Cisco cEdge Routers running IOS XE 17.12 with SD-WAN 20.12

Common Criteria Operational User Guidance and Preparative Procedures

Version: 0.9
Date: 18 December 2024
EDCS: 24706872

Americas Headquarters:
Cisco, Inc. 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Table of Contents

List of Tables

List of Figures

Acronyms

The following acronyms and abbreviations are common and may be used in this Security Target:

Table 1 Acronyms

Acronyms/Abbreviations	Definition
AAA	Administration, Authorization, and Accounting
ACL	Access Control List
AES	Advanced Encryption Standard
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CLI	Command Line Interface
CIMC	Cisco Integrated Management Controller
CM	Configuration Management
DHCP	Dynamic Host Configuration Protocol
DTLS	Datagram Transport Layer Security
EAL	Evaluation Assurance Level
GE	Gigabit Ethernet port
HTTPS	Hyper-Text Transport Protocol Secure
IKE	Internet Key Exchange
IOS	Internet Operating System
IP	Internet Protocol
IPsec	Internet Protocol Security
LAN	Local Area Network
LOM	LAN on Motherboard
NAT	Network Address Translation
NIC	Network Interface Controller
NIM	Network Interface Module
NTP	Network Time Protocol
OS	Operating System
OMP	Overlay Management Protocol
PoE	Power over Ethernet
PP	Protection Profile
SA	Security Association
SD-WAN	Software Defined Wide Area Network
SFP	Small-form-factor pluggable port
SHS	Secure Hash Standard
SNMP	Simple Network Management Protocol
ST	Security Target
SSH	Secure Shell Protocol
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSC	TSF Scope of Control

TSF	TOE Security Function
TSP	TOE Security Policy
UCS	Unified Computing System
UDP	User Datagram Protocol
vKVM	Virtual Keyboard, Video, and Mouse
VM	Virtual Machine
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
VS	Virtual System
WAN	Wide Area Network

Terminology

The following acronyms and abbreviations are common and may be used in this Security Target:

Table 2 Terminology

Term	Definition
Administrator	Synonymous with Authorized Administrator for the purposes of this evaluation.
Authorized Administrator	Any user which has been assigned to a privilege level that is permitted to perform all TSF-related functions.
cEdge (Router)	cEdge routers are routers that provide connectivity across the SD-WAN fabric and forward across the data plane. They are typically located at the remote/branch location, but mat be located in an enterprise data center as well. cEdge routers are Cisco routers running IOS-XE based SD-WAN capable software.
ESXi	ESXi is an enterprise-class hypervisor developed by VMware for deploying and serving virtual devices.
SD-WAN	The Cisco Software Defined – Wide Area Network (SD-WAN) Solution, is a software-based solution that reduces the costs of running enterprise networks and provides straightforward tools to simplify the provisioning and management of large and complex networks that are distributed across multiple locations and geographies. Cisco Software Defined Wide Area Network (SD-WAN) fabric, also called an overlay network, forms a software overlay that runs over standard network transport services, including the public Internet, MPLS, and broadband.
Security Administrator	Synonymous with Authorized Administrator for the purposes of this evaluation.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
vBond	Cisco vBond Orchestrator, automatically authenticates all other Cisco cEdge devices when they join the Cisco SD-WAN overlay network.
vManage	Cisco vManage provides a highly visualized dashboard that simplifies network operations. It provides centralized configuration, management, operation, and monitoring across the entire SD-WAN fabric.
vSmart	Cisco vSmart Controllers, oversee the control plane of the Cisco SD-WAN fabric, efficiently managing provisioning, maintenance, and security for the entire Cisco SD-WAN overlay network.

Document Introduction

Prepared By:
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), Cisco cEdge Routers running IOS XE 17.12 with SD-WAN 20.12. This Operational User Guidance with Preparative Procedures addresses the administration of the TOE software and hardware and describes how to install, configure, and maintain the TOE in the Common Criteria evaluated configuration. Administrators of the TOE may be referred to as administrators, authorized administrators, privileged administrators, semi-privileged administrators, security administrators, and TOE administrators in this document.

Revision History

Version	Date	Change
0.1	January 12, 2024	Initial Version
0.2	May 7, 2024	Addressing lab ORs
0.3	August 7, 2024	Addressing lab ORs
0.4	August 19, 2024	Addressing lab ORs
0.5	September 28, 2024	Addressing lab ORs
0.6	October 25, 2024	Various fixes
0.7	December 11, 2024	Minor fixes
0.8	December 16, 2024	Addressing lab ORs
0.9	December 18, 2024	Minor fixes

1 INTRODUCTION

This Operational User Guidance with Preparative Procedures documents the administration of Cisco cEdge Routers running IOS XE 17.12 with SD-WAN 20.12, the TOE, as it is certified under Common Criteria. Cisco cEdge Routers running IOS XE 17.12 with SD-WAN 20.12 is hereinafter referred to as Cisco cEdge Router(s), Cisco SD-WAN cEdge device(s), or simply the TOE.

Cisco cEdge routers running IOS XE 17.12 with SD-WAN 20.12 is a distributed TOE which consists of cEdge routers running IOS XE version 17.12 and version 20.12 SD-WAN controller. Cisco cEdge Routers running IOS XE 17.12 with SD-WAN 20.12 are comprised of physical devices and virtual machines (VMs). The cEdge routers are purpose-built routing platforms that include firewall functionality provided by the Cisco IOS XE software. SD-WAN is a software-defined WAN solution that provides a software overlay running over standard network transport and simplifies WAN management. The SD-WAN controllers are separate virtual machines running on the same ESXi server to handle management, provisioning, and maintenance of the cEdge routers.

VM's are deployed one of two different models of the Cisco Unified Computing System™ (Cisco UCS), UCS C220 M5S or UCS C240 M5S, which is running VMware's ESXi hypervisor software. The physical devices and VM's together constitute the TOE.

The UCS Server and ESXi virtualization software comprise the Virtual System (VS) which is part of the Evaluated Configuration used to evaluate the TOE, and not considered to be part of the TOE themselves.

1.1 Audience

This document is written for administrators configuring the TOE. This document assumes that you are familiar with the basic concepts and terminologies used in internetworking, have an understanding of your network topology and the protocols that the devices in your network can use, and are trained to use the operating systems on which you are running your network.

It is also assumed you are familiar with virtualization, virtual network devices, and have an understanding of the CISCO SD-WAN solution and are a trusted individual.

1.2 Purpose

This document is the Operational User Guidance with Preparative Procedures for the Common Criteria evaluation. It was written to highlight the specific TOE configuration and administrator functions and interfaces that are necessary to configure and maintain the TOE in the evaluated configuration. The evaluated configuration is the configuration of the TOE that satisfies the requirements as defined in the Security Target (ST). This document does not mandate configuration settings for the features of the TOE that are outside the evaluation scope, which should be set according to your organizational security policies.

This document is not meant to detail specific actions performed by the administrator but rather is a road map for identifying the appropriate locations within Cisco documentation to get the specific details for configuring and maintaining SD-WAN operations. It is recommended that you read all instructions in this document and any references before performing steps outlined and entering commands. Section 5.2 Obtaining Technical Assistance of this document provides information for obtaining assistance.

1.3 Document References

This section lists the Cisco Systems documentation that is also the Common Criteria Configuration Item (CI) List. The documents used are shown below in Table 3. Throughout this document, the guides may be referred to by the "#", such as **[1]** rather than **Cisco SD-WAN Design Guide**.

Table 3 Cisco Documentation

#	Title	Link
[1]	Cisco SD-WAN Design Guide	https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-design-guide.html
[2]	Cisco Catalyst SD-WAN Getting Started Guide	https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book.html
[3]	Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Recommended Computing Resources	https://www.cisco.com/c/en/us/td/docs/routers/sdwan/release/notes/compatibility-and-server-recommendations.html
[4]	Hardware Install Guides: (a) Cisco UCS C220 M5 Server Installation and Service Guide (b) Cisco UCS M240 M5 Server Installation and Service Guide	(a) https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/hw/C220M5/install/C220M5.html (b) https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/hw/C240M5/install/C240M5.html
[5]	VMware ESXi Installation and Setup, VMware ESXi 7.0	https://docs.vmware.com/en/VMware-vSphere/7.0/vsphere-esxi-703-installation-setup-guide.pdf
[6]	SD-WAN Controller Setup Guide (On-Prem, Non Cloud-Managed)	https://community.cisco.com/t5/networking-knowledge-base/sd-wan-controller-setup-guide-on-prem-non-cloud-managed/ta-p/3921360
[7]	Cisco SD-WAN Controller Certificates and Authorized Serial Number File Prescriptive Deployment Guide	https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-controller-cert-deploy-guide.html
[8]	Cisco ASR 1001-HX Router and Cisco ASR 1002-HX Router Hardware Installation Guide	https://www.cisco.com/c/en/us/td/docs/routers/asr1000/install/guide/1001HX_1002HX/b_ASR1001HX-1002HX_HIG.html
[9]	Hardware Installation Guide for Cisco 4000 Series Integrated Services Routers	https://www.cisco.com/c/en/us/td/docs/routers/access/4400/hardware/installation/guide4400-4300/C4400_isr.html
[10]	Hardware Installation Guide for Cisco Catalyst 8300 Series Edge Platforms	https://www.cisco.com/c/en/us/td/docs/routers/cloud_edge/c8300/hardware_installation/b-catalyst-8300-series-edge-platforms-hig.html

#	Title	Link
[11]	Cisco Catalyst 8500 Series Edge Platforms Hardware Installation Guide	https://www.cisco.com/c/en/us/td/docs/routers/cloud_edge/c8500/hardware-installation-guide/b_C8500_HIG.html
[12]	Cisco Catalyst 8000V Edge Software Installation And Configuration Guide	https://www.cisco.com/c/en/us/td/docs/routers/C8000V/Configuration/c8000v-installation-configuration-guide.html
[13]	Cisco Catalyst SD-WAN Portal Configuration Guide	https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/self-serv-por/sdwan-ssp.html
[14]	Cisco Catalyst SD-WAN Segmentation Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x	https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/segmentation/ios-xe-17/segmentation-book-xe.html
[15]	Cisco Catalyst SD-WAN Routing Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x	https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/routing/ios-xe-17/routing-book-xe.html
[16]	Configure Basic Parameters to Form Control Connections on cEdge	https://www.cisco.com/c/en/us/support/docs/routers/xe-sd-wan-routers/218137-configure-basic-parameters-to-form-contr.html
[17]	Cisco Catalyst SD-WAN Command Reference	https://www.cisco.com/c/en/us/td/docs/routers/sdwan/command/sdwan-cr-book.html
[18]	Cisco SDWAN Viptela - Whitelist Serial.Viptela File	https://community.cisco.com/t5/networking-blogs/cisco-sdwan-viptela-whitelist-serial-viptela-file/ba-p/4044876
[19]	Cisco Catalyst SD-WAN Policies Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x	https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/ios-xe-17/policies-book-xe.html
[20]	Cisco Catalyst SD-WAN Security Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x	https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/ios-xe-17/security-book-xe.html
[21]	Using Cisco IOS Software Command Reference - Copy	https://www.cisco.com/E-Learning/bulk/public/tac/cim/cib/using_cisco_ios_software/cmdrefs/copy.htm

1.4 Supported Hardware and Software

The TOE is distributed and comprised of a Virtual Machine (VM) deployment Cisco vManage, a VM deployment of Cisco vSmart, and Cisco vBond, and at least one of the evaluated Cisco cEdge routers. One of the cEdge router solutions is deployed as a virtual machine, while the remaining are physical routers. Virtual and physical routers alike run the Cisco IOS-XE software. The controllers run SD-WAN 20.12 software. The cEdge devices run Cisco IOS-XE 17.12 which is supported with SD-WAN 20.12. Virtual machines are deployed on a virtual system.

The UCS Server and ESXi virtualization software comprise the Virtual System (VS) which is part of the Evaluated Configuration used to evaluate the TOE. The Virtual System is comprised of a single Cisco Unified Computing System™ (Cisco UCS) C220 or C240 M5 Rack Server with Intel Xeon Scalable 2nd Generation (Cascade Lake) processor(s). The bios, firmware, drivers, management software are the same for both models, the UCS C240 M5 is just a more robust server than the smaller C220 M5. VMWare's ESXi 7.0 hypervisor software is running on the UCS server.

Using Virtual System hardware and software components not specified in the ST invalidates the secure configuration. Likewise, using any TOE hardware and software version other than the evaluated software listed in the ST will invalidate the secure configuration. Foe details regarding approved Toe and Virtual System hardware and software, please reference Section 1.7 Physical Scope of the TOE in the Security Target (ST).

Once installed and configured, the TOE is managed via a web browser by an Authorized Administrator using a web browser on a remote management device such as a laptop to access vManage. There may be instances, such as troubleshooting and maintenance related events, when an Authorized Administrator may also connect to vManage via SSH. Additionally, the Administrator may access the TOE via a virtual serial port. This function is fulfilled by the ESXi remote local console. Use of the virtual serial port is typically limited to initial install and during times where network connectivity in an environment may not be available. Management of the other components of the TOE are performed though vManage.

1.5 Operational Environment

1.5.1 Supported non-TOE Hardware/Software/Firmware

The TOE supports (in some cases optionally) the following hardware, software, and firmware in its environment:

Table 4 Operational Environment Components

Component	Required	Usage/Purpose Description for TOE performance
Management Workstation with SSH Client	Yes	This includes any IT Environment Management workstation with a SSH client installed that is used by the TOE administrator to support TOE administration through SSH protected channels. Any SSH client that supports SSHv2 may be used.
Management Workstation with Web Browser using HTTPS	Yes	This includes any IT Environment Management workstation with a supported web browser installed that is used by the TOE administrator to support TOE administration through HTTPS-TLS protected channels.
Management Workstation with Local Console	Yes	For a physical device this includes any IT Environment Console that is directly connected to the TOE via the Serial Console Port and is used by the TOE administrator to support TOE administration. In the case of the VMs, this function is fulfilled by the ESXi remote local console.
Audit (syslog) Server	Yes	This includes any syslog server to which the TOE would transmit syslog messages. Also referred to as audit server in the ST.
VMWare ESXi 7.0	Yes	This includes the hypervisor required for all virtual machines (SD-WAN controllers and C8000V) to run.

1.6 Excluded Functionality

The following functionality is excluded from the evaluation:

Table 5 Excluded Functionality

Excluded Functionality	Exclusion Rationale
SNMP: The Simple Network Management Protocol is an application layer protocol, facilitates the exchange of management information among network devices	SNMP is not associated with Security Functional Requirements claimed.
Telnet	Telnet sends authentication data in plain text. This feature must remain disabled in the evaluated configuration. SSHv2 must be used to secure the trusted path for remote administration for all SSHv2 sessions.
Unified Security Policy / Unified Threat Defense	This feature allows to configure a single unified security policy for firewall and Unified Threat Defense (UTD) security features such as IPS, Cisco URL Filtering, AMP, and TLS/SSL proxy. This is out of scope for the evaluation.

These services will be disabled by configuration settings.

2 SECURE ACCEPTANCE OF THE TOE

To ensure the correct TOE is received, the TOE physical and virtual components should be examined to ensure that that is has not been tampered with during delivery. As a number of the TOE components are virtual machine, the authorized administrator is also advised to investigate the components of the virtual system (VS) as well.

2.1 VS Physical Hardware (UCS) Acceptance

Verify that the VS hardware was not tampered with during delivery performing the following actions:

Step 1 Before unpacking the VS hardware (UCS server), inspect the physical packaging the equipment was delivered in. Verify that the external cardboard packing is printed with the Cisco Systems logo and motifs. If it is not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 2 Verify that the packaging has not obviously been opened and resealed by examining the tape that seals the package. If the package appears to have been resealed, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 3 Verify that the box has a white tamper-resistant, tamper-evident Cisco Systems bar coded label applied to the external cardboard box. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). This label will include the Cisco product number, serial number, and other information regarding the contents of the box.

Step 4 Record the serial number of the VS hardware (UCS server) on the shipping documentation. The serial number displayed on the white label affixed to the outer box will be that of the device. Verify the serial number on the shipping documentation matches the serial number on the separately mailed invoice for the equipment. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 5 Verify that the box was indeed shipped from the expected supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). This can be done by verifying with the supplier that they shipped the box with the courier company that delivered the box and that the consignment number for the shipment matches that used on the delivery. Also, verify that the serial numbers of the items shipped match the serial numbers of the items delivered. This verification should be performed by some mechanism that was not involved in the actual equipment delivery, for example, phone/FAX or other online tracking service.

Step 6 Unpack and Inspect the Cisco Unified Computing System™ UCS C220 M5 Rack Server [1RU] or the UCS C240 M5 2 Rack Unit (2RU) on which ESXi and the SD-WAN VM's are installed or will be installed. Verify that the serial number displayed on the unit itself matches the serial number on the shipping documentation and the invoice. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). Also, verify that the unit has the following external indication:

Table 6 VS Server External Identification

Component	Required	Usage/Purpose Description for TOE performance
Cisco Unified Computing System™ (Cisco UCS)	C220 M5S	UCS C220 M5S
Cisco Unified Computing System™ (Cisco UCS)	C240 M5S	UCS C240 M5S

2.2 VS Software (Hypervisor) Acceptance

Assuming the hypervisor software is already installed, verify the version of the installed software.

Step 1 Log into the UCS Server Cisco Integrated Management Controller (CIMC).

Step 2 Click the link for "Launch vKVM".

Step 3 Click the vKVM Viewer Link

https://[CIMC_IP]:/html/kvmViewer.html

Step 4 You are now at the virtual serial connection for ESXi. The ESXi version number may be read from screen, for example:

VMWare ESXi 7.0.3 (VMKernel Release Build 22348816)

NOTE: *Installing ESXi is beyond the scope of this document. Should an Administrator desire to install, or upgrade to the approved ESXi version, please reference* ***[5] VMware ESXi Installation and Setup, VMware ESXi 7.0*** *as well as the VMWare website ESXi product page:*

2.3 Physical Router (TOE - cEdge) Acceptance

Verify that the TOE physical cEdge router software and hardware were not tampered with during delivery by performing the following actions:

Step 1 Before unpacking the TOE, inspect the physical packaging the equipment was delivered in. Verify that the external cardboard packing is printed with the Cisco Systems logo and motifs. If it is not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 2 Verify that the packaging has not obviously been opened and resealed by examining the tape that seals the package. If the package appears to have been resealed, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 3 Verify that the box has a white tamper-resistant, tamper-evident Cisco Systems bar coded label applied to the external cardboard box. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). This label will include the Cisco product number, serial number, and other information regarding the contents of the box.

Step 4 Note the serial number of the TOE on the shipping documentation. The serial number displayed on the white label affixed to the outer box will be that of the device. Verify the serial number on the shipping documentation matches the serial number on the separately mailed invoice for the equipment. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 5 Verify that the box was indeed shipped from the expected supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). This can be done by verifying with the supplier that they shipped the box with the courier company that delivered the box and that the consignment note number for the shipment matches that used on the delivery. Also verify that the serial numbers of the items shipped match the serial numbers of the items delivered. This verification should be performed by some mechanism that was not involved in the actual equipment delivery, for example, phone/FAX or other online tracking service.

Step 6 Once the TOE is unpacked, inspect the unit. Verify that the serial number displayed on the unit itself matches the serial number on the shipping documentation and the invoice. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 7 Approved methods for obtaining a Common Criteria evaluated software images:

- Download the Common Criteria evaluated software image file from Cisco.com onto a trusted computer system.
- Software images are available from Cisco.com at the following: http://www.cisco.com/cisco/software/navigator.html.
- The TOE ships with the correct software images installed; however, this may not be the evaluated version.

Step 8 Once the file is downloaded, verify that it was not tampered with by using a SHA-512 utility to compute a SHA-512 hash for the downloaded file and comparing this with the SHA-512 hash for the image listed in Table 5 below. If the SHA-512 hashes do not match, contact Cisco Technical Assistance Center (TAC),

http://www.cisco.com/techsupport.

Step 9 To verify the digital signature prior to installation, the show software authenticity file command allows you to display software authentication related information that includes image credential information, key type used for verification, signing information, and other attributes in the signature envelope, for a specific image file. The command handler will extract the signature envelope and its fields from the image file and dump the required information. The show software authenticity file command allows you to display software authentication related information that includes image credential information, key type used for verification, signing information, and other attributes in the signature envelope, for a specific image file. The command handler will extract the signature envelope and its fields from the image file and dump the required information. To display the software public keys that are in the storage with the key types, use the **show software authenticity keys** command in privileged EXEC mode.

TOE-common-criteria# **show software authenticity file** {**bootflash0**:filename | **bootflash1**:filename | **bootflash**:filename | **nvram**:filename | **usbflash0**:filename | **usbflash1**:filename}

To display information related to software authentication for the current ROM monitor (ROMMON), monitor library (monlib), and Cisco IOS image used for booting, use the show software authenticity running command in privileged EXEC mode If the output from **the show software authenticity file** command does not provide expected output, contact Cisco Technical Assistance Center (TAC), http://www.cisco.com/techsupport.

After verifying the digital signature with the show software authenticity file command, an upgrade and reboot should be configured on the router. The router will not boot if the digital signature is not valid, and an error will be displayed on the console: autoboot: boot failed, restarting...

Step 10 To install and configure the router follow the instructions as described in the Configuration Fundamentals Configuration Guide. After powering on your router, confirm that the TOE loads the image correctly, completes internal self-checks and displays the cryptographic export warning on the console.

Step 11 The end-user must confirm once the TOE has booted that they are indeed running the evaluated version. Use the "**show version**" command to display the currently running system image filename and the system software release version. It is also recommended the license level be verified and activated. It is assumed the end-user has acquired a permanent license is valid for the lifetime of the system on which it is installed.

Table 7 Evaluated cEdge Software Images

Models	Software Version	Image Name	Image hash values
ASR1001-HX, ASR1002-HX,	IOS XE 17.12	asr1000-universalk9.17.12.02.SPA.bin (749.94 MB)	06064503d790c414e56a9e78d53d71d010d70d9c06c4842a9dc90005983255d54b534478c638fad276277b5506c94ea3cddcc45ea46a8e631efbc9996ed1cf24
ISR4461		isr4400v2-universalk9.17.12.02.SPA.bin (813.21 MB)	aea237a7d1084bb505b1f6ca27408860211453cde51d11220a14a27c39e13e27e16b9096030a313d901fa3f3c22875269698dd64b24003cbd547059dbeb67724
C8300-1N1S-6T C8300-2N2S-6T		c8000be-universalk9.17.12.02.SPA.bin (837.04 MB)	7d7df2eed8a312f8872b6a847451b2cf64d1571a867be13615a0256cf1363250dbcc19f215b1c5b5f1312df9e9d880f35053982922aa92e2a810d7fa26f0acab
C8500-12X		c8000aep-universalk9.17.12.02.SPA.bin (749.94 MB)	3f7709b031e62ded4a0ee3a2da929a7f157d3a2cf1b7733212148ccfba5921d5ff720bf9df1cb32b21fbbe8eb38aa8171032e25a928b902be7c0e547d7fcb27b
C8000V		c8000v-universalk9.17.12.02.SPA.bin (820.33 MB) c8000V-universalk9.17.12.02.ova (895.99 MB)	894c489470ec2c4ca373f1096093f12b8b215e15180e9d3be0ff4853d4a2b478d1cdf33ad1e715a58e32eacf0f9f32224a000c460a98a416d77c0ef7af3d502a 3be618adcce6d97ecfd23c0d2248ff835eb6636a53290a6ce357d9eaeb087ef86459cce3520471dc5c1a1b58e7ac148364c54b2bcf35e4ec463b43160e4288dd

2.4 Virtual Router (TOE - cEdge) Acceptance

2.4.1 C8000V (TOE) Software – Pre-Installed

When accepting pre-installed controllers, it is assumed the Authorized Administrator has already confirmed the VS components were received from a known vendor and that the VS components showed no evidence of tampering.

Verify that the TOE virtual cEdge router software was not tampered with during delivery by performing the following actions:

Step 1 Boot the Catalyst 8000V Edge by starting the VM in ESXi. Launch the ESXi remote local console.

The TOE will automatically display the hash verification on boot or by using the reload command. The successful hash verification message will display on the successful verification of the boot image. If the image was tampered with in any way, an error would display, and the image will not boot. Confirm that the C8000V loads the image correctly, completes internal self-checks and displays the cryptographic export warning on the console.

Once the image is loaded into bootflash to display information related to software authenticity for a specific image file from the Command Line Interface (CLI), log into the device and use the **verify** command.

For example:

```
C8000V# verify C8000V-mono-universalk9.17.12.01a.SPA.pkg

Verifying file integrity of bootflash:C8000V-universalk9.17.12.01.SPA.pkg...........................................................................................................
...................................................................................................................................

Embedded Hash   SHA1 : 55220DF07C477530A41598C43827B96C6E85D086

Computed Hash   SHA1 : 55220DF07C477530A41598C43827B96C6E85D086

Starting image verification

Hash Computation:    100%Done!

Computed Hash SHA2:
65401c1ebd964835b7e39ed8d5e56277efdcdcd42c817a80a51dc024bb29bdbe7a4b63087ebdf33c4a
4e1789c41a245ba45d9e7aaadc0f1f134e837896f0dd13


Embedded Hash SHA2:
65401c1ebd964835b7e39ed8d5e56277efdcdcd42c817a80a51dc024bb29bdbe7a4b63087ebdf33c4a
4e1789c41a245ba45d9e7aaadc0f1f134e837896f0dd13


Digital signature successfully verified in file bootflash:C8000V-mono-universalk9.17.12.01.SPA.pkg
```

If the image is corrupted, then the following will result:

```
C8000V# verify C8000V-mono-universalk9.17.12.01.SPA.pkg.BAD.SPA

%Error verifying C8000V-mono-universalk9.17.12.01.SPA.pkg.BAD.SPA: Digital signature is not present


C8000V#

*Jul 16 19:37:58.339: %DIGISIGN-4-SIGNATURE_NOT_PRESENT: %WARNING: Digital

signature is not found in file C8000V-mono-universalk9.17.12.01.SPA.pkg.BAD.SPA
```

If the image verification does not complete successfully, contact Cisco Technical Assistance Center (TAC) https://www.cisco.com/c/en/us/support/index.html.

Step 2 The end-user must confirm once the TOE has booted that they are indeed running the evaluated version. Use the "show version" command to display the currently running system image filename and the system software release version.

NOTE: *When updates, including PSIRTS (bug fixes) to the evaluated image are posted, customers are notified that updates are available (if they have purchased continuing support). For information on how to download and verify updates and provided information on how to verify the updates reference* ***2.4.2 C8000V (TOE) Software – Download****.*

2.4.2 C8000V (TOE) Software – Download

The authorized administrator may download current virtual cEdge router software by following these steps:

Step 1 Go to Cisco's Software Download Page

https://software.cisco.com/download/home

Step 2 Enter **Catalyst 8000V Edge Software** in the **Select a Product** field and then click the **Search Icon.**

Step 3 Click **Catalyst 8000V Edge Software** link and then select the **IOS XE Software** link.

Step 4 Select the **Dublin-17.12.2a(ED)** release

Step 5 Choose the type of software to download.

The following file types are available in the Expressway software image package and are used to install or upgrade, respectively, the Expressway software on a hypervisor.

.OVA - Used for deploying the VM and installing the software image on the VM
Description: Cisco Catalyst 8000V IOS XE Universal - Crypto OVA
Release: Cupertino-17.12.2

File Name: **C8000V-universalk9.17.12.02.ova**

.ISO - Used for installing the software image on the VM

Description: Cisco Catalyst 8000V IOS XE Universal - Crypto ISO
Release: Cupertino-17.12.2
File Name: **C8000V-universalk9.17.12.2.iso**

.BIN - Used for upgrading the image on an existing Expressway VM.

