CloudVision CVP Configuration Guide

Arista Networks

www.arista.com

CloudVision CVP Configuration Guide version 2023.2.0

Headquarters	Support	Sales
5453 Great America Parkway Santa Clara, CA 95054 USA		
+1-408-547-5500	+1-408-547-5502 +1-866-476-0000	+1-408-547-5501 +1-866-497-0000
www.arista.com/en/	support@arista.com	sales@arista.com

Contents

Chapter 1

Introduction to CloudVision

CloudVision is a turnkey solution for network-wide workload orchestration and work flow automation. It was specifically designed to complement SDN (virtualization) controller solutions that orchestrate virtual network overlays, by focusing on work flow visibility, automation tasks, and initial or ongoing network provisioning across the underlying physical network.

CloudVision components are packaged as a virtual appliance and operate as a highly available cluster with role based privileges integrated into existing authentication tools (AAA, RADIUS, TACACS). For maximum operational flexibility, CloudVision can be managed with the interactive CVP command line interface (CLI), the open API for granular programmatic access, or a web-based portal interface.

The foundation of CloudVision is an infrastructure service, sharing, and aggregating working state of physical switches running EOS to provide network visibility and central coordination. State from each participating EOS node is registered to CloudVision using the same publish/subscribe architecture of the EOS system database (SysDB). By communicating to each participating switch instance using a high performance binary API, CloudVision will actively synchronize state relevant to network-wide operational tasks.

The CloudVision web-based portal combines the most common operational tasks into a dashboard view decoupled from the underlying hardware. Workflow automation in CloudVision permits operators to execute common deployment and configuration tasks from a single visual touch point. The portal includes a turnkey solution for Arista's Zero Touch Provisioning (ZTP) and extends that from automating initial device provisioning to also include automating ongoing change controls over the operational life cycle of the device.

Using CloudVision, operators can organize devices in logical hierarchies through the use of containers and list of configlets for rapid categorization of devices by role, type, or other specification. Configurations can be broken down into more manageable configlets that are built and stored directly on CloudVision, ready for network-wide or group-specific provisioning. The CloudVision database also keeps historical data, including a history of network state, configuration and software versions. This state can be used for taking a network-wide snapshot for change control verification of the network, helping to simplify the change management process and reduce maintenance window times.

For more information, see:

- CloudVision Portal (CVP) Overview
- CloudVision Portal (CVP) Setup
- Getting Started (CVP)

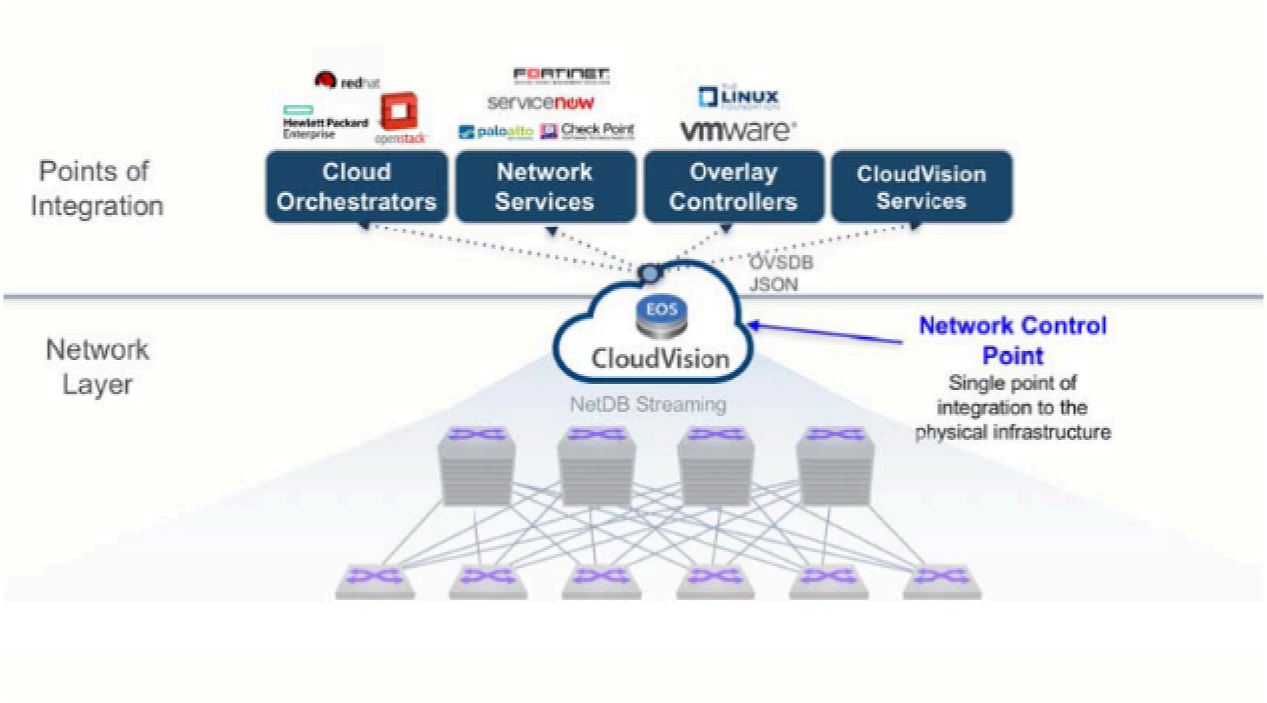
CloudVision Portal (CVP) Overview

CloudVision Portal (CVP) is the web-based GUI for the CloudVision platform.

The Portal provides a turnkey solution for automating network operations, including network device provisioning, compliance, change management, and network monitoring. It communicates southbound to Arista switches via eAPI and has open standard APIs northbound for integration with 3rd-party or inhouse service management suites.

CloudVision Portal (CVP) overview shows CloudVision as the network control point between the physical infrastructure (network layer) and the layer of service management.

Figure 2-1: CloudVision Portal (CVP) overview



Sections in this chapter include:

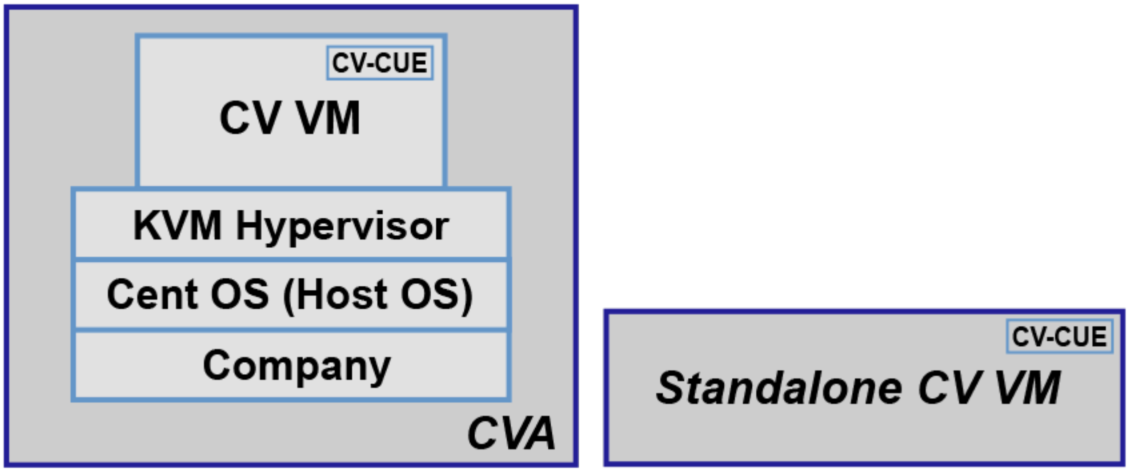
- CV-CUE
- CVP Cluster Mechanism
- System Requirements
- Key CVP Terms
- CVP Virtual Appliance

2.1 CV-CUE

The CV-CUE service is available as a container on the Arista CloudVision platform. Once you activate the CV-CUE service, you can configure, monitor, troubleshoot, and upgrade Arista WiFi access points using the cognitive CV-CUE UI.

CV-CUE Architecture provides a conceptual overview of the Arista CV-CUE solution.

Figure 2-2: CV-CUE Architecture



CV-CUE is containerized within the CV whether it's CVA (CV on a CV appliance) or a standalone CV VM. The CV-CUE service runs on both single-node CV and CV cluster. In case of a CV cluster, CV-CUE operates as a single logical instance in High Availability mode (HA-mode).

- CV-CUE HA Mode Operation
- Key Features of CV-CUE on CV
- Capacity of CV-CUE on CV

2.1.1 CV-CUE HA Mode Operation

When setting up CV-CUE for the first time, it must be enabled on all the nodes of a cluster. Once CV-CUE is enabled, then at boot time, the CV-CUE service on the primary node automatically becomes the Active instance, and the one on the secondary node becomes the Standby instance. The HA failover and recovery mechanisms work exactly as expected. That is, if the primary node goes down, the CV-CUE instance on the secondary node becomes active. When the primary node rejoins the cluster, a split-brain recovery kicks in and re-elects the new active and standby containers.

2.1.2 Key Features of CV-CUE on CV

Except for OS and kernel processes, the CV-CUE service on CV runs all the application processes required to manage Arista CV-CUE and wireless intrusion prevention system (WIPS). Some key features of the CV-CUE service are as follows:

- CV-CUE uses ports 3851 and 161 (both UDP) for all CV communication with external entities. These ports need to be opened in your network.
- CV-CUE consists of two key components:
  - **wifimanager**, the server that manages the CV-CUE network.
  - **aware**, the cognitive CV-CUE UI of the server.

2.1.3 Capacity of CV-CUE on CV

The table below shows the number of access points (APs) that a CV-CUE container supports for the given CPU, RAM, and hard disk settings. The CPU and RAM values displayed in this table are the default settings for a DCA-200 device; the actual capacity may vary based on deployment, environment, and load.

Table 1: Capacity of CV-CUE on CV

Setting	Up to 5000 APs
CPU	8 Core
RAM	32 GB
Hard Disk	250 GB

2.2 CVP Cluster Mechanism

CVP consists of distributed components such as Zookeeper, Hadoop/HDFS and HBase. Zookeeper provides consensus and configuration tracking mechanism across a cluster. Hadoop/HDFS is a distributed and redundant data store while HBase is a distributed key/value store. Running these services in a reliable fashion on multiple nodes require a quorum mechanism which is subject to limitations imposed by that mechanism.

CVP Cluster and Single Node Failure Tolerance

In absence of a quorum or a quorum leader, each node assumes itself to be the cluster leader in a three-node cluster leading to chaos and even data corruption. This leads to the quorum constraint for CVP cluster where only single node failure can survive. For example, a single node is allowed to form a cluster in a three-node cluster. In such cases, if cluster nodes cannot communicate with each other, all three nodes assume itself to be the lone survivor and operate accordingly. This is called a split-brain scenario where the original three-node cluster has split into multiple parts.

In real scenarios, assume only two nodes are active after a reboot and they failed to connect with each other. As no quorum is required, each node elects itself as the cluster leader. Now two clusters are formed where each cluster captures different data. For example, devices can be deleted from one cluster but not from the other. Device status is in compliance in one cluster but not on the other, etc. Additionally, services that store zookeeper configuration now has two copies with different data. Consequently, there is no effective way to reconcile the data when these nodes re-establish communication.

Let's consider HBase component in CVP. HBase is a distributed key-value store and splits its data across all cluster nodes. Let's assume that one node splits off from other two. If a single node can form a cluster, this single node forms one cluster and the other two together forms another cluster. It means that there are 2 HBase masters. That is the process which keeps track of metadata for all key/value pairs in HBase. In other words, HBase creates two independent sets of metadata which can even frustrate manual reconciliation. In essence, distributed infrastructure pieces must meet mandatory quorum requirements and which in turn means we cannot survive more than a single node failure.

Another reason to not tolerate dual node failures in a three-node CVP cluster is that all nodes are not made the same and total capacity of the cluster is more than what a single node can handle. Some services might be configured to run only on two of the three nodes and will fail when attempted to run on another. The total configured capacity of CVP cluster is 2 times that of a single node. That means in a three-node cluster, two nodes will have the capacity to run everything but one node cannot. Hence in a cluster of three CVP nodes, the cluster can survive only one CVP node failure.

2.3 System Requirements

The CloudVision Portal is deployed as a virtual or physical appliance.

Note: As of 2022.2.0, production instances of CloudVision should be deployed in a 3-node cluster. Single-node clusters must be used only for lab deployments.

Table 2: Minimum System Requirements

Required Hardware	
Lab Deployment (< 25 devices)	**Production Deployment**
Single node instances of CVP are supported only in lab environments. The **minimum** hardware requirements to use CVP in a lab environment are: • CPUs: 16 cores • RAM: 32 GB • Disk: 1 TB GB (use RPM installer) • Disk Throughput: 20 MB/s	A 3-node cluster must be used for production deployment. Each node must be configured to meet the minimum system requirements. The **recommended** hardware required per node to deploy CVP in a production environment (3-node cluster) are: • CPUs: 28 cores • RAM: Recommended 52 GB • Disk: 1 TB • Disk Throughput: 40 MB/s

Note: For production deployments, information about device scale is available in the release specific version of the product release notes. For more information on throughput, refer to Troubleshooting and Health Checks.

Note: Deploying a single node instance in a production environment does not provide load sharing or redundancy capabilities; which, in node failure scenarios could lead to data loss or data corruption. Due to these reasons, single node deployments will no longer be supported starting CVP release 2022.1.0. Cloud service deployment model of CloudVision (CVaaS) is recommended for production environments with smaller device scale.

Table 3: Latency Requirements

Latency Requirements
• The latency between two CVP nodes must be up to 10 ms (recommended 5 ms or less). • The latency from a CVP node to an EOS device must be up to 500 ms. • All three nodes must be installed in the same physical location and on the same local area network. • Physical appliances should be installed in the same rack so that traffic can flow between the appliances while only traversing a top-of-rack switch (or a redundant pair preferably). • Physical appliances can be installed in adjacent locations but the latency between devices should be minimized, enough bandwidth must be available, and no firewall devices should be placed in between the appliances. • Virtual appliances should be deployed as part of the same/local virtual infrastructure instance with low latency and no restrictions on traffic between the cluster nodes.

Table 4: Required Software Versions

Required Software Versions
The software versions compatible with CVP are: • EOS license: Z license • CVP license: Full subscription license **Note:** For updates on compatible EOS switches, supported browsers, and supported TerminAttr versions, refer to the release specific version of the product release notes available at https://www.arista.com/en/support/software-download.

Note: CVP 2020.1.0 and future releases support host-to-host vmotion where the storage is shared between ESXI hosts. Only one host can be in vMotion at a given time.

Related topics:

- Key CVP Terms
- CVP Virtual Appliance

2.4 Key CVP Terms

Make sure you are familiar with the following key CloudVision Portal (CVP) terms. These terms are used throughout this guide to describe the various CVP features, and the CVP user interface contains icons that represent each of the key terms.

Icon	Term	Definition
ARISTA	Device	Devices managed by the CloudVision Portal.
▤	Container	Containers are a logical entity used to group network devices, and define a hierarchy to which user configuration can be applied.
📥	Device	Devices define the subset of available devices.
</>	Configlet	Configlets define a subset of a device's configuration.
💿	Image	Images define the software running on a given device.
🏷	Label	Labels are arbitrary tags defined by the user and applied to devices for identification and filtering purposes.
🔔	Notification	Notifications are system messages providing the list of on-going, completed and canceled activities that are not tracked by tasks.
📋	Task	Tasks are work orders for taking an action against a given device.
N/A	Export to CSV	Downloads the table in csv format to your local drive. 📝 **Note:** Replaces hyphen (-) with **N/A** where hyphen indicates empty data. Replaces cells using the **(unknown)** string with empty cells where **(unknown)** indicates data missing due to an error(s).

Related topics:

- CVP Virtual Appliance
- System Requirements

2.5 CVP Virtual Appliance

The CVP virtual appliance is a packaged ova file that consists of Base OS packages, Hadoop, HBase, Apache Tomcat, JAVA jdk and the CVP web application.

You can deploy the virtual appliance as either a single-node (standalone) cluster or a multi-node cluster (cluster of three nodes). A multi-node cluster provides more benefits over a single-node cluster as specified in the table below.

Table 5: Single-Node and Multi-Node Cluster Comparison

Single-Node Cluster	Multi-Node Cluster
Low Scale • Supports 250 devices and 10k interfaces • Increasing resources may not mandatorily help due to bottlenecks of components	**High Scale** • Scalability is 6x times higher than single-node clusters • Supports multiple containers in components • Loads the share across nodes • Optimization, speed, and availability are higher than single-node clusters
No Redundancy - Does not support telemetry provisioning and streaming when the node goes down	**Redundancy** • Supports 2N+1 redundancy **Note:** If a node goes down, kubernetes schedules the lost node pods on the other two nodes. • Provides uninterrupted telemetry provisioning and streaming • Provides Return Merchandise Authorization (RMA) when a node fails • Each state has three replicas
Corruption Management • No recovery is available for lost data • Need manual intervention to fix hbase issues • Must remotely copy backups to a server everyday for restoring the node when the disk gets corrupted	**Corruption Management** • Automatically fixes issues 99% of the time • The feature to share load across nodes provides a faster and smoother experience

The different deployment options will be discussed later on in this section, but for production deployments it is recommended that the cluster option is chosen. The single VM instance is recommended for testing purposes as it provides a simpler setup and requires less resources.

Chapter 3

CloudVision Portal (CVP) Setup

CloudVision Portal (CVP) can be run on ESX or KVM hypervisors. Before you can begin using the CVP, you must complete the CVP setup process which, involves the following:

1. Deploying CVP
2. Configuring CVP

Sections in this chapter include:

- Deploying CVP OVA on ESX
- Deploying CVP on KVM
- Set Up CV-CUE on CV
- Shell-based Configuration
- Shell Reconfiguration of Single-node, Multi-node Systems
- ISO-based Configuration
- Certificate-Based TerminAttr Authentication

There are two different deployment procedures. One for deploying CVP on ESX, and one for deploying CVP on KVM. After you complete the deployment procedures, you then configure CVP. The deployment procedures are:

- Deploying CVP OVA on ESX
- Deploying CVP on KVM

There are two configuration methods for the CloudVision Portal (CVP): shell-based and ISO-based. Both of these methods eliminate the need to directly modify system and CVP configuration files. This simplifies the setup process and reduces the potential for issues.

The configuration methods enable you to configure CVP in both single-node systems and multi-node systems. The configuration methods are:

- Shell-based Configuration (recommended)
- ISO-based Configuration

Note: Reconfiguration is limited to certain parameters on a deployed CVP multi-node cluster.

3.1 Deploying CVP OVA on ESX

Deploying the CVP OVA file should be the first step in any setup. After the CVP OVA file is deployed, you can choose between the two configuration methods for CloudVision Portal (CVP).

Note: Arista does not support VMware Snapshots on CloudVision virtual machines. For more information, refer to VMware vMotion and Snapshot Support.

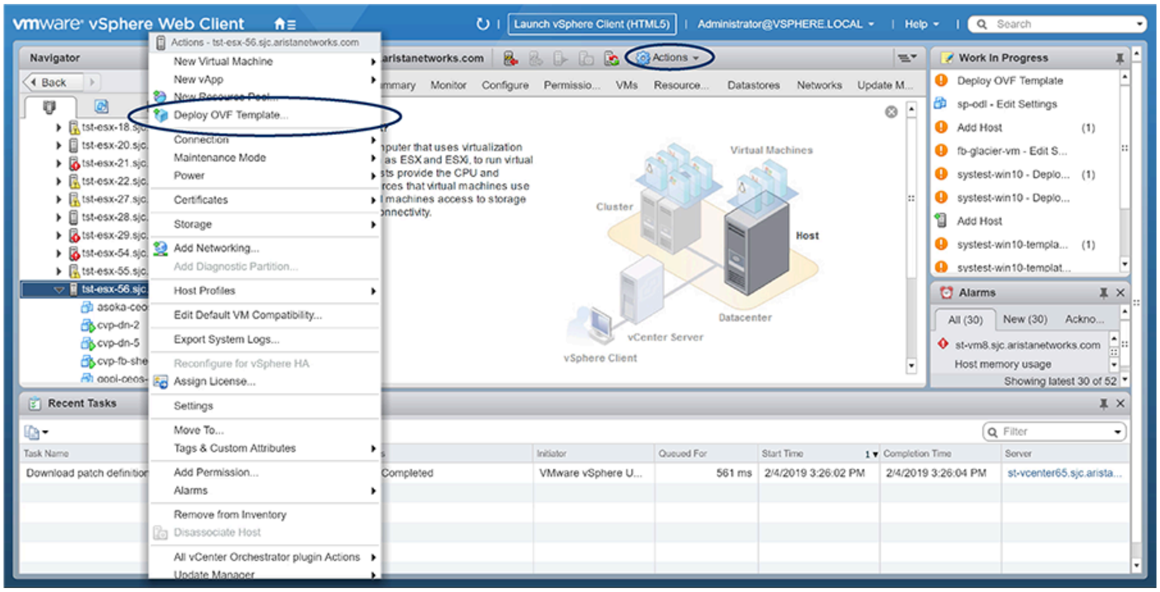
Pre-requisites:

Use of the Deploy OVF Template requires the VMware Client Integration plugin, which is not supported by the Chrome browser after versions 42.

1. The OVA file can be deployed as a VM in a VMware environment by using the drop menu under the Actions heading and selecting **Deploy the OVF template**.

Note: For multi-node setups, the following steps must be completed once for each VM, three times to launch three VMs.

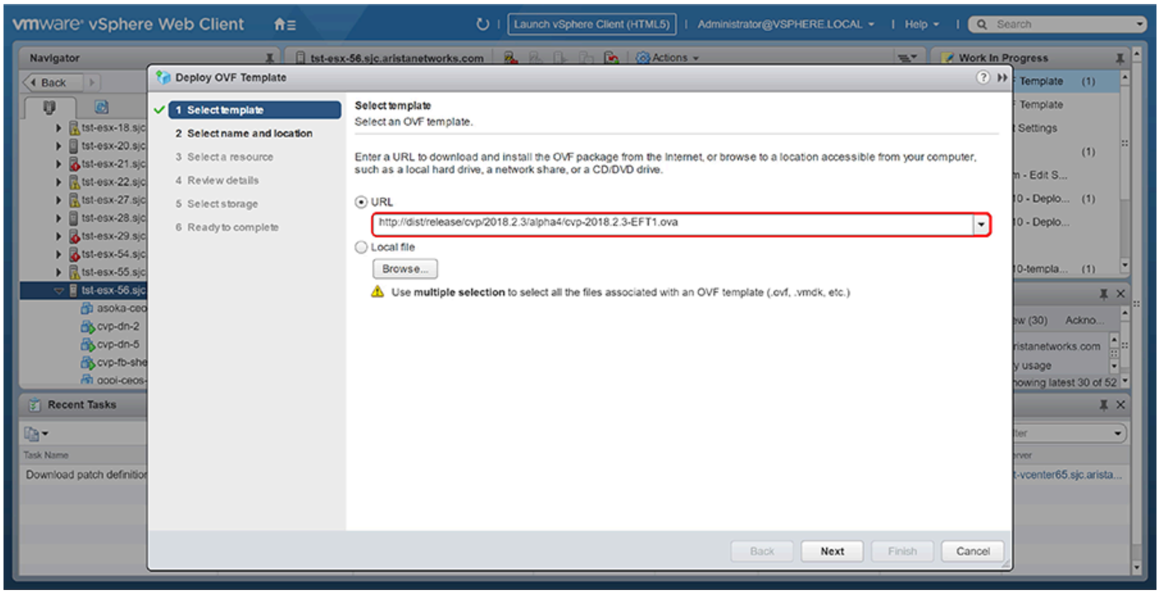
Figure 3-1: Deploy the OVF template



Task Name		Status	Initiator	Queued For	Start Time	Completion Time	Server
Download patch definitior		Completed	VMware vSphere U...	561 ms	2/4/2019 3:26:02 PM	2/4/2019 3:26:04 PM	st-vcenter65.sjc.arista...

2. Having selected the Deploy OVF Template option, VCenter will prompt for the location of the OVA file; this can be either on a local hard disk, network share, or Internet URL. The location of the OVA file should be entered or selected.

Figure 3-2: Location of the OVA file



Select template

Select an OVF template.

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

● URL

http://dist/release/cvp/2018.2.3/alpha4/cvp-2018.2.3-EFT1.ova

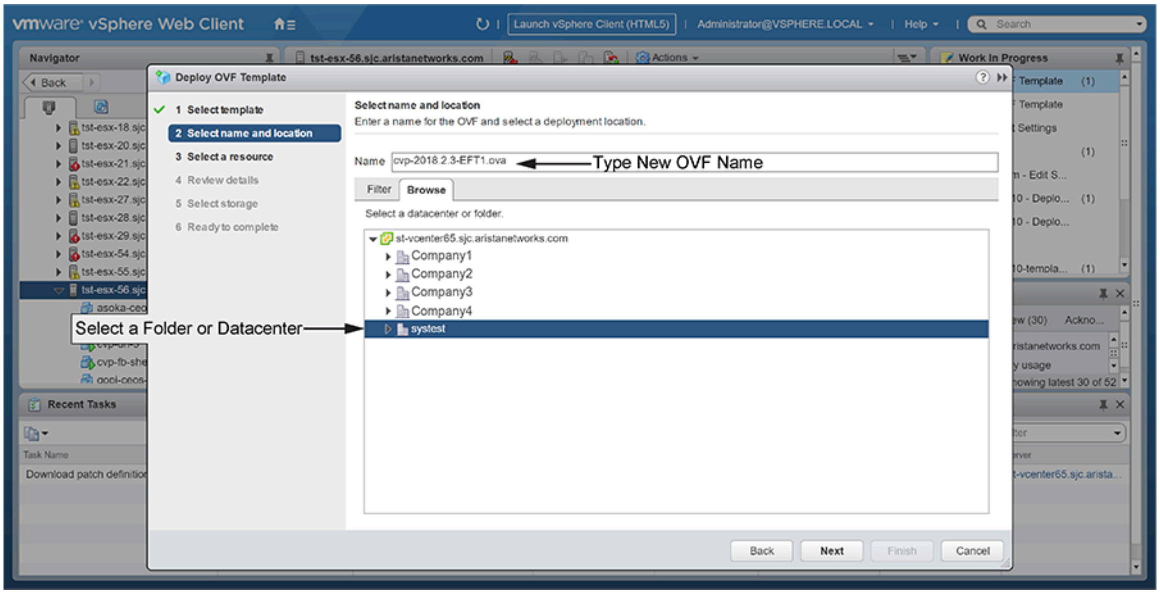
○ Local file

⚠ Use **multiple selection** to select all the files associated with an OVF template (.ovf, .vmdk, etc.)

3. Click **Next** to go to the next task.

4. Type the name for the VM in the **Name** field and select the folder for the OVA file.

Figure 3-3: Select name and folder location for the VM file



Deploy OVF Template

Select name and location

Enter a name for the OVF and select a deployment location.

Name cvp-2018.2.3-EFT1.ova

Select a datacenter or folder.

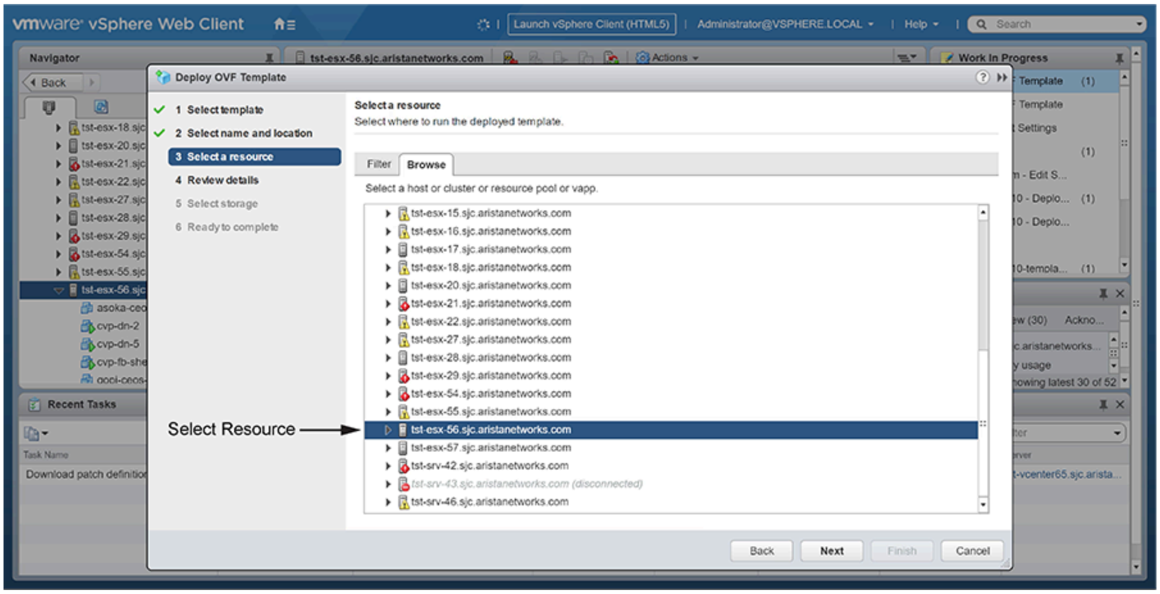
Type New OVF Name

Select a Folder or Datacenter

5. Click **Next** to go to the next task.

6. Select the resource where you want the deployed template (OVA file) to be run.

Figure 3-4: Select the resource



Deploy OVF Template

Select a resource

Select where to run the deployed template.

Select a host or cluster or resource pool or vapp.

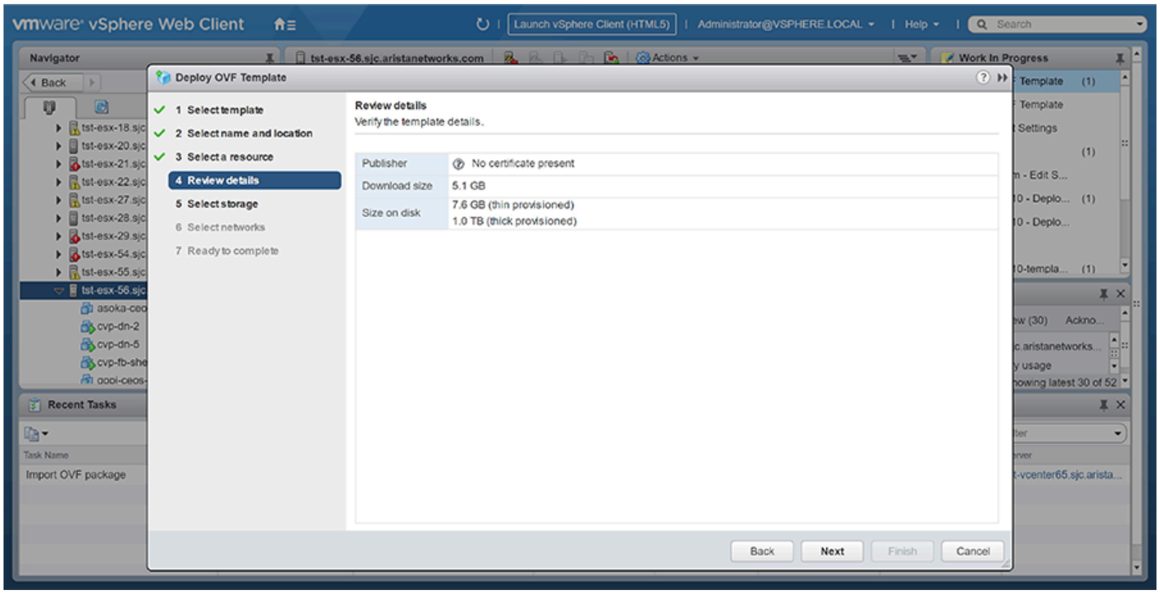
Select Resource

vmware vSphere Web Client
Launch vSphere Client (HTML5)
Administrator@VSPHERE.LOCAL
Help
Search
Navigator
Back
tst-esx-56.sjc.aristanetworks.com
Actions
Work In Progress
1 Select template
2 Select name and location
3 Select a resource
4 Review details
5 Select storage
6 Ready to complete
Filter
Browse
tst-esx-15.sjc.aristanetworks.com
tst-esx-16.sjc.aristanetworks.com
tst-esx-17.sjc.aristanetworks.com
tst-esx-18.sjc.aristanetworks.com
tst-esx-20.sjc.aristanetworks.com
tst-esx-21.sjc.aristanetworks.com
tst-esx-22.sjc.aristanetworks.com
tst-esx-27.sjc.aristanetworks.com
tst-esx-28.sjc.aristanetworks.com
tst-esx-29.sjc.aristanetworks.com
tst-esx-54.sjc.aristanetworks.com
tst-esx-55.sjc.aristanetworks.com
tst-esx-56.sjc.aristanetworks.com
tst-esx-57.sjc.aristanetworks.com
tst-srv-42.sjc.aristanetworks.com
tst-srv-43.sjc.aristanetworks.com (disconnected)
tst-srv-46.sjc.aristanetworks.com
Recent Tasks
Task Name
Download patch definition
Back
Next
Finish
Cancel

7. Click **Next** to go to the next task.

8. Review the OVF template details.

Figure 3-5: Review OVF template details



Deploy OVF Template

- ✓ 1 Select template
- ✓ 2 Select name and location
- ✓ 3 Select a resource
- 4 Review details
- 5 Select storage
- 6 Select networks
- 7 Ready to complete

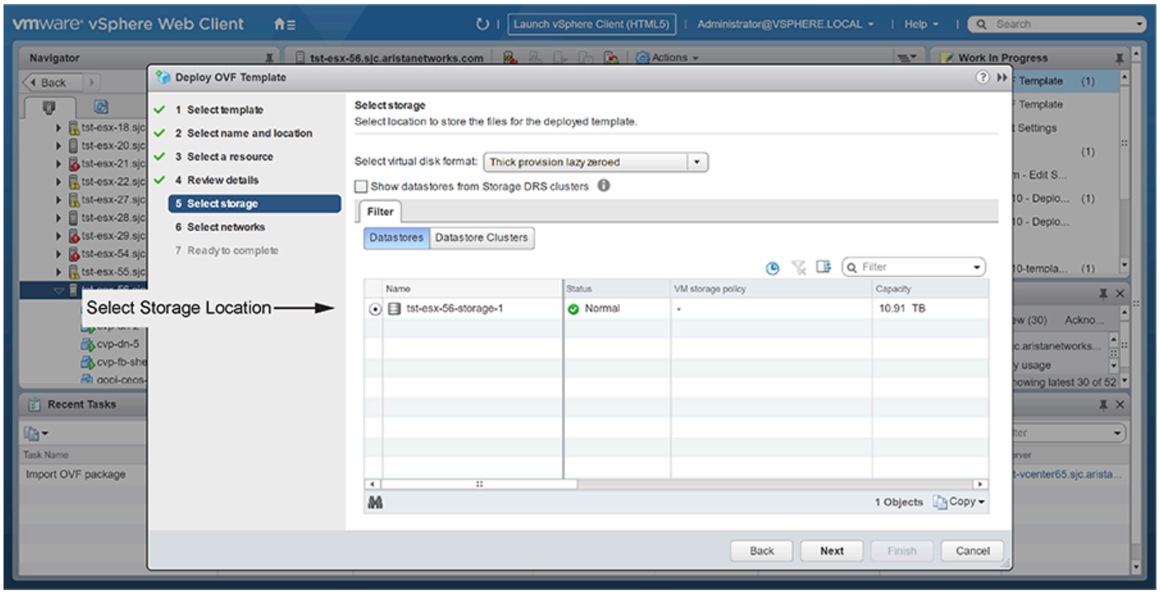
Review details

Verify the template details.

Publisher	No certificate present
Download size	5.1 GB
Size on disk	7.6 GB (thin provisioned) 1.0 TB (thick provisioned)

9. Click **Next** to go to the next task.
10. Select the storage location where you want the files for the deployed template to be stored.

Figure 3-6: Select the destination storage



Deploy OVF Template

- ✓ 1 Select template
- ✓ 2 Select name and location
- ✓ 3 Select a resource
- ✓ 4 Review details
- 5 Select storage
- 6 Select networks
- 7 Ready to complete

Select storage

Select location to store the files for the deployed template.

Select virtual disk format: Thick provision lazy zeroed

□ Show datastores from Storage DRS clusters

	Name	Status	VM storage policy	Capacity
●	tst-esx-56-storage-1	Normal	-	10.91 TB

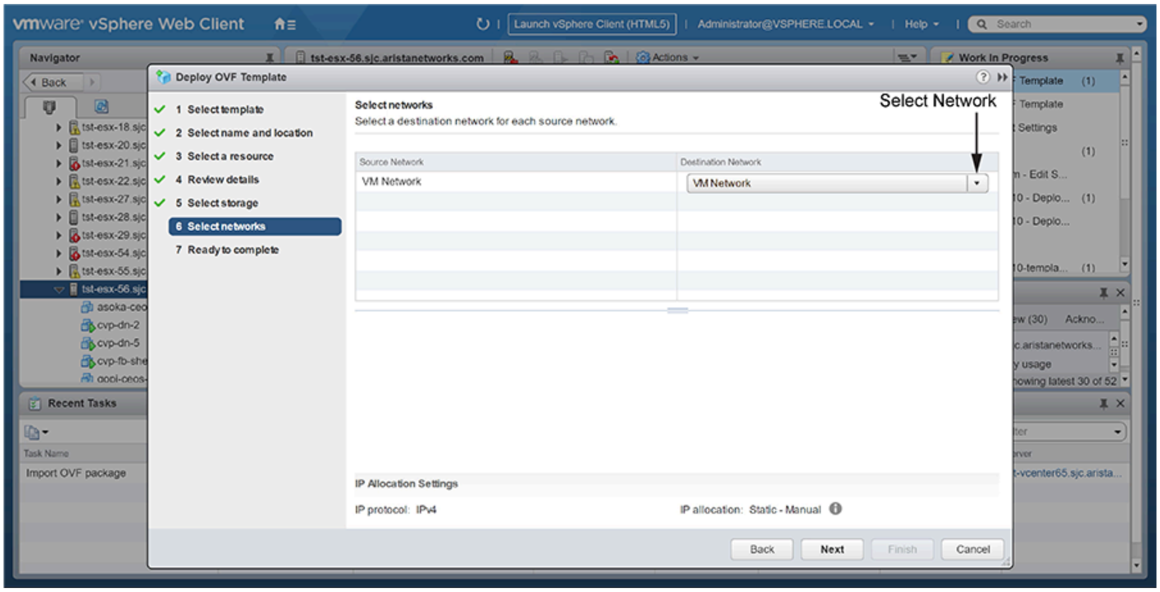
Note:

It is recommended to select **Thick provision lazy zeroed** under the **Select virtual disk format** dropdown menu.

