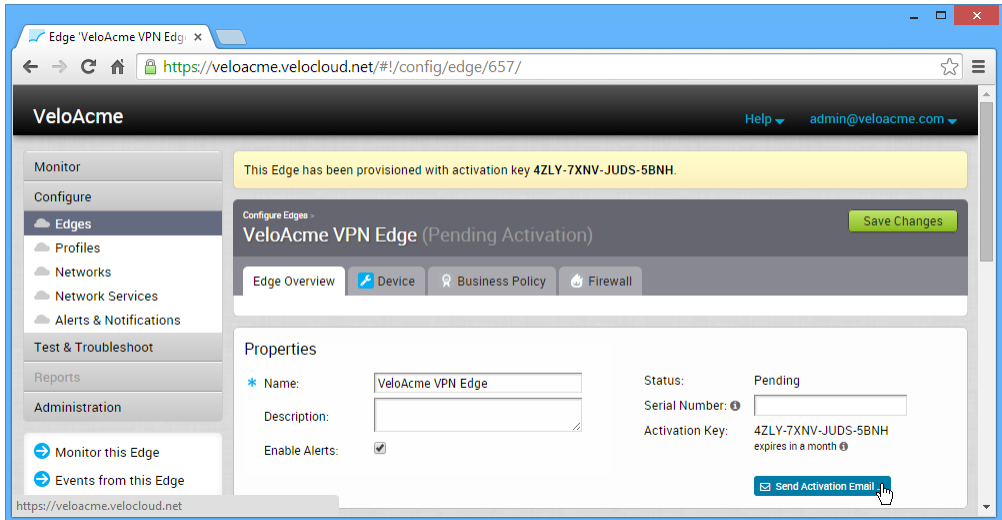
## Configure Edge Access Override

Overrides of Profile settings for Edge Access is an optional step. The override can be specified by selecting the **Enable Edge Override** option for the Edge Access block. Details about each of these options can be found at [Configure Profile Firewall](#).

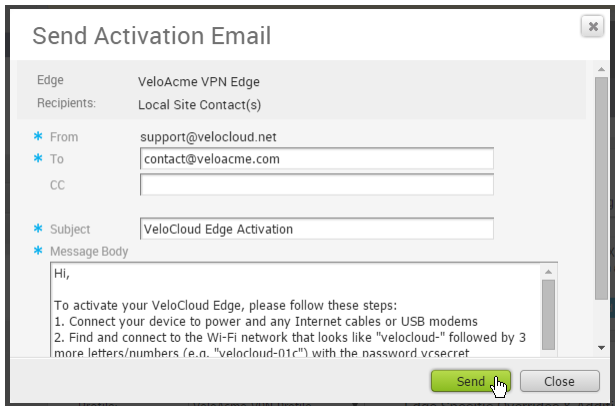
## Configure Edge Activation

This section describes how to initiate Edge activation.

Once an Edge configuration has been saved, it is assigned an activation key. Edge activation begins by clicking the **Send Activation Email** link on the **Edge Overview** Tab.



A **Send Activation Email** dialog box appears with a suggested email to be sent to a Site Contact. Simple instructions are provided for the Site Contact to connect and activate Edge hardware. Specify additional instructions in the email for connecting specific site WAN and LAN networks to the Edge.



## LAN-side NAT Rules at Edge Level

LAN-Side NAT Rules allow you to NAT IP addresses in an unadvertised subnet to IP addresses in an advertised subnet. For both the Profile and Edge levels, within the Device Settings configuration, LAN-side NAT Rules has been introduced for the 3.3.2 release.

### Before you begin:

Enable LAN-side NAT Rules (Go to **Configure Customer > Customer Capabilities** and check the **Enable LAN-side NAT Rules** checkbox.

### Note

- LAN-side NAT Rules can be configured at the Profile level or the Edge level. To configure at the Edge level, make sure the **Enable Edge Override** checkbox is checked.
- LAN-side NAT supports traffic over VCMP tunnel. It does not support underlay traffic.

**Use Case #1:**

In this scenario, a third-party has assigned multiple non-overlapping subnets to a customer's site. The server in the customer's data center recognizes traffic from this third-party by a single IP address at any given site.

**The VeloCloud configuration required for Use Case #1 is listed below:**

- VLAN1 = 192.168.1.0/24 - Do not advertise
- Static route 192.168.5.0/24 - Do not advertise
- Static route 192.168.7.0/24 - Do not advertise
- Static route 57.24.12.0/24 - Do not advertise
- Static route 172.16.24.0/24 - Advertise
- New rule: LAN-side NAT 192.168.1.0/24 -> 172.16.24.4/32

Because the NAT rule is a single IP, TCP and UDP traffic will be PAT'd. So in this example, 192.168.1.50 becomes 172.26.24.4 with an ephemeral source port for TCP/UDP traffic, ICMP traffic becomes 172.26.24.4 with a custom ICMP ID for reverse lookup, and all other traffic will be dropped.

**Use Case #2:**

In this scenario, the LAN subnet is 192.168.1.0/24. However, this is an overlapping subnet with other sites. A unique subnet of equal size, 172.16.24.0/24 has been assigned to use for VPN communication at this site. Traffic from the PC must be NAT'd on the Edge prior to doing the route lookup, otherwise the source route will match 192.168.1.0/24 which is not advertised from this Edge and traffic will drop.

**The VeloCloud configuration required for Use Case #2 is listed below:**

- VLAN1 = 192.168.1.0/24 - Do not advertise
- Static route 172.16.24.0/24 - Advertise
- New rule: LAN-side NAT 192.168.1.0/24 -> 172.16.24.0/24

Because the subnets match in size, all bits matching the subnet mask will be NAT'd. So in this example, 192.168.1.50 becomes 172.16.24.50.

**To apply LAN-Side NAT Rules:**

- 1 From the VCO navigational panel, go to **Configure > Edges**.
- 2 In the **Device Settings** tab screen, scroll down to the **LAN-Side NAT Rules** area.
- 3 In the **LAN-Side NAT Rules** area, complete the following: (See the table below and the Use Cases described above for more information about the fields in the **LAN-Side NAT Rules** area).
  - a Enter an address for the **Inside Address** textbox.
  - b Enter an address for the **Outside Address** textbox.

- c Choose either Source or Destination from the **Type** drop-down menu.
- d Type a description for the rule in the **Description** textbox (optional).

**LAN-Side NAT Rules** ⓘ

* Inside Address	* Outside Address	Type	Description
<input style="width: 100%;" type="text" value="10.0.0.0/24"/>	<input style="width: 100%;" type="text" value="192.168.0.0/24"/>	Source ▼	<input style="width: 100%;" type="text" value="Description (Optional)"/> <span style="float: right;">- +</span>

<b>LAN-side NAT Rules (Filed Name)</b>	<b>Type</b>	<b>Description</b>
Inside Address text box	IPv4 address/prefix, Prefix must be 1-32	The "inside" or "before NAT" IP address (if prefix is 32) or subnet (if prefix is less than 32).
Outside Address text box	IPv4 address/prefix, Prefix must be 1-32	The "outside" or "after NAT" IP address (if prefix is 32) or subnet (if prefix is less than 32).
Type drop-down menu	Select either Source or Destination.	Determine whether this NAT rule should be applied on the source or destination IP address of user traffic.
Description text box	Text	Custom text box to describe the NAT rule.

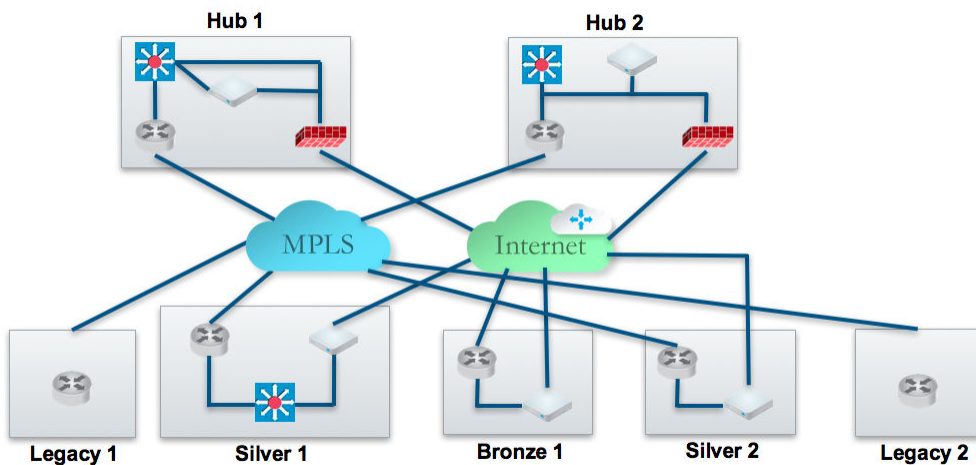
# Site Configurations

# 16

Topologies for data centers that include a VeloCloud hub and VeloCloud branch configurations ( Gold, Silver , and Bronze branches) are configured using both MPLS and Internet connections. Legacy branch configurations (those without a VeloCloud Edge) are included, and hub and branch configurations are modified given the presence of the legacy branches.

The diagram below shows an example topology that includes two data center hubs and the Gold, Silver , and Bronze variations of branch topologies interconnected using MPLS and the Internet. This example will be used to describe the individual tasks required for data center and branch configurations. It is assumed that you are familiar with concepts and configuration details in earlier sections of this documentation. This section will primarily focus on configuring Networks, Profile Device Settings, and Edge configuration required for each topology.

Additional configuration steps for traffic redirection, control routing (such as for backhaul traffic and VPNs), and for Edge failover are also included.



This section primarily focuses on the configuration required for a topology that includes different types of data center and branch locations, and explains the Network, Profile/Edge Device Settings, and Profile/Edge Business Policies required to complete the configurations. Some ancillary configuration steps that may be necessary for a complete configuration – such as for Network Services, Device Wi-Fi Radio, Authentication, SNMP, and Netflow settings – are not described.

This chapter includes the following topics:

- [Data Center Configurations](#)
- [Configure Branch and Hub](#)

## Data Center Configurations

A VeloCloud Edge in a data center can act as a hub to direct traffic to/from branches. The VeloCloud Edge can be used to manage both MPLS and Internet traffic. The hub in a data center can be configured in a one-arm or two-arm configuration. In addition, a data center can be used as a backup.

The following describes the various designs with different options of how VeloCloud Edge can be inserted into the topology.

Option	Description
Hub 1	Data Center or regional hub site with VeloCloud Edge deployed in two-arm topology.
Hub 2	Data Center or regional hub site with VeloCloud Edge deployed in one-arm topology (same interface carries multiple WAN links).
Legacy 1 and 2	Classic MPLS sites.
Silver 1	VeloCloud Edge is deployed off-path. VeloCloud Edge creates overlay across both MPLS and Internet paths. Traffic is first diverted to the VeloCloud Edge.
Silver 2	VeloCloud Edge is deployed in-path as the default gateway. It is always the default gateway. This topology is simpler but makes VeloCloud Edge a single point of failure and may require HA.
Bronze 1	Dual-Internet site (one of the links is behind a NAT router).

## Configure Branch and Hub

This section provides an overview of configuring VeloCloud Edge in a two-arm configuration.

### Overview

To configure the VeloCloud Edge in a two-arm configuration:

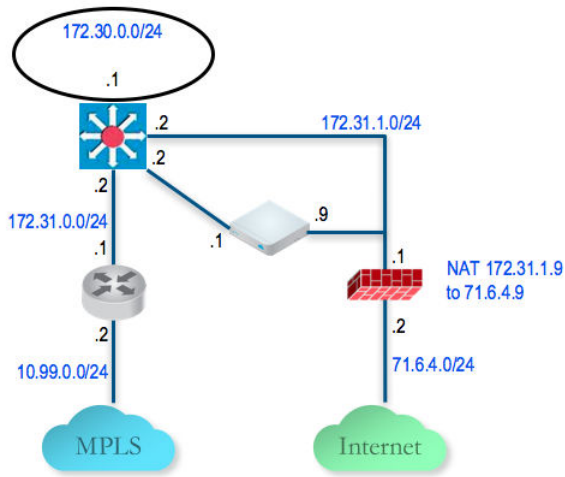
- 1 Configure and activate Hub 1
- 2 Configure and activate the Silver 1 site
- 3 Enable branch-to-hub tunnel (Silver 1 to Hub 1)
- 4 Configure and activate Bronze 1 site
- 5 Configure and activate Hub 2
- 6 Configure and activate Silver 2 site

The following sections describe the steps in more detail.

## Configure and Activate Hub 1

This step helps you understand the typical workflow of how to bring up VeloCloud Edge at the hub location. VeloCloud Edge is deployed with two interfaces (one interface for each WAN link).

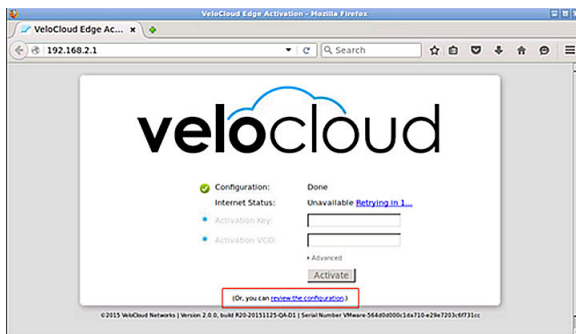
You will use the Virtual Edge as a hub. Below is an example of the wiring and IP address information.



## Configure and Activate Hub 1 VeloCloud Edge to Reach the Internet

Because this is the data center/hub site, it is unlikely that the VeloCloud Edge can get its WAN IP using DHCP. Thus, you will need to first enable the VeloCloud Edge to connect to the Internet through the data center firewall so that VeloCloud Edge can be activated.

- 1 Configure a PC with a static IP **192.168.2.100/24** and gateway **192.168.2.1** which is the default LAN setting for accessing a VeloCloud Edge. Connect the PC to the VeloCloud Edge LAN interface.
- 2 From the PC, browse to <http://192.168.2.1> (the local Web interface of the VeloCloud Edge). Click the link **review the configuration**.

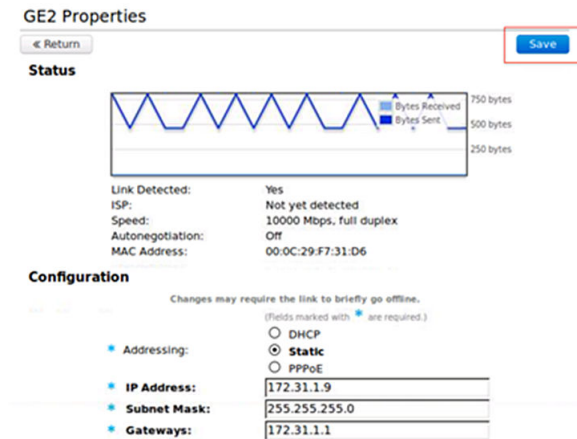


- 3 Configure the GE2 static WAN IP and default gateway of the VeloCloud Edge so that it can reach the Internet.

Click **Save** and provide login/password of **admin/admin**.



Typically at the data center/hub site, the static IP address will be assigned to you and the enterprise IT admin will configure the firewall to translate the VeloCloud Edge WAN IP to a Public IP and also filter the appropriate traffic (outbound: TCP/443, inbound: UDP/2426, UDP/500, UDP/4500).



- At this point, the Internet status should show Connected.

After configuration of the VeloCloud Edge static WAN IP address and associated firewall configuration is complete, the VeloCloud Edge Internet status shows "Connected".



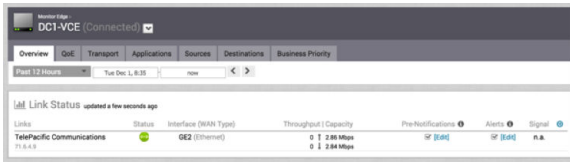
## Enable the Virtual VeloCloud Edge in Default Profile

- Login to the VeloCloud Orchestrator.
- The default VPN profile allows the activation of the VeloCloud Edge 500.

## Activate Hub 1 VeloCloud Edge

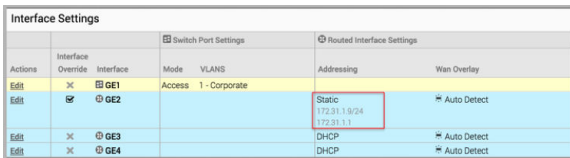
- Go to **Configure > Edges** and add a new VeloCloud Edge. Specify the correct model and the profile (we use the Quick Start VPN Profile).
- Go to the hub VeloCloud Edge (DC1-VCE) and follow the normal activation process. If you already have the email feature set up, an activation email will be sent to that email address. Otherwise, you can go to the device setting page to get the activation URL.
- Copy the activation URL and paste that to the browser on the PC connected to the VeloCloud Edge or just click on the activation URL from the PC browser.
- Click on **Activate** button.

- Now the **DC1-VCE** data center hub should be up. Go to **Monitor > Edges**. Click the **Edge Overview** tab. The public WAN link capacity is detected along with the correct public IP **71.6.4.9** and ISP.

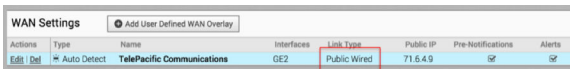


- Go to **Configure > Edges** and select **DC1-VCE**. Go to the **Device** tab and scroll down to the **Interface Settings**.

You will see that the registration process notifies the VeloCloud Orchestrator of the static WAN IP address and gateway that was configured through the local UI. The configuration on the VeloCloud will be updated accordingly.

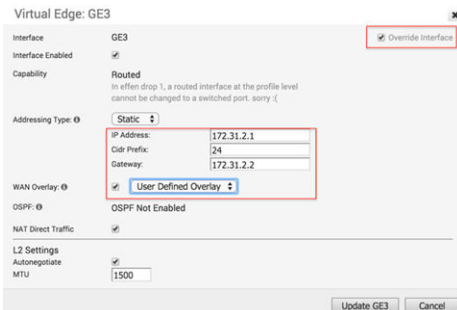


- Scroll down to the **WAN Settings** section. The Link Type should be automatically identified as **Public Wired**.



## Configure the Private WAN Link on Hub 1 VeloCloud Edge

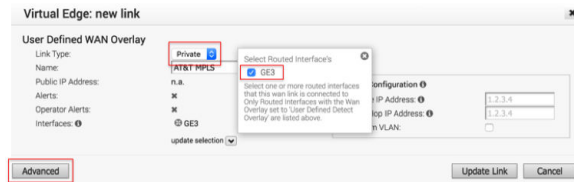
- Configure the private MPLS Edge WAN interface directly from the VeloCloud Orchestrator. Go to **Configure -> Edges** and choose **DC1-VCE**. Go to the **Device** tab and scroll down to the Interface Settings section. Configure static IP on GE3 as **172.31.2.1/24** and default gateway of **172.31.2.2**. Under **WAN Overlay**, select **User Defined Overlay**. This will allow us to define a WAN link manually in the next step.



- Under **WAN Settings**, click the **Add User Defined WAN Overlay** button (see the following screen capture).



- Define the WAN overlay for the MPLS path. Select the **Link Type** as **Private** and specify the next-hop IP (172.31.2.2) of the WAN link in the IP Address field. Choose the GE3 as the interface. Click the **Advanced** button.

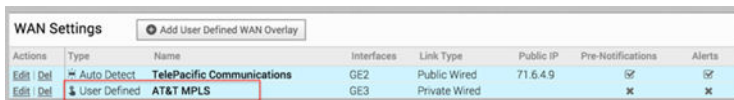


**Tip:** The hub site normally has more bandwidth than the branches. If we choose the bandwidth to be auto-discovered, the hub site will run a bandwidth test with its first peer, e.g. the first branch that comes up, and will end up discovering an incorrect WAN bandwidth. For the hub site, you should always define the WAN bandwidth manually, and that is done in the advanced settings.

- The private WAN bandwidth is specified in advanced settings. The screen shot below shows an example of 5 Mbps upstream and downstream bandwidth for a symmetric MPLS link at the hub.



- Validate that the WAN link is configured and save the changes.



You are done with configuring the VeloCloud Edge on the hub. You will not see the User Defined MPLS overlay that you just added until you enable a branch VeloCloud Edge.

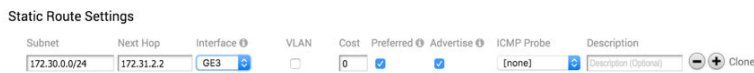
## (Optional) Configure the LAN Interface with Management IP

- Go to **Configure > Edges** and select **DC1-VCE**.
- Navigate to the **Device** tab and scroll down to the VLAN Settings section.
- Click **Edit** and configure the IP address of the interface.



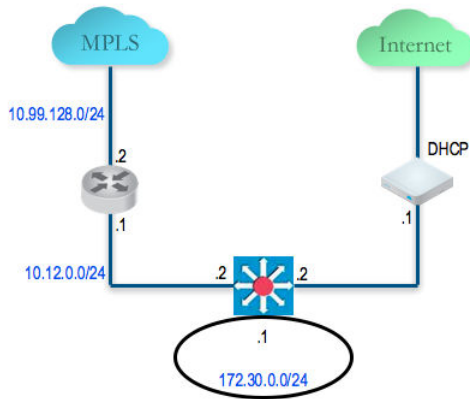
## Configure Static Route to LAN Network Behind L3 Switch

Add a static route to the **172.30.0.0/24** subnet through the L3 switch. You need to specify the interface GE3 to use for routing to the next hop. Make sure you enable the Advertise checkbox so other VCEs can learn about this subnet behind L3 switch (see the following screen capture).



## Configure and Activate Silver 1 Site

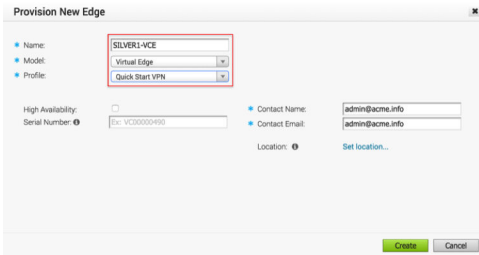
This step helps you understand the typical workflow of how to insert the VeloCloud Edge at a Silver site. The VeloCloud Edge is inserted off-path and relies on the L3 switch to redirect traffic to it. Below is an example of the wiring and IP address information.



## Activate the Silver 1 Site Branch VeloCloud Edge

In this example, we assume that the VeloCloud Edge gets its public IP address using DHCP, so there is no configuration required. VeloCloud Edge ships with default configuration to use DHCP on all routed interfaces.

- 1 Create a new Edge **SILVER1-DCE** and select the appropriate Model and configuration profile (see image below).

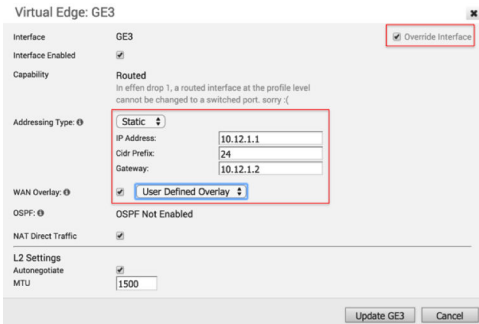


- 2 Activate this VeloCloud Edge by connecting a PC to its LAN or Wi-Fi.
- 3 The VeloCloud Edge should now be active in the VeloCloud Orchestrator with one public link. We can now configure the private WAN link.

## Configure the Private WAN Link on the Silver 1 Site VeloCloud Edge

At this point, we need to build the IP connectivity from the VeloCloud Edge towards the L3 switch.

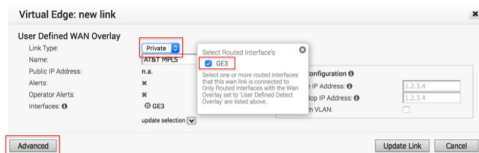
- 1 Go to **Configure > Edges**, select the **SILVER1-VCE** and go to the Device tab and scroll down to the Interface Settings section. Configure static IP on GE3 as **10.12.1.1/24** and default gateway of **10.12.1.2**. Under **WAN Overlay**, select **User Defined Overlay**. This will allow us to define a WAN link manually in the next step.



- 2 Under the **WAN Settings** section, click **Add User Defined WAN Overlay**.



- 3 Define the WAN overlay for the MPLS path. Select the **Link Type** as **Private**. Specify the next-hop IP (10.12.1.2) of the WAN link in the IP Address field. Choose the GE3 as the Interface. Click the **Advanced** button.



**Tip:** Since the hub has already been set up, it is OK to auto-discover the bandwidth. This branch will run a bandwidth test with the hub to discover its link bandwidth.

- 4 Set the Bandwidth Measurement to **Measure Bandwidth**. This will cause the branch VeloCloud Edge to run a bandwidth test with the hub VeloCloud Edge just like what happens when it connects to the VeloCloud Gateway.
- 5 Validate that the WAN link is configured and save the changes (see the following screen capture).



## (Optional) Configure the LAN Interface with Management IP

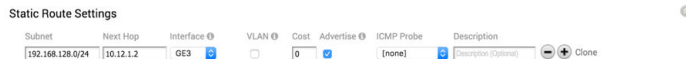
- 1 Go to **Configure > Edges**, select **SILVER1-VCE**. Navigate to the **Device** tab and scroll down to the VLAN Settings section. Click **Edit**. Configure the IP address of the LAN and Management



interfaces.

## Configure Static Route to LAN Network Behind L3 Switch

Add a static route to **192.168.128.0/24** through the L3 switch. You need to specify the Interface GE3. Make sure you enable the Advertise checkbox so other VCEs learn about this subnet behind L3 switch (see the following screen capture).



## Enable Branch to Hub Tunnel (Silver 1 to Hub 1)

This step helps you build the overlay tunnel from the branch into hub. Note that at this point, you may see that the link is up but this is the tunnel to the VeloCloud Gateway over the Internet path and not the tunnel to the hub. We will need to enable Cloud VPN to enable the tunnel from the branch to the hub to be established.

You are now ready to build the tunnel from the branch into the hub.

## Enable Cloud VPN and Edge to VeloCloud Hub tunnel

- 1 Step 1: Go to the **Configure > Profiles**, select **Quick Start VPN Profile** and go to the **Device** tab. Enable the Cloud VPN and do the following.
  - Under **Branch VeloCloud Hubs**, check the **Enable** checkbox.
  - Under **Branch to Branch VPN**, check the **Enable** checkbox.

- Under **Branch to Branch VPN**, uncheck the Use Cloud Gateways checkbox. Doing this will disable the data plane through the VeloCloud Gateway for Branch to Branch VPN. The Branch to Branch traffic will first go through one of the hubs (in the ordered list which you will specify next) while the direct Branch to Branch tunnel is being established.

Click the button **Select VeloCloud Hubs**. Next, move the **DC1-VCE** to the right. This will designate the **DC1-VCE** to be a VeloCloud Hubs. Click the **DC1-VCE** in the VeloCloud Hubs, and click both **Enable Backhaul Hubs** and **Enable B2B VPN Hubs** buttons. We will use the same **DC1-VCE** for both Branch to Branch traffic and to Backhaul Internet traffic to the hub. Under the Cloud VPN section, **DC1-VCE** now shows as both VeloCloud hubs and used for Branch to Branch VPN hubs.

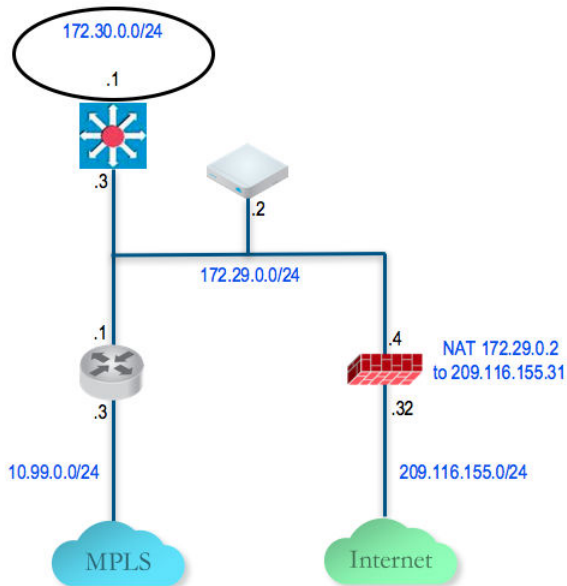
- At this point, the direct tunnel between the branch and the hub VCEs should come up. The debug command will now also show the direct tunnel between the branch and the hub. The below example is from the **SILVER1-VCE**. Note that the additional tunnels to **71.6.4.9** and **172.31.2.1**. These are the direct tunnels to the hub VeloCloud Edge (GE2 over public Internet and GE3 over private link).

## Configure and Activate Bronze 1 Site

This step helps create a Bronze site--a dual Internet site with one DIA and one broadband. Below is an example of the wiring and IP address information. The **BRONZE1-VCE** VeloCloud Edge LAN and activate the VeloCloud Edge. There is no configuration required on the WAN because it uses DHCP for both WAN interfaces.

## Configure and Activate Hub 2

This step helps you to configure the "Steer by IP address" commonly used in one-arm hub deployments. Below is an example of the wiring and IP address information. With one-arm deployment, the same tunnel source IP can be used to create overlay over different paths.



## Configure the Hub 2 VeloCloud Edge to Reach the Internet

- 1 Connect a PC to the VeloCloud Edge and use the browser to point to <http://192.168.2.1>.
- 2 Configure the hub VeloCloud Edge to reach the Internet by configuring the first WAN interface, GE2.

**Configuration**

Changes may require the link to briefly go offline.  
(Fields marked with \* are required.)

\* Addressing:  DHCP  Static  PPPoE

\* IP Address: 172.29.0.2

\* Subnet Mask: 255.255.255.0

\* Gateways: 172.29.0.4

\* Autonegotiation:  On  Off

## Add the Hub 2 VeloCloud Edge to the VeloCloud Orchestrator and Activate

In this step, you will create the second hub VeloCloud Edge, called **DC2.VCE**.

- 1 On the VeloCloud Orchestrator, go to **Configure > Edges**, select **New Edge** to add a new VeloCloud Edge.

**Provision New Edge**

\* Name: DC2-VCE

\* Model: Virtual Edge

\* Profile: Quick Start VPN

High Availability:

Serial Number: VC30000490

Contact Name: admin@acme.info

Contact Email: admin@acme.info

Location: Set location...

Buttons: Create, Cancel

- 2 Go to **Configure > Edges**, select the VeloCloud Edge that you just created, then go to the **Device** tab to configure the same Interface and IP you configured in previous step.

**Virtual Edge: GE2**

Interface: GE2  Override Interface

Interface Enabled:

Capability: Routed

Addressing Type: Static

IP Address: 172.29.0.2

CIDR Prefix: 24

Gateway: 172.29.0.4

WAN Overlay: User Defined Overlay

NAT Direct Traffic:

L2 Settings

Autonegotiate:

MTU: 1500

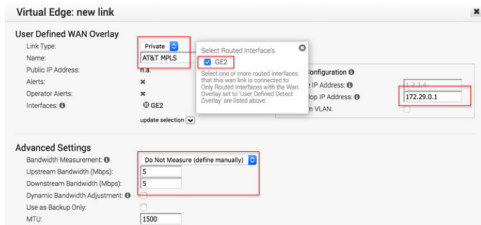
Buttons: Update GE2, Cancel

**Important** Since we are deploying the VeloCloud Edge in one-arm mode (same physical interface but there will be multiple over tunnels from this interface), it is important to specify the WAN Overlay to be User Defined.

- 3 At this point, you need to create the overlay. Under **WAN Settings**, click **Add User Defined WAN Overlay**.



- 4 Create an overlay across the public link. In our example, we will use the next-hop IP of **172.29.0.4** to reach the Internet through the firewall. The firewall is already configured to NAT the traffic to **209.116.155.31**.
- 5 Add the second overlay across the private network. In this example, we specify the next-hop router **172.29.0.1** and also specify the bandwidth since this is the MPLS leg and **DC2-VCE** is a hub.



Add a static route to the LAN side subnet, **172.30.128.0/24** through GE2 (see the following

screen capture).

Subnet	Next Hop	Interface	VLAN	Cost	Preferred	Advertise	ICMP Probe	Description
172.30.128.0/24	172.29.0.3	GE2		0				Predefined Default

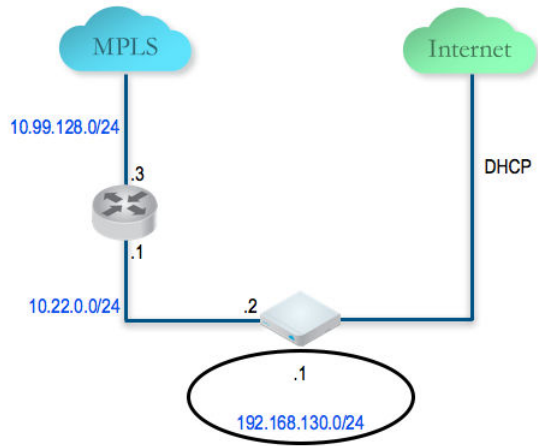
- 6 Activate the VeloCloud Edge. After the activation is successful, come back to the **Device** tab under the edge level configuration. Note the Public IP field is now populated. You should now see the links in the **Monitor > Edges**, under the **Overview** tab. **(Optional) Configure the LAN Interface with Management IP** Go to **Configure > Edges**, select **DC2-VCE**. Navigate to the **Device** tab and scroll down to the VLAN Settings section. Click **Edit**. Configure the IP address of the LAN and Management interfaces.

## Add the Hub 2 VeloCloud Edge to the Hub List in the Quick Start VPN Profile

- 1 Go to **Configure > Profiles** and select the profile **Quick Start VPN**.
- 2 Go to the **Device** tab and add this new VeloCloud Edge to a list of hubs.

## Configure and Activate Silver 2 Site

This step helps you create a Silver site--a hybrid site, which has the VeloCloud Edge behind CE router as well as VeloCloud Edge being the default router for the LAN. Below is an example of the wiring and IP address information for each hardware.



Connect a PC to the VeloCloud Edge LAN or Wi-Fi and use the browser to point to <http://192.168.2.1>.

# Configure Dynamic Routing with OSPF or BGP

# 17

This section describes how to configure dynamic routing with OSPF or BGP.

VeloCloud Edge learns routes from adjacent routers through OSPF and BGP. It sends the learned routes to the Gateway/Controller. The Gateway/Controller acts like a route reflector and sends the learned routes to other VeloCloud SD-WAN Edges. The Overlay Flow Control (OFC) enables enterprise-wide route visibility and control for ease of programming and for full and partial overlay.

VeloCloud supports Inbound/Outbound filters to OSPF neighbors, OE1/OE2 route types, MD5 authentication. Routes learned through OSPF will be automatically redistributed to the controller hosted in the cloud or on-premise. Support for BGP Inbound/Outbound filters and the filter can be set to Deny, or optionally you can Add/Change the BGP attribute to influence the path selection, i.e. RFC 1998 community, MED, and local preference.

---

**Note** For information about OSPF and BGP Redistribution, see the section titled [OSPF/BGP Redistribution](#).

---

**Note** In the 3.2 release, both BGP and OSPF can be enabled in a VeloCloud SD WAN Edge at a time.

---

This chapter includes the following topics:

- [Enable OSPF](#)
- [Enable BGP](#)
- [OSPF/BGP Redistribution](#)
- [Overlay Flow Control](#)

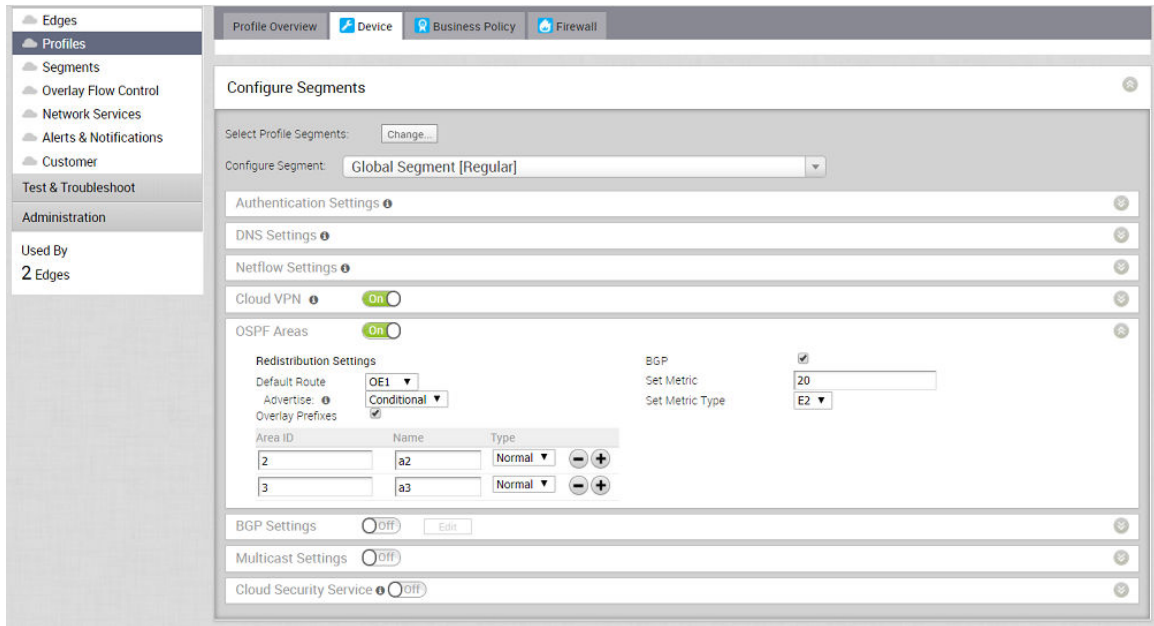
## Enable OSPF

Open Shortest Path First (OSPF) can be enabled only on a LAN interface as a passive interface. The Edge will only advertise the prefix associated with that LAN switch port. To get full OSPF functionality, you must use it in routed interfaces.