Description: Cisco Catalyst 8000V Edge Software
Release: Cupertino-17.12.2
File Name: **C8000V-universalk9.17.12.02.SPA.bin**

NOTE: *The .OVA file is used to both install the VM and installing the router software image. It is recommended to use this option when installing a new VM as it ensures the VM is build according to Cisco specifications. An administrator may manually build a VM and deploy the router using the .ISO image. Also, if an existing VM exists on an earlier load, the VM virtual router may be upgraded using the .BIN image.*

NOTE: *Hovering over the .OVA or the.TAR.GZ file will bring up a pop-up window that includes a SHA512 checksum that will be used to verify a successful download.*

Step 6 For the desired software package, click Download Now or Add to Cart. And then follow the instructions for downloading the software.

Step 7 After downloading the software image, the Administrator should compute the SHA512 checksum of the local/downloaded copy of the software. If the checksum matches the value published by Cisco, then the software was downloaded successfully, and the install/upgrade may commence.

If the checksum values do not match, the Administrator may wish to download the software again. If the values still do not match, the Administrator should investigate the reason for the discrepancy. This may include reaching out to Cisco Technical Assistance Center (TAC) if needed.

The table below shows the evaluated version of Expressway software.

Table 8 Evaluated cEdge Virtual Router Image

Models	Software Version	Image Name	Image hash values
C8000V	IOS XE 17.12	C8000V-universalk9.17.12.02.ova	3be618adcce6d97ecfd23c0d2248ff835eb6636a53290a6ce357d9eaeb087ef86459cce3520471dc5c1a1b58e7ac148364c54b2bcf35e4ec463b43160e4288dd
		C8000V-universalk9.17.12.02.iso	62805becf756e6e59d72e1fa51bcb5b0eb9e09b71524364dc823b5da0f813ce0ba3326e8fc5c

Models	Software Version	Image Name	Image hash values
			0e6cd63ef135a54b83476ce3456182e5ddcb2 0c9331ce81c7178
		C8000V-universalk9.17.12.02.SPA.bin	894c489470ec2c4ca373f1096093f12b8b215e 15180e9d3be0ff4853d4a2b478d1cdf33ad1e7 15a58e32eacf0f9f32224a000c460a98a416d77 c0ef7af3d502a

Step 8 After determining that the checksums match, install the downloaded software image onto a supported Hypervisor as described in **[1] Cisco Catalyst 8000V Edge Software Installation and Configuration Guide** chapter **Installing in VMware ESXi Environment**.

Step 9 Boot the Catalyst 8000V Edge as described in **[1] Cisco Catalyst 8000V Edge Software Installation and Configuration Guide** chapter **Configuring Console Access section Booting the Cisco Catalyst 8000V as the VM.**

The TOE will automatically display the hash verification on boot or by using the reload command. The successful hash verification message will display on the successful verification of the boot image. If the image was tampered with in any way, an error would display and the image will not boot. Confirm that the C8000V loads the image correctly, completes internal self-checks and displays the cryptographic export warning on the console.

Once the image is loaded into bootflash to display information related to software authenticity for a specific image file, use the **verify** command.

For example:

```
C8000V# verify C8000V-mono-universalk9.17.12.01a.SPA.pkg

Verifying file integrity of bootflash:C8000V-universalk9.17.12.01.SPA.pkg..............................................................................................
.......................................................................................................................

Embedded Hash   SHA1 : 55220DF07C477530A41598C43827B96C6E85D086

Computed Hash   SHA1 : 55220DF07C477530A41598C43827B96C6E85D086

Starting image verification

Hash Computation:    100%Done!

Computed Hash SHA2:
65401c1ebd964835b7e39ed8d5e56277efdcdcd42c817a80a51dc024bb29bdbe7a4b63087ebdf33c4a
4e1789c41a245ba45d9e7aaadc0f1f134e837896f0dd13
```

```
Embedded Hash SHA2:
65401c1ebd964835b7e39ed8d5e56277efdcdcd42c817a80a51dc024bb29bdbe7a4b63087ebdf33c4a
4e1789c41a245ba45d9e7aaadc0f1f134e837896f0dd13


Digital signature successfully verified in file bootflash:C8000V-mono-universalk9.17.12.01.SPA.pkg
```

If the image is corrupted, then the following will result:

```
C8000V# verify C8000V-mono-universalk9.17.12.01.SPA.pkg.BAD.SPA
%Error verifying C8000V-mono-universalk9.17.12.01.SPA.pkg.BAD.SPA: Digital signature is not present


C8000V#
*Jul 16 19:37:58.339: %DIGISIGN-4-SIGNATURE_NOT_PRESENT: %WARNING: Digital
signature is not found in file C8000V-mono-universalk9.17.12.01.SPA.pkg.BAD.SPA
```

If the image verification does not complete successfully, contact Cisco Technical Assistance Center (TAC) https://www.cisco.com/c/en/us/support/index.html.

Step 9 The end-user must confirm once the TOE has booted that they are indeed running the evaluated version. Use the “show version” command to display the currently running system image filename and the system software release version.

2.5 Virtual Controllers (TOE - Controllers) Acceptance

2.5.1 Virtual Controllers (TOE) Software – Pre-Installed

When accepting pre-installed controllers, it is assumed the Authorized Administrator has already confirmed the VS components were received from a known vendor and that the VS components showed no evidence of tampering.

Verify that the TOE virtual controller software is correct by performing the following actions:

Step 1 Power on the Controller VM (vManage, vSmart, and vBond) from within ESXi.

Step 2 Identify the software version of each device. There are three ways to identify the software version.

- **From the VMWare Remote Console** enter the necessary credential to log into each controller CLI, and then type “show version”. This will display the active version of software:

  ```
  vManage# show version
  20.12.2
  ```

- **Using and SSH Client** establish a remote SSH session with each controller CLI, enter the necessary credential to log into the CLI, and then type "show version". This produces the same output as using the VMWare Remote Console.

- **Using a Supported Web Browser** establish a remote HTTPS session with the vManage, **https://[CUCM IP or FQDN]** and enter the appropriate credentials. Upon successful login, click the menu in the upper left, then "**Maintenance",** and then "**Software Upgrade**"**.** From that screen select either "**Controller**", which will show the current software version on vSmart and vBond, or select "**vManage**", which will show the current software version on vManage.

Step 3 Verify the installed software version against the validated version. For this certification, the validated version of SD-WAN is 20.12.2. If the version does not match, then follow the steps instruction of section **2.5.2 Virtual Controllers (TOE) Software – Downloaded** in this document.

2.5.2 Virtual Controllers (TOE) Software – Download

The authorized administrator may download current virtual SD-WAN controller software by following these steps:

Step 1 Go to Cisco's Software Download Page

https://software.cisco.com/download/home

Step 2 Enter **SD-WAN** in the **Select a Product** field and then click the **Search Icon**.

Step 3a To download software for a fresh (new or rebuild) of a controller VM, click **SD-WAN** link and then select the **vManage Software, vSmart Software, or vEDGE Cloud** link. If upgrading existing controller, follow Step 3b.

NOTE: *The vBond software is found under the vEDGE Cloud link.*

Step 3b To download software for the upgrade of existing controller VMs, click **SD-WAN** link and then select the **SD-WAN Software update** link.

NOTE: *All controllers need to be installed and communicating with vManage, as the upgrade will be done through vManage.*

Step 4 Select the **20.12.2(ED)** release.

Step 5 Choose the software to download from their respective directories.

Used for deploying the ESXi vManage VM and installing the software image on the VM

Description: vManage New Deployment VMWare Image

Release: 20.12.2

File Name: **viptela-vmanage-20.12.2-genericx86-64.ova**

Used for deploying the ESXi vSmart VM and installing the software image on the VM

Description: vSmart New Deployment VMWare Image

Release: 20.12.2

File Name: **viptela-smart-20.12.2-genericx86-64.ova**

Used for deploying the ESXi vBond VM and installing the software image on the VM

Description: vEdge Cloud and vBond New Deployment VMWare Image

Release: 20.12.2

File Name: **viptela-edge-20.12.2-genericx86-64.ova**

Used for upgrading the vManage appliance

Description: vManage upgrade image

Release: 20.12.2

File Name: **vmanage-20.12.2-x86_64.tar.gz**

Used for upgrading the vSmart and vBond appliances

Description: vSmart and vBond upgrade image

Release: 20.12.2

File Name: **viptela-20.12.2-x86_64.tar.gz**

NOTE: *For fresh installs, software is available in the .OVA, .QCOW2, and .TAR.GZ formats. The evaluated configuration was deployed in an environment using ESXi, so only the .OVA files should be downloaded. Upgrade files are only available in the.TAR.GZ format. These files will be uploaded to the application themselves and are not utilized by ESXi. In other words, the only VM guest operating system and applications are upgraded.*

NOTE: *Hovering over the .OVA or the.TAR.GZ file will bring up a pop-up window that includes a SHA512 checksum that will be used to verify a successful download.*

Step 6 For the desired software package, click Download Now or Add to Cart. And then follow the instructions for downloading the software.

Software details are listed below per controller.

Table 9 Evaluated SD-WAN Controllers Software Images

Models	Software Version	Image Name	Image hash values
vManage	SD-WAN 20.12	viptela-vmanage-20.12.2-genericx86-64.ova	ed9b10c3f077264edb3915359fc69e56c707a7f1d961cd8e2b3d57c0d55de5f074e37a27c45d923eaebdb0489f38b73e46fe21f48bad2dd7ef3bc400fca7c4e6
		vmanage-20.12.2-x86_64.tar.gz	f62edf184cf685570ebbf69e89b5c34843f6e3327738957f4bde9a808fd7200f892146189cc1f9d113605296d735aaa7fb4cae8f76ed34b634cd0220b856de03
vBond		viptela-edge-20.12.2-genericx86-64.ova	b4267f4767626b927e41b61ccd39d4846f582c795ec20eb20bb0de98c3014c7dad5f9fe389ba863ed5c3e1473f51ce26bc2beee88299cfc33d9fc4fbd4d84428
		viptela-20.12.2-x86_64.tar.gz	b56c35cfac386142775c0bb37f96caf9a9f54e8dd6a0cb19415dd8298515e2a825f2ae6a97f5efc0eccd296e2735709d90ab82a59924f793693c83a790335f8f
vSmart		viptela-smart-20.12.2-genericx86-64.ova	4e161e5ac54c9921b325b381e229aa6c6462df37968efb3c280fec811968296b699a1ade0264cfa55e080bedcea077338c61919fb7b6e598aec2686a63669106
		viptela-20.12.2-x86_64.tar.gz	b56c35cfac386142775c0bb37f96caf9a9f54e8dd6a0cb19415dd8298515e2a825f2ae6a97f5efc0eccd296e2735709d90ab82a59924f793693c83a790335f8f

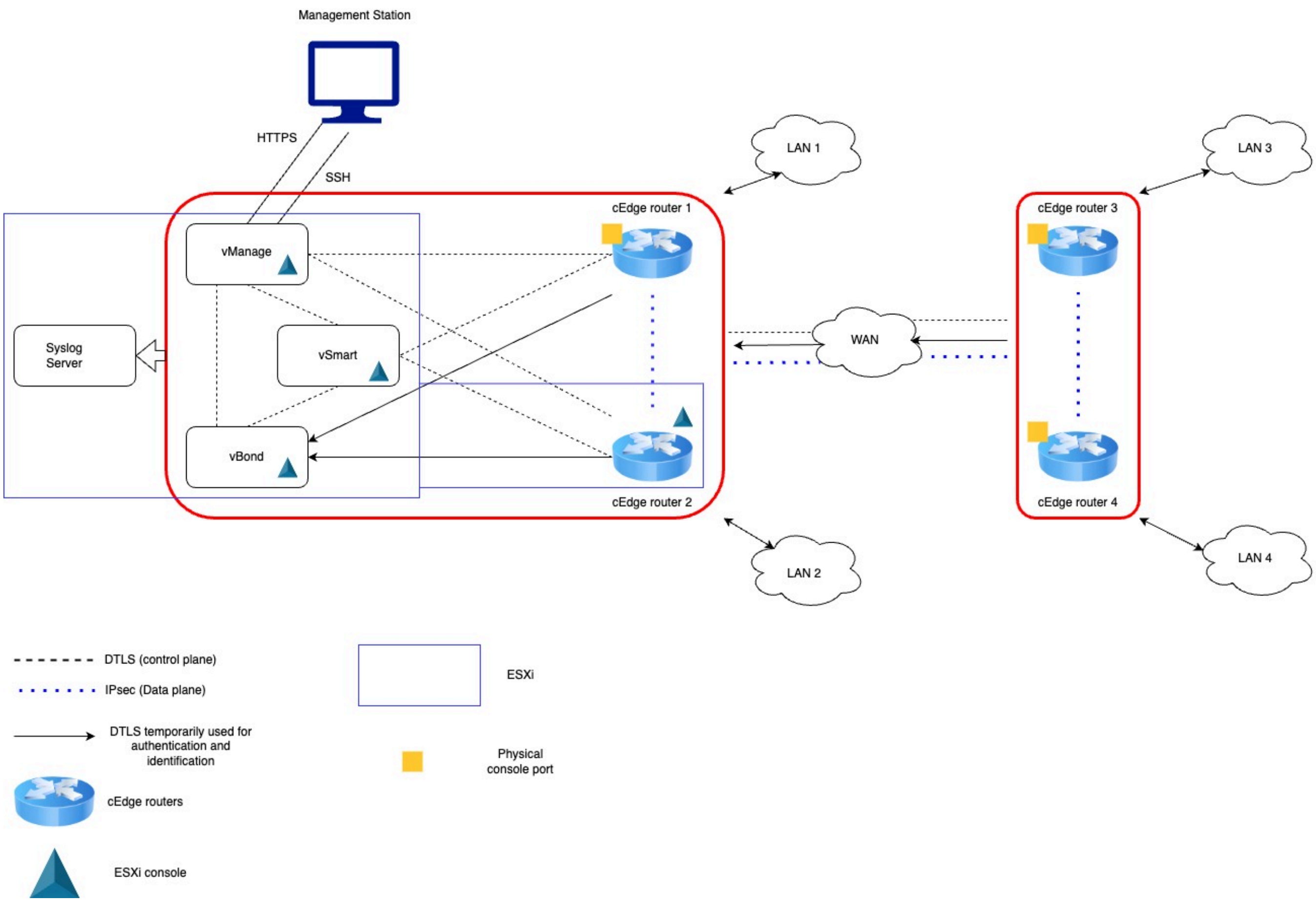
Step 9 The end-user must confirm once the TOE has booted that they are indeed running the evaluated version. The Authorized Administrator may do so following the steps above in 2.5.1 Virtual Controllers (TOE) Software – Pre-Installed.

3 SECURE INSTALLATION AND CONFIGURATION

This section details the installation and configuration for the Virtual System hardware and software (needed for the SD-WAN controller VM's and virtual cEdge router VM's), which are part of the operational environment, as well as installation of the TOE hardware and software components (cEdge routers, SD-WAN controller VM's, and virtual cEdge router VM's).

The following figure provides a visual depiction of a TOE deployment. The TOE boundary is surrounded with a solid red line.

Figure 1. TOE Example Deployment



This section is not a comprehensive configuration guide for the SD-WAN product. The instructions assume the Administrator has a familiarity with the product and highlights configuration steps required for the evaluation of the TOE. Review of the following references by the Authorized Administrator is recommended as they present a high-level overview of the SD-WAN solution, components, components software and hardware compatibilities, capabilities, and pre-requisites:

- **[1] Cisco SD-WAN Design Guide**
- **[2] Cisco Catalyst SD-WAN Getting Started Guide**
- **[3] Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Recommended Computing Resources**

3.1 Physical Installation of VS Hardware (UCS Server)

The following is an overview of a UCS Server install that will be remotely managed. For more details, the Authorized Administrator is referred to instructions in **[4](a)(b)] Cisco UCS C220/C240 M5 Server Installation and Service Guide** chapter **Installing the Server** sections **Preparing for Installation**, **the Server in a Rack**, and **Initial Server Setup**. These references go into greater detail, such as network requirements that must be met before deploying the virtual TOE components.

Step 1 Install the server in a rack.

- Attach the inner rails to the sides of the server.
- Open the front securing plate on both slide-rail assemblies.
- Install the outer slide rails into the rack.
- Insert the server into the slide rails.

Step 2 Attach a power cord to each power supply in your server, and then attach each power cord to a grounded power outlet.

Step 3 Configure the server locally through CIMC.

- Attach a VGA Monitor, USB Keyboard, and either the supported Cisco KVM cable (Cisco PID N20-BKVM); or a USB cable and VGA DB-15 cable.
- Power on and select the CIMC Configuration utility.
- Set the NIC mode to choose which ports to use to access Cisco IMC for server management.
- Choose whether to enable DHCP for dynamic network settings, or to enter static network settings. If selecting "static" supply the address, subnet, and default gateway for the server. Optionally, the administrator may assign a DNS server, hostname, and VLAN.

Step 4 Connect a cable used for management purposes to the LOM port.

Step 5 Connect a cable to be used for VM traffic (SD-WAN) to the desired Cisco Card port.

For this evaluation, the TOE virtual components were deployed on a Cisco UCS C220 M5 server with an Intel processor.

3.2 Software Installation of VS (Hypervisor)

The SD-WAN are installed on VMWare's ESXi. Installing ESXi is beyond the scope of this document. Should an Administrator desire to install, or upgrade to, the approved ESXi version, please reference **[5] VMware ESXi Installation and Setup, VMware ESXi 7.0** as well as the VMWare website ESXi product page:

https://www.vmware.com/products/esxi-and-esx.html

For this evaluation, the TOE VM's were deployed on ESXi 7.0. The Administrator installing and configuring the ESXi host must follow Broadcom's guidance and update the ESXi host to address any vulnerabilities. If Active Directory is used to manage the ESXi users and permissions, the following guidance must be followed:

Secure Default Settings for ESXi Active Directory integration

3.3 Software Installation of TOE (Controller VMs)

Prior to installing VM's it is assumed that the Authorized Administrator has downloaded the correct .OVA files listed is Section 2.5.2 Virtual Controllers (TOE) Software – Download. VM's are deployed via ESXi using the "Deploy a virtual machine from an OVF or OVA file".

Controller VM's should meet the minimum specifications shown below. Increased resources do no impact security operations of the devices but may improve performance of device operation.

Table 10 SD-WAN Controller VM Minimum Specifications

Controller	vCPU	vRAM	vDisk	vNIC
vManage	2 vCPU	32GB	Disk 1: 30GB Disk 2: 100GB	2x 1GB NIC
vSmart	2 vCPU	2GB	Disk 1: 10.5GB (Approx. image size)	2x 1GB NIC
vBond	4 vCPU	4GB	Disk 1: 10.5GB (Approx. image size)	2x 1GB NIC

Additionally, there should be at least two separate virtual networks and switches in ESXi. One for VM management and the other for SD-WAN.

Step 1 From ESXi select "**Create/Register VM**".

Step 2 For vManage, click "**Deploy a virtual machine from an OVF or an OVA file**".

Step 3 Enter a name for your vManage instance and select the downloaded file for vManage.

Step 4 Select the datastore where the VM is going to be stored.

Step 5 Select the VM management network for the VM Network and select "**Thick Provisioning**" for Data Provisioning. Uncheck "**Power on Automatically**".

Step 6 Click "**Finish**" to register the vManage VM.

Step 7 Once VM install is complete, navigate to the **Virtual Machines** and right click the vManage VM and click "**Edit Settings**".

Step 8 Ensure Network Adaptor 1 is configured for the management network.

Step 9 Click "**Add Network Adapter**" and select the defined SD-WAN network for Network Adapter 2.

Step 10 Update Hard Disk 1's size to be 30GB.

Step 11 [vManage Only] Click "**Add Hard Disk**" and select "**New Standard Hard Disk**" add Hard Disk 2 and set size to 100GB, so that vManage has sufficient space to store all controller logs.

Step 12 Click "**Save**".

Step 13 Repeat steps 1 through 12 for vSmart and vBond.

The Authorized Administrator may reference **[6] SD-WAN Controller Setup Guide (On-Prem, Non Cloud-Managed)** for additional details and information.

3.4 Physical Installation of TOE Hardware (Physical cEdge Routers)

The following in instructions are a general overview of the process to install a hardware based cEdge router as it is assumed the Authorized Administrator is familiar with installing network hardware installation. If needed the Authorized Administrator is referred to the following references for additional and/or more detailed information:

- **[8] Cisco ASR 1001-HX Router and Cisco ASR 1002-HX Router Hardware Installation Guide** chapters **Preparing Your Site for Installation** and **Installing the Router**
- **[9] Hardware Installation Guide for Cisco 4000 Series Integrated Services Routers** chapters **Cisco 4000 Series ISRs Preinstallation and Install** and **Connect Cisco 4000 Series ISRs**
- **[10] Hardware Installation Guide for Cisco Catalyst 8300 Series Edge Platforms** chapters **Prepare for Installation** and **Installing and Connect**
- **[11] Cisco Catalyst 8500 Series Edge Platforms Hardware Installation Guide** chapters **Preparing Your Site for Installation** and **Installing the Router**

It is also assumed that the hardware chassis has already been inspected for tampering and or damage.

Step 1 If applicable, install all NIMs before racking and applying power to the device.

Step 2 Attach appropriate rackmount brackets to the device, and then rack the device.

Step 3 Connect the chassis to a reliable earth ground; the ground wire must be installed in accordance with local electrical safety standards.

Step 4 Connect network cables to the desired port(s) t allow for management and SD-WAN traffic.

NOTE: The ISR 4461, ASR 1001HX, and ASR 1002HX routers have dedicated out of band ports for device management purpose. Internally these are designated as interface Gigabit0. The Cat 8300 and 855 models do not have an out of band management interface, so management uses one of the four in band interfaces designated Gigabit 0/0/0 through 0/0/3. VRF's configured on the Cat series routers may be used to limit one interface for only management similar to the dedicated management interface of the ISR and ASR series routers.

Step 5 Connect power cables to the device.

3.5 Software Installation of TOE (Virtual cEdge Routers)

Prior to installing VM's it is assumed that the Authorized Administrator has downloaded the correct .OVA files listed is 2.4.2 C8000V (TOE) Software – Download. VM's are deployed via ESXi using the "Deploy a virtual machine from an OVF or OVA file".

The C8000v cEdge VM's should meet the minimum specifications shown below. Increased resources do no impact security operations of the devices but may improve performance of device operation.

Table 11 C8000v cEdge VM Minimum Specifications

vCPU	vRAM	vDisk	vNIC
4 vCPU	4GB	Disk 1: 8GB	4x 1GB NIC, Type VMXNET 3

Additionally, there should be at least two separate virtual networks and switches in ESXi. One for VM management and the other for SD-WAN.

Step 1 From ESXi select "**Create/Register VM**".

Step 2 For vManage, click "**Deploy a virtual machine from an OVF or an OVA file**".

Step 3 Enter a name for your Cat8000v cEdge router instance and select the downloaded file for the Cat8000v cEdge router.

Step 4 Select the datastore where the VM is going to be stored.

Step 5 Select the VM management network for one of the NIC's and select "**Thick Provisioning**" for Data Provisioning. Uncheck "**Power on Automatically**".

Step 6 Click "**Finish**" to register the vManage VM.

Step 7 Once VM install is complete, navigate to the **Virtual Machines** and right click the vManage VM and click **"Edit Settings**"**.**

Step 8 Set VM CPU count to 4.

Step 9 Add a fourth Network Adaptor. Set it to use the Management switch and port group.

Step 10 Click "**Save**".

The Authorized Administrator may reference **[12] Cisco Catalyst 8000V Edge Software Installation And Configuration Guide**, specifically the chapters **Installation Overview** and **Installing in VMware ESXi Environment** for additional details and information.

3.6 SD-WAN Controller Configurations

This section provides the steps necessary to configure the vManage, vSmart, and vBond controllers. The Authorized Administrator may reference **[6] SD-WAN Controller Setup Guide (On-Prem, Non Cloud-Managed)** for additional details regarding this process.

In addition to the typical network device parameters (IP address, with subnet, default GW, hostname, domain, DNS server, etc.) components in an SD-WAN solution have some additional required configurable parameters. These are listed in the table below.

Table 12 SD-WAN Specific Configuration Parameters

Term	Definition
system-ip	An IP address used internally by the network to identify each device. This is similar to a router ID and is not used for Layer 3 routing.
organization-name	Name of your organization. It must be identical on all the devices in your overlay network, and it must match the name in the certificates for all network devices
sp-organization-name	Name of your service provider. must be identical on all the devices in your overlay network, and it must match the name in the certificates for all network devices
site-id	Numeric identifier of the site in the overlay network. The site ID must be the same for all devices that reside in the same site (i.e., site ID remains the same for vManage, vSmart & vBond).
Vbond (for vManage and vSmart)	IP address of the vBond orchestrator. Must be a public IP address. Example: vbond x.x.x.x
Vbond (for vBond)	Configure this device to act as the vBond orchestrator. Example: vbond x.x.x.x local vbond

NOTE: *Additionally, the controller devices use the parameter VPN. This parameter is not included in the IOS XE available commands, however VRF's are used to achieve the same end.*

For example purposes, throughout this document, the following values will be used.

Table 13. Example SD-WAN Configuration Parameter Values

Parameter	vManage	vBond	vSmart	cEdge Physical	cEdge Virtual
hostname	vManage-1	vBond-1	vSmart-1	ISR4K-1	C8Kv-1
system-ip	10.255.255.10	10.255.255.11	10.255.255.12	10.255.255.13	10.255.255.14
organization-name	"CC CLUS 2023"	"CC CLUS 2023"	"CC CLUS 2023"	"CC CLUS 2023"	"CC CLUS 2023"
site-id	1	1	1	11001	11002
Management Address	172.18.155.5	172.18.155.6	172.18.155.7	172.18.155.8	172.18.155.4
Transport Side Address, Public	10.122.83.211	10.122.83.212	10.122.83.213	10.122.83.214	10.122.83.209
Site Side Address	N/A	N/A	N/A	192.168.10.1	192.168.20.1

In this example, all address belongs to the /24 subnet and the default route for a given subnet id the address who's right most octet is "1". For example, 10.122.83.211 used a default route of 10.122.83.1.

3.6.1 Configure Controller System Information

The steps below are similar for each of the three controllers, except where noted. Table 13. Example SD-WAN Configuration Parameter Values contains the parameter values needed configure each VM (vManage, vSmart, vBond). Start configuration with the vManage device.

Step 1 Power on VM.

Step 2 Lauch the ESXi remote local console.

Step 3 Enter the commands below using the parameters appropriate for the device in question (vManage, vSmart, vBond). Data input for vManage follows:

```
vmanage# config t
Entering configuration mode terminal
vmanage(config)# system
vmanage(config-system)# host-name vManage-1
vManage-1(config-system)# system-ip 10.255.255.10
vManage-1(config-system)# organization-name CC CLUS 2023
vManage-1(config-system)# site-id 1
vManage-1(config-system)# vbond 10.122.83.212
vManage-1(config-system)# commit
Commit complete.
```

NOTE: *When configuring vBond, the "vbond" command will be:*

```
vBond-1(config-system)# vbond 10.122.83.212 local vbond
```

Step 4 Repeat Steps 1 through 3 for the remaining two controllers.

3.6.2 Configure Controller Management VPN

The steps below are similar for each of the three controllers, except where noted. Table 13. Example SD-WAN Configuration Parameter Values contains the parameter values needed configure each VM (vManage, vSmart, vBond). Start configuration with the vManage device.

Step 1 Lauch the ESXi remote local console.

Step 2 Enter the commands below using the parameters appropriate for the device in question (vManage, vSmart, vBond). Data input for vManage follows:

```
vManage-1#
vManage-1# config t
Entering configuration mode terminal
vManage-1(config)# vpn 512
vManage-1(config-vpn-512)# interface eth1
vManage-1(config-interface-eth1)# ip address 172.18.155.5/24
vManage-1(config-interface-eth1)# no shut
vManage-1(config-interface-eth1)# commit
Commit complete.
vManage-1(config-interface-eth1)# exit
vManage-1(config-vpn-512)# ip route 0.0.0.0/0 172.18.155.1
vManage-1(config-vpn-512)# commit
Commit complete.
```

NOTE: *When configuring vBond, configure interface 0 as the management interface using the command: vBond-1(config-vpn-512)#* ***interface eth 0***

Step 3 Repeat Steps 1 through 2 for the remaining two controllers.