11. Click **Next** to go to the next task.

12. Setup the networks that the deployed template should use.

Figure 3-7: Setup the networks



Deploy OVF Template

1 Select template
2 Select name and location
3 Select a resource
4 Review details
5 Select storage
6 Select networks
7 Ready to complete

Select networks
Select a destination network for each source network.

Source Network	Destination Network
VM Network	VM Network

IP Allocation Settings

IP protocol: IPv4

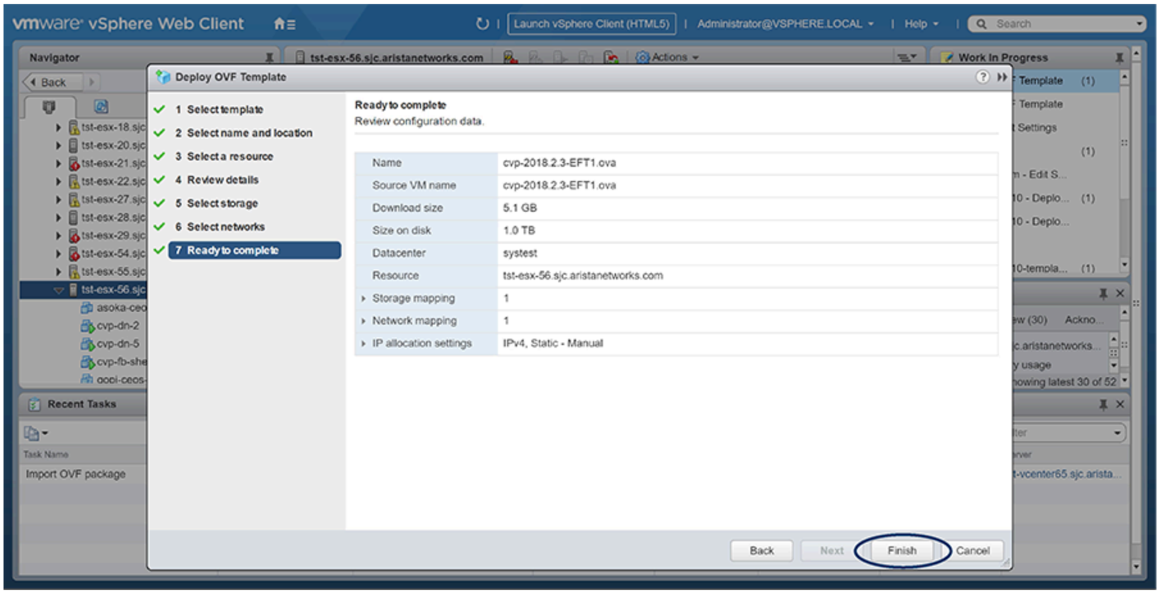
IP allocation: Static - Manual

13. Click **Next**.

VCenter loads the OVA and displays the configuration settings.

14. Review the configuration settings, and click **Finish** to accept and save the configuration.

Figure 3-8: Select the Finish button to accept these settings


vmware vSphere Web Client
Launch vSphere Client (HTML5)
Administrator@VSPHERE.LOCAL
Help
Search
Navigator
Back
tst-esx-56.sjc.aristanetworks.com
Actions
Work In Progress
Recent Tasks
Task Name
Import OVF package
Back
Next
Finish
Cancel

Deploy OVF Template

1 Select template
2 Select name and location
3 Select a resource
4 Review details
5 Select storage
6 Select networks
7 Ready to complete

Ready to complete
Review configuration data.

Name	cvp-2018.2.3-EFT1.ova
Source VM name	cvp-2018.2.3-EFT1.ova
Download size	5.1 GB
Size on disk	1.0 TB
Datacenter	systest
Resource	tst-esx-56.sjc.aristanetworks.com
Storage mapping	1
Network mapping	1
IP allocation settings	IPv4, Static - Manual

VCenter begins to deploy the virtual appliance. Once the appliance is deployed, you can configure the CVP application using either Shell-based Configuration or ISO-based Configuration.

3.1.1 VMware vMotion and Snapshot Support

CloudVision includes the following infrastructure components that are used as the basis for the application services and database. This is not an exhaustive list, but the key components as it relates to this topic.

- Hadoop - open source framework from Apache that is used to store and process large datasets distributed across a cluster of servers
- Hbase - open source database from Apache that runs on Hadoop cluster
- Zookeeper - centralized service for maintaining configuration information, naming, providing distributed synchronization, and providing group services

The CloudVision database (hbase/hadoop) is deployed across the three nodes within the CloudVision cluster. The integrity of this database is critical to the correct functioning of CloudVision, and thus, there are specific requirements on the hypervisor and storage for these virtual machines forming these nodes.

VMware Snapshots

Within the CloudVision infrastructure, data is constantly being written to Apache hadoop by all nodes. Disk snapshots used by VMware have no hooks into the hbase quiesce states, meaning a snapshot of a disk state would almost always be inconsistent and lead to database corruption during a restore process. This results in a snapshot having no meaningful use as a restore point due to the nature of the database, which is typical for database application performance using VMware Snapshots (VMware reference).

VMware Snapshots are very I/O intensive, leaving almost no I/O for the virtual machines during the snapshot process. Impact on resources, such as disk, can lead to hbase and zookeeper failures. These symptoms are evident in multiple cases where the support team has identified snapshots that were in progress before failures.

VMware does not recommend using VM Snapshots as backups (https://kb.vmware.com/s/article/1025279), therefore other backup mechanisms are recommended by Arista as outlined below.

Note: For these reasons, Arista does not support VMware Snapshots on CloudVision virtual machines.

VMware vMotion

CloudVision supports VMware vMotion under specific configuration and operational criteria as follows:

- The virtual machine disks are shared between the source and target ESXi host
- Latency between ESXi hosts is less than 5ms
- Only one CloudVision node may be vMotioned at a time

Note: CVP 2020.1.0 and future releases support host-to-host vmotion where the storage is shared between ESXI hosts. Only one host can be in vMotion at a given time.

Backup Solutions for CloudVision

Daily backups of the CloudVision provisioning data are automatically scheduled to be taken at 2AM UTC. This backup file is stored locally on the CloudVision cluster. Common practice by customers is to schedule a copy of this backup file from the CloudVision cluster to some external data store.

There is an example script to help automate the copying of the backup file available on the Arista Github site (link).

CloudVision telemetry data received from switches is replicated between the CloudVision clusters. In the event a single node becomes unavailable and a new node is added to the cluster, this telemetry data is replicated to the new node.

Arista EOS with the Streaming Telemetry agent (TerminAttr v1.7.1 and later) supports establishing connections to multiple CloudVision clusters. This enables the user to send the telemetry data to a backup CloudVision instance, to maintain an up-to-date redundant store.

There is a detailed explanation of this deployment model available on the Arista EOS Central site (https://arista.my.site.com/AristaCommunity/s/article/cvp-ha-deployment-guide), which would assist with the design and deployment of this HA solution.

3.2 Deploying CVP on KVM

In standard KVM environments, deploying a CVP VM involves the following tasks:

- Downloading and extracting the CVP KVM tarball (.tgz archive)
- Creating Virtual Bridge and Network Interface Cards (NIC)
- Generating the XML file that defines the CVP VM
- Defining and Launching the CVP VM

Once you complete these tasks, you can configure the CVP VM.

3.2.1 Downloading and extracting the CVP KVM tarball (.tgz archive)

The first task in the deployment process involves downloading and extracting the CVP KVM tarball. The tarball is a .tgz archive that contains:

- The CVP VM
- Disk images for the CVP application
- The files used to configure CVP VM.

You download the tarball to the host server that is configured for KVM. The files contained in the .tgz archive include:

	Filename	**Description**
1	disk1.qcow2	VM disk image for the CVP application.
2	disk2.qcow2	Data disk image for the CVP application.
3	cvpTemplate.xml	A template for creating the XML file for libvirt domain specification.
4	generateXmlForKvm.py	A script for generating the CVP VM definition XML based on the XML template.
5	createNwBridges.py	A script for creating the network interfaces for the CVP VM.

Complete the following steps to download and extract the CVP VM .tgz archive:

1. Go to the Arista software downloads webpage and download the CVP VM tarball (`cvp-<version>-kvm.tgz`) to the host server set up for KVM.
2. Extract the tarball (`cvp-<version>-kvm.tgz`).

   The following example shows extracting the `CVP KVM .tgz` archive.

```
[arastra@kvm1 vms]# cd cvpTests
[arastra@kvm1 cvpTests]# ls
cvp-2022.3.0-kvm.tar
[arastra@kvm1 cvpTests]#tar -xvf cvp-2022.3.0-kvm.tar
addIsoToVM.py
createNwBridges.py
cvpTemplate.xml
disk1.qcow2
disk2.qcow2
generateXmlForKvm.py
```

3.2.2 Creating Virtual Bridge and Network Interface Cards (NIC)

The second task in deploying CVP for KVM involves creating the bridges and interfaces that provide network connectivity for the CVP VM. You use the `CreateNwBridges.py` script you extracted in the previous task to create the required bridges and interfaces.

Note: If the required network interfaces for CVP already exist, you do not have to complete this task. Go directly to Generating the XML file that defines the CVP VM

You have the option of deploying CVP with either two bridge interfaces or a single bridge interface.

- Two interfaces (the cluster bridge interface and the device bridge interface).
- Single interface (the device bridge interface).

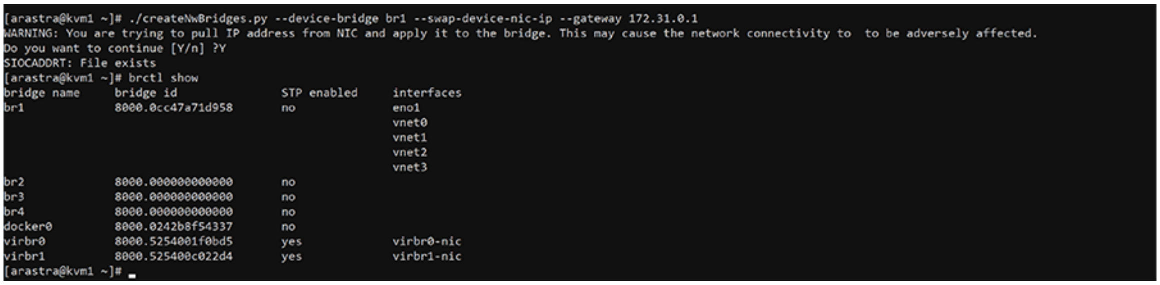
Complete the following steps to create the network interfaces for CVP KVM connectivity:

1. (Optional) Use the `./createNwBridges.py -help` command to view a list of all the parameters available in the script.

   Note: Install the net-tools library using the `yum -y install net-tools` command before running the script.
2. Use the `./createNwBridges.py` to create the device bridge (or bridges) and interfaces needed.

   The figure below shows an example of creating a single device bridge for a single-node deployment.

   Figure 3-9: Creating a device bridge (single node deployment)



```
[arastra@kvm1 ~]# ./createNwBridges.py --device-bridge br1 --swap-device-nic-ip --gateway 172.31.0.1
WARNING: You are trying to pull IP address from NIC and apply it to the bridge. This may cause the network connectivity to  to be adversely affected.
Do you want to continue [Y/n] ?Y
SIOCADDRT: File exists
[arastra@kvm1 ~]# brctl show
bridge name     bridge id               STP enabled     interfaces
br1             8000.0cc47a71d958       no              eno1
                                                        vnet0
                                                        vnet1
                                                        vnet2
                                                        vnet3
br2             8000.000000000000       no
br3             8000.000000000000       no
br4             8000.000000000000       no
docker0         8000.0242b8f54337       no
virbr0          8000.5254001f0bd5       yes             virbr0-nic
virbr1          8000.525400c022d4       yes             virbr1-nic
[arastra@kvm1 ~]# _
```

3. (Optional) Use the `brctl show` command to verify that the bridges were successfully created.
4. (Optional) Use the `ip address show` command to verify that the IP addresses have been allocated. In this example the one IP address for the br1 bridge.

   The following output is an example of verifying bridge creation and IP address allocation. In this example, a bridge br1 was created, and one IP address has been allocated for the bridge.

```
[arastra@kvm1 ~]# ip address show br1
6: br1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
 group default qlen 1000
    link/ether d0:94:66:4f:56:48 brd ff:ff:ff:ff:ff:ff
    inet 172.31.6.78/16 brd 172.31.255.255 scope global br1
       valid_lft forever preferred_lft forever
    inet6 fe80::d294:66ff:fe4f:5648/64 scope link
       valid_lft forever preferred_lft forever
[arastra@kvm1 ~]# ip route show
default via 172.31.0.1 dev br1
172.31.0.0/16 dev br1 proto kernel scope link src 172.31.0.1
[arastra@kvm1 ~]#
```

3.2.3 Generating the XML file that defines the CVP VM

The third task in deploying CVP for KVM involves generating the XML file that you use to define the CVP VM. You use generateXmlForKvm.py script and the cvpTemplate.xml file you extracted previously to generate the XML file you use to define the CVP VM.

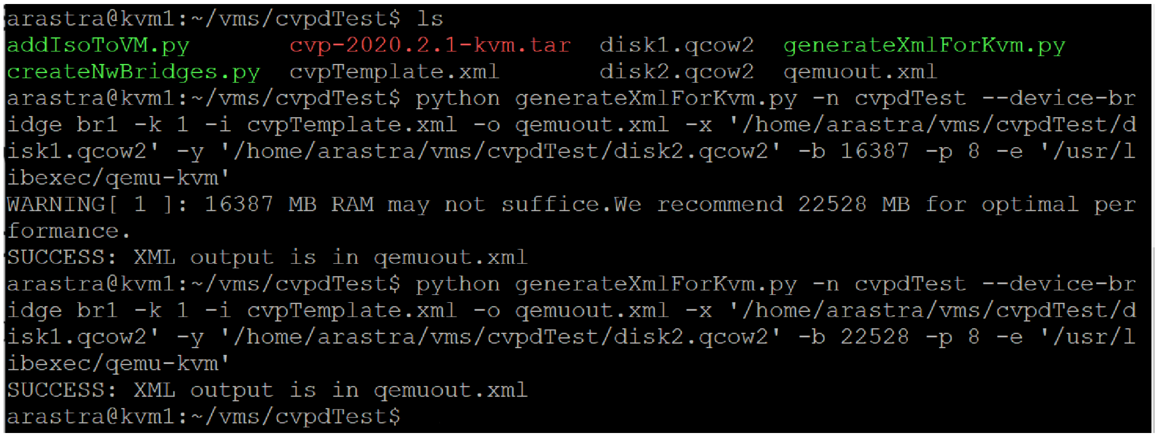
The `cvpTemplate.xml` file is a template that defines wildcard values that are filled by the other parameters that are specified when you execute the script.

Complete the following steps to generate the XML file:

1. (Optional) Use the `python generateXmlForKvm.py -help` command to view a list of all the parameters available in the script.
2. Run the `python generateXmlForKvm.py` script using the XML template (`cvpTemplate.xml`) as one of the inputs.

   Generation of XML file used to define CVP VM shows an example of an XML being generated that can be used to define a CVP VM named cvpTest. The generated XML file is named qemuout.xml.

   Figure 3-10: Generation of XML file used to define CVP VM



```
arastra@kvm1:~/vms/cvpdTest$ ls
addIsoToVM.py       cvp-2020.2.1-kvm.tar   disk1.qcow2  generateXmlForKvm.py
createNwBridges.py  cvpTemplate.xml        disk2.qcow2  qemuout.xml
arastra@kvm1:~/vms/cvpdTest$ python generateXmlForKvm.py -n cvpdTest --device-br
idge br1 -k 1 -i cvpTemplate.xml -o qemuout.xml -x '/home/arastra/vms/cvpdTest/d
isk1.qcow2' -y '/home/arastra/vms/cvpdTest/disk2.qcow2' -b 16387 -p 8 -e '/usr/l
ibexec/qemu-kvm'
WARNING[ 1 ]: 16387 MB RAM may not suffice.We recommend 22528 MB for optimal per
formance.
SUCCESS: XML output is in qemuout.xml
arastra@kvm1:~/vms/cvpdTest$ python generateXmlForKvm.py -n cvpdTest --device-br
idge br1 -k 1 -i cvpTemplate.xml -o qemuout.xml -x '/home/arastra/vms/cvpdTest/d
isk1.qcow2' -y '/home/arastra/vms/cvpdTest/disk2.qcow2' -b 22528 -p 8 -e '/usr/l
ibexec/qemu-kvm'
SUCCESS: XML output is in qemuout.xml
arastra@kvm1:~/vms/cvpdTest$
```

3.2.4 Defining and Launching the CVP VM

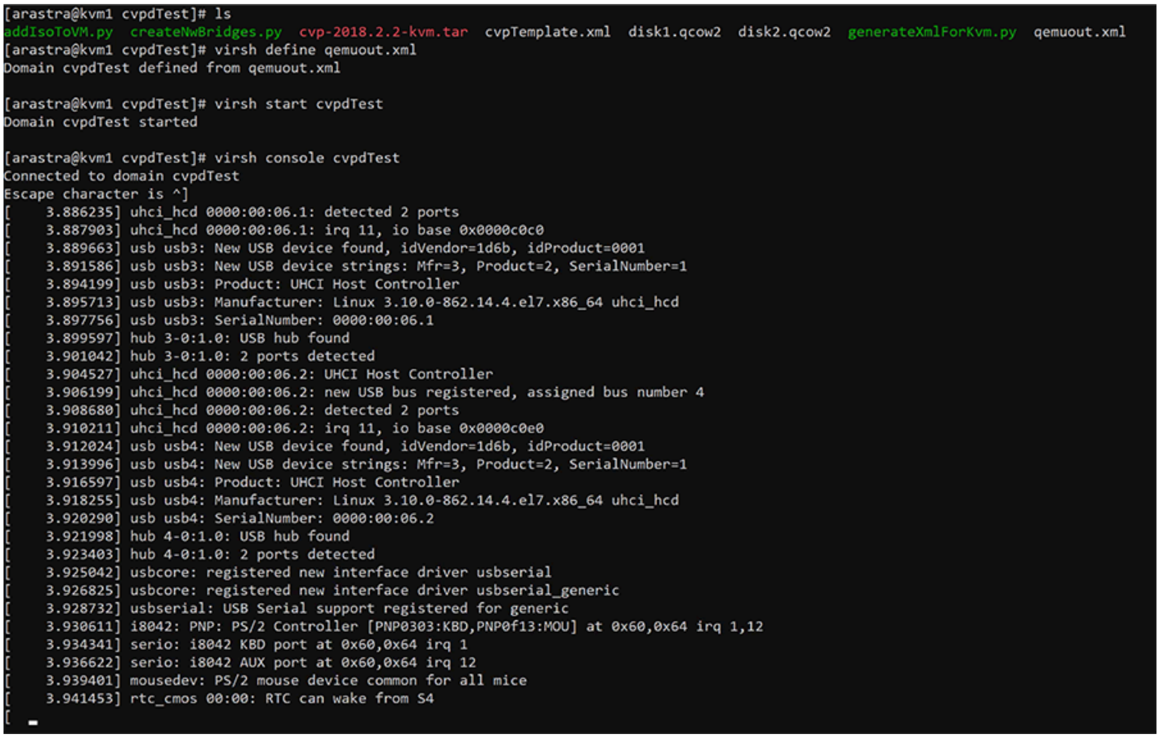
The last task in deploying CVP for KVM is to define and launch the CVP VM. You use the XML file you generated in the previous task to define the CVP VM.

Complete the following steps to define and launch the CVP VM:

1. Run the `virsh define` command to define the CVP VM (specify the generated XML file).
2. Run the `virsh start` command to launch the newly defined CVP VM.
3. Run the `virsh console` command to attach (connect) to the CVP VM console.

Defining and Launching the CVP VM shows an example of the use of the commands to define and launch a CVP VM named cvpTest. The XML file used to define the CVP VM is named qemuout.xml.

Figure 3-11: Defining and Launching the CVP VM



```
[arastra@kvm1 cvpdTest]# ls
addIsoToVM.py  createNwBridges.py  cvp-2018.2.2-kvm.tar  cvpTemplate.xml  disk1.qcow2  disk2.qcow2  generateXmlForKvm.py  qemuout.xml
[arastra@kvm1 cvpdTest]# virsh define qemuout.xml
Domain cvpdTest defined from qemuout.xml

[arastra@kvm1 cvpdTest]# virsh start cvpdTest
Domain cvpdTest started

[arastra@kvm1 cvpdTest]# virsh console cvpdTest
Connected to domain cvpdTest
Escape character is ^]
[    3.886235] uhci_hcd 0000:00:06.1: detected 2 ports
[    3.887903] uhci_hcd 0000:00:06.1: irq 11, io base 0x0000c0c0
[    3.889663] usb usb3: New USB device found, idVendor=1d6b, idProduct=0001
[    3.891586] usb usb3: New USB device strings: Mfr=3, Product=2, SerialNumber=1
[    3.894199] usb usb3: Product: UHCI Host Controller
[    3.895713] usb usb3: Manufacturer: Linux 3.10.0-862.14.4.el7.x86_64 uhci_hcd
[    3.897756] usb usb3: SerialNumber: 0000:00:06.1
[    3.899597] hub 3-0:1.0: USB hub found
[    3.901042] hub 3-0:1.0: 2 ports detected
[    3.904527] uhci_hcd 0000:00:06.2: UHCI Host Controller
[    3.906199] uhci_hcd 0000:00:06.2: new USB bus registered, assigned bus number 4
[    3.908680] uhci_hcd 0000:00:06.2: detected 2 ports
[    3.910211] uhci_hcd 0000:00:06.2: irq 11, io base 0x0000c0e0
[    3.912024] usb usb4: New USB device found, idVendor=1d6b, idProduct=0001
[    3.913996] usb usb4: New USB device strings: Mfr=3, Product=2, SerialNumber=1
[    3.916597] usb usb4: Product: UHCI Host Controller
[    3.918255] usb usb4: Manufacturer: Linux 3.10.0-862.14.4.el7.x86_64 uhci_hcd
[    3.920290] usb usb4: SerialNumber: 0000:00:06.2
[    3.921998] hub 4-0:1.0: USB hub found
[    3.923403] hub 4-0:1.0: 2 ports detected
[    3.925042] usbcore: registered new interface driver usbserial
[    3.926825] usbcore: registered new interface driver usbserial_generic
[    3.928732] usbserial: USB Serial support registered for generic
[    3.930611] i8042: PNP: PS/2 Controller [PNP0303:KBD,PNP0f13:MOU] at 0x60,0x64 irq 1,12
[    3.934341] serio: i8042 KBD port at 0x60,0x64 irq 1
[    3.936622] serio: i8042 AUX port at 0x60,0x64 irq 12
[    3.939401] mousedev: PS/2 mouse device common for all mice
[    3.941453] rtc_cmos 00:00: RTC can wake from S4
[  _
```

You can now login as cvpadmin and complete the configuration of the CVP application. See Configuring a Single-Node CVP Instance using CVP Shell for the steps used to complete the configuration.

Related topics:

- Shell-based Configuration
- ISO-based Configuration
- Deploying CVP OVA on ESX

3.3 Set Up CV-CUE on CV

This section describes the process to:

- Setup CV-CUE on a Standalone CV
- Set Up CV-CUE on a CV Cluster

3.3.1 Setup CV-CUE on a Standalone CV

CV-CUE is disabled by default.

To enable CV-CUE, perform the following steps:

1. Log in to the CV admin shell via the cvpadmin user.
2. Enter **e** to edit the settings. The CV configuration wizard is launched.

Note: If you are setting up CV for the first time, you need to enter the values for all the settings (DNS, IP addresses, etc.) in the configuration wizard. Refer to the Shell-based Configuration for information on these settings. If you have already set up or just upgraded CV, and you only want to enable CV-CUE, go to Step 3.

3. Set the **CV-CUE Enabled** option to **Yes**.
4. Once the cursor is at the bottom of the configuration wizard, enter a to apply the configuration changes.

3.3.2 Set Up CV-CUE on a CV Cluster

A few important points about the CV-CUE service in a cluster deployment:

- CV-CUE is disabled by default.
- For a CV cluster, you first need to Enable CV-CUE on Primary Node and then Set Up CV-CUE on Secondary and Tertiary Nodes .

  Note: The CV-CUE service runs only on the primary and secondary nodes, but you need to apply the configuration changes to all the nodes, including the tertiary node. The CV-CUE service starts on both nodes only after the setup on all the nodes (including the tertiary node) of the cluster has been completed.
- The CV configuration wizard consists of two parts (Enable CV-CUE on Primary Node):
  - **common configuration**: Settings common to all the nodes in the cluster (For example, DNS and services such as CV-CUE).
  - **node configuration**: Settings specific to a node (For example, Hostname and IP settings).

3.3.2.1 Enable CV-CUE on Primary Node

To enable CV-CUE on the primary node, perform the following steps:

1. Log in to the CV admin shell via the **cvpadmin** user.
2. Enter **e** to edit the settings. The CV configuration wizard is launched.

   Note: If you are setting up CV for the first time, you need to enter the values for all the settings (those belonging to the common configuration as well as the node configuration). Refer to Shell-based Configuration and Shell Reconfiguration of Single-node, Multi-node Systems for information on these settings. If you have already set up or just upgraded CV, and you only want to enable CV-CUE, go to Step 3.
3. You can optionally assign a **CV-CUE HA Cluster IP**.

   Note: CV-CUE in HA mode configures an optional IP address, known as HA cluster IP that is automatically assigned to the active node in a cluster. Ensure that the HA Cluster IP address is different from the IP addresses of the actual device and cluster interfaces; but belongs to the same subnet as the Device Interface IP addresses of primary and secondary nodes. If HA cluster IP is not configured, IP addresses of both primary and secondary nodes must be configured on access points.
4. Set the **CV-CUE Enabled** option to **Yes**.

3.3.2.2 Set Up CV-CUE on Secondary and Tertiary Nodes

To set up CV-CUE on the secondary and tertiary nodes, perform the following steps on the respective nodes:

1. Log in to the CV admin shell via the **cvpadmin** user.
2. Enter **e** to edit the settings. The CV configuration wizard is launched.

   Note: The **Shell-based Configuration** settings are not editable on the secondary and tertiary nodes. If you are setting up CV for the first time, you need to enter the values for all the Shell Reconfiguration of Single-node, Multi-node Systems settings. If you have already set up or just upgraded CV, and you only want to enable CV-CUE, go to Step 3.
3. Press **Enter** until the cursor reaches the bottom of the configuration wizard, past all the settings.
4. Once the cursor is at the bottom of the configuration wizard, enter **a** to apply the configuration changes.

Note: Whether **CV-CUE Enabled** is set to **Yes** or **No**, applying the configuration changes causes the secondary and tertiary nodes to update their settings based on the primary node. This will start the CV-CUE service on the primary and secondary nodes.

3.4 Shell-based Configuration

The shell-based configuration can be used to set up either a single-node CVP instance or multi-node CVP instances. The steps you use vary depending on whether you are setting up a single-node instance or a multi-node instance.

Cluster and device interfaces

A cluster interface is the interface that is able to reach the other two nodes in a multi-node installation. A device interface is the interface used by managed devices to connect to CVP. The ZTP configuration file is served over this interface. These two parameters are optional and default to eth0. Configuring these two interfaces is useful in deployments where a private network is used between the managed devices and a public-facing network is used to reach the other two cluster nodes and the GUI.

- Configuring a Single-Node CVP Instance using CVP Shell
- Configuring Multi-node CVP Instances Using the CVP Shell

3.4.1 Configuring a Single-Node CVP Instance using CVP Shell

After initial bootup, CVP can be configured at the VM's console using the CVP config shell. At points during the configuration, you must start the network, NTPD, and CVP services. Starting these services may take some time to complete before moving on to the next step in the process.

Pre-requisites:

Before you begin the configuration process, make sure that you:

- Launch the VM (see Deploying CVP OVA on ESX , or Deploying CVP on KVM.)

To configure CVP using the CVP config shell:

1. Login at the VM console as **cvpadmin**.
2. Enter your configuration and apply it (see the following example).

   In this example, the root password is not set (it is not set by default). In this example of a CVP shell, the bold text is entered by the **cvpadmin** user.

   Accept the default or choose a custom **internal cluster network**, for the internal kubernetes clustering.

   Note: To skip NAT and static routes, simply press **Enter** when prompted.

```
localhost login: cvpadmin
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
CVP Installation Menu

[q]uit [p]rint [s]inglenode [m]ultinode [r]eplace [u]pgrade
>s
Enter the configuration for CloudVision Portal and apply it when done.
Entries marked with '*' are required.


Common Configuration:

 CloudVision Deployment Model [d]efault [w]ifi_analytics: d
```

```
  DNS Server Addresses (IPv4 Only): 172.22.22.40

  DNS Domain Search List: sjc.aristanetworks.com, ire.aristanetworks.com
  Number of NTP Servers: 1
  NTP Server Address (IPv4 or FQDN) #1: ntp.aristanetworks.com
  Is Auth enabled for NTP Server #1: no
  Cluster Interface Name: eth0
  Device Interface Name: eth0
    CloudVision WiFi Enabled: no


 *Enter a private IP range for the internal cluster network (overlay):
 10.42.0.0/16
 *FIPS mode: no
Node Configuration:
─────────────────────────────────────────────
 *Hostname (FQDN): cvp80.sjc.aristanetworks.com
 *IP Address of eth0: 172.31.0.168
 *Netmask of eth0: 255.255.0.0
  NAT IP Address of eth0:
 *Default Gateway: 172.31.0.1  Number of Static Routes: 1
 Route for Static Route #1: 1.1.1.0
 TACACS Server IP Address:

 Singlenode Configuration Menu
────────────────────────────────────────────
[q]uit [p]rint [e]dit [v]erify [s]ave [a]pply [h]elp ve[r]bose
>v
Valid config format.
Applying proposed config for network verification.
saved config to /cvpi/cvp-config.yaml
Running : cvpConfig.py tool...
[  189.568543] vmxnet3 0000:0b:00.0 eth0: intr type 3, mode 0, 9 vectors
 allocated
[  189.576571] vmxnet3 0000:0b:00.0 eth0: NIC Link is Up 10000 Mbps
[  203.860624] vmxnet3 0000:13:00.0 eth1: intr type 3, mode 0, 9 vectors
 allocated
[  203.863878] vmxnet3 0000:13:00.0 eth1: NIC Link is Up 10000 Mbps
[  204.865253] Ebtables v2.0 unregistered
[  205.312888] ip_tables: (C) 2000-2006 Netfilter Core Team
[  205.331703] ip6_tables: (C) 2000-2006 Netfilter Core Team
[  205.355522] Ebtables v2.0 registered
[  205.398575] nf_conntrack version 0.5.0 (65536 buckets, 262144 max)
Stopping: network
Running : /bin/sudo /sbin/service network stop
Running : /bin/sudo /bin/systemctl is-active network
Starting: network
Running : /bin/sudo /bin/systemctl start network.service
[  206.856170] vmxnet3 0000:0b:00.0 eth0: intr type 3, mode 0, 9 vectors
 allocated
[  206.858797] vmxnet3 0000:0b:00.0 eth0: NIC Link is Up 10000 Mbps
[  206.860627] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[  207.096883] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
[  211.086390] vmxnet3 0000:13:00.0 eth1: intr type 3, mode 0, 9 vectors
 allocated
[  211.089157] vmxnet3 0000:13:00.0 eth1: NIC Link is Up 10000 Mbps
[  211.091084] IPv6: ADDRCONF(NETDEV_UP): eth1: link is not ready
[  211.092424] IPv6: ADDRCONF(NETDEV_CHANGE): eth1: link becomes ready
[  211.245437] warning: `/bin/ping' has both setuid-root and effective
 capabilities. Therefore not raising all capabilities.
Warning: External interfaces, ['eth1'], are discovered under /etc/sysconfig/
network-scripts
These interfaces are not managed by CVP.
Please ensure that the configurations for these interfaces are correct.
```

```
Otherwise, actions from the CVP shell may fail.

Valid config.
[q]uit [p]rint [e]dit [v]erify [s]ave [a]pply [h]elp ve[r]bose
```

Validating the Configuration

```
>v
Valid config format.
Applying proposed config for network verification.
saved config to /cvpi/cvp-config.yaml
Running : cvpConfig.py tool...
Stopping: network
Running : /bin/sudo /bin/systemctl stop network
Running : /bin/sudo /bin/systemctl is-active network
Running : /bin/sudo /bin/systemctl is-active network
Starting: network
Running : /bin/sudo /bin/systemctl start network
Warning: External interfaces, ['eth1'], are discovered under /etc/sysconfig/
network-scripts
These interfaces are not managed by CVP.
Please ensure that the configurations for these interfaces are correct.
Otherwise, actions from the CVP shell may fail.

Valid config.
```

Applying the Configuration

```
>a
Valid config format.
saved config to /cvpi/cvp-config.yaml
Applying proposed config for network verification.
saved config to /cvpi/cvp-config.yaml
Running : cvpConfig.py tool...
Stopping: network
Running : /bin/sudo /bin/systemctl stop network
Running : /bin/sudo /bin/systemctl is-active network
Running : /bin/sudo /bin/systemctl is-active network
Starting: network
Running : /bin/sudo /bin/systemctl start network
Warning: External interfaces, ['eth1'], are discovered under /etc/sysconfig/
network-scripts
These interfaces are not managed by CVP.
Please ensure that the configurations for these interfaces are correct.
Otherwise, actions from the CVP shell may fail.

Valid config.
Running : cvpConfig.py tool...
Stopping: network
Running : /bin/sudo /bin/systemctl stop network
Running : /bin/sudo /bin/systemctl is-active network
Running : /bin/sudo /bin/systemctl is-active network
Starting: network
Running : /bin/sudo /bin/systemctl start network
Running : /bin/sudo /bin/systemctl is-active etcd
Internal error, unknown service 'etcd'
Running :  /bin/sudo /bin/systemctl stop kube-cluster.path on 172.30.41.190
Running :  /bin/sudo /bin/systemctl stop kube-cluster.service on
 172.30.41.190
Checking if interface flannelbr0 is present
```

```
Run cmd: sudo -u cvp -- ssh 172.30.41.190 /usr/sbin/ip link show flannelbr0
 0.18
Checking if interface flannel.1 is present
Run cmd: sudo -u cvp -- ssh 172.30.41.190 /usr/sbin/ip link show flannel.1
 0.17
Running : /bin/sudo /bin/systemctl is-active zookeeper
Starting: systemd services
Running : cvpConfig.py tool...
Stopping: cvpi
Running : /bin/sudo /bin/systemctl stop cvpi
Running : /bin/sudo /bin/systemctl is-active cvpi
Running : /bin/sudo /bin/systemctl is-active cvpi
Stopping: cvpi-config
Running : /bin/sudo /bin/systemctl stop cvpi-config
Running : /bin/sudo /bin/systemctl is-active cvpi-config
Running : /bin/sudo /bin/systemctl is-active cvpi-config
Stopping: zookeeper
Running : /bin/sudo /bin/systemctl stop zookeeper
Running : /bin/sudo /bin/systemctl is-active zookeeper
Running : /bin/sudo /bin/systemctl is-active zookeeper
Stopping: cvpi-check
Running : /bin/sudo /bin/systemctl stop cvpi-check
Running : /bin/sudo /bin/systemctl is-active cvpi-check
Running : /bin/sudo /bin/systemctl is-active cvpi-check
Stopping: ntpd
Running : /bin/sudo /bin/systemctl stop ntpd
Running : /bin/sudo /bin/systemctl is-active ntpd
Running : /bin/sudo /bin/systemctl is-active ntpd
Starting: ntpd
Running : /bin/sudo /bin/systemctl start ntpd
Starting: cvpi-check
Running : /bin/sudo /bin/systemctl start cvpi-check
Starting: zookeeper
Running : /bin/sudo /bin/systemctl start zookeeper
Starting: cvpi-config
Running : /bin/sudo /bin/systemctl start cvpi-config
Starting: cvpi
Running : /bin/sudo /bin/systemctl start cvpi
Running : /bin/sudo /bin/systemctl start cvpi-watchdog.timer
Running : /bin/sudo /bin/systemctl enable cert-rotate.timer
Running : /bin/sudo /bin/systemctl start cert-rotate.timer
Running : /bin/sudo /bin/systemctl enable ambassador-cert-rotate.timer
Running : /bin/sudo /bin/systemctl start ambassador-cert-rotate.timer
Running : /bin/sudo /bin/systemctl enable ssl-cert-expiry.timer
Running : /bin/sudo /bin/systemctl start ssl-cert-expiry.timer
Running : /bin/sudo /bin/systemctl enable docker containerd
Running : /bin/sudo /bin/systemctl start docker containerd
Running :  /bin/sudo /bin/systemctl enable kube-cluster.path on
 172.30.41.190
Running :  /bin/sudo /bin/systemctl start kube-cluster.path on 172.30.41.190
Waiting for all components to start. This may take few minutes.
Still waiting for flannel coredns descheduler fluent-bit mutating-webhook-
server mutating-webhook clickhouse namenode datanode nfs3 ... (total 217)
Still waiting for clickhouse hbasemaster regionserver hbase kafka dispatcher
 apiserver nginx-init-V1 nginx-app apiserver-www ... (total 203)
Still waiting for dispatcher apiserver nginx-init-V1 nginx-app apiserver-www
 local-provider radius-provider tacacs-provider aaa disk-usage-monitor ...
 (total 198)
Still waiting for nginx-app apiserver-www local-provider radius-provid
er tacacs-provider aaa disk-usage-monitor ingest elasticsearch-server
 elasticsearch-exporter ... (total 195)
Still waiting for nginx-app apiserver-www local-provider radius-provider
 tacacs-provider aaa ingest elasticsearch-server elasticsearch-exporter
 elasticsearch-dispatcher ... (total 194)
```

```
Still waiting for apiserver-www aaa ingest elasticsearch-server
 elasticsearch-exporter elasticsearch-dispatcher elasticsearch-recorder
 service-accesscontrol aerisdiskmonitor ambassador ... (total 190)
Still waiting for ingest enroll-www turbine-accumulator-seg-sec-1m turbine-
aggregate-connectivity-monitor-15m turbine-aggregate-counter-rate-15m
 turbine-aggregate-counter-rate-1m turbine-aggregate-dom-metrics-15m
 turbine-aggregate-dom-metrics-sfp-1m turbine-aggregate-hardware-table-
usage-15m turbine-aggregate-hardware-table-usage-1m ... (total 92)
Still waiting for ingest enroll-www turbine-count-dot1x-auth-status-per-int
f turbine-device-aggregate-seg-sec-count-1m turbine-entities-dot1x-wired
 turbine-eos-links turbine-event-cusum-stats-connectivity-monitor turbine-
event-ipsec-connectivity-down turbine-event-lin-predictor-stats-hardware
 turbine-event-threshold-analytics-errors ... (total 82)
Still waiting for ingest enroll-www turbine-network-node-event-mapper
 turbine-network-topology-tagger turbine-network-vxlan-neighbors turbine-
rate-bandwidth turbine-rate-intf-counters turbine-rate-openconfig-intf-
counters turbine-rate-port-channel-counters turbine-rate-seg-sec-count
ers ... (total 53)
Still waiting for ingest enroll-www turbine-windfarm-count-bgp-peer turbine-
windfarm-count-intf-roles turbine-windfarm-device-resource-aggregate
 turbine-windfarm-dom-metrics-qsfp turbine-windfarm-dom-metrics-sfp turbine-
windfarm-eos-version turbine-windfarm-event-change-control turbine-windfarm-
event-intf-status ... (total 24)
Still waiting for kube-apiserver kube-controller-manager kube-proxy kube-
scheduler kubelet ingest docker enroll-www etcd turbine-windfarm-lanz-
data ... (total 19)
Running : cvpConfig.py tool...
Stopping wifimanager
Running : su - cvp -c "cvpi stop wifimanager 2>&1"
Stopping aware
Running : su - cvp -c "cvpi stop aware 2>&1"
Disabling wifimanager
Running : su - cvp -c "cvpi disable wifimanager 2>&1"
Disabling aware
Running : su - cvp -c "cvpi disable aware 2>&1"
CVP installation successful
```

3.4.2 Configuring Multi-node CVP Instances Using the CVP Shell

Use this procedure to configure multi-node CVP instances using the CVP shell. This procedure includes the steps to set up a primary, secondary, and tertiary node, which is the number of nodes required for redundancy. It also includes the steps to verify and apply the configuration of each node.