To enable OSPF, perform the steps on this procedure:

- 1 Configure OSPF for VPN profiles.
  - a Go to **Configure > Profile**.
  - b Click the **Device** icon corresponding to the VPN profile for which you want to configure OSPF.

The **Configure Segments** screen appears.



- c In the **OSPF Areas** section, turn **ON** the **OSPF Areas** toggle button.
- d Configure the redistribution settings for OSPF areas.
  - 1 From the **Default Route** drop-down menu, choose an OSPF route type (E1 or E2) to be used for default route.
  - 2 From the **Advertise** drop-down menu, choose either **Always** or **Conditional**. (Choosing Always means to Advertise the default route always. Choosing Conditional means to redistribute default route only when Edge learns via overlay or underlay). The “Overlay Prefixes” option must be checked to use the Conditional default route.
  - 3 If applicable, check the **Overlay Prefixes** checkbox.
  - 4 Optionally, to enable injection of BGP routes into OSPF, select the **BGP** checkbox. BGP routes can be redistributed into OSPF, so if this is applicable, enter or choose the configuration options as follows:
    - a In the **Set Metric** textbox, enter the metric. (This is the metric that OSPF would put in its external LSAs that it generates from the redistributed routes). The default metric is 20.

- b From the **Set Metric Type** drop-down menu, choose a metric type. (This is either type E1 or E2 (OSPF External-LSA type)); the default type is E2).
  - 5 In the **ID** text box, enter an **OSPF Area ID**.
  - 6 In the **Name** textbox, enter a descriptive name for your area.
  - 7 By default, the **Normal** type is selected. Only **Normal** type is supported at this time.
  - 8 Add additional areas, if necessary, by clicking .
- 2 Configure routed interface settings for the OSPF-enabled Edge device.

---

**Note** For the 3.3.1 release, the VeloCloud Orchestrator (VCO) supports OSPF **Point to Point** network mode at the Edge and Profile level.

---

- a In the **Configure Segments** screen, scroll down to the **Device Settings** area of the Edge device for which you want to configure interface and OSPF settings.
- b Click the expand icon corresponding to the Edge.
- c In the **Interface Settings** area, click the **Edit** link of your interface. The Interface Setting screen for the Edge device appears.

**Edge VMware** ? x

**Interface: GE6** Override Interface

Interface Enabled:

Capability: Routed

Segments: All Segments

Addressing Type: Static

IP Address:

CIDR prefix:

Gateway:

WAN Overlay:  User Defined Overlay

OSPF:

OSPF Area: 1 - a1

[toggle advance ospf settings](#)

**Custom Settings**    Inbound Route Learning    Route Advertisement

Hello Timer:  seconds

Dead Timer:  seconds

Enable MD5 Authentication:

Interface Path Cost:

MTU:

Mode: Broadcast

Passive:

Multicast: Multicast is not enabled for the selected segment

RADIUS Authentication:  Require User Authentication to access WAN

x WAN Overlay must be disabled to configure RADIUS Authentication.

Advertise:

ICMP Echo Response:

NAT Direct Traffic:

Underlay Accounting:

Trusted Source:

Reverse Path Filter: Specific

- d Select the **OSPF** checkbox.
- e From the **OSPF Area** drop-down menu, select an OSPF area.
- f Click the **toggle advance ospf settings** link to configure advanced OSPF settings.
  - 1 Create filters for **Inbound Route Learning** and **Route Advertisement**. For more information, see [Route Filters](#).
  - 2 Click the **Customs Settings** tab and configure the following OSPF settings.
    - a In the **Hello Timer** text box, enter the OSPF Hello time interval in seconds. The allowable range is 1 through 255.
    - b In the **Dead Timer** text box, enter the OSPF Dead time interval in seconds. The allowable range is 1 through 65535.
    - c Select the **Enable MD5 Authentication** checkbox to enable MD5 authentication.
    - d In the **Interface Path Cost** text box, enter the OSPF cost for the interface path.

- e In the **MTU** text box, enter the Maximum Transmission Unit (MTU) value of the interface.
  - f From the **Mode** drop-down menu, select **Broadcast** or **Point to Point** as the OSPF network type mode. The default OSPF mode is **Broadcast**.
  - g Select the **Passive** checkbox to enable OSPF Passive mode.
  - h Click the **Update** button.
- 3 Click **Save Changes**.

The **Confirm Changes** dialog box appears requesting you to confirm the OSPF areas you want to enable. It also displays how many Edges are affected.

---

**Note** If you have Edges that are not associated with the OSPF configuration at the Profile level, then you must configure at the Edge level from **Configure > Edges > Device > Interface Settings area**.

---

## Route Filters

There are two different types of routing: inbound and outbound.

- Inbound routing includes preferences that can be learned or ignored from OSPF and installed into the Overlay Flow Control.
- Outbound Routing indicates what prefixes can be redistributed into the OSPF.

**Edge 500: INTERNET2**

Interface: INTERNET2

Interface Enabled:

Capability: Routed

Addressing Type: DHCP

Static/PPPoE addressing details must be configured individually per edge.

WAN Overlay:  User Defined Overlay

OSPF:

OSPF Area: 1 - BRANCHES

[toggle advance ospf settings](#)

Custom Settings    Inbound Route Learning    **Route Advertisement**

Default Action: Advertise

Route	Action
172.17.1.0/25	Ignore

NAT Direct Traffic:

VLAN:

**L2 Settings**

Autonegotiate:

\* MTU: 1500

Update INTERNET2    Cancel

## Enable BGP

The Routing BGP feature is available only if it is enabled by your Operator. To gain access to this feature, see your Operator for more information.

- BGP must be enabled by an Operator (Go to **Configure > Customer** and check the Enable BGP checkbox in the Customer Configuration screen).

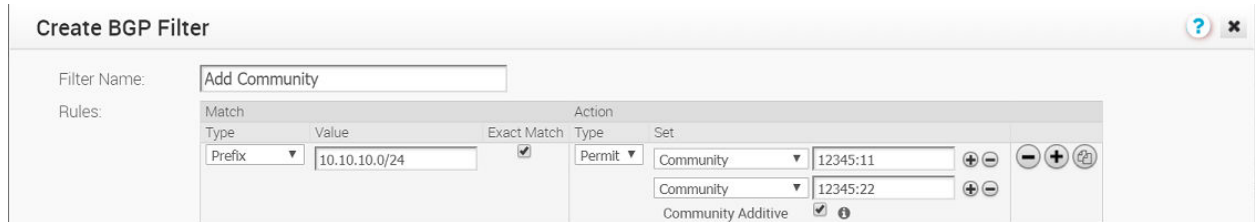
### Note

- 4-Byte ASN BGP is supported (As the ASN of the VCE itself), Peer to a neighbor with 4-Byte ASN- Accept 4-Byte ASNs in route advertisements. Only plain format is supported; asdot/decimal format is not.
- BGP can be configured per segment. You can configure either at the Profile level or the Edge level with the Edge Override enabled.

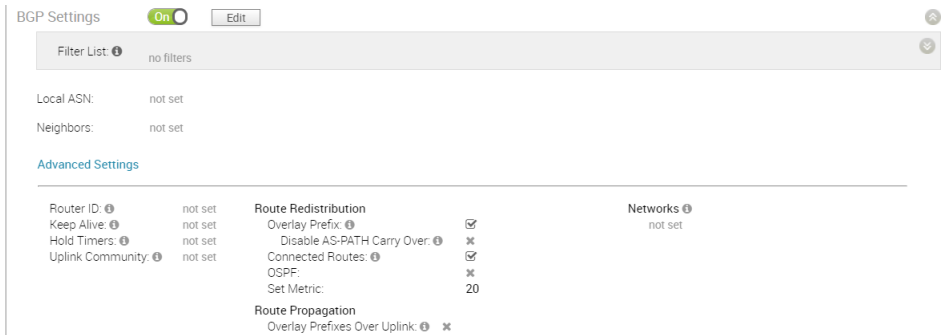
### Community Additive Support



BGP inbound and outbound configuration supports setting BGP communities. Community values can be used to identify the source of the routes. By default, if "additive" is not checked, the existing BGP community will be replaced by the "set" value(s). If the community additive option is checked, we will append the set community values to the existing BGP community. As shown in the example image below, community 12345:11 and 12345:22 will be appended to the existing BGP community. NOTE: The maximum number of community strings supported is twelve.

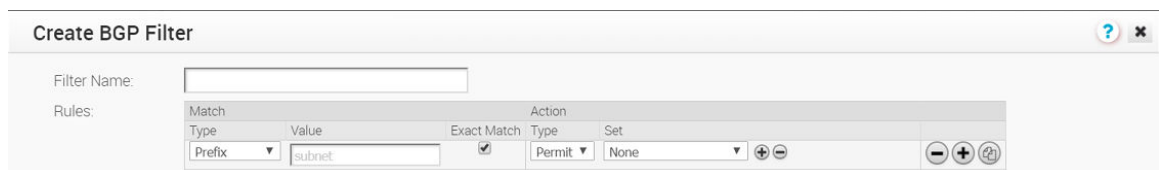


- 1 Configure BGP for VPN profiles:
  - a Go to **Configure > Profile** from the navigation panel.  
The **Configuration Profiles** screen appears.
  - b Select a profile you want to enable BGP for and click the **Device** icon for the applicable Profile.  
The **Device Settings** screen for the selected Profile appears.
- 2 Scroll down to the **BGP Settings** area, and turn **BGP ON** as shown in the image below.



- 3 Click the **Edit** button to define the BGP neighbors.
- 4 In the **BGP Editor**:
  - a Click the **Add Filter** button to create one or more filters. (These filters will be applied to the neighbor to deny or change the attributes of the route. The same filter can be used for multiple neighbors).

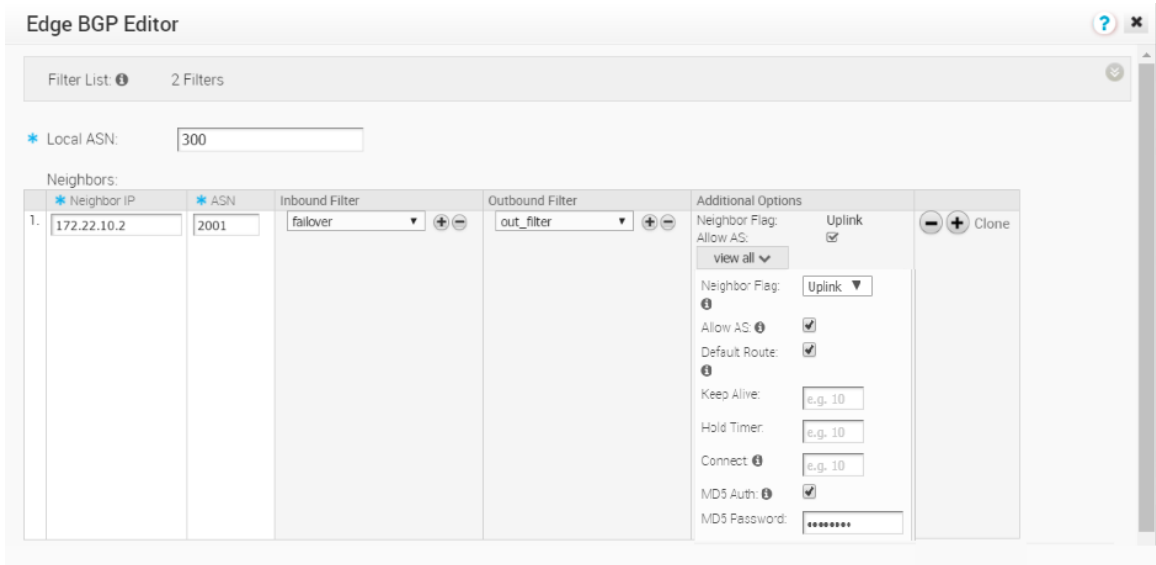
The **Create BGP Filter** dialog appears (image below).



- b In the **Create BGP Filter** dialog:
- 1 Type in a name for the filter in the **Filter Name** textbox.
  - 2 Set the Rules for the filter.
    - Choose Prefix or Community from the **Type** drop-down menu.
    - Set the value for either the Prefix or Community in the **Value** textbox.
    - If applicable, check the **Exact Match** checkbox.
    - Indicate the action type (Permit or Deny) from the **Type** drop-down menu.
    - From the **Set** drop-down menu, choose either None, Local Preference, Metric, AS-Path-Prepend, or Community, Community Additive checkbox. See the section above titled, [Community Additive Support](#)" for more information.
- c After you have set the rules for the filter, click the **OK** button.
- d In the **BGP Editor** dialog box, enter the Local ASN number in the **Local ASN** textbox.
- e In the Neighbor's area, enter the **Neighbor IP** and **ASN** in the appropriate text boxes, and specify Inbound Filters or Outbound Filters from the **Filter** list defined in the previous step.
- f Add additional options by clicking the **view all** button to open the drop-down menu. Apply additional options as needed. (See the table below for a description of each option and the table below for additional reference).

Additional Options Field	Description
Neighbor Flag drop-down menu	Used to flag the neighbor type. Choose between two options from the drop-down menu: None and Uplink. Select Uplink if it is used as the WAN overlay towards MPLS. It will be used as the flag to decide whether the site will become a transit site (e.g. hub) by propagating routes learnt over SD-WAN overlay to WAN link toward MPLS. If need to make it a transit site, also check "Overlay Prefix Over Uplink" in Advanced option.
Allow AS checkbox	Learn BGP routes even though the same AS is in the AS-path.
Default Route checkbox	Advertise a default route to the neighbor. See step "e, ii" below for more information about using the <b>Default Route</b> checkbox.
Connect	Interval in seconds before it tries new TCP connection with the peer if it detects the TCP session is not passive. Default value is 120 seconds.

Additional Options Field	Description
MD5 Auth checkbox	Enables BGP MD5 authentication. The MD5 Auth checkbox is used in a legacy network or federal network, and it is common that BGP MD5 is used as a security guard for BGP peering.
MD5 Password textbox	A password is required when enabling MD5 Auth.



g Click the **Advanced Settings** button.

The **Advanced Settings** area appears.

h In the **Additional Settings** area, you can enter the following additional BGP settings described in the table below. (See the image below for additional reference).

Additional Settings Fields	Description
Router ID	If no ID is configured, an ID will be automatically assigned.
Keep Alive	The frequency (in seconds) that the "Keep Alive" message will be sent to its peer. The default value is 60 seconds. The range is 0-65535.
Hold Timers	Interval in seconds that the peer is considered after not receiving the Keep Alive message. The default value is 180 seconds. The range is 0-65535.
Uplink Community	Uplink refers to link connected to the Provider Edge (PE). Inbound routes (towards the edge) matching this community will be treated as Uplink routes. (For which the Hub/Edge is not considered the owner). Input can be in the original number format or in the new AA:NN format.
Overlay Prefix	Redistributes prefixes learned from the overlay.
Disable AS-PATH Carry Over	By default, this should be left unchecked. In certain topologies, disabling AS-PATH Carry Over will influence the outbound AS-PATH to make the L3 routers prefer a path towards an Edge or a Hub. <b>Warning: When the AS-PATH Carry Over is checked, tune your network to avoid routing loops.</b>

Connected Routes	Redistributes all the connected Interface subnets.
OSPF checkbox	Enables OSPF redistribute into BGP.
Default Route	Redistributes default route only when Edge learns via overlay or underlay.
Set Metric textbox	Optionally, you can enable OSPF, which allows an injection of OSPF routes into BGP. The default BGP metric for the redistributed OSPF routes is MED value of 20.
Overlay Prefixes Over Uplink	Uplink refers to link/neighbor which is configured with the <b>Neighbor</b> flag Uplink (Normally, the link is connected to the Provider Edge(PE) router). Propagates routes learned from Overlay to the Uplink with the <b>Neighbor</b> flag.
Networks	The Network the BGP will advertise in the format 10.10.10.10/21.

### Advanced Settings

Router ID: ⓘ	<input type="text"/>
Keep Alive: ⓘ	<input type="text" value="e.g. 60"/>
Hold Timers: ⓘ	<input type="text" value="e.g. 180"/>
Uplink Community: ⓘ	<input type="text" value="00:00"/>

### Route Redistribution

Overlay Prefix: ⓘ

Disable AS-PATH Carry Over: ⓘ

Connected Routes: ⓘ

OSPF:

Set Metric:

Default Route: ⓘ

Advertise:

### Route Propagation

Overlay Prefixes Over Uplink: ⓘ

### Networks ⓘ

Clone

- i Click **OK** to save the configurations.

---

**Note** If you checked the **Default Route** checkbox located in the **Additional Settings** area, please be aware of the following four scenarios:

- If the global **Default Route** option is enabled with the "Conditional" option selected, and the per BGP neighbor option **Default Route** is not selected, BGP will Redistribute the default route to its neighbor only when the Edge learns an explicit default route via overlay or underlay.
  - If the global **Default Route** option is enabled with the "Conditional" option selected, and the per BGP neighbor option **Default Route** is selected, the Per Neighbor configuration overrides the Global configuration hence "Advertise default route to BGP peer Always."
  - If the global **Default Route** option is not enabled and the per BGP neighbor option **Default Route** is selected, Advertise default route to BGP peer Always.
  - If the global **Default Route** option is not enabled and per the BGP neighbor option **Default Route** is not selected, Do not Advertise/Redistribute default route to BGP peer.
- 

**Note** All the above options are available at the Edge level and can be configured with Edge override enabled for BGP settings.

---

## OSPF/BGP Redistribution

Each of routing protocols OSPF and BGP may be enabled independently and the prior model of allowing only one routing protocol to be enabled on the system has been removed with this release. This release also allows the possibility of redistributing OSPF into BGP or BGP into OSPF (or both simultaneously), along with other possible route sources like prefixes learnt over the overlay, connected routes, static routes, etc.

In addition, with release 3.2, we are standardizing the redistribution behavior along more traditional lines (similar to that in other routing vendors). For example, if there is more than one route available for the same prefix, then only the best route for that prefix in the system RIB will be redistributed to the destination protocol if the configuration in the destination protocol allows redistribution for that route type.

Consider, as an example, redistribution of the prefix 192.168.1.0/24 into BGP. Let's say routes to the prefix 192.168.1.0/24 are locally available, learned from OSPF and separately learned as an Overlay prefix. Let's further assume that between the OFC flow ordering for the prefix, and route metrics, and route preference the OSPF route ranks above (is better than) the learned overlay route for that same prefix. Then, the OSPF route will be redistributed into BGP if OSPF redistribution has been turned on in BGP. Note that since the overlay learned prefix is not the best route for that prefix in the system RIB, it will not be redistributed into BGP even if the redistribution of overlay prefixes has been turned on in BGP.

In cases like the above, in order to facilitate the redistribution of the best route for a prefix into a given destination protocol, the user can enable redistribution for the specific route type that is the best route in the system.

Alternately, if the user prefers a different route source for that prefix to be redistributed into the destination protocol, the user can control the relative precedence of the route in the system RIB using the Overlay Flow Control facility provided by the management interface, or by varying the route metric.

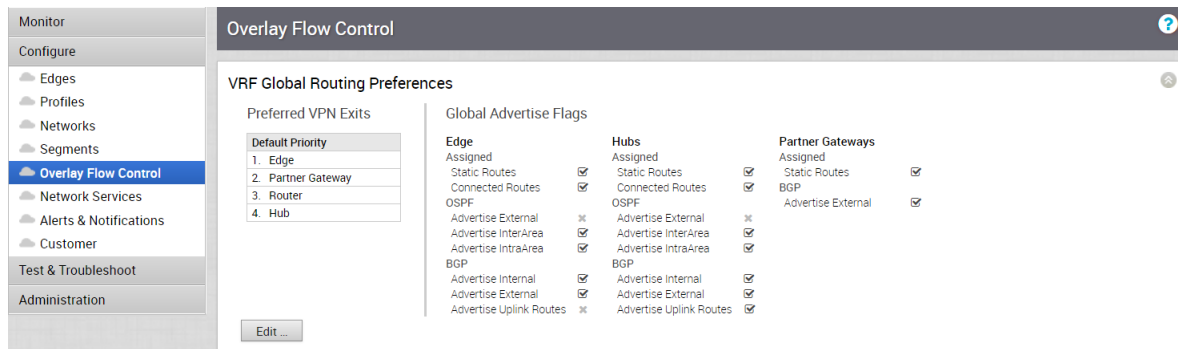
See [Enable OSPF](#) and [Enable BGP](#) for more information.

## Overlay Flow Control

The **Overlay Flow Control** screen displays a summary view of all the routes in your network.

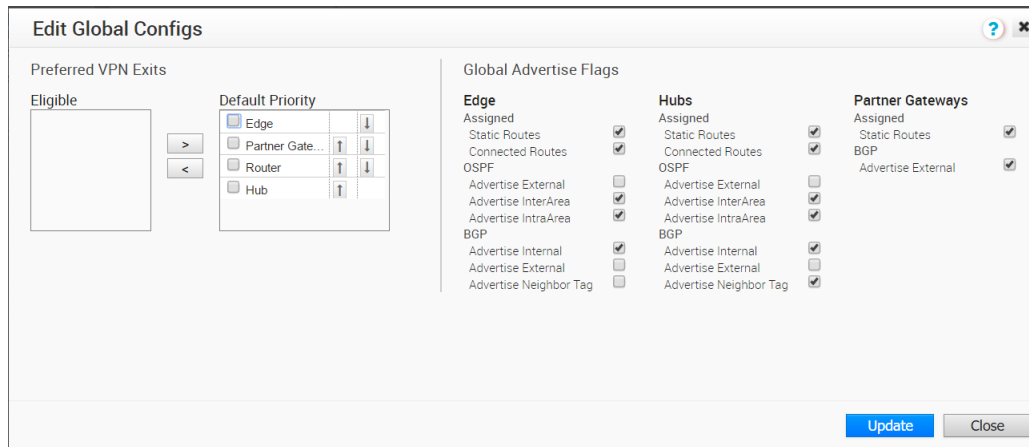
### Global Routing Preferences

This section describes global routing preferences.



### Data Forwarding Preferences

The **Data Forwarding Preferences** area is where you decide the priority of the destinations where the traffic should be routed. To change the priority, click the **Edit** button (see image above) located at the bottom of the **Global Routing Preferences** area to open up the **Edit Global Configs** dialog.



- Advertise Internal refers to IBGP routes.
- Advertise External refers to EBGP routes.
- Advertise Uplink Routes refers routes with Uplink tag (U).

## Overlay Flow Control Table

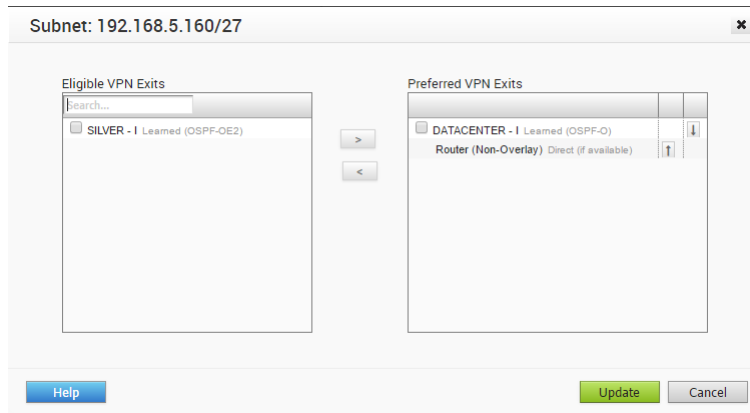
All routes are displayed in the **Overlay Flow Control** table, which includes the following: segment , subnet, route type, and preferences.

Modify	Segment	Subnet	Preferred VPN Exits	Route Type	Last Update	Actions
<a href="#">Edit</a>	Global Segment	192.168.30.0/30	CS-VCG-02-DU adjacencies ... CS-VCG-01-LO adjacencies ...	Learned (E-BGP) metrics ... Learned (E-BGP) metrics ...	Mon Jul 10, 10:08:55 Mon Jul 10, 10:08:58	Tue. ^ Mon
<a href="#">Edit</a>	Global Segment	8.8.8.8/32	CS-VCG-01-LO adjacencies ... CS-VCG-02-DU adjacencies ... CS-VCG-03-SG adjacencies ...	Learned (E-BGP) metrics ... Learned (E-BGP) metrics ... Learned (E-BGP) metrics ...	Mon Jul 10, 10:08:49 Mon Jul 10, 10:08:51 Mon Jul 10, 10:08:55	Tue. Tue. Tue.
<a href="#">Edit</a>	Global Segment	10.3.64.0/24	CS-VCG-01-LO adjacencies ... CS-VCG-02-DU adjacencies ... CS-VCG-03-SG adjacencies ...	Learned (E-BGP) metrics ... Learned (E-BGP) metrics ... Learned (E-BGP) metrics ...	Mon Jul 10, 10:08:49 Mon Jul 10, 10:08:51 Mon Jul 10, 10:08:55	Tue. Tue. Tue.
<a href="#">Edit</a>	Global Segment	10.32.0.0/24	CS-VCG-01-LO adjacencies ...	Learned (E-BGP) metrics ...	Mon Jul 10, 10:08:49	Tue. v

Column Name	Description
Subnet	The network that this route corresponds to along with a list of Edges that learned this route.
Route Type	Connected: A network that is directly connected to the interface. Types include: OSPF-O, OSPF-OE2, BGP, Static, and Connected.
Preferences	VeloCloud (B2B)- VeloCloud Route Direct: Direct interface route if a Private link is present.

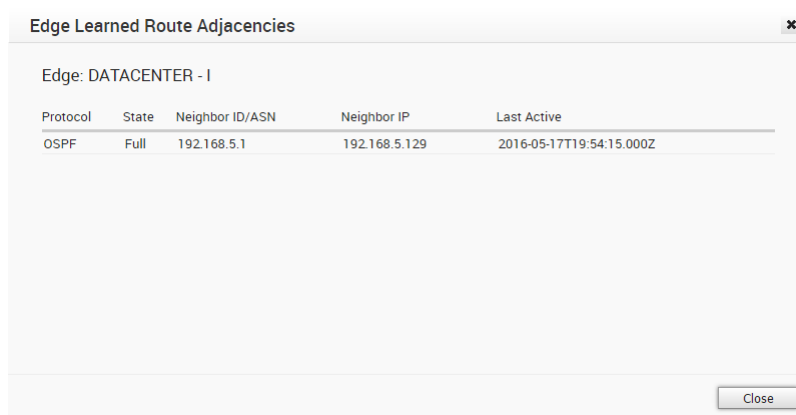
## Edit Routes

You can also change the destination of your preferences. Click the **Edit** button from the **Overlay Flow Control** table. If you change the destination preference, the change applies only to that specific route/subnet.



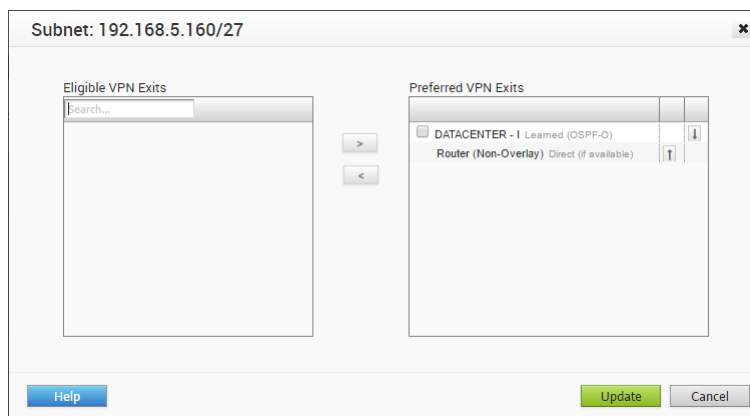
## Adjacencies

Adjacencies display routes between OSPF, BGP neighbors, and the Edge as shown in the following figure. Click the **Adjacencies** link to view these neighboring relationships.



## Re-prioritize Routes

You can re-prioritize routes by clicking the **Edit** button from **Overlay Flow Control** area. These are the final exit points to reach the destination subnet.





# Configure Alerts

# 18

The VeloCloud Orchestrator provides an alert function to notify one or more Enterprise Administrators (or other support users) when a problem occurs.

---

**Note** If you are logged in using a user ID that has Customer Support privileges, you can view VeloCloud Orchestrator objects but not create new objects or configure/update existing ones.

---

Alerts can be sent when a VeloCloud Edge goes offline or comes back online, a WAN link goes down, a VPN tunnel goes down, or when an Edge HA failover occurs. A delay for sending the alert after it is detected can be entered for each of the alert types.

The following screen capture shows the **Configure Alerts** page where the alerts of interest are selected, the **Notification Delay** for each alert type is entered, and the email addresses where the alerts will be sent are configured. You can also select if SMS alerts are sent to a mobile phone number.

This chapter includes the following topics:

- [Configure SNMP Traps](#)

## Configure SNMP Traps

SNMP (Simple Network Management Protocol) Traps are notifications that can be sent to an SNMP Agent to indicate that an event has occurred.

The VCO can send SNMP Traps corresponding to existing alerts (e.g. 'Edge Down' and 'Edge Up') and 'SMS' and 'Email' alerts.

**Alert Configuration** Save Changes ?

Select Alerts

<input type="checkbox"/>	Alert Type	Notification Delay
<input type="checkbox"/>	Edge Down ⓘ	3 minutes
<input type="checkbox"/>	Edge Up ⓘ	1 minutes
<input type="checkbox"/>	Link Down ⓘ	3 minutes
<input type="checkbox"/>	Link Up ⓘ	1 minutes
<input type="checkbox"/>	VPN Tunnel Down ⓘ	3 minutes
<input type="checkbox"/>	Edge HA Failover ⓘ	1 minutes

Customers

Admin	User Role	✕	Email ⓘ	✕	SMS ⓘ
	Superuser	<input type="checkbox"/>		✕	<not set> <span>Test</span>

Email Addresses

Add a comma separated list of emails

Phone Numbers

Name	Phone
<input type="text" value="Name"/>	<input type="text" value="Phone"/> <span>[-] [+]</span>

SNMP Traps

<input type="checkbox"/>	Version	Hostname / IP Address	Port	Version Specific Attributes
<input type="checkbox"/>	v2c ▾	<input type="text" value="Hostname / IP Address"/>	<input type="text" value="162"/>	Community: <input type="text" value="public"/> <span>Test</span> <span>[-] [+]</span>

Click **Save Changes** after you have chosen the Alert Configuration you want.

This section describes Administration.

This chapter includes the following topics:

- [Configure System Settings](#)
- [Monitor Edge Licensing](#)

## Configure System Settings

This section describes system settings.

### 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 Enterprise User

To setup Single Sign On (SSO) authentication for Enterprise user, perform the steps in this procedure.

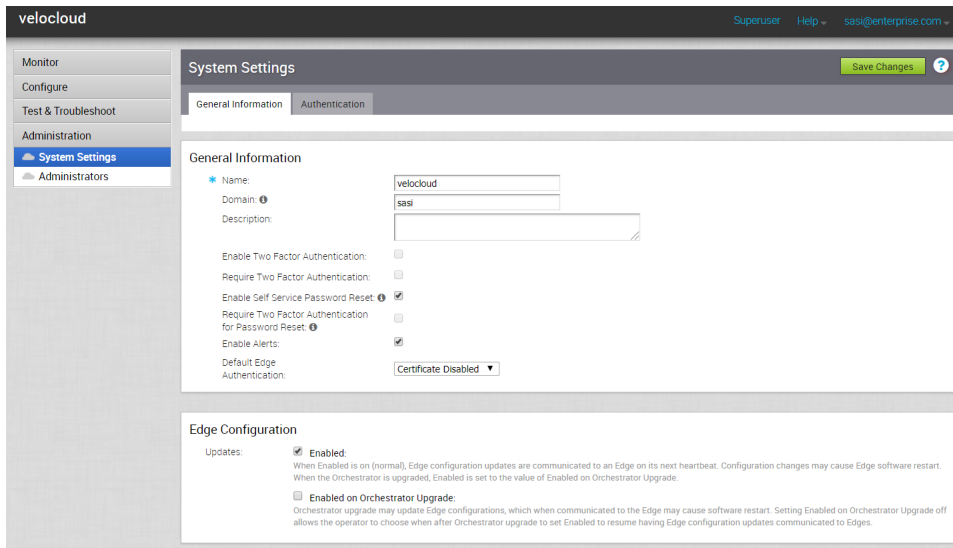
#### Prerequisites

- Ensure that you have the Enterprise super user permission.

- Before setting up the SSO authentication, ensure 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](#).

## Procedure

- 1 Log in to a Velocloud Orchestrator (VCO) application as Enterprise super user, with your login credentials.
- 2 Click **Administration > System Settings**  
The **System Settings** screen appears.



- 3 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.

---

- 4 Click the **Authentication** tab and from the **Authentication Mode** drop-down menu, select **SSO**.

The screenshot shows the 'System Settings' page in the VeloCloud interface. The 'Authentication' tab is selected. Under 'Enterprise Authentication', the 'Authentication Mode' is set to 'SSO'. The 'Identity Provider template' is also set to 'SSO'. The 'OIDC well-known config URL' is empty. The 'Issuer', 'Authorization Endpoint', 'Token Endpoint', and 'User Information Endpoint' fields are also empty. The 'Client Id' is empty, and the 'Client Secret' is 'openid.profile,email,offline\_access'. The 'Scopes' field is empty. The 'Role Attribute' is 'groups'. The 'Role Map' section shows mappings for Enterprise Superuser (superuser), Enterprise Standard Admin (standard), Enterprise Support (support), and Enterprise Read Only (readonly). The 'Use Default Role' and 'Use Identity Provider Roles' radio buttons are both unselected.

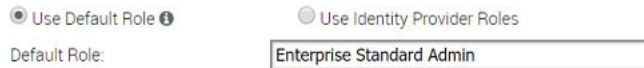
- 5 From the **Identity Provider template** drop-down menu, select your preferred Identity Provider (IDP) that you have configured for Single Sign On.

**Note** If 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.

- 6 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`.
- 7 The VCO application auto-populates endpoint details such as Issuer, Authorization Endpoint, Token Endpoint, and User Information Endpoint for your IDP.
- 8 In the **Client Id** text box, enter the client identifier provided by your IDP.
- 9 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.
- 10 To determine user's role in VCO, select one of the options:
- **Use Default Role** – Allows user to configure a static role as default by using the **Default Role** text box that appears on selecting this option. The supported roles are: Enterprise Superuser, Enterprise Standard Admin, Enterprise Support, and Enterprise Read Only.



- **Use Identity Provider Roles** – Uses the roles set up in the IDP.
- 11 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.
- 12 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>*.
- 13 Update the allowed redirect URLs in OIDC provider website with VCO URL (<https://<vco>/login/ssologin/openidCallback>).
- 14 Click **Save Changes** to save the SSO configuration.
- 15 Click **Test Configuration** to validate the entered 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 will be displayed.

## Results

The SSO authentication setup is complete.