3.6.3 Configure Controller Transport VPN

The steps below are similar for each of the three controllers, except where noted. Table 13. Example SD-WAN Configuration Parameter Values contains the parameter values needed configure each VM (vManage, vSmart, vBond). Start configuration with the vManage device.

Step 1 Lauch the ESXi remote local console.

Step 2 Enter the commands below using the parameters appropriate for the device in question (vManage, vSmart, vBond). Data input for vManage follows:

```
vManage-1#
vManage-1# config t
```

```
Entering configuration mode terminal
vManage-1(config)# vpn 0
vManage-1(config-vpn-0)# interface eth0
vManage-1(config-interface-eth0)# ip address 10.122.83.211/24
vManage-1(config-interface-eth0)# no shut
vManage-1(config-interface-eth0)# tunnel-interface
vManage-1(config-tunnel-interface)# allow-service dhcp
vManage-1(config-tunnel-interface)# allow-service dns
vManage-1(config-tunnel-interface)# allow-service icmp
vManage-1(config-tunnel-interface)# allow-service https
vManage-1(config-tunnel-interface)# no allow-service sshd
vManage-1(config-tunnel-interface)# no allow-service netconf
vManage-1(config-tunnel-interface)# no allow-service ntp
vManage-1(config-tunnel-interface)# no allow-service stun
vManage-1(config-tunnel-interface)# commit
Commit complete.
vManage-1(config-tunnel-interface)# exit
vManage-1(config-interface-eth0)# exit
vManage-1(config-vpn-0)# ip route 0.0.0.0/0 10.122.83.1
vManage-1(config-vpn-0)# commit
Commit complete.
```

NOTE: *When configuring vBond, configure interface 0 as the management interface using the command: vBond-1(config-vpn-0)#* ***interface ge0/0***

Step 3 Repeat Steps 1 through 2 for the remaining two controllers.

3.6.4 Configure Controller for Enterprise Certificates

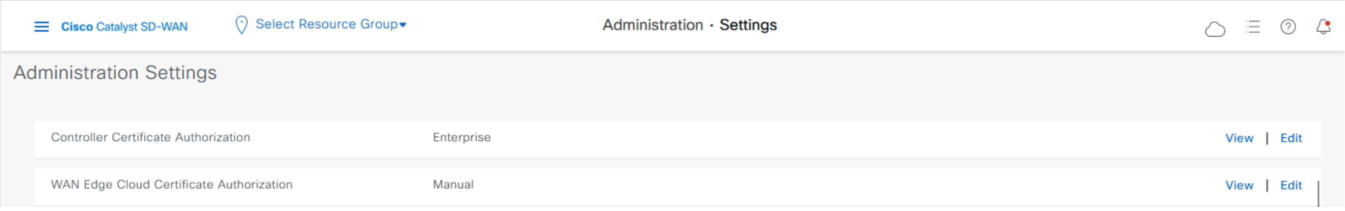
This section provides the steps necessary to configure the vManage, vSmart, and vBond controllers. The Authorized Administrator may reference **[7] Cisco SD-WAN Controller Certificates and Authorized Serial Number File Prescriptive Deployment Guide** for additional details regarding this process.

By default, the solution is configured to use self-signed certificates. The steps below will allow the use of CA signed certificates.

Step 1 Login to the vManage web console, by navigating to "**https://<vManage Public IP Address>:8443**" in a web browser.

Step 2 Using the menu in the upper left and navigate to **Administration** then **Settings**. Scroll down to the settings for **Controller Certificate Authorization** and **WAN Edge Cloud Certificate Authorization**.

Figure 2. Administration Settings

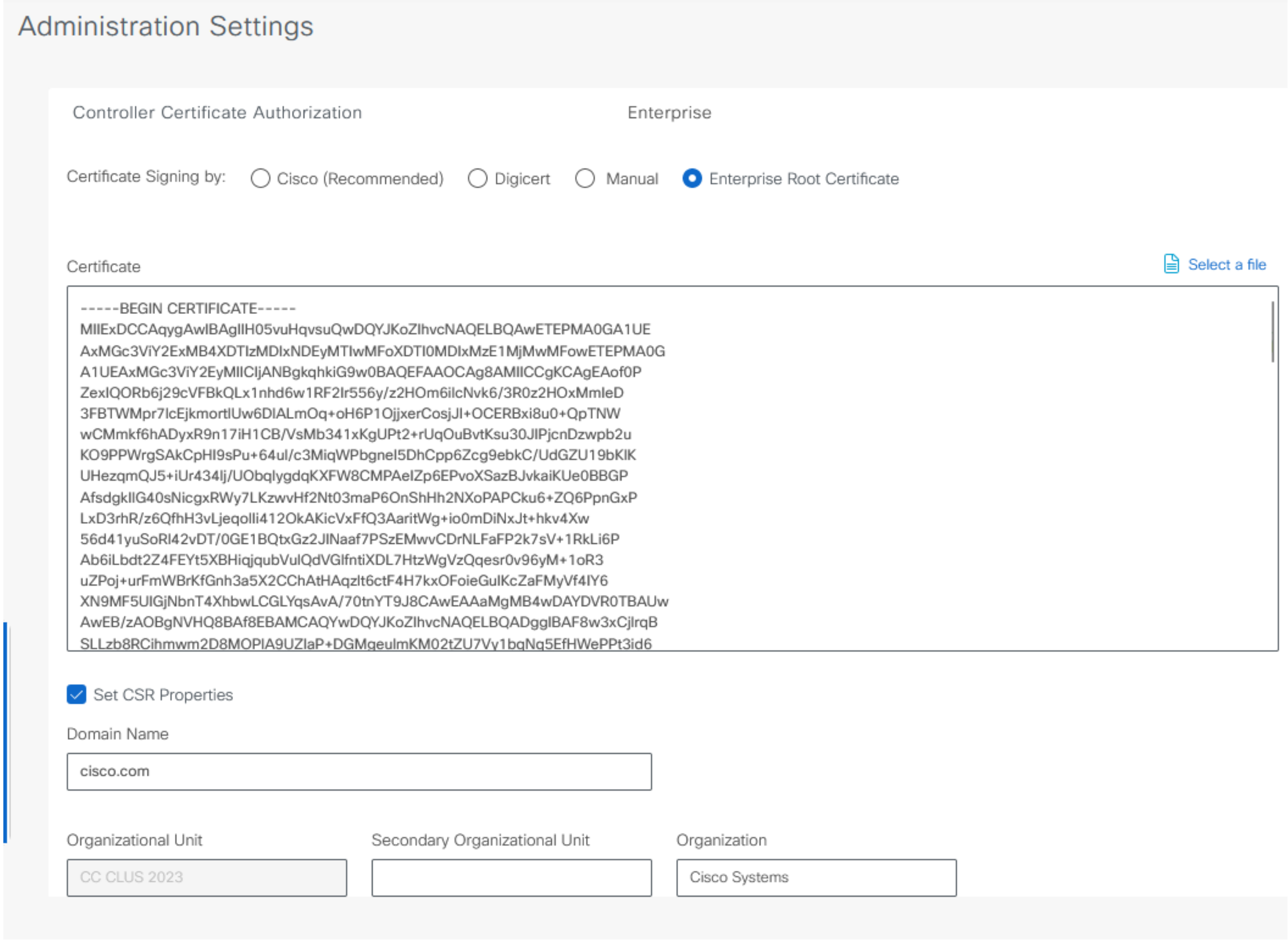


Administration Settings

Controller Certificate Authorization	Enterprise	View | Edit
WAN Edge Cloud Certificate Authorization	Manual	View | Edit

Step 3 Select **Edit** for **Controller Certificate Authorization** and check Enterprise Root Certificate, upload the CA Trust Chain using the Select a file link, check Set CSR Properties, and enter the values to be used when CSR's are generated.

Figure 3. Controller Certificate Authorization Settings



Administration Settings

Controller Certificate Authorization   Enterprise

Certificate Signing by: ○ Cisco (Recommended) ○ Digicert ○ Manual ● Enterprise Root Certificate

Certificate

```
-----BEGIN CERTIFICATE-----
MIIExDCCAqygAwIBAgIIH05vuHqvsuQwDQYJKoZIhvcNAQELBQAwETEPMA0GA1UE
AxMGc3ViY2ExMB4XDTIzMDIxNDEyMTIwMFoXDTI0MDIxMzE1MjMwMFowETEPMA0G
A1UEAxMGc3ViY2EyMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAof0P
ZexIQORb6j29cVFBkQLx1nhd6w1RF2Ir556y/z2HOm6ilcNvk6/3R0z2HOxMmleD
3FBTWMpr7lcEjkmortlUw6DIALmOq+oH6P1OjjxerCosjJI+OCERBxi8u0+QpTNW
wCMmkf6hADyxR9n17iH1CB/VsMb341xKgUPt2+rUqOuBvtKsu30JIPjcnDzwpb2u
KO9PPWrgSAkCpHI9sPu+64ul/c3MiqWPbgnel5DhCpp6Zcg9ebkC/UdGZU19bKlK
UHezqmQJ5+iUr434lj/UObqlygdqKXFW8CMPAeIZp6EPvoXSazBJvkaiKUe0BBGP
AfsdgkIIG40sNicgxRWy7LKzwvHf2Nt03maP6OnShHh2NXoPAPCku6+ZQ6PpnGxP
LxD3rhR/z6QfhH3vLjeqolli412OkAKicVxFfQ3AaritWg+io0mDiNxJt+hkv4Xw
56d41yuSoRl42vDT/0GE1BQtxGz2JINaaf7PSzEMwvCDrNLFaFP2k7sV+1RkLi6P
Ab6iLbdt2Z4FEYt5XBHiqjqubVulQdVGlfntiXDL7HtzWgVzQqesr0v96yM+1oR3
uZPoj+urFmWBrKfGnh3a5X2CChAtHAqzlt6ctF4H7kxOFoieGulKcZaFMyVf4lY6
XN9MF5UIGjNbnT4XhbwLCGLYqsAvA/70tnYT9J8CAwEAAaMgMB4wDAYDVR0TBAUw
AwEB/zAOBgNVHQ8BAf8EBAMCAQYwDQYJKoZIhvcNAQELBQADggIBAF8w3xCjlrqB
SLLzb8RCihmwm2D8MOPlA9UZIaP+DGMgeulmKM02tZU7Vy1bqNq5EfHWePPt3id6
```

☑ Set CSR Properties

Domain Name

cisco.com

Organizational Unit	Secondary Organizational Unit	Organization
CC CLUS 2023		Cisco Systems

When uploading the trust chain, the individual certificates should be boarder by

> "-----BEGIN CERTIFICATE-----" above and
> "-----END CERTIFICATE-----" below.

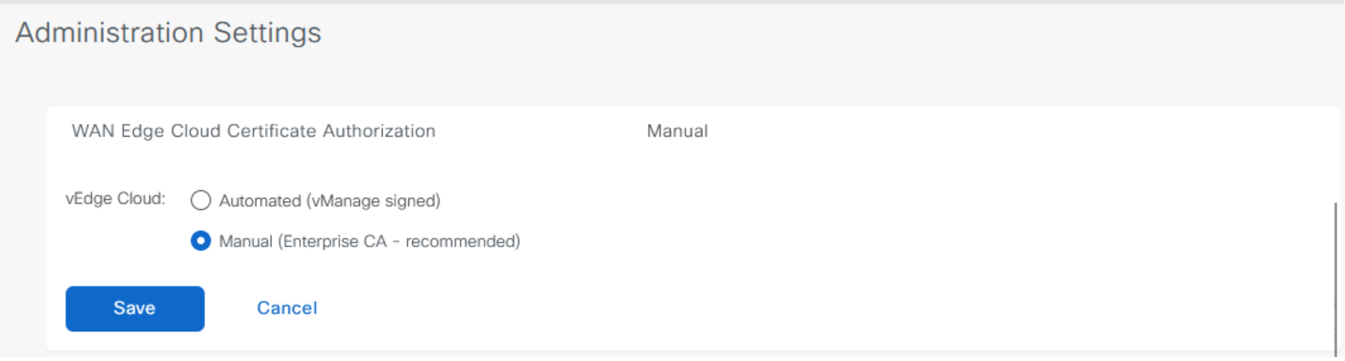
The trust chain should be listed such that the root certificate is at the bottom of the file. Ensure that there are no additional characters between the certificates.

NOTE: When data filling the CSR Properties, Organization Unit field MUST match the device organization name. However, the Organization field may be any value.

Step 4 Select **Import & Save** when done.

Step 5 Select **Edit** for **WAN Edge Cloud Certificate Authorization**, then check **Manual (Enterprise CA – Recommended)**, and select **Save** when done.

Figure 4. WAN Edge Cloud Certificate Authorization Settings



Administration Settings

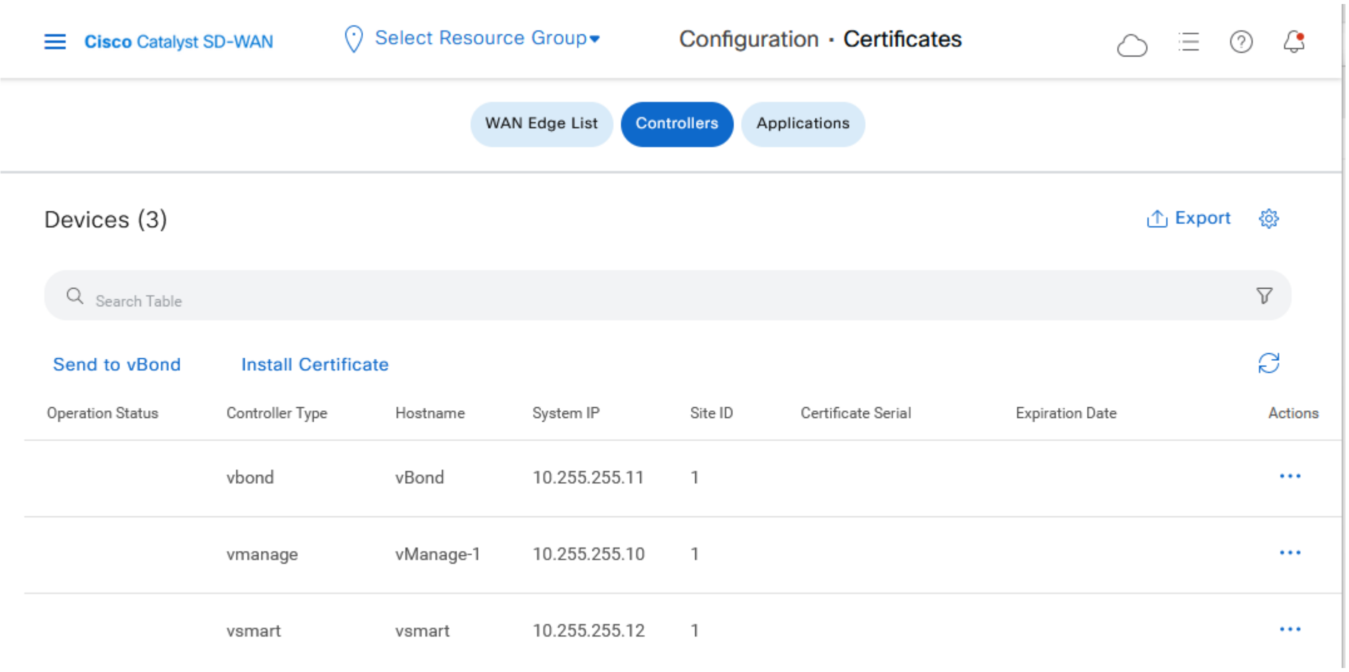
WAN Edge Cloud Certificate Authorization Manual

vEdge Cloud: ○ Automated (vManage signed)

● Manual (Enterprise CA - recommended)

Step 6 Using the menu in the upper left and navigate to **Configuration** then **Certificates** then select **Controllers.**

Figure 5. Controller Certificate Management Page



Operation Status	Controller Type	Hostname	System IP	Site ID	Certificate Serial	Expiration Date	Actions
	vbond	vBond	10.255.255.11	1			···
	vmanage	vManage-1	10.255.255.10	1			···
	vsmart	vsmart	10.255.255.12	1			···

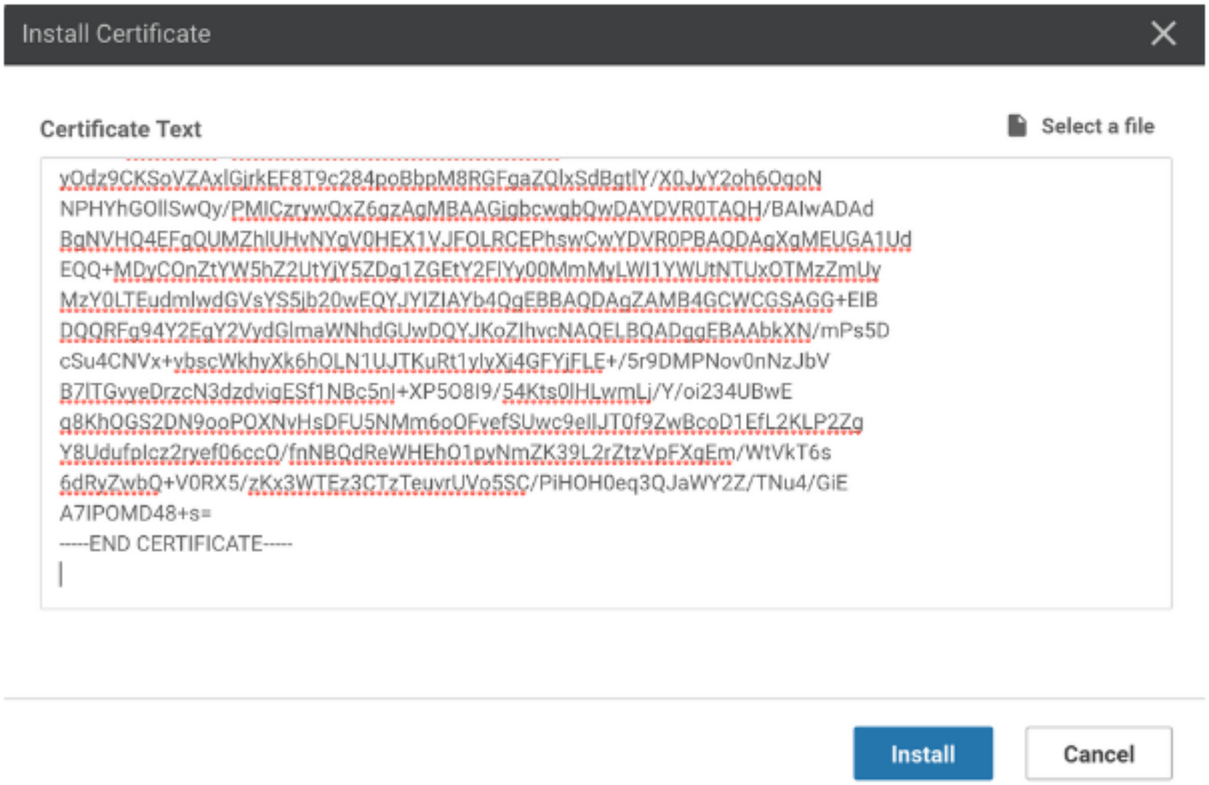
Step 7 On the right side under **Actions**, select the **...** icon, and then select **Generate CSR** for vManage. A pop-up window appears with the certificate signing request. Download or copy the certificate signing request to submit for signing. Repeat this process for vSmart and vBond.

Step 8 Submit the CRS's to the CA to sign the requests.

Step 9 Once signed, return to the vManage and navigate to **Configuration** then **Certificates** then select **Controllers.** This time select the **Install Certificate** link. No specific controller needs to be selected. vManage applies the certificates to the proper controller.

Step 10 From the popup window that appears, use Select a file to navigate to the signed vManage certificate. Once uploaded, click install.

Figure 6. Controller Certificate Install



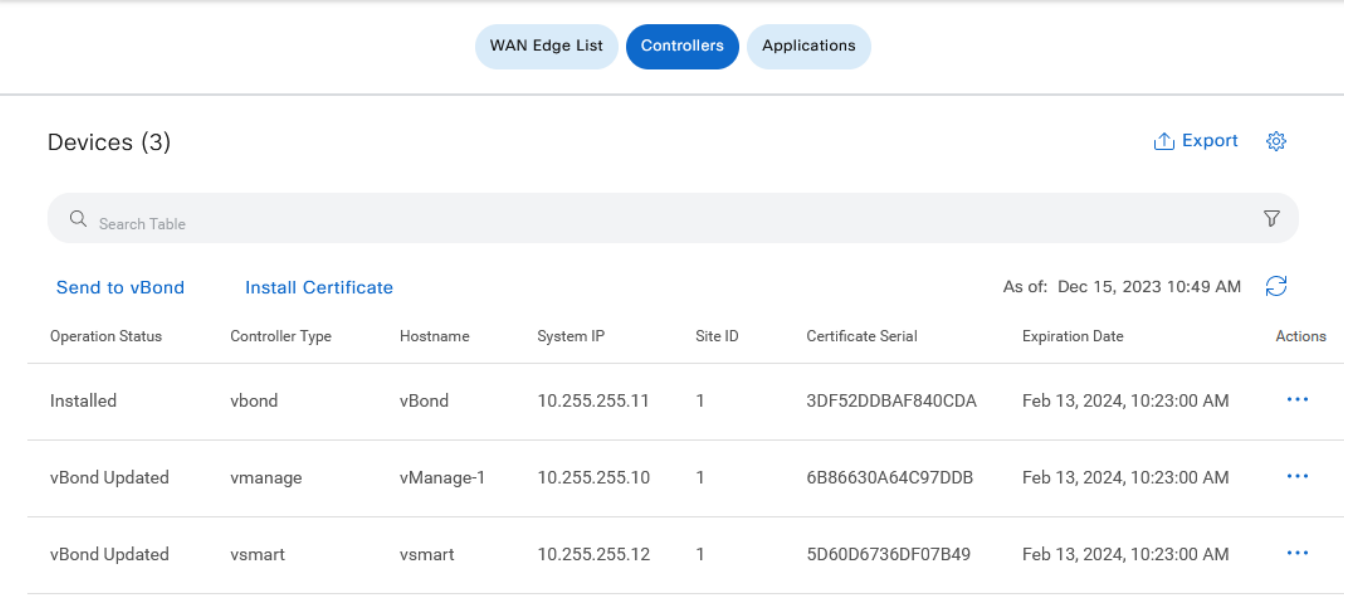
Certificate Text

```
yOdz9CKSoVZAxlGjrkEF8T9c284poBbpM8RGFgaZQlxSdBgtlY/X0JyY2oh6OgoN
NPHYhGOllSwQy/PMICzrywQxZ6gzAgMBAAGjgbcwgbQwDAYDVR0TAQH/BAIwADAd
BgNVHQ4EFgQUMZhlUHvNYgV0HEX1VJFOLRCEPhswCwYDVR0PBAQDAgXgMEUGA1Ud
EQQ+MDyCOnZtYW5hZ2UtYjY5ZDg1ZGEtY2FlYy00MmMyLWI1YWUtNTUxOTMzZmUy
MzY0LTEudmlwdGVsYS5jb20wEQYJYIZIAYb4QgEBBAQDAgZAMB4GCWCGSAGG+EIB
DQQRFg94Y2EgY2VydGlmaWNhdGUwDQYJKoZIhvcNAQELBQADggEBAAbkXN/mPs5D
cSu4CNVx+ybscWkhyXk6hOLN1UJTKuRt1ylyXj4GFYjFLE+/5r9DMPNov0nNzJbV
B7lTGvyeDrzcN3dzdvigESf1NBc5nl+XP5O8I9/54Kts0lHLwmLj/Y/oi234UBwE
q8KhOGS2DN9ooPOXNvHsDFU5NMm6oOFvefSUwc9ellJT0f9ZwBcoD1EfL2KLP2Zg
Y8Udufplcz2ryef06ccO/fnNBQdReWHEhO1pyNmZK39L2rZtzVpFXgEm/WtVkT6s
6dRyZwbQ+V0RX5/zKx3WTEz3CTzTeuvrUVo5SC/PiHOH0eq3QJaWY2Z/TNu4/GiE
A7IPOMD48+s=
-----END CERTIFICATE-----
```

Step 11 Repeat Steps 9 and 10 for vSmart and vBond.

Step 12 Once installed, the certificates should be populated on the Certificate Management page.

Figure 7. Controller Certificates



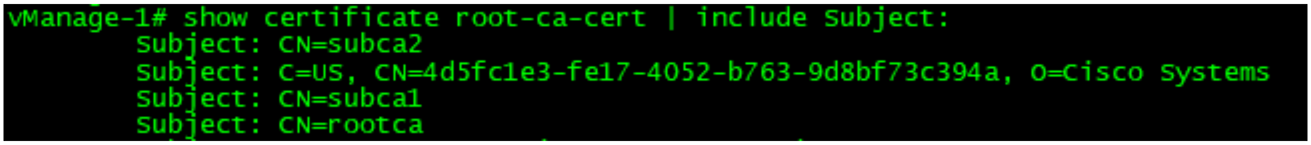
Devices (3)

As of: Dec 15, 2023 10:49 AM

Operation Status	Controller Type	Hostname	System IP	Site ID	Certificate Serial	Expiration Date	Actions
Installed	vbond	vBond	10.255.255.11	1	3DF52DDBAF840CDA	Feb 13, 2024, 10:23:00 AM	···
vBond Updated	vmanage	vManage-1	10.255.255.10	1	6B86630A64C97DDB	Feb 13, 2024, 10:23:00 AM	···
vBond Updated	vsmart	vsmart	10.255.255.12	1	5D60D6736DF07B49	Feb 13, 2024, 10:23:00 AM	···

Step 13 Additionally, verify certificate installation in each controller by entering the cli command **show certificate root-ca-cert | include Subject:** to confirm each device has the signed cert and trust chain.

Figure 8. VManage CLI Cert Verification



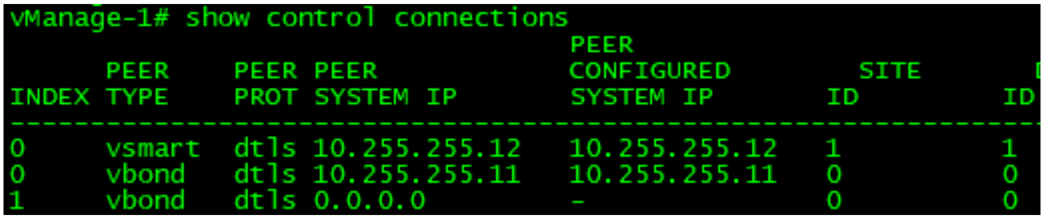
```
vManage-1# show certificate root-ca-cert | include Subject:
        Subject: CN=subca2
        Subject: C=US, CN=4d5fc1e3-fe17-4052-b763-9d8bf73c394a, O=Cisco Systems
        Subject: CN=subca1
        Subject: CN=rootca
```

NOTE: *Some output was removed for brevity.*

3.6.5 Verify Controller Deployment

Using the "**show control connections**" command while an SSH connection to one of the controllers has been established can be useful in troubleshooting connection issues between controllers. The command should return a list of successful connections to the other controllers.