The sequence of steps in this procedure follow the process described in the basic steps in the process

Pre-requisites:

Before you begin the configuration process, make sure that you:

- Launch the VM (see Deploying CVP OVA on ESX , or Deploying CVP on KVM.)
- Login to the VM console for each of the three(3) nodes (login as **cvpadmin** on each node).

Complete the following steps to configure multi-node CVP instances:

1. Login at the VM console for the primary node as **cvpadmin**.
2. At the **cvp installation mode** prompt, type **m** to select a multi-node configuration.
3. At the prompt to select a role for the node, type **p** to select primary node.

   Note: You **must** select primary first. You cannot configure one of the other nodes before you configure the primary node.
4. Follow the CloudVision Portal prompts to specify the configuration options for the primary node. All options with an asterisk (*) are required. The options include:

- Root password (*)
- Default route (*)
- DNS (*)
- NTP (*)
- Telemetry Ingest Key
- Cluster interface name (*)
- Device interface name (*)
- Hostname (*)
- IP address (*)
- Netmask (*)
- Number of static routes
- Route for each static route
- Interface for static route
- TACACS server ip address
- TACACS server key/port
- IP address of primary (*) for secondary/tertiary only

Note: If there are separate cluster and device interfaces (the interfaces have different IP addresses), make sure that you enter the hostname of the cluster interface. If the cluster and device interface are the same (for example, they are eth0), make sure you enter the IP address of eth0 for the hostname.

Note: The following is an example of the configuration information that requires verification. A CVP cluster MUST be able to resolve A and PTR records in DNS for each cluster node. This forward and reverse DNS lookup MUST be verified. Perform `nslookup` to verify the forward and reverse lookup. This is an important step to CVP forming the cluster during initial setup. For more information on how to use nslookup, refer to Connectivity Requirements.

Note: NTP synchronization is important for CVP cluster nodes, and for EOS streaming telemetry to CVP. NTP service verified using a tool such as `ntpdate`. For more information on how to use `ntpdate`, refer to Connectivity Requirements.

5. At the following prompt, type **v** to verify the configuration.

```
[q]uit, [p]rint, [e]dit, [v]erify, [s]ave, [a]pply, [h]elp ve[r]bose.
```

   If the configuration is valid, the system shows a Valid config status message.
6. Type **a** to apply the configuration for the primary node and wait for the line Waiting for other nodes to send their hostname and ip with spinning wheel.

   The system automatically saves the configuration as a YAML document and shows the configuration settings in pane 1 of the shell.)
7. When `Waiting for other nodes to send their hostname and ip` line is printed by the primary node, go to the shell for the **secondary** node, and specify the configuration settings for the **secondary** node (All options with an asterisk (*) are required, including primary node IP address)
8. At the following prompt, type **v** to verify the configuration.

```
[q]uit, [p]rint, [e]dit, [v]erify, [s]ave, [a]pply, [h]elp ve[r]bose.
```

   If the configuration is valid, the system shows a Valid config status message.
9. Type **a** to apply the configuration for the primary node and wait for the line **Waiting** for other nodes to send their hostname and IP.

   The system automatically saves the configuration as a YAML document and displays the configuration settings in pane 1 of the shell.
10. At the **Primary's root password** prompt, type (enter) the password for the primary node, and then press **Enter**.

11. Go to the shell for the **tertiary** node, and specify the configuration settings for the node. (All options with an asterisk (*) are required.)
12. At the following prompt, type **v** to verify the configuration.

    ```
    [q]uit, [p]rint, [e]dit, [v]erify, [s]ave, [a]pply, [h]elp ve[r]bose.
    ```

    If the configuration is valid, the system shows a Valid config status message.
13. At the **Primary IP** prompt, type the IP address of the primary node.
14. At the **Primarys root password** prompt, press **Enter**.

    The system automatically completes the CVP installation for all nodes (this is done by the primary node). A message appears indicating that the other nodes are waiting for the primary node to complete the CVP installation.

    When the CVP installation is successfully completed for a particular node, a message appears in the appropriate pane to indicate the installation was successful. (This message is repeated in each pane.)
15. Go to shell for the primary node, and type **q** to quit the installation.
16. At the cvp login prompt, login as **root**.
17. At the **[root@cvplogin]#** prompt, switch to the **cvp** user account by typing **su cvp**, and then press **Enter**.
18. Run the `cvpi status all` command, and press **Enter**.

    The system automatically checks the status of the installation for each node and provides status information in each pane for CVP. The information shown includes some of the configuration settings for each node.

    For more information about the process, see:

    - Rules for the Number and Type of Nodes
    - The Basic Steps in the Process
    - The CVP Shell
    - Examples

3.4.2.1 Rules for the Number and Type of Nodes

Three nodes are required for multi-node CVP instances, where a node is identified as either the primary, secondary, or tertiary. You define the node type (primary, secondary, or tertiary) for each node during the configuration.

3.4.2.2 The Basic Steps in the Process

All multi-node configurations follow the same basic process. The basic steps are:

1. Specify the settings for the nodes in the following sequence (you apply the configuration later in the process):

    - Primary node
    - Secondary node
    - Tertiary node
2. Verify and then apply the configuration for the **primary** node. (During this step, the system automatically saves the configuration for the primary node as a YAML document. In addition, the system shows the configuration settings.)

    Once the system applies the configuration for the primary node, the other nodes need to send their hostname and IP address to the primary node.
3. Verify and then apply the configuration for the **secondary** node.

    As part of this step, the system automatically pushes the hostname, IP address, and public key of the secondary node to the primary node. The primary node also sends a consolidated YAML to the secondary node, which is required to complete the configuration of the secondary node.

Note: To ensure the environment variables are generated, only apply configuration when the following messages are displayed.

Only apply the secondary and tertiary nodes if the primary has finished its configuration and displays: "Waiting for other nodes to send their hostname and ip."

The secondary and tertiary nodes will display the following message: "Please wait for primary to show "Waiting for other nodes to send their hostname and ip" before applying."

If the configuration is applied before the message is displayed, the environment variables will not be generated.

4. The previous step (verifying and applying the configuration) is repeated for the **tertiary** node. (The automated processing of data described for the secondary node is also repeated for the tertiary node.)

   Once the configuration for all nodes has been applied (steps 1 through 4 above), the system automatically attempts to complete the CVP installation for all nodes (this is done by the primary node). A message appears indicating that the other nodes are waiting for the primary node to complete the CVP installation.
5. You quit the installation, then login as root and check the status of CVP.

   The system automatically checks the status and provides status information in each pane for the CVP service.

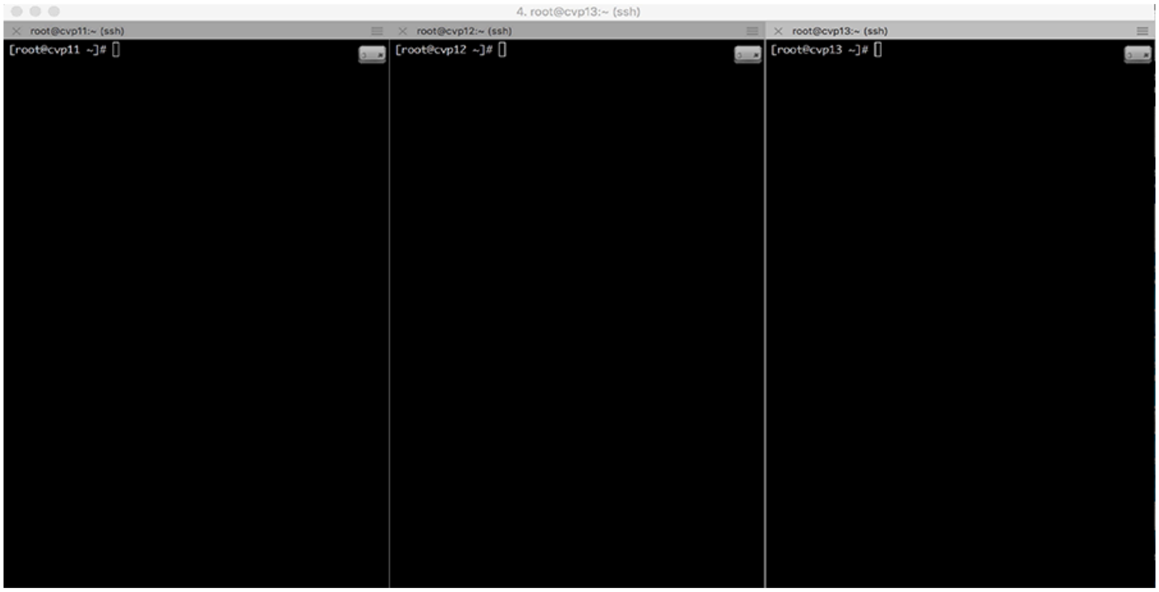
3.4.2.3 The CVP Shell

For multi-node configurations, you need to open 3 CVP consoles (one for each node). Each console is shown in it's own pane. You use each console to configure one of the nodes (primary, secondary, or tertiary).

The system also provides status messages and all of the options required to complete the multi-node configuration. The status messages and options are presented in the panes of the shell that correspond to the node type.

Figure 14: CVP Console Shells for Multi-node Configurations shows three CVP Console shells for multi-node configurations. Each shell corresponds to a CVP Console for each node being configured.

Figure 3-12: CVP Console Shells for Multi-node Configurations



```
[root@cvp11 ~]#
```

```
[root@cvp12 ~]#
```

```
[root@cvp13 ~]#
```

3.4.2.4 Examples

The following examples show the commands used to configure (set up) the primary, secondary, and tertiary nodes, and apply the configurations to the nodes. Examples are also included of the system output shown as CVP completes the installation for each of the nodes.

- Primary Node Configuration
- Secondary Node Configuration
- Tertiary Node Configuration
- Verifying the Primary Node Configuration and Applying it to the Node
- Verifying the Tertiary Node Configurations and Applying them to the Nodes
- Waiting for the Primary Node Installation to Finish
- Waiting for the Secondary and Tertiary Node Installation to Finish

3.4.2.4.1 Primary Node Configuration

This example shows the commands used to configure (set up) the primary node.

```
localhost login: cvpadmin
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
Enter a command
[q]uit [p]rint [s]inglenode [m]ultinode [r]eplace [u]pgrade
>m
Choose a role for the node, roles should be mutually exclusive
[p]rimary [s]econdary [t]ertiary
>p

Enter the configuration for CloudVision Portal and apply it when done.
Entries marked with '*' are required.

common configuration:
  dns: 172.22.22.40, 172.22.22.10
  DNS domains: sjc.aristanetworks.com, ire.aristanetworks.com
  ntp: ntp.aristanetworks.com
  Telemetry Ingest Key: arista
  CV-CUE Enabled: no
  CV-CUE HA cluster IP:
  Cluster Interface name: eth0
  Device Interface name: eth0
node configuration:
 *hostname (fqdn): cvp57.sjc.aristanetworks.com
 *default route: 172.31.0.1
  Number of Static Routes:
  TACACS server ip address:
 *IP address of eth0: 172.31.0.186
 *Netmask of eth0: 255.255.0.0
[q]uit [p]rint [e]dit [v]erify [s]ave [a]pply [h]elp ve[r]bose
>
```

3.4.2.4.2 Secondary Node Configuration

This example shows the commands used to configure (set up) the secondary node.

Note: To ensure the environment variables are generated, only apply configuration when the following messages are displayed.

Only apply the secondary and tertiary nodes if the primary has finished its configuration and displays: "Waiting for other nodes to send their hostname and ip."

The secondary and tertiary nodes will display the following message: "Please wait for primary to show "Waiting for other nodes to send their hostname and ip" before applying." S

If the configuration is applied before the message is displayed, the environment variables will not be generated.

```
localhost login: cvpadmin
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
Enter a command
[q]uit [p]rint [s]inglenode [m]ultinode [r]eplace [u]pgrade
>m
Choose a role for the node, roles should be mutually exclusive
[p]rimary [s]econdary [t]ertiary
>s

Enter the configuration for CloudVision Portal and apply it when done.
Entries marked with '*' are required.

common configuration:
  dns: 172.22.22.40, 172.22.22.10
  DNS domains: sjc.aristanetworks.com, ire.aristanetworks.com
  ntp: ntp.aristanetworks.com
  Telemetry Ingest Key: arista
  CV-CUE Enabled: no
  CV-CUE HA cluster IP:
  Cluster Interface name: eth0
  Device Interface name: eth0
  *IP address of primary: 172.31.0.186
node configuration:
 *hostname (fqdn): cvp65.sjc.aristanetworks.com
 *default route: 172.31.0.1
  Number of Static Routes:
  TACACS server ip address:
 *IP address of eth0: 172.31.0.153
 *Netmask of eth0: 255.255.0.0
>
```

3.4.2.4.3 Tertiary Node Configuration

This example shows the commands used to configure (set up) the tertiary node.

Note: To ensure the environment variables are generated, only apply configuration when the following messages are displayed.

Only apply the secondary and tertiary nodes if the primary has finished its configuration and displays: "Waiting for other nodes to send their hostname and ip."

The secondary and tertiary nodes will display the following message: "Please wait for primary to show "Waiting for other nodes to send their hostname and ip" before applying."

If the configuration is applied before the message is displayed, the environment variables will not be generated.

```
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
Enter a command
[q]uit [p]rint [s]inglenode [m]ultinode [r]eplace [u]pgrade
>m
Choose a role for the node, roles should be mutually exclusive
[p]rimary [s]econdary [t]ertiary
>t

Enter the configuration for CloudVision Portal and apply it when done.
Entries marked with '*' are required.

common configuration:
  dns: 172.22.22.40, 172.22.22.10
  DNS domains: sjc.aristanetworks.com, ire.aristanetworks.com
  ntp: ntp.aristanetworks.com
  Telemetry Ingest Key: arista
  Cluster Interface name: eth0
  Device Interface name: eth0
 *IP address of primary: 172.31.0.186
node configuration:
  hostname (fqdn): cvp84.sjc.aristanetworks.com
 *default route: 172.31.0.1
  Number of Static Routes:
  TACACS server ip address:
 *IP address of eth0: 172.31.0.213
 *Netmask of eth0: 255.255.0.0
[q]uit [p]rint [e]dit [v]erify [s]ave [a]pply [h]elp ve[r]bose
>
```

3.4.2.4.4 Verifying the Primary Node Configuration and Applying it to the Node

This example shows the commands used to verify the configuration of the primary node and apply the configuration to the node.

```
[q]uit [p]rint [e]dit [v]erify [s]ave [a]pply [h]elp ve[r]bose
>v
Valid config format.
Applying proposed config for network verification.
saved config to /cvpi/cvp-config.yaml
Running : cvpConfig.py tool...
[ 8608.509056] vmxnet3 0000:0b:00.0 eth0: intr type 3, mode 0, 9
 vectors allocated
[ 8608.520693] vmxnet3 0000:0b:00.0 eth0: NIC Link is Up 10000 Mbps
[ 8622.807169] vmxnet3 0000:13:00.0 eth1: intr type 3, mode 0, 9
 vectors allocated
[ 8622.810214] vmxnet3 0000:13:00.0 eth1: NIC Link is Up 10000 Mbps
Stopping: network
Running : /bin/sudo /sbin/service network stop
Running : /bin/sudo /bin/systemctl is-active network
Starting: network
Running : /bin/sudo /bin/systemctl start network.service
```

```
[ 8624.027029] vmxnet3 0000:0b:00.0 eth0: intr type 3, mode 0, 9
 vectors allocated
[ 8624.030254] vmxnet3 0000:0b:00.0 eth0: NIC Link is Up 10000 Mbps
[ 8624.032643] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[ 8624.238995] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
[ 8638.294690] vmxnet3 0000:13:00.0 eth1: intr type 3, mode 0, 9
 vectors allocated
[ 8638.297973] vmxnet3 0000:13:00.0 eth1: NIC Link is Up 10000 Mbps
[ 8638.300454] IPv6: ADDRCONF(NETDEV_UP): eth1: link is not ready
[ 8638.302186] IPv6: ADDRCONF(NETDEV_CHANGE): eth1: link becomes ready
[ 8638.489266] warning: `/bin/ping' has both setuid-root and effective
 capabilities. Therefore not raising all capabilities.
Warning: External interfaces, ['eth1'], are discovered under /etc/
sysconfig/network-scripts
These interfaces are not managed by CVP.
Please ensure that the configurations for these interfaces are
 correct.
Otherwise, actions from the CVP shell may fail.

Valid config.
[q]uit [p]rint [e]dit [v]erify [s]ave [a]pply [h]elp ve[r]bose
>
```

3.4.2.4.5 Verifying the Tertiary Node Configurations and Applying them to the Nodes

This example shows the commands used to verify the configurations of the tertiary nodes and apply the configurations to the nodes.

```
[q]uit [p]rint [e]dit [v]erify [s]ave [a]pply [h]elp ve[r]bose
>v
Valid config format.
Applying proposed config for network verification.
saved config to /cvpi/cvp-config.yaml
Running : cvpConfig.py tool...
[ 9195.362192] vmxnet3 0000:0b:00.0 eth0: intr type 3, mode 0, 9
 vectors allocated
[ 9195.365069] vmxnet3 0000:0b:00.0 eth0: NIC Link is Up 10000 Mbps
[ 9195.367043] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[ 9195.652382] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
[ 9209.588173] vmxnet3 0000:13:00.0 eth1: intr type 3, mode 0, 9
 vectors allocated
[ 9209.590896] vmxnet3 0000:13:00.0 eth1: NIC Link is Up 10000 Mbps
[ 9209.592887] IPv6: ADDRCONF(NETDEV_UP): eth1: link is not ready
[ 9209.594222] IPv6: ADDRCONF(NETDEV_CHANGE): eth1: link becomes ready
Stopping: network
Running : /bin/sudo /sbin/service network stop
Running : /bin/sudo /bin/systemctl is-active network
Starting: network
Running : /bin/sudo /bin/systemctl start network.service
[ 9210.561940] vmxnet3 0000:0b:00.0 eth0: intr type 3, mode 0, 9
 vectors allocated
[ 9210.564602] vmxnet3 0000:0b:00.0 eth0: NIC Link is Up 10000 Mbps
[ 9224.805267] vmxnet3 0000:13:00.0 eth1: intr type 3, mode 0, 9
 vectors allocated
[ 9224.808891] vmxnet3 0000:13:00.0 eth1: NIC Link is Up 10000 Mbps
[ 9224.811150] IPv6: ADDRCONF(NETDEV_UP): eth1: link is not ready
[ 9224.812899] IPv6: ADDRCONF(NETDEV_CHANGE): eth1: link becomes ready
Warning: External interfaces, ['eth1'], are discovered under /etc/
sysconfig/network-scripts
```

```
These interfaces are not managed by CVP.
Please ensure that the configurations for these interfaces are
 correct.
Otherwise, actions from the CVP shell may fail.

Valid config.
[q]uit [p]rint [e]dit [v]erify [s]ave [a]pply [h]elp ve[r]bose
>
```

3.4.2.4.6 Waiting for the Primary Node Installation to Finish

These examples show the system output shown as CVP completes the installation for the primary node.

- Waiting for primary node installation to pause until other nodes send files

```
[q]uit [p]rint [e]dit [v]erify [s]ave [a]pply [h]elp ve[r]bose
>a
Valid config format.
saved config to /cvpi/cvp-config.yaml
Applying proposed config for network verification.
saved config to /cvpi/cvp-config.yaml
Running : cvpConfig.py tool...
[15266.575899] vmxnet3 0000:0b:00.0 eth0: intr type 3, mode 0, 9 vectors
 allocated
[15266.588500] vmxnet3 0000:0b:00.0 eth0: NIC Link is Up 10000 Mbps
[15266.591751] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[15266.672644] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
[15280.937599] vmxnet3 0000:13:00.0 eth1: intr type 3, mode 0, 9 vectors
 allocated
[15280.941764] vmxnet3 0000:13:00.0 eth1: NIC Link is Up 10000 Mbps
[15280.944883] IPv6: ADDRCONF(NETDEV_UP): eth1: link is not ready
[15280.947038] IPv6: ADDRCONF(NETDEV_CHANGE): eth1: link becomes ready
Stopping: network
Running : /bin/sudo /sbin/service network stop
Running : /bin/sudo /bin/systemctl is-active network
Starting: network
Running : /bin/sudo /bin/systemctl start network.service
[15282.581713] vmxnet3 0000:0b:00.0 eth0: intr type 3, mode 0, 9 vectors
 allocated
[15282.585367] vmxnet3 0000:0b:00.0 eth0: NIC Link is Up 10000 Mbps
[15282.588072] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[15282.948613] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
[15296.871658] vmxnet3 0000:13:00.0 eth1: intr type 3, mode 0, 9 vectors
 allocated
[15296.875871] vmxnet3 0000:13:00.0 eth1: NIC Link is Up 10000 Mbps
[15296.879003] IPv6: ADDRCONF(NETDEV_UP): eth1: link is not ready
[15296.881456] IPv6: ADDRCONF(NETDEV_CHANGE): eth1: link becomes ready
Warning: External interfaces, ['eth1'], are discovered under /etc/sysconfig/
network-scripts
These interfaces are not managed by CVP.
Please ensure that the configurations for these interfaces are correct.
Otherwise, actions from the CVP shell may fail.

Valid config.
Running : cvpConfig.py tool...
[15324.884887] vmxnet3 0000:0b:00.0 eth0: intr type 3, mode 0, 9 vectors
 allocated
[15324.889169] vmxnet3 0000:0b:00.0 eth0: NIC Link is Up 10000 Mbps
[15324.893217] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[15324.981682] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
```

```
[15339.240237] vmxnet3 0000:13:00.0 eth1: intr type 3, mode 0, 9 vectors
 allocated
[15339.243999] vmxnet3 0000:13:00.0 eth1: NIC Link is Up 10000 Mbps
[15339.247119] IPv6: ADDRCONF(NETDEV_UP): eth1: link is not ready
[15339.249370] IPv6: ADDRCONF(NETDEV_CHANGE): eth1: link becomes ready
Stopping: network
Running : /bin/sudo /sbin/service network stop
Running : /bin/sudo /bin/systemctl is-active network
Starting: network
Running : /bin/sudo /bin/systemctl start network.service
[15340.946583] vmxnet3 0000:0b:00.0 eth0: intr type 3, mode 0, 9 vectors
 allocated
[15340.950891] vmxnet3 0000:0b:00.0 eth0: NIC Link is Up 10000 Mbps
[15340.953786] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[15341.251648] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
[15355.225649] vmxnet3 0000:13:00.0 eth1: intr type 3, mode 0, 9 vectors
 allocated
[15355.229400] vmxnet3 0000:13:00.0 eth1: NIC Link is Up 10000 Mbps
[15355.232674] IPv6: ADDRCONF(NETDEV_UP): eth1: link is not ready
[15355.234725] IPv6: ADDRCONF(NETDEV_CHANGE): eth1: link becomes ready
Waiting for other nodes to send their hostname and ip
\
```

- Waiting for the primary node installation to finish

```
Waiting for other nodes to send their hostname and ip
-
Running : cvpConfig.py tool...
[15707.665618] vmxnet3 0000:0b:00.0 eth0: intr type 3, mode 0, 9
vectors allocated
[15707.669167] vmxnet3 0000:0b:00.0 eth0: NIC Link is Up 10000 Mbps
[15707.672109] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[15708.643628] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
[15722.985876] vmxnet3 0000:13:00.0 eth1: intr type 3, mode 0, 9
vectors allocated
[15722.990116] vmxnet3 0000:13:00.0 eth1: NIC Link is Up 10000 Mbps
[15722.993221] IPv6: ADDRCONF(NETDEV_UP): eth1: link is not ready
[15722.995325] IPv6: ADDRCONF(NETDEV_CHANGE): eth1: link becomes ready
[15724.245523] Ebtables v2.0 unregistered
[15724.940390] ip_tables: (C) 2000-2006 Netfilter Core Team
[15724.971820] ip6_tables: (C) 2000-2006 Netfilter Core Team
[15725.011963] Ebtables v2.0 registered
[15725.077660] nf_conntrack version 0.5.0 (65536 buckets, 262144 max)
Stopping: ntpd
Running : /bin/sudo /sbin/service ntpd stop
Running : /bin/sudo /bin/systemctl is-active ntpd
Starting: ntpd
Running : /bin/sudo /bin/systemctl start ntpd.service
--
Verifying configuration on the secondary node
Verifying configuration on the tertiary node
Starting: systemd services
Starting: cvpi-check
Running : /bin/sudo /bin/systemctl start cvpi-check.service
Starting: zookeeper
Running : /bin/sudo /bin/systemctl start zookeeper.service
Starting: cvpi-config
Running : /bin/sudo /bin/systemctl start cvpi-config.service
Starting: cvpi
Running : /bin/sudo /bin/systemctl start cvpi.service
Running : /bin/sudo /bin/systemctl enable zookeeper
Running : /bin/sudo /bin/systemctl start cvpi-watchdog.timer
Running : /bin/sudo /bin/systemctl enable docker
Running : /bin/sudo /bin/systemctl start docker
Running : /bin/sudo /bin/systemctl enable kube-cluster.path
Running : /bin/sudo /bin/systemctl start kube-cluster.path
Waiting for all components to start. This may take few minutes.
Still waiting for aaa aeriadiakmonitor alertmanager-multinode-service
 ambassador apiserver apiserver-www apiserver-www apiserver-www audit
 aware ... {total 271)
Still waiting for aaa aerisdisknonitor alertmanager-multinode-service
 anbassador apiserver apiserver-www apiserver-www apiserver-www audit
 bapmaintmode ... (total 235)
Still waiting for asa aerisdiskmonitor alertmanager-multinode-service
 ambassador apiserver apiserver-www spiserver-www apiserver-www audit
 bgpmaintmode ... (total 236)
Still waiting for aaa aerisdiskmonitor alertmanager-multinode-service
 ambassador apiserver apiserver-www apiserver-www apiserver-www audit
 bgpmaintmode ... {total 235)
Still waiting for aaa aerisdiskmonitor alertmanager-multinode-service
 ambassador apiserver apiserver-www apiserver-www apiserver-www audit
 bgpmaintmode ... {total 235)
Still waiting for aaa aeriasdiskmonitor alertmanager-multinode-service
 ambassador apiserver apiserver-www apiserver-www apiserver-www audit
 bgpmaintmode ... (total 235)
Still waiting for aaa aerisdisknenitor alertmanager-multinode-service
 ambassador apiserver apiserver-www apiserver-www apiserver-wwww audit
 bgpmaintmode ... (total 236)
Still waiting for eae aerisdiskmonitor alertmanager-multinode-service
 ambassador apiserver apiserver-www apiserver-wrw apiserver-www audit
 bgpmaintmode ... (total 229)
Still waiting for aaa aerisdisknonitor alertmanager-multinode-service
 ambassador apiserver apiserver-www apiserver-www apiserver-www audit
 bgpmaintmode ... (total 228)
Still waiting for aaa aerisdiskmonitor alertmanager-multinode-service
 ambassador apiserver apiserver-www apiserver-www apiserver-www audit
 bgpmaintmode ... (total 213)
Still waiting for aaa alertmanager-multinode-service ambassador apiserver
 apiserver-www apiserver-www apiserver-www audit bgpmaintmode bugalerts-que
ry-tagger ... (total 199)
Still waiting for aaa alertmanager-multinode-service ambassador apiserver
 apiaserver apiserver apiserver-www apiserver-www apiserver-www audit ...
 (total 181)
Still waiting for ase ambassador spisercver-www apiserver-www episerver-www
 audit bgpmaintmode bugalerts-update ccapi cemgr ... (total 121)
Still waiting for aaa ambassador apiserver-www apiserver-www apiserver-www
 audit bgpmaintmode ccapi ccmgr certs ... (total 78)
Still waiting for saa ambassador apiserver-www apiserver-www apiserver-www
 audit certs cloudmanager compliance cvp-backend ... (total 44)
Still waiting for aaa ambassador apiserver-www apiserver-www apiserver-www
 certs cloudmanager cloudmanager cloudmanager compliance ... (total 35)
Still waiting for aaa cvp-frontend cvp-frontend cvp-frontend cvp-www cvp-www
 cvp-www inventory ztp
Still waiting for aaa cvp-frontend cvp-frontend cvp-frontend cvp-www cvp-www
 cvp-www inventory ztp
Still waiting for aaa cvp-frontend cvp-frontend cvp-frontend cvp-www cvp-www
 cvp-www inventory ztp
Still waiting for aaa cvp-frontend cvp-frontend cvp-frontend cvp-www cvp-www
 cvp-www inventory ztp
Still waiting for aaa cvp-frontend cvp-frontend cvp-frontend cvp-www cvp-www
 cvp-www inventory ztp
Still waiting for aaa cvp-frontend cvp-frontend cvp-frontend cvp-www cvp-www
 cvp-www inventory ztp
Still waiting for aaa evp-frontend evp-frontend evp-frontend cvp-www evp-www
 cvp-www inventory ztp
Still waiting for cvp-frontend cvp-frontend cvp-frontend
CVP installation successful
Running : cvpConfig.py tool...
```

```
Stopping wifimanager
Running : su - cvp -c "cvpi stop wifimanager"
Stopping aware
Running : su - cvp -c "cvpi stop aware"
Disabling wifimanager
Running : su - cvp -c "cvpi disable wifimanager"
Disabling aware
Running 1 su - cvp -c "cvpi disable aware"

[q]uit [p]rint [e]dit [v]erify [s]ave [a]pply [h]elp ve[r]bose
```

3.4.2.4.7 Waiting for the Secondary and Tertiary Node Installation to Finish

This example shows the system output displayed as CVP completes the installation for the secondary and tertiary nodes.

```
[q]uit [p]rint [e]dit [v]erify [s]ave [a]pply [h]elp ve[r]bose
>a
Valid config format.
saved config to /cvpi/cvp-config.yaml
Applying proposed config for network verification.
saved config to /cvpi/cvp-config.yaml
Running : cvpConfig.py tool...
[15492.903419] vmxnet3 0000:0b:00.0 eth0: intr type 3, mode 0, 9
 vectors allocated
[15492.908473] vmxnet3 0000:0b:00.0 eth0: NIC Link is Up 10000 Mbps
[15492.910297] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[15493.289569] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
[15507.118778] vmxnet3 0000:13:00.0 eth1: intr type 3, mode 0, 9
 vectors allocated
[15507.121579] vmxnet3 0000:13:00.0 eth1: NIC Link is Up 10000 Mbps
[15507.123648] IPv6: ADDRCONF(NETDEV_UP): eth1: link is not ready
[15507.125051] IPv6: ADDRCONF(NETDEV_CHANGE): eth1: link becomes ready
Stopping: network
Running : /bin/sudo /sbin/service network stop
Running : /bin/sudo /bin/systemctl is-active network
Starting: network
Running : /bin/sudo /bin/systemctl start network.service
[15508.105909] vmxnet3 0000:0b:00.0 eth0: intr type 3, mode 0, 9
 vectors allocated
[15508.108752] vmxnet3 0000:0b:00.0 eth0: NIC Link is Up 10000 Mbps
[15522.301114] vmxnet3 0000:13:00.0 eth1: intr type 3, mode 0, 9
 vectors allocated
[15522.303766] vmxnet3 0000:13:00.0 eth1: NIC Link is Up 10000 Mbps
[15522.305580] IPv6: ADDRCONF(NETDEV_UP): eth1: link is not ready
[15522.306866] IPv6: ADDRCONF(NETDEV_CHANGE): eth1: link becomes ready
Warning: External interfaces, ['eth1'], are discovered under /etc/
sysconfig/network-scripts
These interfaces are not managed by CVP.
Please ensure that the configurations for these interfaces are
 correct.
Otherwise, actions from the CVP shell may fail.

Valid config.
Running : cvpConfig.py tool...
[15549.664989] vmxnet3 0000:0b:00.0 eth0: intr type 3, mode 0, 9
 vectors allocated
[15549.667899] vmxnet3 0000:0b:00.0 eth0: NIC Link is Up 10000 Mbps
[15549.669783] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[15550.046552] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
```

```
[15563.933328] vmxnet3 0000:13:00.0 eth1: intr type 3, mode 0, 9
 vectors allocated
[15563.937507] vmxnet3 0000:13:00.0 eth1: NIC Link is Up 10000 Mbps
[15563.940501] IPv6: ADDRCONF(NETDEV_UP): eth1: link is not ready
[15563.942113] IPv6: ADDRCONF(NETDEV_CHANGE): eth1: link becomes ready
Stopping: network
Running : /bin/sudo /sbin/service network stop
Running : /bin/sudo /bin/systemctl is-active network
Starting: network
Running : /bin/sudo /bin/systemctl start network.service
[15565.218666] vmxnet3 0000:0b:00.0 eth0: intr type 3, mode 0, 9
 vectors allocated
[15565.222324] vmxnet3 0000:0b:00.0 eth0: NIC Link is Up 10000 Mbps
[15565.225193] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[15565.945531] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
[15579.419911] vmxnet3 0000:13:00.0 eth1: intr type 3, mode 0, 9
 vectors allocated
[15579.422707] vmxnet3 0000:13:00.0 eth1: NIC Link is Up 10000 Mbps
[15579.424636] IPv6: ADDRCONF(NETDEV_UP): eth1: link is not ready
[15579.425962] IPv6: ADDRCONF(NETDEV_CHANGE): eth1: link becomes ready
Running : cvpConfig.py tool...
[15600.608075] vmxnet3 0000:0b:00.0 eth0: intr type 3, mode 0, 9
 vectors allocated
[15600.610946] vmxnet3 0000:0b:00.0 eth0: NIC Link is Up 10000 Mbps
[15600.613687] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[15600.986529] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
[15615.840426] vmxnet3 0000:13:00.0 eth1: intr type 3, mode 0, 9
 vectors allocated
[15615.843207] vmxnet3 0000:13:00.0 eth1: NIC Link is Up 10000 Mbps
[15615.845197] IPv6: ADDRCONF(NETDEV_UP): eth1: link is not ready
[15615.846633] IPv6: ADDRCONF(NETDEV_CHANGE): eth1: link becomes ready
[15616.732733] Ebtables v2.0 unregistered
[15617.213057] ip_tables: (C) 2000-2006 Netfilter Core Team
[15617.233688] ip6_tables: (C) 2000-2006 Netfilter Core Team
[15617.261149] Ebtables v2.0 registered
[15617.309743] nf_conntrack version 0.5.0 (65536 buckets, 262144 max)
Stopping: ntpd
Running : /bin/sudo /sbin/service ntpd stop
Running : /bin/sudo /bin/systemctl is-active ntpd
Starting: ntpd
Running : /bin/sudo /bin/systemctl start ntpd.service
Pushing hostname, ip address and public key to the primary node
Primary's root password:
Transferred files
Receiving public key of the primary node
-
Waiting for primary to send consolidated yaml
-
Received authorized keys and consolidated yaml files
Running : /bin/sudo /bin/systemctl start cvpi-watchdog.timer
Running : cvpConfig.py tool...
[15748.205170] vmxnet3 0000:0b:00.0 eth0: intr type 3, mode 0, 9
 vectors allocated
[15748.208393] vmxnet3 0000:0b:00.0 eth0: NIC Link is Up 10000 Mbps
[15748.210206] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[15748.591559] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
[15752.406867] vmxnet3 0000:13:00.0 eth1: intr type 3, mode 0, 9
 vectors allocated
[15752.409789] vmxnet3 0000:13:00.0 eth1: NIC Link is Up 10000 Mbps
[15752.412015] IPv6: ADDRCONF(NETDEV_UP): eth1: link is not ready
[15752.413603] IPv6: ADDRCONF(NETDEV_CHANGE): eth1: link becomes ready
Stopping: zookeeper
Running : /bin/sudo /sbin/service zookeeper stop
Running : /bin/sudo /bin/systemctl is-active zookeeper
```

```
Stopping: cvpi-check
Running : /bin/sudo /sbin/service cvpi-check stop
Running : /bin/sudo /bin/systemctl is-active cvpi-check
Stopping: ntpd
Running : /bin/sudo /sbin/service ntpd stop
Running : /bin/sudo /bin/systemctl is-active ntpd
Starting: ntpd
Running : /bin/sudo /bin/systemctl start ntpd.service
Starting: cvpi-check
Running : /bin/sudo /bin/systemctl start cvpi-check.service
Starting: zookeeper
Running : /bin/sudo /bin/systemctl start zookeeper.service
Running : /bin/sudo /bin/systemctl enable docker
Running : /bin/sudo /bin/systemctl start docker
Running : /bin/sudo /bin/systemctl enable kube-cluster.path
Running : /bin/sudo /bin/systemctl start kube-cluster.path
Running : /bin/sudo /bin/systemctl enable zookeeper
Running : /bin/sudo /bin/systemctl enable cvpi
Waiting for primary to finish configuring cvp.
-
Please wait for primary to complete cvp installation.
[q]uit [p]rint [e]dit [v]erify [s]ave [a]pply [h]elp ve[r]bose
>
```

Related concepts

Getting Started (CVP)

The login screen is displayed when you first connect to the application using a web browser.