## What to do next

[Chapter 5 Log in to VCO Using SSO for Enterprise User.](#)

## Configure Single Sign On for Identity Partners

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

### 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.

---

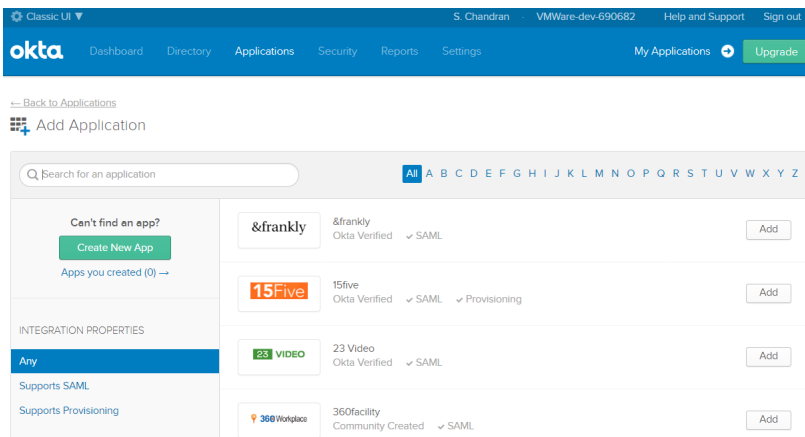
**Note** If you are in the Developer Console view, then you must switch to the Classic UI view by selecting **Classic UI** from the **Developer Console** drop-down list.

---

- 2 To create a new application:

- a In the upper navigation bar, click **Applications** > **Add Application**.

The **Add Application** screen appears.



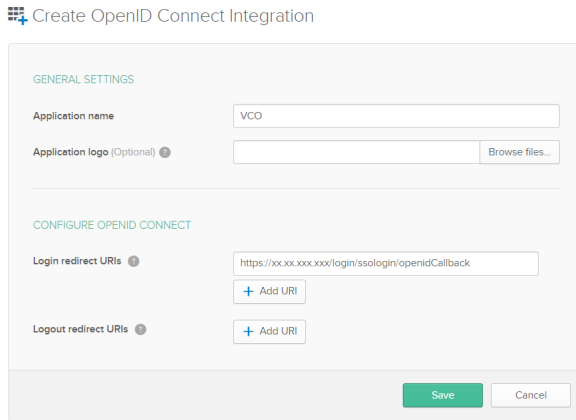
- b Click **Create New App**.

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.

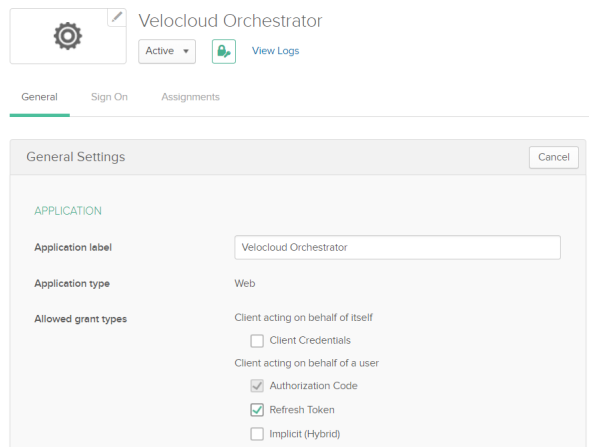


- e Under the **General Settings** area, in the **Application name** text box, enter the name for your application (for example, VCO).
- f Under the **CONFIGURE OPENID CONNECT** area, in the **Login redirect URIs** text box, enter the redirect URL that your VCO application uses as the callback endpoint.

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.

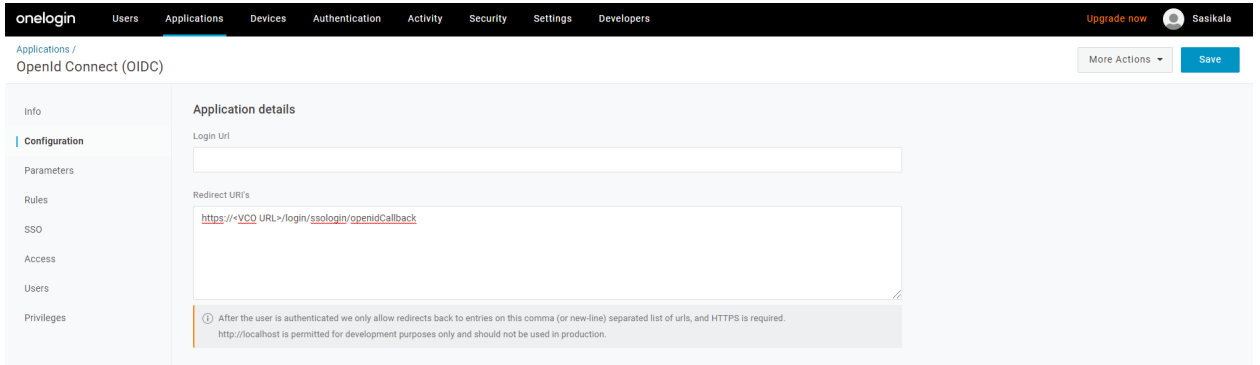
The **Add OpenId Connect (OIDC)** screen appears.

The screenshot shows the OneLogin administration interface for adding a new OpenID Connect (OIDC) application. The top navigation bar includes 'onelogin', 'Users', 'Applications', 'Devices', 'Authentication', 'Activity', 'Security', 'Settings', and 'Developers'. The main header area shows 'App Listing / Add OpenId Connect (OIDC)' with 'Cancel' and 'Save' buttons. The configuration area is divided into sections: 'Portal' with a 'Display Name' field containing 'OpenId Connect (OIDC)', a 'Visible in portal' toggle switch that is turned on, and two icon upload options: 'Rectangular Icon' and 'Square Icon'. Below these are instructions for icon uploads. The 'Description' section has a text box with a 200-character limit.

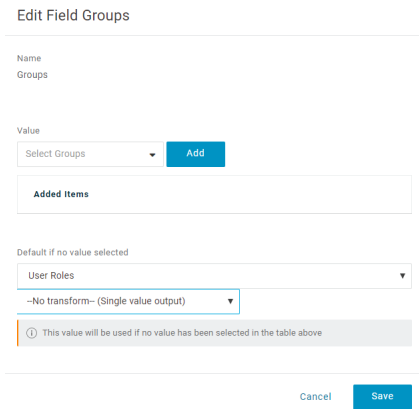
c In the **Display Name** text box, enter the name for your application (for example, VCO) and click **Save**.

- 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.

The screenshot shows the 'Enable OpenID Connect' configuration page in OneLogin. The left sidebar has tabs for Info, Configuration, Parameters, Rules, SSO, Access, Users, and Privileges. The main content area is titled 'Enable OpenID Connect' and includes the following fields and options:

- Client ID:** 14d05920-8c0c-0137-20f5-0a84509636a0151851
- Client Secret:** (Redacted)
- Show client secret:** [Show client secret](#) [Regenerate client secret](#)
- OpenID Provider Configuration Information:** [OpenID Provider Configuration Information](#)
- Application Type:** Application Type dropdown menu set to 'Web'.
- Token Endpoint:** Authentication Method dropdown menu set to 'POST'.

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

The screenshot shows the 'Policy' configuration page in OneLogin. The left sidebar has tabs for Info, Configuration, Parameters, Rules, SSO, Access, Users, and Privileges. The main content area is titled 'Policy' and includes the following fields and options:

- Policy:** By default all your users will be using this policy to log into this app. Policy dropdown menu set to '- None -'.
- Role-based policy:** Do you know you can set a policy for a certain role? [Add role-specific policy](#)
- Roles:** 'Default' and 'superuser' roles are selected with checkmarks.

- 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.

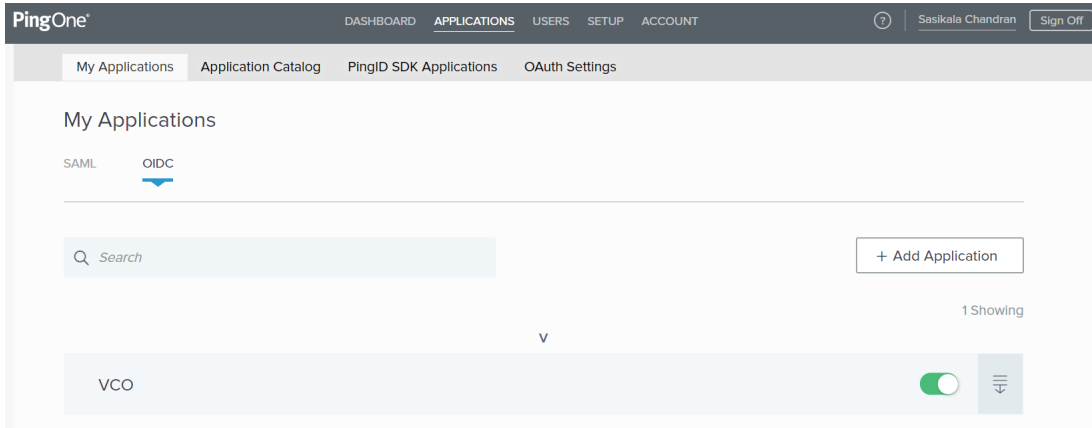
---

### Procedure

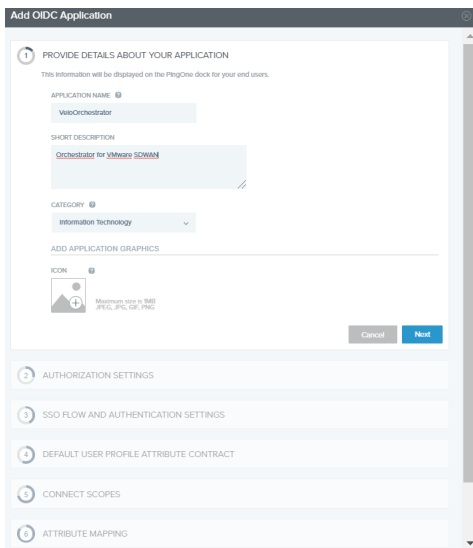
1 Log in to your [PingOne](#) account as an Admin user.

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.

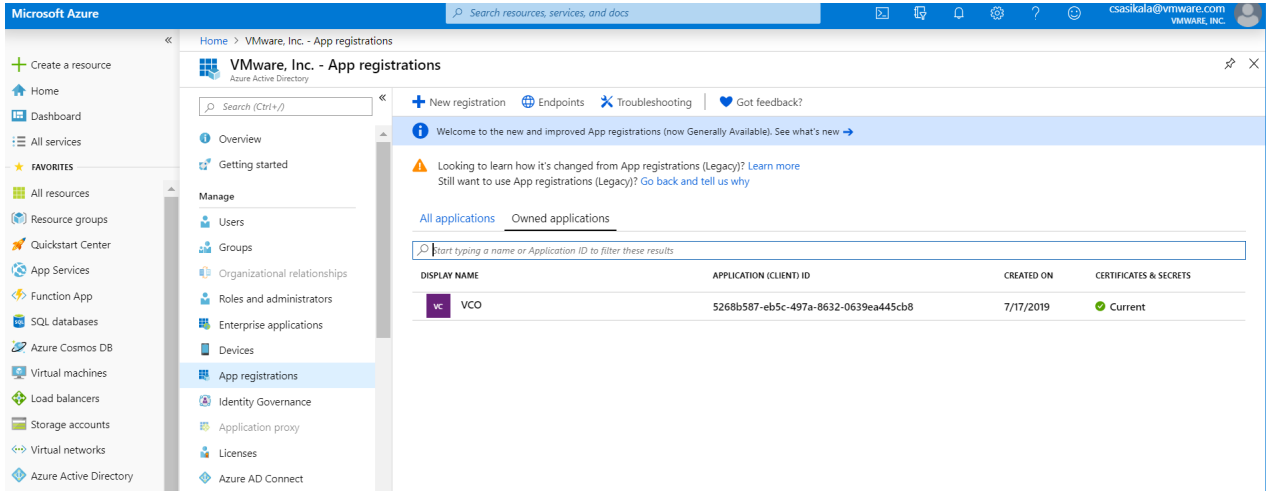
#### Procedure

- 1 Log in to your [Microsoft Azure](#) account as an Admin user.  
The **Microsoft Azure** home screen appears.



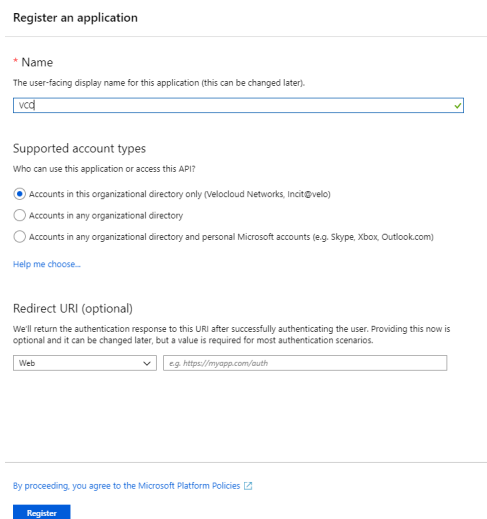
2 To create a new application:

- 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**.

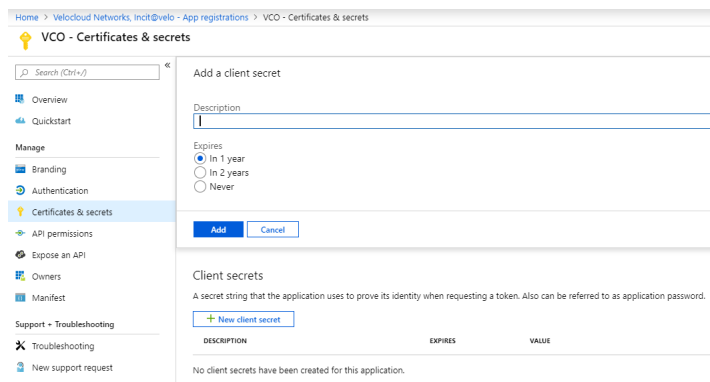
Your VCO application will be registered and displayed in the **All applications** and **Owned applications** tabs. Make sure to note down the Client ID/Application ID to be used during the SSO configuration in VCO.

- 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.

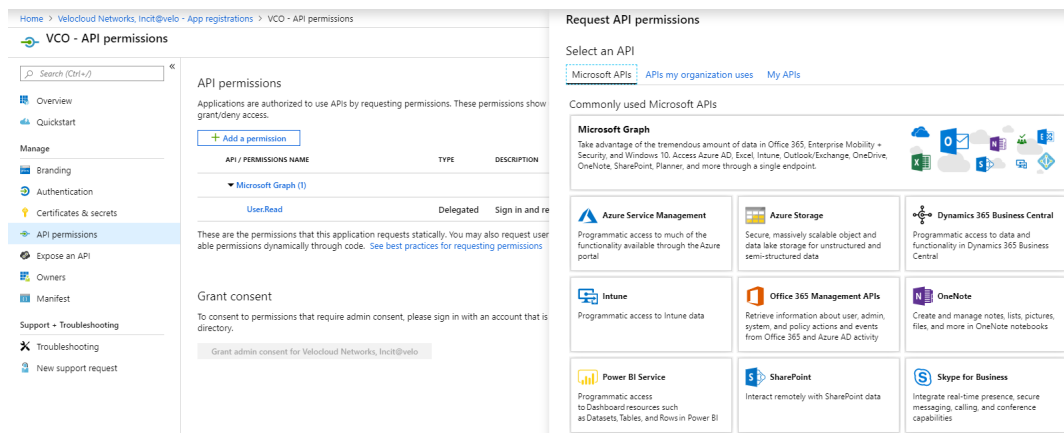


- i Provide details such as description and expiry value for the secret and click **Add**.

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**.

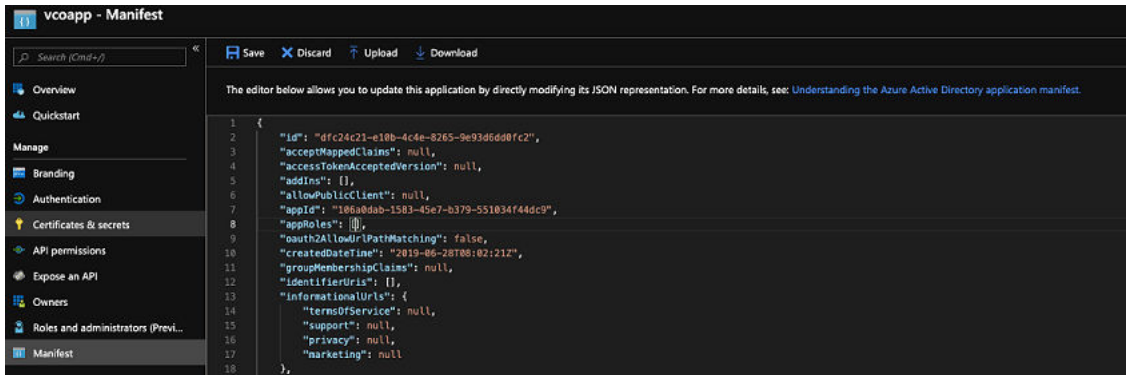
The **Request API permissions** screen appears.



- 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**.

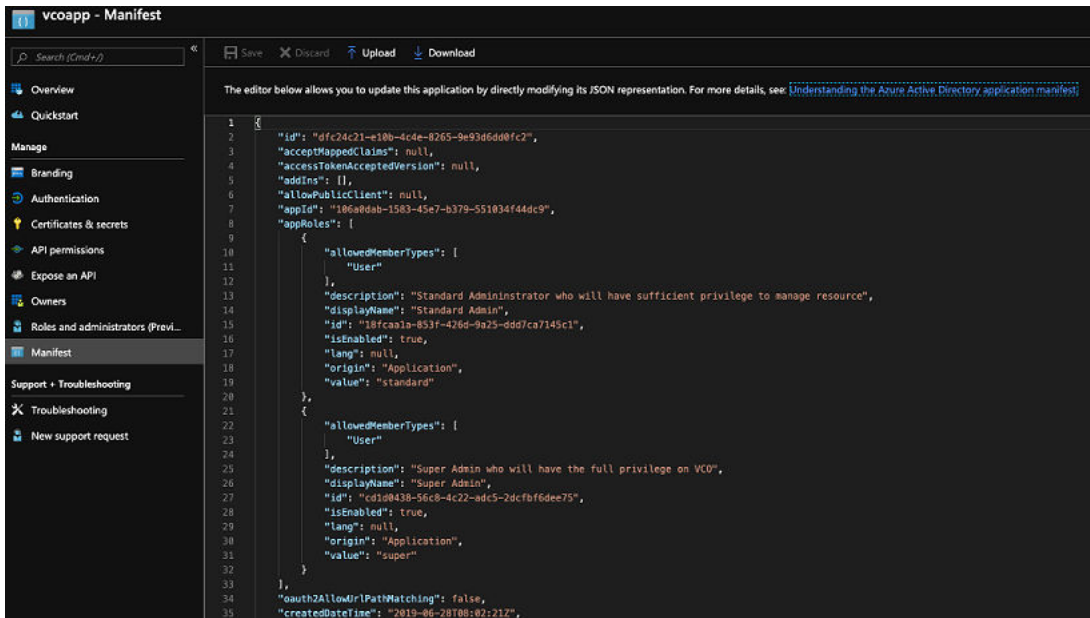
A web-based manifest editor opens, allowing you to edit the manifest within the portal. Optionally, you can select **Download** to edit the manifest locally, and then use **Upload** to reapply it to your application.



- 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 Adminstrator 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](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.

**Configure Authentication** Save Changes ?

**Operator Authentication**

Authentication Mode: SSO

Identity Provider template: VMwareCSP

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

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

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

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

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

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

Client Id: e1UmTD4TPps0h8vak0UMiOf0HCVwMw0MDta

Client Secret: [REDACTED]

Scopes: openid

Use Default Role  Use Identity Provider Roles

Role Attribute: perms

**Role Map**

Operator Superuser: external/1e73b58c-475f-4065-95d8-5f

Operator Standard Admin: external/1e73b58c-475f-4065-95d8-5f

Operator Support: support

Operator Business: business

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

The user is navigated to the 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](#).

## Self-service Password Reset

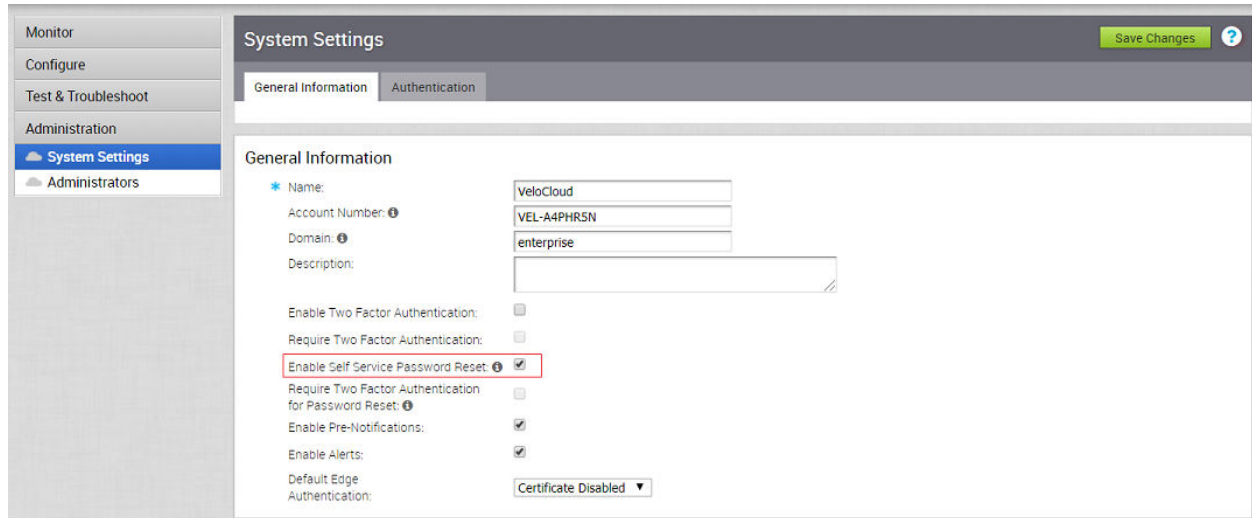
VCO users can perform a self-service password reset. This section describes how users can enable/disable this feature as well as how to reset their password with or without two factor authentication.

**Note** The "Self-service Password Reset" section is new for the 3.3.0 release.

### Enable Self-service Password Reset

When a new user is created, the Self-service Password Reset feature is enabled by default. For VCOs upgrading to version 3.3 from a prior release, the Self-service Password Reset feature will be enabled by default for those users as well. The following Operators can enable/disable Self-service Password Reset: Superuser, Standard, and Business Specialist. Customer Support Operators do not have access to this feature.





## Disable Self-service Password Reset

To disable self-service password reset for the users of a certain Enterprise, uncheck the **Enable Self-service Password Reset** checkbox and click the **Save Changes** button.

User Role Guidelines:

- The following Operators can enable/disable Self-service Password Reset: Operator Superusers, Operator Standard Admins, and Operator Business Specialists. Customer Support Operators do not have access to this feature.
- For Enterprise users, Superusers and Standard Admins can enable and disable the Self-service Password Reset feature. Customer Support users cannot enable or disable this feature; they have read-only access.
- Partner Superusers, Standard Admins, Business Specialists, and Customer Support can enable and disable the Self-service Password Reset feature for Partner Customers.

## Require Two Factor Authentication for Password Reset

Only Superuser, Standard, Business Specialists can require Two Factor Authentication for the Self-service Password Reset feature. (Customer Support Operators do not have access to this feature). Those with access can require Two Factor Authentication for Password Reset by selecting both the '**Enable Self Service Password Reset**' and the '**Require Two Factor Authentication for Password Reset**' checkboxes. For more information see section titled, "Two Factor Authentication."

**Note** If the customer's account has Two Factor Authentication configured for administrators, or Two Factor is required for password reset globally in System Properties, the customer will first be redirected to a Two Factor Authentication page, and will be prompted to enter a one-time code. After entering a valid code, the customer will be redirected to **New Password** page. In the **New Password** page, the customer will type a new password in the **Password** textbox, and will type the new password again in the **Confirm** textbox.

## Reset Your Password

If an end user has forgotten their password, or needs to change their password, the end user can reset it from the VCO login page if Self-service Password Reset is enabled.

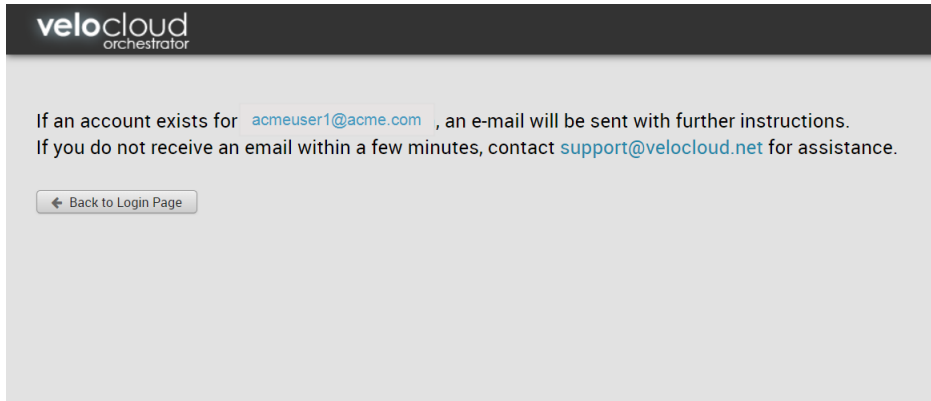
To reset your password:

- 1 From the VCO Login page, click the reset password link (**Click here to reset your password**). NOTE: For Partners responsible for password reset, the contact email address (support@velocloud.net) is configurable. The value can be overridden with the branding package.

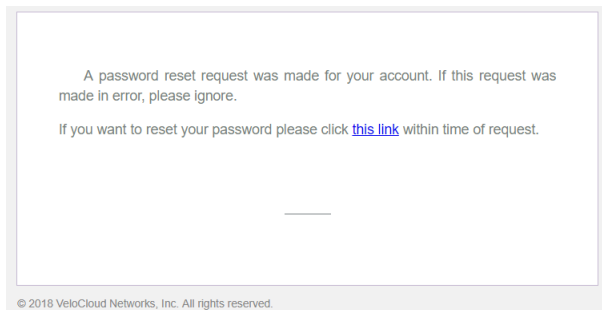
- 2 In the next screen, enter your username. (Make sure the username has an existing mailbox account).

- 3 Type in the Captcha as indicated. (Refresh if necessary).
- 4 Click **Submit**.

The following screen appears, prompting you to check your email for further instructions.



- 5 If the customer's username is an existing mailbox, and Self-service Password Reset is enabled, you will receive an email with a link to reset your password. The URL provided in the email is for a one-time use to reset your password, and will only be valid for 24 hours. If you try to change your password with the URL after the time limit has expired, you will be prompted to resubmit your request.



- 6 Type your new password in the **Password** textbox. Type your new password again in the **Confirm** textbox.
- 7 When you click the link provided in the email to reset your password, a new password page displays.

## Two Factor Authentication with Password Reset

If the customer's account has Two Factor authentication configured for administrators, or Two Factor is required for password reset globally in System Properties, the customer will first be redirected to a Two Factor Authentication page, and will be prompted to enter a one-time code. After entering a valid code, the customer will be redirected to New Password page. In the New Password page, the customer will type a new password in the **Password** textbox, and will type the new password again in the **Confirm** textbox.

## Configure Two-factor Authentication

VeloCloud Orchestrator provides two-factor authentication with SMS for Operators, MSP, and Enterprises. You can enable authentication at the Customer/MSP level or at the Operator level.

You can enable two-factor authentication after providing valid mobile numbers for all the users.

## Prerequisites

Ensure that you provide a valid mobile number for all admin users before enabling two-factor authentication. You can enter the mobile number by selecting the user in the **Administration > Administrators** screen.

## Procedure

- 1 In the Enterprise portal, click **Administration > System Settings**.
- 2 Select the **Enable Two Factor Authentication** checkbox.
- 3 To mandate the user login with two-factor authentication, select the **Require Two Factor Authentication** checkbox.
- 4 Click **Save Changes**.

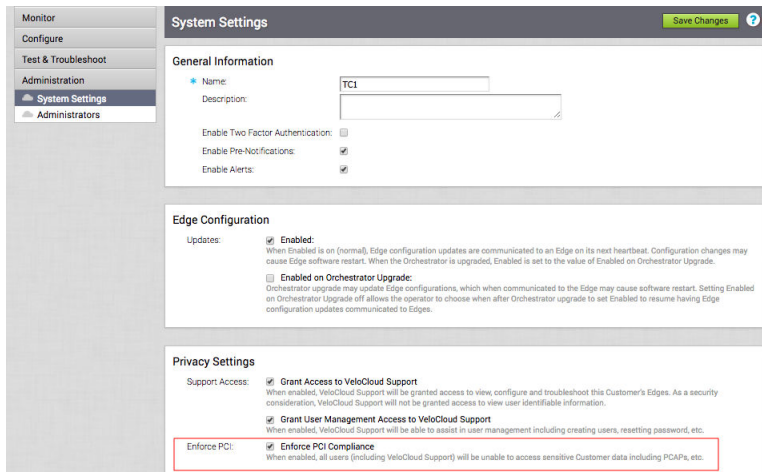
## Results

After enabling the two-factor authentication, when you try to login with your user credentials, you also need to enter the six-digit pin that you receive as SMS in your mobile.

## Enforce PCI Compliance on VCO

To enforce PCI compliance on the VCO.

- 1 Go to the VCO navigation panel and choose **Administration > System Settings**.
- 2 In the **Privacy Settings** area, select the **Enforce PCI Compliance** checkbox. This disables PCAP and removes the **Core Dump** option in **Test & Troubleshoot > Diagnostic Bundles** screen.



## Monitor Edge Licensing

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.

---

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

---

From the list of license types, users must assign license types to their Edges. See the Edge Overview Tab section, [Edge License](#), for information on how to assign license types.

## Generate an Edge Licensing Report

Standard Administrator Superusers, Standard Administrators, Business Specialists, and Customer Support users can generate a report listing the license types that are assigned to Edges.

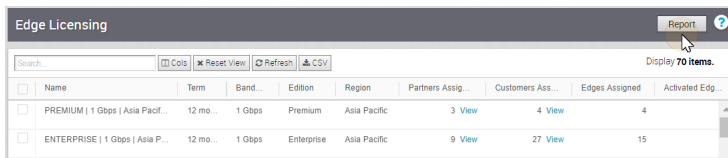
---

**Note** The "Generate an Edge Licensing Report" section is new for the 3.3.0 release.

---

To generate an Edge Licensing Report:

- 1 From the VCO navigation panel, go to **Administration > Edge Licensing**.
- 2 From the **Edge Licensing** screen, click the **Report** button.



The screenshot shows the 'Edge Licensing' interface. At the top right, there is a 'Report' button with a question mark icon. Below the header, there is a search bar and several utility buttons: 'Cols', 'Reset View', 'Refresh', and 'CSV'. The main content is a table with the following columns: Name, Term, Bandwidth, Edition, Region, Partners Assigned, Customers Assigned, Edges Assigned, and Activated Edges. The table contains two rows of data:

Name	Term	Bandwidth	Edition	Region	Partners Assigned	Customers Assigned	Edges Assigned	Activated Edges
PREMIUM   1 Gbps   Asia Pacif...	12 mo...	1 Gbps	Premium	Asia Pacific	3 <a href="#">View</a>	4 <a href="#">View</a>	4	
ENTERPRISE   1 Gbps   Asia P...	12 mo...	1 Gbps	Enterprise	Asia Pacific	9 <a href="#">View</a>	27 <a href="#">View</a>	15	

At the bottom right of the table area, it says 'Display 70 Items'.

The Excel spreadsheet report automatically downloads.

# Configure VCE High Availability

# 20

This section describes how to enable high availability on VCE.

This chapter includes the following topics:

- [Overview of VeloCloud Edge HA](#)
- [Prerequisites](#)
- [High Availability Options](#)
- [Split-Brain Detection and Prevention](#)
- [Failure Scenarios](#)
- [Support for BGP Over HA Link](#)
- [Selection Criteria to Determine Active and Standby Status](#)
- [VLAN-tagged Traffic Over HA Link](#)
- [Configure HA](#)
- [HA Event Details](#)

## Overview of VeloCloud Edge HA

The VeloCloud Edge (VCE) is the VeloCloud SD-WAN data plane component that is deployed at an end user's branch location. VCEs configured in High Availability (HA) mode are mirror images of each other and they show up on the VeloCloud Orchestrator (VCO) as a single VCE.

There are two options when configuring in HA mode:

- 1 HA Option 1
- 2 HA Option 2

For a description of both options, see *High Availability (HA) Options*.

This document describes the steps necessary to enable High Availability (HA) and bring up a second VCE as a Standby device to an activated Edge.

## Prerequisites

This section describes HA requirements that must be met before configuring a VCE as a Standby.

- The two VCEs must be the same model.
- Only one VCE should be provisioned on the VeloCloud Orchestrator (VCO).
- The Standby VCE must not have an existing configuration on it.

## High Availability Options

Edges can be installed as a single standalone device or paired with another Edge to provide High Availability (HA) support. However, the HA configuration is only for wired WAN connections.

### HA Options

There are two options when configuring in HA mode (Option 1 and Option 2). Both options are described below.

### HA Considerations

Considerations for both HA options:

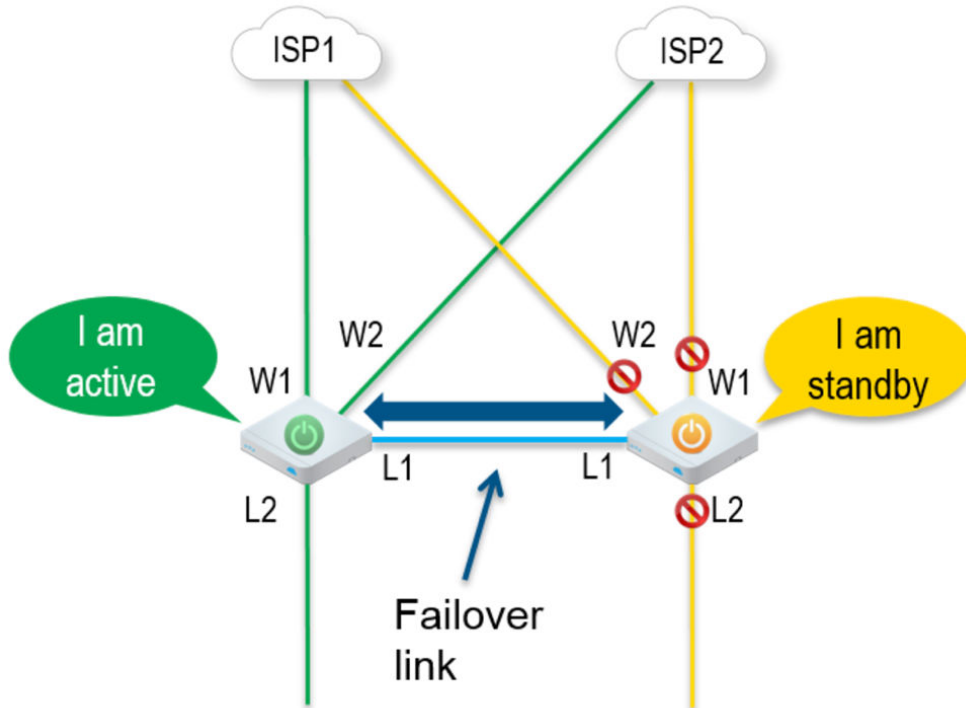
- Edges automatically select either Option 1 or Option 2. Edges will select Option 1 if both Edges are connected to the same WAN links. Edges will select Option 2 if the Edges detect that they are connected to different WAN links.
- There are no UI changes on the VCO for these two options.
- Both options are supported on all VCE platforms: 510, 520, 520v, 540, 840, 2000, and Virtual Edge.
- HA is supported only between the identical VCE platform models (see <https://www.velocloud.com/get-started/> for the various Edge platform models).

### HA Option 1: Standard HA

This section describes HA Option 1: Standard HA.

#### Topology Overview for HA Option 1

The following figure shows a conceptual overview of HA Option 1.



The Edges, one Active and one Standby, are connected by L1 ports to establish a failover link. The Standby VeloCloud Edge blocks all ports except the L1 port for the failover link.