Figure 9. VManage CLI Deployment Verification



```
vManage-1# show control connections
                                   PEER
      PEER     PEER PEER           CONFIGURED        SITE
INDEX TYPE     PROT SYSTEM IP      SYSTEM IP       ID         ID
------------------------------------------------------------------
0     vsmart   dtls 10.255.255.12  10.255.255.12   1          1
0     vbond    dtls 10.255.255.11  10.255.255.11   0          0
1     vbond    dtls 0.0.0.0        -               0          0
```

3.7 cEdge Configurations

The various cEdge routers, physical and virtual, all run IOS XE, so configuration of the devices is similar. The most noticeable difference between the devices is the management port and NIC designations. The ASR and ISR routers have a designated management interface, while the Catalyst switches do not. For this example, ports assignments will be as follows:

Table 14 cEdge Router Port Assignments

	Port Assignment		
Network	ASR 1001HX/1002HX ISR 4461	Catalyst 8300/8500	Catalyst 8000v
Transport Side 10.122.83.0/24	GigabitEthernet0/0/1	GigabitEthernet0/0/1	GigabitEthernet1
Unused	GigabitEthernet0/0/2	GigabitEthernet0/0/2	GigabitEthernet2
LAN Side 192.168.x.0/24	GigabitEthernet0/0/3	GigabitEthernet0/0/3	GigabitEthernet3
Management 172.18.155.0/20	GigabitEthernet0	GigabitEthernet0/0/0	GigabitEthernet4

***NOTE:** For this example, there are only three networks configured. The cEdge routers may be configured with a second transport network, which does not affect the security performance or claims of the TOE.*

Additionally, refer to Table 13. Example SD-WAN Configuration Parameter Values for additional configuration parameters that will also be used in this section.

The instructions that follow in the subsequent sub-section guide the Administrator through the steps necessary to configure the cEdge routers, physical and virtual, to be used with the SD-WAN solution in conjunction with the previously installed controllers. If needed the Authorized Administrator is referred to the following references for additional and/or more detailed information:

- **[2] Cisco Catalyst SD-WAN Getting Started Guide**
- **[7] Cisco SD-WAN Controller Certificates and Authorized Serial Number File Prescriptive Deployment Guide**
- **[8] Cisco ASR 1001-HX Router and Cisco ASR 1002-HX Router Hardware Installation Guide** chapters **Preparing Your Site for Installation** and **Installing the Router**
- **[9] Hardware Installation Guide for Cisco 4000 Series Integrated Services Routers** chapters **Cisco 4000 Series ISRs Preinstallation and Install** and **Connect Cisco 4000 Series ISRs**
- **[10] Hardware Installation Guide for Cisco Catalyst 8300 Series Edge Platforms** chapters **Prepare for Installation and Installing and Connect**
- **[11] Cisco Catalyst 8500 Series Edge Platforms Hardware Installation Guide chapters Preparing Your Site for Installation and Installing the Router**
- **[12] Cisco Catalyst 8000V Edge Software Installation And Configuration Guide**
- **[13] Cisco Catalyst SD-WAN Portal Configuration Guide**

- **[14] Cisco Catalyst SD-WAN Segmentation Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x**
- **[15] Cisco Catalyst SD-WAN Routing Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x**
- **[16] Configure Basic Parameters to Form Control Connections on cEdge**
- **[17] Cisco Catalyst SD-WAN Command Reference**
- **[18] Cisco SDWAN Viptela - Whitelist Serial.Viptela File**

3.7.1 Upload cEdge Serial File to vManage

In order for the WAN Edge devices to come up and be active in the overlay, you must have a valid authorized serial number file uploaded to vManage. This authorized serial number file lists the serial and chassis numbers for all the WAN Edge routers allowed in the network. The vManage sends this file to the controllers, and only devices that match serial numbers on this list will be validated and authenticated successfully by the controllers.

Authorized serial number files for cEdge routers can be downloaded from the Plug and Play (PnP) Connect portal. For access to the portal, as well as the Smart Licensing portal, the Administrator should reach out to their Cisco Account Representative. The steps that follow assume the Administrator already has an account and access to the portal.

The Administrator is referred to **[7] Cisco SD-WAN Controller Certificates and Authorized Serial Number File Prescriptive Deployment Guide** section **Process 2: Deploying the Signed WAN Edge Authorized Serial Number List** and **[18] Cisco SDWAN Viptela - Whitelist Serial.Viptela File** for additional information.

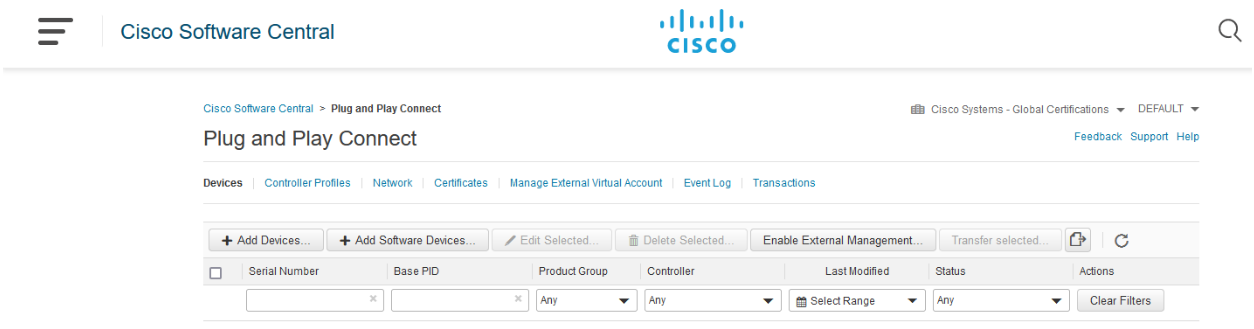
Step 1 Navigate to Cisco Software Central via the link:

https://software.cisco.com/#

And then scroll down to the **Smart Licensing** section and look for **Network Plug and Play**.

Step 2 Under Network Plug and **Play select Manage Devices** to access **Plug and Play Connect**.

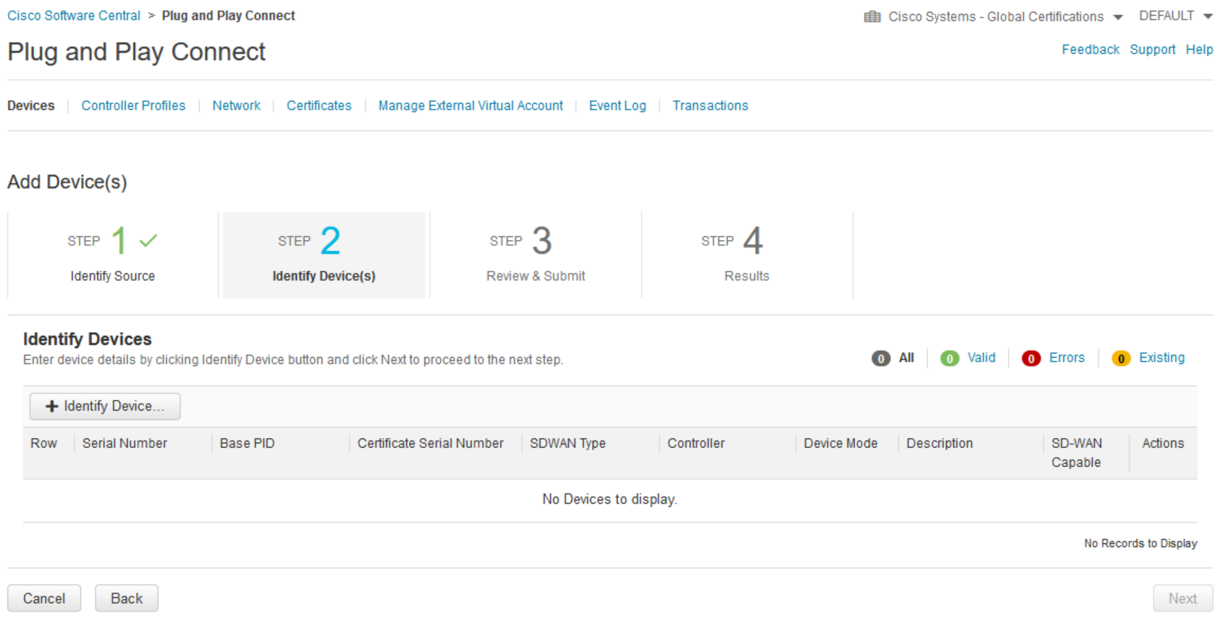
Figure 10. Plug and Play (PnP) Connect Web Page



Step 3 If devices are already loaded, proceed to Step x. Otherwise, to add a physical device select **+ Add Device**. There is an option to “**Import using a CSV file**” or “**Enter Device info manually**”. In this example check “**Enter Device info manually**” and then select Next.

Step 4 One the next screen select the **+ Identify Device** tab.

Figure 11. Plug and Play (PnP) Identify Device


Cisco Software Central > Plug and Play Connect
Cisco Systems - Global Certifications
DEFAULT
Plug and Play Connect
Feedback Support Help
Devices | Controller Profiles | Network | Certificates | Manage External Virtual Account | Event Log | Transactions
Add Device(s)
STEP 1 ✓ Identify Source
STEP 2 Identify Device(s)
STEP 3 Review & Submit
STEP 4 Results
Identify Devices
Enter device details by clicking Identify Device button and click Next to proceed to the next step.
0 All | 0 Valid | 0 Errors | 0 Existing
+ Identify Device...
Cancel
Back
Next

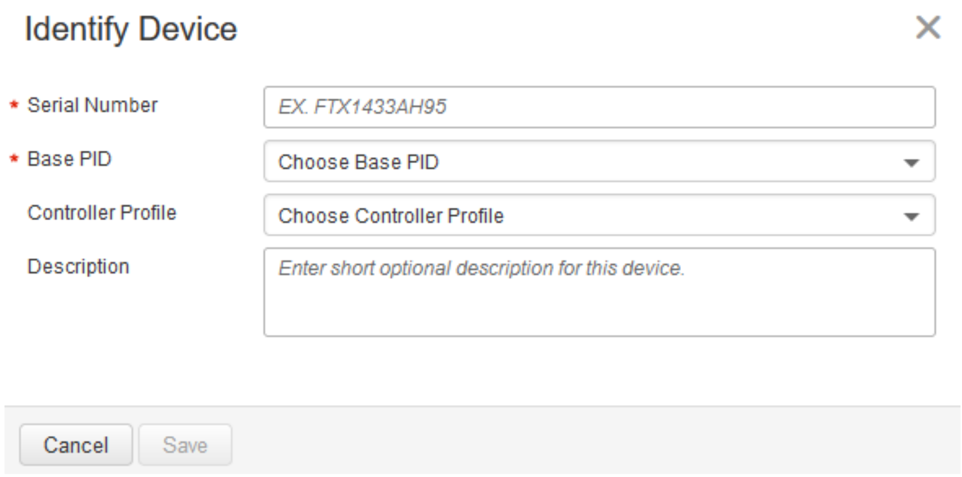
Row	Serial Number	Base PID	Certificate Serial Number	SDWAN Type	Controller	Device Mode	Description	SD-WAN Capable	Actions

No Devices to display.

No Records to Display

Step 5 One the window that pops up, provide the serial number and PID (Product ID) of the device. These can be found on the devices physical chassis or while consoled in using the **show license udi** command from CLI.

Figure 12. Plug and Play (PnP) Enter Device Details

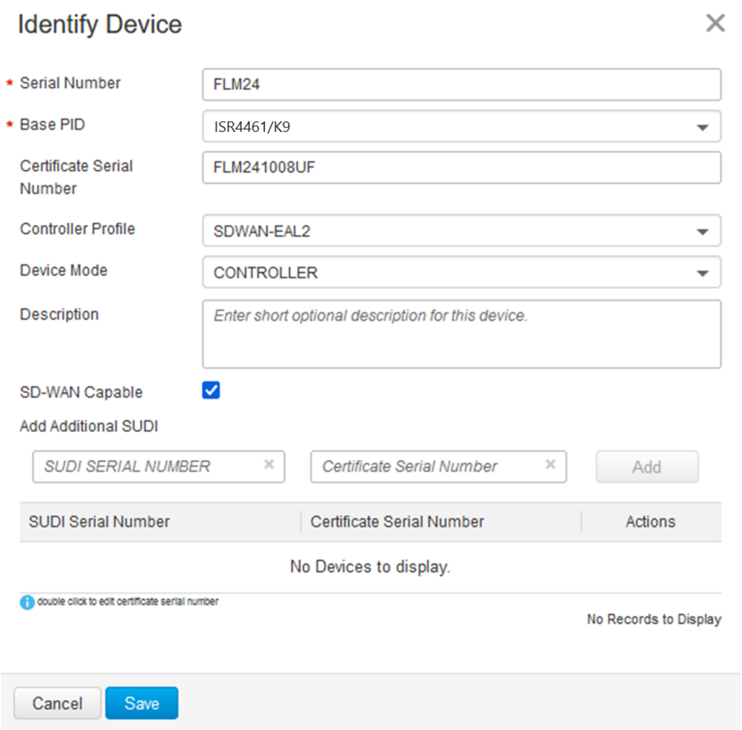


* Serial Number	EX. FTX1433AH95
* Base PID	Choose Base PID
Controller Profile	Choose Controller Profile
Description	Enter short optional description for this device.

Once a valid Serial Number and PID are entered, additional dropdowns appear. Enter the devices **Certificate Serial Number**. The **Controller Profile** dropdown will contain valid controllers for the account. At that point select the correct controller, set **Device Mode** to **Controller**, and check **SD-WAN Capable**, and then select **Save** then **Next**.

NOTE: *The devices serial certificate serial number can be found using the command "**show crypto pki certificates**" from the devices command line interface (CLI). The certificate in question is the one whose issuer is listed as "cn=ACT2 SUDI CA".*

Figure 13. Plug and Play (PnP) Device Details Data Filled



Identify Device

* Serial Number: FLM24

* Base PID: ISR4461/K9

Certificate Serial Number: FLM241008UF

Controller Profile: SDWAN-EAL2

Device Mode: CONTROLLER

Description: Enter short optional description for this device.

SD-WAN Capable ☑

Add Additional SUDI

SUDI Serial Number	Certificate Serial Number	Actions
No Devices to display.		

double click to edit certificate serial number

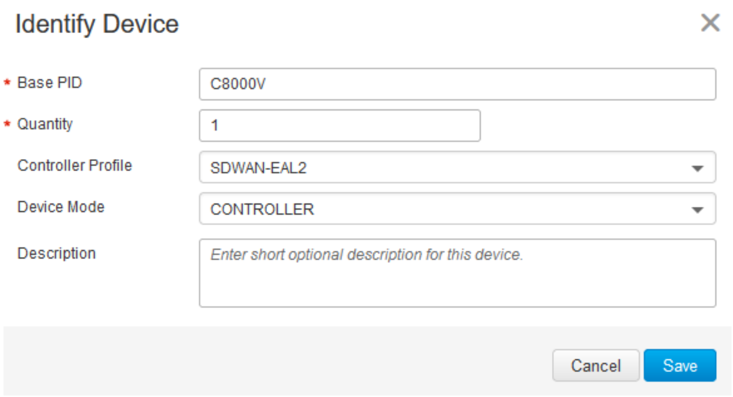
No Records to Display

Step 6 The device will now appear in the Review & Submit. Click **Submit** and then **Done**, and the device will be added.

Step 7 If the device to add is a Cat8000V virtual cEdge device, then from the Plug and Play Connect **Devices** tab select **+ Add Software Devices** then on the subsequent page click **+ Add Software Devices** again.

Step 8 The **show license udi** command also works on virtual routers. Data fill the **Identity Device** popup window and then select **Save** and then **Next**.

Figure 14. Plug and Play (PnP) Software Device Details Data Filled



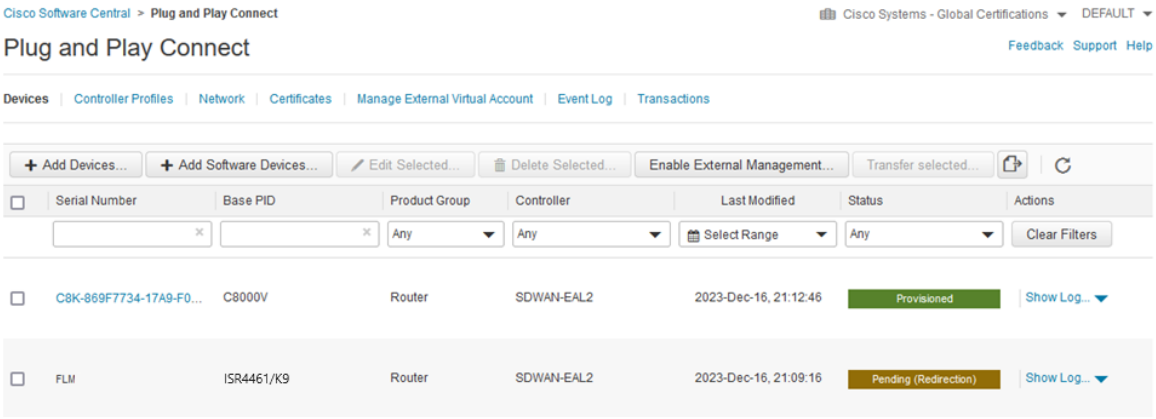
Identify Device

* Base PID	C8000V
* Quantity	1
Controller Profile	SDWAN-EAL2
Device Mode	CONTROLLER
Description	Enter short optional description for this device.

Step 9 The device will now appear in the Review & Submit. Click **Submit** and then **Done**, and the device will be added.

Step 10 The added devices will be listed in the summary page.

Figure 15. Plug and Play (PnP) with Added Devices



Cisco Software Central > Plug and Play Connect

Plug and Play Connect

Cisco Systems - Global Certifications DEFAULT

☐	Serial Number	Base PID	Product Group	Controller	Last Modified	Status	Actions
☐	C8K-869F7734-17A9-F0...	C8000V	Router	SDWAN-EAL2	2023-Dec-16, 21:12:46	Provisioned	Show Log...
☐	FLM	ISR4461/K9	Router	SDWAN-EAL2	2023-Dec-16, 21:09:16	Pending (Redirection)	Show Log...

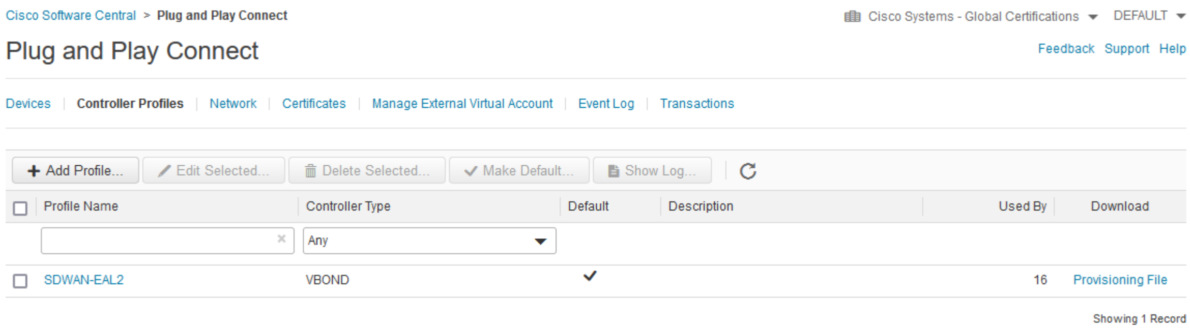
Feedback Support Help
Devices | Controller Profiles | Network | Certificates | Manage External Virtual Account | Event Log | Transactions
+ Add Devices...
+ Add Software Devices...
Edit Selected...
Delete Selected...
Enable External Management...
Transfer selected...
Any
Select Range
Clear Filters

Once added select the **Controller Profiles** tab.

NOTE: *Unique software stings are generated for the software devices in lieu of an actual serial number.*

Step 11 From the **Controller Profiles** tab, locate the intended controller and select the **Provisioning file** link associated with that controller.

Figure 16. Plug and Play (PnP) with Added Devices


Cisco Software Central > Plug and Play Connect
Cisco Systems - Global Certifications
DEFAULT
Plug and Play Connect
Feedback Support Help
Devices | Controller Profiles | Network | Certificates | Manage External Virtual Account | Event Log | Transactions
+ Add Profile...
Edit Selected...
Delete Selected...
Make Default...
Show Log...

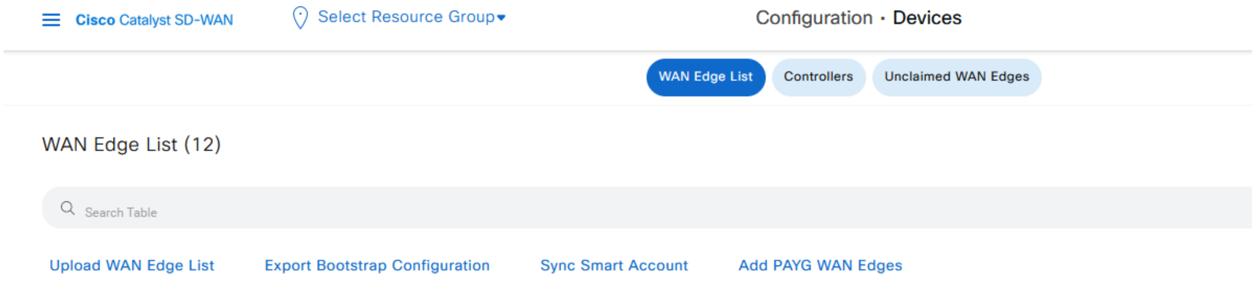
□	Profile Name	Controller Type	Default	Description	Used By	Download
		Any				
□	SDWAN-EAL2	VBOND	✓		16	Provisioning File

Showing 1 Record

Step 12 On the popup that appears, set the **Controller Versions** drop down to **18.3 and newer** and click download. This will download a file named **serialFile.viptela**.

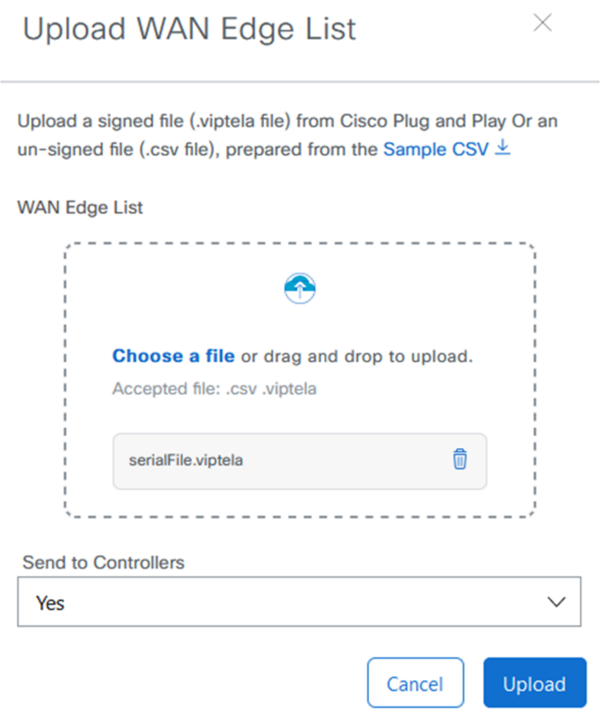
Step 13 Login into the vManage GUI and navigate to **Configuration** then **Device** then **WAN Edge List**. From here select the **Upload WAN Edge List** link.

Figure 17. vManage WAN Edge List



Step 14 In the popup window that appear, select the **serialFile.viptela** file, select **Yes** for **Send to Controller**, and the click **Upload**.

Figure 18. vManage Serial Number File Upload



Upload WAN Edge List

Upload a signed file (.viptela file) from Cisco Plug and Play Or an un-signed file (.csv file), prepared from the Sample CSV

WAN Edge List

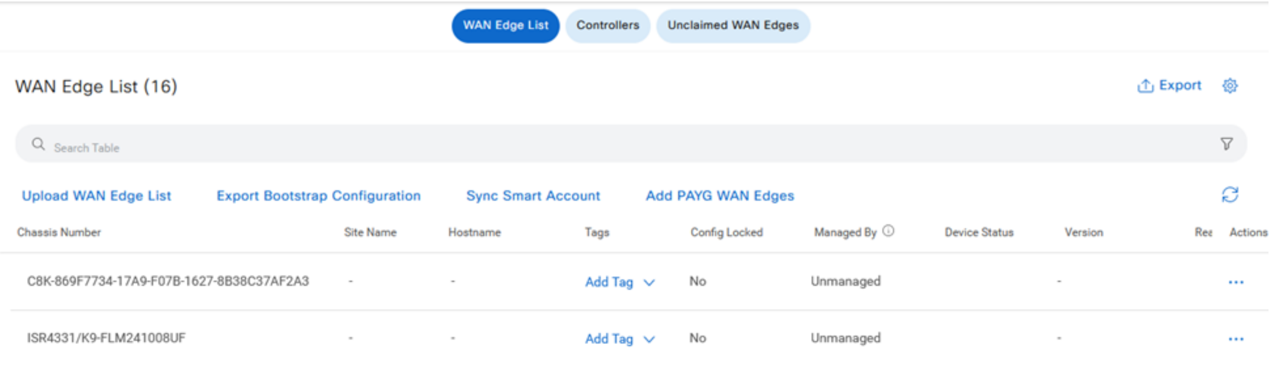
Choose a file or drag and drop to upload.
Accepted file: .csv .viptela

serialFile.viptela

Send to Controllers: Yes

Step 15 The controllers will be displayed showing status of deployment. Once done, status will be success. At this point navigate back to the WAN Edge List to confirm the devices have been added.

Figure 19. vManage Device Serial Number Addition Verification



WAN Edge List (16)

Chassis Number	Site Name	Hostname	Tags	Config Locked	Managed By	Device Status	Version	Rea	Actions
C8K-869F7734-17A9-F07B-1627-8B38C37AF2A3	-	-	Add Tag	No	Unmanaged		-		...
ISR4331/K9-FLM241008UF	-	-	Add Tag	No	Unmanaged		-		...

3.7.2 Verify/Configure Controller Mode

Logging in via local console (or ESXi remote local console) issue the "**show platform software device-mode**" command and verify the **routers mode of operation. The two expected values are:**

Router operating mode: Autonomous or
Router operating mode: Controller-Managed

These lines are near the end of the "**show platform software device-mode**" output. If the output indicates **"Router operating mode: Controller-Managed"** proceed to the next section, otherwise the router mode of operation needs to be changed.

```
C8Kv-1#controller-mode enable
Enabling controller mode will erase the nvram filesystem, remove all configuration files, and reload the box!
Ensure the BOOT variable points to a valid image
Continue? [confirm]
```

As indicated by the warning, this action will reload the router and erase existing configurations. To confirm and continue press the enter key. Once rebooted, confirm cEdge router in in Controller-Managed mode and continue with configuring the router.

3.7.3 Configuration Basics

The configuration below will set the hostname, create a username and password, set the enable password, and allow SSH for remote administration.

```
router# config-t
router(config)# hostname C8Kv-1
router(config)#
router(config)# username admin privilege 15 secret <password>
router(config)#
router(config)# enable secret <password>
router(config)#
router(config)# line vty 0 4
router(config-line)# transport input ssh
router(config-line)#
router(config-line)# commit
Commit complete.
C8Kv-1(config-line)#
```

The username command is creating a administration account with full privileges (privilege class 15). The configured password will be an encrypted string when looking at the running configuration output. Setting an enable command ensures that if an admin with a privilege class less than 15 is created, they cannot enter the privilege (enable) mode. Together these two settings can be used to set appropriate levels of access for multiple administrators with different roles/responsibilities and prevent unintended privilege escalation through use of the **enable** command.

The command **transport input ssh** limits remote access to only the SSH protocol for access to command line functions.