3.5 Shell Reconfiguration of Single-node, Multi-node Systems

The configuration of single-node systems and multi-node systems can be reconfigured using the CVP shell, even after the installation is complete. The reconfiguration process brings down the applications and CVPI for a brief period of time until reconfiguration is complete.

- Single-node Shell Reconfiguration
- Multi-node Shell Reconfiguration

3.5.1 Single-node Shell Reconfiguration

The process for reconfiguring a single-node system is based on the process used to complete the initial installation. You can change any of the configuration settings during the reconfiguration.

Note: The system must be in healthy state before reconfiguration is attempted.

To change an existing single-node configuration, do the following:

1. Follow the same steps you use for an initial single-node, shell-based install (see Configuring a Single-Node CVP Instance using CVP Shell).
2. When prompted with the message **Are you sure you want to replace config and restart? yes/no:** enter **yes**, and then press **Enter**. (Make sure there are no configuration errors.)

   This system automatically completes the configuration.

3.5.2 Multi-node Shell Reconfiguration

The process for reconfiguring a multi-node system is based on the process used to complete the initial installation. Just like initial installations, you can only edit the configuration of the node you are logged into.

- Configurable and Read-only Parameters
- Shifting Parameters
- Example of Primary Node Reconfiguration
- Procedure

3.5.2.1 Configurable and Read-only Parameters

You can change some, but not all of the configuration settings during the reconfiguration. The configuration parameters you cannot change are read-only after the initial configuration.

The configurable and read-only parameters are:

- Configurable parameters
  - default route (gateway)
  - dns
  - ntp
  - aeris ingest key
  - TACACS server IP address
  - TACACS server key/port
  -
- Read-only parameters
  - Cluster interface name
  - Device interface name
  - hostname (fqdn)
  - ip address
  - netmask
  - Number of static routes
  - Route for each static route
  - Interface for static route
  - Primary IP address (use current primary ip address)

Note: The cluster must be in healthy state before reconfiguration is attempted. Also, do not edit `cvp-config.yaml` directly. Make sure you use the shell-based install to reconfigure it.

3.5.2.2 Shifting Parameters

You have the option of shifting common-level parameters (parameters that apply to the cluster), down to the node-level section, and from the node-level section up to the common-level. One example of a common-level parameters you can shift down is default gateway.

Note: If you shift parameters from one level to the other, you may encounter the “Incomplete config” warning during the verify section. If this happens, acknowledge the warning by typing “Y” at the prompt, and then continue with the install.

This example shows the “Incomplete config” warning:

```
>v
Incomplete config - Missing
secondary:
- default route
tertiary:
- default route

Override warnings? [Y/n] : Y
Valid config format
```

3.5.2.3 Example of Primary Node Reconfiguration

```
localhost login: cvpadmin
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
Enter a command
[q]uit [p]rint [s]inglenode [m]ultinode [r]eplace [u]pgrade
>m
Choose a role for the node, roles should be mutually exclusive
[p]rimary [s]econdary [t]ertiary
>p
...
[q]uit [p]rint [e]dit [v]erify [s]ave [a]pply [h]elp ve[r]bose
>e
CVP service is configured and may be running,
reconfigure may be limited to certain parameters
common configuration:
  dns: 172.22.22.40
  ntp: ntp.aristanetworks.com
  Telemetry Ingest Key: modified_ingest_key_for_telemetry <-- modified key
  Cluster Interface name: eth0
  Device Interface name: eth0
node configuration:
 *hostname (fqdn): cvp57.sjc.aristanetworks.com
 *default route: 172.31.0.1
  Number of Static Routes:
  TACACS server ip address:
 *IP address of eth0: 172.31.0.186
 *Netmask of eth0: 255.255.0.0
>v
Valid config format.
Using existing settings for new proposed network verification.
Warning: External interfaces, ['eth1'], are discovered under /etc/sysconfig/
network-scripts
These interfaces are not managed by CVP.
Please ensure that the configurations for these interfaces are correct.
Otherwise, actions from the CVP shell may fail.

Valid config.
[q]uit [p]rint [e]dit [v]erify [s]ave [a]pply [h]elp ve[r]bose
>a
Valid config format.
saved config to /cvpi/cvp-config.yaml
Using existing settings for new proposed network verification.
Warning: External interfaces, ['eth1'], are discovered under /etc/sysconfig/
network-scripts
These interfaces are not managed by CVP.
Please ensure that the configurations for these interfaces are correct.
Otherwise, actions from the CVP shell may fail.

Valid config.
Are you sure you want to replace config and restart? yes/no: no
```

3.5.2.4 Procedure

To change an existing multi-node configuration, do the following:

1. Follow the same steps you use for an initial multi-node, shell-based install (see Configuring Multi-node CVP Instances Using the CVP Shell).

2. When prompted with the message **Are you sure you want to replace config and restart? yes/no:** enter **yes**, and then press **Enter**. (Make sure there are no configuration errors.)

   Note: You will also be prompted for primary node ip address and root passwords during reconfiguration.

Related concepts

Getting Started (CVP)
The login screen is displayed when you first connect to the application using a web browser.

3.6 ISO-based Configuration

The ISO-based configuration can be used to set up either a single-node or multi-node CVP instance(s). Before configuring and starting CVP, the following tasks must be completed.

Quick Start Steps:

- Launch the VM (see Deploying CVP OVA on ESX or Deploying CVP on KVM).
- Create a YAML Document
- Feed the YAML File into the geniso.py Tool
- Map ISO to the VM's CD-ROM Drive
- Verify the host name, reachability of the name server, and VM connectivity.

3.6.1 Create a YAML Document

Create a YAML document describing the node(s) (one or three) in your CVP deployment. When creating a YAML document, the following should be considered:

- The version field is required and must be 2.
- The `dns` and `ntp` entries are lists of values.
- The mode parameter is required. Options are: `mode: singlenode` or `mode: multinode`
- The `dns`, and `ntp` parameters are optional, but recommended to use.

Note: The parameters, which are the same for all nodes, can be specified only once in the common section of the YAML. For example, `default_route` can be specified only once in the common section and not three times, once for each node.

Example:

The following example of a YAML document shows the use of separate (different) interfaces for cluster and device-facing networks. These parameters are explained in the previous section. For a single-node deployment, remove the sections for `node2` and `node3` (assuming all nodes are on the same subnet and have the same default route).

```
>cat multinode.yaml
version: 2
common:
 aeris_ingest_key: magickey
 cluster_interface: eth0
 default_route: 172.31.0.1
 mode: multinode
 device_interface: eth0
 dns:
 - 172.22.22.40
 ntp:
 - ntp.aristanetworks.com
node1:
hostname: cvp6.sjc.aristanetworks.com
interfaces:
eth0:
 ip_address: 172.31.3.236
 netmask: 255.255.0.0
 vmname: cvp6

node2:
   vmname: cvp9
   hostname : cvp9.sjc.aristanetworks.com
   interfaces:
      eth0:
         ip_address: 172.31.3.239
         netmask: 255.255.0.0
      eth1:
         ip_address: 10.0.0.2
         netmask: 255.255.255.0
node3:
   vmname: cvp10
   hostname: cvp10.sjc.aristanetworks.com
   interfaces:
      eth0:
         ip_address: 172.31.3.240
         netmask: 255.255.0.0
      eth1:
         ip_address: 10.0.0.3
         netmask: 255.255.255.0
```

3.6.2 Feed the YAML File into the *geniso.py* Tool

Once you have created the YAML file, you are ready to feed it into the tool so that you can generate the ISO files for the CVP nodes. The root password can be provided at the command line or prompted from the user. If password is empty, no password will be set for root.

Note: The `geniso.py` tool is provided by `cvp-tools-1.0.1.tgz` which can be found at https://www.arista.com/en/support/software-download. The package also contains a README file with more details and requirements for `geniso.py`.

Complete the following steps:

1. Run the `yum install mkisofs` command.
2. Feed the YAML document into the `geniso.py` tool.

   The system generates the ISO files for the nodes using the input of the YAML document.

   Example:

   - In this example, you are prompted for the root password.

   ```
   > mkdir tools
   > tar zxf cvp-tools-1.0.1.tgz -C tools
   > cd tools

   ...<edit multinode.yaml>...

   > ./geniso.py -y multinode.yaml
   Please enter a password for root user on cvp
   Password:
   Please re-enter the password:
   Building ISO for node1 cvp1: cvp.iso.2015-11-04_00:16:23/node1-cvp1.iso
   Building ISO for node2 cvp2: cvp.iso.2015-11-04_00:16:23/node2-cvp2.iso
   Building ISO for node3 cvp3: cvp.iso.2015-11-04_00:16:23/node3-cvp3.iso
   ```
3. In case of using KVM as a hypervisor in a multi-node setup, copy the following ISO files to the corresponding nodes:

- SCP node2's ISO to node 2

```
[root@localhost cvp]# scp node2-cvp-appliance-2.iso root@172.28.161.44://
data/cvp/
root@172.28.161.44's password:
node2-cvp-appliance-2.iso

100%  360KB  57.5MB/s   00:00
```

- SCP node3's ISO to node 3

```
[root@localhost cvp]# scp node3-cvp-appliance-3.iso root@172.28.161.45://
data/cvp/
root@172.28.161.45's password:
node3-cvp-appliance-3.iso

100%  360KB  54.7MB/s   00:00
```

Note: The script has to be run on one machine only. This generates three ISO images which contains the same ssh keys, thus allowing the nodes to send files without a password. If the script is run individually on each node, it result in images containing different ssh keys and the deployment process fails, until the user manually adds the ssh keys in `~/.ssh/authorized_keys`.

3.6.3 Map ISO to the VM's CD-ROM Drive

You can map the ISO to the VM's CD-ROM drive through either ESXi or KVM.

Note: The following script was created with Python 2.7.

On all hosts:

1. Create the folder where the ISO will be stored.

```
mkdir -p /data/ISO
```

2. Create the folder where the VM will be stored. (If this procedure is used to re-install a CVP cluster on CVA appliances then make sure to remove old files from the /data/cvp folder)

```
mkdir -p /data/cvp
cd /data/cvp
```

3. Download the CVP image you want to deploy.

```
wget http://dist/release/cvp/2018.2.5/final/cvp-2018.2.5-kvm.tgz
```

4. Unarchive it.

```
tar -xvf cvp-2018.2.5-kvm.tgz
```

5. Download the CVP tools.

```
wget http://dist/release/cvp/2018.2.5/final/cvp-tools-2018.2.5.tgz
```

6. Unarchive it.

```
tar -xvf cvp-tools-2018.2.5.tgz
```

On the primary:

1. Modify the multinode.yaml file extracted from cvp-tools. It should look something like:

```
common:
  cluster_interface: eth0
  device_interface: eth0
  dns:
  - 172.22.22.10
  ntp:
  - 172.22.22.50
node1:
  default_route: 172.28.160.1
  hostname: cvp-applicance-1.sjc.aristanetworks.com
  interfaces:
    eth0:
      ip_address: 172.28.161.168
      netmask: 255.255.252.0
  vmname: cvp-appliance-1
node2:
  default_route: 172.28.160.1
  hostname: cvp-applicance-2.sjc.aristanetworks.com
  interfaces:
    eth0:
      ip_address: 172.28.161.169
      netmask: 255.255.252.0
  vmname: cvp-appliance-2
node3:
  default_route: 172.28.160.1
  hostname: cvp-applicance-3.sjc.aristanetworks.com
  interfaces:
    eth0:
      ip_address: 172.28.161.170
      netmask: 255.255.252.0
  vmname: cvp-appliance-3
version: 2
```

Note: The example above is from CVP 2018.2.5, more recent versions might have different key value pairs so it is always best to log into an existing VM and check /cvpi/cvp-config.yaml.

2. Use the geniso.py script extracted from CVP-tools to generate the images for ISO based installation and feed the yaml file into it:

```
[root@localhost cvp]# ./geniso.py -y multinode.yaml
Please enter a password for root user on cvp
Password:
Please re-enter the password:
Building ISO for node1 cvp-appliance-1: cvp.iso.2019-07-26_17:01:14/node1-
cvp-appliance-1.iso
Building ISO for node2 cvp-appliance-2: cvp.iso.2019-07-26_17:01:14/node2-
cvp-appliance-2.iso
Building ISO for node3 cvp-appliance-3: cvp.iso.2019-07-26_17:01:14/node3-
cvp-appliance-3.iso
```

3. SCP the generated ISOs to the corresponding nodes.

```
mv node1-cvp-appliance-1.iso /data/ISO
scp node2-cvp-appliance-2.iso root@172.28.161.44://data/ISO/
scp node3-cvp-appliance-3.iso root@172.28.161.45://data/ISO/
```

4. On each node generate the xml file for KVM.

```
./generateXmlForKvm.py -n cvp --device-bridge devicebr -k 1 -i
cvpTemplate.xml -o qemuout.xml -x "/data/cvp/disk1.qcow2" -y
"/data/cvp/disk2.qcow2" -b 22528 -p 8 -e "/usr/libexec/qemu-kvm"
```

Note: The above will generate the VM specs with 8 CPU and 22GB of RAM, for production use please refer to our Release Notes.

To use both bridges (devicebr and clusterbr) the command would look like this:

```
./generateXmlForKvm.py -n cvp --device-bridge devicebr
--cluster-bridge clusterbr -k 1 -i cvpTemplate.xml -o
qemuout.xml -x "/data/cvp/disk1.qcow2" -y
"/data/cvp/disk2.qcow2" -b 54525 -p 28 -e "/usr/libexec/qemu-kvm
```

5. Define the VM.

```
virsh define qemuout.xml
```

6. Start the VM.

```
virsh start cvp
```

7. Add the ISO image to the VM.

   a. Node1

   ```
   ./addIsoToVM.py -n cvp -c /data/ISO/node1-cvp-appliance-1.iso
   ```

   b. Node2

   ```
   ./addIsoToVM.py -n cvp -c /data/ISO/node2-cvp-appliance-2.iso
   ```

   c. Node3

   ```
   ./addIsoToVM.py -n cvp -c /data/ISO/node3-cvp-appliance-3.iso
   ```

The VM will be rebooted and configured automatically, so you just have to login and wait until the components come up

```
virsh console cvp
```

```
[root@localhost cvp]# virsh console cvp
Connected to domain cvp
Escape character is ^]
[   30.729182] Ebtables v2.0 unregistered
[   31.253141] ip_tables: (C) 2000-2006 Netfilter Core Team
[   31.290314] ip6_tables: (C) 2000-2006 Netfilter Core Team
[   31.338226] Ebtables v2.0 registered
[   31.401887] nf_conntrack version 0.5.0 (65536 buckets, 262144 max)
[  124.829593] FS-Cache: Loaded
[  124.881829] FS-Cache: Netfs 'nfs' registered for caching

CentOS Linux 7 (Core)
Kernel 3.10.0-957.1.3.el7.x86_64 on an x86_64

cvp-applicance-1 login:
CentOS Linux 7 (Core)
Kernel 3.10.0-957.1.3.el7.x86_64 on an x86_64

cvp-applicance-1 login:
CentOS Linux 7 (Core)
Kernel 3.10.0-957.1.3.el7.x86_64 on an x86_64

cvp-applicance-1 login: root
Password:
[root@cvp-applicance-1 ~]# su cvp
```

```
c[cvp@cvp-applicance-1 root]$ cvpi status all

Current Running Command: [/cvpi/bin/cvpi -v=3 start all]
Current Command Running Node: primary
Executing command. This may take a few seconds...
primary  18/75 components running, 57 failed
secondary  16/86 components running, 70 failed
tertiary  13/42 components running, 29 failed
```

A few minutes later:

```
[cvp@cvp-applicance-1 root]$ cvpi status all

Current Running Command: None
Executing command. This may take a few seconds...
primary  75/75 components running
secondary  86/86 components running
tertiary  42/42 components running
```

3.7 Certificate-Based TerminAttr Authentication

Arista/EOS switches use TerminAttr for streaming network data to CVP in the following network configurations:

- Firewalls or dynamic NAT is deployed between CloudVision and EOS devices
- Multi-Factor Authentication (MFA) or One-Time-Passwords (OTPs) are used for authentication

Note: When terminattr authentication is enabled, CVP does not require EAPI-over-HTTPS connections. Any CVP authenticated user is also authenticated with the devices that CVP manages.

Each TerminAttr connection must be authenticated using either shared keys or certificate. The certificate-based TerminAttr authentication provides the following additional security features:

- Eliminates the shared key from the switch's configuration
- Uniquely authenticates each TerminAttr connection between the switch and CVP

Note: Third party devices can use only the shared key authentication. The minimum required version of TerminAttr to use this feature is *v1.6.1*.

The following sections describes configuring devices with certificate-based TerminAttr authentication:

- Enabling Certificate-Based TerminAttr Authentication
- Reboarding Existing Devices
- Re-ZTP On-Boarded Devices
- Switching the Authentication from Shared Keys to Certificates
- Switching the Authentication from Certificates to Shared Keys

3.7.1 Enabling Certificate-Based TerminAttr Authentication

When on-boarding a device through Zero Touch Provisioning (ZTP) or direct import, the certificate-based TerminAttr authentication uses a temporary token to enroll client certificates from CVP. The SYS_TelemetryBuilderV3 generates the TerminAttr configuration that uses certificate-based TerminAttr authentication.

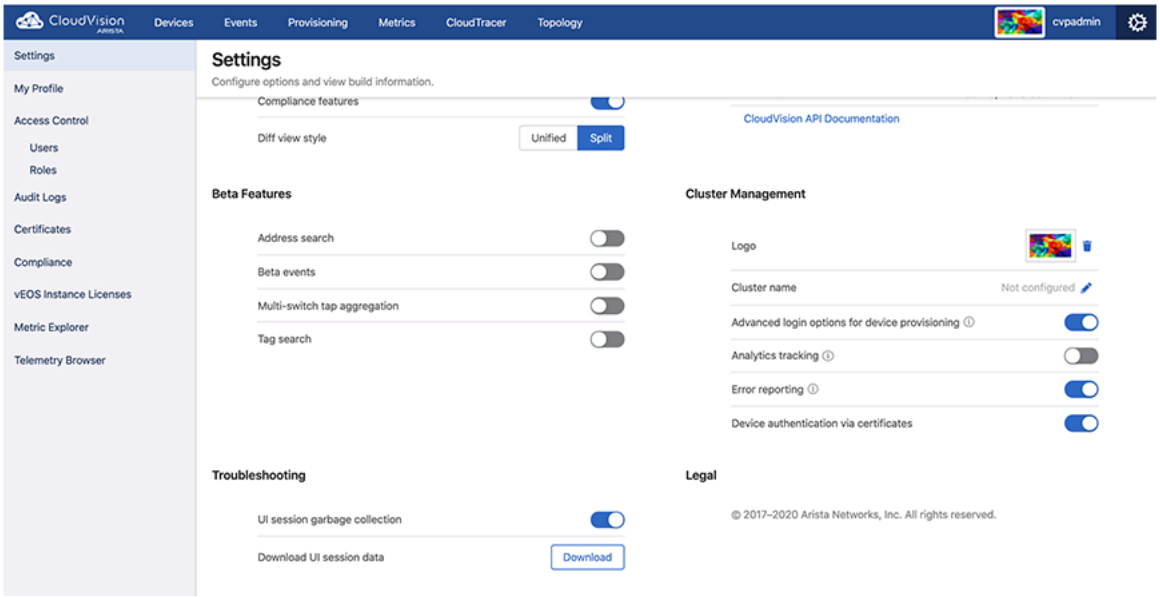
Note: Cerificate-based TerminAttr authentication is used as the default method as of version 2021.2.0, but can be changed to shared key if needed. Shared key authentication support is not supported in version 2023.1.0 and newer.

Perform the following steps to enable certificate-based TerminAttr authentication:

1. In CloudVision portal, click the gear icon at the upper right corner of the page.

   The system displays the Settings screen.
2. Under the Cluster Management pane, enable **Device authentication via certificates** using the toggle button.

   Figure 3-13: Enable Device Authentication via Certificates



Settings

Configure options and view build information.

Compliance features ●

Diff view style: Unified [✓ Split]

Beta Features

Address search ○

Beta events ○

Multi-switch tap aggregation ○

Tag search ○

Troubleshooting

UI session garbage collection ●

Download UI session data

Cluster Management

Logo

Cluster name: Not configured

Advanced login options for device provisioning ●

Analytics tracking ○

Error reporting ●

Device authentication via certificates ●

Legal

© 2017–2020 Arista Networks, Inc. All rights reserved.

3.7.2 Switching the Authentication from Certificates to Shared Keys

Perform the following steps for switching the authentication from certificates to shared keys:

1. Disable the **Device authentication via certificates** option on the settings page.

   See Enabling Certificate-Based TerminAttr Authentication.
2. Regenerate the configlets for all devices using SYS_TelemetryV3 builder.

   The generated configlets starts using shared key authentication.
3. Execute resulting tasks.

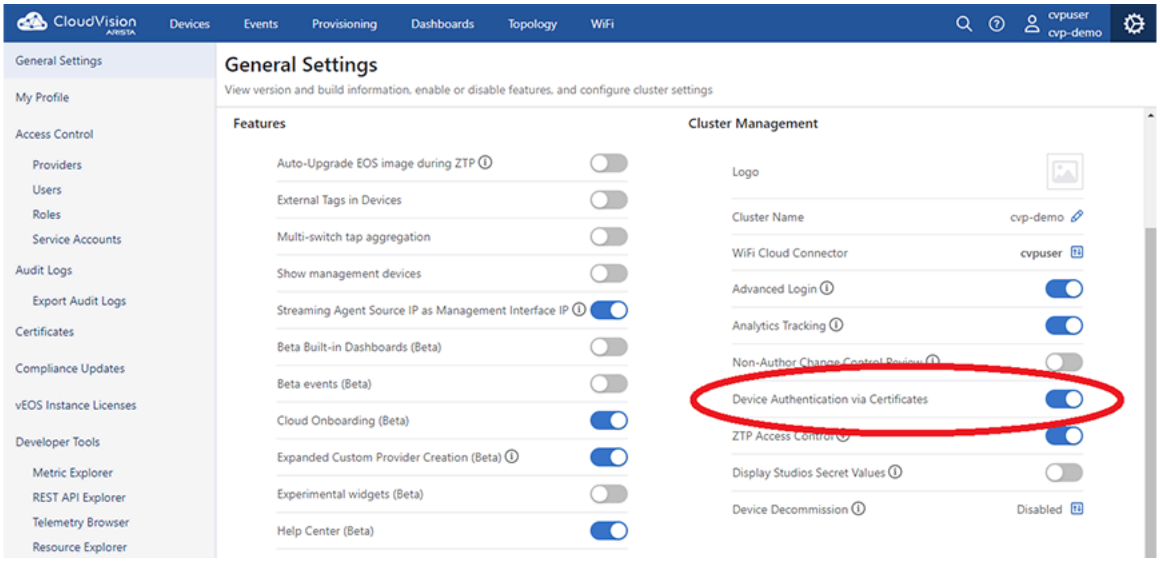
3.7.3 Switching the Authentication from Shared Keys to Certificates

Perform the following steps for switching the authentication from shared keys to certificates:

Note: As of version 2021.2.0, Certificate Authentication is enabled by default for all new on-prem installations. For previous releases, the TerminAttr certificate authentication can be turned ON by enabling the **Device authentication via certificates** setting in the Settings page.

Note: No action is required if the setting is no longer visible in a cluster running version 2022.2 or newer. If the setting is visible in a cluster running version 2022.2 release or newer, then a warning will be displayed during the upgrade process to warn about this deprecated feature. CloudVision users are encouraged to move all the devices to use certificate authentication.

Figure 3-14: General Settings



General Settings

View version and build information, enable or disable features, and configure cluster settings

Features

Auto-Upgrade EOS image during ZTP ⓘ	○
External Tags in Devices	○
Multi-switch tap aggregation	○
Show management devices	○
Streaming Agent Source IP as Management Interface IP ⓘ	●
Beta Built-in Dashboards (Beta)	○
Beta events (Beta)	○
Cloud Onboarding (Beta)	●
Expanded Custom Provider Creation (Beta) ⓘ	●
Experimental widgets (Beta)	○
Help Center (Beta)	●

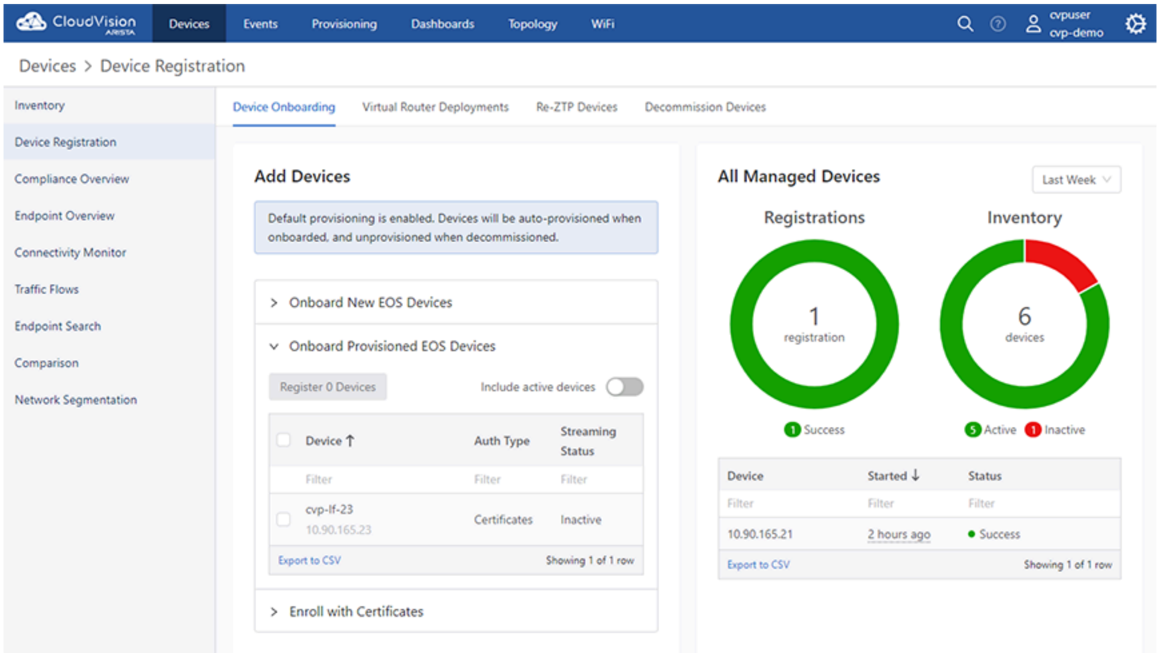
Cluster Management

Logo	
Cluster Name	cvp-demo
WiFi Cloud Connector	cvpuser
Advanced Login ⓘ	●
Analytics Tracking ⓘ	●
Non-Author Change Control Review ⓘ	○
Device Authentication via Certificates	●
ZTP Access Control ⓘ	●
Display Studios Secret Values ⓘ	○
Device Decommission ⓘ	Disabled

The following procedure will enable certificate-based authentication for TerminAttr when there are devices already devices provisioned.

1. Select **Devices** and the **Device Registration** tab. Within **Device Onboarding** select **Onboard Provisioned EOS Devices**.

   Figure 3-15: Devices - Device Registration



Add Devices

Default provisioning is enabled. Devices will be auto-provisioned when onboarded, and unprovisioned when decommissioned.

> Onboard New EOS Devices

Onboard Provisioned EOS Devices

Register 0 Devices   Include active devices ○

☐	Device ↑	Auth Type	Streaming Status
	Filter	Filter	Filter
☐	cvp-lf-23 10.90.165.23	Certificates	Inactive

Export to CSV   Showing 1 of 1 row

> Enroll with Certificates

All Managed Devices

Device	Started ↓	Status
Filter	Filter	Filter
10.90.165.21	2 hours ago	● Success

Export to CSV   Showing 1 of 1 row

2. If you have a large list, the **Auth Type** column can be sorted by selecting the column header.
3. Select all the devices with“**Auth Type** as **Ingest Key** and then select **Register n devices**.
4. The **Auth Type** of the device will change to **Certificates**.
5. The device needs to be reconciled because it is out of compliance. Go to **Provisioning** and select **Network Provisioning**. A topographical view of your device will be displayed.

6. Select the device that is out of compliance (yellow in color). Click on **Manage** and then **Configlet**.
7. Select **SYS_TelemetryBuilderV4** and then click **Generate** to generate the configuration. When complete click **Validate**. (If VRF is used on the management interface then select VRF before generating the configuration).
8. Click **Save**. The configuration is applied and the device will be compliant now.

3.7.4 Reboarding Existing Devices

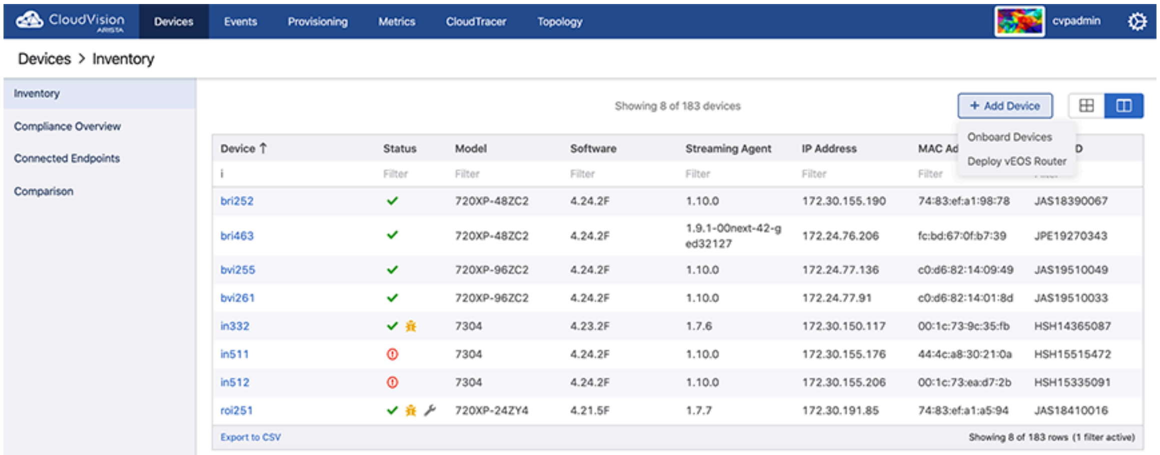
You must reboard a device when the certificate-based TerminAttr authentication fails due to missing or invalid client certificates.

Perform the following steps to reboard devices:

1. In CloudVision portal, click the **Devices** tab.

   The system displays the Inventory screen.

   Figure 3-16: Inventory Screen



Showing 8 of 183 devices

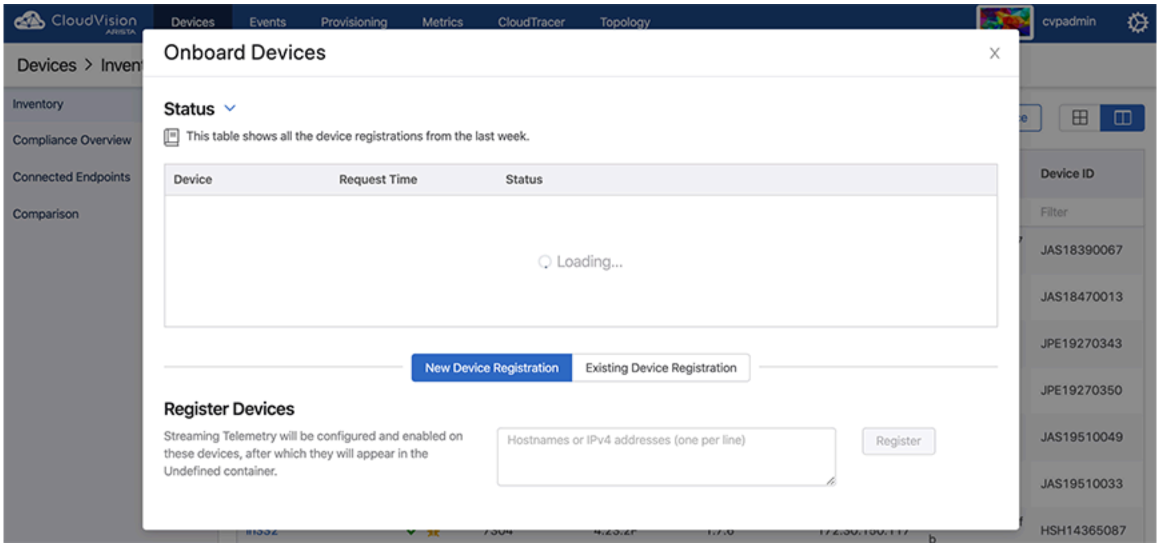
Device ↑	Status	Model	Software	Streaming Agent	IP Address	MAC Ad	D
i	Filter	Filter	Filter	Filter	Filter	Filter	
bri252	✓	720XP-48ZC2	4.24.2F	1.10.0	172.30.155.190	74:83:ef:a1:98:78	JAS18390067
bri463	✓	720XP-48ZC2	4.24.2F	1.9.1-00next-42-ged32127	172.24.76.206	fc:bd:67:0f:b7:39	JPE19270343
bvi255	✓	720XP-96ZC2	4.24.2F	1.10.0	172.24.77.136	c0:d6:82:14:09:49	JAS19510049
bvi261	✓	720XP-96ZC2	4.24.2F	1.10.0	172.24.77.91	c0:d6:82:14:01:8d	JAS19510033
in332	✓	7304	4.23.2F	1.7.6	172.30.150.117	00:1c:73:9c:35:fb	HSH14365087
in511	ⓘ	7304	4.24.2F	1.10.0	172.30.155.176	44:4c:a8:30:21:0a	HSH15515472
in512	ⓘ	7304	4.24.2F	1.10.0	172.30.155.206	00:1c:73:ea:d7:2b	HSH15335091
roi251	✓	720XP-24ZY4	4.21.5F	1.7.7	172.30.191.85	74:83:ef:a1:a5:94	JAS18410016

Showing 8 of 183 rows (1 filter active)

2. Select **Onboard Devices** from the **Add Device** drop-down menu at the upper right corner of the **Inventory** screen.