### Prerequisites for HA option 1

- The LAN side switches in the following configuration descriptions must be STP capable and configured with STP.
- In addition, VeloCloud Edge LAN and WAN ports must be connected to different L2 switches. If it is necessary to connect the ports to the same switch, then the LAN and WAN ports must be isolated.
- The two VCEs must have mirrored physical WAN and LAN connections.

### Deployment Types for HA option 1

HA option 1 has two possible deployment types:

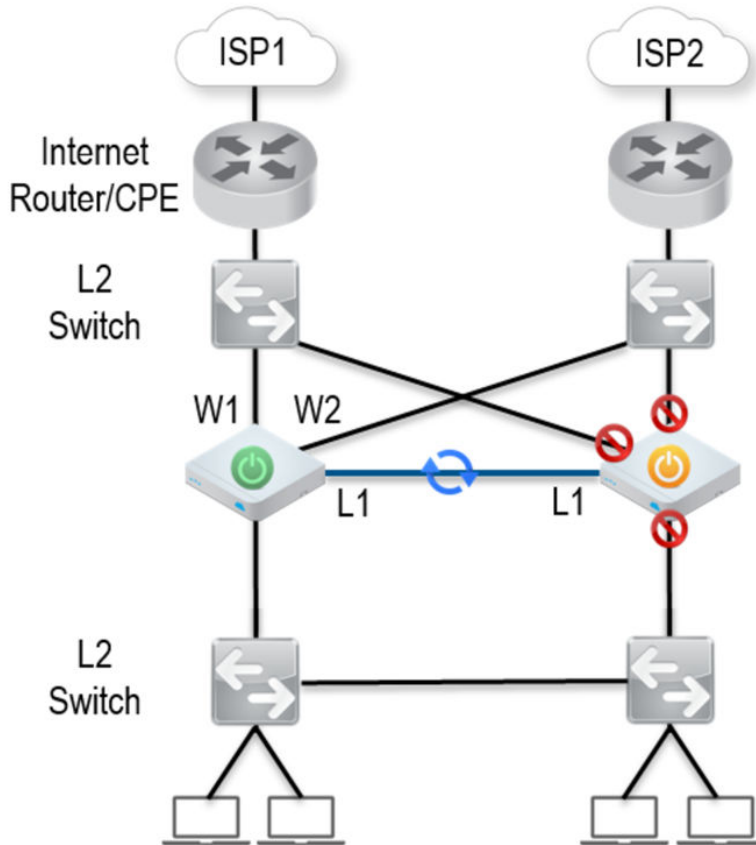
- Deployment Type One uses L2 switches
- Deployment Type 2 uses a combination of L2 and L3 switches

The following sections describe these two deployment types.

#### Deployment Type One: High Availability (HA) using L2 Switches

The following figure shows the network connections using only L2 switches.





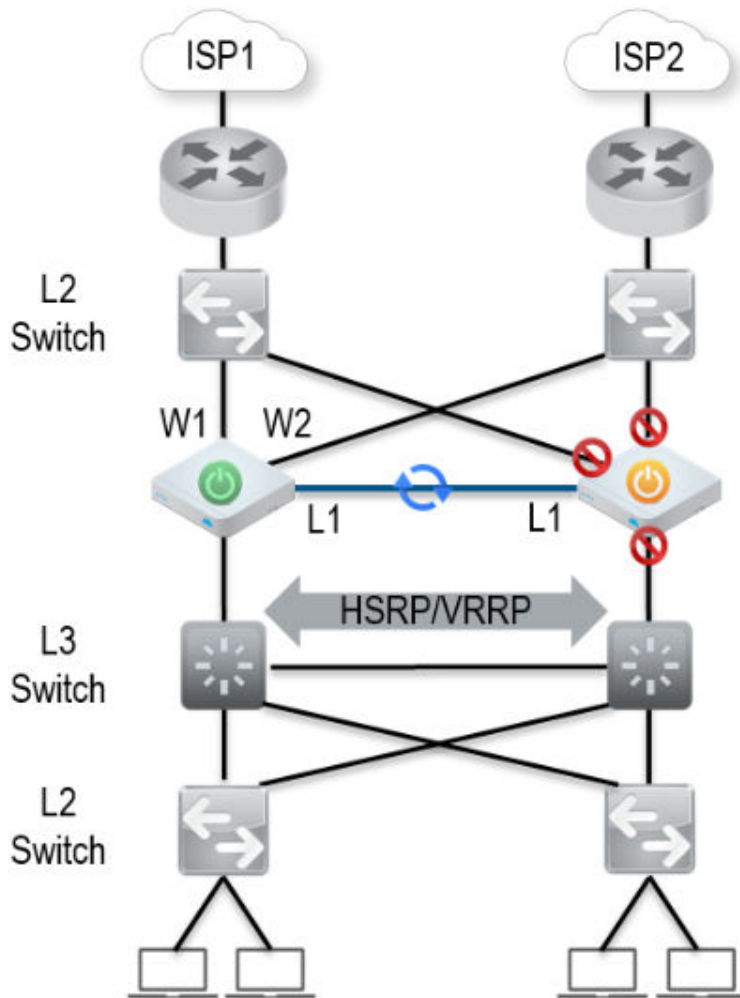
W1 and W2 are WAN connections used to connect to the L2 switch to provide WAN connectivity to both ISPs. The L1 link connects the two VCEs and is used for 'keep-alive' and communication between the VCEs for HA support. The VCE's LAN connections are used to connect to the access layer L2 switches.

### Considerations for Deployment Type One

- The same ISP link must be connected to the same port on both Edges.
- Use the L2 switch to make the same ISP link available to both Edges.
- The Standby VCE does not interfere with any traffic by blocking all its ports except the failover link (L1 port).
- Session information is synchronized between the Active and Standby VeloCloud Edges through the failover link.
- If the Active Edge detects a loss of a LAN link, it will also failover to the Standby if it has an Active LAN link.

### Deployment Type Two: HA Availability (HA) using L2/L3 Switches

The following figure shows the network connections using L2 and L3 switches.



The VeloCloud Edge WAN connections (W1 and W2) are used to connect to L2 switches to provide a WAN connection to ISP1 and ISP2 respectively. The L1 connections on the VeloCloud Edges are connected to provide a failover link for HA support. The VeloCloud Edge LAN connections are used to connect L2 Switches, which have several end-user devices connected.

### Considerations for Deployment Type Two

- HSRP/VRRP is required on the L3 switch pair.
- The VeloCloud Edge's static route points to the L3 switches' HSRP VIP as the next hop to reach the end stations behind L2 switches.
- The same ISP link must be connected to the same port on both VeloCloud Edges. The L2 switch must make the same ISP link available to both Edges.
- The Standby VeloCloud Edge does not interfere with any traffic by blocking all of its ports except the failover link (L1 port).
- The session information is synchronized between the Active and Standby VeloCloud Edges through the failover link.

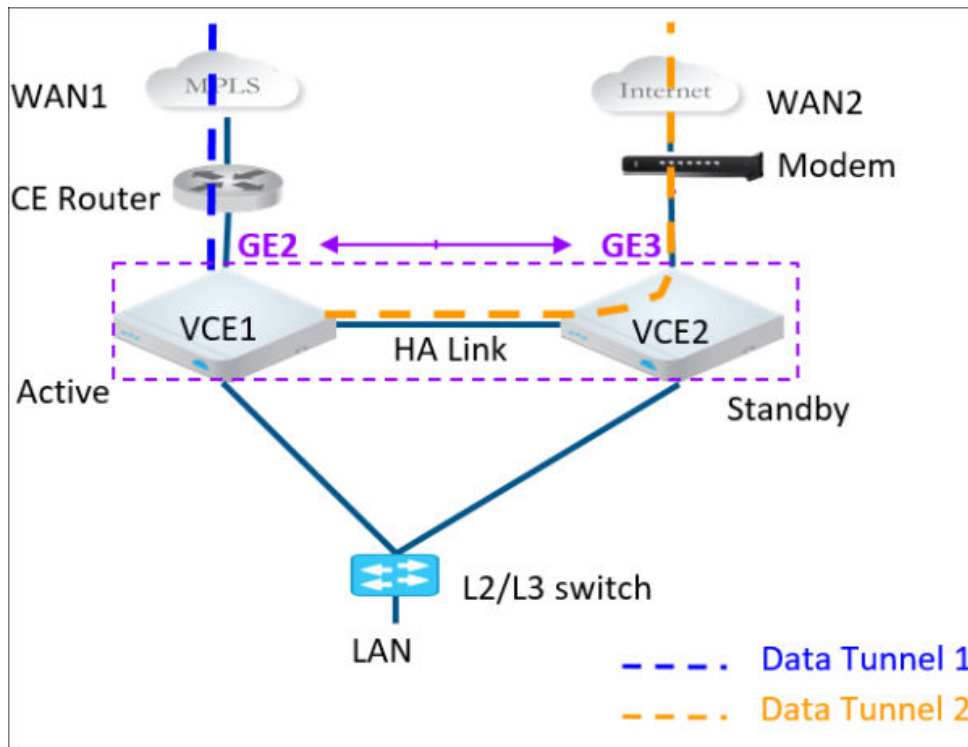
- The HA pair also does a failover from Active to Standby on detecting the L1 loss of LAN / WAN links.
  - If Active and Standby have the same number of LAN links which are up, but Standby has more WAN links up, then a switchover to Standby will occur.
  - If the Standby Edge has more LAN links up and has at least one WAN link up, then a failover to the Standby will occur. In this situation, it is assumed that the Standby Edge has more users on the LAN side than the Active Edge, and that the Standby will allow more LAN side users to connect to the WAN, given that there is some WAN connectivity available.

## HA Option 2: Enhanced HA

This section describes options for High Availability (HA) Option 2: Enhanced HA

The HA Option 2 eliminates the need for L2 Switches on WAN side of the Edges. This option is chosen when the Active Edge detects different WAN link(s) connected to the Standby Edge when compared to the link(s) connected to itself.

The following figure shows a conceptual overview of the HA option 2.



The Edges, one Active and one Standby, are connected by L1 ports to establish a failover link. The Standby VeloCloud Edge blocks all ports except the L1 port for the failover link. As shown in the figure, the Active Edge establishes overlay tunnels on both WAN links (connected to itself and the Standby Edge).

---

**Note** The two VCEs should not have mirrored physical WAN connections. As shown in the figure, if VCE1 has GE2 as the WAN link, VCE2 cannot have GE2 as its WAN link.

---

In order to leverage the WAN link connected to the Standby Edge, the Active Edge establishes the overlay tunnel through the HA link. Traffic from the LAN is forwarded to the Active Edge. The business policy for the branch defines the traffic distribution across the overlay tunnels.

## Split-Brain Detection and Prevention

The "Split-Brain Condition section and the Split-Brain Detection and Prevention" section is new for the 3.3.0 release.

### Split-Brain Condition

When the HA link is disconnected or when the Active and Standby Edges fail to communicate with each other, both Edges assume the Active role. As a result, both Edges start responding to ARP requests on their LAN interfaces. This causes LAN traffic to be forwarded to both Edges, which could result in spanning tree loops on the LAN.

Typically, switches run the Spanning Tree Protocol to prevent loops in the network. In such a condition, the switch would block traffic to one or both Edges. This would cause a total loss of traffic through the Edge pair.

---

**Note** Tunnel to Primary Gateway is a requirement for split-brain detection. Therefore, in WAN 2 (as shown in the the following figure), there should be a tunnel to VCG.

---

### Split-Brain Detection and Prevention

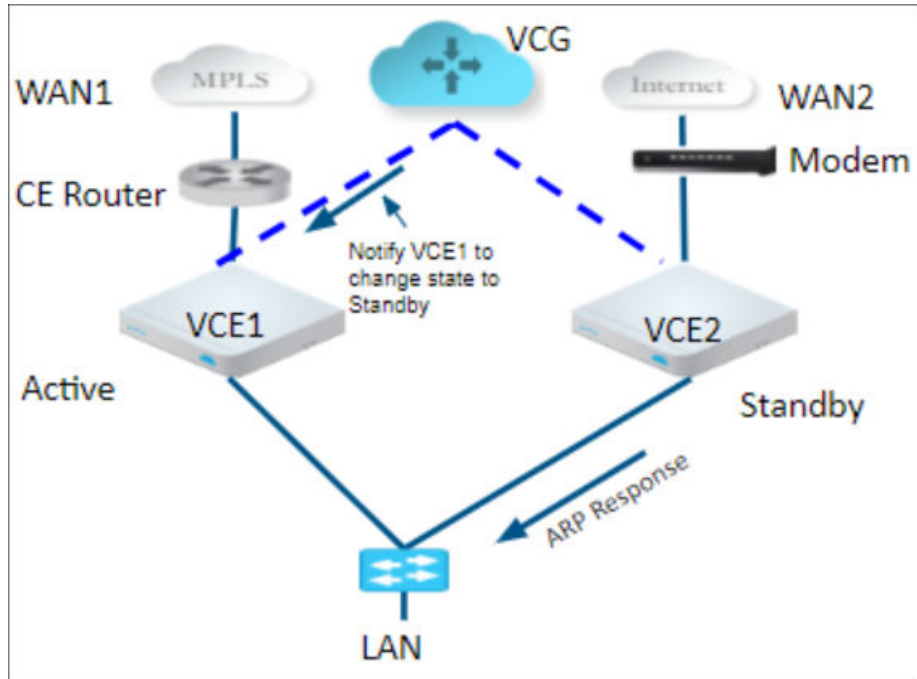
The primary Gateway is used to prevent split brain conditions.

The Gateway has a pre-existing connection to the Active VCE (VCE1 in the "Normal State" diagram above). In a split-brain condition, the Standby VCE (VCE2 in the "Split-brain Condition" diagram above), changes state to Active and establishes a tunnel with the Gateway. The Gateway allows the VCE2 to establish the new tunnel. However, the tunnels are not torn down. The Gateway informs the Edge VCE1 to move to the Standby state. In the 3.3.0 software release, in the Split-brain state, the Standby will also maintain tunnels to the Gateways. Only the LAN interfaces remain blocked (as long as the HA cable is down). As illustrated in the diagram below, the Gateway signals VCE1 to go into Standby mode on the LAN. This will logically prevent the Split-brain scenario from occurring.

---

**Note** The normal failover from Active to Standby in a Split-brain scenario is not the same as the normal failover. It could take a few extra milliseconds/seconds to converge.

---



## Failure Scenarios

This section describes the following scenarios that can trigger a failover from an Active to a Standby Edge.

- WAN link failure
- LAN link failure
- Edge functions not responding
- Edge crash or reboot or unresponsive

## Support for BGP Over HA Link

In case the Edges switch to the enhanced HA option, the Active VCE will exchange BGP routes over the HA link. BGP on the Active Edge can now establish neighborship with a peer connected only to the standby Edge's WAN link.

This will enable the Active Edge to learn routes from the WAN link(s) connected to the Standby Edge. The routing daemon on standby will not involve in any of the functionality. The standby Edge itself will just do a pass-through.

**Note** Routes are not synced between the active and the standby Edges. Therefore, in the above scenario, if there is a failover and a standby Edge becomes active, the BGP daemon on the newly active edge will establish a new neighborship with the same BGP peer.

## Selection Criteria to Determine Active and Standby Status

This section describes the selection criteria used to determine Active and Standby Status.

- Check for the Edge that has a higher number (L2 and L3) LAN interfaces. The Edge with the higher number of LAN interfaces is chosen as the Active one. Note that the interface used for the HA link is not counted as a LAN interface.
- If both Edges have the same number of LAN interfaces, the Edge with the higher number of WAN interfaces is chosen as the Active one.

---

**Note** There is no preemption if the two Edges have the same number of LAN and WAN interfaces.

---

- Additional Support Matrix:
  - Static/DHCP/PPPoE links are supported.
  - Multiple WAN links each tagged with a separate VLAN ID on a single interface (e.g. Sub-Interfaces) are supported.
  - USB modems are not recommended on HA. The interface will not be used when present in the Standby Edge.

## VLAN-tagged Traffic Over HA Link

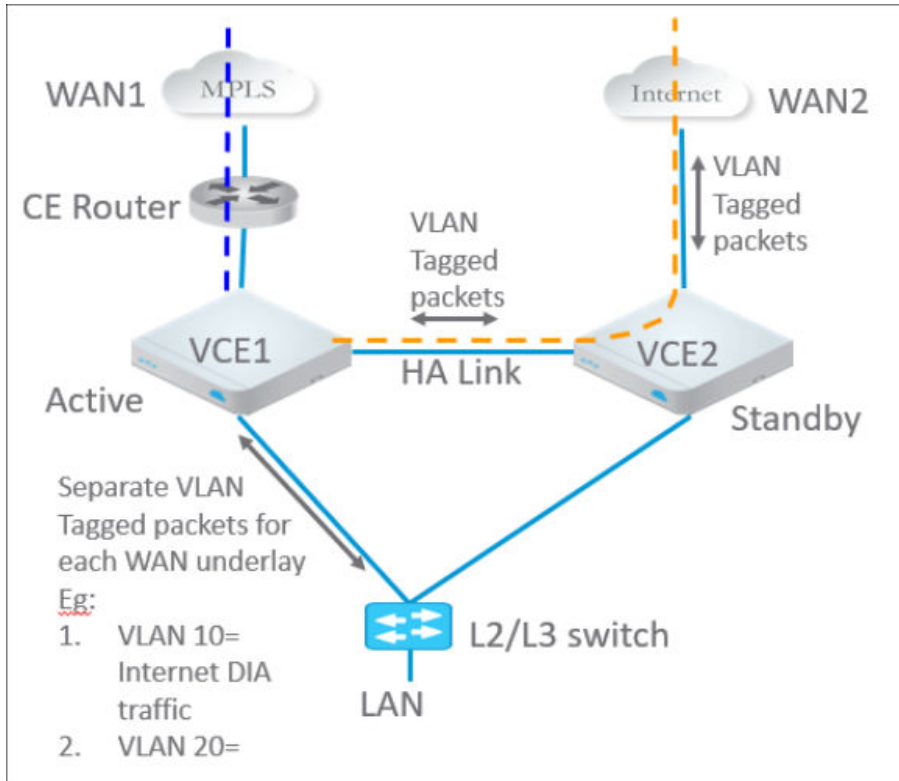
This section describes the VLAN-tagged Traffic over an HA Link.

---

**Note** The "VLAN Tagged Traffic Over HA Link" section is new for the 3.3.0 release.

---

- Internet traffic from ISP2 is VLAN tagged.
- Customer will have separate VLANs for Enterprise traffic versus DIA traffic.
- The WAN link on the Standby has sub-interfaces to carry Internet traffic.
- Multi segments



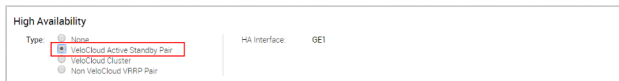
## Configure HA

For HA enhancements, there are no changes to the UI of the VCO.

### 1. Enable High Availability (HA)

To enable the HA feature on the VCO:

- 1 From the navigation panel, go to **Configure > Edges**.
- 2 Select your VeloCloud Edge (VCE), and then click the **Device** tab.
- 3 From the **High Availability** area, click the radio button **VeloCloud Active Standby Pair**.



By default, the GE1 or LAN1 interface will be used as the HA interface to connect the pair depending on the VCE model.

**Note** This is available on as an Edge Override and is not configurable at the Profile level. Do not connect the Standby VCE.

### 2. Wait for VCE to Assume Active

After the High Availability feature is enabled on the VCO, wait for the existing VCE to assume an Active role, and wait for the VCO Events to display **High Availability Going Active**.

ⓘ	Sun Jul 10, 23:00	High Availability Going Active	DC1 - Hub1	Notice	VeloCloud Edge going active, peer has not been detected
ⓘ	Sun Jul 10, 23:00	Edge service startup	DC1 - Hub1	Notice	VeloCloud edge service started
ⓘ	Sun Jul 10, 23:00	Edge online	DC1 - Hub1	Info	Management Daemon Started, version 2.1.0 build R21- ██████████
ⓘ	Sun Jul 10, 22:56	ENDPOINT_ACCEPTED_CERTIFICATE	DC1 - Hub1	Info	AE18A7B61185ABE827DBD8B98556C5AACA36C3ED
ⓘ	Sun Jul 10, 22:56	EDGE_OSPF_NSM	DC1 - Hub1	Notice	Edge NSM event: interface=172.31.2.1 nbr=172.31.2.2 router_id=172.31.2.2 status=Full
ⓘ	Sun Jul 10, 22:56	Link alive	DC1 - Hub1	Info	Link GE4 is no longer DEAD
ⓘ	Sun Jul 10, 22:56	Edge Interface Up	DC1 - Hub1	Info	Interface GE4 is up
ⓘ	Sun Jul 10, 22:56	Edge Interface Up	DC1 - Hub1	Info	Interface GE3 is up

### 3. Connect the Standby VCE to the Active Edge

To connect the Standby VCE to the Active Edge:

- 1 Power on the Standby VCE without any network connections.
- 2 After it boots up, connect the LAN1/GE1 interface (as indicated on the **Device** tab) to the same interface on the Active VCE.
- 3 Wait for the Active VCE to detect and activate the standby VCE automatically. The VCO Events displays **HA Standby Activated** when the VCO successfully activates the standby VCE.

ⓘ	Fri Nov 18, 14:31:54	Edge service startup	██████████	Notice	VeloCloud edge service started
ⓘ	Fri Nov 18, 14:31:07	HA Standby Activated	██████████	Notice	Standby has been detected

The standby Edge will then begin to synchronize with the active VCE and reboot automatically during the process.

**Note** It may take up to 10 minutes for the Standby VCE to sync with the Active Edge and upgrade its software.

ⓘ	Fri Nov 18, 14:37:27	High Availability Ready	██████████	Notice	Standby state ready for failover
ⓘ	Fri Nov 18, 14:37:25	Edge service startup	██████████	Notice	VeloCloud edge service started
ⓘ	Fri Nov 18, 14:37:08	Edge online	██████████	Info	Management Daemon Started, version 2.2.1 build R221- 20161109-GA
ⓘ	Fri Nov 18, 14:36:25	HA Peer State Unknown	██████████	Notice	Peer state unknown
ⓘ	Fri Nov 18, 14:34:59	Standby device software update started	██████████	Info	Begin HA Standby update with new software version
ⓘ	Fri Nov 18, 14:32:15	High Availability Ready	██████████	Notice	Standby state ready for failover
ⓘ	Fri Nov 18, 14:32:14	Edge service startup	██████████	Notice	VeloCloud edge service started

### 4. Connect LAN and WAN Interfaces on Standby VCE

Connect the LAN and WAN interfaces on the standby VCE mirroring the network connectivity on the Active Edge.

The VCO Events will display **Standby device software update completed**. The **HA State** (under **Monitor > Edges** on the VCO) appears green when ready.

Edge	Status	HA	Links	Gateways	Profile	Operator Profile
1 Bronze VCE	●	●	●	View	SF Branch Profile	Initial Operator Profile
2 DC1 - Hub1	●	●	●	View	DC1 Hub Profile	Hub Operator profile - no S...
3 DC2 - Hub1	●	●	●	View	DC2 Hub Profile	Hub Operator profile - no S...
4 SF1 - MPLS_Internet Branch	●	●	●	View	SF Branch Profile	Initial Operator Profile
5 SF2 - Dual Internet Branch	●	●	●	View	SF Branch Profile	Initial Operator Profile
6 Silver1 VCE	●	●	●	View	SF Branch Profile	Initial Operator Profile
7 Silver2 VCE	●	●	●	View	SF Branch Profile	Initial Operator Profile



## HA Event Details

This section describes HA events.

HA Event	Description
HA_GOING_ACTIVE	A standby VCE is taking over as Active because it has not heard a heartbeat from the peer.
HA_STANDBY_ACTIVATED	When a new Standby is detected by the Active, the Active tries to activate the Edge by sending this event to the VCO. On a successful response from the VCO, the Active will sync the configurations and sync data.
HA_FAILED	Typically happens after the HA pair has formed and the Active VCE no longer hears from the Standby VCE. For example, if the Standby VCE reboots, you will receive this message.
HA_READY	Means the Active VCE now hears from the Standby VCE. Once the Standby VCE comes back up and reestablishes the heartbeat, then you will receive this message.
HA_TERMINATED	When the HA configuration is disabled, and it is successfully applied on the Edges, this Event is generated.
HA_ACTIVATION_FAILURE	If the VCO is unable to verify the HA activation, it will generate this Event. Examples include: <ul style="list-style-type: none"> <li>■ the VCO is unable to generate a certificate</li> <li>■ the HA has been deactivated (rare)</li> </ul>

# Testing and Troubleshooting

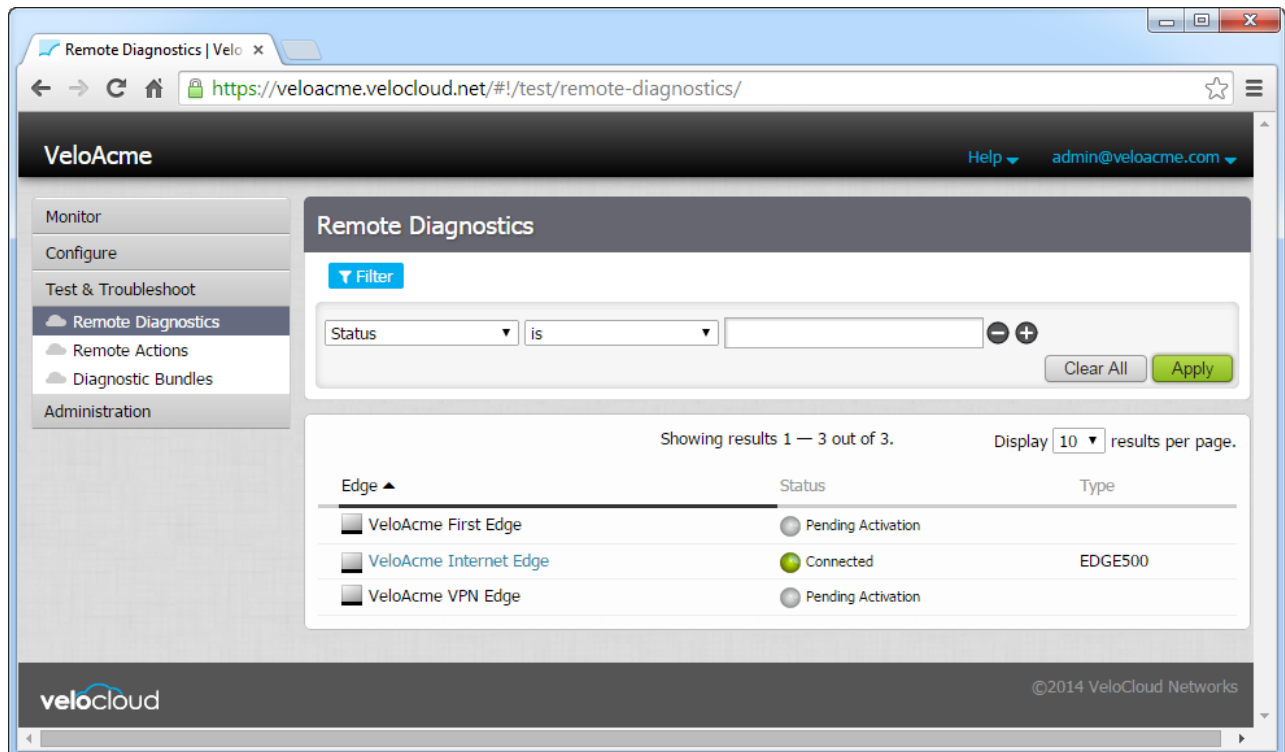
# 21

The VeloCloud Orchestrator Test & Troubleshoot functionality provides tools to test the status of the VeloCloud service, perform Edge actions, and gather Packet Capture information for an individual Edge.

You can access these features under the **Test & Troubleshoot** section of the navigation panel listed as follows:

- [Remote Diagnostics](#)
- [Remote Actions](#)
- [Diagnostic Bundles](#)

When you click **Test & Troubleshoot**, the **Remote Diagnostics** screen appears. It displays all the Edges you have defined in the **Edge** column at the bottom of the screen.



You can use the **Filter** to find Edges based on connection Status, Name, IP address, Serial Number, Software Version, and Software Build. However, before you can perform any of the Test & Troubleshoot options, you must select an Edge from the **Edge** column. See the sections below for more information regarding each of the Test & Troubleshooting options from the navigation panel (Remote Diagnostics, Remote Actions, and Diagnostic Bundles).

This chapter includes the following topics:

- [Remote Diagnostics](#)
- [Remote Actions](#)
- [Diagnostic Bundles](#)

## Remote Diagnostics

You can run tests on a single Edge to obtain diagnostic information by clicking **Remote Diagnostics** under **Test & Troubleshoot**.

To run a diagnostic test on a single Edge:

- 1 Click **Remote Diagnostic** under **Test & Troubleshoot**.
- 2 Search for an Edge if necessary using the **Filter**, and click **Apply**.
- 3 Select a connected Edge.

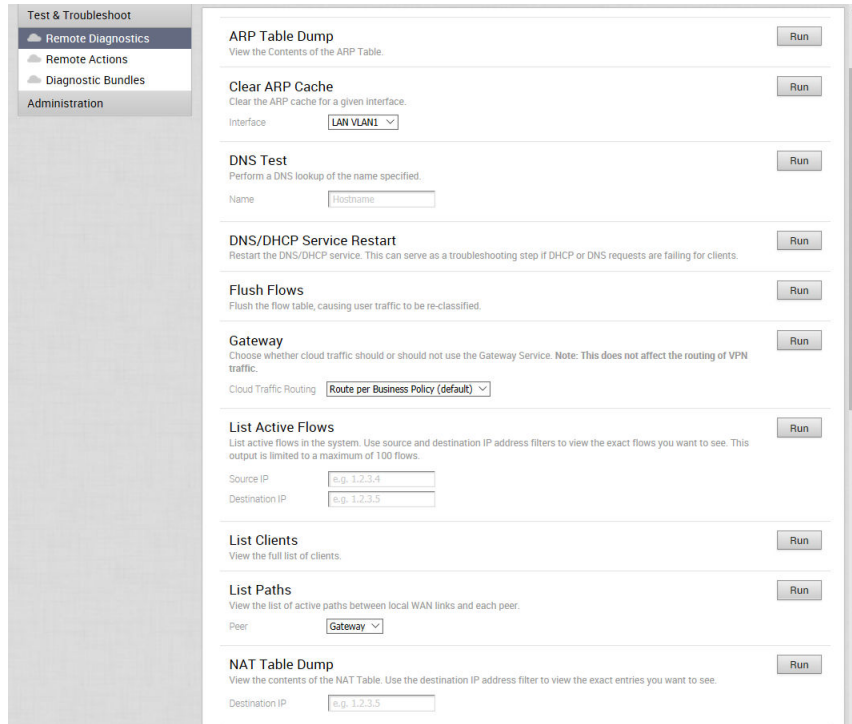
The **Remote Diagnostics** screen appears showing all the possible tests you can run on an Edge.

- 1 Choose a test to run. A description is located under each diagnostic test name. (See image below).
- 2 Click **Run**.

---

**Note** When you run the **Bandwidth Test** in a single-link environment, all other traffic will be interrupted. However, this excess traffic will only last a few moments until the test is finished.

---



## Supported Remote Diagnostics Tests

Remote Diagnostics Test	Description
ARP Table Dump	Run this test to view the contents of the ARP table. The output is limited to display 1000 ARP entries.
Clear ARP Cache	Run this test to clear the ARP cache entries for the specified interface.
DNS Test	Run this test to perform a DNS lookup of the specified domain name.
DNS/DHCP Service Restart	Run this test to restart the DNS/DHCP service. This can serve as a troubleshooting step if DHCP or DNS requests are failing for clients.
Flush Flows	Run this test to flush the flow table, causing user traffic to be re-classified. Use source and destination IP address filters to flush specific flows.
Flush NAT	Run this test to flush the NAT table.
Interface Status	Run this test to view the MAC address and connection status of physical interfaces.
List Active Flows	Run this test to list active flows in the system. Use source and destination IP address filters to view the exact flows you want to see. This output is limited to a maximum of 1000 flows.
List Clients	Run this test to view the complete list of clients.
List Paths	Run this test to view the list of active paths between local WAN links and each peer.

Remote Diagnostics Test	Description
MIB for VeloCloud Edge	Run this test to dump Edge MIBs.
NAT Table Dump	Run this test to view the contents of the NAT Table. Use the destination IP address filter to view the exact entries you want to see. This output is limited to a maximum of 1000 entries.
NTP Dump	Run this test to view the current date and time on Edge and NTP information.
Ping Test	Run a ping test to the destination specified.
Route Table Dump	Run this test to view the contents of the Route Table.
System Health	Run this test to view system information such as system load, recent WAN stability statistics, monitoring services. WAN stability statistics include the number of times individual VPN tunnels and WAN links lost connectivity for at least 700 milliseconds.
Traceroute	Run a traceroute via the Gateway or directly out any of the WAN interfaces to the destination specified.
Troubleshoot BGP - List BGP Redistributed Routes	Run this test to view routes redistributed to BGP neighbors.
Troubleshoot BGP - List BGP Routes	Run this test to view the specific BGP routes from neighbors, leave prefix empty to view all.
Troubleshoot BGP - List Routes per Prefix	Run this test to view all the Overlay and Underlay routes for a prefix and the related details.
Troubleshoot BGP - Show BGP Neighbor Advertised Routes	Run this test to view the BGP routes advertised to a neighbor.
Troubleshoot BGP - Show BGP Neighbor Learned Routes	Run this test to view all the accepted BGP routes learned from a neighbor after filters.
Troubleshoot BGP - Show BGP Neighbor Received Routes	Run this test to view all the BGP routes learned from a neighbor before filters.
Troubleshoot BGP - Show BGP Routes per Prefix	Run this test to view all the BGP routes and their attributes for the specified prefix.
Troubleshoot BGP - Show BGP Summary	Run this test to view the existing BGP neighbor and received routes.
Troubleshoot BGP - Show BGP Table	Run this test to view the BGP table.
Troubleshoot OSPF - List OSPF Redistributed Routes	Run this test to view all the routes redistributed to OSPF neighbor.
Troubleshoot OSPF - List OSPF Routes	Run this test to view the OSPF routes from neighbors for the specified Prefix. Displays all the OSPF routes from the neighbors if the Prefix is not specified.
Troubleshoot OSPF - Show OSPF Database	Run this test to view the OSPF link state database summary.
Troubleshoot OSPF - Show OSPF Database for E1 Self-Originate Routes	Run this test to view the E1 LSA's self-originated routes that are advertised to OSPF router by the Edge.

Remote Diagnostics Test	Description
Troubleshoot OSPF - Show OSPF Neighbors	Run this test to view all the OSPF neighbors and associated information.
Troubleshoot OSPF - Show OSPF Route Table	Run this test to view the existing OSPF route table.
Troubleshoot OSPF - Show OSPF Setting	Run this test to view the OSPF setting and neighbor status.
VPN Test	Use ping to test VPN connectivity to each peer.
VeloCloud Gateway	Run this test by choosing whether cloud traffic should or should not use the Gateway Service.  <b>Note</b> This does not affect the routing of VPN traffic.
WAN Link Bandwidth Test	Run the bandwidth test on a specified WAN link. This test has the benefit of being non-disruptive in multi-link environments. Only the link under test is blocked for user traffic. This means that you can re-run the test on a specific link and the other link(s) will continue to serve user traffic.

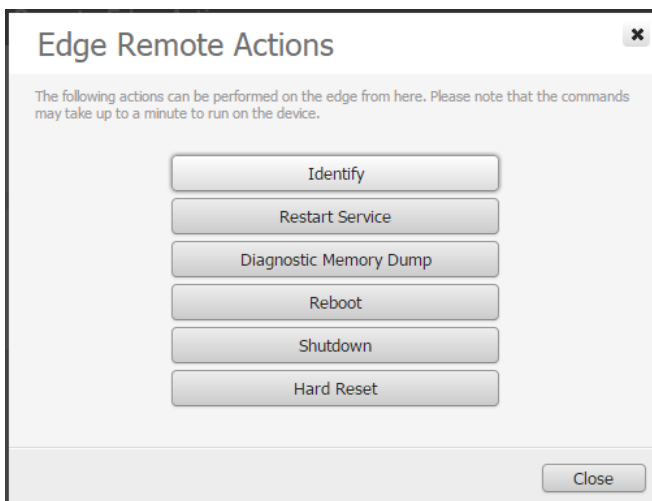
## Remote Actions

When you click **Remote Actions** (located under **Test & Troubleshoot**), the **Remote Edge Actions** screen appears, listing the Edges that are defined in the Edge column.