NOTE: *When setting the administrative user's password, the password should conform to the standard adapted by the organization.*

3.7.4 Configure cEdge Management Interface

The configuration below will configure the management interface for a Cat8000v cEdge router.

```
C8Kv-1# config-transaction
C8Kv-1(config)#
C8Kv-1(config)# hostname C8Kv-1
C8Kv-1(config)#
C8Kv-1(config)# vrf definition Mgmt-intf
C8Kv-1(config-vrf)# description Mgmt-intf VPN
C8Kv-1(config-vrf)# rd 1:512
C8Kv-1(config-vrf)# address-family ipv4
C8Kv-1(config-ipv4)# route-target export 1:512
C8Kv-1(config-ipv4)# route-target import 1:512
C8Kv-1(config-ipv4)# exit-address-family
C8Kv-1(config-vrf)#
C8Kv-1(config-vrf)# interface GigabitEthernet4
C8Kv-1(config-if)# description Mgmt-intf
C8Kv-1(config-if)# vrf forwarding Mgmt-intf
C8Kv-1(config-if)# ip address 172.18.155.4 255.255.255.0
C8Kv-1(config-if)# negotiation auto
C8Kv-1(config-if)# no shutdown
C8Kv-1(config-if)#
C8Kv-1(config-if)# ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 172.18.155.1
C8Kv-1(config)#
C8Kv-1(config)# sdwan
C8Kv-1(config-sdwan)# system
C8Kv-1(config-system)# no track-default-gateway
C8Kv-1(config-system)# commit
Commit complete.
```

After the hostname, the next few line define VRF Mgmt-intf which will be used for separation of management from data traffic (512 corresponds to the VPN the controller associates with management), interface GigabitEthernet4 is selected as the management interface assigned to VRF Mgmt-intf and given an IP address, and finally VRF Mgmt-intf is given a default route.

If this was a Cat 8300 or 8500 cEdge router, the difference would be the assignment of management functionality to **interface GigabitEthernet0/0/0** versus **interface GigabitEthernet4**.

If this was an ASR or ISR, there are some additional differences as these routes already have a defined VRF called “Mgmt-intf”, but still needs to be associated with VPN 512. Additionally, the assignment of management functionality to **interface GigabitEthernet0** versus **interface GigabitEthernet4**. In that case the configuration would be performed as follows:

```
ASR# config-transaction
ASR(config)#
ASR(config)# hostname ASR
ASR(config)#
ASR(config)# vrf definition Mgmt-intf
ASR(config-vrf)# description Mgmt-intf VPN
ASR(config-vrf)# rd 1:512
ASR(config-vrf)# address-family ipv4
ASR(config-ipv4)# route-target export 1:512
ASR(config-ipv4)# route-target import 1:512
ASR(config-ipv4)# exit-address-family
ASR(config-vrf)#
ASR(config-vrf)# interface GigabitEthernet0
ASR(config-if)# description Mgmt-intf
ASR(config-if)# vrf forwarding Mgmt-intf
ASR(config-if)# ip address 172.18.155.4 255.255.255.0
ASR(config-if)# negotiation auto
ASR(config-if)# no shutdown
ASR(config-if)#
ASR(config-if)# ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 172.18.155.1
ASR(config)#
ASR(config)# sdwan
ASR(config-sdwan)# system
ASR(config-system)# no track-default-gateway
ASR(config-system)# commit
Commit complete.
```

3.7.5 Configure cEdge Transport Interface

Configuring the transport interface requires tasks be performed in a particular order to ensure proper deployment as there will be tunnels associated with this traffic.

```
C8Kv-1(config)# interface GigabitEthernet1
C8Kv-1(config-if)# ip address 10.122.83.209 255.255.255.0
C8Kv-1(config-if)# negotiation auto
C8Kv-1(config-if)# no shutdown
C8Kv-1(config-if)#
C8Kv-1(config-if)# ip route 0.0.0.0 0.0.0.0 10.122.83.1
C8Kv-1(config)#
C8Kv-1(config)# commit
Commit complete.
```

The above configuration statements turn up interface GigabitEthernet1, assign an IP route, and provide a default route. There is no VRF associated as this interface uses the global routing table which also corresponds to VPN 0 in the controller configurations.

The interface must be configured, and the configuration committed before configuring the tunnel or SD-WAN parameters.

```
C8Kv-1(config)# interface Tunnel1
C8Kv-1(config-if)# no shutdown
C8Kv-1(config-if)# ip unnumbered GigabitEthernet1
C8Kv-1(config-if)# tunnel source GigabitEthernet1
C8Kv-1(config-if)# tunnel mode sdwan
C8Kv-1(config-if)# exit
C8Kv-1(config)#
C8Kv-1(config)# sdwan
C8Kv-1(config-sdwan)# interface GigabitEthernet1
C8Kv-1(config-interface-GigabitEthernet1)# tunnel-interface
C8Kv-1(config-tunnel-interface)# encapsulation ipsec
C8Kv-1(config-tunnel-interface)# color public-internet
C8Kv-1(config-tunnel-interface)# allow-service all
C8Kv-1(config-tunnel-interface)#
C8Kv-1(config-tunnel-interface)# commit
Commit complete.
```

Once configured, interface GigabitEthernet1 is associated with Tunnel1 and traffic source from the interface uses the tunnel. Additionally from an SD-WAN perspective, traffic using this tunnel will be encrypted via IPsec and will be assigned a "color" to be used by the controllers to route between other cEdge devices.

If this was a physical cEdge router, the difference would be the assignment of **interface GigabitEthernet0/0/1**.

NOTE*: Some routers may only have 10 GB face interfaces, in which case the command would reflect this, for example* ***interface TenGigabitEthernet0/0/1****.*

3.7.6 Configure cEdge LAN Side Interface

The purpose of SD-WAN is to create a software defined wide are network that allows transport between the various site side interfaces. The following example configures a site side interface for a location which also allows OSPF to be used between the various sites to learn routing for the site side, however all transport will use the tunnel created on the transport interface. The example configuration is as follows:

```
Cat8Kv-Site2# config-t
C8Kv-1(config)# vrf definition 2
C8Kv-1(config-vrf)# description Service-Side-VPN
C8Kv-1(config-vrf)# rd 1:2
C8Kv-1(config-vrf)# address-family ipv4
C8Kv-1ASR(config-ipv4)# route-target export 1:2
C8Kv-1ASR(config-ipv4)# route-target import 1:2
C8Kv-1ASR(config-ipv4)# exit-address-family
C8Kv-1(config-vrf)#
C8Kv-1(config-vrf)# interface GigabitEthernet3
C8Kv-1(config-if)# description LAN
```

```
C8Kv-1(config-if)# vrf forwarding 2
C8Kv-1(config-if)# ip address 192.168.20.1 255.255.255.0
C8Kv-1(config-if)# ip ospf 2 area 0
C8Kv-1(config-if)# negotiation auto
C8Kv-1(config-if)# no mop enabled
C8Kv-1(config-if)# no mop sysid
C8Kv-1(config-if)#
C8Kv-1(config-if)# router ospf 2 vrf 2
C8Kv-1(config-router)# commit
Commit complete.
```

Firstly FRF 2 is defined for site side us and is assigned to interface GigabitEthernet3. OSPF is enabled with an id of “2” and area 0 is assigned to interface GigabitEthernet3. Finally, OSPF is associated with VRF2.

If this was a physical cEdge router, the difference would be the assignment of configuration and assignment of **interface GigabitEthernet0/0/3**.

NOTE*: Some routers may only have 10 GB face interfaces, in which case the command would reflect this, for example* ***interface TenGigabitEthernet0/0/3****. Ten gigabit interfaces do not support the mop commands, so this capability is essentially disabled already. As a result, the* ***no mop enabled*** *and no* ***mop sysid*** *commands are not applicable to the TenGigabiteEthernet interfaces.*

For more information regarding site side routing, the Administrator is referred to **[14] Cisco Catalyst SD-WAN Segmentation Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x** and **[15] Cisco Catalyst SD-WAN Routing Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x** chapter **Unicast Overlay Routing**.

3.7.7 Configure cEdge System Settings

In order to join the SD-WAN fabric, the cEdge needs basic overlay information under system so that it can start the authentication with vBond.

```
Cat8Kv-Site1# config-t
Cat8Kv-Site1(config)# sdwan
Cat8Kv-Site1(config-sdwan)# system
Cat8Kv-Site1(config-system)# system-ip 10.255.255.15
Cat8Kv-Site1(config-system)# site-id 11002
Cat8Kv-Site1(config-system)# organization-name "CC CLUS 2023"
Cat8Kv-Site1(config-system)# vbond 10.122.83.212 port 12346
Cat8Kv-Site1(config-system)# commit
```

Once the system configuration is committed, all that is needed for the cEdge device to build control connections to vManage and vSmart is to install the trust chain in the cEdge device..

3.7.8 Install Trusted CA Certificate Chain

To allow the communications needed for the cEdge device to sync with the vManage, the cEdge device need to have the Enterprise Trust Chain used in the vManage installed on the cEdge device as well.

Step 1 The trust chain used in 3.6.4 Configure Controller for Enterprise Certificates will also be used here. If The trust chain is not available, the Administrator may retrieve the installed trust chain by following 3.6.4 Configure Controller for Enterprise Certificates steps 1 through 3, but rather than copying the trust chain into vManage, the Administrator will copy what is already in vManage into a file.

NOTE: The file can be created with a text editor, but the file should be saved with the name "root.pem".

NOTE: For a trust chain, the individual certificates should be boarder by

```
“-----BEGIN CERTIFICATE-----" above and
“-----END CERTIFICATE-----" below.
```

The trust chain should be listed such that the root certificate is at the bottom of the file. Ensure that there are no additional characters between the certificates.

Step 2 The file then needs to be copied to the bootflash of the cEdge device. For a hardware device this can be done using the USB port on the device, but for a virtual cEdge, a network protocol such as TFTP, FTP, SFTP, or SCP is needed. As an example, the TFTP commands are as follows:

```
Cat8Kv-Site1#copy tftp://[TFTP Server IP]/root.pem bootflash:
Destination filename [root.pem]?
Accessing tftp://[ TFTP Server IP]//root.pem...
Loading root.pem from [TFTP Server IP] (via GigabitEthernet4): !
[OK - 5188 bytes]

5188 bytes copied in 0.126 secs (41175 bytes/sec)
Cat8Kv-Site1#
```

***Note:** For more information regarding the use of the **copy** command, the Administrator is referred to **[21] Using Cisco IOS Software Command Reference – Copy**.*

Step 3 Once the file is copied to bootflash, it can be added as the trust chain using the **request platform software sdwan root-cert-chain install bootflash:root.pem** command.

```
Cat8Kv-Site1#request platform software sdwan root-cert-chain install bootflash:root.pem
Uploading root-ca-cert-chain via VPN 0
Copying ... /bootflash/root.pem via VPN 0
Updating the root certificate chain..
Successfully installed the root certificate chain
Cat8Kv-Site1#
```

Step 4 Once the trust chain is updated, the Administrator using the **show sdwan cert root-ca-cert** command.

```
Cat8Kv-Site1#show sdwan cert root-ca-cert
Certificate:
   Data:
      [Certificate Data Omitted]
Cat8Kv-Site1#
```

3.7.9 Virtual cEdge Router Activation

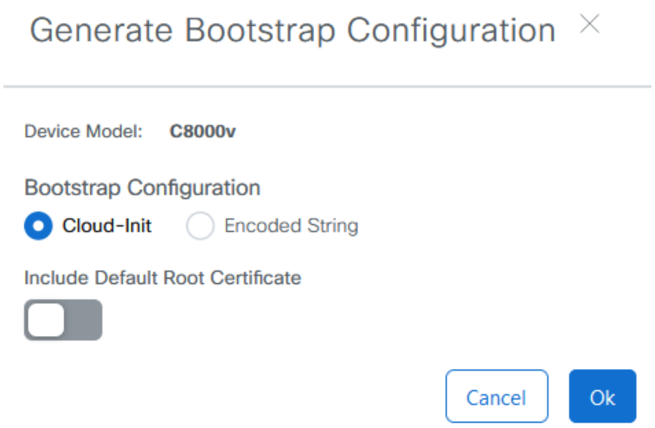
cEdge virtual routers require an extra step to associate a chassis and a token since they are not real hardware and the Universal Unique Device Identifier (UUDI) is virtual.

Step 1 Login into the vManage GUI and navigate to **Configuration** then **Device** then **WAN Edge List**. Find an available virtual router Chassis ID to deploy. In this example the ID associated with C8000V added in Section 3.7.1 Upload cEdge Serial File to vManage will be used: **C8K-869F7734-17A9-F07B-1627-8B38C37AF2A3**.

Step 2 From the far-right column, **Actions**, click the **...** icon, and then select **Generate Bootstrap Configuration**.

Step 3 From the window that pops up click **OK**. Additionally, **Include Default Root** Certificate may be disable by moving the slider to the left.

Figure 20. vManage Virtual cEdge Bootstrap Request



Generate Bootstrap Configuration

Device Model: C8000v

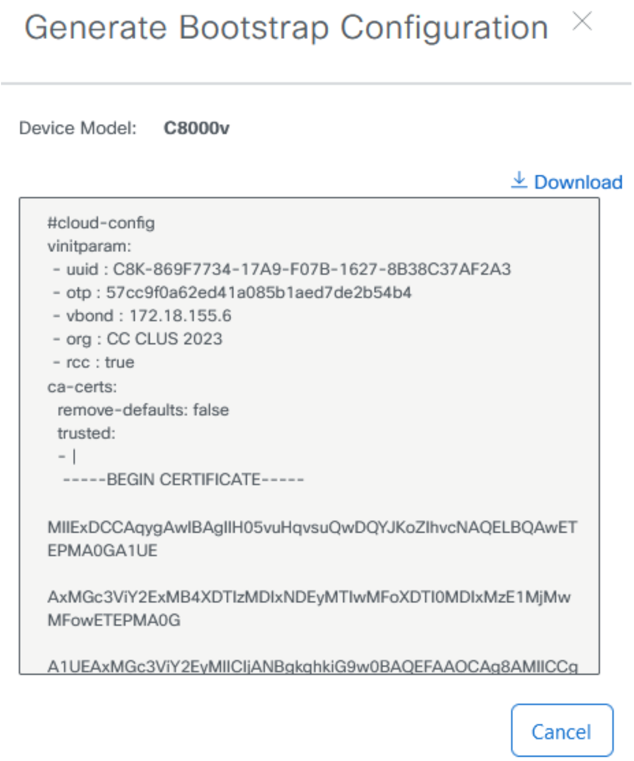
Bootstrap Configuration

● Cloud-Init ○ Encoded String

Include Default Root Certificate

Step 4 The bootstrap information will appear. Save the information, specifically the UUID and OTP (One Time Password).

Figure 21. vManage Virtual cEdge Bootstrap Info



Generate Bootstrap Configuration

Device Model: **C8000v**

```
#cloud-config
vinitparam:
 - uuid : C8K-869F7734-17A9-F07B-1627-8B38C37AF2A3
 - otp : 57cc9f0a62ed41a085b1aed7de2b54b4
 - vbond : 172.18.155.6
 - org : CC CLUS 2023
 - rcc : true
ca-certs:
  remove-defaults: false
  trusted:
  - |
   -----BEGIN CERTIFICATE-----

MIIExDCCAqygAwIBAgIIH05vuHqvsuQwDQYJKoZIhvcNAQELBQAwET
EPMA0GA1UE

AxMGc3ViY2ExMB4XDTIzMDIxNDEyMTIwMFoXDTI0MDIxMzE1MjMw
MFowETEPMA0G

A1UEAxMGc3ViY2EyMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCg
```

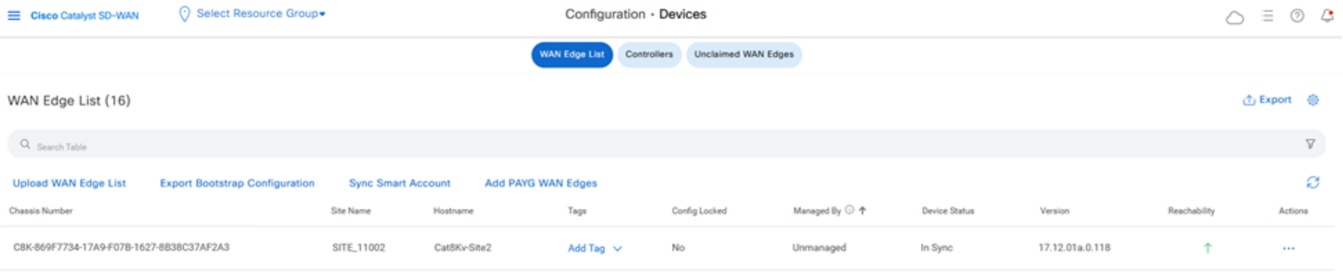
Step 4 From the C8000v CLI, issue the command **request platform software sdwan vedge_cloud activate chassis-number C8K-869F7734-17A9-F07B-1627-8B38C37AF2A3 token 57cc9f0a62ed41a085b1aed7de2b54b4.**

```
Cat8Kv-Site2# request platform software sdwan vedge_cloud activate chassis-number C8K-869F7734-17A9-F07B-1627-8B38C37AF2A3 token 57cc9f0a62ed41a085b1aed7de2b54b4
```

NOTE: *There is only a single space between chassis-number, the UUID, and token. Also, the period at the end of the OTP is not part of the OTP.*

Step 5 Once completed, the device will appear in the WAN Edge list showing a status of **In Sync**, will be listed as **Reachable**, and will have the **Site Name**, **Hostname** and **Version** fields populate.

Figure 22. vManage Virtual cEdge Router Activated



WAN Edge List (16)

Chassis Number	Site Name	Hostname	Tags	Config Locked	Managed By	Device Status	Version	Reachability	Actions
C8K-869F7734-17A9-F07B-1627-8B38C37AF2A3	SITE_11002	Cat8Kv-Site2	Add Tag	No	Unmanaged	In Sync	17.12.01a.0.118	↑	···

3.7.10 cEdge Certificate Installation

This section provides the steps necessary to install certificates on a cEdge router from vManage. The process is similar to that used for certificate installation on the controllers themselves.

Step 1 Using the menu in the upper left and navigate to **Configuration** then **Certificates** then select **WAN Edge List**.

Step 2 On the right side under **Actions**, select the **...** icon, and then select **Renew Device CSR** for vManage. A pop-up window appears with the certificate signing request. Download or copy the certificate signing request to submit for signing.

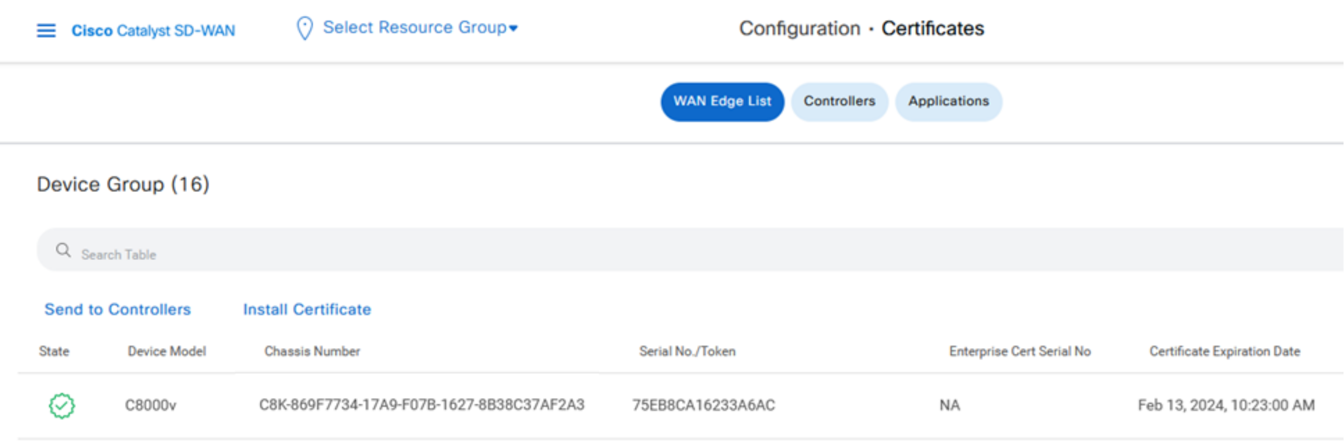
NOTE: *If pop-ups are not enabled/allowed by the Administrators browser, navigate to* ***Configuration*** *then* ***Certificates*** *then select* ***WAN Edge List****. From here select the* ***...*** *icon, and then select* ***Renew Device CSR*** *for vManage. The Administrator can copy the CSR from here.*

Step 3 Submit the CRS's to the CA to sign the requests.

Step 4 Once signed, return to the vManage and navigate to **Configuration** then **Certificates** then select **WAN Edge list**. This time select the **Install Certificate** link. No specific controller needs to be selected. vManage applies the certificates to the proper device.

Step 5 Once the process completes, the Certificates WAN Edge List will show the certificate serial number and certificate expiration for the cEdge device.

Figure 23. vManage cEdge Certificate Installed



State	Device Model	Chassis Number	Serial No./Token	Enterprise Cert Serial No	Certificate Expiration Date
✓	C8000v	C8K-869F7734-17A9-F07B-1627-8B38C37AF2A3	75EB8CA16233A6AC	NA	Feb 13, 2024, 10:23:00 AM

Step 6 Certificate installation may also be verified from the CLI, though the command is slightly different in IOS XE. Use the **show sdwan certificate root-ca-cert | include Subject:** command.

```
C8Kv-1# show sdwan certificate root-ca-cert | include Subject:
```

The **show sdwan certificate installed** may be used to view the actual device certificate.

```
C8Kv-1# show sdwan certificate installed
```

3.8 Setting SD-WAN Components to be Managed by vManage

One of the advantages of the SD-WAN solution is the idea of central management. Being able manage and distribute configurations to the various controllers and edge devices from vManage simplifies configuration management. To allow for configuration management and large-scale configuration updates of the controllers and edge devices, vManage makes use of configuration templates. Templates may be created for the various device models and tailored to site specific requirements. This allows performing configuration changes to the solution with less effort.

Additionally, once cEdge devices are managed by vManage the **commit** command is disabled in the controllers and cEdge routers. This improves security, but limiting device configuration management to a single device, as well as preventing accident out of sync issues by preventing confirmation changes to a device from the device. This ensures the configuration in vManage is the actual configuration on the device.

In the event of network connectivity issues, a device that loses contact with vManage will allow an authorized administrator that is remotely logged into the device to locally modify the configurations. This feature is for trouble shooting purposes. Once network connectivity is re-established, the device will use the latest configuration stored in vManage and it will be automatically applied.

There are essentially two types of templates, Feature Templates and Device Templates. Feature templates are for features. Features may be System Info, VPN Info, Interface, routing protocols (OSBF, EIGRP, OSPF), etc. Device templates are collections of feature templates. For a given device model/type there may multiple device templates depending on hardware difference (different NICs for example), site architecture (two ISP to one box, two to separate boxes, two boxes with HSRP), etc.

Templates have Default values assigned. When a parameter is set to Default, the default setting for the device will be used. For example, the default SSH time out setting for the cEdge routers is 120 minutes. Default may be changed to one of two other values:

- Global: Setting is none default, but consistent in the enterprise. As an example, the organization-name must be set, and it is the same in all devices.
- Device-Specific: Treated as a variable and at the time of deployment, user needs to provide specific values for each site. As an example, the IP address on a specific interface, such as G0/0/0, varies from device to device and must be uniquely set.

Providing site specific variable is done either manually or with a CSV file.

3.8.1 Create Templates

Device templates are built by combining/associating various feature templates. There are two options for creating a device template. Once is to start by creating a device template, and step through the feature template selection process for each feature. The option to create a new feature template exists within the device template creation process. The second option is to create the feature templates first and then when creating a device temple simply select the already created feature templates. For this example, feature templates are created before creating the device template. This method displays a little more flexibility in the GUI, but each method is equally acceptable.

In this example, the Template will be made for a Catalyst 8000V cEdge router, but the principles are the same for other cEdge devices or controllers. The templates will be configured to match the previously described CLI input configuration. There are a number of types of feature templates, but to build this configuration, only the following are needed:

Cisco AAA Template
Cisco System Template
Cisco VPN Template
Cisco VPN Interface Ethernet
Cisco Logging
CLI Add-On Template

There will be more than five templates created, but only these five template types will be needed. To create a feature template the process initial process is the same:

Step 1 From withing the vManage GUI, navigate to **Configuration** > **Templates** > **Feature Templates**.

Step 2 Select **Add Template**.

Step 3 From the **Select Device** list check the device type, **C8000v** in this example.

Step 4 From the list on the right, click the specific template, for example, **Cisco AAA**.

In the examples that follow, if a parameter is not specifically mentioned, the value for that parameter will be left as is, in other words the default setting will be used.

3.8.1.1 Create Cisco System Template

The Cisco System template contains basic device system information such as Site ID, System IP, and Hostname. In this instance console baud rate will also be configured, which is more important for the physical cEdge routers.

Step 1 Begin feature template configuration as described in section 3.8.1 Create Templates above and select Cisco System as the template type.

Step 2 Enter a **Template Name** and **Description**, for example, "C8Kv-01-System" (for both)

Step 3 Ensure **Site ID** is set as device specific. Variable name is [system_site_id].

Step 4 Ensure **System IP** is set as device specific. Variable name is [system_system_ip].

Step 5 Ensure **Hostname** is set as device specific. Variable name is [system_host_name].

Step 6 Configure Console Baud Rate (bps) as global and set to 9600.

Step 7 Click **Save** to save/create the feature template.

3.8.1.2 Create Cisco AAA Template

The Cisco AAA template contains access and authentication, including local user access, remote authentication using RADIUS, and 802.1x. In this instance local users will be configured.

Step 1 Begin feature template configuration as described in section 3.8.1 Create Templates above and select Cisco AAA as the template type.

Step 2 Enter a **Template Name** and **Description**, for example, "C8Kv-01-AAA" (for both)

Step 3 Click **New User**.

Step 4 Provide a **Name**, **Password**, and **Privilege** level (1 or 15) for the administrator. Leave the parameters set as global. Then click **Add.**

Step 5 Repeat Steps 3 and 4 for any additional administrators.

Step 6 Ensure **ServerGroups priority order** is set to global and select **local.**

Step 7 Click **Save** to save/create the feature template.

3.8.1.3 Create Cisco VPN Templates

The Cisco VPN template contains settings related to the VPN/VRF configurations and includes default route configurations. Three templates will be needed, one for VPN0 (transport side), VPN512 (management), and VPN2 (service side).

Start by creating a template for VPN0.

Step 1 Begin feature template configuration as described in section 3.8.1 Create Templates above and select Cisco VPN as the template type.

Step 2 Enter a **Template Name** and **Description**, for example, "C8Kv-01-VPN0" (for both)

Step 3 Ensure **VPN** is set as global and is set to **0**.

Step 4 Set **Name** to global and provide a name, such as "Transport Side VPN".

Step 5 To add a default route, click New IPv4 Route.

Step 6 Set **Prefix** to global and set as **0.0.0.0/0**, and ensure **Gateway** is set to **Next Hop**.

Step 7 Click **+ Add Next Hop** and then **Add Next Hop** on the popup window.

Step 8 Set **Address** to device specific. Variable name is [vpn_next_hop_ip_address_0].

Step 9 Click **Add** in the popup window and then **Add** in the IPv4 section.

Step 10 Click **Save** to save/create the feature template.

To create a template for VPN512, we will use the template from VPN0 as the basis versus configuring from scratch. This will show the usefulness of the copy and edit functions.

Step 1 Using the Feature Template list, find the previously created template for VPN0. From the far right of that template, click the **...** icon and select **Copy**.

Step 2 Enter a **Template Name** and **Description**, for example, "C8Kv-01-VPN512" (for both), and then click **Copy**.

Step 3 Using the Feature Template list, find the newly copied template. From the far right of that template, click the **...** icon and select **Edit**.

Step 4 Change the **VPN** setting to **512.**

Step 5 Change the **Name** to something such as "Management VPN".

***NOTE**: The default router may remain unchanged. This will be used as the default route for VRF/VPN 512 only. And the actual default was a variable so can be set at the time of template upload to the device.*

Step 6 Click **Save** to save/create the feature template.

To create a template for VPN2, the service side VPN in this example, we will use the template from VPN0 as the basis versus configuring from scratch.

Step 1 Using the Feature Template list, find the previously created template for VPN0. From the far right of that template, click the **...** icon and select **Copy**.

Step 2 Enter a **Template Name** and **Description**, for example, "C8Kv-01-VPN2" (for both), and then click **Copy**.