   The system displays the Onboard Devices pop-up window.
3. Click the **Existing Device Registration** tab at the lower end of the **Onboard Devices** pop-up window.

   Figure 3-17: Existing Device Registration Tab



Onboard Devices

Status

This table shows all the device registrations from the last week.

Device	Request Time	Status

Register Devices

Streaming Telemetry will be configured and enabled on these devices, after which they will appear in the Undefined container.

Note: To view all devices, disable the **Show only inactive devices** option using the toggle button.

4. Select the required device.
5. Click **Register n Device(s)** where *n* is the count of selected devices.

   The system refreshes the selected device with new certificates, returns to the last provisioning state, and resumes streaming to CVP.

3.7.5 Re-ZTP On-Boarded Devices

Manual intervention is required to re-ZTP on-boarded devices after enabling the certificate-based TerminAttr authentication. This prevents unauthorized or malicious software from spoofing previously on-boarded devices.

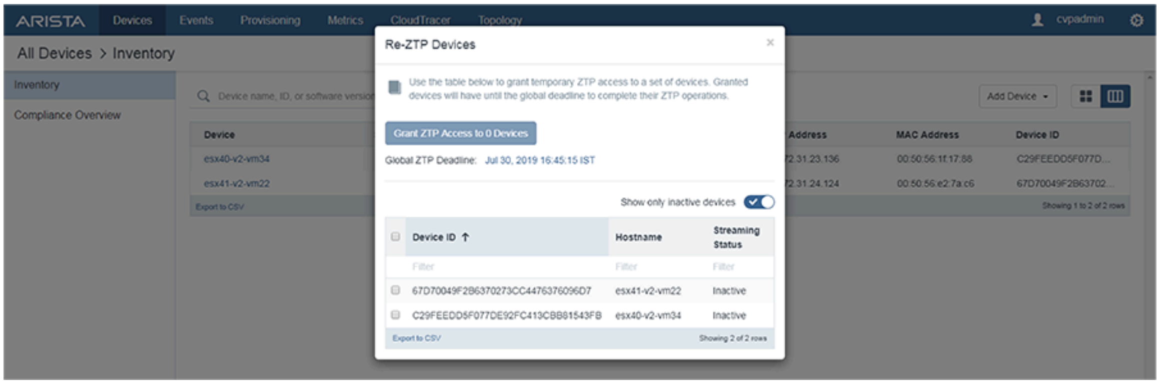
Perform the following steps to re-ZTP devices:

1. In CloudVision portal, click the **Devices** tab.

   The system displays the Inventory screen.
2. Select Re-ZTP Devices from the Add Device drop-down menu at the upper right corner of the Inventory screen.

   The system displays the Re-ZTP Devices pop-up window.

   Figure 3-18: Re-ZTP Devices Pop-Up Window



Use the table below to grant temporary ZTP access to a set of devices. Granted devices will have until the global deadline to complete their ZTP operations.

Global ZTP Deadline: Jul 30, 2019 16:45:15 IST

□	Device ID ↑	Hostname	Streaming Status
	Filter	Filter	Filter
□	67D70049F2B6370273CC4476376096D7	esx41-v2-vm22	Inactive
□	C29FEEDD5F077DE92FC413CBB81543FB	esx40-v2-vm34	Inactive

Note: To view all devices, disable the Show only inactive devices option using the toggle button.

3. Select the required device.
4. (Optional) Click the time next to Global ZTP Deadline and configure the preferred time to re-ZTP selected devices.
5. Click **Grant ZTP Access to *n* Device(s)** where n is the count of selected devices.

   Devices must complete their re-ZTP before the enrollment window closes.

3.8 NAT Support

CloudVision cluster can be deployed behind a network address translation (NAT) box in which a different public IP address is exposed towards devices streaming to the cluster. The devices can only reach the CloudVision cluster via the public NAT IP. Enabling the feature involves assigning the NAT public IP address to the nodes.

Related topics:

- NAT Support Pre 2021.3.0
- NAT Support Post 2021.3.0

- Known Caveats

3.8.1 NAT Support Pre 2021.3.0

Add the `interfaces/eth0/nat_ip_address` parameter in the configuration while installing the cluster. The interface name can be Ethernet interface(eth0, eth1, eth2, ...). The internal IP addresses are assigned in the ip_address field (marked in bold).

```
node1:
  default_route: 172.XX.XX.X
  hostname: dummy.comNAT
  interfaces:
    eth0:
      ip_address: 172.XX.XX.XXX
      netmask: 255.XX.XX.XX
  interfaces/eth0/nat_ip_address: 172.XX.XX.X (Public NAT IP)
node2:
  default_route: 172.XX.XX.X
  hostname: dummy.com
  interfaces:
    eth0:
      ip_address: 172.XX.XX.XXX
      netmask: 255.XX.XX.XX
  interfaces/eth0/nat_ip_address: 172.XX.XX.X
node3:
  default_route: 172.XX.XX.X
  hostname: dummy.com
  interfaces:
    eth0:
      ip_address: 172.XX.XX.XXX
      netmask: 255.XX.XX.XX
  interfaces/eth0/nat_ip_address: 172.XX.XX.X
```

3.8.2 NAT Support Post 2021.3.0

Add interfaces/eth0/nat_ip_address parameter in the configuration while installing the cluster. The interface name can be Ethernet interface(eth0, eth1, eth2, ...). The internal Ip addresses are assigned in the ip_address field.

This can be configured via the CVP Shell using the NAT IP address prompt.

CVP Installation Menu

```
[root@localhost ~]# su cvpadmin

CVP Installation Menu
────────────────────────────────────
[q]uit [p]rint [s]inglenode [m]ultinode [r]eplace [u]pgrade
>s
Enter the configuration for CloudVision Portal and apply it when done.
Entries marked with '*' are required.

Common Configuration:
────────────────────────────────────
  CloudVision Deployment Model [d]efault [w]ifi_analytics: d
  DNS Server Addresses (IPv4 Only): 172.22.22.40
  DNS Domain Search List: sjc.aristanetworks.com, ire.aristanetworks.com
  Number of NTP Servers: 1
  NTP Server Address (IPv4 or FQDN) #1: ntp.aristanetworks.com
  Cluster Interface Name: eth0
  Device Interface Name: eth0
  CloudVision WiFi Enabled: no
 *Enter a private IP range for the internal cluster network (overlay):
 10.42.0.0/16
 *FIPS mode: no

Node Configuration:
 ─────────────────────────────────────────────
 *Hostname (FQDN): cvp80.sjc.aristanetworks.com
 *IP Address of eth0: 172.31.0.168
 *Netmask of eth0: 255.255.0.0
  NAT IP Address of eth0:
 *Default Gateway: 172.31.0.1
  DNS Domain Search List:
  Number of NTP Servers:
  Number of static Routes:
  TACACS Server IP Address:

Singlenode Configuration Menu
────────────────────────────────────────────
[q]uit [p]rint [e]dit [v]erify [s]ave [a]pply [h]elp ve[r]bose
```

Singlenode Configuration Menu

```
Singlenode Configuration Menu
────────────────────────────────────────────
[q]uit [p]rint [e]dit [v]erify [s]ave [a]pply [h]elp ve[r]bose
>p
common:
  cluster_interface: eth0
  cv_wifi_enabled: 'no'
  deployment_model: DEFAULT
  device_interface: eth0
  dns:
  - 8.8.8.8
```

3.8.3 Known Caveats

When CVP is behind NAT and some of their devices are in the same network as CVP and some outside, this feature may not work.

When both the device and the CVP cluster are inside the same NAT network, configuring TerminAttr (TA) on the devices to reach the cluster’s public NAT IP address may not work in all cases. (This will depend on how NAT is configured.)

Chapter 4

CloudVision as-a-Service

CloudVision as-a-Service is an Arista-managed, multi-tenant cloud service deployed in tier one public cloud providers. CloudVision as-a-Service features include secure state-streaming and analytics on top of an Arista managed multi-tenant scale-out architecture. Customers are assigned to a unique organization (tenant) in a specific region. All devices and users of that customer are part of this organization. Organizations are isolated from each other and a user in one organization cannot access any data from other organizations. Authentication is tied to the customer's AAA provider. CloudVision as-a-Service provides device provisioning workflows and state streaming.

Sections in this chapter include:

- Prerequisites
- Onboarding Procedures
- AAA Providers

4.1 Prerequisites

Verify the following requirements before installing CloudVision as-a-Service.

- Software Requirements
- Connectivity Requirements
- Authentication Requirements

4.1.1 Software Requirements

Minimum software requirements are:

- EOS 4.20 or newer
- TerminAttr 1.19.5 or newer

4.1.2 Connectivity Requirements

EOS devices need to be able to connect to arista.io on port 443 (apiserver.arista.io:443).

Note: CloudVision as-a-Service only needs port 443 to be opened to initiate a secure connection to an EOS device.

To verify proper connectivity to apiserver.arista.io:443 use the following commands:

1. Verify proper DNS resolution.

```
switch#bash nslookup apiserver.arista.io
```

Note: If this is unsuccessful please check your DNS server configuration. If no DNS servers are available, add the `ip name-server` configuration as follows:

```
switch(config)# ip name-server 8.8.8.8
```

2. Verify connectivity to CloudVision Service using the `curl` command:

```
switch# bash
```

```
[admin@switch]$ curl apiserver.arista.io:443
curl: (52) Empty reply from server
```

If multiple VRFs are configured, first change the VRF context:

```
switch# bash
[admin@switch]$ sudo ip netns exec ns-MGMT curl apiserver.arista.io:443
```

4.1.3 Authentication Requirements

CloudVision as-a-Service supports OAuth 2.0 for authorization. OAuth is one of the most common methods used to pass authorization from a single sign-on (SSO) service to another cloud application. While there are many OAuth providers in the market today, CloudVision as-a-Service supports Google OAuth, OneLogin, Okta & Microsoft Azure AD.

Note that CloudVision as-a-Service is transparent to 3rd party MFA (Multi-Factor Authentication) Providers. As long as the customer is using one of the above listed OAuth Providers for identity management, CloudVision Service should be able to authorize against that OAuth provider.

Authentication options:

- Using Google OAuth or Microsoft Azure AD
- Not using Google OAuth or Microsoft Azure AD
- AAA Providers

4.1.3.1 Using Google OAuth or Microsoft Azure AD

Only admin email addresses are required when using Google OAuth or Azure AD as a provider. Select the **Sign in with Google** or **Sign in with Microsoft** link at: https://www.arista.io/cv

4.1.3.2 Not using Google OAuth or Microsoft Azure AD

If you are using Okta, OneLogin, or another OAuth Provider, the following information is required to onboard CloudVision as-a-Service:

- OAuth Endpoint
- ClientID
- ClientSecret

Refer to the respective OAuth Provider documentation for information about obtaining this information.

Your OneLogin or Okta administrator will use this information to add CloudVision to their authorized applications and adjust user permissions to allow access to the service. If you experience any OAuth errors, open an Arista TAC support request for assistance. Provide a the full URL and a screen capture of the output,

Note: Email IDs are case sensitive when used for CloudVision Service login. If the case is First.Last@company.com, it will need to match exactly to the CloudVision Service login.

Once the CloudVision Service account is set up, an Invitation URL will be provided by Arista to login to the CloudVision Service.

For further onboarding procedures see Onboarding Authentication Providers.

4.2 Onboarding Procedures

This section contains:

- Onboarding Authentication Providers
- Onboarding Devices: Token-Based Authentication

- Subscribing to CloudVision as-a-Service updates

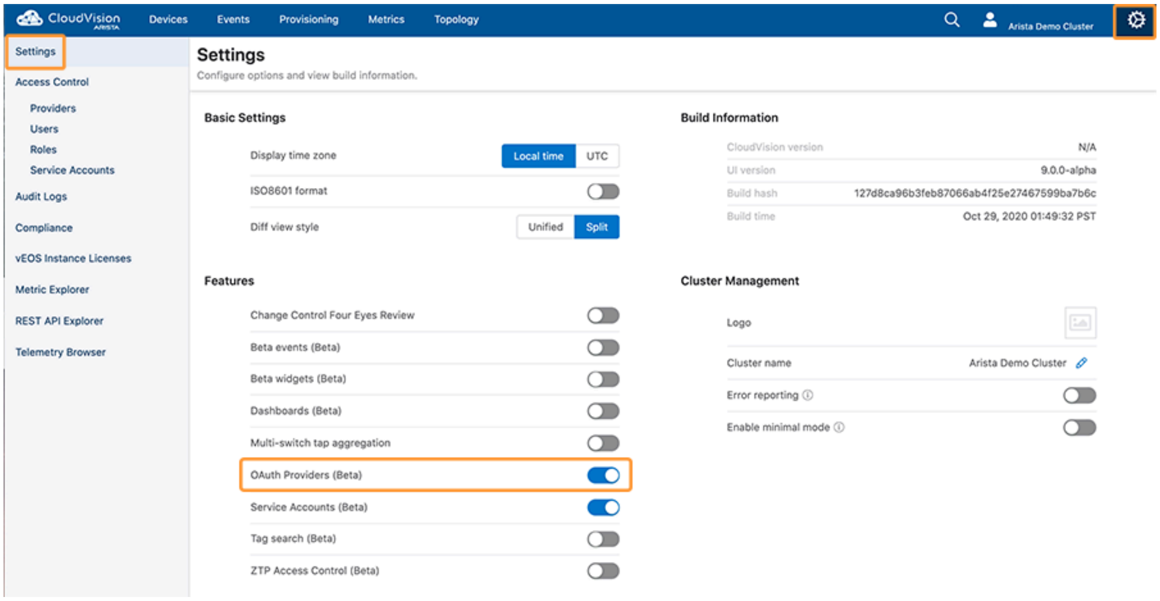
4.2.1 Onboarding Authentication Providers

Once the CloudVision as-a-Service instance is set up, use the following procedure to add a preferred authentication provider.

To add a preferred authentication provider:

1. Navigate to **Settings** using the gear icon. Verify under the **Features** section **OAuth Providers** is toggled on.

   Figure 4-1: OAuth Providers



Settings

Configure options and view build information.

Basic Settings

Display time zone	Local time / UTC
ISO8601 format	
Diff view style	Unified / Split

Build Information

CloudVision version	N/A
UI version	9.0.0-alpha
Build hash	127d8ca96b3feb87066ab4f25e27467599ba7b6c
Build time	Oct 29, 2020 01:49:32 PST

Features

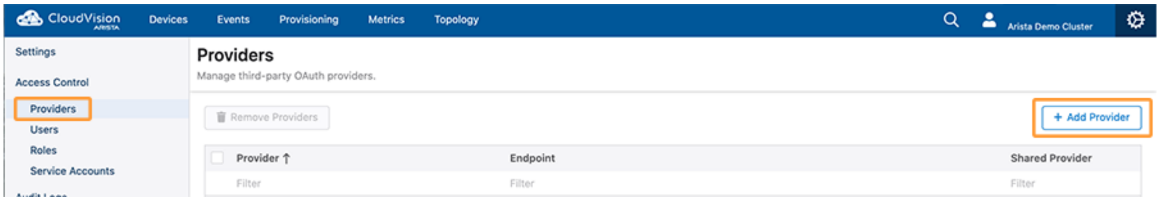
- Change Control Four Eyes Review
- Beta events (Beta)
- Beta widgets (Beta)
- Dashboards (Beta)
- Multi-switch tap aggregation
- OAuth Providers (Beta)
- Service Accounts (Beta)
- Tag search (Beta)
- ZTP Access Control (Beta)

Cluster Management

Logo	
Cluster name	Arista Demo Cluster
Error reporting	
Enable minimal mode	

2. Navigate to **Access Control** and then **Providers**. To add a new authentication provider, click the 'Add Provider' button.

   Figure 4-2: Add Provider



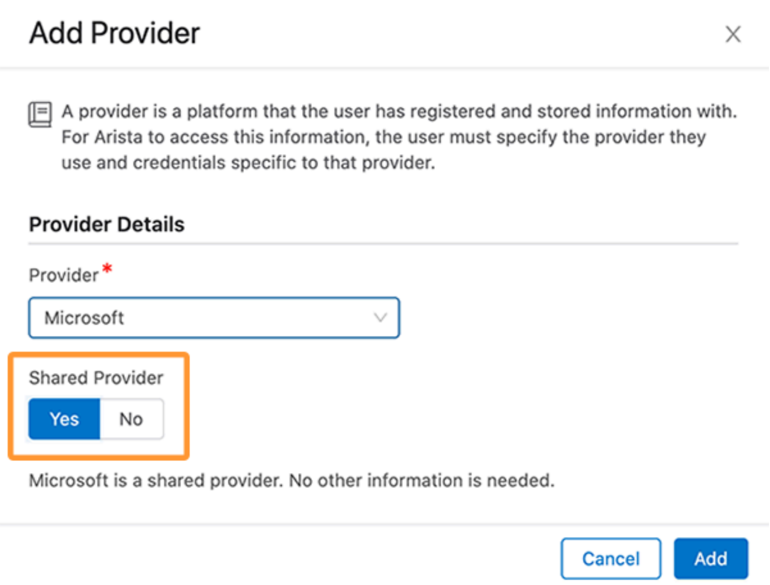
Providers

Manage third-party OAuth providers.

Provider ↑	Endpoint	Shared Provider
Filter	Filter	Filter

3. Select a provider that your organization uses.

Figure 4-3: Shared Provider



Add Provider

A provider is a platform that the user has registered and stored information with. For Arista to access this information, the user must specify the provider they use and credentials specific to that provider.

Provider Details

Provider*: Microsoft

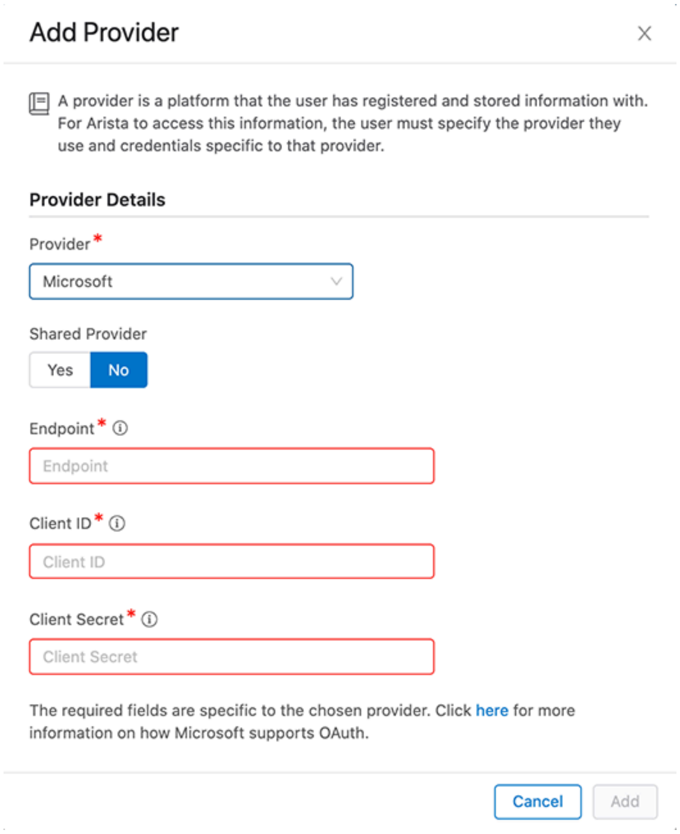
Shared Provider: [✓ Yes] No

Microsoft is a shared provider. No other information is needed.

Note that currently Google and Microsoft are supported as a Shared Providers. Shared Providers use an Arista-provided set of credentials so no other information is required from the customer for the onboarding.

Other providers are currently supported as non-shared providers. Additional required form fields will appear upon selecting these providers. These fields will need to be filled out with credentials specific to your account with that provider.

Figure 4-4: Non-shared Provider



Add Provider

A provider is a platform that the user has registered and stored information with. For Arista to access this information, the user must specify the provider they use and credentials specific to that provider.

Provider Details

Provider*: Microsoft

Shared Provider: Yes [✓ No]

Endpoint*: Endpoint

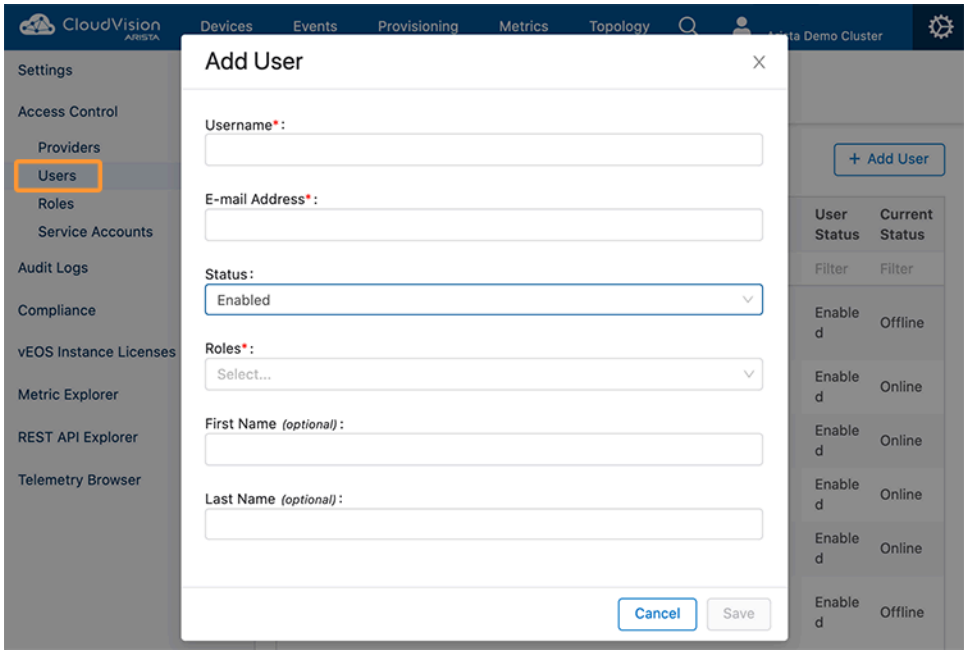
Client ID*: Client ID

Client Secret*: Client Secret

The required fields are specific to the chosen provider. Click here for more information on how Microsoft supports OAuth.

4. Saving the provider will send a registration request to the CloudVision Service backend along with the related information.
5. Once the authentication provider is set up, make sure to add the admin email address and verify the login process before the Invitation URL expires. To add a user account navigate to **Users** and then the **Add User** screen.

Figure 4-5: Add User



Username*:

E-mail Address*:

Status: Enabled

Roles*: Select...

First Name (optional):

Last Name (optional):

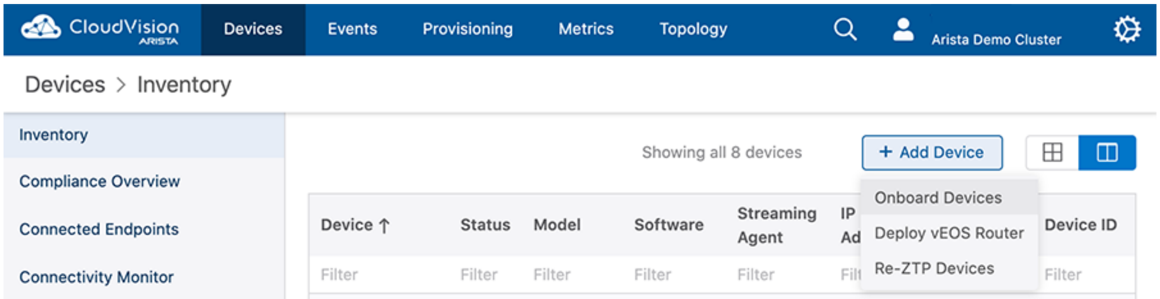
User Status	Current Status
Filter	Filter
Enabled	Offline
Enabled	Online
Enabled	Online
Enabled	Online
Enabled	Online
Enabled	Offline

4.2.2 Onboarding Devices: Token-Based Authentication

To onboard the devices using token-based authentication.

1. To onboard the devices navigate to **Devices** and then **Inventory** and then **Add Devices** and then **Onboard Devices.**

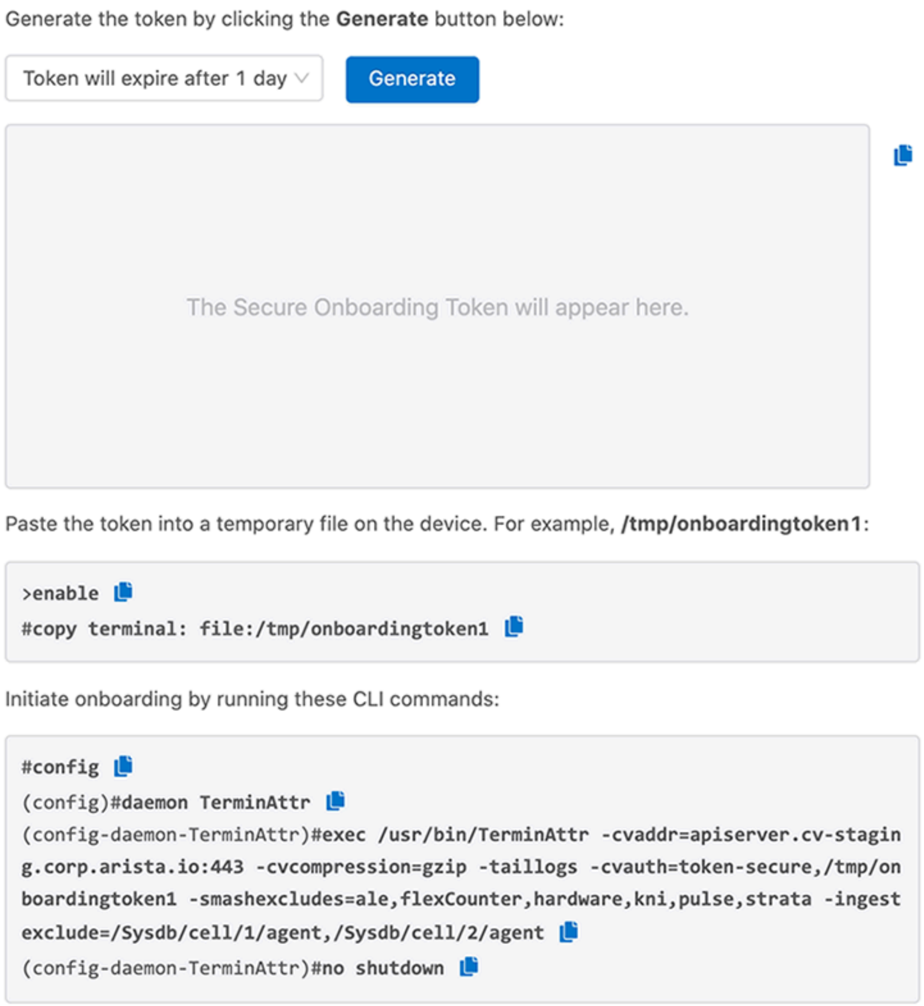
Figure 4-6: Onboarding Devices



2. Details on how to create a token, and using that token to onboard the devices are listed under the **Onboard Devices**. Please follow the directions to create a token and onboard your devices to CloudVision Service.

Note: You can use the same token to onboard multiple devices. CloudVision Service will use the device serial number to identify a device.

Figure 4-7: Onboarding Devices



Generate the token by clicking the **Generate** button below:

Token will expire after 1 day
Generate
The Secure Onboarding Token will appear here.

Paste the token into a temporary file on the device. For example, **/tmp/onboardingtoken1**:

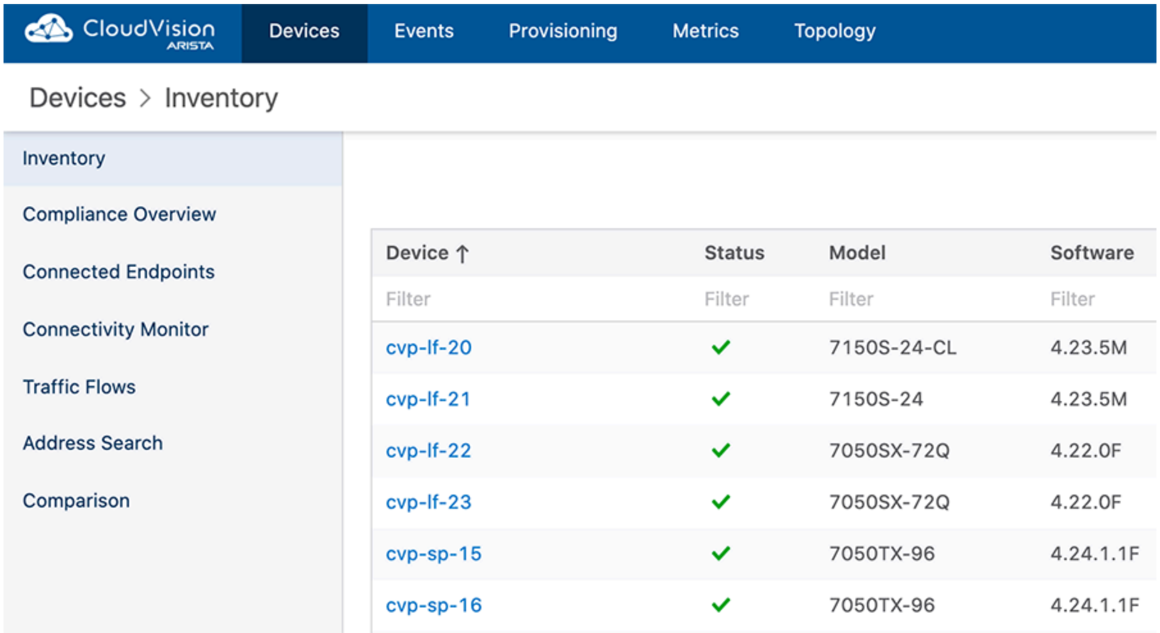
```
>enable
#copy terminal: file:/tmp/onboardingtoken1
```

Initiate onboarding by running these CLI commands:

```
#config
(config)#daemon TerminAttr
(config-daemon-TerminAttr)#exec /usr/bin/TerminAttr -cvaddr=apiserver.cv-stagin
g.corp.arista.io:443 -cvcompression=gzip -taillogs -cvauth=token-secure,/tmp/on
boardingtoken1 -smashexcludes=ale,flexCounter,hardware,kni,pulse,strata -ingest
exclude=/Sysdb/cell/1/agent,/Sysdb/cell/2/agent
(config-daemon-TerminAttr)#no shutdown
```

3. Once you successfully onboard the devices you should be able to see them under the **Devices** tab.

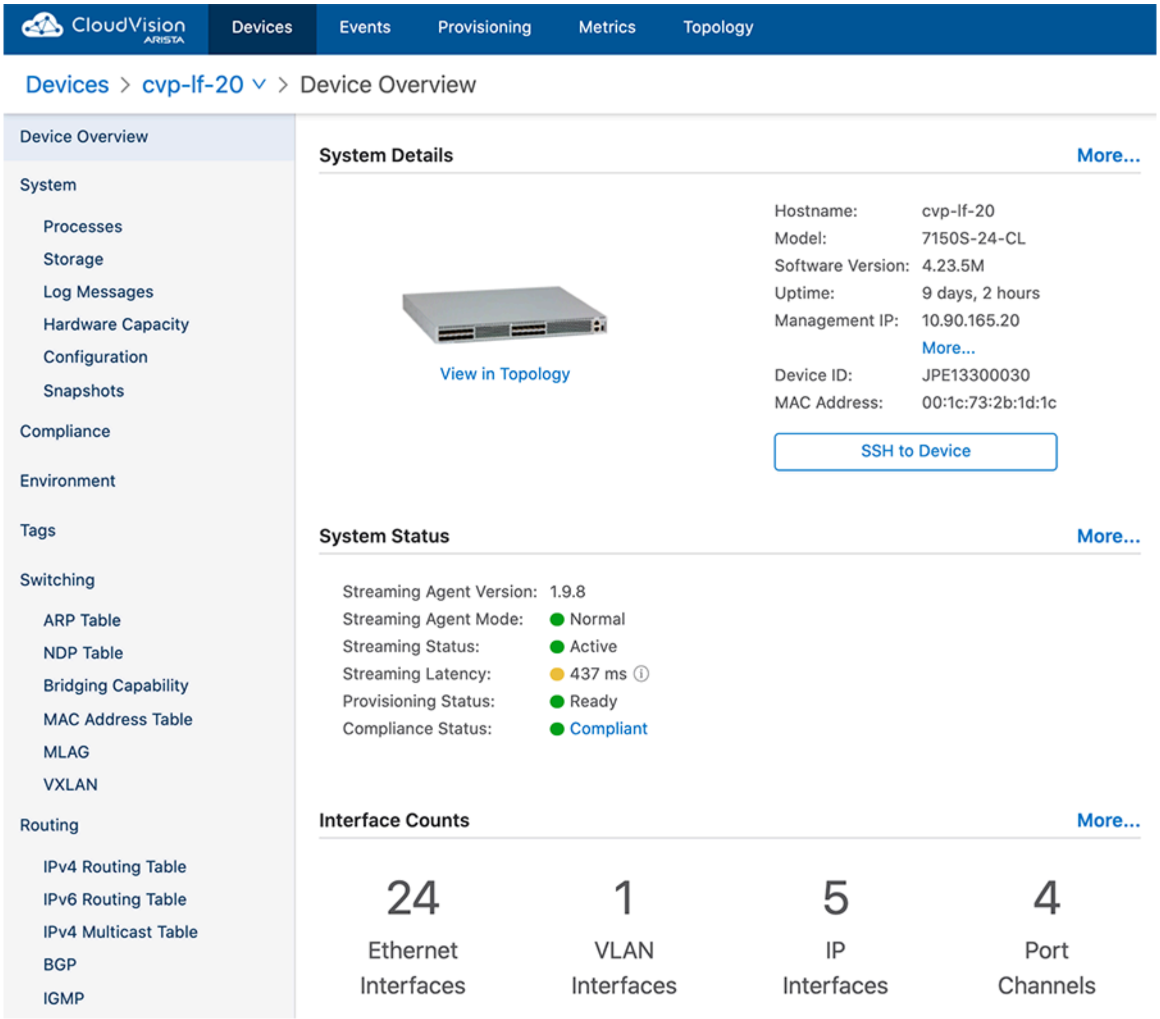
Figure 4-8: Device Inventory Screen



Device ↑	Status	Model	Software
Filter	Filter	Filter	Filter
cvp-lf-20	✓	7150S-24-CL	4.23.5M
cvp-lf-21	✓	7150S-24	4.23.5M
cvp-lf-22	✓	7050SX-72Q	4.22.0F
cvp-lf-23	✓	7050SX-72Q	4.22.0F
cvp-sp-15	✓	7050TX-96	4.24.1.1F
cvp-sp-16	✓	7050TX-96	4.24.1.1F

4. Click on the wrench icon (#) to provision the device. This will take you to the device-specific page. Select the **Device Overview** tab and then select **Provision Device** to provision the device in CloudVision Service.

Figure 4-9: Device Overview



System Details

Hostname: cvp-lf-20
Model: 7150S-24-CL
Software Version: 4.23.5M
Uptime: 9 days, 2 hours
Management IP: 10.90.165.20
Device ID: JPE13300030
MAC Address: 00:1c:73:2b:1d:1c

System Status

Streaming Agent Version: 1.9.8
Streaming Agent Mode: ● Normal
Streaming Status: ● Active
Streaming Latency: ● 437 ms ⓘ
Provisioning Status: ● Ready
Compliance Status: ● Compliant

Interface Counts

24 Ethernet Interfaces
1 VLAN Interfaces
5 IP Interfaces
4 Port Channels

Note: Prior to **Provision Device** make sure the user account exists in the EOS device. For example:

Assuming john.smith@company.com is the email address used for OAuth authentication you need to have john.smith as a user (for Arista Demo you will need to use

```
username@arista.com):
sw(config)#username john.smith privilege 15 <nopassword/secret>
```

If you have TACACS+ configured for authentication, in order for CloudVision as-a-Service to properly provision the device, the exact user account should already exist in the TACACS+ Server.

If you have a Radius server for EOS authentication, you need to add the `--disableaaa` argument into the TerminaAttr config.

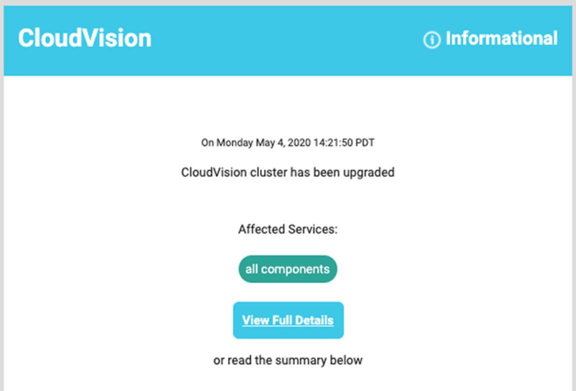
For additional information on migrating an EOS device with a TACACS+/Radius authentication to the CloudVision Service, please refer to Authentication Prerequisites.

4.2.3 Subscribing to CloudVision as-a-Service updates

You can monitor CloudVision Service live status through *https://status.arista.io* . You can also subscribe to CloudVision Service notification via email/text using **Subscribe to CloudVision**.

Following are informational and disruption notification examples you would get after subscribing to CloudVision Service updates:

Figure 4-10: Informational Notification



On Monday May 4, 2020 14:21:50 PDT

CloudVision cluster has been upgraded

Affected Services:

or read the summary below

4.3 AAA Providers

Authentication And Authorization (AAA) Providers create and log in to CloudVision through any provider. The OAuth and SAMLproviders are pre-configured and require additional information to create the provider.