To conduct a remote Edge action on a single Edge:

- 1 Click **Remote Actions** under **Test & Troubleshoot**.
- 2 Search for an Edge if necessary using the **Filter**, and click **Apply**.
- 3 Select a connected Edge.

The **Edge Remote Actions** dialog box appears listing all possible actions you can run on the Edge. Definitions for each action in the **Edge Remote Actions** dialog box are provided later in this section.



- 4 Click an Edge remote action. The pop-up message **Action Sent Successfully** appears in the top right corner of the screen.
- 5 Click **Close**.

---

**Note** The actions may take up to a minute to run on the device.

---

## Edge Remote Action Definitions

The following list defines each action in the **Edge Remote Actions** dialog box.

Action	Description
Identify	Randomly flash lights on the Edge so it can be identified.
Restart Service	Restarts the VeloCloud service.
Diagnostic Memory Dump	Forces the save of a memory dump on the Edge.
Reboot	Performs an Edge reboot.
Shutdown	Shuts down the VeloCloud Edge.
Hard Reset	Returns the Edge hardware to its factory default state.

## Reset Edges to Factory Settings

are required to be reset to factory settings for several reasons, some of which are as follows:

- When you repurpose the Edge for another site, you must clear the existing configuration so that the Edge can be activated to the new site.
- Your site is encountering an issue for which Support recommends that you perform a hard reset to revert the Edge to factory settings and reactivate the Edge to the site to see if that resolves the issue.
- The Edge is inaccessible or non-responsive and multiple power cycles are not resolving the issue. It is recommended that you perform a hard reset to revert the Edge to factory settings and see if that resolves the issue.

You can reset an Edge to factory settings using one of the following methods:

- **Soft Reset or Deactivation**—The Edge is deactivated and all the existing configuration that the Edge is using is completely removed. The Edge now uses the original factory configuration. However, the Edge software is not affected and it retains the software version it had prior to the soft reset. A soft reset Edge can be reactivated to another site or to the same site.
- **Hard Reset**—The Edge is fully reset to factory settings, that is the Edge is not only deactivated and uses the factory configuration, but the Edge software is also changed to the factory software version. The Edge is effectively as it was when it was shipped from the factory.

If you reset an Edge that is actively used at a site, you will completely lose the client device connectivity at the site until you either reactivate the same Edge at the site or activate another Edge at the site.

For instructions on how to reset an Edge to factory settings, see [How to Factory Reset a VMware SD-WAN Edge](#).

## Diagnostic Bundles

From the **Diagnostic Bundles** window (accessed via **Test & Troubleshooting > Diagnostic Bundles** in the VCO), Operators can request PCAP Bundles and Diagnostic Bundles. Standard Admins and Customer Support can only request PCAP Bundles.

## Request Packet Capture

The Packet Capture function is used to collect debugging information from an Edge device.

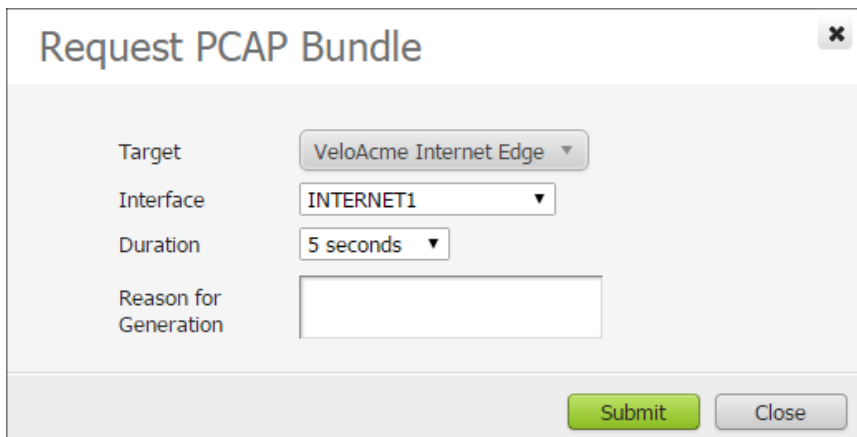
Access Packet Capture from **Test & Troubleshoot > Packet Capture**.

To request a packet capture:

- 1 Click **Packet Capture** under **Test & Troubleshoot**.

The **Packet Capture** screen appears. If applicable, the status of previous requests are shown.

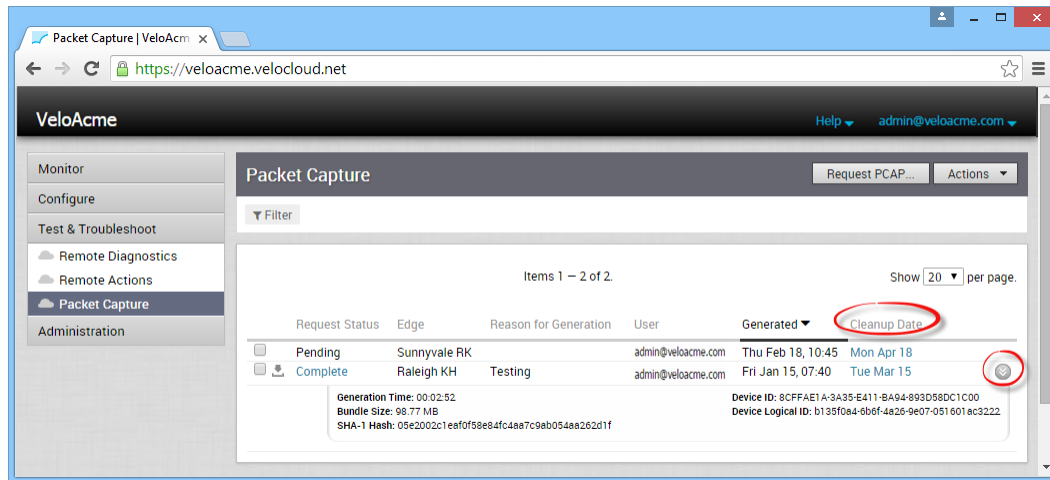
- 2 Click the **Request PCAP** button at the top right corner of the screen.
- 3 In the **Request PCAP Bundle** dialog box, choose your Target, Interface, and Duration. If necessary, type in a reason for the generation.



- 4 Click **Submit**. A pop-up message (Successful Request) appears in the top right corner of the screen.

The **Packet Capture** screen updates to show the status of the request. Refresh your screen or click **Packet Capture** from the navigation panel to display status results. When complete, you can get detailed information (Generation Time, Bundle Size, etc.) by clicking the gray arrow located next to the last column on the far right.





**Note** The Packet Capture data for a particular Edge will get deleted from the system on the date displayed in the **Cleanup Date** column. Click the **Cleanup Date** link to indicate a date to remove the data or select the **Keep Forever** checkbox and the data will not get deleted; it will be kept until you indicate otherwise.

Click the **Actions** button to download or delete the bundle. See the sections below for more information.

## Download Bundle

When the request is complete, you can download the bundle in one of the following ways:

- Click the Download symbol next to a completed PCAP request under the **Request Status** column.
- Click the **Complete** link in the **Request Status** column for your selected Edge.
- Select the checkbox of one or more completed PCAP requests, and click the down arrow of the **Action** button (top, right corner of the screen) and choose **Download**.

You can forward the downloaded bundle to a VeloCloud Networks Support representative.

## Delete Bundle

If you want to delete a Packet Capture, select one or more Packet Captures from the **Request Status** column and choose **Delete** from the **Actions** button.

**Note** If a Packet Capture request is pending, you can delete the request before the request is completed. Select the checkbox of the pending request you want to delete, and click the **Action** button, and choose **Delete**.

## Request Diagnostic Bundle

Only Operators can request Diagnostic Bundles. If you are an Operator, you will see the **Diagnostic Bundle** button in the top right corner of the Diagnostic Bundles screen in the VCO (**Test & Troubleshooting > Diagnostic Bundles**).

To request a diagnostic bundle:

- 1 Click the **Request Diagnostic Bundle** button located on the top right corner of the **Diagnostic Bundles** screen.
- 2 In the **Request Diagnostic Bundle** dialog box:
  - a In the **Target** drop-down menu, select the specific Edge from which you will receive the data.
  - b If you want to indicate the reason for request, include that in the **Reason for Generation** textbox.
  - c For an advanced request, click the **Advanced** button and choose a limit from the **Core Limit** drop-down menu. The Core Limit is used to reduce the size of the uploaded bundle when the Internet connectivity is experiencing errors.
  - d Click the Submit button.

The screenshot shows a dialog box titled "Request Diagnostic Bundle". It has a search icon and a close button in the top right corner. The form includes:

- Target:** A dropdown menu showing "edge540-215".
- Reason for Generation:** A text input field.
- Core Limit:** A dropdown menu with "No Limit" selected. The dropdown list is open, showing options: "No Limit", "3", "2", "1", and "No Cores".
- Advanced:** A button to toggle advanced options.
- Submit:** A green button to submit the request.
- Close:** A button to close the dialog.

The Diagnostic Request bundle for the selected Edge is in the Pending state, as shown in the Request Status column in the Diagnostic Bundles window. When finished, the status will change to **Complete**. The **Complete** status is a link that you can click to download the bundle.

# VeloCloud Virtual Edge Deployment Guide

# 22

This guide describes VeloCloud Virtual Edge deployment.

This chapter includes the following topics:

- [Overview of Virtual Edge](#)
- [Deployment Prerequisites](#)
- [Special Considerations for VeloCloud Virtual Edge deployment](#)
- [Overview of cloud-init](#)
- [Install Virtual Edge on KVM](#)
- [Install Virtual Edge on VMware ESXi](#)

## Overview of Virtual Edge

The Virtual Edge is available as a virtual machine that can be installed on standard hypervisors.

The following sections provide information on how to install the Virtual Edge on KVM and VMware ESXi hypervisors.

## Deployment Prerequisites

This section describes deployment prerequisites and instance requirements.

## Virtual Edge Requirements

Keep in mind the following requirements before you deploy Virtual Edge:

- 2 x Intel vCPUs.
- AES-NI CPU capability must be passed to the Virtual Edge appliance.
- 4Gb of memory.
- Virtual disk (approximately 8 Gb of disk space).
- 3 to 8 vNICs (default is 2 x L2 interfaces and 6 x L3 interfaces).

---

**Note** Over-subscription of Virtual Edge resources such as CPU, memory, and storage, is not supported.

---

## Firewall/NAT Requirements

If the VeloCloud Virtual Edge is deployed behind the Firewall and/or a NAT device, the following requirements apply:

- The Firewall must allow outbound traffic from the VeloCloud Virtual Edge to TCP/443 (for communication with the VeloCloud Orchestrator).
- The Firewall must allow traffic outbound to Internet on ports UDP/2426 (VCMP).

## Special Considerations for VeloCloud Virtual Edge deployment

Describes the special considerations for VeloCloud Virtual Edge deployment.

- The VeloCloud Edge is a latency-sensitive application. Refer to the [VMware documentation](#) to adjust the Virtual Machine (VM) as a latency-sensitive application.
- Recommended Host settings:
  - BIOS settings to achieve highest performance:
    - CPUs at 2.0 GHz or higher
    - Enable Intel Virtualization Technology (Intel VT)
    - Disable hyperthreading
    - Virtual Edge supports paravirtualized vNIC VMXNET 3 and passthrough vNIC SR-IOV:
      - When using VMXNET3, disable SR-IOV on host BIOS and ESXi
      - When using SR-IOV, enable SR-IOV on host BIOS and ESXi
      - To enable SR-IOV on VMware and KVM, see:
        - KVM - [Enable SR-IOV on KVM](#)
        - VMware - [Enable SR-IOV on VMware](#)
  - Disable power savings on CPU BIOS for maximum performance
  - Enable CPU turbo
  - Enable AES-NI, SSE3, SSE4, and RDTSC instruction sets
  - Recommend reserving 2 cores for Hypervisor workloads
 

For example, for a 10-core CPU system, recommend running one 8-core virtual edge or two 4-core virtual edge and reserve 2 cores for Hypervisor processes.
- For a dual socket host system, make sure the hypervisor is assigning network adapters, memory and CPU resources that are within the same socket (NUMA) boundary as the vCPUs assigned.

- Recommended VM settings:
  - 2, 4, or 8 CPUs (dedicated)
  - 4 GB RAM for a 2 Core VM, 8 GB RAM for a 4 or 8 Core VM
  - Memory should be set to '100% reserved'
- The default username for the VCE ssh console: root

## Overview of cloud-init

This section provides an overview of the cloud-init package.

### About cloud-init

Cloud-init is a Linux package responsible for handling 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. This mode of installation requires two files, meta-data and user-data.

Cloud-init's behavior can be configured via user-data. User-data can be given by the user at the time of launching the instance. 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 Virtual Edge supports cloud-init and all essential configurations packaged in an ISO image.

## Create the cloud-init meta-data and user-data Files

---

**Note** This section has been updated for the 3.3.0 release.

---

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 name it `meta-data`. This file provides information that identifies the instance of the VeloCloud Virtual Edge being installed. The instance-id can be any identifying name, and the local-hostname should be a host name that follows your site standards.

- 1 Create the meta-data file that contains the instance name. `instance-id: vedge1` `local-hostname: vedge1`
- 2 Create the `network-config` file that contains the WAN configuration. Only WAN interfaces that require static IP addressing need to be specified here. By default, all VCE WAN interfaces are configured for DHCP. Multiple interfaces can be specified.

```
version: 1
config:
  - type: physical
    name: GE3
    subnets:
```

```

- type: static
  address: 10.1.0.2
  netmask: 255.255.255.0
  gateway: 10.1.0.1

```

- 3 Create the user-data file. This file contains three main modules: VCO, Activation Code, and Ignore Certificates Errors.

Module	Description
vco	IP Address/URL of the VCO.
activation_code	Activation code for the Virtual Edge. The activation code is generated while creating an Edge instance on the VCO.
vco_ignore_cert_errors	Option to verify or ignore any certificate validity errors.

The activation code is generated while creating an Edge instance on the VCO.

**Important** There is no default password in VCE image. The password must be provided in cloud-config:

```

#cloud-config
password: password
chpasswd: { expire: False }
ssh_pwauth: True
velocloud:
  vce:
    vco: 10.32.0.3
    activation_code: F54F-GG4S-XGFI
    vco_ignore_cert_errors: true

```

## Create the 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 seed.iso in the example below), is created with the following command on Linux system:

```
genisoimage -output seed.iso -volid cidata -joliet -rock user-data meta-data network-config
```

Including network-config is optional. If the file is not present, the DHCP option will be used by default.

Once the ISO image is generated, transfer the image to a datastore on the host machine.

## Install Virtual Edge on KVM

This section describes how to install and activate the Virtual Edge on KVM using a cloud-init config file. The cloud-init config contains interface configurations and the activation key of the Edge. The Virtual Edge has been tested on host OS Ubuntu 14.04.LTS with KVM version 2.0.

KVM provides multiple ways to provide networking to virtual machines. VeloCloud recommends the following options:

- SR-IOV
- Linux Bridge
- OpenVSwitch Bridge

If you decide to use SR-IOV mode, enable SR-IOV on KVM. For steps, see [Enable SR-IOV on KVM](#):

To install VeloCloud Virtual Edge on KVM, see [Install a Virtual Edge on KVM](#).

## Considerations

KVM provides multiple ways to provide networking to virtual machines. The following have been used by VeloCloud:

- SR-IOV
- Linux Bridge
- OpenVSwitch Bridge

## Enable SR-IOV on KVM

To enable SR-IOV on KVM, perform the following steps.

If you don't have Virtual Functions, but you have a NIC that supports Virtual Functions, you will need to enable it.

- 1 Enable SR-IOV in BIOS.

This will be dependent on your BIOS. Login to the BIOS console and look for SR-IOV Support/DMA. You can verify support on prompt by checking that Intel has the correct CPU flag.

```
cat /proc/cpuinfo | grep vmx
```

- 2 Add the Options on Boot (in /etc/default/grub).

```
GRUB_CMDLINE_LINUX="intel_iommu=on"
```

- a After this, run the following commands:

```
update-grub
update-initramfs -u
```

- b Reboot and make sure iommu is enabled.

```
velocloud@KVMperf3:~$ dmesg | grep -i IOMMU
```

```
[ 0.000000] Command line: BOOT_IMAGE=/vmlinuz-3.13.0-107-generic root=/dev/mapper/qa--
multiboot--002--vg-root ro intel_iommu=on splash quiet vt.handoff=7
[ 0.000000] Kernel command line: BOOT_IMAGE=/vmlinuz-3.13.0-107-generic root=/dev/mapper/qa--
multiboot--002--vg-root ro intel_iommu=on splash quiet vt.handoff=7
```

```
[ 0.000000] Intel-IOMMU: enabled
[ 0.083191] dmar: IOMMU 0: reg_base_addr fbffc000 ver 1:0 cap d2078c106f0466 ecap f020de
[ 0.083197] dmar: IOMMU 1: reg_base_addr c7ffc000 ver 1:0 cap d2078c106f0466 ecap f020de
velocloud@KVMperf3:~$
```

- 3 Add the ixgbe Driver in Linux by clicking the link below. <https://downloadcenter.intel.com/download/14687/Intel-Network-Adapter-Driver-for-PCIe-Intel-10-Gigabit-Ethernet-Network-Connections-Under-Linux->
  - a On the left section of the Intel website ( **Other Versions** section), click the **5.2.1** link.
  - b Download ixgbe from Intel. Follow compile options.
  - c Configure ixgbe config (tar and sudo make install).

```
velocloud@KVMperf1:~$ cat /etc/modprobe.d/ixgbe.conf
```

- d If the file doesn't exist, create it.

```
options ixgbe max_vfs=32,32
options ixgbe allow_unsupported_sfp=1
options ixgbe MDD=0,0
blacklist ixgbev
```

- e Execute the following command and reboot:

```
update-initramfs -u
```

- f Use modinfo to see if it is property installed.

```
velocloud@KVMperf1:~$ modinfo ixgbe and ip link
filename: /lib/modules/4.4.0-62-generic/updates/drivers/net/ethernet/intel/ixgbe/ixgbe.ko
version: 5.0.4
license: GPL
description: Intel(R) 10GbE PCI Express Linux Network Driver
author: Intel Corporation, <linux.nics@intel.com>
srcversion: BA7E024DFE57A92C4F1DC93
```

After rebooting the VM, you should see the interfaces.

To properly validate that SR-IOV is ready to be used:

- Verify this by running:

```
lspci | grep -i ethernet
```

- Verify that you have Virtual Functions:

```
01:10.0 Ethernet controller: Intel Corporation 82599 Ethernet Controller Virtual Function (rev 01)
```

## Install a Virtual Edge on KVM

These steps explain how to run VeloCloud Virtual Edge on KVM using the libvirt. This deployment was tested in Ubuntu 14.04LTS.



To run VeloCloud Virtual Edge on KVM using the libvirt:

- 1 Use gunzip to extract the qcow2 file to the image location (for example, /var/lib/libvirt/images).
- 2 Create the Network pools that you are going to use for the device. Provided below sample on pool using SR-IOV and pool using OpenVswitch.

## SR-IOV Sample

```
<network>
  <name>sriovpool</name> <!--This is the name of the file you created-->
  <forward mode='hostdev' managed='yes'>
    <pf dev='eth1' /> <!--Use the netdev name of your SR-IOV devices PF here-->
  </forward >
</network>
```

## OpenVSwitch Sample

```
<network>
  <name>passthrough</name>
  <model type='virtio' />
  <forward mode="bridge" />
  <bridge name="passthrough" />
  <virtualport type='openvswitch'>
</virtualport>
  <vlan trunk='yes'>
  <tag id='33' nativeMode='untagged' />
  <tag id='200' />
  <tag id='201' />
  <tag id='202' />
</vlan>
</network>
Bridge
<network>
  <name>passthrough</name>
  <model type='virtio' />
  <forward mode="bridge" />
</network>
<domain type='kvm'>
  <name>vedge1</name>
  <memory unit='KiB'>4194304</memory>
  <currentMemory unit='KiB'>4194304</currentMemory>
  <vcpu placement='static'>2</vcpu>
  <resource>
  <partition>/machine</partition>
</resource>
  <os>
  <type arch='x86_64' machine='pc-i440fx-trusty'>hvm</type>
  <boot dev='hd' />
</os>
  <features>
  <acpi />
  <apic />
```

```

<pae/>
</features>
<!--
Set the CPU mode to host model to leverage all the available features on the host CPU
-->
<cpu mode='host-model'>
<model fallback='allow'/>
</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>
<!--
Below is the location of the qcow2 disk image
-->
<disk type='file' device='disk'>
<driver name='qemu' type='qcow2'/>
<source file='/var/lib/libvirt/images/edge-VC_KVM_GUEST-x86_64-2.3.0-18- R23-20161114-GA-updatable-
ext4.qcow2'/>
<target dev='sda' bus='sata'/>
<address type='drive' controller='0' bus='0' target='0' unit='0'/>
</disk>
<!--
If using cloud-init to boot up virtual edge, attach the 2nd disk as CD-ROM
-->
<disk type='file' device='cdrom'>
<driver name='qemu' type='raw'/>
<source file='/home/vcadmin/cloud-init/vedge1/seed.iso'/>
<target dev='sdb' bus='sata'/>
<readonly/>
<address type='drive' controller='1' bus='0' target='0' unit='0'/>
</disk>
<controller type='usb' index='0'>
<address type='pci' domain='0x0000' bus='0x00' slot='0x01' function='0x2'/>
</controller>
<controller type='pci' index='0' model='pci-root'/>
<controller type='sata' index='0'>
<address type='pci' domain='0x0000' bus='0x00' slot='0x05' function='0x0'/>
</controller>
<controller type='ide' index='0'>
<address type='pci' domain='0x0000' bus='0x00' slot='0x01' function='0x1'/>
</controller>
<!--
The first two interfaces are for the default L2 interfaces, NOTE VLAN support just for SR-I/OV and
OpenvSwitch
-->
< interfacetype='network'>
< modeltype='virtio'/>
< sourcenetwork='LAN1'/>
< vlan>< tagid='#hole2_vlan#'></ vlan>
< aliasname=LAN1/>
< addresstype='pci' domain='0x0000' bus='0x00' slot='0x12' function='0x0'/>
</ interface>

```

```

< interfacetype='network'>
< modeltype='virtio' />
< sourcenetwork=LAN2 />
< vlan>< tagid='#LAN2_VLAN#' /></ vlan>
< aliasname='hostdev1' />
< addresstype='pci' domain='0x0000' bus='0x00' slot='0x13' function='0x0' />
</ interface>

```

```
<!--
```

The next two interfaces are for the default L3 interfaces. Note that additional 6 routed interfaces are supported for a combination of 8 interfaces total

```
-->
```

```

< interfacetype='network'>
< modeltype='virtio' />
< sourcenetwork=WAN1 />
< vlan>< tagid='#hole2_vlan#' /></ vlan>
< aliasname=LAN1 />
< addresstype='pci' domain='0x0000' bus='0x00' slot='0x12' function='0x0' />
</ interface>
< interfacetype='network'>
< modeltype='virtio' />
< source network=LAN2 />
< vlan>< tag id='#LAN2_VLAN#' /></ vlan>
< aliasname='hostdev1' />
< addresstype='pci' domain='0x0000' bus='0x00' slot='0x13' function='0x0' />
</ interface>
<serial type='pty'>
<target port='0' />
</serial>
<console type='pty'>
<target type='serial' port='0' />
</console>
<input type='mouse' bus='ps2' />
<input type='keyboard' bus='ps2' />
<graphics type='vnc' port='-1' autoport='yes' listen='127.0.0.1'>
<listen type='address' address='127.0.0.1' />
</graphics>
<sound model='ich6'>
<address type='pci' domain='0x0000' bus='0x00' slot='0x04' function='0x0' />
</sound>
<video>
<model type='cirrus' vram='9216' heads='1' />
<address type='pci' domain='0x0000' bus='0x00' slot='0x02' function='0x0' />
</video>
<memballoon model='virtio'>
<address type='pci' domain='0x0000' bus='0x00' slot='0x06' function='0x0' />
</memballoon>
</devices>
</domain>

```

## Instructions

- 1 Save the above domain XML file (for example, vedge1.xml).

- 2 Run the following command to create the VM:

```
virsh define vedge1.xml
```

- 3 Run the following command to start the VM:

```
virsh start vedge1
```

---

**Note** `vedge1` is the name of the VM defined in the `<name>` element of the domain XML file. Replace `vedge1` with the name you specify in the `<name>` element.

---

The Cloud-init already includes the activation key, which was generated while creating a new Virtual Edge on the VCO. The Virtual Edge is configured with the config settings from the Cloud-init file. This will configure the interfaces as the Virtual Edge is powered up. Once the Virtual Edge is online, it will activate with the VCO using the activation key. The VCO IP address and the activation key have been defined in the Cloud-init file.

## Install Virtual Edge on VMware ESXi

This section describes how to install and activate the Virtual Edge on VMware ESXi using a cloud-init config file. The cloud-init config contains interface configurations and the activation key of the Edge.

KVM provides multiple ways to provide networking to virtual machines. VeloCloud recommends the following options:

- SR-IOV
- Linux Bridge
- OpenVSwitch Bridge

If you decide to use SR-IOV mode, enable SR-IOV on VMware ESXi. For steps, see [Enable SR-IOV on VMware](#):

To install VeloCloud Virtual Edge on VMware ESXi, see [Installing a Virtual Edge on VMware ESXi](#).

### Enable SR-IOV on VMware

This section describes how to enable SR-IOV on VMware. This step is optional, but it is necessary to realize the full benefit of DPDK to improve packet processing performance.

#### Prerequisites

This requires a specific NIC card. As of today, only the following chipset is certified by VeloCloud to work with the VCG.

- Intel 82599/82599ES
- X550 (under experimenting as this requires the latest Intel ixgbevf driver on the VCG VM and Malicious Driver Detection disabled on the ESXi host ixgbe driver)

## Instructions to Enable SR-IOV

To enable SR-IOV on VMware:

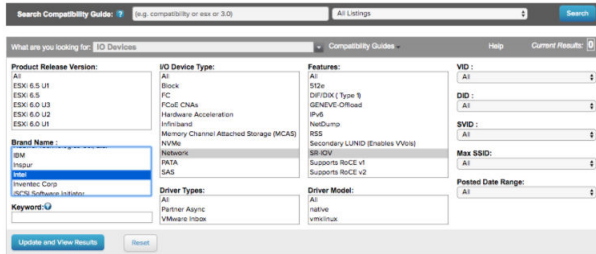
- 1 Make sure that your NIC card supports SR-IOV. Check the VMware Hardware Compatibility List (HCL) at <https://www.vmware.com/resources/compatibility/search.php?deviceCategory=io>

**Brand Name:** Intel

**I/O Device Type:** Network

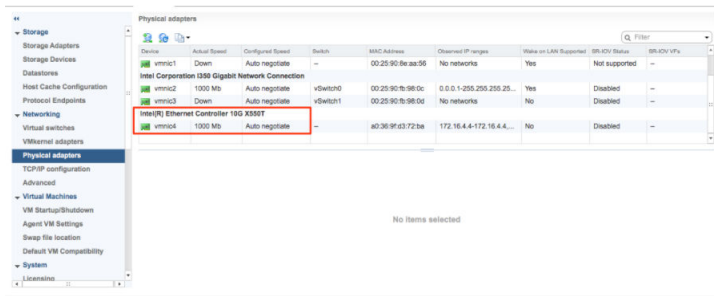
**Features:** SR-IOV

### VMware Compatibility Guide

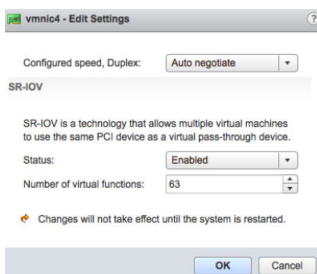


The following VMware KB article provides details of how to enable SR-IOV on the supported NIC: <https://kb.vmware.com/s/article/2038739>

- 2 Once you have a support NIC card, go to the specific VMware host, select the **Configure** tab, and then choose **Physical adapters**.



- 3 Select **Edit Settings**. Change **Status** to **Enabled** and specify the number of virtual functions required. This number varies by the type of NIC card.
- 4 Reboot the hypervisor.



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

Physical adapters

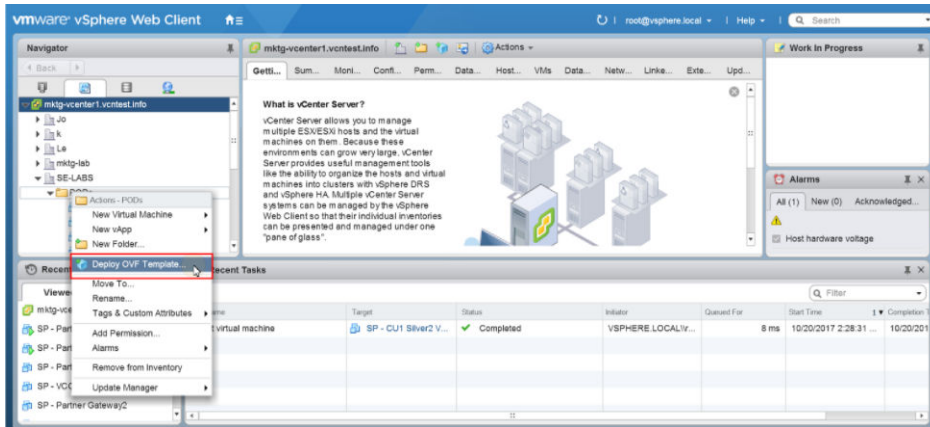
Device	Actual Speed	Configured Speed	Switch	MAC Address	Observed IP ranges	Wake on LAN Supported	SR-IOV Status	SR-IOV VFs
Intel(R) Ethernet Controller 10G X550T								
vmnic4	1000 Mb	Auto negotiate	--	80:35:3F:d3:72:ba	172.16.4.4-172.16.4.4	No	Enabled	63 (61 currently)
Intel Corporation I350 Gigabit Network Connection								
vmnic2	1000 Mb	Auto negotiate	vSwitch0	00:25:90:fb:98:0c	0.0.0.1-255.255.255.25...	Yes	Disabled	--
vmnic3	1000 Mb	Auto negotiate	vSwitch1	00:25:90:fb:98:0d	No networks	No	Disabled	--
GLLogic Corporation NetXtreme II BCM57810 10 Gigabit Ethernet								
vmnic0	Down	Auto negotiate	--	00:25:90:8e:aa:54	No networks	Yes	Not supported	--

## Installing a Virtual Edge on VMware ESXi

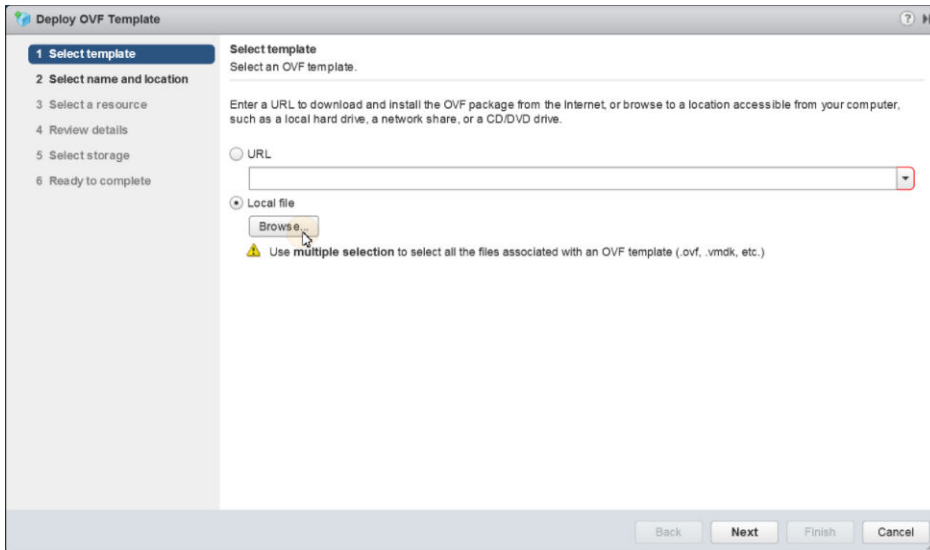
Describes how to install a Virtual Edge on VMware ESXi.

To install:

- Use the vSphere client to deploy an OVF template, and then select the VCE OVA file.

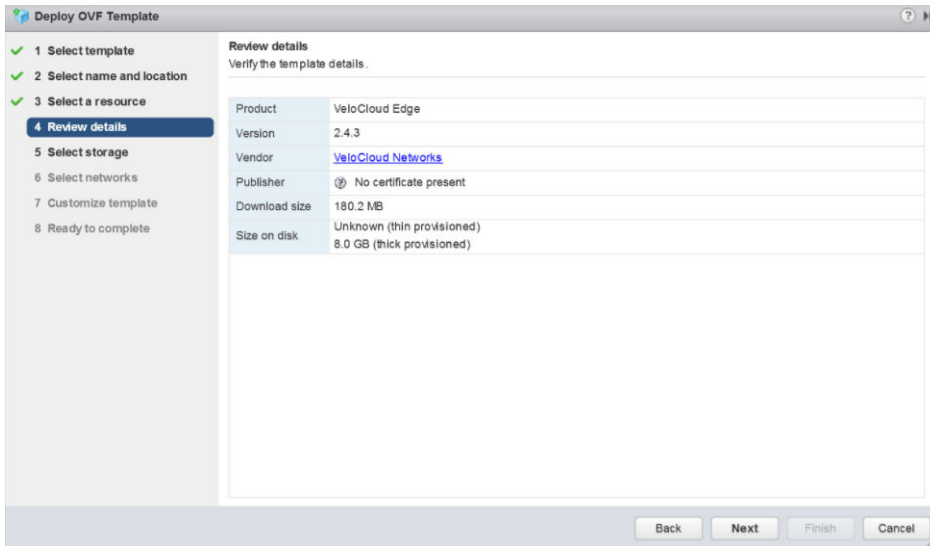


- Select an OVF template from an URL or Local file.

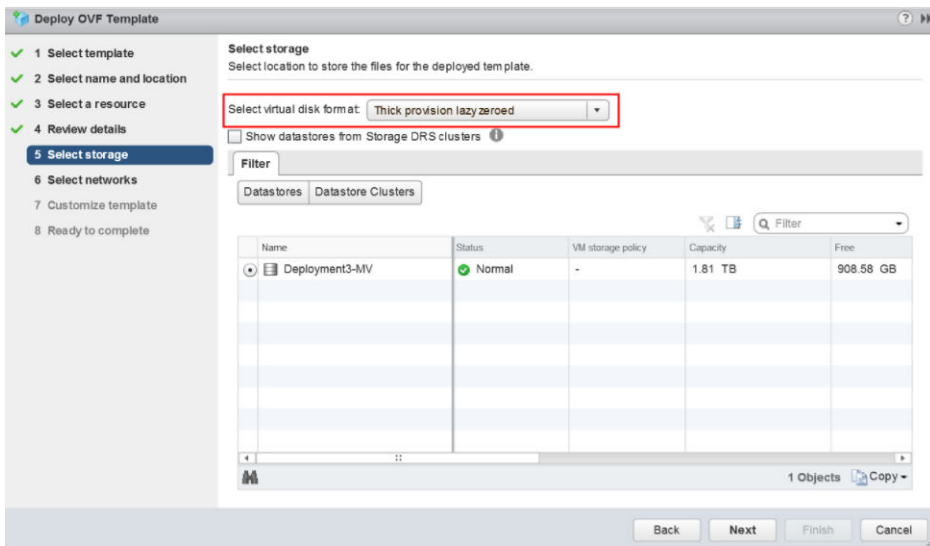


- Select a name and location of the virtual machine.
- Select a resource.