Step 3 Using the Feature Template list, find the newly copied template. From the far right of that template, click the **...** icon and select **Edit**.

Step 4 Change the **VPN** setting to **2.**

Step 5 Change the **Name** to something such as "Service Side VPN".

Step 6 Use the delete (trash can icon) to remove the IPv4 route.

NOTE: *Service side will use directly connected router and routers learned through OSPF (in this example), so no default router is needed.*

Step 7 Click **Save** to save/create the feature template.

3.8.1.4 Create Cisco VPN Interface Ethernet Templates

The Cisco VPN Ethernet Interface template contains settings related to the ethernet interface configurations and includes ip address, speed, and duplex configurations. Three templates will be needed, one for GigabitEthernet1 (transport side), GigabitEthernet4 (management), and GigabitEthernet3 (service side).

Start by creating a template for GigabitEthernet1 (transport side).

Step 1 Begin feature template configuration as described in section 3.8.1 Create Templates above and select Cisco VPN Interface Ethernet as the template type.

Step 2 Enter a **Template Name** and **Description**, for example, "C8Kv-01-VPN0-Eth1" (for both)

Step 3 Set **Shutdown** as global and is set to **No**.

Step 4 Set **Interface Name** as global and is set to **GigabitEthernet1**.

Step 5 Set **Description** as global and provide a description, such as "Transport Side Public Internet".

Step 6 Ensure interface is set to use a **Static** address.

Step 7 Set **IPv4 Address/ prefix-length** to device specific. Variable name is [vpn_if_ipv4_address].

Step 8 Set **Tunnel Interface** as global and is set to **On**.

Step 9 Set **Interface Name** as global and is set to **GigabitEthernet1**.

Step 10 Set **Color** as global and is set to **public-internet**.

Step 11 Set **Groups** as global and is set to **1**.

Step 12 Set Allow Service **All** as global and is set to **on**.

Step 13 Set **Autonegotiation** as global and is set to **On**.

Step 14 Click **Save** to save/create the feature template.

Now create a template for GigabitEthernet4 (management).

Step 1 Using the Feature Template list, find the previously created template for GigabitEthernet1. From the far right of that template, click the **...** icon and select **Copy**.

Step 2 Enter a **Template Name** and **Description**, for example, “C8Kv-01-VPN512-Eth4” (for both), and then click **Copy**.

Step 3 Using the Feature Template list, find the newly copied template. From the far right of that template, click the **...** icon and select **Edit**.

Step 4 Change **Interface Name** setting **GigabitEthernet3**.

Step 6 Change **Description** setting to something such as “Management”.

Step 7 Change **Tunnel Interface** to default. Verify off is checked.

Step 8 Click **Save** to save/create the feature template.

Lastly create a template for GigabitEthernet3 (service side).

Step 1 Using the Feature Template list, find the previously created template for GigabitEthernet1. From the far right of that template, click the **...** icon and select **Copy**.

Step 2 Enter a **Template Name** and **Description**, for example, “C8Kv-01-VPN2-Eth3” (for both), and then click **Copy**.

Step 3 Using the Feature Template list, find the newly copied template. From the far right of that template, click the **...** icon and select **Edit**.

Step 4 Change **Interface Name** setting **GigabitEthernet3**.

Step 6 Change **Description** setting to something such as “Service Side”.

Step 7 Change **Tunnel Interface** to default. Verify off is checked.

Step 8 Click **Save** to save/create the feature template.

3.8.1.5 Create Cisco Logging Templates

The SD-WAN solution allows for storing logs local and to a remote server. To configure the local storage and remote storage options, perform the following steps.

Step 1 Begin feature template configuration as described in section 3.8.1 Create Templates above and select Cisco Logging as the template type.

Step 2 Enter a **Template Name** and **Description**, for example, "C8Kv-01-Logging" (for both)

NOTE: *By default, logging to local disk is enabled and local logging will allow a maximum of ten 10 MB files. Once a tenth file is created, subsequent record will over-write the oldest file. If this is sufficient, no configuration of Disk settings is required, and the Administrator can skip to step 5.*

Step 3 To change the size of the log files, set **Maximum File Size (MB)** to a global parameter and enter a value of 1 to 20.

Step 4 To change the size of the number of files used in the log file rotation, set **Rotations** to a global parameter and enter a value of 1 to 10.

Step 5 To configure a Syslog Server, select **New Server**.

Step 6 Set **Hostname/IPv4 Address** as global and enter the IP or FQDN of the Syslog Server.

NOTE: *By default, traffic to the Syslog Server will use VPN 0 and the associated interface to reach the server. If necessary, the Administrator can specify a different VPN and interface appropriate for their topology by configuring the* ***VPN ID*** *and* ***Source Interface*** *parameters.*

Step 7 To use TLS for Syslog data, set **TLS** parameter a type global and set the parameter to **On**.

Step 8 Select **Add**.

Step 9 Click **Save** to save/create the feature template.

3.8.1.6 Create Cisco CLI Add-On Templates

The Cisco Cli Add-On allows entering CLI supported commands from the device template for commands that may not be supported through the other feature templates. In the example below, the CLI Add-On template will be used to add an enable password, OSPF routing, "platform console serial" used for virtual console access, and three system commands. These commands are necessary for this example deployment but cannot be added by any other feature template.

NOTE: *Changes in command line commands may require periodic updates to reflect changes in code format/option.*

Step 1 Begin feature template configuration as described in section 3.8.1 Create Templates above and select Cisco CLI Add-On Template as the template type.

Step 2 Enter a **Template Name** and **Description**, for example, "C8Kv-01-CLI-AddOn" (for both)

Step 3 Paste text-based commands into the text window, for example:

```
enable secret Password

interface GigabitEthernet3
ip ospf 2 area 0

router ospf 2 vrf 2

platform console serial

system
  no track-default-gateway
  upgrade-confirm      15
  vbond 10.122.83.212 port 12346
```

NOTE: *These are essentially global style command. To change make a command device specific carry out the steps below.*

Step 4 To change a value from a global parameter to a device specific parameter, with the mouse and cursor highlight the text to change. For example, in the above commands highlight "Password".

Step 5 Click the Encrypt Type 6 link.

Step 6 The Command line will encrypt the password and will change it to "$CRYPT_CLUSTER$..". In this example:

```
enable secret Password
```

becomes

```
enable secret $CRYPT_CLUSTER$O+1MrrTXIEwmcBNqBciQVg==$6Yrn0BLt9Wvnrz6H8kW8eg==
```

Step 7 Click **Save** to save/create the feature template.

3.8.1.7 Create Device Templates

Having created all the necessary feature templates, the overarching device template may be created. The previously created feature templates are listed in the table below for reference.

Table 15 Created Feature Templates

Feature Template Name	Template Type
C8Kv-01-System	Cisco System
C8Kv-01-AAA	Cisco AAA
C8Kv-01-VPN0	Cisco VPN
C8Kv-01-VPN512	Cisco VPN
C8Kv-01-VPN2	Cisco VPN
C8Kv-01-VPN0-Eth1	Cisco VPN Interface Ethernet
C8Kv-01-VPN512-Eth4	Cisco VPN Interface Ethernet
C8Kv-01-VPN2-Eth3	Cisco VPN Interface Ethernet
C8Kv-01-Logging	Cisco Logging
C8Kv-01-CLI-AddOn	CLI Template

Step 1 From withing the vManage GUI, navigate to **Configuration** > **Templates** > **Device Templates.**

Step 2 Select the **Create Template** dropdown and then from the dropdown select **From Feature Template**.

Step 3 On the page that appears next, from the **Device Model** dropdown select the device type, **C8000v** in this example.

Step 4 From the **Device Role** dropdown select the device type, **SDWAN Edge** in this example.

Step 5 Provide a **Template Name** and **Description**, such as "C8Kv-01-DeviceTemp" (for both).

Step 6 For **Cisco System** dropdown select the Cisco System template, **C8Kv-01-System** in this example.

Step 7 For **Cisco Logging** dropdown select the Cisco Logging template, **C8Kv-01-Logging** in this example.

Step 8 For **Cisco AAA** dropdown select the Cisco AAA template, **C8Kv-01-AAA** in this example.

Step 9 For **Cisco VPN 0** dropdown select the Cisco VPN template for VPN0, **C8Kv-01-VPN0** in this example.

Step 10 Under **Cisco VPN 0** For **Cisco VPN Interface Ethernet** dropdown select the Cisco VPN Interface Ethernet to be used for VPN 0 (which uses interface GigabitEthernet1), **C8Kv-01-VPN0-Eth1** in this example.

Step 11 For **Cisco VPN 512** dropdown select the Cisco VPN template for VPN0, **C8Kv-01-VPN512** in this example.

Step 12 To the right under **Additional Cisco VPN 512 Templates** click **+ Cisco VPN Interface Ethernet.** A Cisco VPN Interface Ethernet drop down will now appear under Cisco VPN 512.

Step 13 Under **Cisco VPN 512** For **Cisco VPN Interface Ethernet** dropdown select the Cisco VPN Interface Ethernet to be used for VPN 0 (which uses interface GigabitEthernet1), **C8Kv-01-VPN512-Eth4** in this example.

Step 14 Under **Service VPN** click Add **VPN.**

Step 15 An Add VPN window appears. Select the Cisco VPN template for service side from the available column (left), **C8Kv-01-VPN2** in this case, and use the arrows to move it to the Selected column (right). Then Click **Next.**

Step 16 To the right under **Additional Cisco VPN Templates** click **+ Cisco VPN Interface Ethernet**. A Cisco VPN Interface Ethernet drop down will now appeas.

Step 17 In the window, for **Cisco VPN Interface Ethernet** dropdown select the Cisco VPN Interface Ethernet to be used for VPN 2 (which uses interface GigabitEthernet1), **C8Kv-01-VPN2-Eth3** in this example.

Step 18 Click **Add**.

Step 19 Scroll down to **Additional Templates**. Under the **CLI Add-On Template** dropdown, select the CLI Template (if any) to be applied. In this example the template is **C8Kv-01-CLI-AddOn**.

Step 20 Click **Create**.

The template is now displayed in the list of available Device Templates.

3.8.2 Attach Device to Template

The devices may now be attached (associated) to the template. Once competed successfully, the device configuration will be managed solely through vManage.

Step 1 From withing the vManage GUI, navigate to **Configuration** > **Templates** > **Device**.

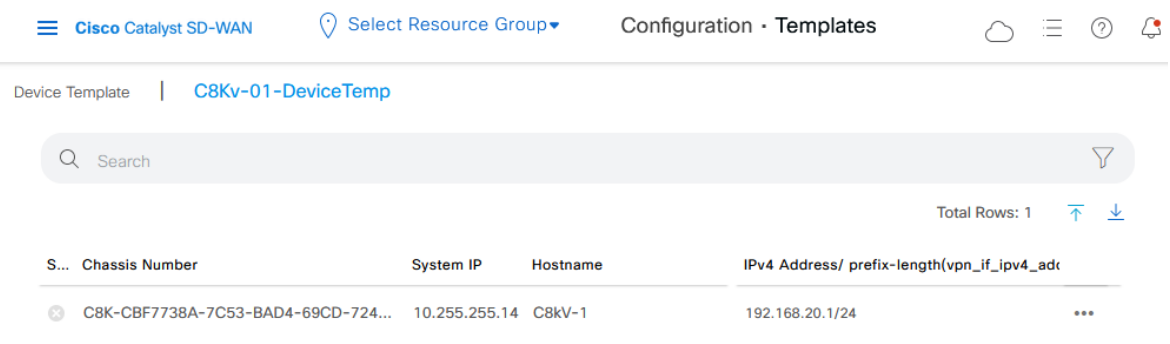
Step 2 Find the template in question and click on the **...** icon to the far right of the template. Select **Attach Devices.**

Step 3 From the Attach Device popup window, use the mouse and cursor to select the device(s) in question from the **Available Devices** column (left). Then use the arrows to move them to the **Select Devices** column (right).

Step 4 Click **Attach** from within the popup window.

Step 5 In the next page use the Down Arrow (upper right area) to download the template for device specific variable.

Figure 24. Download Device Specific Variable



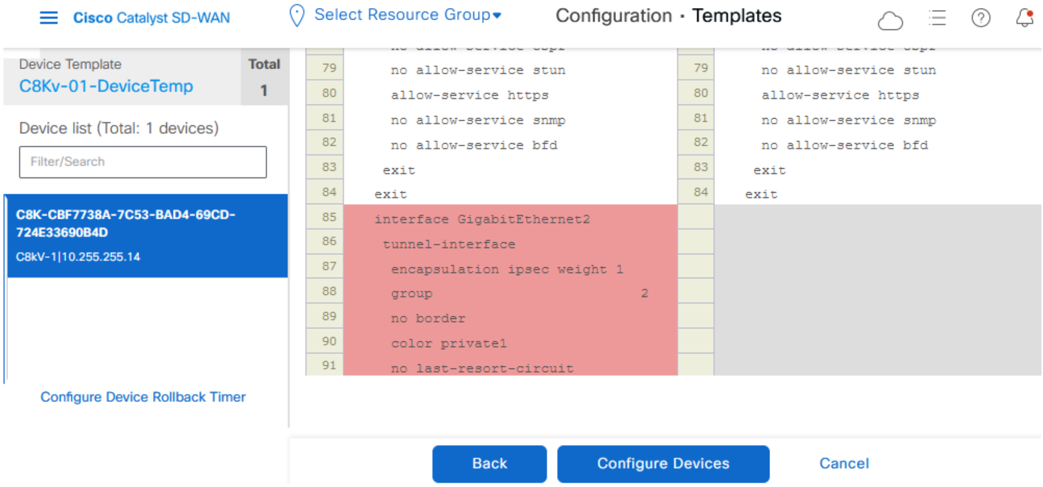
S...	Chassis Number	System IP	Hostname	IPv4 Address/ prefix-length(vpn_if_ipv4_adc
☒	C8K-CBF7738A-7C53-BAD4-69CD-724...	10.255.255.14	C8kV-1	192.168.20.1/24

Step 6 Data fill the template. All site-specific variable, such as interface ip addresses, default gateways, site ID, etc. will need to be entered here.

Step 7 Use the Up Arrow to upload the data back to vManage. Assuming data has been provided for all variable, a green check box will appear to the left of the device chassis ID(s). Prior to upload, a grayed out "X" appears. See above figure.

Step 8 Click **Next.** A list of devices appears on the left. By clicking on the device, you can preview the CLI commands that vManage will push to the device to configure it (Config Preview) or compare the configuration to be pushed to what is already running on the device (Config Diff). Additionally, when comparing the configurations Inline and Side-by-Side views are available.

Figure 25. Configuration Comparison



```
    no allow-service stun
    allow-service https
    no allow-service snmp
    no allow-service bfd
   exit
  exit
  interface GigabitEthernet2
   tunnel-interface
    encapsulation ipsec weight 1
    group                      2
    no border
    color private1
    no last-resort-circuit
```

```
    no allow-service stun
    allow-service https
    no allow-service snmp
    no allow-service bfd
   exit
  exit
```

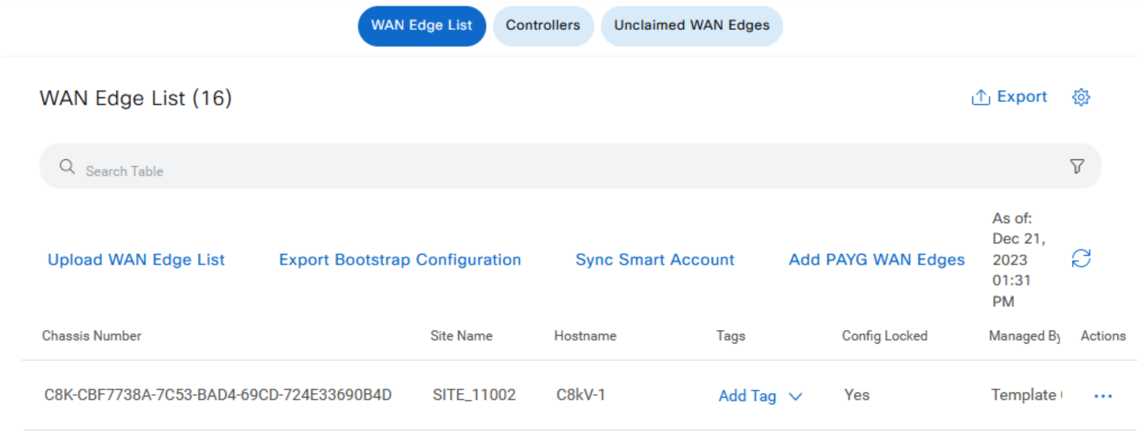
Note: *While not required, the comparison tool may help quickly identify potential error before pushing a configuration.*

Note: *There is also a rollback timer that ca be configured. The default setting is 5 minutes.*

Step 9 To continue the deployment, click **Configure Devices**. vManage will validate the configuration, then start the push. Once competed the screen will indicate the template was successfully attached.

By navigating to **Configuration** > **Devices**, the device now shows managed by Template and Config (from local) is now locked. The device can no longer be configured remote via SSH or ESXi Virtual Remote Console, except for trouble shooting purposes when the device loses connectivity to the controllers,

Figure 26. Device Managed



Chassis Number	Site Name	Hostname	Tags	Config Locked	Managed By	Actions
C8K-CBF7738A-7C53-BAD4-69CD-724E33690B4D	SITE_11002	C8kV-1	Add Tag	Yes	Template	···

If there had been a problem with the configuration, say network connectivity lost as a result of the push, or an invalid parameter entered in the variable template, or an error in processing the request by the edge device the configuration would revert as a result of the Rollback Timer. In the even this occurs, a log listing why the rollback occurred will be available to the administrator.

3.8.3 Editing Device Templates and Configuration Changes

Once brought into management by vSmart devices may have configuration changes made by editing/modifying the associated templates.

Consider a change to a feature template make a change to feature template used by the device template to which device(s) is attached.

Step 1 From within the vManage GUI, navigate to **Configuration** > **Templates** > **Feature Templates**.

Step 2 Using the Feature Template list, find a template such as “C8Kv-01-VPN2-Eth3”. From the far right of that template, click the **...** icon and select **Edit**.

Step 3 Change **Description** setting from “Service Side” to “LAN”, then click **Update**.

Step 4 vManage will display the device associated with the template. In the event the change introduces a new device specific variable, you will need to download the variable file, add the data, then upload the completed file.

In the event the change is not device specific, but rather global, there will be a green check mark beside the device(s).

Step 5 Click **Next.**

Step 6 If desired, review the CLI config that will be pushed and/or perform a configuration comparison.

Step 7 Click **Configure Devices**.

Step 8 To continue the deployment, click **Configure Devices**. vManage will validate the configuration, then start the push. Once competed the screen will indicate the template was successfully attached.

By navigating to **Configuration** > **Devices**, the device now shows managed by Template and Config (from local) is now locked. The device can no longer be configured remote via SSH or ESXi Virtual Remote Console, except for trouble shooting purposes when the device loses connectivity to the controllers,

If there had been a problem with the configuration, say network connectivity lost as a result of the push, or an invalid parameter entered in the variable template, or an error in processing the request by the edge device the configuration would revert as a result of the Rollback Timer. In the even this occurs, a log listing why the rollback occurred will be available to the administrator.

Consider a change directly to the device template.

Step 1 From within the vManage GUI, navigate to **Configuration** > **Templates** > **Device Templates**.

Step 2 Scroll down to additional Templates and from the **Cisco Banner** dropdown select **Create Template**.

Step 3 Set **Template Name** and **Description**, such as "C8Kv-01-Banner".

Step 4 Set **Login Banner** to global and enter text "**Authorized Administrators Only**".

Step 5 Click **Save**.

Step 6 Click **Update**.

Step 7 vManage will display the device associated with the template. In the event the change introduces a new device specific variable, you will need to download the variable file, add the data, then upload the completed file.

In the event the change is not device specific, but rather global, there will be a green check mark beside the device(s).

Step 8 Click **Next.**

Step 9 If desired, review the CLI config that will be pushed and/or perform a configuration comparison.

Step 10 Click **Configure Devices**.

Step 11 To continue the deployment, click **Configure Devices**. vManage will validate the configuration, then start the push. Once competed the screen will indicate the template was successfully attached.

By navigating to **Configuration** > **Devices**, the device now shows managed by Template and Config (from local) is now locked. The device can no longer be configured remote via SSH or ESXi Virtual Remote Console, except for trouble shooting purposes when the device loses connectivity to the controllers,

If there had been a problem with the configuration, say network connectivity lost as a result of the push, or an invalid parameter entered in the variable template, or an error in processing the request by the edge device the configuration would revert as a result of the Rollback Timer. In the even this occurs, a log listing why the rollback occurred will be available to the administrator.

3.8.4 Detach Device Template

There may be instance where a device needs to be detached from a template. Once competed successfully, the device configuration will be managed solely through vManage.

Step 1 From withing the vManage GUI, navigate to **Configuration** > **Templates** > **Device Templates**.

Step 2 Find the template in question and click on the **...** icon to the far right of the template. Select **Detach Devices**.

Step 3 From the Detach Device popup window, use the mouse and cursor to select the device(s) in question from the **Available Devices** column (left). Then use the arrows to move them to the **Select Devices** column (right).

Step 4 Click **Detach** from within the popup window. Once competed the screen will indicate the template was successfully attached.

By navigating to **Configuration** > **Devices**, the device now shows unmanaged by Template and Config (from local) is no longer locked.

4 SECURE MANAGEMENT

Note: Once a device is in template mode, the CLI will be limited. Administrators login in via CLI will be have full access to the TOE CLI options but no administrative changes in *exec mode* can be saved. Any "**commit**" attempt will result in the following error message:
Aborted: 'system is-vmanaged': This device is being managed by vManage, configuration through CLI is not allowed.

This section details the installation and configuration for the Virtual System hardware and software (needed for the SD-WAN controller VM's and virtual cEdge router VM's), which are part of the operational environment, as well as installation of the TOE hardware and software components (cEdge routers, SD-WAN controller VM's, and virtual cEdge router VM's).

4.1 User Roles

The credentials configured during initial component installation are system credentials and should not be used for ongoing management. Separate usernames/accounts should be configured for each authorized administrator for ongoing TOE access.

NOTE: *While the products that comprise the TOE allow assigning users to multiple roles with varying/limited levels of access, in the CC configuration only the Security Administrator role should be used. For Controller components this means assignment to the "netadmin" role. For cEdge devices this means providing "level 15" access. The sections that follow shows how to configure the Security Administrators to meet those requirements.*

4.1.1 User Roles for Controller TOE Components

The Controller devices allow the creation of administrator accounts, and in the process, associating those administrators with a User Group. User Groups provide differing levels of read/write access to different feature levels (Policy, Routing, Security, Interface). This allows providing an administrator with only the level of access needed to perform their role, assuming multiple administrators with different roles are requires. To review the User Groups and their level of access, from withing the vManage Web GUI, navigate to **Administration** then **Manage Users** then **User Groups**. Clicking on a particular User Group on the left will display the level of access for that User Group.

4.1.1.1 vManage User Management from vManage GUI

Users or Administrators added via the vManage GUI provide access to only vManage. This access is for both Web GUI and CLI.

To add an Administrator to vManage, perform the followings steps.

Step 1 Navigate to **Administration** then **Manage Users** then **Users**.

Step 2 Select **Add User**.

Step 3 In the pop-up window that appears provide the administrators name, username, password, and select the User Group. When completed, select **Add.**

To remove an Administrator to vManage, perform the followings steps.

Step 1 Navigate to **Administration** then **Manage Users** then **Users**.

Step 2 Find the User in question and click on the **...** icon to the far right of the template. Select **Delete.**

Step 3 In the pop-up window that appears click **OK**.

4.1.1.2 Controller User Management from CLI

To add a user to one of the controllers via CLI, enter the following commands into the CLI.

```
vsmart# config t
Entering configuration mode terminal
vsmart(config)# system
vsmart(config-system)# aaa
vsmart(config-aaa)# user admin2 group netadmin
vsmart(config-user-admin2)# password <password>
vsmart(config-user-admin2)# commit
Commit Complete.
```

In the example above User “admin2” was created and associated with the group “netadmin” and a password was assigned.

To remove a user from CLI, enter the following commands into the CLI.

```
vsmart# config t
Entering configuration mode terminal
vsmart(config)# system
vsmart(config-system)# aaa
vsmart(config-aaa)# no user admin2
vsmart(config-aaa)# commit
Commit complete.
```

4.1.1.3 Controller User Management from Template

Note: *For vBond, the feature template is listed as vEdge Cloud.*
To add a user to a controller via template, perform the following steps.

Step 1 From within the vManage GUI, navigate to **Configuration** > **Templates** > **Feature Templates**.

Step 2 Scroll down and find the AAA template used by the controller device templated to which the controller is associated, such as, "vSmart-01-AAA. From the far right of that template, click the **...** icon and select **Edit**.

Step 3 Scroll down to the local section and Click **New User**.

Step 4 Provide a **Name**, **Password**, and **User Group** for the administrator. Leave the parameters set as global. Then click **Add**.

Step 5 Repeat Steps 3 and 4 for any additional administrators.

Step 6 Click **Update** to save the feature template changes.

To remove a user from a controller via template, perform the following steps.

Step 1 From within the vManage GUI, navigate to **Configuration** > **Templates** > **Feature Templates**.

Step 2 Scroll down and find the AAA template used by the controller device templated to which the controller is associated, such as, "vSmart-01-AAA. From the far right of that template, click the **...** icon and select **Edit**.

Step 3 Scroll down to the local section and Click **New User**.

Step 4 Click the **Delete** (trash can) icon.

Step 5 Click **Update** to save the feature template changes.

4.1.2 User Roles for cEdge TOE Components

cEdge device run IOS XE software which has both privileged and semi-privileged administrator roles as well as non- administrative access. Non-administrative access is granted to authenticated neighbor routers for the ability to receive updated routing tables. There is no other access or functions associated with non-administrative access.

A semi-privileged access one with the most basic level of access for viewing and executing commands. Privileged access is defined by any privilege level entered during the creation of the administrator account. Privilege levels are number 0-15, where the number specifies the level for the administrator. The privilege levels are not necessarily hierarchical. Privilege level 15 has access to all commands on the TOE. Privilege levels 0 and 1 are defined by default, while levels 2-14 are undefined by default. Levels 0-14 can be set to include any of the commands available to the level 15 administrator and are considered the semi-privileged administrator for purposes of this evaluation. The privilege level determines the functions the user can perform, hence the authorized administrator with the appropriate privileges.

4.1.2.1 cEdge User Management from CLI

To add a user to one of the controllers via CLI, enter the following commands into the CLI.

router# **config-t**

```
router(config)# username admin2 privilege 15 secret 9 <password>
router(config)#
```

In the example above User “admin2” was created and associated with privilege level 15 and a password was assigned.

To remove a user from CLI, enter the following commands into the CLI.

```
router# config-t
router(config)# no username admin2
router(config)#
```

4.1.2.2 cEdge User Management from Template

To add a user to a controller via template, perform the following steps.

Step 1 From within the vManage GUI, navigate to **Configuration** > **Templates** > **Feature Templates**.

Step 2 Scroll down and find the Cisco AAA template used by the controller device templated to which the controller is associated, such as, “C8Kv-01-AAA. From the far right of that template, click the **...** icon and select **Edit**.

Step 3 Scroll down to the local section and Click **New User**.

Step 4 Provide a **Name**, **Password**, and **User Group** for the administrator. Leave the parameters set as global. Then click **Add**.

Step 5 Repeat Steps 3 and 4 for any additional administrators.

Step 6 Click **Update** to save the feature template changes.

To remove a user from a controller via template, perform the following steps.

Step 1 From within the vManage GUI, navigate to **Configuration** > **Templates** > **Feature Templates**.

Step 2 Scroll down and find the Cisco AAA template used by the controller device templated to which the controller is associated, such as, “c8Kv-01-AAA. From the far right of that template, click the **...** icon and select **Edit**.

Step 3 Scroll down to the local section and Click **New User**.

Step 4 Click the **Delete** (trash can) icon.

