



## vEdge Cloud Router

The vEdge Cloud is a virtualized version of the vEdge router, inheriting all the capabilities offered on Viptela's physical branch routers. vEdge Cloud can be instantiated as a virtual machine (VM) on a KVM hypervisor or as a VM on a VMware ESXi hypervisor, as well as in public cloud environments, such as Amazon AWS or Google Cloud Platform. vEdge Cloud can be used as a Virtual Network Function (VNF) for a Virtual CPE (vCPE) deployment at the branch. It can also be used as a Virtual Private Cloud (VPC) Gateway for customers that have workload residing in Amazon Web Services (AWS).

### Start and Configure the vEdge Cloud Router

To start the vEdge Cloud router, you create a VM instance for it on a server on which the VMware vSphere ESXi Hypervisor or the Kernel-based Virtual Machine (KVM) Hypervisor software is installed. For server requirements, see [Server Hardware Requirements](#).

To create a vEdge Cloud VM instance, see [Deploy the vEdge Routers](#).

To configure the vEdge Cloud router, see [Configure the vEdge Routers](#).

### vEdge Cloud Router Default Configuration

Each vEdge Cloud router has a default configuration. The default configuration file sets the default CLI prompt to vEdge#, configures OMP, and enables logging of syslog messages to a file.

The default configuration file looks like this:

```
vEdge# show running-configsystem host-name vedge vbond ztp.viptela.com aaa auth-order
local radius tacacs usergroup basic task system read write task interface read write
! usergroup netadmin ! usergroup operator task system read task interface read
task policy read task routing read task security read ! user admin password
$6$FlrfcIs0C/GI3RPs$jo/<wbr/>wLF0Ivv2aOlsIW03qThVIFAVjpoIbz<wbr/>1EzckuzFLXvK59UhpccF7rtqY6ni<wbr/>eg/0m.X85SxShYxy9PQ7.r.
!! logging disk enable !!omp no shutdown graceful-restart advertise connected
advertise static!security ipsec authentication-type ah-shal-hmac sha1-hmac !!vpn 0 interface
ge0/0 ip dhcp-client tunnel-interface encapsulation ipsec no allow-service bgp
allow-service dhcp allow-service dns allow-service icmp no allow-service sshd no
allow-service netconf no allow-service ntp no allow-service ospf no allow-service
stun ! no shutdown !!vpn 512 interface eth0 ip dhcp-client no shutdown !!
```

- [Declaration of Conformity, on page 2](#)

# Declaration of Conformity

The Viptela products are controlled under the Commerce Control List (CCL) of the U.S. Export Administration Regulations (EAR) as networking equipment within the following U.S. Export Control Classification Numbers (ECCN): 5A002, 5D002, and 5E002.

The vEdge hardware and software products and the Viptela encryption technology can be delivered to most end users and destinations worldwide without a licensing requirement. The Viptela solution and products have undergone a one-time review by the Government of the United States of America and qualify for License Exception ENC. As such, they are eligible for export according to Section 740.17 of the EAR.

The Viptela solutions and products can be delivered to most end users worldwide, except to entities or end users in the following countries: Cuba, Iran, North Korea, Sudan, and Syria.

## Controlled Technologies

Viptela manages technology subject to the U.S. Export Administration Regulations (EAR). These controlled technologies may include items under U.S. ECCN 5E002 encryption technology. The Viptela encryption technology is for the development, production, and use of Viptela products that implement or use encryption.

The Viptela software distribution policy allows only authenticated users to download the Viptela encryption software. Recipients of controlled technology are obliged to maintain adequate controls to prevent nationals from outside the U.S. and Canada from accessing Viptela information, subject to ECCN5E002, without first obtaining authorization from the U.S. government.

For additional information on controlled technologies, please contact Viptela support at [support@viptela.com](mailto:support@viptela.com).