5 Verify the template details.

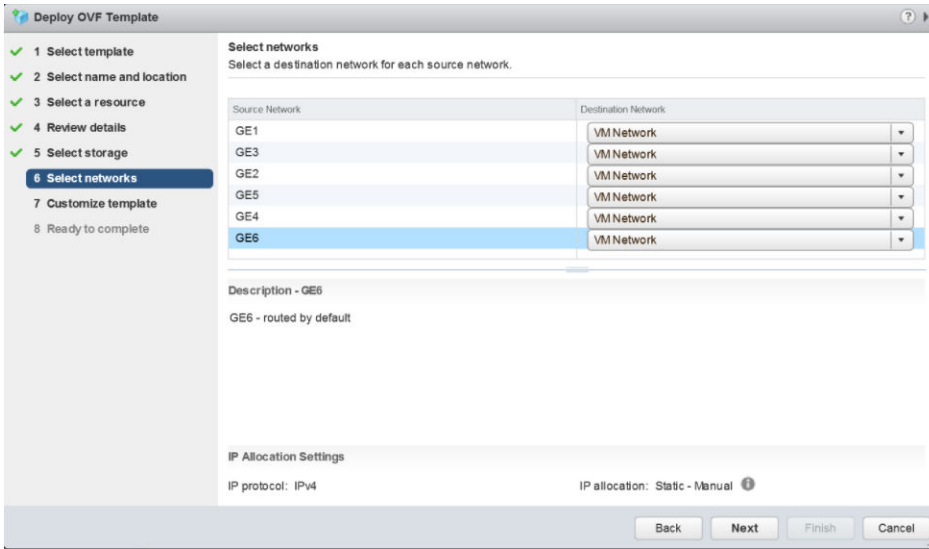


6 Select the storage location to store the files for the deployment template.

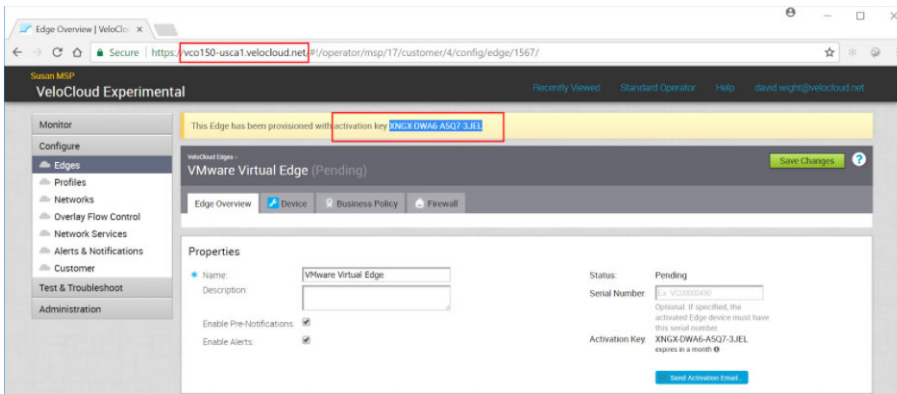


7 Configure the networks for each of the interfaces.

**Note** Skip this step if you are using a cloud-init file to provision the Virtual Edge on ESXi.

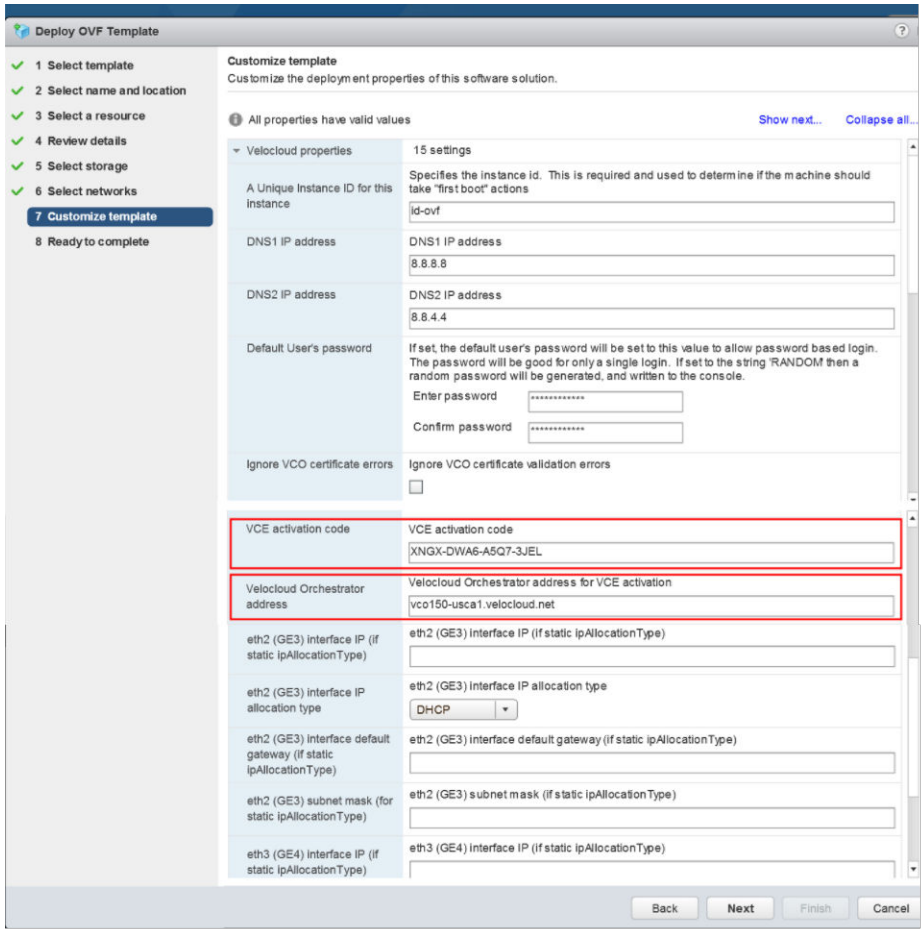


- 8 Customize the template by specifying the deployment properties. See the image below of the VCO that highlights the following substeps.
  - a From the VCO UI, retrieve the VCO URL/IP Address. You will need this address for Step c below.
  - b Create a new Virtual Edge on the VCO for the Enterprise. Once the Edge is created, copy the Activation Key. You will need the Activation Key for Step c" below.

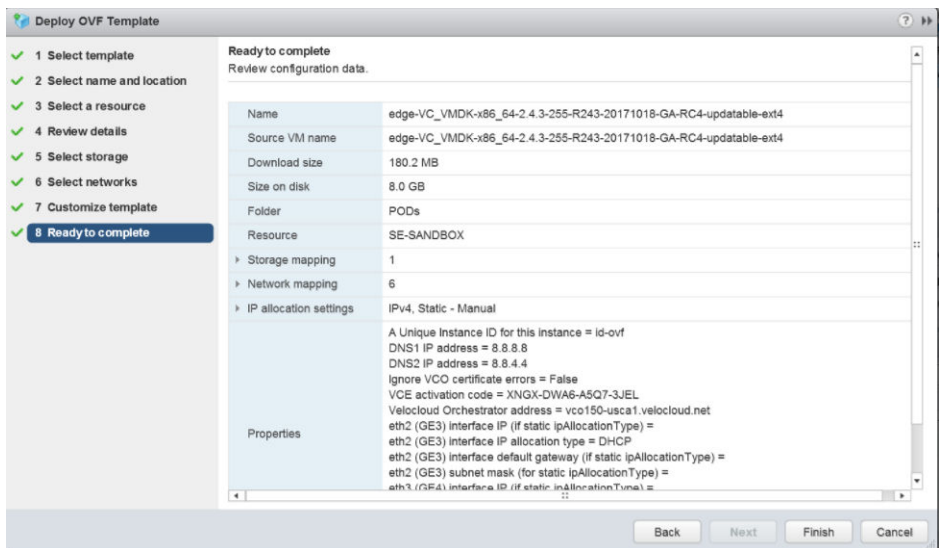


- c On the customize template page shown in the image below, type in the Activation Code that you retrieved in Step b above, and the VCO URL/IP Address retrieved in Step a above, into the corresponding fields.

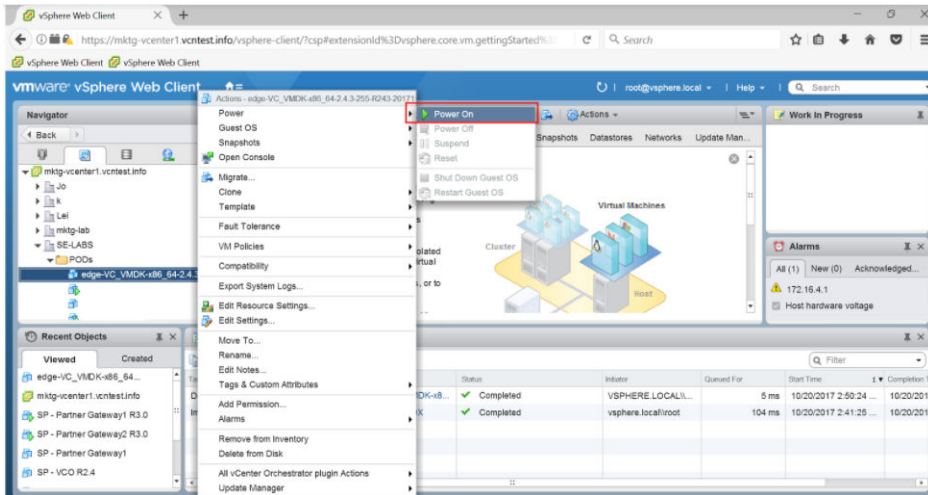




9 Review the configuration data.



10 Power on the Virtual Edge.



Once the Edge powers up, it will establish connectivity to the VCO.

# AliCloud Virtual Edge Deployment Guide

# 23

This document provides instructions for AliCloud Virtual Edge deployment.

This chapter includes the following topics:

- [AliCloud vVCE Deployment Overview](#)
- [Topology A - Virtual Edge Deployment on AliCloud VPC](#)
- [Topology B - Virtual Edge Deployment on AliCloud Single-Arm Topology](#)
- [Create a Virtual Private Cloud](#)
- [Create a VSwitch](#)
- [Create a Security Group](#)
- [Add Security Group Rules](#)
- [Create Custom Route Tables and Associate VSwitches](#)
- [Provision an Edge on the VCO](#)
- [Create an Elastic Network Interface](#)
- [Create Elastic IP and Assign it to Public Interface of the Edge](#)
- [Bind an ENI to an Edge instance](#)
- [Create a LAN Instance](#)
- [Add a Custom Route Table Entry](#)
- [Create a Jump Host Instance](#)
- [SSH Login to Edge using EIP](#)
- [SSH to Private IP of the Edge from Jump Host](#)
- [Activate the Edge Against the VCO](#)

## AliCloud vVCE Deployment Overview

More customers are moving workload to Public Cloud infrastructure and expect to extend SD-WAN from remote sites to public cloud to guarantee SLA. There are multiple options offered by

VeloCloud, leveraging distributed VCGs to establish IPsec towards public cloud private network or deploy virtual edge directly in AliCloud.

This document illustrates the high-level workflow of the following two topologies to deploy a virtual VeloCloud Edge (vVCE) on AliCloud:

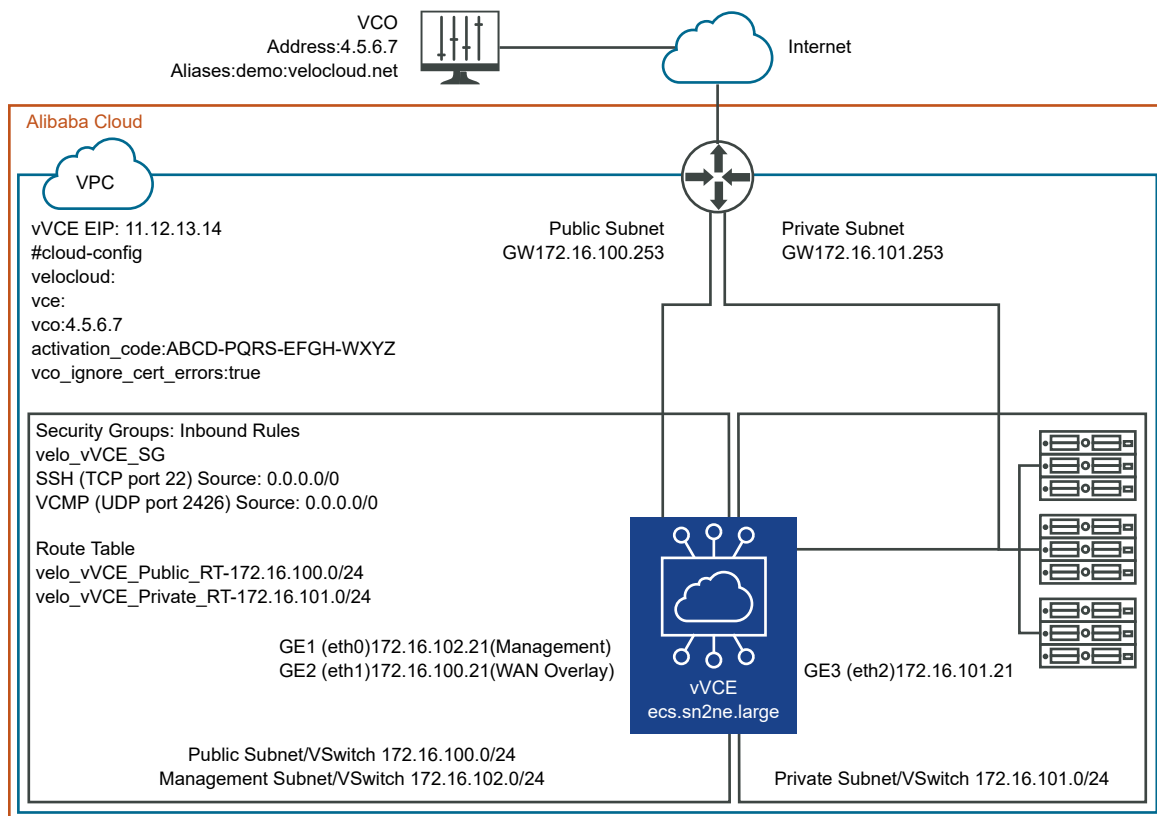
- [Topology A - Virtual Edge Deployment on AliCloud VPC](#)
- [Topology B - Virtual Edge Deployment on AliCloud Single-Arm Topology](#)

## Prerequisites

- Ensure you have an Alibaba Cloud account and login information for the Alibaba Cloud Console.
- Ensure you have the VCO host name and admin account to login.

## Topology A - Virtual Edge Deployment on AliCloud VPC

Describes the Virtual Edge deployment on the AliCloud Virtual Private Cloud (VPC) with three VSwitches, each for a subnet connected to the Edge as shown in the following topology diagram.



## High-Level Workflow

To deploy a VeloCloud Virtual Edge on [Alibaba Cloud ECS](#), perform the following steps:

- 1 Create a Virtual Private Cloud (VPC). For steps, see [Create a Virtual Private Cloud](#).
- 2 Create three VSwitches, each for a subnet connected to the Edge as shown in the topology diagram. For steps, see [Create a VSwitch](#).
  - Management Subnet/VSwitch for console/management access to the Edge through Management Interface GE1.
  - Public Subnet/VSwitch for Internet access from the Edge through WAN-side Interface GE2.
  - Private Subnet/VSwitch for LAN-side device access through LAN-side Interface GE3.
- 3 Create a Security Group (velo\_vVCE\_SG) and add inbound rules. For steps, see [Create a Security Group](#).
- 4 Create two custom (secondary) route tables (Velo\_vVCE\_Public\_RT and Velo\_vVCE\_Private\_RT) and associate it with the respective VSwitches (Public and Private). For steps, see [Create Custom Route Tables and Associate VSwitches](#).
- 5 Provision a VeloCloud Edge (VCE) on the VeloCloud Orchestrator (VCO) as follows:
  - a Create an edge of type **Virtual Edge**.
  - b Change GE2 interface to **Routed** from **Switched**.
  - c Disable **WAN Overlay** for GE3 interface and **NAT Direct Traffic**, which will be the next hop for devices connected to Private Subnets (LAN devices).
  - d Add JH IP in firewall SSH access list.

For more information, see [Provision an Edge on the VCO](#).
- 6 Create and launch a virtual VeloCloud Edge (vVCE) instance with Management Interface (GE1). For steps, see [Create a vVCE Instance on the ECS Console](#).
- 7 Create two Elastic Network Interfaces (ENIs): one Private LAN-side interface (GE3) and another Public WAN-side interface (GE2). For steps, see [Create an Elastic Network Interface](#).
- 8 Create an Elastic IP and assign it to the Public Interface (GE2) of the Edge. For steps, see [Create Elastic IP and Assign it to Public Interface of the Edge](#).
- 9 Bind the Public (GE2) and Private (GE3) interfaces to the Edge instance (vVCE) and then restart the Edge instance to make sure the interfaces are connected to the Edge. For steps, see [Bind an ENI to an Edge instance](#).

The Edge instance will be activated against the VCO and the Edge will be able to establish the VCMP tunnel to the Gateway.

10 (Optional) Within the VPC, if you want to access your Edge from a Private subnet, not over the Internet, then you have to create a Jump Host (JH) instance (Linux instance) with one interface in Public subnet for Internet connectivity with EIP and the other interface in Management subnet, over which the Edge will be accessed. For steps, see [Create a Jump Host Instance](#).

- a Create a Jump Host.
- b Create an EIP and bind it to the Jump Host Instance.

---

**Note** VCAdmin users will be able to access the Edge over Management subnet interface from JH.

---

- c Login to the virtual Edge (vVCE) from Jump Host.
- d Activate the Edge Against the VCO from Shell.

---

**Note** After the Edge activation starts, if you want to SSH to the Edge from a Private subnet then you must ensure to add the JH IP in the firewall SSH access list.

---

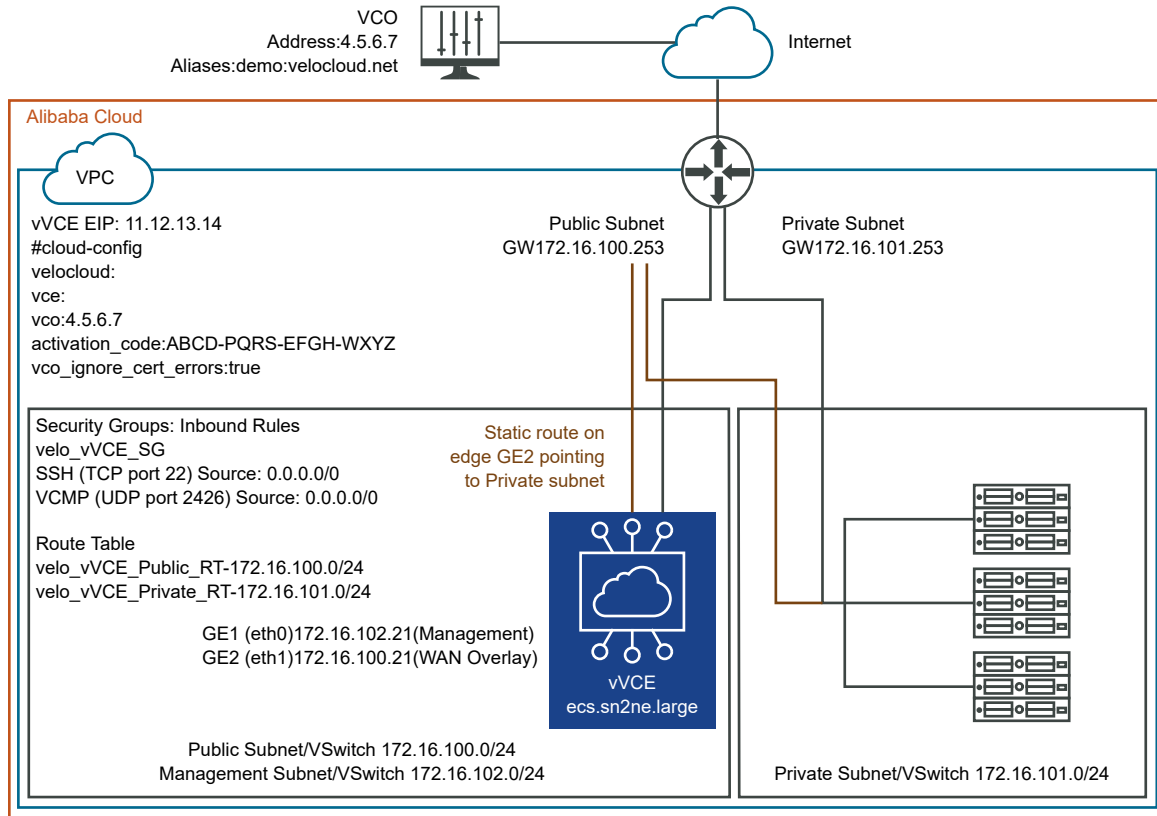
11 Create a LAN instance with the Primary interface connected to Private subnet. For steps, see [Create a LAN Instance](#).

- a In the Private routing table (Velo\_vVCE\_Private\_RT), create a new route entry that points to GE3 interface of edge for default route. For steps, see [Add a Custom Route Table Entry](#).

12 Verify if the virtual Edge (vVCE) is up in the VCO.

## Topology B - Virtual Edge Deployment on AliCloud Single-Arm Topology

Describes the Virtual Edge deployment on the AliCloud Virtual Private Cloud (VPC) with three VSwitches, each for a subnet connected to the Edge as shown in the following Single-Arm topology diagram.



## High-Level Workflow

To deploy a VeloCloud Virtual Edge on [Alibaba Cloud ECS](#), perform the following steps:

- 1 Create a Virtual Private Cloud (VPC). For steps, see [Create a Virtual Private Cloud](#).
- 2 Create three VSwitches, each for a subnet connected to the Edge as shown in the topology diagram. For steps, see [Create a VSwitch](#).
  - Management Subnet/VSwitch for console/management access to the Edge through Management Interface GE1.
  - Public Subnet/VSwitch for Internet access from the Edge through WAN-side Interface GE2.
  - Private Subnet/VSwitch for LAN-side device access through LAN-side Interface GE3.
- 3 Create a Security Group (velo\_vVCE\_SG) and add inbound rules. For steps, see [Create a Security Group](#).
- 4 Provision a VeloCloud Edge (VCE) on the VeloCloud Orchestrator (VCO) as follows:
  - a Create an edge of type **Virtual Edge**.
  - b Change GE2 interface to **Routed** from **Switched**.
  - c Add a static route on the Edge that points to the Private Subnet/VSwitch.
  - d Add JH IP in firewall SSH access list.

For more information, see [Provision an Edge on the VCO](#).

- 5 Create and launch a virtual VeloCloud Edge (vVCE) instance with Management Interface (GE1). For steps, see [Create a vVCE Instance on the ECS Console](#).
- 6 Create a public Elastic Network Interface (GE2) on the WAN side. For steps, see [Create an Elastic Network Interface](#).
- 7 Create an Elastic IP and assign it to the Public Interface (GE2) of the Edge. For steps, see [Create Elastic IP and Assign it to Public Interface of the Edge](#).
- 8 Bind the Public (GE2) interface to the Edge instance (vVCE) and then restart the Edge instance to make sure the interface is connected to the Edge. For steps, see [Bind an ENI to an Edge instance](#).

The Edge instance will be activated against the VCO and the Edge will be able to establish the VCMP tunnel to the Gateway.

- 9 Login to the Edge using the EIP and verify Edge activation.
- 10 Create a LAN instance with the Primary interface connected to the Management subnet. For steps, see [Create a LAN Instance](#).
  - a In the Primary routing table, create a new route entry that points to GE2 interface of edge for default route. For steps, see [Add a Custom Route Table Entry](#).
- 11 Verify if the virtual Edge (vVCE) is up in the VCO.

## Create a Virtual Private Cloud

A Virtual Private Cloud (VPC) is a virtual private network in which you can deploy your cloud resources. The Cloud resources cannot be directly deployed in a VPC. They must be deployed in a VSwitch (subnet) of the VPC.

### Prerequisites

Ensure you have an AliCloud account and login information.

### Procedure

- 1 Log on to the [VPC console](#).
- 2 Select the region in which you want to create a VPC.
 

The VPC must be in the same region as the cloud resources that you want to deploy.
- 3 In the left navigation pane, click **VPCs**.



- 4 On the **VPC** page, click **Create VPC**.

The **Create VPC** page appears.

### Create VPC

---

**VPC**

**Region**  
India (Mumbai)

**Name** ?

Velo\_demo\_VPC 13/128 ✓

**IPv4 CIDR Block** ?

Default CIDR Block  
 Custom CIDR Block

192.168.0.0/16 ▼

ⓘ The CIDR cannot be changed once the VPC is created.

**Description** ?

0/256

---

OK Cancel

- 5 On the **Create VPC** page, set the following parameters, and then click **OK**.
- a In the **Name** text box, enter the name for the VPC.
  - b Under **IPv4 CIDR Block**, select one of the following options:
    - **Default CIDR Block:** Select 192.168.0.0/16, 172.16.0.0/12, or 10.0.0.0/8.
    - **Custom CIDR Block:** Select 192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8, or their subnets. The CIDR block mask must be 8 to 24 bits in length.

During VPC creation itself, you can create one or more VSwitches by clicking the **+ Add** button. For more information about creating a VSwitch, see [Create a VSwitch](#).

---

**Note** After the VPC is created, you cannot change its IPv4 CIDR block.

---

What to do next

- [Create a VSwitch](#)

## Create a VSwitch

A VSwitch is a basic network device of a VPC and used to connect different cloud product instances. After creating a VPC, you can further segment your virtual private network to one or

more subnets by creating VSwitches. The VSwitches within a VPC are interconnected. Therefore, you can deploy different applications in the different VSwitches of different zones to improve the service availability.

### Prerequisites

Ensure that you have already created a VPC.

### Procedure

- 1 Log on to the [VPC console](#).
- 2 In the left-side navigation pane, click **VSwitches**.
- 3 Select the region of the VPC in which you want to create a VSwitch.
- 4 Click **Create VSwitch**.

The **Create VSwitch** page appears.

**Create VSwitch**

**VPC**

**IPv4 CIDR Block**  
 192.168.0.0/16

**Name** ⓘ  
 20/128 ✓

**Zone** ⓘ

**Zone Resource** ⓘ  
 ECS ✓ RDS ✓ SLB ✓

**IPv4 CIDR Block**  
 -  -  -  /

ⓘ The CIDR cannot be changed once the VPC is created.

**Number of Available Private IPs**  
 252

**Description** ⓘ

- 5 On the **Create VSwitch** page, set the following parameters, and then click **OK**.
  - a From the **VPC** drop-down menu, select a VPC to which the VSwitch belongs.
  - b In the **Name** text box, enter the name for the VPC.

- c From the **Zone** drop-down menu, select the zone to which the VSwitch belongs.
- d In the **IPv4 CIDR Block** text box, enter the IPv4 CIDR block of the VSwitch.
  - The IPv4 CIDR block of the VSwitch can be the same as that of the VPC to which the VSwitch belongs or be a subset of the VPC CIDR block.

For example, if the CIDR block of the VPC is 192.168.0.0/16, the CIDR block of the VSwitch in the VPC can be 192.168.0.0/16, or any CIDR block between 192.168.0.0/17 and 192.168.0.0/29.

---

**Note** If the CIDR block of the VSwitch is the same as that of the VPC, you can only create one VSwitch.

---

- The subnet mask of the VSwitch CIDR block can be 16 to 29 bits. It means that the VSwitch can provide 8 to 65,536 IP addresses.
- The first IP address and the last three IP addresses in the VSwitch CIDR block are reserved.

For example, if the VSwitch CIDR block is 192.168.1.0/24, the IP addresses 192.168.1.0, 192.168.1.253, 192.168.1.254, and 192.168.1.255 are reserved.

- If the VSwitch needs to communicate with VSwitches of other VPCs or on-premises data centers, you need to make sure that the CIDR blocks involved do not conflict with each other.

---

**Note** After the VSwitch is created, you cannot change its IPv4 CIDR block.

---

#### What to do next

- [Create a Security Group](#)
- [Add Security Group Rules](#)
- [Create Custom Route Tables and Associate VSwitches](#)

## Create a Security Group

A security group is a virtual firewall for an ECS instance. This topic describes how to create a security group in the ECS console.

#### Prerequisites

If you want to create a VPC-type security group, ensure that a VPC and a VSwitch have been created. For more information, see [Create a Virtual Private Cloud](#) and [Create a VSwitch](#).

#### Procedure

- 1 Log on to the [ECS console](#).
- 2 In the left-side navigation pane, choose **Network & Security** > **Security Groups**.

### 3 On the **Security Groups** page, click **Create Security Group**.

The dialog box appears.

Create Security Group ? Creating security group ×

Template:

\* Security Group Name:   
 The name must be 2 to 128 characters in length and can contain periods (.), underscores (\_), hyphens (-), and colons (:). It cannot start with a special character or digit.

Description:   
 It must be 2 to 256 characters in length and cannot start with "http://" or "https://".

Network Type:

\*VPC:  [Create VPC](#)

Tag:

Inbound  Outbound

Authorization Object	Protocol Type	Port Range	Action

### 4 In the **Create Security Group** dialog box, configure the following parameters:

- From the **Template** drop-down menu, select a suitable template to simplify security group rule configuration. For example, select **Customize**.
- In the **Security Group Name** text box, enter a valid name for the security group.
- From the **Network Type** drop-down menu, select **VPC**.
- From the **VPC** drop-down menu, select your VPC.

### 5 Click **OK**.

A pop-up message recommending you create security group rules appears.

#### Results

After the security group is created, a new security group is added to the security group list.

#### What to do next

After creating a security group, it is recommended to immediately create security group rules. Otherwise, you may not be able to access the internal network or Internet. For steps, see [Add Security Group Rules](#).

## Add Security Group Rules

You can use security group rules to control the access to public or internal networks of the ECS instances in a security group. To add security group rules, perform the steps on this procedure.

### Prerequisites

- Ensure that you have created a security group. For more information, see [Create a Security Group](#).
- Ensure that you know which internal or public network requests need to be allowed or denied for your instance.

### Procedure

- 1 Click **Create Rules Now**.

The **Security Group** page appears.

- 2 Click **Add Security Group Rule**.

The **Add Security Group Rule** dialog box appears.

Add Security Group Rule ⓘ Add security group rules

NIC Type: Internal Network ▼

Rule Direction: Inbound ▼

Action: Allow ▼

Protocol Type: Customized UDP ▼

\* Port Range: 2426/2426 ⓘ

Priority: 1 ⓘ

Authorization Type: IPv4 CIDR Block ▼

\* Authorization Objects: 0.0.0.0/0 ⓘ Tutorial

Description:   
 It must be 2 to 256 characters in length and cannot start with "http://" or "https://".

OK Cancel

- 3 From the **Rule Direction** drop-down menu, select **Inbound**.

By default, all Outbound traffic is allowed.

- 4 From the **Action** drop-down menu, select **Allow**.

- 5 To allow inbound connectivity to your Edge, select **Protocol Type** and **Port Range**.

The port range is based on the protocol type. The following are some of the examples:

- VCMP: UDP port 2426
- SSH: TCP port 22
- SNMP UDP port 161
- ICMP Request/Reply

- 6 Select **Authorization Type** and **Authorization Objects**.

The authorized IP address is based on the authorization type. For example, for IPv4 CIDR block, specifying 0.0.0.0/0 will allow or deny all IP addresses, based on the authorization policy.

- 7 Click **OK**.

### Results

Click the refresh icon to confirm that the security group rule is added. Changes to security group rules are automatically applied to Elastic Compute Service (ECS) instances in the security group.

## Create Custom Route Tables and Associate VSwitches

A route table is a list of route entries in a VPC. The network traffic is routed based on the configurations of the route entries in the route table. After a VPC is created, the system automatically creates a default route table and adds system routes to the route table for traffic management.

You cannot create or delete the default route table. However, you can create a custom route table and associate it with a VSwitch to control the routes of the corresponding subnet. To create a custom route table and associate it with a VSwitch, perform the following steps:

### Prerequisites

Ensure that a VPC and VSwitches have been created. For steps, see [Create a Virtual Private Cloud](#) and [Create a VSwitch](#).

### Procedure

- 1 Log on to the [VPC console](#).
- 2 In the left-side navigation pane, click **Route Tables**.
- 3 Select the region of the route table to be created.

- 4 On the **Route Tables** page, click **Create Route Table**.

The **Create Route Table** page appears.

Create Route Table ✕

---

**VPC**

Velo\_demo\_VPC/vpc-a2da47yffs3rkqxn10hr ▾

**Name**

Velo\_demo\_Private\_RT 20/128

**Description**

0/256

---

OK Cancel

- 5 Configure the following parameters, and then click **OK**.

- a From the **VPC** drop-down menu, select your VPC.
- b In the **Name** text box, enter the name for the routing table.

The route table is created, and it gets added to the list of Route Tables.

- 6 On the **Route Tables** page, select the route table that you have created and then click the **Associated VSwitches** tab.

## 7 Click **Associate VSwitch**.

The **Associate VSwitch** page appears.

Associate VSwitch
✕

---

i The process of binding the route table to the switch is asynchronous. The routing policy matching the resources such as ECS in the switch is gradually replaced with a new routing policy.

**Route Table**

vtb-a2dmkmaqj0rkx2xfre9b/Velo\_demo\_Public\_RT

**• VSwitch**

Velo\_demo\_Public\_SN/vsw-a2d7r065bdwzd9cmrfzcy
▼

- 8 From the **VSwitch** drop-down menu, select the relevant VSwitch to be associated with the Route Table.

### Results

Click **Refresh** to confirm that the VSwitch is associated with the Routing Table.

### What to do next

- [Provision an Edge on the VCO](#)
- [Create a vVCE Instance on the ECS Console](#)

## Provision an Edge on the VCO

To provision a VeloCloud Edge, perform the steps on this procedure.

### Prerequisites

Ensure you have the VCO host name and admin account to login.



## Procedure

- 1 Log in to the VCO application as Admin user, with your login credentials.

The **VCO Home** screen appears.

- 2 Go to **Configure > Edges**. The **VeloCloud Edges** page appears.

- 3 Click **New Edge**.

The **Provision New Edge** dialog box appears.

**Provision New Edge**

\* Name:

\* Model:

\* Profile:

Authentication:

High Availability:

Serial Number:   
 Optional. If specified, the activated Edge device must have this serial number.

\* Contact Name:

\* Contact Email:

Location: ⓘ [Set Location...](#)

- 4 In the **Name** text box, enter a unique name for the Edge.
- 5 From the **Model** drop-down menu, select **Virtual Edge**.
- 6 From the **Profile** drop-down menu, select **Quick Start Profile** and click **Create**.

The Edge is provisioned, and the activation key is displayed on the top of the page. Make a note of the activation key to use it for launching the Edge from the AliCloud Console.

- 7 Configure Virtual Edge interfaces. The following steps are explained considering [Topology A - Virtual Edge Deployment on AliCloud VPC](#).
  - a Click the **Device** tab and go to the **Interface Settings** area.
  - b Click **Edit** corresponding to the **GE2 Interface** and select **Override Interface** checkbox.

- c From the **Capability** drop-down menu, select **Routed** and click **Update GE2**.

**Virtual Edge** ? x

**Interface: GE2** Override Interface

Interface Enabled:

Capability: **Routed**

Segments: **All Segments**

Addressing Type: **DHCP**

IP Address: n.a

CIDR prefix: n.a

Gateway: n.a

WAN Overlay:  **Auto-Detect Overlay**

OSPF:  OSPF not enabled for the selected Segment.

Multicast:  Multicast is not enabled for the selected segment

RADIUS Authentication:  **Require User Authentication to access WAN**  
 WAN Overlay must be disabled to configure RADIUS Authentication.