The following sections describe procedures to configure AAA providers:

1. Requirements
2. Setting up an OAuth/SAML Provider in CloudVision
3. Setting up CloudVision with Identity Provider
4. Logging in with a Provider
5. Adding Launchpad as a Provider

4.3.1 Requirements

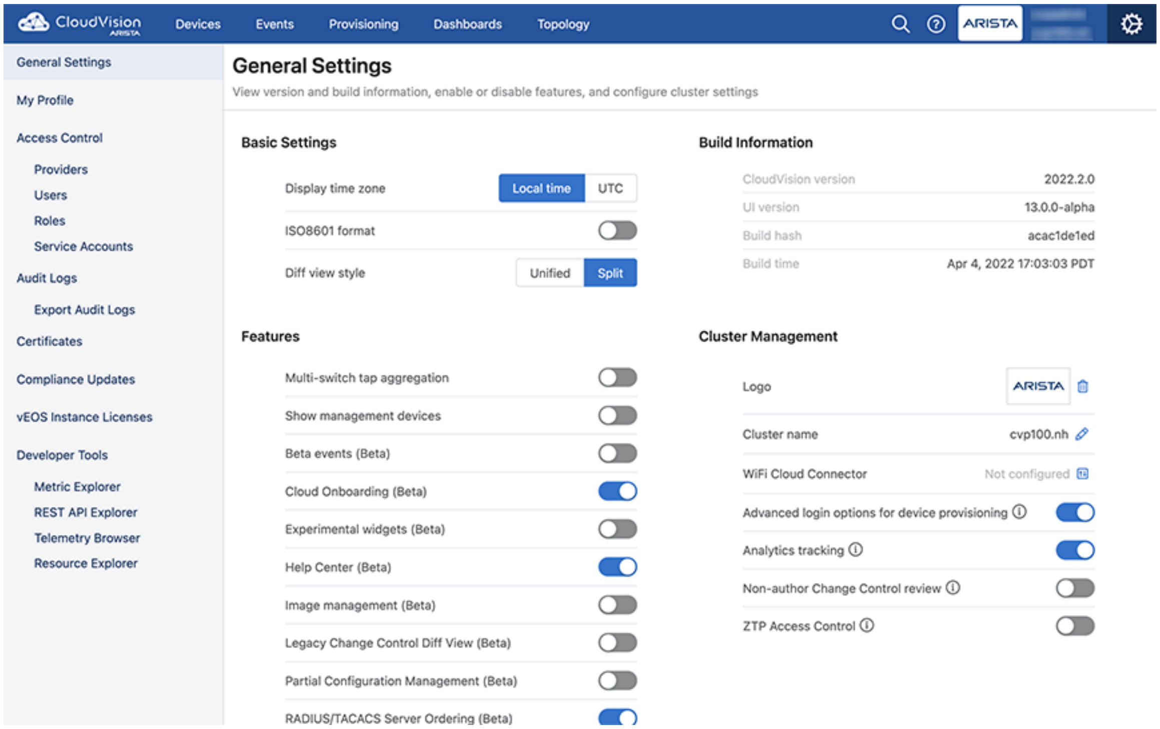
Pre-requisites:

- The device must have internet access.
- To create the OAuth or SAML provider, you must be registered with and have access to the Service Provider (SP) credentials.

Perform the following steps to create and edit SAML Providers:

1. Click on the gear icon.

Figure 4-11: General Settings Screen



General Settings

View version and build information, enable or disable features, and configure cluster settings

Basic Settings

Display time zone	[✓ Local time] UTC
ISO8601 format	○
Diff view style	Unified [✓ Split]

Build Information

CloudVision version	2022.2.0
UI version	13.0.0-alpha
Build hash	acac1de1ed
Build time	Apr 4, 2022 17:03:03 PDT

Features

Multi-switch tap aggregation	○
Show management devices	○
Beta events (Beta)	○
Cloud Onboarding (Beta)	●
Experimental widgets (Beta)	○
Help Center (Beta)	●
Image management (Beta)	○
Legacy Change Control Diff View (Beta)	○
Partial Configuration Management (Beta)	○
RADIUS/TACACS Server Ordering (Beta)	●

Cluster Management

Logo	ARISTA
Cluster name	cvp100.nh
WiFi Cloud Connector	Not configured
Advanced login options for device provisioning	●
Analytics tracking	●
Non-author Change Control review	○
ZTP Access Control	○

2. On the General Settings page, under **Features**, enable **SAML Providers (Beta)** using the toggle button.

4.3.2 Setting up an OAuth and SAML Providers in CloudVision

You can setup an OAuth or SAML provider in CloudVision through the **Providers** screen. To open the **Providers** screen, click on the gear icon and navigate to **Access Control** > **Providers**. This screen lists current registered OAuth and SAML providers in corresponding tables and provides the following functionalities:

- Adding OAuth Providers
- Adding SAML Providers
- Removing OAuth Providers
- Removing SAML Providers

Note: The **Shared Provider** column lists the providers where Arista has a special account for CloudVision-as-a-Service (CVaaS).

4.3.2.1 Adding OAuth Providers

Pre-requisites:

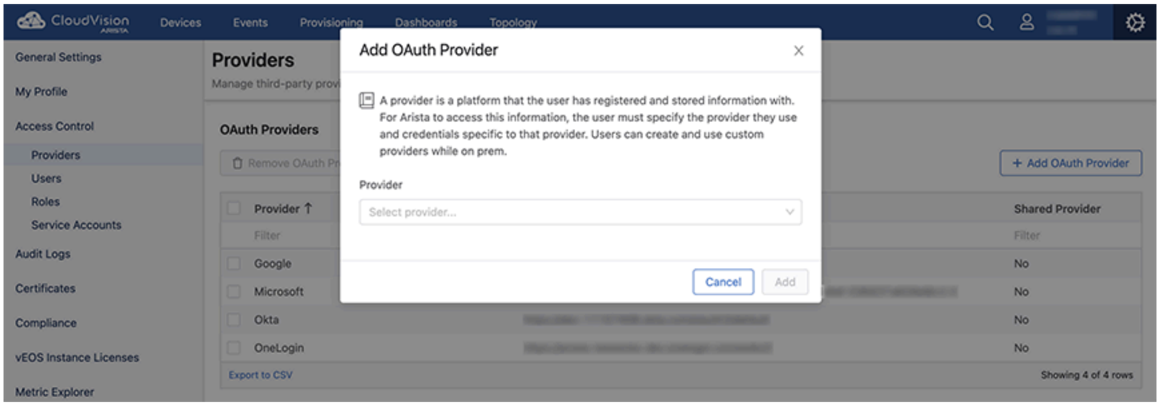
- Shared providers does not require the additional information like endpoint, client ID, and client secret. This functionality is not supported on-prem or on the custom providers.
- The link at the bottom of the **Add OAuth Providers** window explains how the selected provider uses OAuth and where you can find the information required by the form.
- You can use the **Custom OAuth** option if your provider is not listed under the **Provider** drop-down menu.

Perform the following steps to add an OAuth provider:

1. Click the **+ Add OAuth Provider** tab.

The system opens the **Add OAuth Provider** screen.

Figure 4-12: Add OAuth Provider Screen



Providers

Manage third-party prov

OAuth Providers

Provider ↑		Shared Provider
Filter		Filter
Google		No
Microsoft	[redacted]	No
Okta	[redacted]	No
OneLogin	[redacted]	No

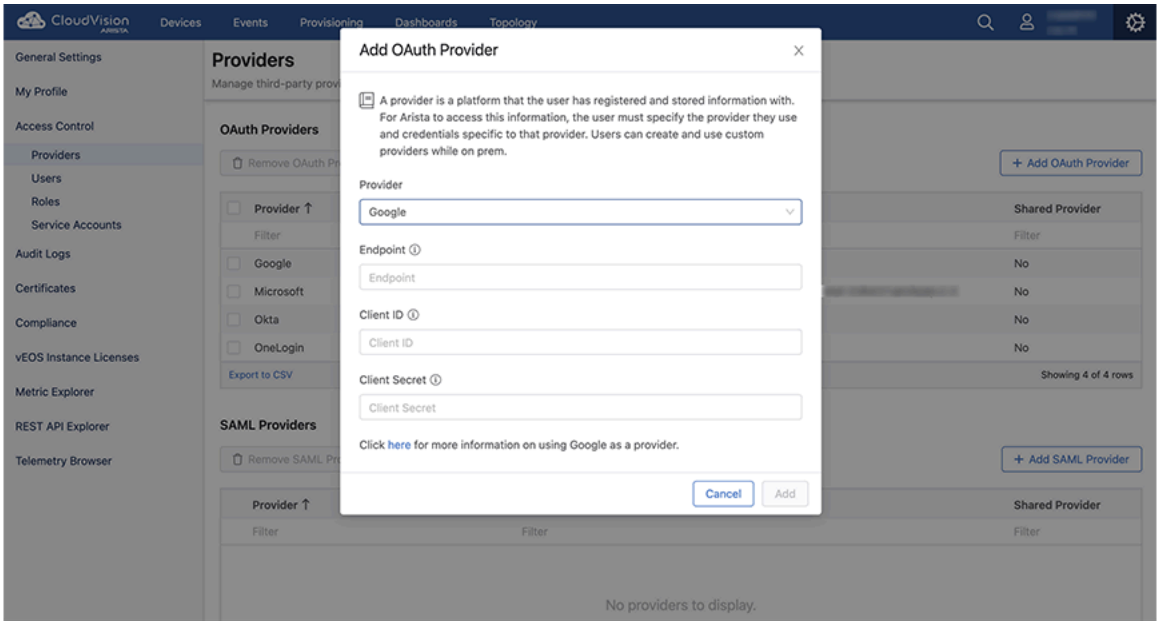
Add OAuth Provider ×

A provider is a platform that the user has registered and stored information with. For Arista to access this information, the user must specify the provider they use and credentials specific to that provider. Users can create and use custom providers while on prem.

Provider: Select provider...

2. Select the required OAuth provider from the **Provider** drop-down menu.

Figure 4-13: Add OAuth Provider Screen to Configure a Provider



Providers

Manage third-party prov

OAuth Providers

Provider ↑		Shared Provider
Filter		Filter
Google		No
Microsoft	[redacted]	No
Okta		No
OneLogin		No

SAML Providers

Provider ↑		Shared Provider
Filter	Filter	Filter

No providers to display.

Add OAuth Provider ×

A provider is a platform that the user has registered and stored information with. For Arista to access this information, the user must specify the provider they use and credentials specific to that provider. Users can create and use custom providers while on prem.

Provider: Google

Endpoint ⓘ: Endpoint

Client ID ⓘ: Client ID

Client Secret ⓘ: Client Secret

Click here for more information on using Google as a provider.

3. In the **Endpoint** field, type the provider URL where the Client ID and Client Secret are used to authorize the client.
4. In the **Client ID** field, type the unique public identifier the provider assigns to the client at the time of registration.
5. In the **Client Secret** field, type the unique private identifier the provider assigns to the client at the time of registration.
6. Click **Add**.

   The system registers the new OAuth provider and lists it in the OAuth providers table.

4.3.2.2 Adding SAML Providers

Pre-requisites:

- The link at the bottom of the **Add SAML Providers** window explains how the selected provider uses SAML and where you can find the information required by the form. The only provider that does not have this information is Launchpad.

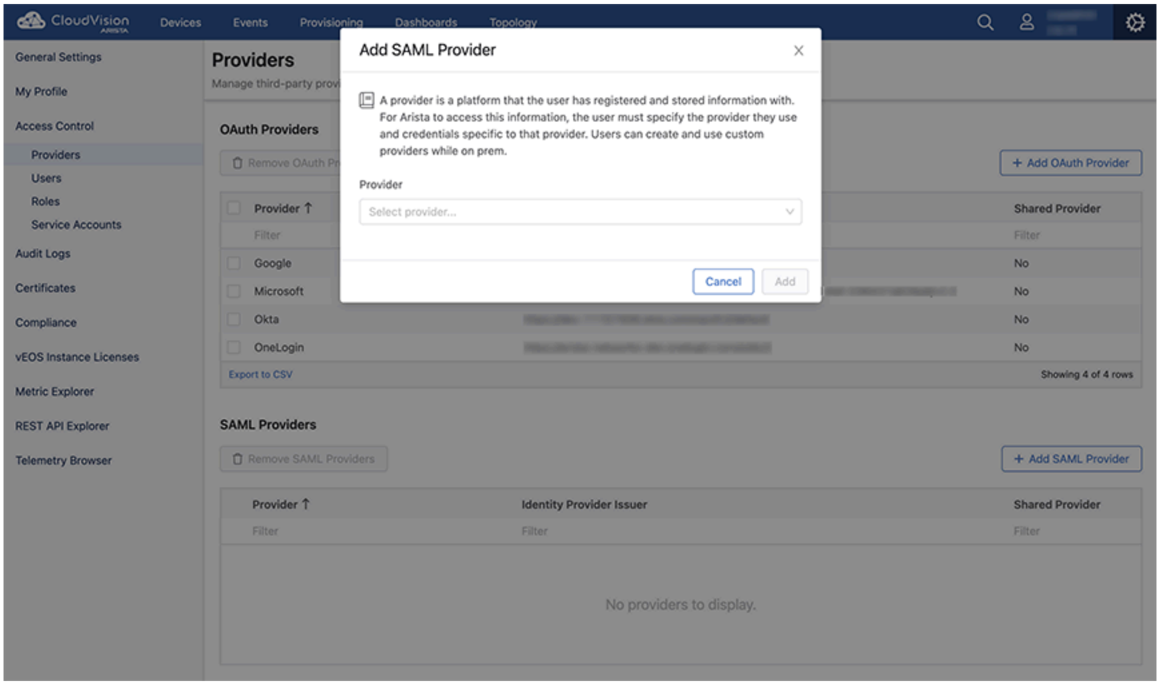
- You can use the **Custom SAML** option if your provider is not listed under the **Provider** drop-down menu.

Perform the following steps to add an SAML provider:

1. Click the **+ Add SAML Provider** tab.

   The system opens the **Add SAML Provider** window.

   Figure 4-14: Add SAML Provider Screen



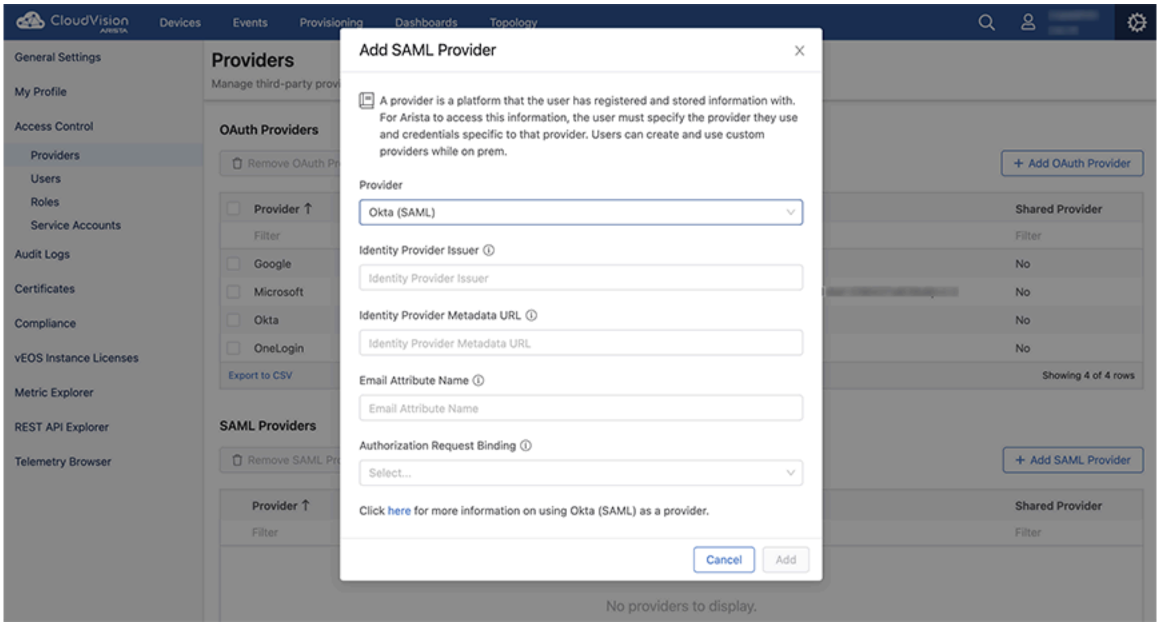
Add SAML Provider

A provider is a platform that the user has registered and stored information with. For Arista to access this information, the user must specify the provider they use and credentials specific to that provider. Users can create and use custom providers while on prem.

Provider: Select provider...

2. Select the required SAML provider from the **Provider** drop-down menu.

   Figure 4-15: Add SAML Provider Screen to Configure a Provider



Add SAML Provider

A provider is a platform that the user has registered and stored information with. For Arista to access this information, the user must specify the provider they use and credentials specific to that provider. Users can create and use custom providers while on prem.

Provider: Okta (SAML)

Identity Provider Issuer: Identity Provider Issuer

Identity Provider Metadata URL: Identity Provider Metadata URL

Email Attribute Name: Email Attribute Name

Authorization Request Binding: Select...

Click here for more information on using Okta (SAML) as a provider.

3. In the **Identity Provider Issuer** field, type the Issuer or Entity ID.

   Note: An Issuer or Entity ID is a URL that uniquely identifies a SAML identity provider.

4. In the **Identity Provider Metadata URL** field, type the URL to fetch identity provider metadata.
5. In the **Email Attribute Name** field, type the attribute name for the email ID in SAML.
6. In the **Authorization Request Binding** field, select the protocol binding used for the SAML authentication request to the identity provider.
7. Click **Add**.

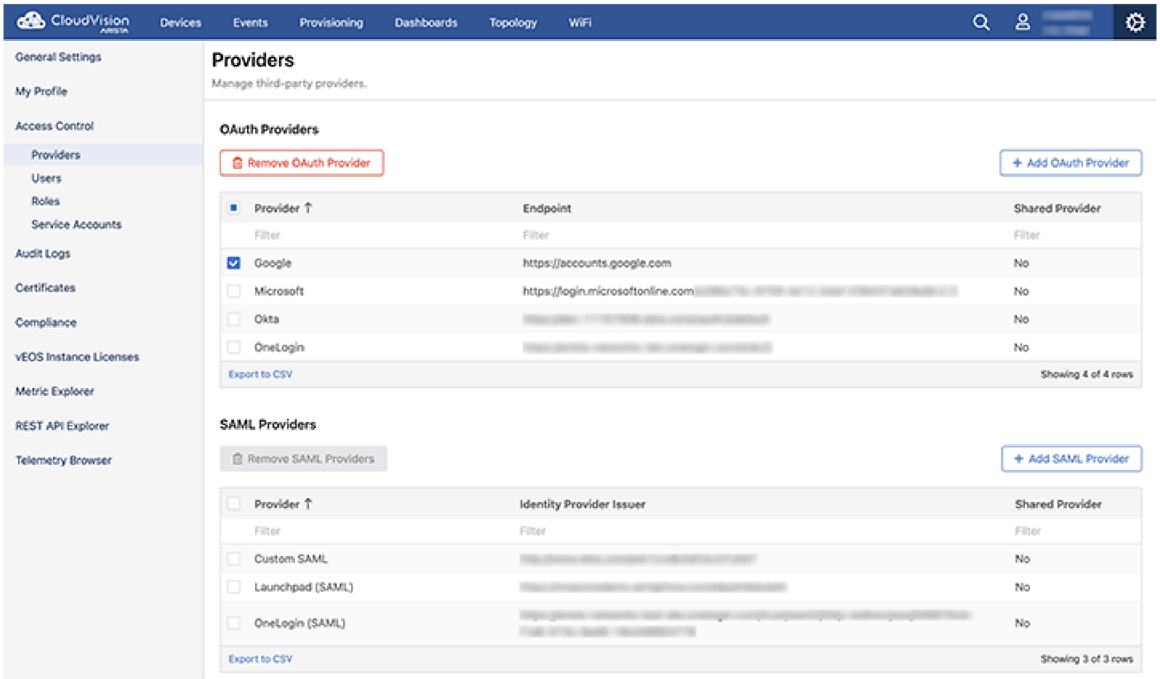
   The system registers the new SAML provider and lists it in the SAML providers table.

4.3.2.3 Removing OAuth Providers

Perform the following steps to remove an OAuth provider:

1. On the **Providers** screen, under **OAuth Providers**, select the redundant provider from the OAuth provider table.

   Figure 4-16: Removing OAuth Provider(s)



Providers

Manage third-party providers.

OAuth Providers

	Provider ↑	Endpoint	Shared Provider
	Filter	Filter	Filter
☑	Google	https://accounts.google.com	No
□	Microsoft	https://login.microsoftonline.com[redacted]	No
□	Okta	[redacted]	No
□	OneLogin	[redacted]	No

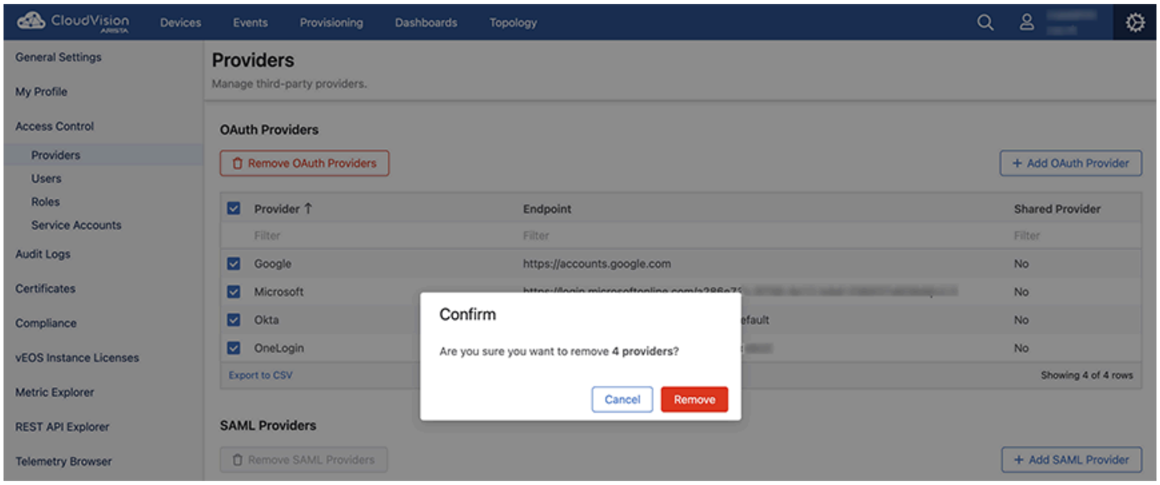
SAML Providers

□	Provider ↑	Identity Provider Issuer	Shared Provider
	Filter	Filter	Filter
□	Custom SAML	[redacted]	No
□	Launchpad (SAML)	[redacted]	No
□	OneLogin (SAML)	[redacted]	No

2. Click the **Remove OAuth Provider** button.

The system opens the **Confirm** screen.

Figure 4-17: Remove OAuth Provider(s) Confirm Screen



Providers

Manage third-party providers.

OAuth Providers

☑	Provider ↑	Endpoint	Shared Provider
	Filter	Filter	Filter
☑	Google	https://accounts.google.com	No
☑	Microsoft	https://login.microsoftonline.com/a286a7 [redacted]	No
☑	Okta	efault	No
☑	OneLogin	[redacted]	No

Showing 4 of 4 rows

SAML Providers

Confirm

Are you sure you want to remove **4 providers**?

3. Click **Remove** to confirm the removal.

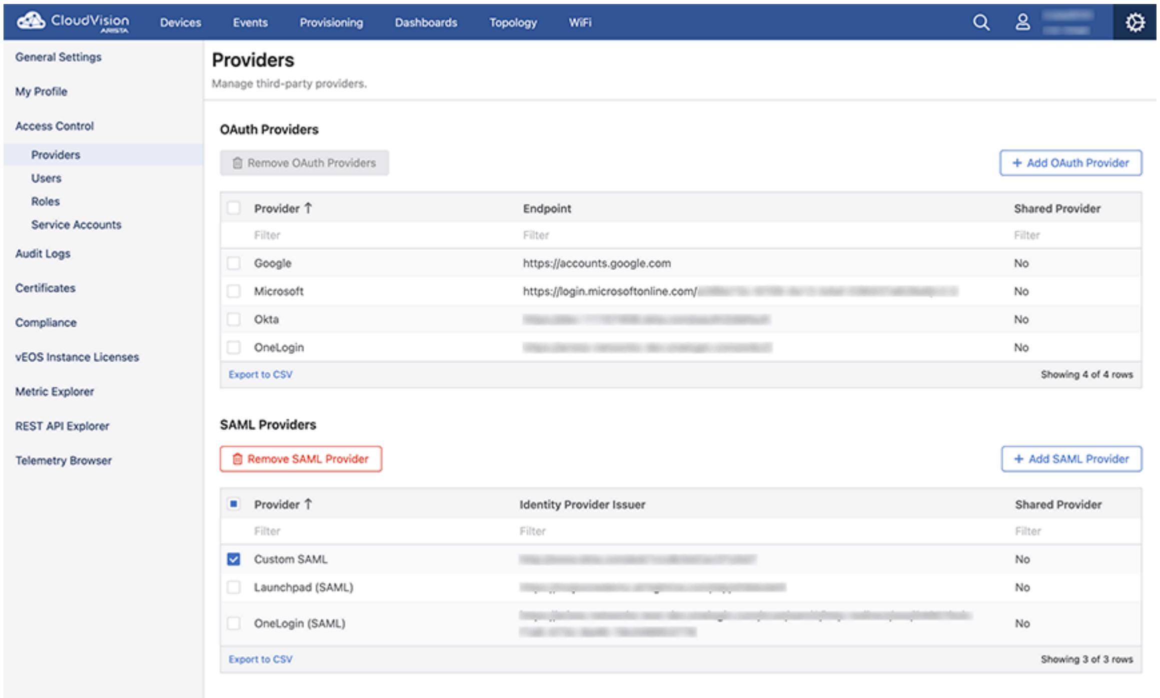
   The system permanently removes the OAuth provider.

4.3.2.4 Removing SAML Providers

Perform the following steps to remove an SAML provider:

1. On the **Providers** screen, under **SAML Providers**, select the redundant provider from the SAML provider table.

   Figure 4-18: Removing SAML Provider(s)



Providers

Manage third-party providers.

OAuth Providers

□	Provider ↑	Endpoint	Shared Provider
	Filter	Filter	Filter
□	Google	https://accounts.google.com	No
□	Microsoft	https://login.microsoftonline.com/[redacted]	No
□	Okta	[redacted]	No
□	OneLogin	[redacted]	No

Showing 4 of 4 rows

SAML Providers

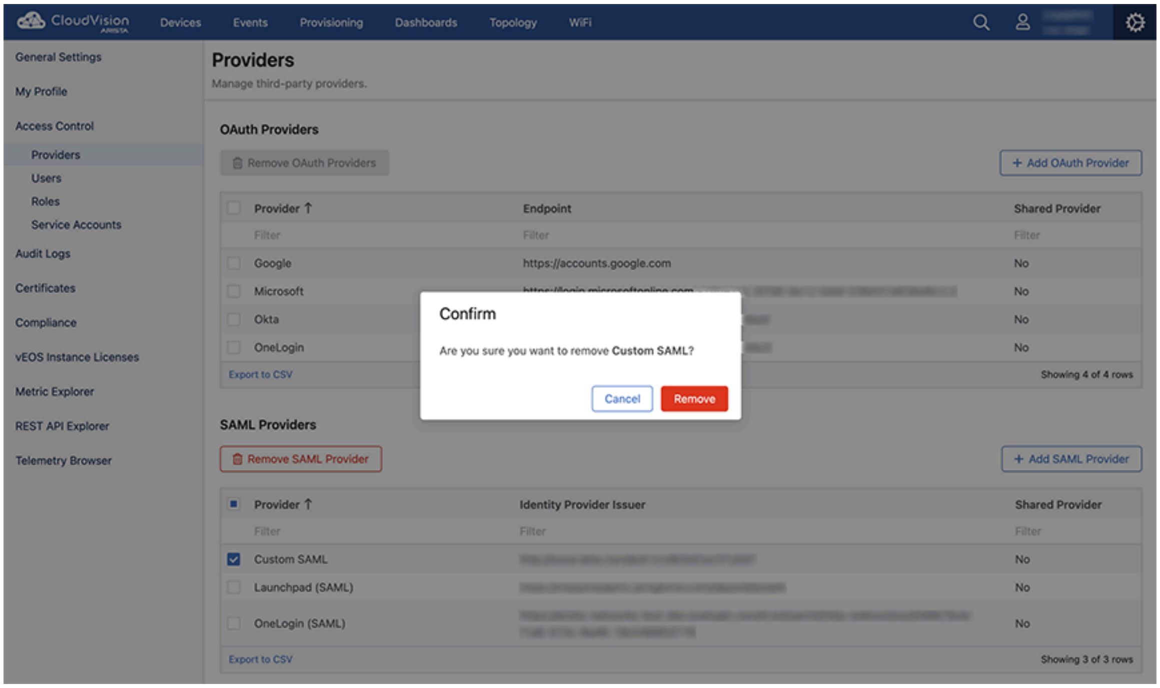
■	Provider ↑	Identity Provider Issuer	Shared Provider
	Filter	Filter	Filter
☑	Custom SAML	[redacted]	No
□	Launchpad (SAML)	[redacted]	No
□	OneLogin (SAML)	[redacted]	No

Showing 3 of 3 rows

2. Click the **Remove SAML Provider** button.

The system opens the **Confirm** screen.

Figure 4-19: Remove SAML Provider(s) Confirm Screen



Providers

Manage third-party providers.

OAuth Providers

□	Provider ↑	Endpoint	Shared Provider
	Filter	Filter	Filter
□	Google	https://accounts.google.com	No
□	Microsoft	https://login.microsoftonline.com [redacted]	No
□	Okta	[redacted]	No
□	OneLogin	[redacted]	No

Showing 4 of 4 rows

SAML Providers

■	Provider ↑	Identity Provider Issuer	Shared Provider
	Filter	Filter	Filter
☑	Custom SAML	[redacted]	No
□	Launchpad (SAML)	[redacted]	No
□	OneLogin (SAML)	[redacted]	No

Showing 3 of 3 rows

Confirm

Are you sure you want to remove **Custom SAML**?

3. Click **Remove** to confirm the removal.

   The system permanently removes the SAML provider.

4.3.3 Setting up CloudVision with Identity Provider

You must setup CloudVision with your Identity Provider.

For instructions on setting up CloudVision with identity providers, refer to the CloudVision as a Service (CVaaS) Quick Start Guide at https://www.arista.com/en/support/product-documentation or reference documentation at https://www.arista.com/en/support/toi/cvp-2021-2-0/14834-aaa-providers-oauth-and-saml-support.

4.3.4 Logging in Using SAML IDP

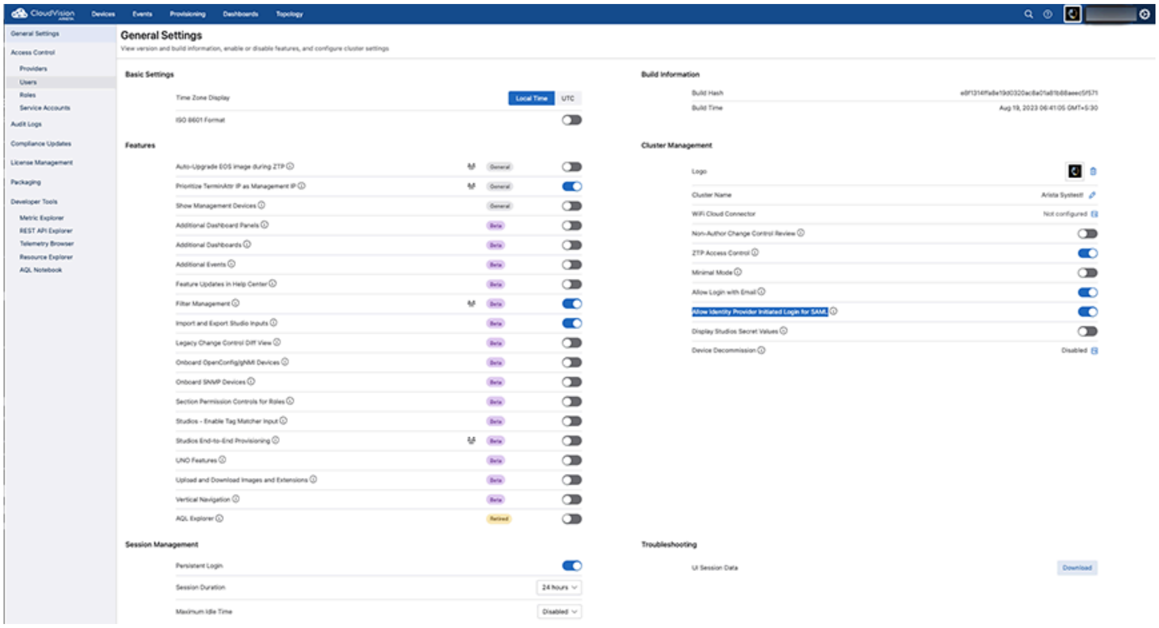
Starting with the 2023.2.0 release, you can login to CloudVision through an Identity Provider (IDP) instead of directly through the CloudVision application. When you log in to the IDP and your identity is verified, then, that verification process is used to access the CloudVision portal.

Note: This feature is available only for SAML providers and is disabled by default. When enabled, all CloudVision users of your organization can login to CloudVision through their SAML IDP.

Enabling SAML IDP Login

The SAML IDP initiaited login can be enabled in CloudVision portal by toggling (enabling) the **Allow Identity Provider Initiated Login for SAML** on **General Settings** > **Cluster Management** page as in the image below:

Figure 4-20: General Settings - SAML IDP Login Enable



General Settings

View version and build information, enable or disable features, and configure cluster settings

Basic Settings

Time Zone Display	[● Local Time] UTC
ISO 8601 Format	○

Features

Auto-Upgrade EOS image during ZTP ⓘ	General	○
Prioritize TerminAttr IP as Management IP ⓘ	General	●
Show Management Devices ⓘ	General	○
Additional Dashboard Panels ⓘ	Beta	○
Additional Dashboards ⓘ	Beta	○
Additional Events ⓘ	Beta	○
Feature Updates in Help Center ⓘ	Beta	○
Filter Management ⓘ	Beta	●
Import and Export Studio Inputs ⓘ	Beta	●
Legacy Change Control Diff View ⓘ	Beta	○
Onboard OpenConfig/gNMI Devices ⓘ	Beta	○
Onboard SNMP Devices ⓘ	Beta	○
Section Permission Controls for Roles ⓘ	Beta	○
Studios - Enable Tag Matcher Input ⓘ	Beta	○
Studios End-to-End Provisioning ⓘ	Beta	○
UNO Features ⓘ	Beta	○
Upload and Download Images and Extensions ⓘ	Beta	○
Vertical Navigation ⓘ	Beta	○
AQL Explorer ⓘ	Retired	○

Session Management

Persistent Login	●
Session Duration	24 hours
Maximum Idle Time	Disabled

Build Information

Build Hash	e0f1314ffa8e19d0320ac8a01a81b88aeec5f571
Build Time	Aug 19, 2023 06:41:05 GMT+5:30

Cluster Management

Logo	
Cluster Name	Arista Systest
WiFi Cloud Connector	Not configured
Non-Author Change Control Review ⓘ	○
ZTP Access Control ⓘ	●
Minimal Mode ⓘ	○
Allow Login with Email ⓘ	●
Allow Identity Provider Initiated Login for SAML ⓘ	●
Display Studios Secret Values ⓘ	○
Device Decommission ⓘ	Disabled

Troubleshooting

UI Session Data	Download

Setting SAML IDP Login

For SAML IDP initiated login to function with CloudVision, you should define a *default relay state* value while setting up the SAML provider in your IDP. It is expected that your IDP should have an optional field to configure the default relay state.

For example, while configuring IDP, enter the details in the **Relay State** (Optional) field in the following format:

<**ProviderID**>:<**OrgName**>:<**NextURL**>, where:

- ProviderID: is the provider identifier that has been set up on CloudVision. Append "*saml*" to the name of the provider as below:
  - Okta: Use **oktasaml** as the ProviderID
  - OneLogin: Use **oneloginsaml** as the ProviderID
  - Microsoft: Use **microsoftsaml** as the ProviderID
  - Launchpad: Use **launchpadsaml** as the ProviderID
  - Custom SAML Provider: Use the *ProviderID* entered while setting up CloudVision
- OrgName: For On-prem users, the organization name is always the *default* value**.** This is the value that you have entered as your organization name. You can overwrite this value with a custom value later. For CVaaS users, this is the name of the organization entered at login time.
- NextURL: This is the URL that gets redirected to after logging in. This can be the **Entity ID** on the IDP followed by **/settings/aaa-providers**. This value must be base 64 RawURL encoded.

For example, if the URL is *https://www.cvp.arista.io* the base 64 RawURL encoding is, **aHR0cHM6Ly93d3cuY3ZwLmFyaXN0YS5pby9zZXR0aW5ncy9hYWEtcHJvdmlkZXJz** and this encoded value gets included in the **Relay State** field. You can leave the URL empty, in which case you are redirected to a default URL, which is the **Entity ID** followed by **/cv**.

For Example, if a user from the organization, Foo is setting up a Microsoft Provider and wants to be redirected to *https://www.cloudvision.domain/settings/aaa-providers*, then the **Relay State** should be, *microsoftsaml:Foo:aHR0cHM6Ly93d3cuY3ZwLmFyaXN0YS5pby9zZXR0aW5ncy9hYWEtcHJvdmlkZXJz*. You can also enter the Relay State without the NextURL details as *microsoftsaml:Foo:*, where you will be redirected to *https://<your FQDN>/cv*, where *<your FQDN>* is the DNS name you configured for the cluster.