Step 5 Click **Update** to save the feature template changes.

4.2 Passwords

It is assumed the Organization will have requirements related to acceptable passwords, such as:

- Minimum password length, such as limiting the minimum number of characters in a password.
- Complexity requirements, such as the password must be a combination of upper and lower case letters (a-z and A-Z), numbers (0-9), and the following special characters "!", "@", "#", "$", "%", "^", "&", "*", "(",")".
- Not allowing words found in the dictionary, such as "password".

While the Administrator and Users are ultimately responsible for password policy enforcement, so SD-WAN components allow configurations that help enforce such policies.

4.2.1 vManage Password Policies

The IOS-XE cEdge cloud routers do not support password-policy configuration from CLI or from vManage using feature-based templates, include Cisco CLI Add-on templates. Password policies will be determined by the organization, and Administrators and Users will be responsible for adhering to those policies when setting passwords.

4.3 Identification and Authentication

Configuration of Identification and Authentication settings is restricted to the privileged administrator. In the evaluated configuration the TOE components perform local authentication, though it can also perform authentication with a RADIUS server.

4.3.1 Controller Local Authentication

The sections below detail how to configure local authentication for controller via CLI and template.

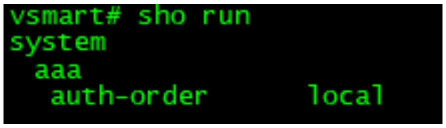
4.3.1.1 Controller Local Authentication Configuration via CLI

Note: CLI configuration will be overwritten by any feature templates. This feature might be used when setting up cEdge routers.
To configure a controller for only local authentication from the CLI, enter the following commands into the CLI

```
vsmart# config t
vsmart(config)# system
vsmart(config-system)# aaa
vsmart(config-aaa)# auth-order local
vsmart(config-aaa)# commit
Commit complete.
```

Once completed, the configuration can be verified using the show **run command** from CLI.

Figure 27. Controller Local Authentication Verification



```
vsmart# sho run
system
  aaa
   auth-order       local
```

NOTE: *Some output has been omitted for clarity.*

4.3.1.2 Controller Local Authentication Configuration via Template

To add a user to a controller via template, perform the following steps.

Step 1 From within the vManage GUI, navigate to **Configuration** > **Templates** > **Feature Templates**.

Step 2 Scroll down and find the AAA template used by the controller device templated to which the controller is associated, such as, “vSmart-01-AAA. From the far right of that template, click the **...** icon and select **Edit**.

Step 3 Authentication Order should be set for global.

Step 4 Click on the value and uncheck “radius” and “tacacs”.

Step 5 Verify **Authentication Order** only contains “local” at this point.

Step 6 If any changes were made, click **Update** to save the feature template changes.

The show run command used above can be used to verify configuration here as well.

4.3.2 cEdge Local Authentication

The sections below detail how to configure local authentication for cEdge routers via CLI and template.

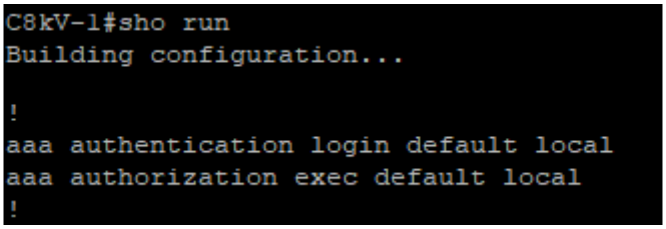
4.3.2.1 cEdge Local Authentication Configuration via CLI

Note: CLI configuration will be overwritten by any feature templates. This feature might be used when setting up cEdge routers.
To configure a cEdge router for only local authentication from the CLI, enter the following commands into the CLI

```
C8kV-1#config-t
C8kV-1(config)# aaa authentication login default local
C8kV-1(config)# aaa authorization exec default local
C8kV-1(config)# commit
Commit complete.
```

Once completed, the configuration can be verified using the show **run command** from CLI.

Figure 28. cEdge Local Authentication Verification



```
C8kV-1#sho run
Building configuration...

!
aaa authentication login default local
aaa authorization exec default local
!
```

NOTE: *Some output has been omitted for clarity.*

4.3.2.2 cEdge Local Authentication Configuration via Template

To add a user to a controller via template, perform the following steps.

Step 1 From within the vManage GUI, navigate to **Configuration** > **Templates** > **Feature Templates**.

Step 2 Scroll down and find the AAA template used by the controller device templated to which the controller is associated, such as, "C8Kv-01-AAA. From the far right of that template, click the **...** icon and select **Edit**.

Step 3 Scroll down to the **Authentication and Authorization Order** section

Step 4 **ServerGroups priority order** should only have "local" listed. If not, remove "radius" and "tacacs".

Step 5 Verify **ServerGroups priority order** only contains "local" at this point.

Step 6 If any changes were made, click **Update** to save the feature template changes.

The show run command used above can be used to verify configuration here as well.

4.4 Session Management

TOE components can be configured to ensure sessions no longer in use time out and limit the number of failed attempts for access by a given user account.

Note: *An authorized user who is configured with privilege level 15 cannot be locked out with this feature. The number of users with privilege level 15 must be kept to a minimum.*

4.4.1 vManage GUI Session Management

To configure vManage GUI session management, perform the following steps.

Step 1 From within the vManage GUI, navigate to **Administration** > **Settings.**

Step2 To configure session timeout, scroll to **Client Session Timeout** and click **Edit.**

Step 3 Set **Session Timeout** to Enabled, set the **Timeout** (minutes) between 10 and 30, and click **Save**.

Step 4 To set the number of failed login attempts, scroll down to **Number of failed login attempts** and click **Edit**.

Step5 Configure the lockout parameters as needed and click **Save**.

Table 16 vManage GUI Number of Failed Login Attempts Configurable Parameters

Parameter	Description	Allowed Values
Number of failed login attempts before lockout	Number of failed logins at which lockout occurs.	1-3600
Duration within which the failed attempts are counted (minutes)	Interval during which successive failed lockouts will be counted towards lockout.	1 - 60
Cooldown or Lockout period	If enable account will reset and be allowed access after a specified time interval.	Enabled or Disabled
Lockout Interval (minutes)	After a lockout occurs, the time interval after which the account may attempt access again.	1 – 60

4.4.2 Controller and cEdge GUI Session Timeout

To configure vManage This parameter is configured using the AAA or Cisco AAA feature template. To configure vManage SSH session management, perform the following steps.

Step 1 From within the vManage GUI, navigate to **Configuration > Templates**.

Step2 Search for the previously created System or Cisco System templates used in the currently associated/deployed device templates, for example the feature template “C8Kv-01-AAA” used by the device template “C8Kv-01-DeviceTemp”. On the far right click the **...** icon and select **Edit**.

Step3 Scroll to the **ADVANCED** section and set Idle Timeout as a global time out and set the time out duration, in minutes from 0 (disabled) to 300.

Step 4 Click **Update** to save the feature template changes.

4.4.3 Controller SSH Session Lockout

Most parameters available for configuration for GUI Session Lockout are available for the controllers SSH sessions when configured from the CLI.

```
vsmart# config t
```

```
Entering configuration mode terminal
vsmart(config)# system
vsmart(config-system)# aaa
vsmart(config-aaa)# lockout-policy
vsmart(config-lockout-policy)# fail-attempts
vsmart(config-lockout-policy)# fail-interval
vsmart(config-lockout-policy)# lockout-interval
vsmart(config-lockout-policy)# num-inactive-days
vsmart(config-lockout-policy)# commit
Commit complete.
```

Table 17 Controller SSH Number of Failed Login Attempts Configurable Parameters

Parameter	Description	Allowed Values
fail-attempts	Number of failed authentication attempts before lockout.	1-3600
fail-interval	Interval for consecutive authentication failures in seconds	1-3600
lockout-interval	Interval user is locked out after failure (seconds) - 0 for indefinite lockout	0 - 3600
num-inactive-days	Lockout user if inactive for these many days	2 - 365

NOTE: *When the controllers are managed by vManage using templates, the above parameters are not configurable via feature templates. "fail-attempts" is set to 5 by default.*

4.4.4 cEdge SSH Session Lockout

For cEdge routers lockout is configurable using the Cisco CLI Add-on template.

Step 1 From within the vManage GUI, navigate to **Configuration** > **Templates** > **Feature Templates**.

Step2 Search for the previously created System or Cisco System templates used in the currently associated/deployed device templates, for example the feature template "C8Kv-01-CLI-AddOn" used by the device template "C8Kv-01-DeviceTemp". On the far right click the **...** icon and select **Edit**.

Step 3 Add the following CLI command to the template, **aaa local authentication attempts max-fail x**. In this case, x may range from 0 to 65535.

Step 4 Optionally, to allow for use of a variable, Highlight "**x**", click **Create Variable**, provide a variable name, such as login_fail_attempts, and click **Create Variable**.

Step 5 Click **Update** to save the changes to the template.

4.5 Login Banners

The TOE components provide the authorized administrator the ability to configure a banner that displays on the Web GUI and CLI management interfaces prior to allowing any administrative access to the TOE.

4.5.1 vManage Web GUI Login Banner

Step 1 From withing the vManage Web GUI, navigate to **Administration** then **Settings**.

Step 2 Find the Banner configuration line and select **Edit**.

Step 3 Enable the banner and supply the desired Banner text. Alternatively, a file containing the banner may be uploaded.

Step 4 Select **Save**.

During subsequent logins, administrator will see the text, after entering valid credentials, and will need to acknowledge the text before continuing to the management interface.

4.5.2 Controller Login Banner via CLI

Note: CLI configuration will be overwritten by any feature templates. This feature might be used when setting up controllers.

The Controller CLI message must be configured at the CLI. To configure the CLI banner execute the following commands from the CLI.

```
vsmart#  config t
Entering configuration mode terminal
vManage-1(config)# banner login
(<string, min: 1 chars, max: 2048 chars>): Authorized Administrators Only
vManage-1(config-banner)# commit
Commit complete.
```

Subsequent logins will display the banner before credentials are entered.

4.5.3 cEdge Login Banner via CLI

Note: CLI configuration will be overwritten by any feature templates. This feature might be used when setting up cEdge routers.

cEdge banners work like the Controller CLI banner and are configured as follows.

```
Cat8Kv-Site2# config-t
Cat8Kv-Site2(config)# banner login Authorized Administrators Only
Cat8Kv-Site2(config)# commit
```

Commit complete.

Subsequent logins will display the banner before credentials are entered.

4.5.4 Login Banner via Template

Banners can be configured using the Banner or Cisco Banner feature templates, for controllers and cEdge devices respectively. As stated in 3.8.1 Create Templates, Feature templates can be created separately then added to a device template or created from withing the device template. In this example we start with the device template.

Note: *To prevent truncation of the login banner from a template being pushed onto cEdge devices, an administrator must configure the login banner as follows:*

\n\n This is a Banner test \n \”

To add a banner, perform the following steps.

Step 1 From withing the vManage GUI, navigate to **Configuration** > **Templates** > **Device Templates**.

Step 2 Using the Device Template list, find the previously created template for the device(s) to be configured, for example “C8Kv-01-DeviceTemp”. From the far right of that template, click the **...** icon and select **Edit**.

Step 3 Scroll down to the bottom section, and for **Banner/Cisco Banner** use the drop down to select **Create Template**.

Step 3 Set **Template Name** and **Description**, such as “C8Kv-01-Banner”.

Step 4 Set **Login Banner** to global and enter text, such as “**Authorized Administrators Only**”.

Step 5 Click **Save** to save the template and confirm it is now the select Banner/Cisco Banner template.

Step 6 Click **Update** to save the device template with the desired Banner/Cisco Banner template.

To Edit a banner, edit the Banner/Cisco Banner feature template by performing the following steps.

Step 1 From within the vManage GUI, navigate to **Configuration** > **Templates** > **Feature Templates**.

Step 2 Scroll down and find the previously created banner template, “C8Kv-01-Banner” in this example. From the far right of that template, click the **...** icon and select **Edit**.

Step 3 Set **Template Name** and **Description**, such as “C8Kv-01-Banner”.

Step 4 Change **Login Banner** text to “**Unauthorized Personnel Only – Unauthorized Users Will Be Prosecuted**”.

Step 5 Click **Update**.

To remove a banner, perform the following steps.

Step 1 From withing the vManage GUI, navigate to **Configuration** > **Templates** > **Device Templates**.

Step 2 Using the Device Template list, find the previously created template for the device(s) to be configured, for example "C8Kv-01-DeviceTemp". From the far right of that template, click the **...** icon and select **Edit**.

Step 3 Scroll down to the bottom section, and for **Banner/Cisco Banner** use the drop down to select **None**.

Step 5 Verify there is no longer an associated feature template.

Step 6 Click **Update** to save the device template without a Banner/Cisco Banner template.

4.6 Firewall

The TOE provides stateful traffic firewall functionality including IP address-based filtering to address the issues associated with unauthorized disclosure of information, inappropriate access to services, misuse of services, disruption or denial of services, and network-based reconnaissance. Address filtering can be configured to restrict the flow of network traffic between protected networks and WAN based on source and/or destination IP addresses. Port filtering can be configured to restrict the flow of network traffic between protected networks and other attached networks based on the originating (source) and/or receiving (destination) port (service). System monitoring functionality includes the ability to generate audit messages for any explicitly defined (permitted or denied) traffic flow. TOE administrators have the ability to configure permitted and denied traffic flows, including adjusting the sequence in which flow control rules will be applied, and to apply rules to any network interface of the cEdge routers.

Firewall rules are built through vManage as a Security policy using a policy configuration wizard. For firewall policies, the Administrator configures zones and a policy to apply to those zones. Each zone consists of one or more VPNs in the overlay network. Additionally, the Administrator defines a source zone, which identifies the VPNs from which data traffic originates, and a destination zone, which identifies the VPNs to which the traffic is being sent.

The firewall policy consists of a series of numbered (ordered) sequences of match-action pairs that are evaluated in order, from the lowest sequence number to the highest sequence number. When a data packet matches the match conditions, the associated action or actions are taken, and policy evaluation on that packet stops. If a packet matches no parameters in any of the policy sequences, the default action, which is configurable, is taken.

The examples that follow are designed as a general overview of configuration and deployment of Security Policies, however the Administrator is referred to **[19] Cisco Catalyst SD-WAN Policies Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x** and **[20] Cisco Catalyst SD-WAN Security Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x** for additional information.

The policy configuration wizard is a tool that allows the Administrator to create policy components used to configure firewall policies. Specifically, the policy configuration wizard allows the Administrator to:

- **Create Lists** – Lists are groupings of related items that you reference in the match portion of the firewall policy configuration.
- **Create Firewall Policy** – Which is a Container for a firewall policy.
- **Apply Configuration**

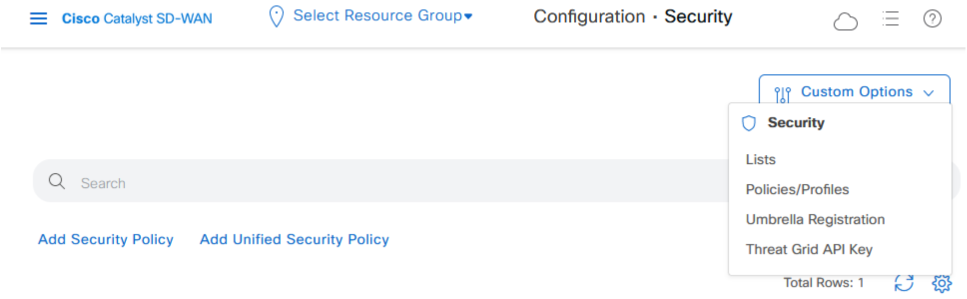
Similar to the creation of feature and device templates, some components may be defined prior to building the firewall rule, they may be defined during the firewall build process, or a mix of the two.

The Administrator may define Lists, a.k.a. Groups of Interest, as follows:

Step 1 in vManage navigate to **Configure > Security**.

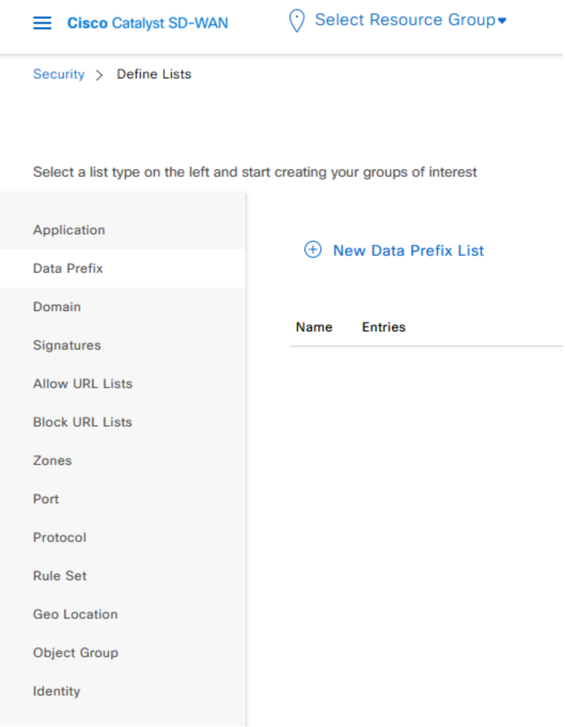
Step 2 In the upper right of the screen, click the **Custom Options** dropdown and click **Lists.**

Figure 29. Path to List Types



NOTE: *On the left hand side now appears a selection of list types for creating groups of interests. The groups of interest include Application, Data Prefix, Zones, etc. This allows the Administrator to configure policies that are looking specific traffic based on such things as type of application, IP addresses (source or destination), and VPN (source or destination), respectively.*

Figure 30. Available List Types



Select a list type on the left and start creating your groups of interest

Step 3 Create a new list, such as a Zone. In the list to the left click **Zones** and then **+ New Zone List.**

Step 4 Provide **Zone List Name**, select **Zone Type** (VPN or Interface), and then provide the **VPN or Interface Name**. When completed Click **Add.** Repeat this step to add multiple Zone Lists.

Zone List examples are shown in the table below.

Table 18 Example Zone Lists

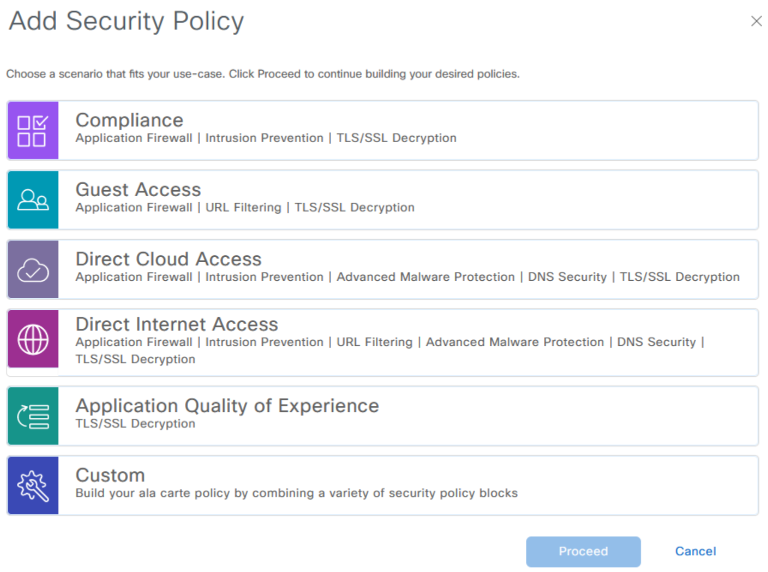
Zone List Name	Entries
Inside	GigabitEthernet0/0/1
VPN1	1

NOTE: *ZONES can be defined as a VPN or as the more traditional interface.*

NOTE: *A VPN Zone can contain multiple VPN ID's, but they must be separated by commas, i.e., VPN 1 and VPN 2 are listed as 1,2. A VPN Zone can contain more than a single interface by using the* ***+*** *icon to the right of the box where the interface name is added. This will add a second box for a second interface. Subsequent interfaces can be added similarly.*

When using the template to create Firewall Rules, the Administrator will need to select the security policy use case.

Figure 31. Security Policy Use Cases



Add Security Policy

Choose a scenario that fits your use-case. Click Proceed to continue building your desired policies.

- Compliance
  Application Firewall | Intrusion Prevention | TLS/SSL Decryption
- Guest Access
  Application Firewall | URL Filtering | TLS/SSL Decryption
- Direct Cloud Access
  Application Firewall | Intrusion Prevention | Advanced Malware Protection | DNS Security | TLS/SSL Decryption
- Direct Internet Access
  Application Firewall | Intrusion Prevention | URL Filtering | Advanced Malware Protection | DNS Security | TLS/SSL Decryption
- Application Quality of Experience
  TLS/SSL Decryption
- Custom
  Build your ala carte policy by combining a variety of security policy blocks

Based on the selection, the wizard will present only relevant elements for configuration. The table below provides a description of what is configured by a given use case.

Table 19 Security Use Case Policy Descriptions

Security Policy Use-Case	Description
Compliance	Applies application firewall and intrusion prevention.
Guest Access	Applies application firewall and Cisco URL Filtering.
Direct Cloud Access	Applies application firewall, intrusion prevention, Advanced Malware Protection, and DNS Umbrella security.
Direct Internet Access	Applies application firewall, intrusion prevention, Cisco URL Filtering, Advanced Malware Protection, and DNS Umbrella security.
Application Quality of Experience	Applies encryption.
Custom	Build your own security policy by combining various security policy blocks.

***NOTE:** When Custom is chosen, the wizard will step through all possible elements and the Administrator will determine what elements are relevant and need to be configured versus what may be skipped. For skipped elements, there may be default configurations applied.*

With this basic understanding of the components of Fire Wall configuration, the next subsections will walk through some actual example configurations.

4.6.1 FW Example 1 – Inspect ICMP Traffic

In this example the Firewall Policy will be configured to inspect ICMP traffic that is sourced from IPv4 addresses 10.8.61.0/28 and destined for IPv4 addresses 10.8.61.32/28 through VPN1 in a given device.

4.6.1.1 Configure the Policy

To configure the Firewall Policy and Security Policy, the Administrator carriers out the following steps.

Step 1 in vManage navigate to **Configure > Security**.

Step 2 In the upper right of the screen, click the **Custom Options** dropdown and click **Lists.**

Step 3 In the list to the left click **Zones** and then **+ New Zone List.**

Step 4 Provide **Zone List Name**, select **Zone Type** (VPN or Interface), and then provide the **VPN or Interface Name.** When completed Click **Add.** Repeat this step to add multiple Zone Lists.

Zone List examples are shown in the table below.

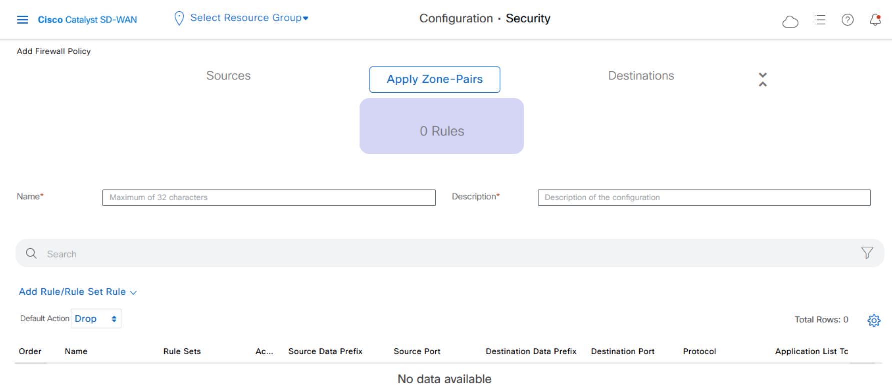
Table 20 Example Zone Lists

Zone List Name	Entries
Inside	GigabitEthernet0/0/1
VPN1	1

Step 5 Navigate back to the **Security** page, select **Add Security Policy**, select the user-case, such as **Custom**, and then click **Proceed.** See table below for various option.

Step 6 Click the **Add Firewall Policy** dropdown and click **Create New**.

Figure 32. Firewall Policy Template



Order	Name	Rule Sets	Ac...	Source Data Prefix	Source Port	Destination Data Prefix	Destination Port	Protocol	Application List Tc

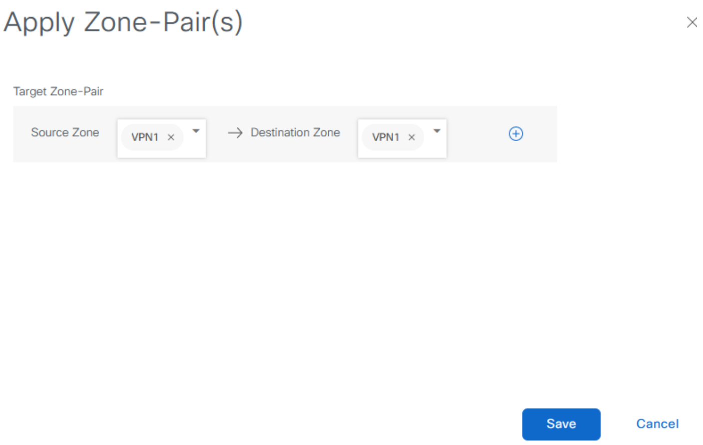
No data available

Step 7 Provide a policy name and description, such as “Security_Policy_11_2_0_VPN1”.