Advertise:

ICMP Echo Response:

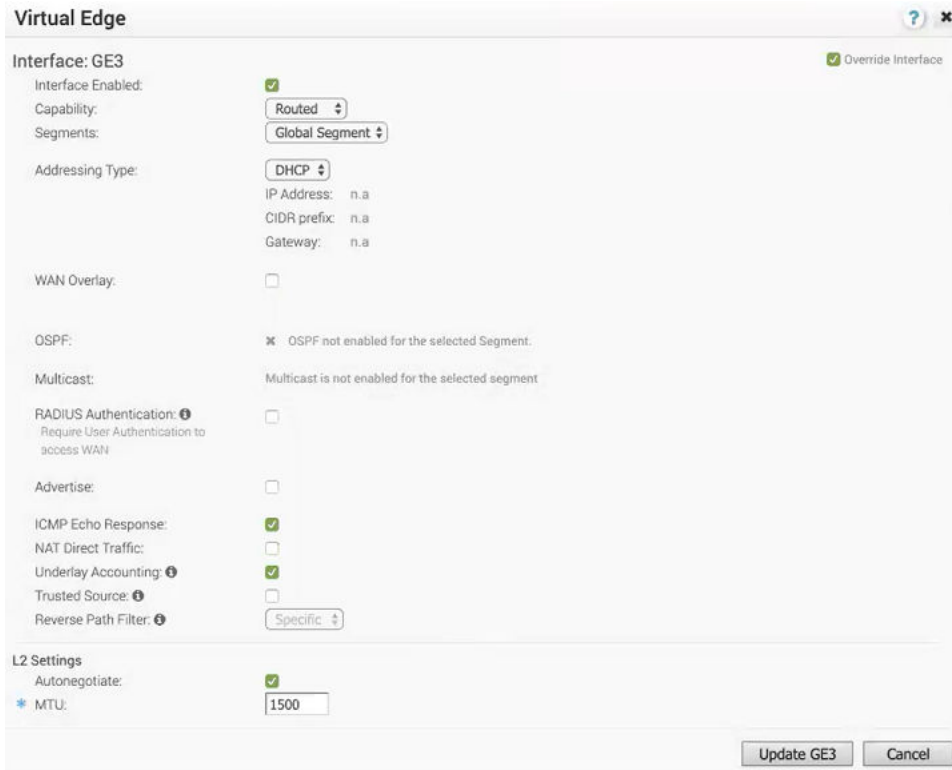
NAT Direct Traffic:

Underlay Accounting:

Trusted Source:

**Update GE2** **Cancel**

- d Click **Edit** corresponding to the **GE3 Interface** and select **Override Interface** checkbox.
- e Disable **WAN Overlay** and **NAT Direct Traffic**, as this interface will be used LAN-side, and Click **Update GE3**.



**Note** If you are using an Edge instance with only two interfaces as illustrated in [Topology B - Virtual Edge Deployment on AliCloud Single-Arm Topology](#), then the public interface (GE2) will be used for both WAN and LAN connectivity. For the LAN network to point to the GE2 interface, under **Static Route Settings**, configure a static route on the Edge that points to the Private Subnet/VSwitch as shown in the following screenshot.

Static Route Settings

* Subnet	Source IP	* Next Hop	* Interface	VLAN	* Cost	Preferred	Advertise	ICMP Probe	Description
192.168.101.0/24	11/a	192.168.100.253	GE2	<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	[none]	Description (Optional)

- 8 Under the **Configure VLAN** area, edit the VLAN settings to update the **Edge LAN IP Address**.
- 9 (Optional) If you are using a Jump Host, to allow SSH access to the Edge from the jump server, make sure to enable the **Support access** for the Jump Host server’s IP in the **Firewall** page.

Edge Access

Support Access

Enable Edge Override

Deny All

Allow the following IPs

172.16.102.213

Separate each IP with a comma (,)

**10** Click **Save Changes**.

## What to do next

- [Create a vVCE Instance on the ECS Console](#)

## Create a vVCE Instance on the ECS Console

Instances are the core components of Elastic Compute Service (ECS). This topic describes how to create a Pay-As-You-Go Edge instance on the ECS console.

## Prerequisites

- Ensure you have an AliCloud account and login information.

## Procedure

- 1 Log on to the [ECS console](#).
- 2 In the left-side navigation pane, click **Instances & Images > Instances**.
- 3 On the **Instances** page, click **Create Instance**.  
The **Custom Launch** purchase page appears.
- 4 Set up **Basic Configurations** by performing the following steps.
  - a Select a billing method. For example, **Pay-As-You-Go**.
  - b From the **Region** drop-down menu, select a region. The system randomly allocates a zone by default.

---

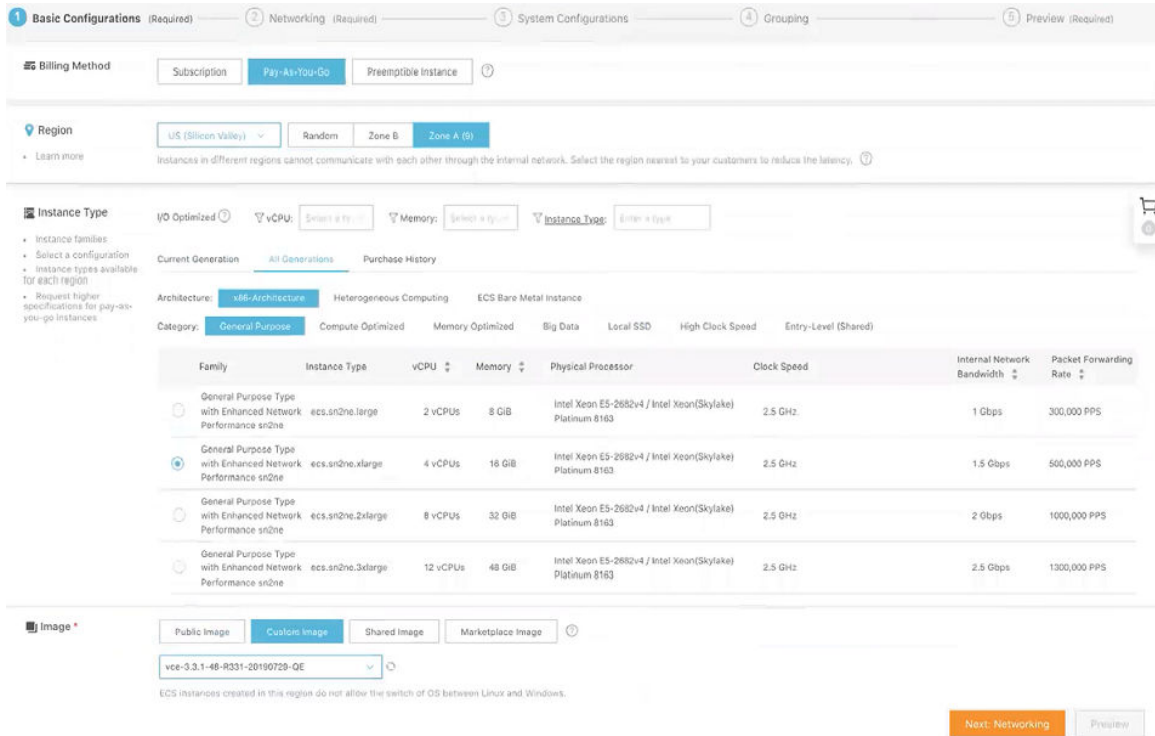
**Note** After an instance is created, you cannot change its region or zone.

---

- c In the **Instance Type** area, go to **All Generations > x86-Architecture > General Purpose** and select the **4 vCPU + 16 GiB** memory (ecs.sn2ne.xlarge) instance type.

The available instance type family is determined by the region you selected.

- d In the **Image** area, click **Custom Image** and select an Edge image, for example, vce-3.3.1-48-R331-20190727-QE.
- e Select a storage space. By default, a 40 GiB Ultra Cloud Disk is selected.



- 5 Click **Next: Networking** to set up the networking and security group configuration.
  - a Select **VPC** as the network type and select the VPC where you are going to deploy your Edge and attach the Console interface of your Edge to MGMT\_SN.
  - b Set the network billing method.

- c Select your VPC-type security group.
- d Add an Elastic Network Interface (ENI). You can skip this step if the selected instance type does not support ENI.

## 6 Click **Next: System Configurations**.

- a Configure **Logon Credentials** by selecting one of the following options: **Key Pair**, **Inherit Password From Image**, and **Password**. By default, **Set Later** option is selected.
- b In the **Instance Name** text box, enter a unique name for your Edge instance.
- c Under the **Advance** area, you can provide the cloud-init user data for your edge in the following sample format for activation purpose. According to your VCO set up, you must change the vco name and activation code.

```
#cloud-config
velocloud:
  vce:
    vco: 1.211.224.11
    activation_code: 12XX-ABC1-6DD3-3EFG
    vco_ignore_cert_errors: true
```

Basic Configurations (Required) | Networking (Required) | **3 System Configurations** | Grouping | Preview (Required)

Logon Credentials:  Key Pair  Inherit Password From Image  Password  Set Later

Key Pair:  [Learn More](#) | [Create Key Pair](#)

Instance Name:   The name must be 2 to 128 characters in length and can contain letters, Chinese characters, digits, and the following special characters: -.\_. The name must start with a letter or Chinese character.

Description:  The description must be 2 to 256 characters in length. It cannot start with "http://" or "https://".

Host:   For Linux systems and other operating systems: The name must be 2 to 64 characters in length. It can contain several segments delimited by periods (.). Each segment can contain letters, digits, and hyphens (-), but consecutive periods (.) or hyphens (-) are not allowed. The name cannot start or end with a period (.) or hyphen (-).

Sequential Suffix:  Add Sequential Suffix to Instance Name and Hostname  
Sequential suffixes can be from 001 to 999. For example: Localhost001, Localhost002 or MyInstance001, MyInstance002.

Release Protection:  Prevent users from releasing the instance inadvertently by using the console or API (?)

---

**Advanced (based on instance RAM roles or cloud-init)**

RAM Role:   [Learn More](#) | [Create Instance RAM Role](#)

User Data:  Enter Base64 Encoded Information

```

yeloCloud:
X50:
  X50I: 3.213.224.82
  activation_code: YZFM-YBQM-LB73-SEX6
  X50I@N0@C@E@C@T@_@0@I@S@: true
  
```

Both bat and PowerShell are supported in Windows. When you use Base64 to encode custom data, make sure that [bat] or [powershell] appears as the first line. For Linux, shell script is supported. For more formats, see [cloud-init](#) | [Learn More](#)

[Prev: Networking](#) | [Next: Grouping](#) | [Preview](#)

- 7 Click **Next: Grouping** and set the options as needed.
- 8 Click **Next: Preview** and confirm the selected configuration. You can also click the edit icon to modify the configurations.
- 9 Read and confirm **Terms of Service**, and then click **Create Instance**.

## Results

Click **Console** to return to the ECS console. Click the refresh button to check if the Edge instance is created. If the newly created Edge instance is in a **Running** status, then the Edge is created successfully.

## What to do next

- [Create an Elastic Network Interface](#)

# Create an Elastic Network Interface

An Elastic Network Interface (ENI) is a virtual network interface that can be attached to an ECS instance in a VPC. This topic describes how to create an ENI in the ECS console.

## Prerequisites

- A VPC and a VSwitch are created. For steps, see [Create a Virtual Private Cloud](#).
- A security group is created in the same VPC. For steps, see [Create a Security Group](#).

Procedure

- 1 Log on to the [ECS console](#).
- 2 In the left-side navigation pane, choose **Network & Security** > .  
The **Network Interfaces** page appears.
- 3 Click **Create ENI**.  
The **Create ENI** page appears.

Create ENI ? Create ENI
✕

---

Network Interface Name:

The name must be 2 to 128 characters in length and can contain Chinese characters, letters, digits, hyphens (-), and underscores (\_). It cannot start with "http://" or "https://". The name must start with a letter or Chinese character.

\* VPC:

\* VSwitch:

The available zone of the selected switch needs to be the same as the instance to be bound  
CIDR: 192.168.100.0/24 (us-west-1a)

Primary Private IP:

Must be the free address in the address section of the VSwitch to which it belongs. By default, the free address in the switch is allocated randomly.

\* Security Group:

Description:

It must be 2 to 256 characters in length and cannot start with "http://" or "https://".

---

Tag:



#### 4 Provide the following configuration details.

- a In the **Network Interface Name** text box, enter a unique name for the ENI.
- b From the **VPC** drop-down menu, select the same VPC associated with the instance to which you want the ENI to be bound. When you attach an ENI to an instance, they must be in the same VPC.

---

**Note** After an ENI is created, you cannot change the VPC.

---

- c From the **VSwitch** drop-down menu, select the VSwitch to which you want the ENI to be bound. When you attach an ENI to an instance, they must be in the same zone, but they do not have to be in the same VSwitch.

---

**Note** After an ENI is created, you cannot change the VSwitch.

---

- d From the **Security Group** drop-down menu, select your security group in the selected VPC.

#### 5 Click **OK**.

#### Results

On the **Network Interfaces** page, click **Refresh** to view the newly created ENI instance.

#### What to do next

- After creating an ENI, you can attach an ENI to an Edge instance. For steps, see [Bind an ENI to an Edge instance](#).

## Create Elastic IP and Assign it to Public Interface of the Edge

Elastic IP Addresses (EIPs) are public IP address resources that you can purchase and hold independently. You can create an EIP or reinstate a released EIP through the console. This topic describes how to create an EIP and bind it to the secondary (public) interface.

#### Prerequisites

- Ensure you have an AliCloud account and login information.
- Ensure you have an Elastic Network Interface (ENI) to assign the Elastic IP. For steps to create ENI, see [Create an Elastic Network Interface](#).

#### Procedure

- 1 Log on to the [VPC console](#).
- 2 In the left-side navigation pane, click **Elastic IP Addresses**.

The **Elastic IP Addresses** page appears.

**3** Click **Create EIP**.

The **Elastic IP** page appears.

**4** Configure EIP.

- a Select the region of the EIP to be created.

Ensure that the EIP and the cloud instance to be associated with the EIP belong to the same region.

- b Set the maximum bandwidth for the EIP to be created, depending on the requirement.

- c Select the number of the EIPs that you want to create with the same configurations. The default value for **Quantity** is 1.

**5** Click **Buy Now**.

The **Confirm Order** page appears.

**6** Enable **Elastic IP Agreement of Service** checkbox and click **Activate**.

On the **Elastic IP Addresses** page, click **Refresh** to view the newly created EIP instance.

- 7 To associate the EIP instance to a secondary (public) Elastic Network Interface (ENI) of the Edge, click **Bind** under the **Actions** column. The **Bind Elastic IP Address** page appears.

### Bind Elastic IP Address

**IP Address:**

198.11.177.194

• **Instance Type**

Secondary ENI

**Mode**

NAT Mode

**Secondary ENI**

Velo\_demo\_Public\_Intf/eni-rj929mvms5w1ir14op93

**Info:**

1. The elastic IP address binds to the ENI as a NAT IP. The ENI supports both public IP address and private IP address.
2. You cannot view the elastic IP address in the OS. However, you can use Open API to retrieve the public IP address of a specified ENI.
3. NAT mode does not support NAT ALG protocols such as H.323, SIP, DNS, RTSP, TFTP.

OK Cancel

- From the **Instance Type** drop-down menu, select **secondary ENI**.
- From the **Secondary ENI** drop-down menu, select the interface to which you want to bind the EIP.
- Click **OK**.

#### What to do next

- [Bind an ENI to an Edge instance](#)

## Bind an ENI to an Edge instance

To bind secondary Elastic Network Interfaces (ENIs) to an Edge instance, perform the steps on this procedure.

## Prerequisites

- Ensure that you have created an ENI. For steps, see [Create an Elastic Network Interface](#).

## Procedure

- 1 Log on to the [ECS console](#).
- 2 In the left-side navigation pane, choose **Network & Security** > **ENI**.
- 3 On the **Network Interfaces** page, select an ENI and click **Bind to Instance** under the **Actions** column.

The **Bind to Instance** pop-up window appears.

**Bind to Instance** ⓘ Attach ENI to instance

---

ID/Name: eni-rj929mvms5w1ir14op93/Velo\_demo\_Public\_Intf

\*Select Instance:

The eni is created in us-west-1a and only the instances under that zone can be selected.

---

**OK** **Cancel**

- 4 From the **Select Instance** drop-down menu, select the Edge instance to which you want to bind the ENI.
- 5 Click **OK**.

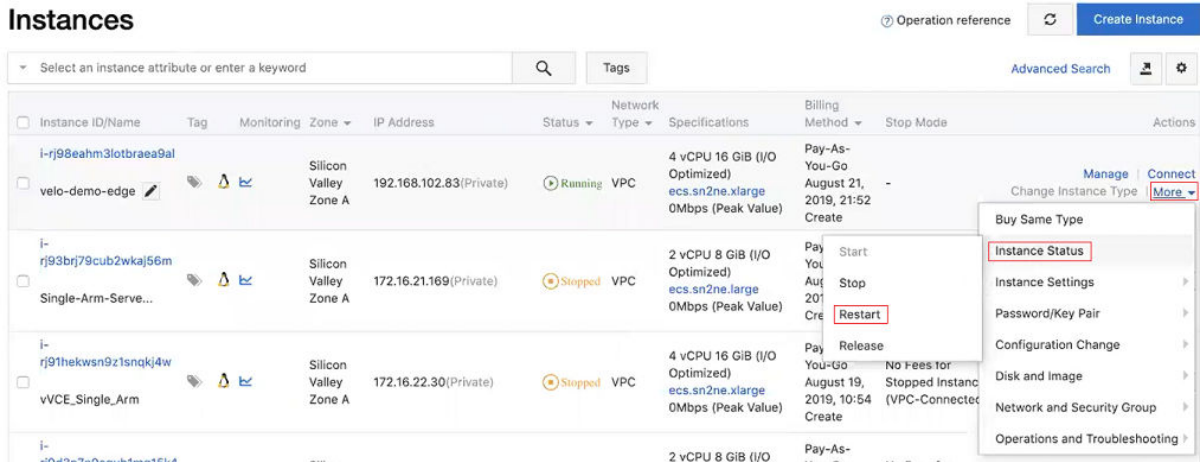
## Results

The selected ENI is bound to the Edge instance.

## What to do next

Restart your Edge instance for the newly associated interfaces to get effect, by performing the following step.

- 1 In the left-side navigation pane, click **Instances**.
- 2 On the **Instances** page, go to your Edge instance, and click **More** under the **Actions** column.
- 3 Go to **Instance Status** > **Restart**.
- 4 Click **OK**.



## Create a LAN Instance

Describes how to create a LAN (Linux) instance on the ECS console.

### Prerequisites

- Ensure you have an AliCloud account and login information.

### Procedure

- Log on to the [ECS console](#).
- In the left-side navigation pane, click **Instances & Images > Instances**.
- On the **Instances** page, click **Create Instance**.

The **Custom Launch** purchase page appears.

- Set up **Basic Configurations** by performing the following steps.
  - Select a billing method. For example, **Pay-As-You-Go**.
  - From the **Region** drop-down menu, select a region. The system randomly allocates a zone by default.

---

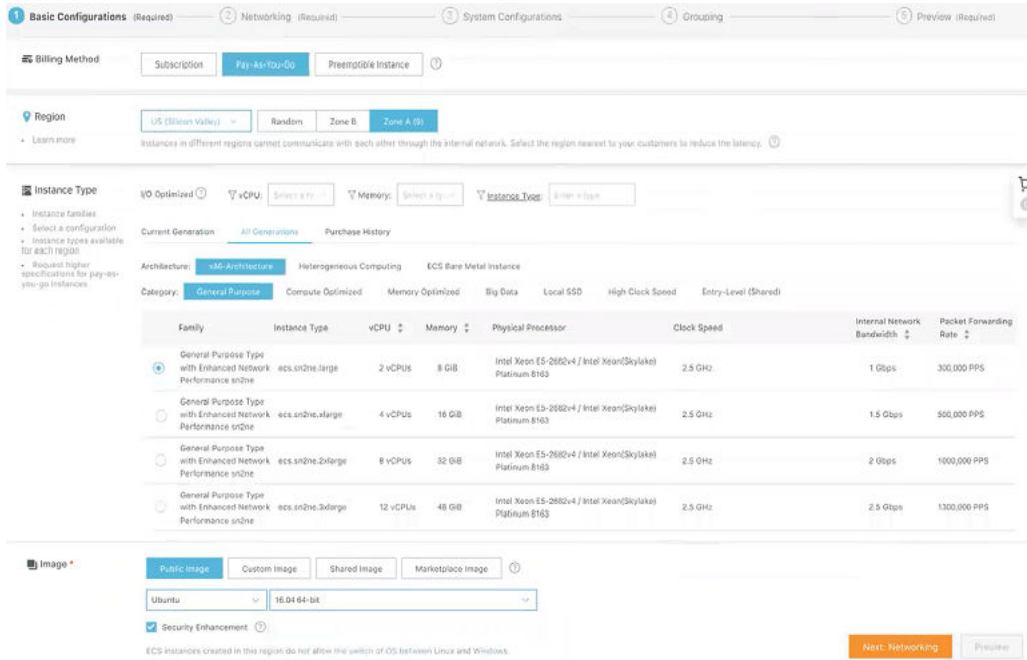
**Note** After an instance is created, you cannot change its region or zone.

---

- In the **Instance Type** area, go to **All Generations > x86-Architecture > General Purpose** and select an instance type.

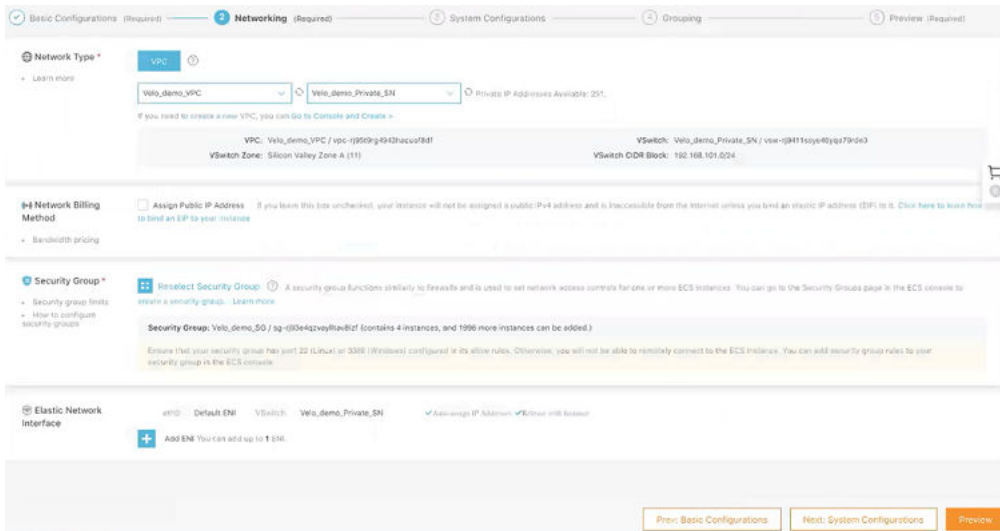
The available instance type family is determined by the region you selected.

- d In the **Image** area, click **Public Image** and select an Ubuntu image, for example, 16.04.64.bit.
- e Select a storage space. By default, a 40 GiB Ultra Cloud Disk is selected.



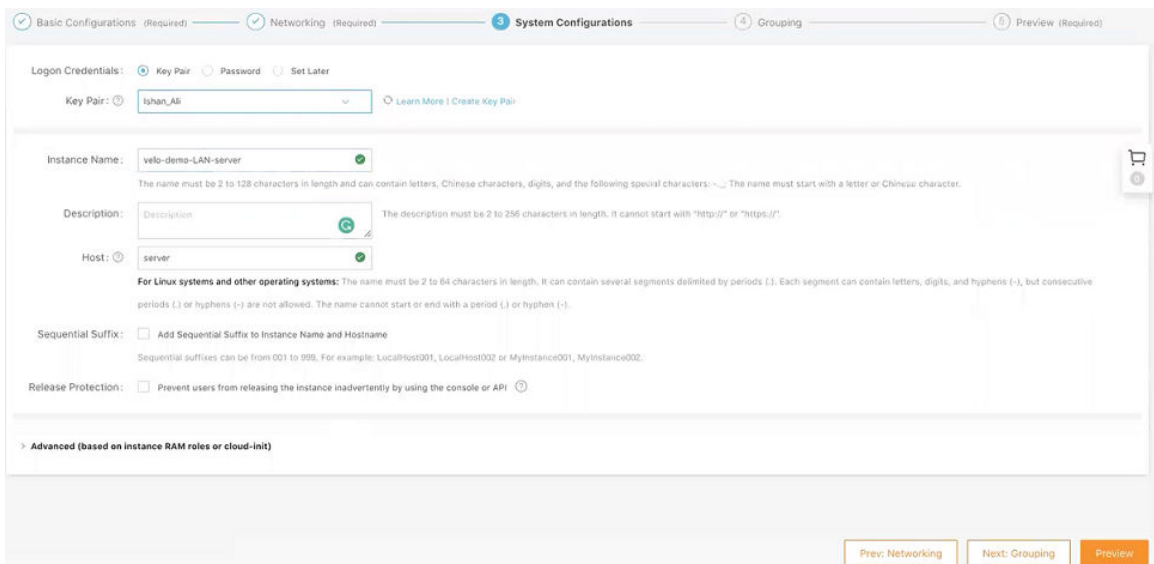
- 5 Click **Next: Networking** to set up the networking and security group configuration.
  - a Select **VPC** as the network type and select the VPC where you are going to deploy your LAN device and the Subnet/VSwitch to which you want the primary interface to be connected.
  - b Set the network billing method.

- c Select your VPC-type security group.
- d Add an Elastic Network Interface (ENI). You can skip this step if the selected instance type does not support ENI.



**6 Click Next: System Configurations.**

- a Configure **Logon Credentials** by selecting one of the following options: **Key Pair**, **Inherit Password From Image**, and **Password**. By default, **Set Later** option is selected.
- b In the **Instance Name** text box, enter a unique name for the LAN instance.



- 7 Click Next: Grouping** and set the options as needed.
- 8 Click Next: Preview** and confirm the selected configuration. You can also click the edit icon to modify the configurations.
- 9 Read and confirm Terms of Service**, and then click **Create Instance**.

## Results

Click **Console** to return to the ECS console. Click the refresh button to check if the LAN instance is created. If the newly created LAN instance is in a **Running** status, then the instance is created successfully.

## Add a Custom Route Table Entry

Describes how to add a custom route entry in a custom route table.

### Prerequisites

- Ensure that you have created a VPC and VSwitches. For steps, see [Create a Virtual Private Cloud](#) and [Create a VSwitch](#).
- Ensure that you have a custom route table associated with a VSwitch. For steps, see [Create Custom Route Tables and Associate VSwitches](#).

### Procedure

- 1 Log on to the [VPC console](#).
- 2 In the left-side navigation pane, click **Route Tables**.
- 3 On the **Route Tables** page, find the target route table, and then click **Manage** in the **Actions** column.
- 4 In the **Route Table Details** area, click **Route Entry List** tab, and then click **Add Route Entry**.

The **Add Route Entry** page appears.

### Add Route Entry

---

• **Name** ?

Default\_route\_for\_internet 26/128 ✓

• **Destination CIDR Block**

0 . 0 . 0 . 0 / 0 ▼

• **Next Hop Type**

Secondary NetworkInterface ▼

• **Secondary NetworkInterface**

Velo\_demo\_Private\_Intf/eni-rj93r5zaev0gjtbf85c0 ▼

---

OK

Cancel



- 5 In the **Name** text box, enter the unique name for the route entry.
- 6 In **Destination CIDR Block**, specify the destination CIDR block address.
- 7 From the **Next Hop Type** drop-down menu, select the next hop interface type, for example, **Secondary NetworkInterface**, and then select the interface.
- 8 Click **OK**.

## Create a Jump Host Instance

Creating a Jump Host (JH) instance is an optional step for the Edge deployment. However, to locally manage the virtual Edge, you must deploy a JH and assign an Elastic IP to it. To SSH to an Edge over a private network using a JH, create a JH (Linux instance) in VPC with one interface in the Public subnet (for Internet connectivity with EIP), and the other interface in the management subnet.

To create a JH instance on the ECS console, perform the following steps.

### Prerequisites

- Ensure you have an AliCloud account and login information.

### Procedure

- 1 Log on to the [ECS console](#).
- 2 In the left-side navigation pane, click **Instances & Images > Instances**.
- 3 On the **Instances** page, click **Create Instance**.  
The **Custom Launch** purchase page appears.
- 4 Set up **Basic Configurations** by performing the following steps.
  - a Select a billing method. For example, **Pay-As-You-Go**.
  - b From the **Region** drop-down menu, select a region. The system randomly allocates a zone by default.

---

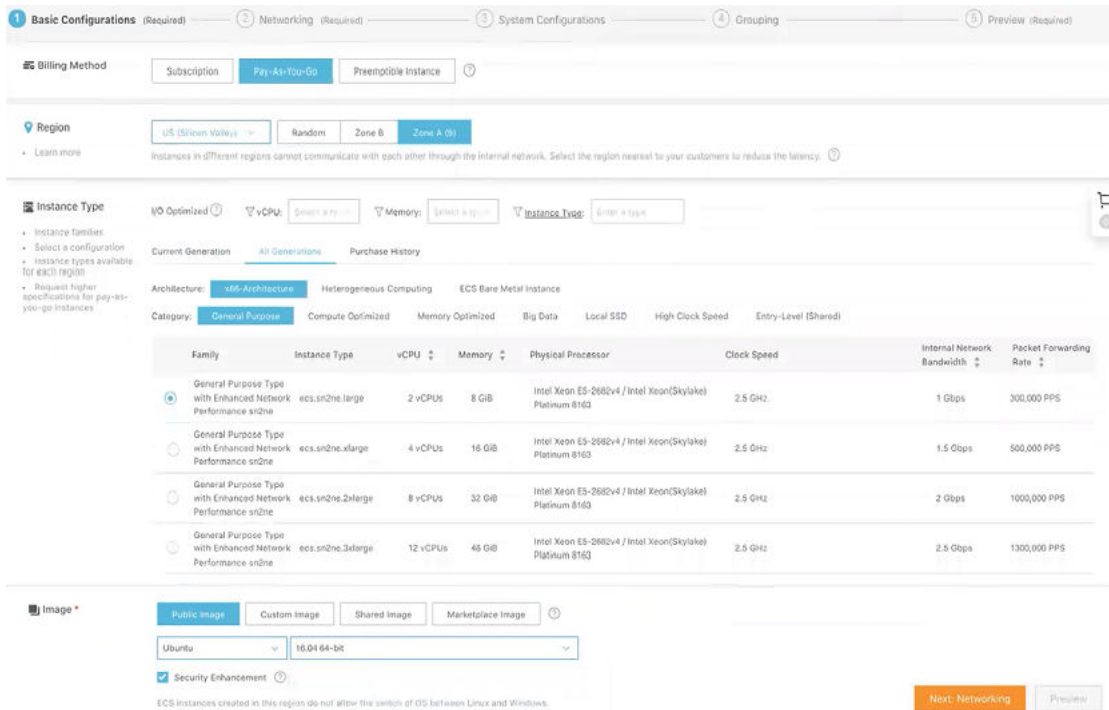
**Note** After an instance is created, you cannot change its region or zone.

---

- c In the **Instance Type** area, go to **All Generations > x86-Architecture > General Purpose** and select an instance type.

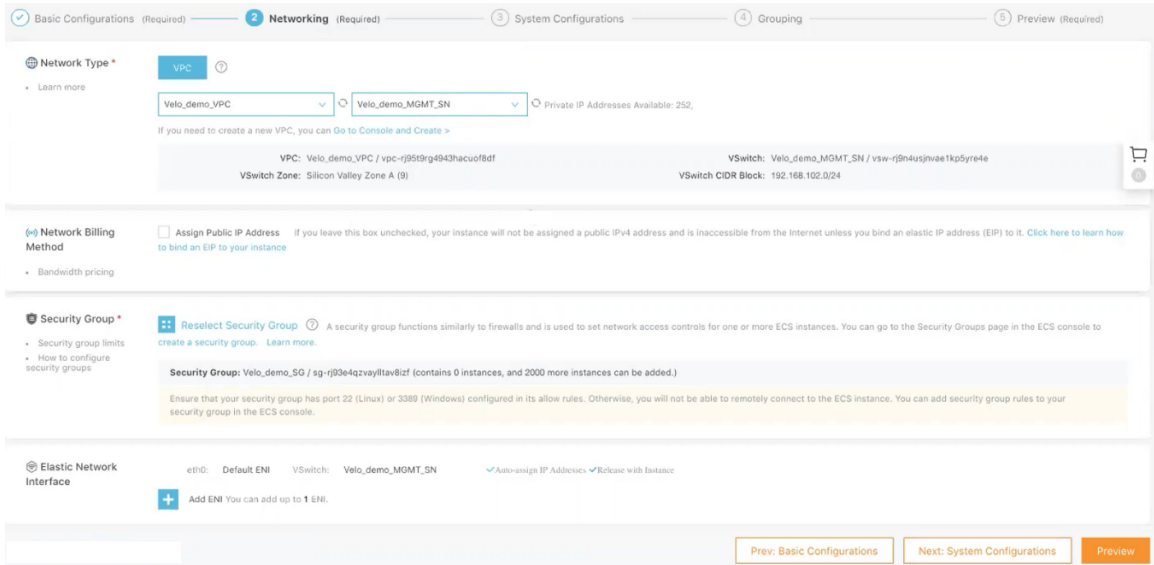
The available instance type family is determined by the region you selected.

- d In the **Image** area, click **Public Image** and select an Ubuntu image, for example, 16.04.64.bit.
- e Select a storage space. By default, a 40 GiB Ultra Cloud Disk is selected.



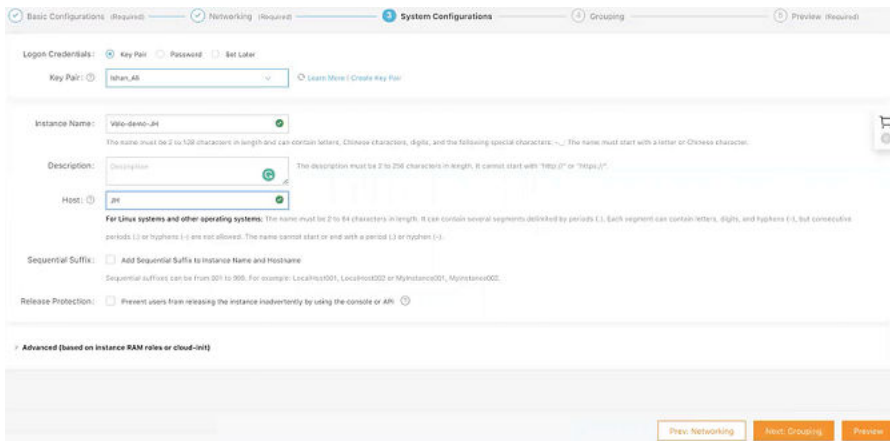
- 5 Click **Next: Networking** to set up the networking and security group configuration.
  - a Select **VPC** as the network type and select the VPC where you are going to deploy your JH and attach the Console interface of your Edge to MGMT\_SN.
  - b Set the network billing method.

- c Select your VPC-type security group.
- d Add an Elastic Network Interface (ENI). You can skip this step if the selected instance type does not support ENI.



**6 Click Next: System Configurations.**

- a Configure **Logon Credentials** by selecting one of the following options: **Key Pair**, **Inherit Password From Image**, and **Password**. By default, **Set Later** option is selected.
- b In the **Instance Name** text box, enter a unique name for the JH instance.



- 7 Click Next: Grouping** and set the options as needed.
- 8 Click Next: Preview** and confirm the selected configuration. You can also click the edit icon to modify the configurations.
- 9 Read and confirm Terms of Service**, and then click **Create Instance**.





# Azure Virtual WAN VCG Automation

# 24

For the 3.3.1 release, VeloCloud Orchestrator (VCO) supports Azure Virtual WAN and VeloCloud Gateway (VCG) integration and automation to enable branch-to-VPN connectivity.

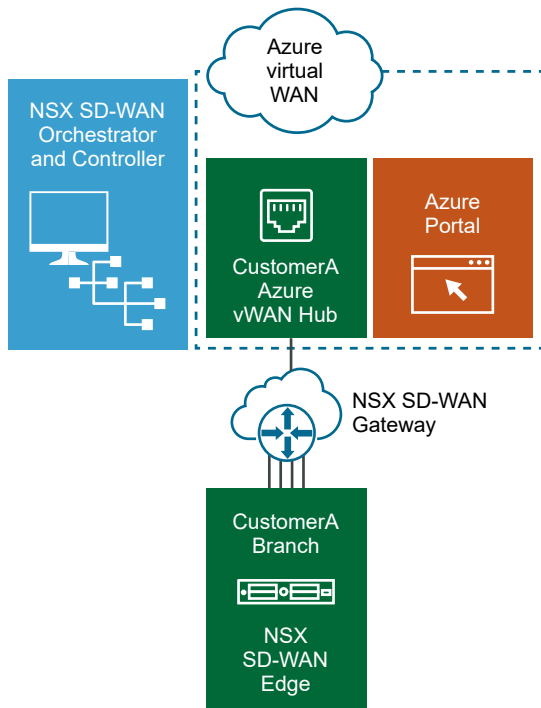
This chapter includes the following topics:

- [Azure Virtual WAN VCG Automation Overview](#)
- [Prerequisite Azure Configuration](#)
- [Configure Azure Virtual WAN for Branch-to-Azure VPN Connectivity](#)
- [Configure VCO for Branch-to-Azure VPN Connectivity](#)

## Azure Virtual WAN VCG Automation Overview

Azure Virtual WAN is a network service that facilitates optimized and automated Virtual Private Network (VPN) connectivity from enterprise branch locations to or through Microsoft Azure. Azure subscribers' provision Virtual Hubs corresponding to Azure regions and connect branches (which may or may not be SD-WAN enabled) through IP security (IPSec) VPN connections.