4.3.5 Logging in with a Provider

You can use your registered providers on the CloudVision login screen to log in to cloud and on-premise CloudVision deployments. Click on the provider that has been created to log in through that provider.

Note: The login screen of the CloudVision with Cloud Deployments displays all supported providers regardless of which ones were created. Whereas, the login screen of the CloudVision with Cloud Deployments only displays providers that have been created.

4.3.6 Adding Launchpad as a Provider

You can add a launchpad using one of the following methods as per your requirement:

- Adding a Launchpad for CVaaS Deployments
- Adding a Launchpad for On-Premise Deployments
- Adding a Launchpad for CVaaS and On-Premise Deployments

4.3.6.1 Adding a Launchpad for CVaaS Deployments

This section applies to non-CV-CUE customers who want to use launchpad as an identity provider.

To add launchpad as a shared provider for CVaas deployments, request the list of users to be created in launchpad by emailing to wifi-cloudops-tickets@

Note:

- For cv-dev and cv-play, use the following information to configure Launchpad in Cloudvision:

  Provider: `launchpad` Identity Provider Issuer: `https://mojoonedemo.airtightnw.com/idp/shibboleth` Identity Provider Metadata URL: `https://mojoonedemo.airtightnw.com/idp/shibboleth` Email Attribute Name: `User.email` Authorization Request Binding: `HTTP-Redirect SAML protocol binding`
- For cv-staging and production, use the following information to configure Launchpad in Cloudvision:

  Provider: `launchpad` Identity Provider Issuer: `https://login.mojonetworks.com/idp/shibboleth` Identity Provider Metadata URL: `https://login.wifi.arista.com/casui/idp-metadata.xml` Email Attribute Name: `User.email` Authorization Request Binding: `HTTP-Redirect SAML protocol binding`

4.3.6.2 Adding a Launchpad for On-Premise Deployments

Perform the following steps to add a launchpad for on-premise deployments:

1. Log into the tenant/cluster and get the SAML metadata from the desired cluster by going to the *CLUSTER_URL*`/api/v1/saml_sp_metadata` URL.

   Note:
2. Email the metadata obtained in **Step 1** to wifi-cloudops-tickets@ requesting to create the first user account in Launchpad and to get Launchpad configured with the SAML metadata to trust this CloudVision cluster.

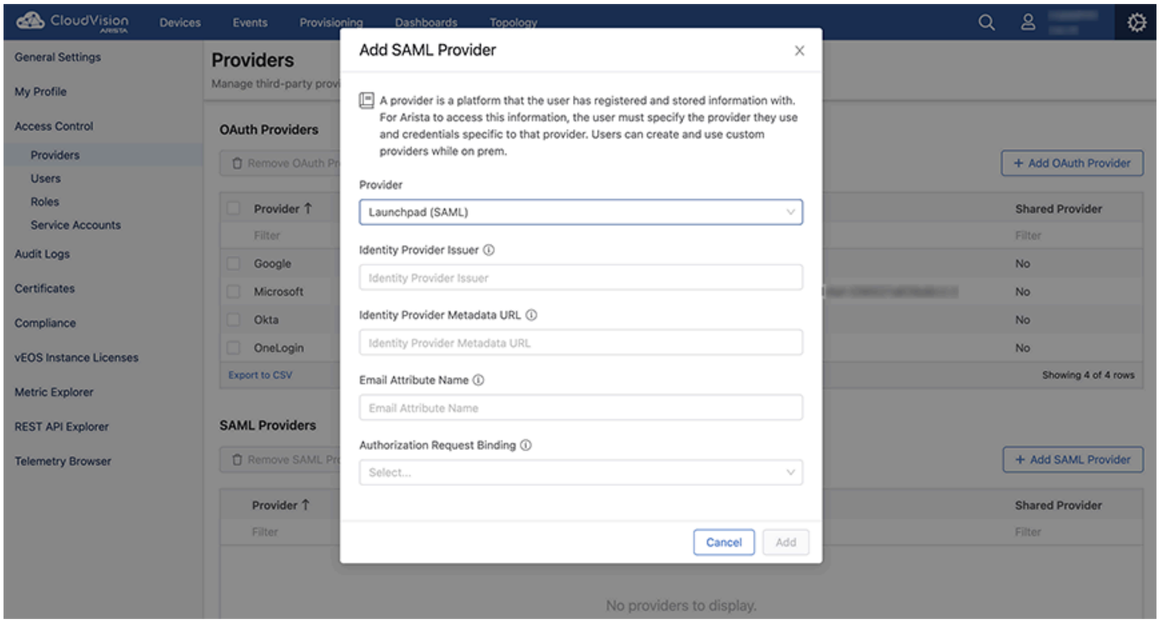
   Note: Other accounts for this customer/org can be created by the first account created for this org by the cloudops team.
3. Get the IdentityProvider Issuer URL, Identity Provider Metadata URL and the Email attribute name from Launchpad.

4.3.6.3 Adding a Launchpad for CVaaS and On-Premise Deployments

Perform the following steps to add a launchpad for CVaaS and on-premise deployments:

1. Log in to the CVP.
2. Click on the gear icon.
3. On the General Settings screen, under **Features**, enable **SAML Providers (Beta)**.
4. Navigate to **Access Control** > **Providers** and click the **+ Add SAML Provider** button.
5. Select **Launchpad (SAML)** from the **Provider** drop-down menu.

Figure 4-21: Add SAML Provider Screen to Configure Launchpad



Add SAML Provider ×

A provider is a platform that the user has registered and stored information with. For Arista to access this information, the user must specify the provider they use and credentials specific to that provider. Users can create and use custom providers while on prem.

Provider: Launchpad (SAML)

Identity Provider Issuer: Identity Provider Issuer

Identity Provider Metadata URL: Identity Provider Metadata URL

Email Attribute Name: Email Attribute Name

Authorization Request Binding: Select...

Cancel | Add

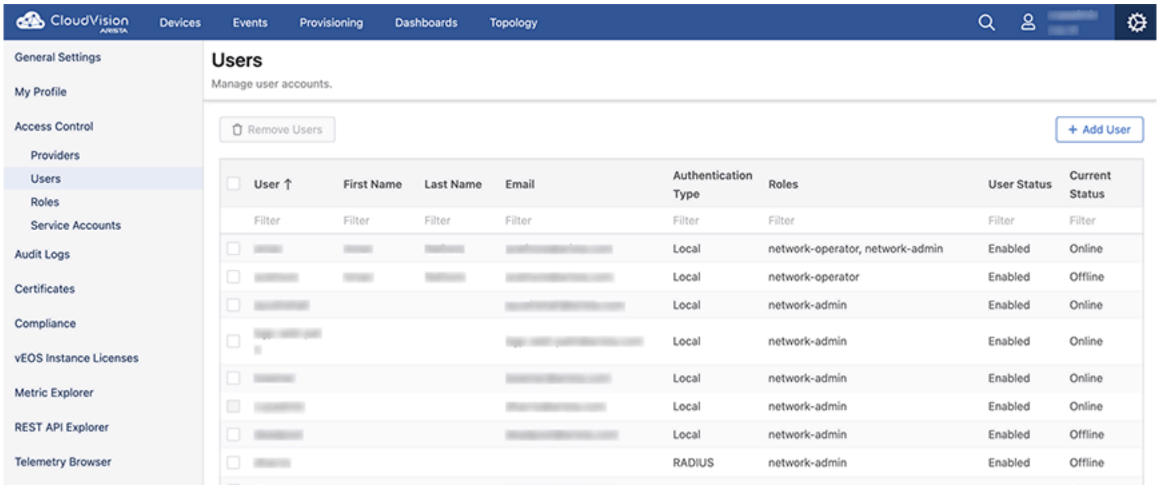
6. In the **Identity Provider Issuer** field, type the Issuer or Entity ID.

Note: An Issuer or Entity ID is a URL that uniquely identifies a SAML identity provider.

7. In the **Identity Provider Metadata URL** field, type the URL to fetch identity provider metadata.
8. In the **Email Attribute Name** field, type the attribute name for the email ID in SAML.
9. In the **Authorization Request Binding** field, select the protocol binding used for the SAML authentication request to the identity provider.
10. Click **Add**.
11. Under **Access Control** in the left pane, click **Users**.

The system opens the **Users** screen.

Figure 4-22: Users Screen



Users

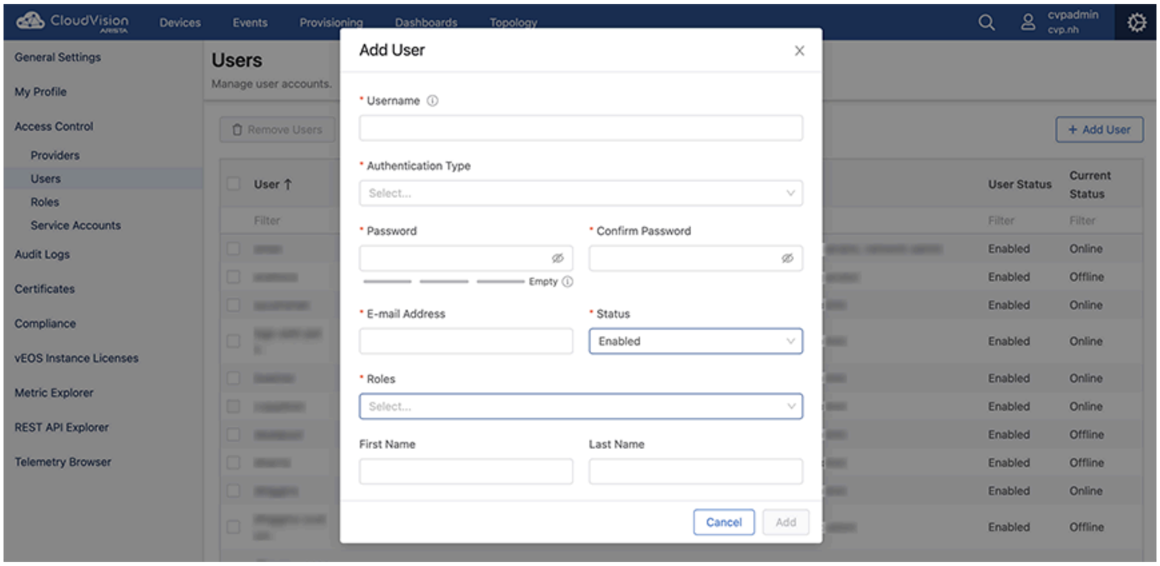
Manage user accounts.

User ↑	First Name	Last Name	Email	Authentication Type	Roles	User Status	Current Status
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
[illegible]	[illegible]	[illegible]	[illegible]	Local	network-operator, network-admin	Enabled	Online
[illegible]	[illegible]	[illegible]	[illegible]	Local	network-operator	Enabled	Offline
[illegible]			[illegible]	Local	network-admin	Enabled	Online
[illegible]			[illegible]	Local	network-admin	Enabled	Online
[illegible]			[illegible]	Local	network-admin	Enabled	Online
[illegible]			[illegible]	Local	network-admin	Enabled	Online
[illegible]			[illegible]	Local	network-admin	Enabled	Offline
[illegible]				RADIUS	network-admin	Enabled	Offline

12. On the **Users** screen, click **+ Add User**.

    The system opens the **Add User** screen.

    Figure 4-23: Add User Screen



Add User

* Username

* Authentication Type: Select...

* Password

* Confirm Password

Empty

* E-mail Address

* Status: Enabled

* Roles: Select...

First Name

Last Name

13. Provide the required information in corresponding fields.

    Note:

    - CloudVision usernames and EOS switch usernames must match for CloudVision to manage configuration and images on the switches.
    - Type the email address which you used to sign up with Launchpad in the **Email Address** field.

14. Click **Add**.
15. Logout from the CVP.
16. Login to your account via launchpad.

Chapter 5

Getting Started (CVP)

The login screen is displayed when you first connect to the application using a web browser.

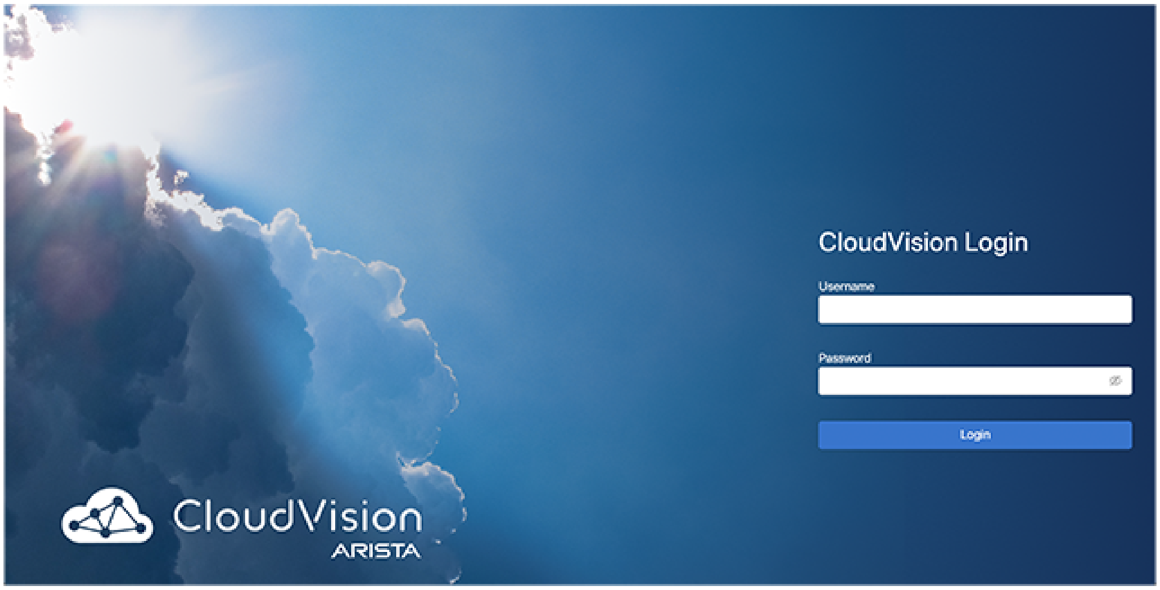
The CloudVision Portal (CVP) application is accessible after the CVP service has been started on the appliance. The login screen is displayed when you first connect to the application using a web browser. JavaScript must be enabled in the browser for the web application to work.

Sections in this chapter include:

5.1 Accessing the CVP Login Page

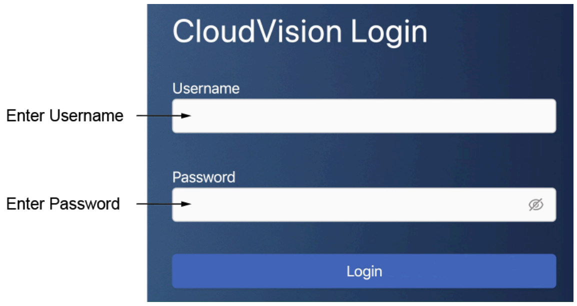
1. To access the login page, point your browser to the CloudVision Portal (http://HOSTNAME or https://HOSTNAME).The system opens the CVP login page.

Figure 5-1: CVP Login Page



2. Enter login credentials in the CVP login section.

Figure 5-2: Login Section



Note:

The username and passwords required will depend on the authentication method and accounts previously set up. Login using the username and password created when CVP was installed. If you chose the local authentication and authorization options, login initially using *cvpadmin* for the username and password.

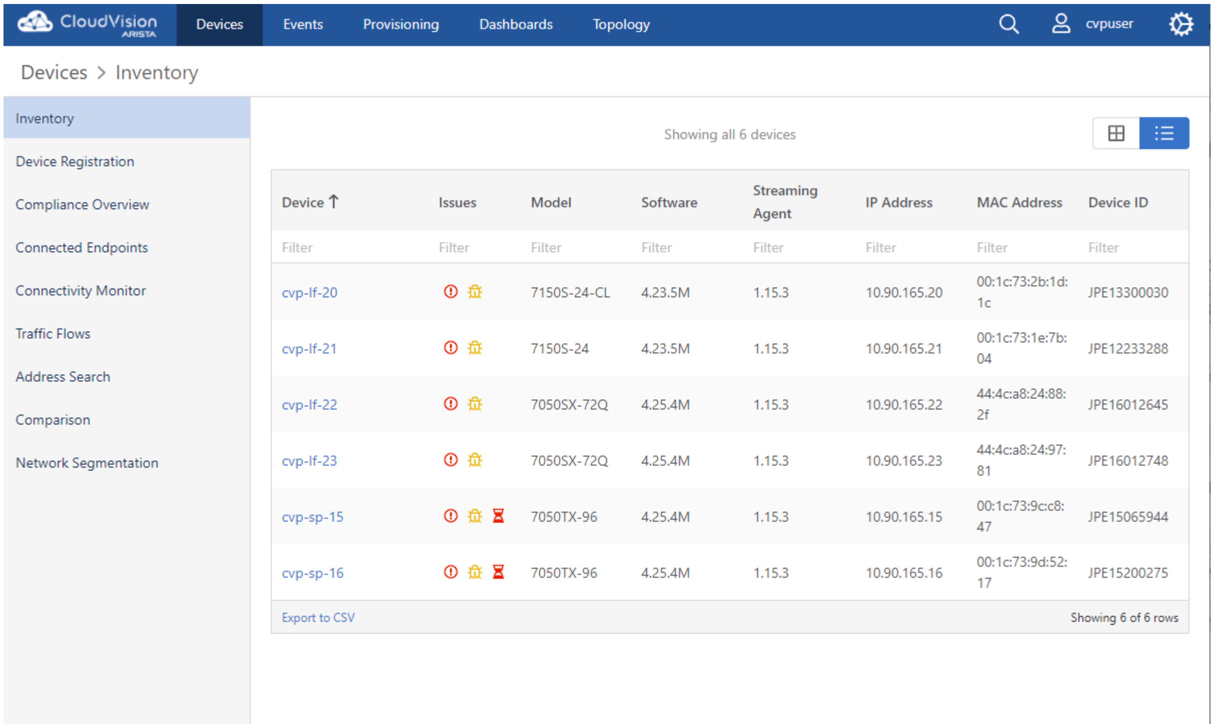
3. Click **Login**. The system opens the CVP home page.

5.2 Accessing the Home Page

All features including Devices, Events, Provisioning, Dashboards, and Topology are displayed on the home panel.

Note: You must have required privileges to access a switch.

Figure 5-3: Home Page



Showing all 6 devices

Device ↑	Issues	Model	Software	Streaming Agent	IP Address	MAC Address	Device ID
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
cvp-lf-20	❗ 🐞	7150S-24-CL	4.23.5M	1.15.3	10.90.165.20	00:1c:73:2b:1d:1c	JPE13300030
cvp-lf-21	❗ 🐞	7150S-24	4.23.5M	1.15.3	10.90.165.21	00:1c:73:1e:7b:04	JPE12233288
cvp-lf-22	❗ 🐞	7050SX-72Q	4.25.4M	1.15.3	10.90.165.22	44:4c:a8:24:88:2f	JPE16012645
cvp-lf-23	❗ 🐞	7050SX-72Q	4.25.4M	1.15.3	10.90.165.23	44:4c:a8:24:97:81	JPE16012748
cvp-sp-15	❗ 🐞 ⌛	7050TX-96	4.25.4M	1.15.3	10.90.165.15	00:1c:73:9c:c8:47	JPE15065944
cvp-sp-16	❗ 🐞 ⌛	7050TX-96	4.25.4M	1.15.3	10.90.165.16	00:1c:73:9d:52:17	JPE15200275

Export to CSV

Showing 6 of 6 rows

The home page provides the following selections.

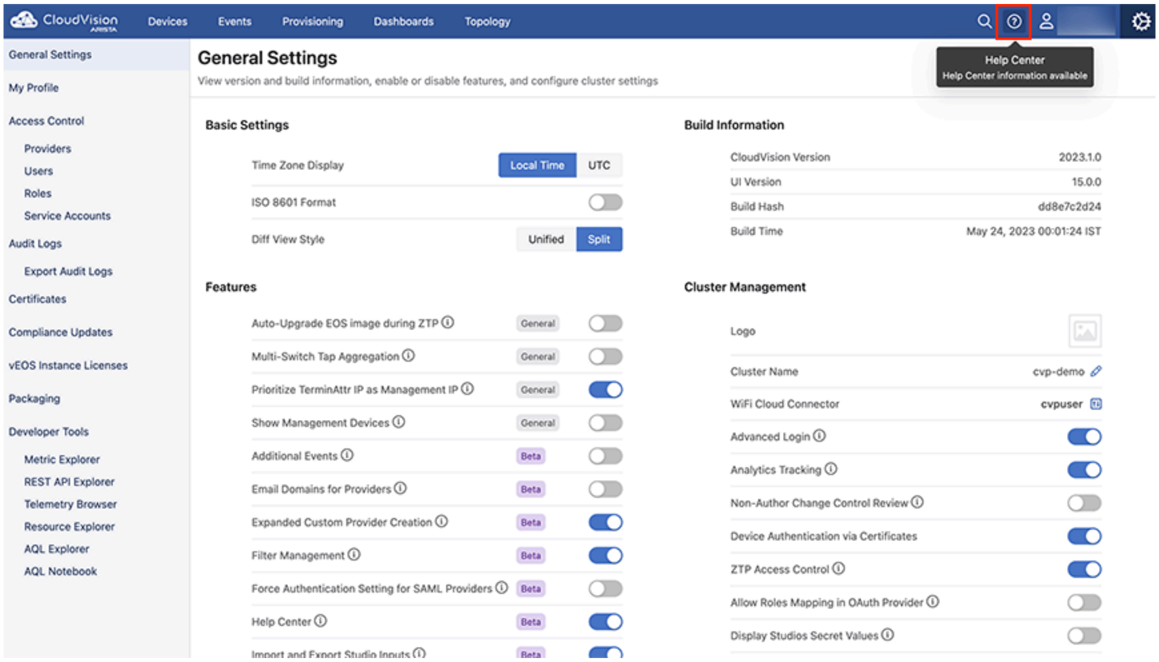
- **Devices**: View all devices across multiple topologies.
- **Events**: View multiple events on multiple devices.
- **Provisioning**: Hierarchical tree structure of the network is maintained here. All the configuration and image assignment to the network switches are made via this module.
- **Dashboards**: View multiple metrics across multiple devices. Select at least one metric and one device to begin.
- **Topology**: View the location of devices in individual topologies.

5.3 Accessing Help Center Documentation

Starting with 2023.2.0 release, CloudVision provides you with in-product documentation support called **Help Center**. The Help Center allows you to access detailed information on CloudVision features and functionalities. Prior to 2023.2.0 release, Help Center was available as a beta functionality.

You can access Help Center, which is represented by a (?) icon in a circle, in the top-right corner of every CloudVision page as shown below:

Figure 5-4: Help Center



General Settings

View version and build information, enable or disable features, and configure cluster settings

Help Center
Help Center information available

Basic Settings

Time Zone Display	[✓ Local Time] UTC
ISO 8601 Format	○
Diff View Style	Unified [✓ Split]

Features

Auto-Upgrade EOS image during ZTP ⓘ	General	○
Multi-Switch Tap Aggregation ⓘ	General	○
Prioritize TerminAttr IP as Management IP ⓘ	General	●
Show Management Devices ⓘ	General	○
Additional Events ⓘ	Beta	○
Email Domains for Providers ⓘ	Beta	○
Expanded Custom Provider Creation ⓘ	Beta	●
Filter Management ⓘ	Beta	●
Force Authentication Setting for SAML Providers ⓘ	Beta	○
Help Center ⓘ	Beta	●
Import and Export Studio Inputs ⓘ	Beta	●

Build Information

CloudVision Version	2023.1.0
UI Version	15.0.0
Build Hash	dd8e7c2d24
Build Time	May 24, 2023 00:01:24 IST

Cluster Management

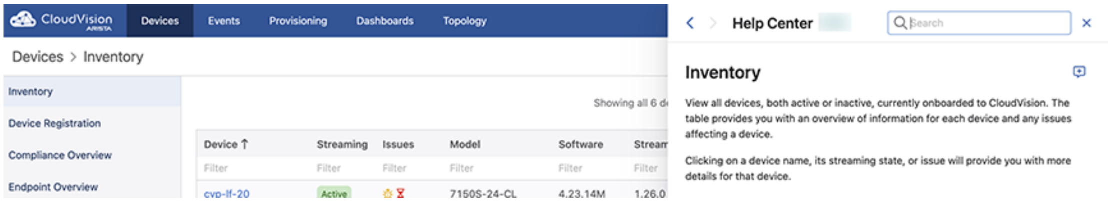
Logo	
Cluster Name	cvp-demo
WiFi Cloud Connector	cvpuser
Advanced Login ⓘ	●
Analytics Tracking ⓘ	●
Non-Author Change Control Review ⓘ	○
Device Authentication via Certificates	●
ZTP Access Control ⓘ	●
Allow Roles Mapping in OAuth Provider ⓘ	○
Display Studios Secret Values ⓘ	○

When you click on the Help Center icon (?), the Help Center page for the corresponding CloudVision screen is displayed. The main article explains the CloudVision screen you are viewing and the workflow. Additionally, the **Related Articles** section displays a list of related topics that are relevant to the main topic.

Navigating the Help Center

The Help Center provides various functionalities that allow you to navigate the CloudVision portal and documentation. By default, the displayed Help Center article corresponds to the CloudVision page on which you clicked the Help Center icon. That is, the Help Center and the CloudVision UI are synchronized, by default. See image below:

Figure 5-5: Help Center Search Functionality



Device ↑	Streaming	Issues	Model	Software	Stream
Filter	Filter	Filter	Filter	Filter	Filter
cvp-lf-20	Active		7150S-24-CL	4.23.14M	1.26.0

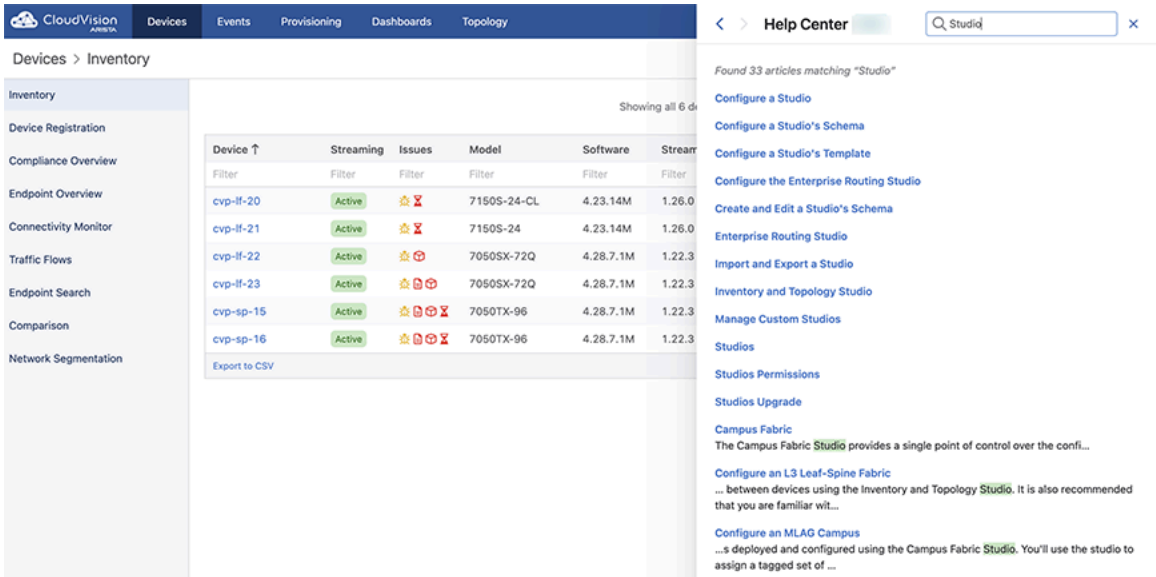
Inventory

View all devices, both active or inactive, currently onboarded to CloudVision. The table provides you with an overview of information for each device and any issues affecting a device.

Clicking on a device name, its streaming state, or issue will provide you with more details for that device.

The Search function within the Help Center page allows you to search the Help Center documentation using a keyword or term, where you can find articles non-related to the current page. When you search for a term or a keyword, the Help Center displays a list of articles related to the searched term. For example, while in the Devices Inventory page, if you had searched for *Studios*, the Help Center displays the Studios page as shown below:

Figure 5-6: Help Center - Searched Page



Device ↑	Streaming	Issues	Model	Software	Stream
Filter	Filter	Filter	Filter	Filter	Filter
cvp-lf-20	Active		7150S-24-CL	4.23.14M	1.26.0
cvp-lf-21	Active		7150S-24	4.23.14M	1.26.0
cvp-lf-22	Active		7050SX-72Q	4.28.7.1M	1.22.3
cvp-lf-23	Active		7050SX-72Q	4.28.7.1M	1.22.3
cvp-sp-15	Active		7050TX-96	4.28.7.1M	1.22.3
cvp-sp-16	Active		7050TX-96	4.28.7.1M	1.22.3

Found 33 articles matching "Studio"

Configure a Studio

Configure a Studio's Schema

Configure a Studio's Template

Configure the Enterprise Routing Studio

Create and Edit a Studio's Schema

Enterprise Routing Studio

Import and Export a Studio

Inventory and Topology Studio

Manage Custom Studios

Studios

Studios Permissions

Studios Upgrade

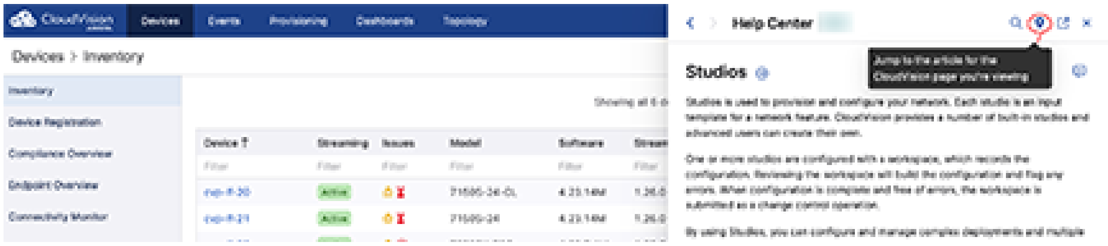
Campus Fabric
The Campus Fabric Studio provides a single point of control over the confi...

Configure an L3 Leaf-Spine Fabric
... between devices using the Inventory and Topology Studio. It is also recommended that you are familiar wit...

Configure an MLAG Campus
...s deployed and configured using the Campus Fabric Studio. You'll use the studio to assign a tagged set of ...

If you want to go back to the article corresponding to the CloudVision UI, click on the Location icon on the currently displayed Help Center page as shown below:

Figure 5-7: Help Center - Location Page



Studios

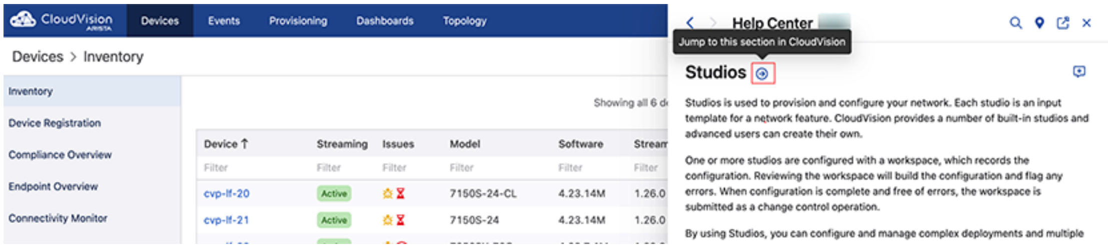
Studios is used to provision and configure your network. Each studio is an input template for a network feature. CloudVision provides a number of built-in studios and advanced users can create their own.

One or more studios are configured with a workspace, which records the configuration. Reviewing the workspace will build the configuration and flag any errors. When configuration is complete and free of errors, the workspace is submitted as a change control operation.

By using Studios, you can configure and manage complex deployments and multiple

To open the CloudVision UI page corresponding to the searched Help Center article, click on the arrow (→) next to the Help Center article title as below:

Figure 5-8: Help Center -Relevant UI page



Device ↑	Streaming	Issues	Model	Software	Stream
Filter	Filter	Filter	Filter	Filter	Filter
cvp-lf-20	Active		7150S-24-CL	4.23.14M	1.26.0
cvp-lf-21	Active		7150S-24	4.23.14M	1.26.0

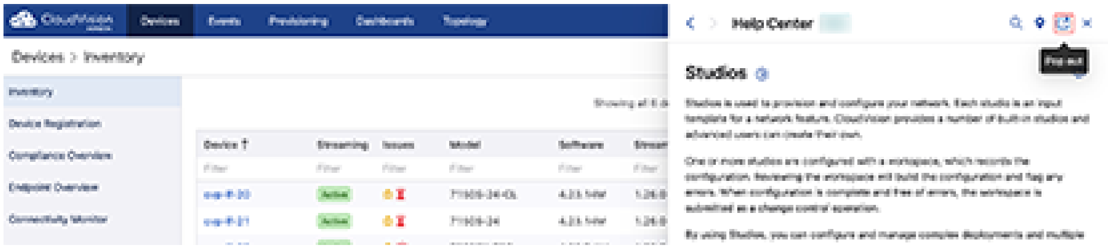
Studios is used to provision and configure your network. Each studio is an input template for a network feature. CloudVision provides a number of built-in studios and advanced users can create their own.

One or more studios are configured with a workspace, which records the configuration. Reviewing the workspace will build the configuration and flag any errors. When configuration is complete and free of errors, the workspace is submitted as a change control operation.

By using Studios, you can configure and manage complex deployments and multiple

By default, the Help Center page opens as a drawer in the CloudVision portal. Click on the pop-out icon on the Help Center page (see image below) if you want to open the Help Center page as an independent window enabling you to move around the Help Center so that it does not obstruct the CloudVision portal.

Figure 5-9: Help Center - Help Pop Out



Device ↑	Streaming	Issues	Model	Software	Stream
Filter	Filter	Filter	Filter	Filter	Filter
cvp-lf-20	Active		7150S-24-CL	4.23.14M	1.26.0
cvp-lf-21	Active		7150S-24	4.23.14M	1.26.0

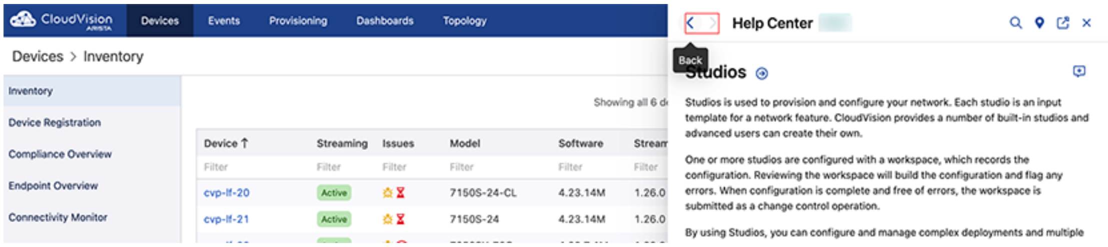
Studios is used to provision and configure your network. Each studio is an input template for a network feature. CloudVision provides a number of built-in studios and advanced users can create their own.

One or more studios are configured with a workspace, which records the configuration. Reviewing the workspace will build the configuration and flag any errors. When configuration is complete and free of errors, the workspace is submitted as a change control operation.

By using Studios, you can configure and manage complex deployments and multiple

On the Help Center page, you can navigate forward and backwards through opened articles and search menus as shown below:

Figure 5-10: Help Center - Navigation



Device ↑	Streaming	Issues	Model	Software	Stream
Filter	Filter	Filter	Filter	Filter	Filter
cvp-lf-20	Active		7150S-24-CL	4.23.14M	1.26.0
cvp-lf-21	Active		7150S-24	4.23.14M	1.26.0

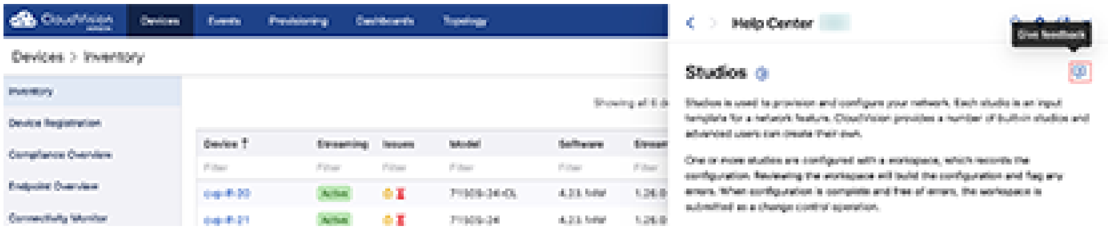
Studios is used to provision and configure your network. Each studio is an input template for a network feature. CloudVision provides a number of built-in studios and advanced users can create their own.

One or more studios are configured with a workspace, which records the configuration. Reviewing the workspace will build the configuration and flag any errors. When configuration is complete and free of errors, the workspace is submitted as a change control operation.

By using Studios, you can configure and manage complex deployments and multiple

The Help Center also supports documentation feedback. You can click on the feedback icon, enter your comments in the text box, and then click Continue. The feedback is emailed to the CloudVision team at Arista Support.

Figure 5-11: Help Center - Feedback



Device ↑	Streaming	Issues	Model	Software	Stream
Filter	Filter	Filter	Filter	Filter	Filter
cvp-lf-20	Active		7150S-24-CL	4.23.14M	1.26.0
cvp-lf-21	Active		7150S-24	4.23.14M	1.26.0

Studios is used to provision and configure your network. Each studio is an input template for a network feature. CloudVision provides a number of built-in studios and advanced users can create their own.