Step 8 Click on Apply Zone-Pairs and select the **Source Zone** and **Destination Zone.** They may be different zones or the same depending on the intent, say “VPN1” for both. A second zone-pair may be added using the **+** icon to the right of the destination zone box. Once zone-pair info is added click **Save.**

Step 9 Click the **Add Rule/Rule Set Rule** dropdown click **Add Rule.**

Figure 33. Zone-Pair Configureation



Apply Zone-Pair(s)

Target Zone-Pair

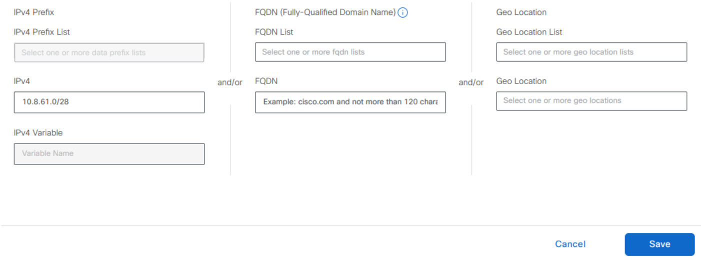
Source Zone: VPN1 × → Destination Zone: VPN1 ×

Step 10 From the **Edit Firewall Rule** window, set the:

Name - such as “11.2.8_Inspect_10.8.61.32”
Action - either Inspect, Pass, or Drop. In this case **Inspect**.
Source – such as IPv4 network “10.8.61.0/28”
Destination – such as IPv4 network “10.8.61.32/28”
Protocol – such as ICMP

Note: *To add source, destination, etc., click the* ***+*** *icon by the associated label, data fill the desired element type (IPv4 or FQDN for example), then click* ***Save****.*

Figure 34. Firewall Rules Template – Source Field



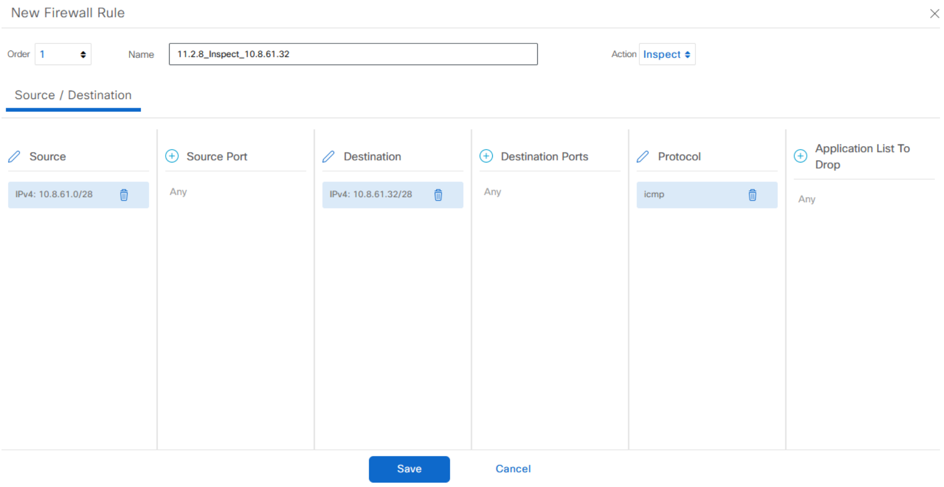
IPv4: 10.8.61.0/28

IPv4 Prefix
IPv4 Prefix List
Select one or more data prefix lists
IPv4 Variable
Variable Name
and/or
FQDN (Fully-Qualified Domain Name)
FQDN List
Select one or more fqdn lists
FQDN
Example: cisco.com and not more than 120 chara
and/or
Geo Location
Geo Location List
Select one or more geo location lists
Geo Location
Select one or more geo locations
Cancel
Save

Note: *When entering Source and Destination information, pre-defined IPv4 and FQDN lists may also be used. These would be created in a fashion similar to creating Zone Lists as described in steps 2 and 3* *above. The difference is that from the list type list* ***Data Prefix*** *would be selected and then click on* ***+ New Data Prefix List.***

Step 11 Once the rules are defined, click **Save.**

Figure 35. Firewall Rules Template


New Firewall Rule

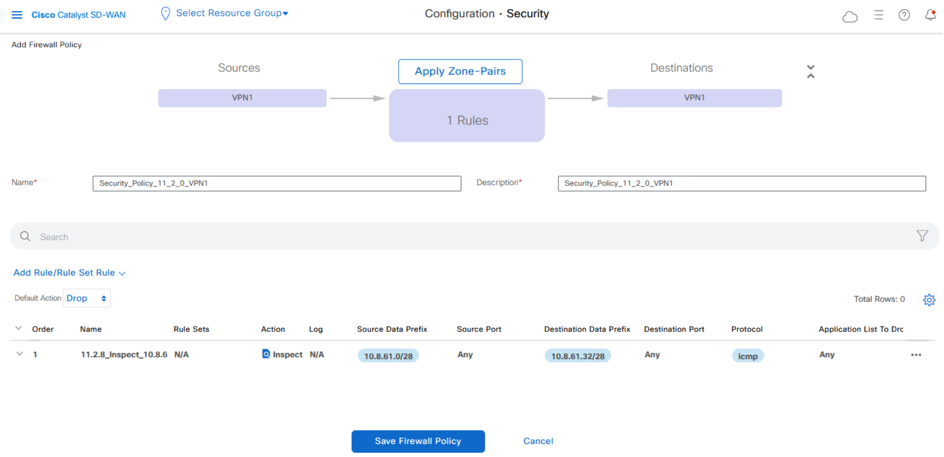
Order 1 Name 11.2.8_Inspect_10.8.61.32 Action Inspect

Source / Destination

Source	Source Port	Destination	Destination Ports	Protocol	Application List To Drop
IPv4: 10.8.61.0/28	Any	IPv4: 10.8.61.32/28	Any	icmp	Any

Step 12 Click **Save Firewall Policy.**

Figure 36. Firewall Policy Template – Data Filled



Name* Security_Policy_11_2_0_VPN1 Description* Security_Policy_11_2_0_VPN1

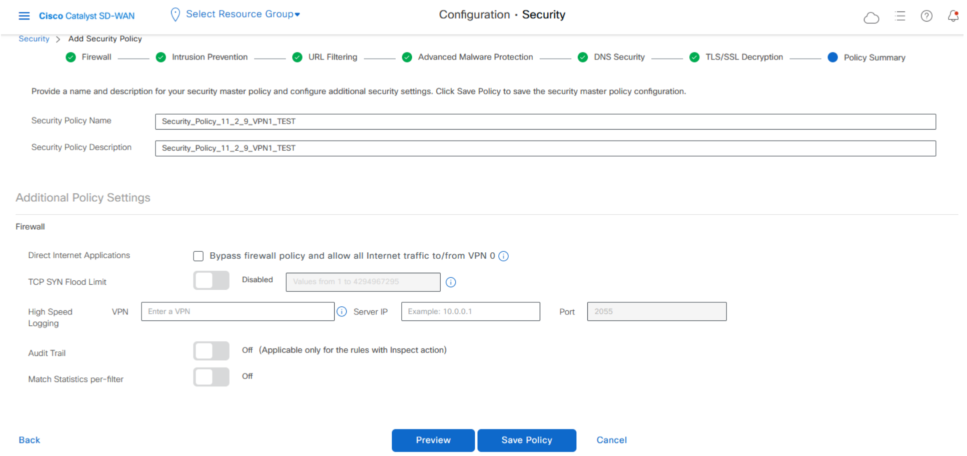
Default Action Drop

Total Rows: 0

Order	Name	Rule Sets	Action	Log	Source Data Prefix	Source Port	Destination Data Prefix	Destination Port	Protocol	Application List To Drc
1	11.2.8_Inspect_10.8.6	N/A	Inspect	N/A	10.8.61.0/28	Any	10.8.61.32/28	Any	icmp	Any

Step 13 Click Next until at the **Policy Summary** tab. Provide a name, such as "Security_Policy_11_2_9_VPN1_TEST".

Figure 37. Security Policy Summary



Provide a name and description for your security master policy and configure additional security settings. Click Save Policy to save the security master policy configuration.

Security Policy Name: Security_Policy_11_2_9_VPN1_TEST

Security Policy Description: Security_Policy_11_2_9_VPN1_TEST

Additional Policy Settings

Firewall

Direct Internet Applications: □ Bypass firewall policy and allow all Internet traffic to/from VPN 0

TCP SYN Flood Limit: Disabled — Values from 1 to 4294967295

High Speed Logging: VPN — Enter a VPN; Server IP — Example: 10.0.0.1; Port — 2055

Audit Trail: Off (Applicable only for the rules with Inspect action)

Match Statistics per-filter: Off

Step 14 Click **Preview** to see the CLI commands that will be deployed.

```
      policy
       zone-based-policy Security_Policy_11_2_0_VPN1
          sequence 1
           seq-name 11.2.8_I-191164727
           match
            source-ip 10.8.61.0/28
            destination-ip 10.8.61.32/28
            protocol 6 17
            protocol-name icmp
           !
           action inspect
           !
          !
        default-action drop
       !
        zone VPN1
         vpn 1
        !
        zone-pair ZP_VPN1_VPN1_Security__921775297
         source-zone VPN1
         destination-zone VPN1
         zone-policy Security_Policy_11_2_0_VPN1
        !
       zone-to-nozone-internet deny
!
```

Step 15 Click **Save Policy Changes** to save the policy.

4.6.1.2 Apply the Policy and Verification

Firewall Policies are localized policies and applied to devices. As an example of how to deploy a firewall policy, use the following steps.

Step 1 From within the vManage GUI, navigate to **Configuration > Templates**.

Step2 Search for the previously created Device templates used in the currently associated/deployed device templates, for example the feature template, such as "C8Kv-01-DeviceTemp". On the far right click the **...** icon and select **Edit**.

Step 3 Scroll down to the **Additional Templates** section and under the Security Policy dropdown select the desired security policy, such as the policy "Security_Policy_11_2_9_VPN1_TEST" above.

Step 4 Click **Update** to apply the Security Policy Template.

Step 5 If any devices are attached to the configuration, the Administrator will be provided a list of attached devices. Assuming no variables were defined in the Security Policy, the attached devices should have green checkmarks to the left of their Chassis Number, and the Administrator just clicks **Next**. Otherwise, variables will need to be uploaded before continuing.

Step 6 From the next screen the Administrator may either click **Configure Devices** or click **Config Preview** to review the changes and the click **Configure Devices**.

Step 7 Once the Status of the changes to Success the Security Policy has successfully been deployed.

The operation of the policy may now be verified. Perform the following steps.

Step1 If desired, execute the following commands (command are in bold face below) from CLI of the device in question to confirm the policy is in place. The fourth command will also provide the Zone-Pair name deployed in the device, which will be useful in verifying the performance of the policy a few steps down.

```
C8kV-1#show object-group
Network object group Security_Policy_11_2_0_VPN1-11.2.8_l-191164727-nw-dstn_
 10.8.61.32 255.255.255.240

Network object group Security_Policy_11_2_0_VPN1-11.2.8_l-191164727-nw-src_
 10.8.61.0 255.255.255.240

Service object group Security_Policy_11_2_0_VPN1-11.2.8_l-191164727-svc_
 ip

C8kV-1#show policy-map type inspect
  Policy Map type inspect Security_Policy_11_2_0_VPN1
    Class Security_Policy_11_2_0_VPN1-seq-1-cm_
      Inspect
    Class class-default
      Pass

C8kV-1#show zone-pair security
Zone-pair name ZP_VPN2_VPN2_Securit_-1654598303 1
    Source-Zone VPN2  Destination-Zone VPN2
    service-policy Security_Policy_11_2_0_VPN1

C8kV-1#show policy-firewall config
Zone-pair              : ZP_VPN1_VPN1_Securit_-1654598303
Source Zone            : VPN1
Destination Zone       : VPN1
Service-policy inspect : Security_Policy_11_2_0_VPN1
  Class-map : Security_Policy_11_2_0_VPN1-seq-1-cm_ (match-all)
   Match class-map Security_Policy_11_2_0_VPN1-s11.2.8_l-191164727-l4-cm_
   Match access-group name Security_Policy_11_2_0_VPN1-seq-11.2.8_l-191164727-acl_
  Action : inspect
   Parameter-map : Default
  Class-map : class-default (match-any)
   Match any
  Action : pass log
   Parameter-map : Default
---------------------------
Parameter-map Configuration:
  Parameter-map type inspect-global
  --------------------------------
   aggressive aging threshold (max-incomplete): disabled
   aggressive aging threshold (total-sessions): disabled
   alert messages                        : on
   all application inspection            : on
   lisp inner packet inspection          : off
   multi-tenancy                         : on
   icmp unreachable                      : drop
   Session reclassify                    : disable
   vpn zone security                     : enable
   vpn zone security allow-dia           : disable
   logging dropped-packets               : on
   logging flow-export FNF disabled
   sessions, max-incomplete icmp sessions     : unlimited
   sessions, max-incomplete tcp sessions      : unlimited
   sessions, max-incomplete udp sessions      : unlimited
   sessions, max-incomplete sessions          : unlimited
   No default UTD policy attached
   tcp loose window scaling enforcement       : off
   tcp syn-flood limit                   : unlimited
```

```
vrf and parameter-map binding:
  vrf name: default bound to parameter-map: vrf-default
zone mismatch drop option                  : off
```

Step 2 From within the device, execute the following commands to clear existing FW statistics.

```
show platform hardware qfp active feature firewall drop clear
show platform hardware qfp active statistics drop clear
clear zone-pair counter
clear zone-pair inspect session
clear logging
```

Step 3 Generate traffic that meets the requirements of the FW policy. Optionally you may also generate traffic that does not meet to confirm that no packets will be inspected when the criteria is not met.

Step 4 Check for inspected packets using the command **show policy-map type inspect zone-pair**.

NOTE: This command will generate output for all inspect policies. If more than one policy is in place, the Administrator may display the output of a single policy by specifying that policy using the command as follows, **show policy-map type inspect zone-pair ZP_VPN1_VPN1_Securit_-1654598303**.

```
C8kV-1#show policy-map type inspect zone-pair ZP_VPN1_VPN1_Securit_-1654598303
  Zone-pair: ZP_VPN1_VPN1_Securit_-1654598303
  Service-policy inspect : Security_Policy_11_2_0_VPN1

    Class-map: Security_Policy_11_2_0_VPN1-seq-1-cm_ (match-all)
      Match: class-map match-any Security_Policy_11_2_0_VPN1-s11.2.8_l-191164727-l4-cm_
        Match: protocol icmp
      Match: access-group name Security_Policy_11_2_0_VPN1-seq-11.2.8_l-191164727-acl_
      Inspect
        Packet inspection statistics [process switch:fast switch]
        icmp packets: [0:24]
        Session creations since subsystem startup or last reset 0
        Current session counts (estab/half-open/terminating) [0:0:0]
        Maxever session counts (estab/half-open/terminating) [0:0:0]
        Last session created never
        Last statistic reset never
        Last session creation rate 0
        Last half-open session total 0

    Class-map: class-default (match-any)
      Match: any
      Pass
        0 packets, 0 bytes
```

***NOTE:** If no traffic meets the requirements, then no ICMP traffic should be seen.*

4.6.2 FW Example 2 – Drop ICMP Traffic

In this example, we will configure a policy to drop ICMP traffic sourced from 10.8.61.4 through VPN1. The Administrator could simply build a new policy following the same process specified in 4.6.2.1 Configure the Policy only for the Firewall Rules specify only the source IP (10.8.61.4/32), the protocol (ICMP), and set the Action to Drop.

Alternatively, the Administrator may edit the exiting rule, which will be done below. The previously saved policy now appears in the list of security policies when navigating to **Configurations > Security**. As with Device and Feature templates, the policy may be edited by clicking the **...** icon to the right of the policy name and clicking **Edit**.

Once Edit has been selected, the **Policy Summary** tab is visible. The general process for editing the template is carried out using the following steps.

Step 1 From summary page, click the **Firewall** tab.

Step 2 Click the **...** icon to the right of the security policy, then click **Edit**.

Step 3 From here, the Administrator may:

- Click **Zone-Pairs** to edit/re-define the Zone Pair(s). Click **Save** after any changes.
- Update the **Name** and **Description** of the Policy.
- Change the **Default Action**.
- Add new rules, delete old rules or edit the existing rule by clicking the **...** icon to the right of the **rule and clicking Edit. Click Save after any changes.**

Step 4 After making all changes, click **Save Firewall Policy** and then **Save Policy Changes**.

The specific step-by-step process for this example follows.

4.6.1.1 Edit the Existing Policy

To edit the previously created policy the Administrator should perform the following steps.

Step 1 Navigate to **Configurations > Security**. Localte the previous Security Policy, "Security_Policy_11_2_9_VPN1_TEST", click the **...** icon to the right of the policy name and click **Edit.**

Step 2 One the Summary page that appears, click the **Firewall** tab.

Step 3 Click the **...** icon to the right of the security policy, then click **Edit.**

Step 4 Find the Firewall Rule “11.2.8_Inspect_10.8.61.32” and click the **...** icon to the right of the policy name and click **Edit.**

Step 5 Make the following changes, then click **Save.**

Name – change to “11.2.8_Deny_ICMP”
Action – change to **Drop.**
Source – change to “10.8.61.4/32”.
Destination – delete existing address.
Protocol – leave as ICMP

Step 6 Click **Save Firewall Policy.**

Step 7 Click **Preview** to see the CLI commands that will be deployed.

```
      policy
       zone-based-policy Security_Policy_11_2_0_VPN1
          sequence 1
           seq-name 11.2.8_Deny_ICMP
           match
            source-ip 10.8.61.4/32
            protocol 6 17
            protocol-name icmp
           !
           action drop
           !
          !
        default-action pass
       !
        zone VPN1
         vpn 1
        !
        zone-pair ZP_VPN1_VPN1_Security__921775297
         source-zone VPN1
         destination-zone VPN1
         zone-policy Security_Policy_11_2_0_VPN1
        !
       zone-to-nozone-internet deny
!
```

Step 8 Click **Save Policy Changes.**

Step 9 If any devices are attached to the configuration, the Administrator will be provided a list of attached devices. Assuming no variables were defined in the Security Policy, the attached devices should have green checkmarks to the left of their Chassis Number, and the Administrator just clicks **Next.** Otherwise, variables will need to be uploaded before continuing.

Step 10 From the next screen the Administrator may either click **Configure Devices** or click **Config Preview** to review the changes and the click **Configure Devices**.

4.6.2.2 Policy Verification

The verification steps for the new policy are the same as for the previous example, but are included for completeness.

Step1 If desired, execute the following commands (command are in bold face below) from CLI of the device in question to confirm the policy is in place. The fourth command will also provide the Zone-Pair name deployed in the device, which will be useful in verifying the performance of the policy a few steps down.

```
C8kV-1#show object-group
Network object group Security_Policy_11_2_0_VPN1-11.2.8_Deny_ICMP-nw-src_
 host 10.8.61.4

Service object group Security_Policy_11_2_0_VPN1-11.2.8_Deny_ICMP-svc_
 Ip

C8kV-1#show policy-map type inspect
  Policy Map type inspect Security_Policy_11_2_0_VPN1
    Class Security_Policy_11_2_0_VPN1-seq-1-cm_
      Drop
    Class class-default
      Pass

C8kV-1#show zone-pair security
Zone-pair name ZP_VPN1_VPN1_Security__921775297 2
    Source-Zone VPN1  Destination-Zone VPN1
    service-policy Security_Policy_11_2_0_VPN1

C8kV-1#show policy-firewall config
Zone-pair name ZP_VPN1_VPN1_Security__921775297 2
    Source-Zone VPN1  Destination-Zone VPN1
    service-policy Security_Policy_11_2_0_VPN1



C8kV-1#show policy-firewall config
Zone-pair              : ZP_VPN1_VPN1_Security__921775297
Source Zone             : VPN1
Destination Zone        : VPN1
Service-policy inspect : Security_Policy_11_2_0_VPN1
  Class-map : Security_Policy_11_2_0_VPN1-seq-1-cm_ (match-all)
   Match class-map Security_Policy_11_2_0_VPN1-s11.2.8_Deny_ICMP-l4-cm_
```

```
    Match access-group name Security_Policy_11_2_0_VPN1-seq-11.2.8_Deny_ICMP-acl_
   Action : drop log
    Parameter-map : Default
   Class-map : class-default (match-any)
    Match any
   Action : pass log
    Parameter-map : Default
 ---------------------------
 Parameter-map Configuration:
   Parameter-map type inspect-global
   ---------------------------------
    aggressive aging threshold (max-incomplete): disabled
    aggressive aging threshold (total-sessions): disabled
    alert messages                        : on
    all application inspection            : on
    lisp inner packet inspection          : off
    multi-tenancy                         : on
    icmp unreachable                      : drop
    Session reclassify                    : disable
    vpn zone security                     : enable
    vpn zone security allow-dia           : disable
    logging dropped-packets               : on
    logging flow-export FNF disabled
    sessions, max-incomplete icmp sessions     : unlimited
    sessions, max-incomplete tcp sessions      : unlimited
    sessions, max-incomplete udp sessions      : unlimited
    sessions, max-incomplete sessions          : unlimited
    No default UTD policy attached
    tcp loose window scaling enforcement       : off
    tcp syn-flood limit                   : unlimited
    vrf and parameter-map binding:
      vrf name: default bound to parameter-map: vrf-default
    zone mismatch drop option             : off
```

Step 2 From within the device, execute the following commands to clear existing FW statistics.

```
show platform hardware qfp active feature firewall drop clear
show platform hardware qfp active statistics drop clear
clear zone-pair counter
clear zone-pair inspect session
clear logging
```

Step 3 Generate traffic that meets the requirements of the FW policy. Optionally you may also generate traffic that does not meet to confirm that no packets will be inspected when the criteria is not met.

Step 4 Check for inspected packets using the command **show policy-map type inspect zone-pair**.

NOTE: This command will generate output for all inspect policies. If more than one policy is in place, the Administrator may display the output of a single policy by specifying that policy using the command as follows, **show policy-map type inspect zone-pair ZP_VPN1_VPN1_Security__921775297**.

```
C8kV-1# show policy-map type inspect zone-pair ZP_VPN1_VPN1_Security__921775297
 Zone-pair: ZP_VPN1_VPN1_Security__921775297
 Service-policy inspect : Security_Policy_11_2_0_VPN1

  Class-map: Security_Policy_11_2_0_VPN1-seq-1-cm_ (match-all)
   Match: class-map match-any Security_Policy_11_2_0_VPN1-s11.2.8_Deny_ICMP-l4-cm_
    Match: protocol icmp
   Match: access-group name Security_Policy_11_2_0_VPN1-seq-11.2.8_Deny_ICMP-acl_
   Drop
    12 packets, 504 bytes

  Class-map: class-default (match-any)
   Match: any
   Pass
    0 packets, 0 bytes
```

NOTE: *If no traffic meets the requirements, then no drops should be seen.*

4.7 FIPS mode

The administrator needs to configure the cEdge routers for FIPS mode of operation. This configuration only applies to cEdge routers as SD-WAN controllers are in FIPS mode by default.

Step 1 Begin feature template configuration as described in section 3.8.1 Create Templates above and select Cisco CLI Add-On Template as the template type.

Warning: Configuring FIPS mode will prevent further configuration changes via device templates. When configuring FIPS mode, Deploy all configuration except FIPs-mode first. Then modify the existing CLI Add-on template (if applicable) or create a separate CLI Add-on template (if none already exists) with the line below (Step 3), update or apply the CLI Add-on template to the device template, and then associate a device with the Device Template (Step 6).

Step 2 Enter a **Template Name** and **Description**, for example, "C8Kv-01-CLI-AddOn" (for both)

Step 3 Paste text-based commands into the text window:

platform ipsec fips-mode

Step 4 Click **Update** to save the device template.

Step 5 Click **Next** and wait for the device template to appear.

Step 6 Select the device in the column on the left side and click **Configure Devices**.

Step 7 Confirm the template was pushed successfully.

Step 8 Go to Menu on the left-hand side, select **Maintenance** then **Device Reboot**.

Step 9 Select all the devices that received the templates and click **Reboot**.

Step 10 Confirm on the cEdge routers with the following command:

```
C8kV-1# show sdwan security-info

        security-info fips-mode Enabled
```

Warning: Following enablement of FIPS mode, configuration changes via device templates to a device are essentially locked. To make any future changes to a router configuration once the router is in FIPS-mode, the authorized administrator must go through the following steps:

1. Detach template from the device
2. Remove FIPS mode on the router CLI using the command: no platform ipsec fips-mode
3. Reboot the device
4. Modify template
5. Push the modified template
6. Push the modified template with CLI Add-on

4.8 Cryptographic self-tests

The TOE runs a suite of self-tests during initial start-up to verify correct operation of cryptographic modules. If any component reports failure for the POST, the system crashes and appropriate information is displayed on the local console. All ports are blocked from moving to forwarding state during the POST. If all components of all modules pass the POST, the system is placed in FIPS PASS state and ports are allowed to forward data traffic. If any of the tests fail, a message is displayed to the local console and the TOE component will automatically reboot. If the Administrator observes a cryptographic self-test failure, they should contact Cisco Technical Support. Refer to the Contact Cisco section of this document.

If the Administrator needs to execute cryptographic self-tests for the Switch after the image is loaded enter the following command:

```
test crypto self-test
```

5 SECURITY RELEVANT EVENTS

The TOE is able to generate audit records that are stored internally within the TOE whenever an audited event occurs, as well as simultaneously offloaded to an external syslog server. The administrator can set the level of the audit records to be stored in a local buffer, sent to the syslog server, or both. Additionally, the Administrator may view files from the local CLI or vManage GUI. The details for configuration of these settings are covered in 3.8.1.5 Create Cisco Logging Templates.

Any data flow between cEdge devices, including a remote site cEdge back to a data center cEdge router, will use IPsec. However, this does not extend beyond the TOE to the Syslog Server itself. The TOE components allow for configuring logging data transfer from themselves all the way to the Syslog server itself. The configuration steps required for this are also found in section 3.8.1.5 Create Cisco Logging Templates.

The local log buffer is circular. Newer messages overwrite older messages after the buffer is full. Administrators are instructed to monitor the log buffer using the show logging privileged EXEC command to view the audit records. The first message displayed is the oldest message in the buffer.

When configured for a syslog backup, the TOE will simultaneously offload events from a separate buffer to the external syslog server. This buffer is used to queue events to be sent to the syslog server if the connection to the server is lost. It is a circular buffer, so when the events overrun the storage space, it overwrites older events. Table 21 Auditable Events below includes the security relevant events that are applicable to the TOE.

The **show logging** command can be used to display. The “i” after the pipe is to include a specific keyword like “ssh”:

```
C8Kv-2#show logging | i ssh
*Jan 16 14:02:23.697: %SSH-5-SSH2_SESSION: SSH2 Session request from 10.26.163.191 (tty = 0)
using crypto cipher 'aes128-ctr', hmac 'hmac-sha2-256-etm@openssh.com' Succeeded
```

To ensure audit records are generated for the required auditable events, the TOE must be configured in its evaluated configuration as specified in this document. This is to ensure that auditing is enabled and the audit records are being generated for the required auditable events.

Additional Audit Information is described in Column 3 of the table below.

Table 21 Auditable Events

SFR	Auditable Event	Additional Audit Record Contents
FDP_IFF.1	All decisions on requests for information flow	None
FFW_RUL_EXT.1	Application of rules configured with the ‘log’ operation	Source and destination addresses Source and destination ports Transport Layer Protocol

SFR	Auditable Event	Additional Audit Record Contents
		TOE Interface
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded. Administrator lockout due to excessive authentication failures	Origin of the attempt (e.g., IP address)
FIA_PMG_EXT.1	None	None
FIA_UID.1	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address)
FIA_UAU.2	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FMT_MOF.1 (1)	Any attempt to initiate a manual update	None
FMT_SMF.1	All management activities of TSF data	None
FPT_STM.1	Changes to the time.	The identity of the authorized administrator performing the operation. The old and new values for the time. Origin of the attempt (e.g., IP address)
FTA_SSL.1	The termination of a local session by the session locking mechanism.	None
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None
FTA_SSL.4	The termination of an interactive session.	None

SFR	Auditable Event	Additional Audit Record Contents
FTP_TRP.1	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.	None.

5.1 Deleting Audit Records

The cEdge TOE components provides the privileged Administrator the ability to delete audit records audit records stored within the TOE. This is done with the **clear logging** command.

```
C8Kv-2#clear logging
Clear logging buffer [confirm]
```

The Controller TOE components to no allow logs to be cleared by the Administrator.

5.2 Audit Records Description

The TOE generates an audit record whenever an audited event occurs. The types of events that cause audit records to be generated include cryptography related events, identification and authentication related events, and administrative events (the specific events and the contents of each audit record are listed in the table below). Each of the events is specified in syslog records in enough detail to identify the user with which the event is associated, when the event occurred, where the event occurred, the outcome of the event, and the type of event that occurred.

Additionally, the startup and shutdown of the audit functionality is audited.
The local audit trail consists of the individual audit records: one audit record for each event that occurred. The audit record can contain up to 80 characters and a percent sign (%), which follows the time-stamp information. The audit fields in each audit event will contain at a minimum the following:

E Example Audit Event: ****Jan 16 14:02:26.875: %SSH-5-SSH2_USERAUTH: User 'admin' authentication for SSH2 Session from 10.26.163.191 (tty = 0) using crypto cipher 'aes128-ctr', hmac 'hmac-sha2-256-etm@openssh.com' Succeeded***

Date: January 16
Time: 14:02:26
Type of event: SSH authentication
Subject identity: admin
Source: 10.26.163.191

Outcome (Success or Failure): Success may be explicitly stated with “success”,“passed” or “accepted”.

More specifically, for failed logins, a “Login failed” will appear in the audit event. For successful logins, a “Login success” will appear in the associated audit event. For failed events, “failure” will be denoted in the audit event. For other audit events, a detailed description of the outcome may be given in lieu of an explicit success or failure.

To ensure audit records are generated for the required auditable events, the TOE must be configured in its evaluated configuration as specified in this document. This is to ensure that auditing is enabled and the audit records are being generated for the required auditable events.

6 OBTAINING DOCUMENTATION AND SUBMITTING A SERVICE REQUEST

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation at:

With CCO login: http://www.cisco.com/en/US/partner/docs/general/whatsnew/whatsnew.html

Without CCO login: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

You can access the most current Cisco documentation on the World Wide Web at the following sites:

http://www.cisco.com

6.1 Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click Feedback in the toolbar and select Documentation. After you complete the form, click Submit to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc., Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

6.2 Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at any time, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com