For the 3.3.1 release, VeloCloud Orchestrator (VCO) supports Azure Virtual WAN and VeloCloud Gateway (VCG) integration and automation by leveraging the Azure backbone to establish branch-to-Azure VPN connectivity through the VCG as shown in the following diagram.



The following sections describe the procedures for configuring the VCO and Azure to enable branch-to-Azure VPN connectivity through the VeloCloud Gateway (VCG):

- [Configure Azure Virtual WAN for Branch-to-Azure VPN Connectivity](#)
- [Configure VCO for Branch-to-Azure VPN Connectivity](#)

## Prerequisite Azure Configuration

Enterprise network administrators must complete the following prerequisite configuration tasks at the Azure portal to ensure that the VeloCloud Orchestrator (VCO) application can function as the Service Principal (identity for the application) for the purposes of Azure Virtual WAN and VCG integration.

- [Register VCO Application](#)
- [Assign the VCO Application to Contributor Role](#)
- [Register a Resource Provider](#)
- [Create a Client Secret](#)

## Register VCO Application

Describes how to register a new application in Azure Active Directory (AD).

To register a new application in Azure AD:

## Prerequisites

- Ensure you have an Azure subscription. If not, create a [free account](#).

## Procedure

- 1 Log in to your [Microsoft Azure](#) account.

The **Microsoft Azure** home screen appears.

- 2 Click **All Services** and search for **Azure Active Directory**.

- 3 Select **Azure Active Directory** and go to **App registrations > New registration**.

The **Register an application** screen appears.

### Register an application

---

#### \* Name

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

vcc 

#### Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (VeloCloud Networks, Incit@velo)
- Accounts in any organizational directory
- Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)

[Help me choose...](#)

#### Redirect URI (optional)

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

Web 

---

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

**Register**

- 4 In the **Name** field, enter the name for your VCO application.
- 5 Select a supported account type, which determines who can use the application.
- 6 Click **Register**.



## Results

Your VCO application will be registered and displayed in the **All applications** and **Owned applications** tabs.

Make sure to note down the Directory (tenant) ID and Application (client) ID to be used during the VCO configuration for IaaS Subscription.

## What to do next

- [Assign the VCO Application to Contributor Role](#)
- [Create a Client Secret](#)

## Assign the VCO Application to Contributor Role

To access resources in your Azure subscription, you must assign the application to a role. You can set the scope at the level of the subscription, resource group, or resource. Permissions are inherited to lower levels of scope.

To assign a Contributor role at the subscription scope:

### Prerequisites

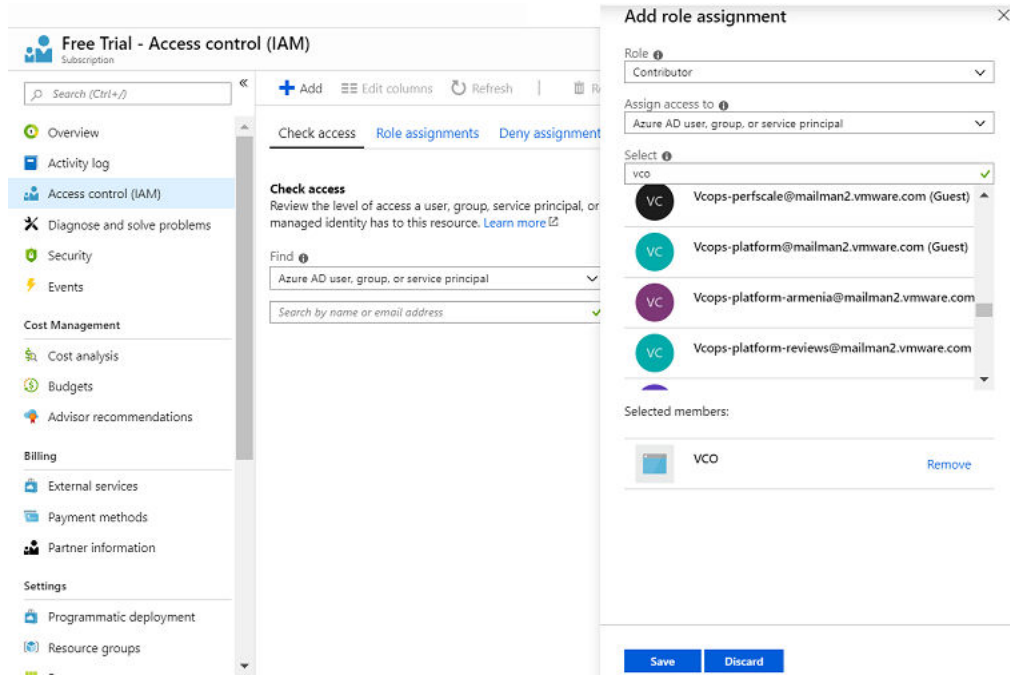
- Ensure you have an Azure subscription. If not, create a [free account](#).

### Procedure

- 1 Click **All Services** and search for **Subscriptions**.
- 2 From the list of subscriptions, select the subscription to which you want to assign your application. If you do not see the subscription you are looking for, select **global subscriptions filter**. Make sure the subscription you want is selected for the portal.
- 3 Click **Access control (IAM)**.

#### 4 Click **+Add > Add role assignment**.

The **Add role assignment** dialog box appears.



#### 5 From the **Role** drop-down menu, select the **Contributor** role to assign to the application.

To allow the application to execute actions like **reboot**, **start** and **stop** instances, it is recommended that users assign the **Contributor** role to the App Registration.

#### 6 From the **Assign access to** drop-down menu, select **Azure AD user, group, or service principal**.

By default, Azure AD applications are not displayed in the available options. To find your application, search for the name and select it.

#### 7 Select **Save**.

### Results

The application is assigned to the Contributor role and it appears in the list of users assigned to a role for that scope.

### What to do next

- [Create a Client Secret](#)
- [Configure Azure Virtual WAN for Branch-to-Azure VPN Connectivity](#)

## Register a Resource Provider

To download Virtual WAN Virtual Private Network (VPN) configurations, the VeloCloud Orchestrator (VCO) requires a Blob Storage Account that acts as an intermediary data store from where the configurations can be downloaded. The VCO aims to create seamless user experience

by provisioning a transient storage account for each of the download task. To download VPN site configurations, you must manually register the **Microsoft.Storage** resource provider on your Azure Subscription. By default, the **Microsoft.Storage** resource provider is not registered on Azure Subscriptions.

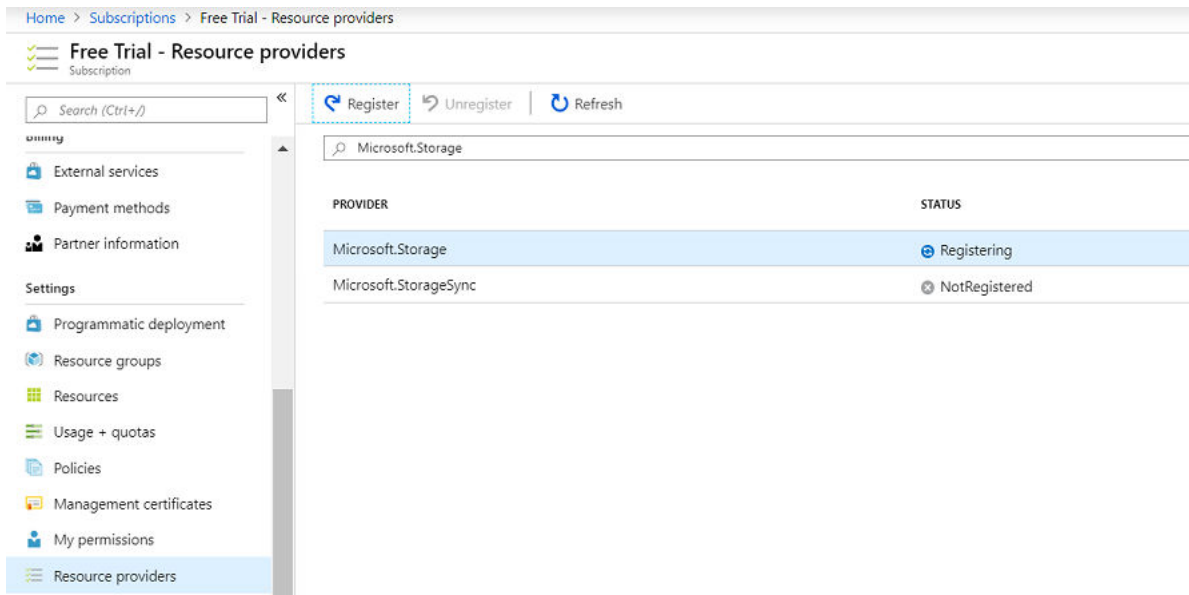
To register a resource provider for your subscription:

### Prerequisites

- Ensure you have an Azure subscription. If not, create a [free account](#).
- Ensure you have the Contributor or Owner roles permission.

### Procedure

- 1 Log in to your [Microsoft Azure](#) account.
- 2 Click **All Services** and search for **Subscriptions**.
- 3 From the list of subscriptions, select your subscription.
- 4 Under the **Settings** tab, select **Resource providers**.



- 5 From the list of available resource providers, select **Microsoft.Storage**. and click **Register**.

### Results

The resource provider is registered and also configures your subscription to work with the resource provider.

### What to do next

You can create the resources in Azure, for steps, see [Configure Azure Virtual WAN for Branch-to-Azure VPN Connectivity](#).

## Create a Client Secret

Describes how to create a new client secret in Azure AD for the purpose of authentication.

To create a new client secret in Azure AD:

### Prerequisites

- Ensure you have an Azure subscription. If not, create a [free account](#).

### Procedure

- 1 Log in to your [Microsoft Azure](#) account.

The **Microsoft Azure** home screen appears.

- 2 Select **Azure Active Directory** > **App registrations**.

- 3 On the **Owned applications** tab, click on your registered VCO application.

- 4 Go to **Certificates & secrets** > **New client secret**.

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

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

### Results

The client secret is created for the registered application.

**Note** Copy and save the new client secret value to be used during the IaaS subscription in VCO.

### What to do next

- [Configure Azure Virtual WAN for Branch-to-Azure VPN Connectivity](#)
- [Configure VCO for Branch-to-Azure VPN Connectivity](#)

# Configure Azure Virtual WAN for Branch-to-Azure VPN Connectivity

This section describes the procedures to configure Azure for integrating Azure Virtual WAN and VeloCloud Gateway (VCG) to enable the branch-to-Azure VPN connectivity.

Before you begin to configure the Azure Virtual WAN and the other Azure resources:

- Verify that none of the subnets of your on-premises network overlap with the existing virtual networks that you want to connect to. Your virtual network does not require a gateway subnet and cannot have any virtual network gateways. For steps to create a virtual network, see [Create a Virtual Network](#).
- Obtain an IP address range for your Hub region and ensure that the address range that you specify for the Hub region does not overlap with any of your existing virtual networks that you connect to.
- Ensure you have an Azure subscription. If not, create a [free account](#).

For step-by-step instructions about the various procedures that need to be completed in the Azure portal side for integrating Azure Virtual WAN and VeloCloud Gateway (VCG), see:

- [Create a Resource Group](#)
- [Create a Virtual WAN](#)
- [Create a Virtual Hub](#)
- [Create a Virtual Network](#)
- [Create a Virtual Connection between VNet and Hub](#)

## Create a Resource Group

Describes how to create a resource group in Azure.

To create a resource group in Azure:

### Prerequisites

- Ensure you have an Azure subscription. If not, create a [free account](#).

### Procedure

- 1 Log in to your [Microsoft Azure](#) account.  
The **Microsoft Azure** home screen appears.
- 2 Click **All Services** and search for **Resource groups**.

- 3 Select **Resource groups** and click **+Add**.

The **Create a resource group** screen appears.

[Home](#) > [Resource groups](#) > Create a resource group

## Create a resource group

---

Basics
Tags
Review + create

**Resource group** - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. [Learn more](#) ↗

**Project details**

\* Subscription ⓘ

\* Resource group ⓘ

**Resource details**

\* Region ⓘ

Review + create

< Previous

Next : Tags >

- 4 From the **Subscription** drop-down menu, select your Microsoft Azure subscription.

- 5 In the **Resource group** text box, enter a unique name for your new resource group.

A resource group name can include alphanumeric characters, periods (.), underscores (\_), hyphens (-), and parenthesis (), but the name cannot end with a period.

- 6 From the **Region** drop-down menu, select the location for your resource group, where the majority of your resources will reside.

- 7 Click **Review+create** and then click **Create**.

### Results

A resource group is created and appears on the Azure portal dashboard.

## What to do next

Create an Azure Virtual WAN. For steps, see [Create a Virtual WAN](#).

## Create a Virtual WAN

Describes how to create a Virtual WAN in Azure.

To create a Virtual WAN in Azure:

### Prerequisites

- Ensure you have an Azure subscription. If not, create a [free account](#).
- Ensure you have a resource group created to add the Virtual WAN.

### Procedure

- 1 Log in to your [Microsoft Azure](#) account.  
The **Microsoft Azure** home screen appears.
- 2 Click **All Services** and search for **Virtual WANs**.
- 3 Select **Virtual WANs** and click **+Add**.  
The **Create WAN** screen appears.

## Create WAN

**Basics**   Review + create

The virtual WAN resource represents a virtual overlay of your Azure network and is a collection of multiple resources. [Learn more](#)

### Project details

Subscription *	Microsoft Azure Enterprise	▼
Resource group *	MIL-AZAUSSYD-PROD-ARG	▼

[Create new](#)

### Virtual WAN details

Resource group location *	Australia East	▼
Name *	Velocloud_vWan	✓
Type ⓘ	Standard	▼

- 4 From the **Subscription** drop-down menu, select your Microsoft Azure subscription.

- 5 From the **Resource group** drop-down menu, select your resource group to add the Virtual WAN.
- 6 From the **Resource group location** drop-down menu, select the location where the metadata associated with the Virtual WAN will reside.
- 7 In the **Name** text box, enter a unique name for your Virtual WAN.
- 8 From the **Type** drop-down menu, select **Standard** as the Virtual WAN type.
- 9 Click **Create**.

#### Results

A Virtual WAN is created and appears on the Azure portal dashboard.

#### What to do next

Create Virtual Hubs. For steps, see [Create a Virtual Hub](#).

## Create a Virtual Hub

Describes how to create a Virtual Hub in Azure.

To create a Virtual Hub in Azure:

#### Prerequisites

- Ensure you have an Azure subscription. If not, create a [free account](#).
- Ensure you have a resource group created to add the Azure resources.

#### Procedure

- 1 Log in to your [Microsoft Azure](#) account.  
The **Microsoft Azure** home screen appears.
- 2 Go to **All resources** and from the list of available resources, select the Virtual WAN that you have created.
- 3 Under the **Virtual WAN architecture** area, click **Hubs**.



#### 4 Click **+New Hub**.

The **Create virtual hub** screen appears.

**Create virtual hub**

---

[Basics](#) [Site to site](#) [Point to site](#) [ExpressRoute](#) [Routing](#) [Tags](#) [Review + create](#)

A virtual hub is a Microsoft-managed virtual network. The hub contains various service endpoints to enable connectivity from your on-premises network (vpnsite). The hub is the core of your network in a region. There can only be one hub per Azure region. When you create a hub using Azure portal, it creates a virtual hub VNet and a virtual hub vpngateway. [Learn more](#)

**Project details**

The hub will be created under the same subscription and resource group as the vWAN.

\* Subscription

\* Resource group

**Virtual Hub Details**

\* Region

\* Name

\* Hub private address space

---

**i** Creating a hub with a gateway will take 30 minutes.

[Review + create](#) [Previous](#) [Next : Site to site >](#)

#### 5 In the **Basics** tab, enter the following Virtual Hub details.

- From the **Region** drop-down menu, select the location where the Virtual Hub resides.
- In the **Name** text box, enter the unique name for your Hub.
- In the **Hub private address space** text box, enter the address range for the Hub in Classless inter-domain routing (CIDR) notation.

#### 6 Click **Next: Site to site >** and enable Site to site (VPN gateway) before connecting to VPN sites by selecting **Yes**.

**Note** A VPN Gateway is required in order for NVS automation to work, otherwise it is not possible to create VPN connections.


**Create virtual hub**

---

[Basics](#)
[Site to site](#)
[Point to site](#)
[ExpressRoute](#)
[Routing](#)
[Tags](#)
[Review + create](#)


You will need to enable Site to site (VPN gateway) before connecting to VPN sites. You can do this after hub creation, but doing it now will save time and reduce the risk of service interruptions later. [Learn more](#)

Do you want to create a Site to site (VPN gateway)?  Yes  No

AS Number  

\* Gateway scale units

---

 Creating a hub with a gateway will take 30 minutes.

[Review + create](#)
[Previous](#)
[Next : Point to site >](#)

a From the **Gateway scale units** drop-down menu, select a scaling value.

## 7 Click **Review + Create**.

### Results

A Virtual Hub is created and appears on the Azure portal dashboard.

### What to do next

- Create Virtual Connection between Hubs and Virtual Networks (VNETs). For steps, see [Create a Virtual Connection between VNet and Hub](#).
- If you do not have an existing VNet, you can create one by following the steps in [Create a Virtual Network](#).

## Create a Virtual Network

Describes how to create a Virtual Network in Azure.

To create a Virtual Network in Azure:

### Prerequisites

- Ensure you have an Azure subscription. If not, create a [free account](#).

### Procedure

- 1 Log in to your [Microsoft Azure](#) account.  
The **Microsoft Azure** home screen appears.
- 2 Click **All Services** and search for **Virtual networks**.

- 3 Select **Virtual networks** and click **+Add**.

The **Create virtual network** screen appears.

**Create virtual network**

\* Name  
 ✓

\* Address space ⓘ  
 ✓  
 10.0.0.0 - 10.0.0.255 (256 addresses)

\* Subscription  
 ▼

\* Resource group  
 ▼  
[Create new](#)

\* Location  
 ▼

Subnet

\* Name  
 ✓

\* Address range ⓘ  
 ✓  
 10.0.0.0 - 10.0.0.255 (256 addresses)

DDoS protection ⓘ  
 Basic  Standard

Service endpoints ⓘ

[Automation options](#)

- 4 In the **Name** text box, enter the unique name for your virtual network.
- 5 In the **Address space** text box, enter the address range for the virtual network in Classless inter-domain routing (CIDR) notation.
- 6 From the **Subscription** drop-down menu, select your Microsoft Azure subscription.
- 7 From the **Resource group** drop-down menu, select your resource group to add the virtual network.
- 8 From the **Location** drop-down menu, select the location where the virtual network resides.
- 9 Under the **Subnet** area, enter the name and address range for the subnet.

Do not make any changes to the other default settings of DDos protection, Service endpoints, and Firewall.

- 10 Click **Create**.

## Results

A Virtual network is created and appears on the Azure portal dashboard.

## What to do next

Create Virtual Connection between Hubs and Virtual Networks (VNETs). For steps, see [Create a Virtual Connection between VNet and Hub](#).

## Create a Virtual Connection between VNet and Hub

Describes how to create a virtual connection between Virtual Networks (VNETs) and the Virtual Hub in a particular Azure region.

To create a virtual network connection between a VNet and a Virtual Hub in a particular Azure region:

### Prerequisites

- Ensure you have an Azure subscription. If not, create a [free account](#).
- Ensure you have Virtual Hubs and Virtual Networks created.

### Procedure

- 1 Log in to your [Microsoft Azure](#) account.

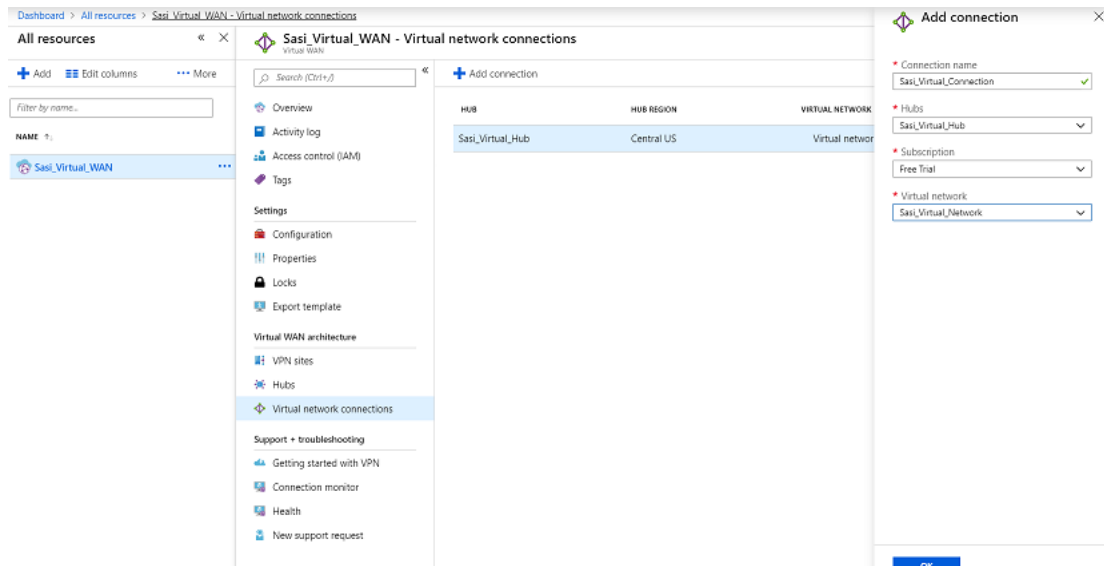
The **Microsoft Azure** home screen appears.

- 2 Go to **All resources** and from the list of available resources, select the Virtual WAN that you have created.

- 3 Under the **Virtual WAN architecture** area, click **Virtual network connections**.

- 4 Click **+Add connection**.

The **Add connection** screen appears.



- 5 In the **Connection name** text box, enter the unique name for the virtual connection.
- 6 From the **Hubs** drop-down menu, select the Hub you want to associate with this connection.
- 7 From the **Subscription** drop-down menu, select your Microsoft Azure subscription.
- 8 From the **Virtual network** drop-down menu, select the virtual network you want to connect to this Hub.
- 9 Click **OK**.

### Results

A peering connection is established between the selected Vnet and the Hub.

### What to do next

- [Configure VCO for Branch-to-Azure VPN Connectivity](#)

## Configure VCO for Branch-to-Azure VPN Connectivity

This section describes the procedures to configure VCO for integrating Azure Virtual WAN and VeloCloud Gateway (VCG) to enable the branch-to-Azure VPN connectivity.

---

**Note** By default, for the 3.3.1 release, the Azure Virtual WAN feature is disabled. To enable the feature, you must set the `session.options.enableAzureVirtualWAN` system property to true.

---

Before you begin the VCO configuration for Azure Virtual WAN - VCG automation, ensure you have completed all the steps explained in the [Prerequisite Azure Configuration](#) and [Configure Azure Virtual WAN for Branch-to-Azure VPN Connectivity](#) sections.

For step-by-step instructions about the various procedures that need to be completed in the VCO side for integrating Azure Virtual WAN and VeloCloud Gateway (VCG), see:

- [Configure an IaaS Subscription Network Service](#)
- [Configure a Microsoft Azure Non-VeloCloud Site](#)
- [Synchronize VPN Configuration](#)

### Configure an IaaS Subscription Network Service

Describes how to configure an Infrastructure as a Service Provider (IaaS) subscription in VCO.

To configure an IaaS subscription in VCO:

#### Prerequisites

Ensure you have registered the VCO application and created Client secret in the Azure portal. For steps, see [Prerequisite Azure Configuration](#).

## Procedure

- 1 From the navigation panel in the VCO, go to **Configure > Network Services**.

The **Services** screen appears.

- 2 In the **IaaS Subscriptions** area, click the **New** button.

The **Configure IaaS Subscription** dialog box appears.

**Configure IaaS Subscription**

- \* Subscription Type: Microsoft Azure Subscription
- \* Active Directory Tenant ID: 22eb73a3-5c68-47b6-8098-08952150a401
- \* Client ID: 5188a0f1-8215-49d0-9085-ea3043a12721
- \* Client Secret: .....
- \* Subscription: Pay-As-You-Go(Converted to EA)

Save Changes Cancel

- 3 From the **Subscription Type** drop-down-menu, select **Microsoft Azure Subscription**.
- 4 Enter the Active Directory Tenant ID, Client ID, and Client Secret corresponding to your VCO Application Registration.
- 5 Click the **Get Subscriptions** button to retrieve the list of Azure Subscriptions for which the App Registration has been allocated an IAM role.
- 6 Click **Save Changes**.

## What to do next

Configure a Non-VeloCloud Site (NVS) of type Microsoft Azure Virtual Hub. For more information, see [Configure a Microsoft Azure Non-VeloCloud Site](#).

## Configure a Microsoft Azure Non-VeloCloud Site

Describes how to configure a Non-VeloCloud Site (NVS) of type **Microsoft Azure Virtual Hub** in VCO.

To configure a NVS of type **Microsoft Azure Virtual Hub** in VCO:

### Prerequisites

- Ensure you have configured an IaaS subscription. For steps, see [Configure an IaaS Subscription Network Service](#).
- Ensure you have created Virtual WAN and Hubs in Azure. For steps, see [Configure Azure Virtual WAN for Branch-to-Azure VPN Connectivity](#).

## Procedure

- 1 From the navigation panel in the VCO, go to **Configure > Network Services**.

The **Services** screen appears.

- 2 In the **Non-VeloCloud Sites** area, click the **New** button.

The **New Non-VeloCloud Site** dialog box appears.

- 3 In the **Name** text box, enter the name for the Non-VeloCloud site.
- 4 From the **Type** drop-down menu, select **Microsoft Azure Virtual Hub**.
- 5 From the **Subscription** drop-down menu, select a subscription.  
The application fetches all the available Virtual WANs dynamically from Azure.
- 6 From the **Virtual WAN** drop-down menu, select a virtual WAN.  
The application auto-populates the resource group to which the virtual WAN is associated.
- 7 From the **Virtual Hub** drop-down menu, select a Virtual Hub.  
The application auto-populates the Azure region corresponding to the Hub
- 8 Select the **Enable Tunnel(s)** checkbox to enable VeloCloud VPN Gateways initiate VPN connections to the target Virtual Hub, as soon as the site is successfully provisioned.

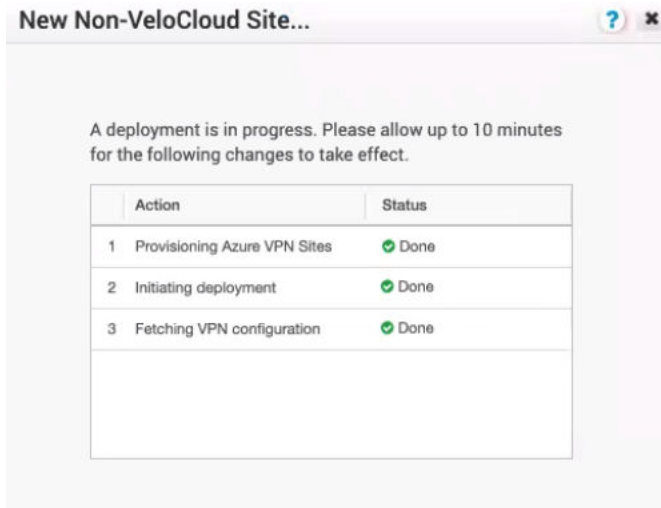
---

**Note** VeloCloud VPN Gateways will not initiate IKE negotiation until this Non-VeloCloud Site (NVS) is configured on at least one profile.

---

- 9 Click **Next**.

The VCO automatically initiates deployment, provisions Azure VPN Sites, and downloads the VPN Site Configuration for the newly configured sites and stores the configuration in the VCO's Non-VeloCloud site configuration database.



## Results

Once the Azure VPN sites are provisioned at the VCO side, you can view the VPN sites (Primary and Redundant) in the Azure portal by navigating to your **Virtual WAN** page > **Virtual WAN architecture** > **VPN sites**.

## What to do next

- Associate the Microsoft Azure Non-VeloCloud Site to a Profile in order to establish a tunnel between a branch and Azure Virtual Hub. For more information, see [Associate a Non-VeloCloud Site to a Profile](#).
- You must add SD-WAN routes in to Azure network manually. For more information, see [Edit a VPN Site](#).

## Associate a Non-VeloCloud Site to a Profile

After configuring a Non-VeloCloud Site (NVS) of type **Microsoft Azure Virtual Hub** in VeloCloud Orchestrator (VCO), you have to associate the Non-VeloCloud Site to the desired Profile in order to establish the tunnels between VeloCloud Gateways (VCGs) and Microsoft Azure Virtual Hub.

To associate a Non-VeloCloud Site to a Profile, perform the following steps:

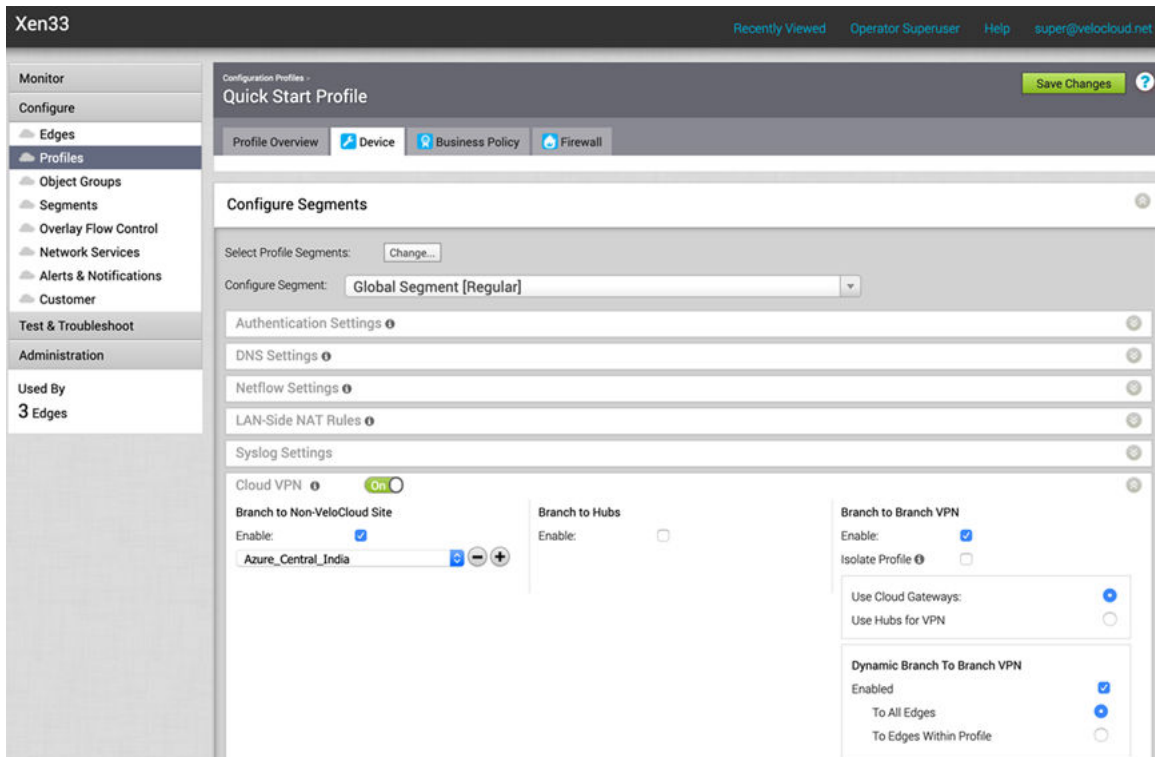
### Procedure

- 1 From the VCO navigation panel, go to **Configure** > **Profiles**.

The **Configuration Profiles** page appears.



- 2 Select a profile you want to associate your Non-VeloCloud Site of type **Microsoft Azure Virtual Hub** and click the icon under the **Device** column.



The **Device Settings** page for the selected profile appears.

- 3 Go to **Cloud VPN** area and enable Cloud VPN by turning the toggle button to **On**.
- 4 Under **Branch to Non-VeloCloud Site**, select the **Enable** checkbox.
- 5 From the drop-down menu, select your Non-VeloCloud Site of type **Microsoft Azure Virtual Hub** to establish VPN connection between the branch and the Microsoft Azure Non-VeloCloud Site.
- 6 Click **Save Changes**.

## Results

A tunnel is established between the branch and the Microsoft Azure Non-VeloCloud Site. For more information, see [Configure Branch to VPNs](#).

## Edit a VPN Site

Describes how to add SD-WAN routes into the Azure network manually.

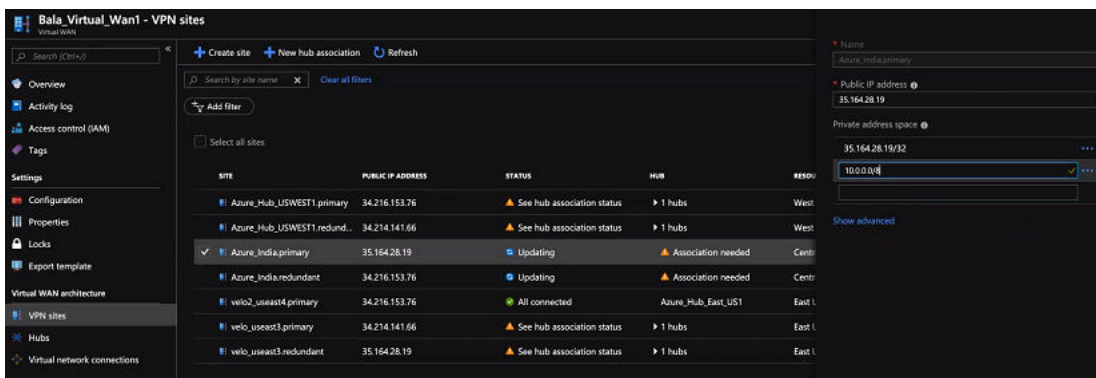
To add SD-WAN routes manually in to the Azure network:

### Prerequisites

Ensure you have completed provisioning the Azure VPN sites at the VCO side.

## Procedure

- 1 Log in to your [Microsoft Azure](#) account.  
The **Microsoft Azure** home screen appears.
- 2 Go to **All resources** and from the list of available resources, select the Virtual WAN that you have created.
- 3 Under the **Virtual WAN architecture** area, click **VPN sites**.
- 4 From the available list of VPN sites, select your VPN site (for example, *Non-VeloCloud site name.primary*), that is added as a result of NVS provisioning step done using the VCO.
- 5 Click on the name of the selected VPN site and from the top of the next screen, select **Edit site**.



- 6 In the **Private address space** text box, enter the address range for the SD-WAN routes.
- 7 Click **Confirm**.

Similarly, you can edit your Redundant VPN site by following the above steps.

## Synchronize VPN Configuration

After successful Non-VeloCloud Site (NVS) provisioning, whenever there are changes in the endpoint IP address of the Azure Hub or static routes, you need to resynchronize Azure Virtual Hub and NVS configurations. Clicking the **Resync configuration** button in the **Non-VeloCloud Sites** area will automatically fetch the VPN configuration details from the Azure portal and will update the VCO local configuration.

## Delete a Non-VeloCloud Site

Describes the steps to delete a VCO's Non-VeloCloud Site (NVS) corresponding to the Azure's Virtual Hub and thereby ensure Virtual WAN deployment state is consistent between the VeloCloud Orchestrator (VCO) and Azure following the deletion.

### Procedure

- 1 Delete the Azure VPN Connections associated to the VPN Sites targeted for deletion.

- 2 Delete the Azure VPN Sites provisioned on behalf of the NVS VCGs selected for that Virtual Hub by using an Azure API.

---

**Note** Deletion of the Azure VPN Sites will fail if the VPN connections associated to the VPN Sites (targeted for deletion) are not removed.

---

# VeloCloud Edge Appliance Documentation

# 25

To access VMware SD-WAN by VeloCloud Edge Appliance quick start guides and user manuals, please visit <https://www.velocloud.com/get-started/>