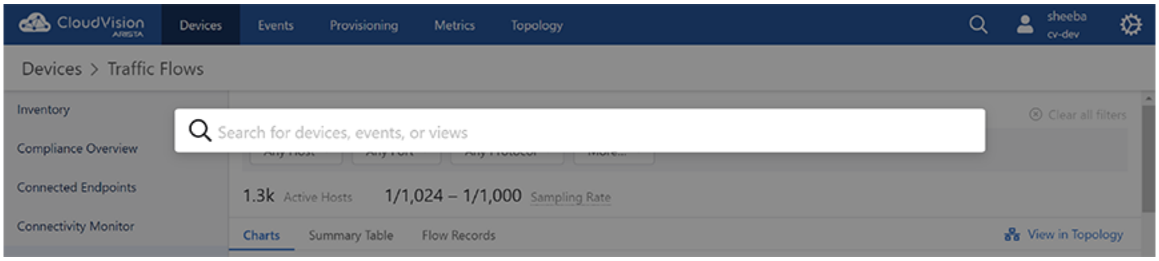
One or more studios are configured with a workspace, which records the configuration. Reviewing the workspace will build the configuration and flag any errors. When configuration is complete and free of errors, the workspace is submitted as a change control operation.

5.4 Omnibox

The omnibox performs a search and displays results from all sections in CloudVision. You must select a result for navigating to the corresponding CloudVision section.

Click the search icon at the upper-right corner of the CVP screen to access the omnibox.

Figure 5-12: Omnibox



Note:

- You can refine search results by adding more keywords to the query.
- Omnibox hotkeys are **Command #** + **K** in Mac; and **Ctrl** + **K** in Windows.

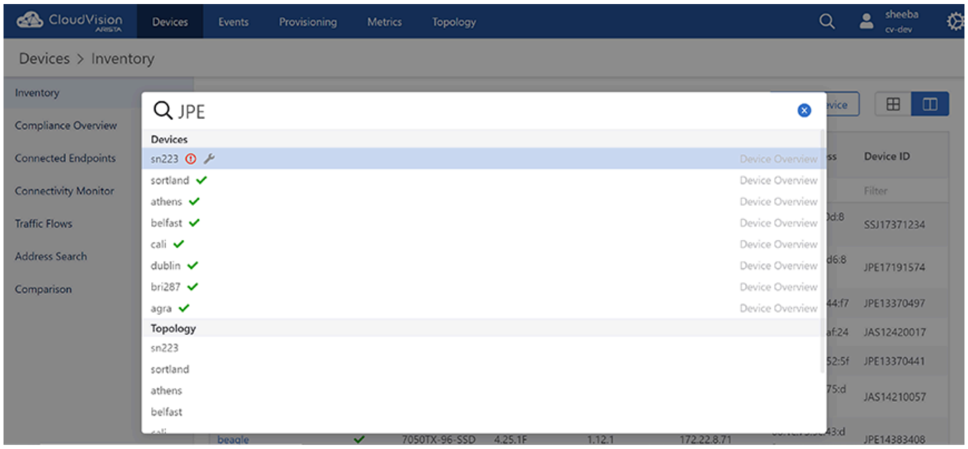
The Omnibox provides a variety of results classifying them by the section it belongs to, an associated device or section name, and sometimes a description that explains what kind of result it is.The list of potential search result modules are:

- **Devices**
  - Matching devices
  - Sections of matching devices
- **Events**
  - Matching event types
  - If a keyword matches a device hostname, it provides an option to view all events on that device
  - Matching event configurations
- **Metrics**
  - Matching metrics
  - Matching metric dashboards
- **Topology** - Matching devices in topology
- **Provisioning** - Matching **Provisioning** sections
- **Settings** - Matching **Settings** sections

Note: Multiple results from the same section are grouped together.

CloudVision displays matching results from **Devices** and **Topology** sections when a search is performed using the `JPE` keyword.

Figure 5-13: Omnibox Search with JPE Keyword

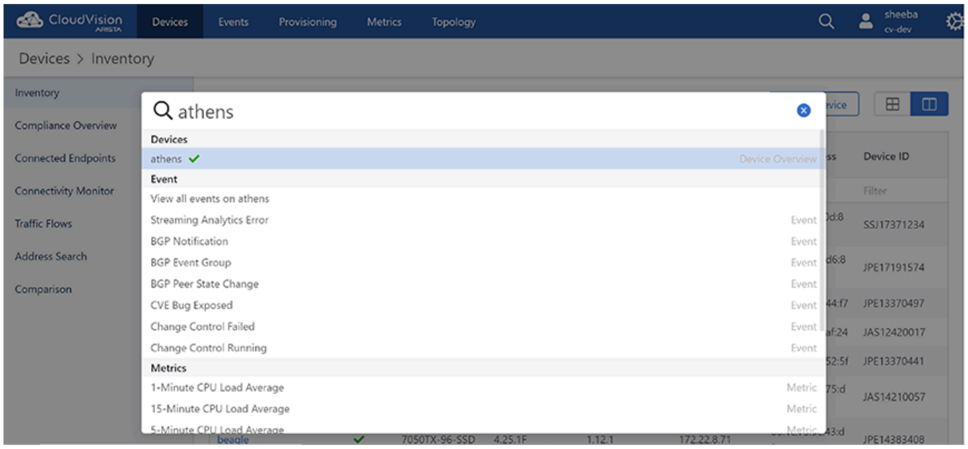


Note:

- If you select *athens* from the **Devices** section, CloudVision displays the Device Overview screen of athens.
- If you select *athens* from the **Topology** section, CloudVision displays athens node in the Topology view.

If a search is performed with the `athens` keyword, CloudVision displays results from **Devices**, **Event**, **Metrics**, and **Topology** sections.

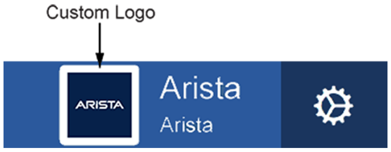
Figure 5-14: Omnibox Search with Athens Keyword



5.5 Customizing the Home Screen and Dashboard Logo

CloudVision enables you to customize the visible options and dashboard logo shown on the home page. You change the visible options and dashboard logo by customizing them from the Settings page.

By default, no dashboard logo is selected. The image you select for the logo appears in the dashboard next to the notifications icon.



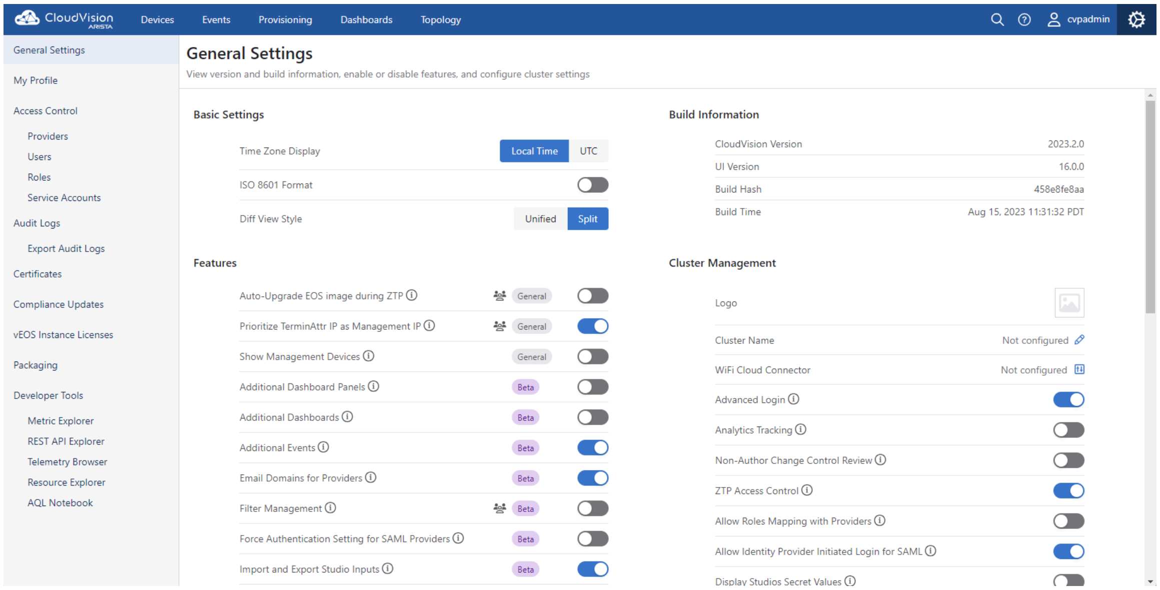
Note: Note Any image you select for either the Home screen background or dashboard logo must not exceed 200 KB for each image. In addition, the images must JPG, PNG, or GIF.

Complete the following steps to customize the visible and dashboard logo:

1. Login to CVP.
2. Click the gear icon at the upper right corner of the page.

3. Click **Settings** in the left menu.
4. Select the required options provided under **Basic Settings**, **Beta Features**, **Cluster Management**, and **Troubleshooting** sections.

Figure 5-15: Default Settings for Home Page and Dashboard Logo



General Settings

View version and build information, enable or disable features, and configure cluster settings

Basic Settings

Time Zone Display	[✓ Local Time] UTC
ISO 8601 Format	○
Diff View Style	Unified [✓ Split]

Features

Auto-Upgrade EOS image during ZTP ⓘ	General	○
Prioritize TerminAttr IP as Management IP ⓘ	General	●
Show Management Devices ⓘ	General	○
Additional Dashboard Panels ⓘ	Beta	○
Additional Dashboards ⓘ	Beta	○
Additional Events ⓘ	Beta	●
Email Domains for Providers ⓘ	Beta	●
Filter Management ⓘ	Beta	○
Force Authentication Setting for SAML Providers ⓘ	Beta	○
Import and Export Studio Inputs ⓘ	Beta	●

Build Information

CloudVision Version	2023.2.0
UI Version	16.0.0
Build Hash	458e8fe8aa
Build Time	Aug 15, 2023 11:31:32 PDT

Cluster Management

Logo	
Cluster Name	Not configured
WiFi Cloud Connector	Not configured
Advanced Login ⓘ	●
Analytics Tracking ⓘ	○
Non-Author Change Control Review ⓘ	○
ZTP Access Control ⓘ	●
Allow Roles Mapping with Providers ⓘ	○
Allow Identity Provider Initiated Login for SAML ⓘ	●
Display Studios Secret Values ⓘ	○

5. To customize the dashboard logo, perform the following steps:
   - Click the image box next to the logo field.
   - In the Upload logo dialog, Click **Select file**.
   - Navigate to the desired image, and click **Open**. (The imported image is displayed next the Select file box.)
   - Click **Upload**.

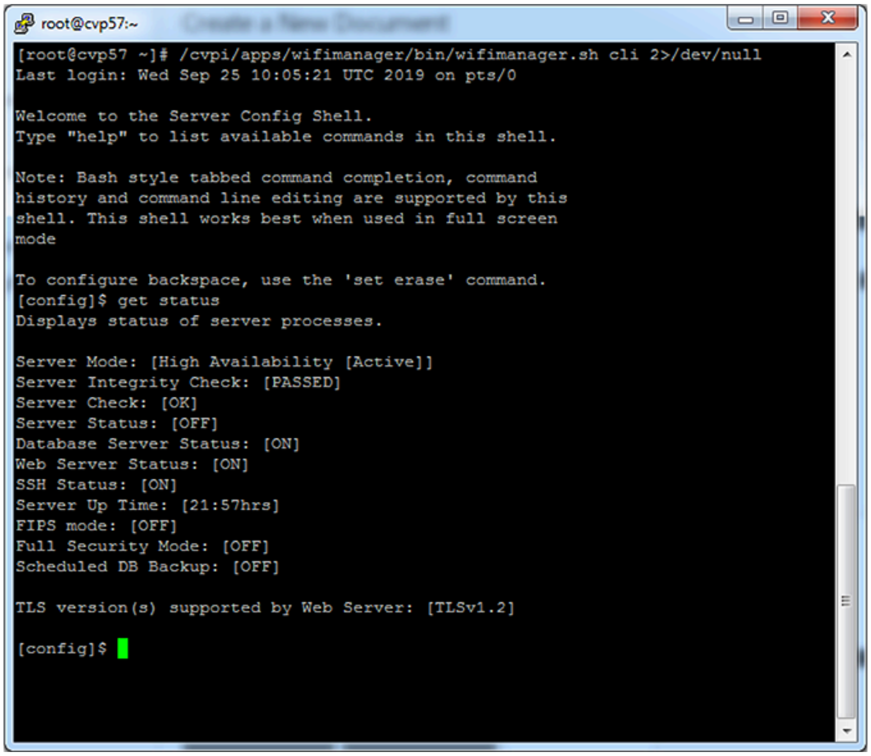
5.6 Accessing CV-CUE

You can access the CV-CUE service via either the CLI Access or the UI Access.

CLI Access

To log in to the wifimanager container using CLI, run the `/cvpi/apps/wifimanager/bin/wifimanager.sh cli 2>/dev/null` command on the primary or the secondary node.

Figure 5-16: CLI Access



```
[root@cvp57 ~]# /cvpi/apps/wifimanager/bin/wifimanager.sh cli 2>/dev/null
Last login: Wed Sep 25 10:05:21 UTC 2019 on pts/0

Welcome to the Server Config Shell.
Type "help" to list available commands in this shell.

Note: Bash style tabbed command completion, command
history and command line editing are supported by this
shell. This shell works best when used in full screen
mode

To configure backspace, use the 'set erase' command.
[config]$ get status
Displays status of server processes.

Server Mode: [High Availability [Active]]
Server Integrity Check: [PASSED]
Server Check: [OK]
Server Status: [OFF]
Database Server Status: [ON]
Web Server Status: [ON]
SSH Status: [ON]
Server Up Time: [21:57hrs]
FIPS mode: [OFF]
Full Security Mode: [OFF]
Scheduled DB Backup: [OFF]

TLS version(s) supported by Web Server: [TLSv1.2]

[config]$
```

You can now run wifimanager commands. See the Wifimanager CLI Commands for a list of wifimanager CLI commands and their descriptions.

UI Access

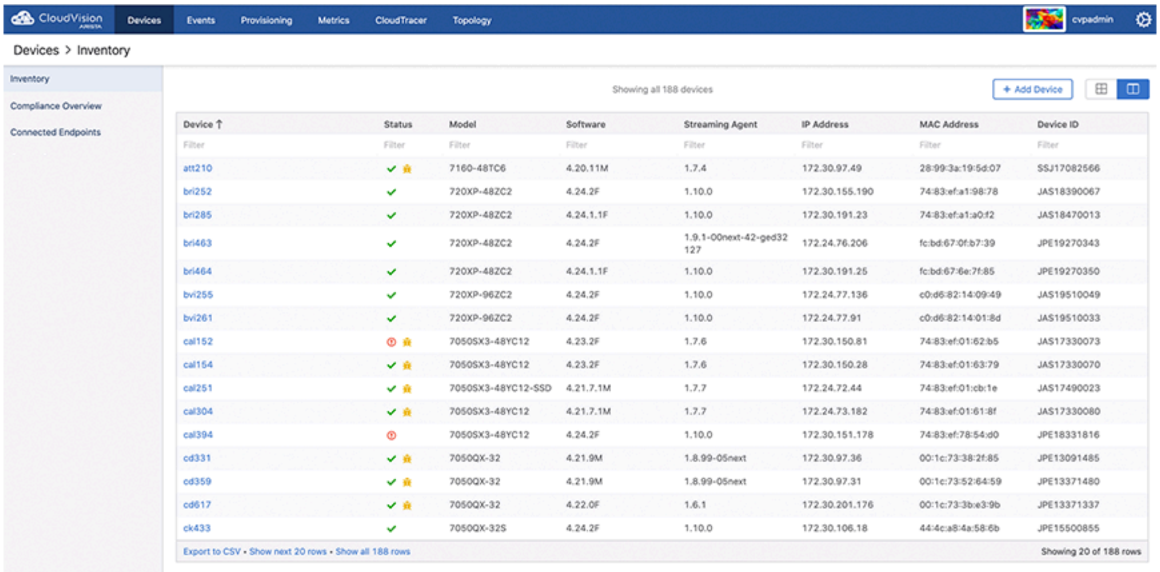
The URL to access the wifimanager UI is **http(s)://<*CVP-IP*>/wifi/wifimanager** is where CVP-IP refers to the actual CloudVision Portal (CVP) IP/domain name.

The URL to access the cognitive Wifi UI is **http(s)://<*CVP-IP*>/wifi/aware** where ***CVP-IP*** refers to either the actual CVP IP or domain name.

For example, if the IP address of CVP is *10.12.3.4*, then the URL to access the wifimanager UI is *https://10.2.3.4/wifi.wifimanager* and the cognitive Wifi UI is *https:////10.12.3.4/wifi/aware*.

You can access CV-CUE UI by clicking on the **WiFi** tab in the CVP UI, or you can access it directly using the URLs of either wifimanager UI or Wifi UI.

Figure 5-17: UI Access



Showing all 188 devices

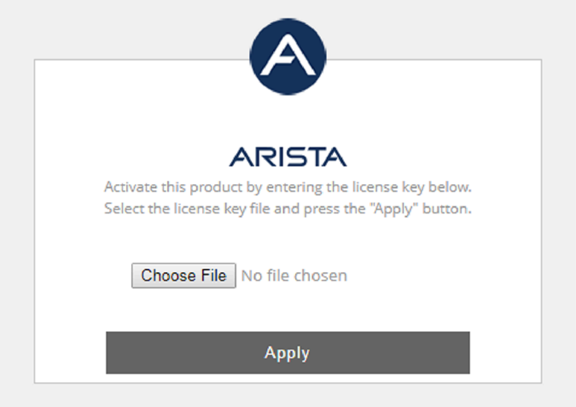
Device ↑	Status	Model	Software	Streaming Agent	IP Address	MAC Address	Device ID
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
att210	✓ ⚠	7160-48TC6	4.20.11M	1.7.4	172.30.97.49	28:99:3a:19:5d:07	SSJ17082566
bri252	✓	720XP-48ZC2	4.24.2F	1.10.0	172.30.155.190	74:83:ef:a1:98:78	JAS18390067
bri285	✓	720XP-48ZC2	4.24.1.1F	1.10.0	172.30.191.23	74:83:ef:a1:a0:f2	JAS18470013
bri463	✓	720XP-48ZC2	4.24.2F	1.9.1-00next-42-ged32 127	172.24.76.206	fc:bd:67:0f:b7:39	JPE19270343
bri464	✓	720XP-48ZC2	4.24.1.1F	1.10.0	172.30.191.25	fc:bd:67:6e:7f:85	JPE19270350
bvi255	✓	720XP-96ZC2	4.24.2F	1.10.0	172.24.77.136	c0:d6:82:14:09:49	JAS19510049
bvi261	✓	720XP-96ZC2	4.24.2F	1.10.0	172.24.77.91	c0:d6:82:14:01:8d	JAS19510033
cal152	⊘ ⚠	7050SX3-48YC12	4.23.2F	1.7.6	172.30.150.81	74:83:ef:01:62:b5	JAS17330073
cal154	✓ ⚠	7050SX3-48YC12	4.23.2F	1.7.6	172.30.150.28	74:83:ef:01:63:79	JAS17330070
cal251	✓ ⚠	7050SX3-48YC12-SSD	4.21.7.1M	1.7.7	172.24.72.44	74:83:ef:01:cb:1e	JAS17490023
cal304	✓ ⚠	7050SX3-48YC12	4.21.7.1M	1.7.7	172.24.73.182	74:83:ef:01:61:8f	JAS17330080
cal394	⊘	7050SX3-48YC12	4.24.2F	1.10.0	172.30.151.178	74:83:ef:78:54:d0	JPE18331816
cd331	✓ ⚠	7050QX-32	4.21.9M	1.8.99-05next	172.30.97.36	00:1c:73:38:2f:85	JPE13091485
cd359	✓ ⚠	7050QX-32	4.21.9M	1.8.99-05next	172.30.97.31	00:1c:73:52:64:59	JPE13371480
cd617	✓ ⚠	7050QX-32	4.22.0F	1.6.1	172.30.201.176	00:1c:73:3b:e3:9b	JPE13371337
ck433	✓	7050QX-32S	4.24.2F	1.10.0	172.30.106.18	44:4c:a8:4a:58:6b	JPE15500855

Export to CSV • Show next 20 rows • Show all 188 rows

Showing 20 of 188 rows

When you access the UI for the first time, you need to apply the CV-CUE service license.

Figure 5-18: CV-CUE Service License



Activate this product by entering the license key below.
Select the license key file and press the "Apply" button.

Note:

- For the license file, please write an email to **support-wifi@arista.com**
- Use the `ifconfig` command on the CV root shell to get the eth0 MAC addresses of the primary and secondary CV servers (you need not access the wifimanager CLI for this). You need to include both these MAC addresses when you email support to request a license. One license is generated for the two (primary and secondary) MAC addresses.

Once you apply the license, you must log in to the CV-CUE UI using the following default credentials:

Username: **admin**

Password: **admin**

You can then change the password and add other users.

Note: You can now also connect Arista access points to the server.

5.7 Key CV-CUE Operations and Directories

CV-CUE is containerized as a service on CV. See the Wifimanager CLI Commands section for a list of CV-CUE CLI commands and their descriptions.

For details on how to configure, monitor, and troubleshoot WiFi using CV-CUE, see the CV-CUE User Guide on the Arista CV-CUE Support Portal at https://www.arista.com/support/customer-portal. You can access the portal from the WiFi - Support Portal tile on your dashboard. For details and credentials to access the portal, contact support-wifi@arista.com.

CVPI Commands for CV-CUE

The following table lists the operations you can perform on wifimanager and the corresponding CVPI commands used.

Table 6: CVPI Commands

Operation	CVPI Command
start	cvpi start wifimanager
stop	cvpi stop wifimanager
status	cvpi status wifimanager
restart	cvpi restart wifimanager
reset	cvpi reset wifimanager
backup	cvpi backup wifimanager
restore	cvpi restore wifimanager </path/to/backup/file>
debug	cvpi debug wifimanager

Note: The backup restore fails if the user running the restore command does not have access to the path where the backup file is stored.

The restart command restarts the wifimanager service, whereas the **reset** command resets wifimanager settings and data to factory default values. The **debug** command generates a debug bundle containing log files and configuration files that can be used to troubleshoot issues.

The following table lists the operations you can perform on aware and the corresponding CVPI commands used.

Table 7: Aware CVPI Commands

Operation	CVPI Command
start	cvpi start aware
stop	cvpi stop aware
status	cvpi status aware

5.7.1 Wifimanager Directories

CV-CUE stores its data in docker volumes that reside under the **/data/wifimanager** directory on the CV. The following table lists the important wifimanager directories and the information they contain.

Table 8: Contents of wifimanager Directories

Directory on CV	Contains
/data/wifimanager/log/glog	Application logs
/data/wifimanager/data/conf	Configuration files
/data/wifimanager/data/data	System data files/directories
/data/wifimanager/data/instances	Customer data files/directories
/data/wifimanager/data/pgsql_data	Postgres data
/data/wifimanager/log/slog	System logs
/data/wifimanager/backup	On-demand backups

5.8 Wifimanager CLI Commands

The following table provides the list of wifimanager CLI commands and their descriptions.

Table 9: Wifimanager CLI Commands

Command	Description
db backup	Backs up the database to the specified remote server.
db clean	Cleans up resources without disrupting services.
db restore	Restores the database from a previous backup on a remote server.
db reset	Resets the database to factory defaults but maintains network settings.
get cert	Generates a self-signed certificate.
get openconfig mode	Displays current OpenConfig mode.
get cors	Displays the current status of CORS support.
get certreq	Generates a Certificate Signing Request.
get db backup info	Displays scheduled DB backup information.
get debug	Creates a debug information tarball file. This file can be used for debugging.
get debug verbose	Creates a basic debug information tarball.
get debug ondemand	Displays the debug information.
get device upgrade bundles	Displays information about device upgrade bundles available in the local repository.
get device repo config	Displays configuration (Mode and Hostnames) for repositories that store upgrade bundles and device capability information.
get idle timeout	Displays the current idle timeout value. A value of 0 indicates no timeout.
get integrity status	Checks the integrity of critical server components.
get ha	Displays High Availability (HA) Pair configuration and service status.
get lldp	Displays the LLDP configuration.
get remote logging	Displays the remote logging configuration.
get log config	Displays the logger configuration.
get log level gui	Displays log levels of GUI modules.
get log level aruba	Displays the log level of Aruba Mobility Controller Adapter module.
get log level wlc	Displays the log level of the Cisco WLC Adapter module.
get log level msmcontroller	Displays the log level of HP MSM Controller Integration.
get msmcontroller cert	Generates a self-signed certificate for HP Adapter.

Command	Description
get msmcontroller certreq	Generates a Certificate Signing Request for HP Adapter.
get access address	Shows access IP Address/Hostname of this server.
get server config	Displays complete server configuration.
get server cert	Uploads server certificate to a remote host.
get server check	Runs a server consistency check and displays results. If any fatal item fails, a failure result is recorded.
get server tag	Displays the custom tag set by the user.
get serverid	Displays the server ID.
get sensor debug logs	Uploads AP debug logs to the specified upload URL.
get sensor list	Displays the list of APs.
get sensor reset button	Displays the state of the AP's pinhole reset button.
get status	Displays the status of server processes.
get ssh	Displays the SSH server status.
get version	Displays the version and build of all the server components.
get packet capture	Captures packets on Public and HA/Management network interface(s).
set scan config	Modify AP background scanning parameters.
set openconfig mode	Enable/disable OpenConfig mode.
set cert	Installs a signed SSL certificate.
set cors	Enables or disables CORS support.
set dbserver	Starts/stops database server.
set db backup info	Sets scheduled DB backup information.
set device capability	Updates the device capability information.
set device upgrade bundles	Upload/delete device upgrade bundles in the local repository.
set device repo config	Sets configuration (Mode and Hostnames) for repositories that store upgrade bundles and device capability information.
set erase	Configures the backspace key.
set ha dead time	Changes the Dead Time of High Availability (HA) service.
set ha link timeout	Sets the timeout in seconds to signal Data Sync Link failure.
set idle timeout <*timeout-in-minutes*>	Sets the idle timeout for the command shell. A value of 0 disables the idle timeout.

Command	Description
set lldp	Sets LLDP configuration.
set remote logging	Sets remote logging configuration.
set log config	Sets the configuration of the logger.
set log level gui	Sets log levels of GUI modules.
set log level aruba	Sets the log level of Aruba Mobility Controller Adapter Module.
set log level wlc	Sets log level of Cisco WLC Adapter Module.
set log level msmcontroller	Sets log level of HP MSM Controller Integration.
set msmcontroller cert	Installs a signed SSL certificate for HP Adapter.
set loginid case sensitivity	Toggles login ID case sensitivity.
set server	Starts/stops application server.
set server discovery	Changes server discovery settings on given AP(s).
set server tag	Configure a custom tag for files generated by this server.
set access address	Sets access IP Address/Hostname of the server.
set serverid	Sets server ID.
set ssh	Starts/stops SSH access to the server.
set communication passphrase	Sets the communication passphrase used for AP-server authentication and to encrypt the communication between APs and the server.
set communication key	Sets the communication key used for AP-server authentication and to encrypt the communication between APs and the server.
set communication key default	Resets the communication key used for AP-server authentication and to encrypt the communication between APs and the server.
set sensor legacy authentication	This allows/disallows APs running on versions lower than 6.2 to connect to the server.
set sensor reset button	Sets the state of the AP's pinhole reset button (select AP models only).
set smart device oui	Add, remove MAC OUI's for specific smart device type IDs.
set webserver	Starts/stops web server.
set wlc mapper	Manage Cisco WLC Custom Mapper file.
exit	Exits the config shell session.
ping <*Hostname/IP Address*>	Ping a host.
reset locked gui	Unlocks Graphical User Interface (GUI) account for the "admin" user.

Command	**Description**
reset password gui	Sets Graphical User Interface (GUI) password for the "admin" user to factory default value.
upload db backup	Uploads successful DB backup(s) to an external server.
application signature update	Updates app visibility signature.

General Customizations

CloudVision Portal (CVP) enables you to customize the grid columns of CVP graphical user interface (GUI) pages. You can customize the grid columns of all CVP GUI grids.

CVP also enables you to easily paginate (navigate) through the pages of the grids of the GUI. The pagination controls are available in all grids.

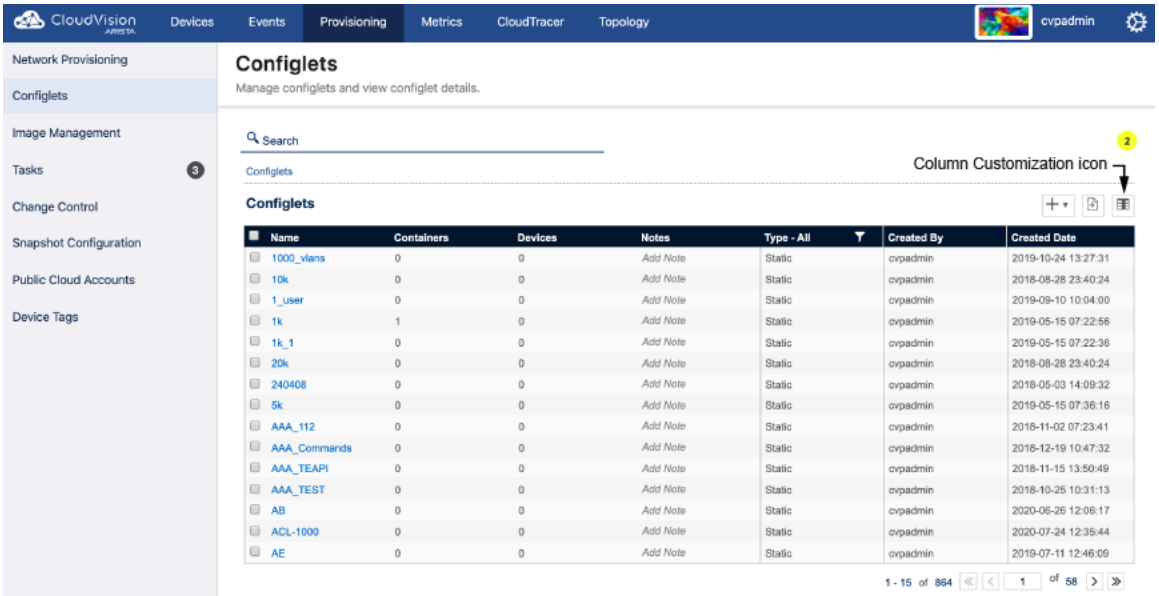
- Column Customization
- Pagination Controls

6.1 Column Customization

CloudVision Portal (CVP) enables you to customize the columns of the grids of CVP graphical user interface (GUI) pages. You can customize columns of any grid of the CVP GUI.

You use the **Columns Settings** dialog to customize the columns of the active grid. You can open the **Columns Settings** dialog by clicking the column customization icon, which is available of every page of the GUI.

Figure 6-1: Configlet Management page



Configlets

Manage configlets and view configlet details.

Configlets

Configlets

□	Name	Containers	Devices	Notes	Type - All	Created By	Created Date
□	1000_vlans	0	0	*Add Note*	Static	cvpadmin	2019-10-24 13:27:31
□	10k	0	0	*Add Note*	Static	cvpadmin	2018-08-28 23:40:24
□	1_user	0	0	*Add Note*	Static	cvpadmin	2019-09-10 10:04:00
□	1k	1	0	*Add Note*	Static	cvpadmin	2019-05-15 07:22:56
□	1k_1	0	0	*Add Note*	Static	cvpadmin	2019-05-15 07:22:36
□	20k	0	0	*Add Note*	Static	cvpadmin	2018-08-28 23:40:24
□	240408	0	0	*Add Note*	Static	cvpadmin	2018-05-03 14:09:32
□	5k	0	0	*Add Note*	Static	cvpadmin	2019-05-15 07:36:16
□	AAA_112	0	0	*Add Note*	Static	cvpadmin	2018-11-02 07:23:41
□	AAA_Commands	0	0	*Add Note*	Static	cvpadmin	2018-12-19 10:47:32
□	AAA_TEAPI	0	0	*Add Note*	Static	cvpadmin	2018-11-15 13:50:49
□	AAA_TEST	0	0	*Add Note*	Static	cvpadmin	2018-10-25 10:31:13
□	AB	0	0	*Add Note*	Static	cvpadmin	2020-06-26 12:06:17
□	ACL-1000	0	0	*Add Note*	Static	cvpadmin	2020-07-24 12:35:44
□	AE	0	0	*Add Note*	Static	cvpadmin	2019-07-11 12:46:09

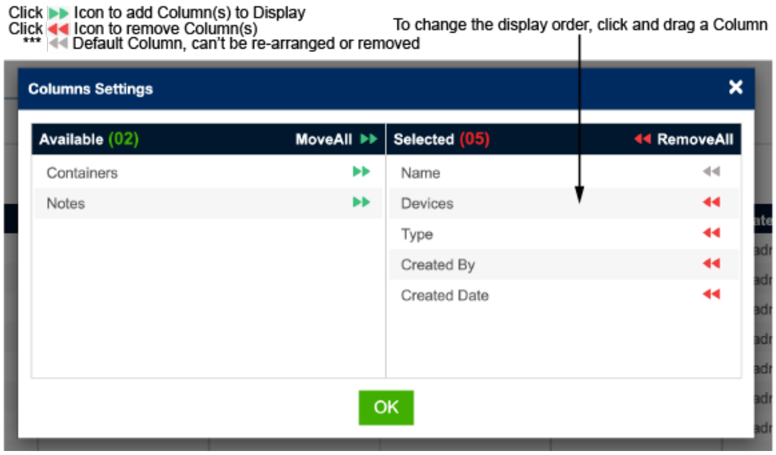
1 - 15 of 864 « ‹ 1 of 58 › »

Complete these steps to customize grid columns.

1. Go to a page that has the grid you want to customize.

2. Click the column customization icon.

Figure 6-2: Column Settings dialog


Click ▶▶ Icon to add Column(s) to Display
Click ◀◀ Icon to remove Column(s)
*** ◀◀ Default Column, can't be re-arranged or removed

To change the display order, click and drag a Column

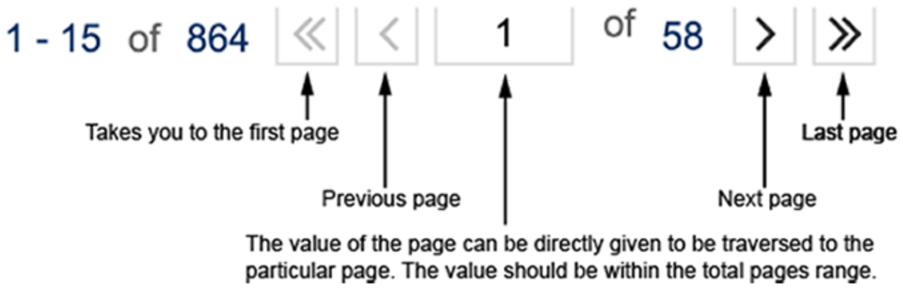
3. Use the arrow icons to rearrange the columns of the grid as needed.
4. Once you are done rearranging the grid columns, click **OK** to save the changes.

6.2 Pagination Controls

The pagination controls you use to navigate through the pages of grids are available for each grid. The controls enable you to:

- Go to the previous page of the grid
- Go to the next page of the grid
- Go to the first page of the grid
- Go to the last page of the grid
- Go to directly to a specific page

Figure 6-3: Pagination controls of the CVP GUI grids



Takes you to the first page

Previous page

Next page

Last page

The value of the page can be directly given to be traversed to the particular page. The value should be within the total pages range.

Chapter 7

Device Management

CloudVision Portal (CVP) provides a powerful, event-driven, streaming analytics platform that enables you to monitor the state of all devices currently managed by CVP.

By configuring devices to stream device-state data to CVP, you can manage all of the devices in your current inventory of devices to gain valuable insights into the state of your devices, including real-time updates about changes in device state.

The device inventory is comprised of all devices that you have imported into CVP. After a device is imported into CVP, it can be configured and monitored using the various CVP modules.

7.1 Requirements

Make sure you review the software and hardware requirements for deploying and using the Telemetry platform before you begin deploying the platform.

System Requirements

Note: If you upgraded from a previous version of CVP, you must verify that all of the CVP node VMs on which you want to enable Telemetry have the required resources to use Telemetry. See *Resource Checks* for details on how to check CVP node VM resources and perform any modifications needed to increase the current CVP node VM resources.

Verify the clocks on the switches are synchronized to an NTP server.

- If a clock on a device is not synched to an NTP server on the switches and the clock difference between CVP and the device is larger than 300 seconds, onboarding will fail.
- Streaming latency which must be less than 500ms as per our system requirements. Streaming latency is the time difference between the TerminAttr agent receiving the state change on a device and the notification being processed by the CloudVision Analytics backend after storage in NetDB. Without NTP the relative streaming latency between devices streaming to CVP can exceed limits and state changes

happening on different switches may appear to be incorrectly ordered within CVP. For more information refer to: https://www.arista.com/en/cg-cv/cv-system-requirements

7.2 Limitations

The following table lists the current limitations of the Telemetry platform. Review the limitations to ensure you do not inadvertently attempt configurations that exceed the limitations.

Table 10: CVP Telemetry Platform Limitations

Limitations	
Maximum number of devices	This represents the total number of devices currently configured to stream Telemetry data.
Device-state data	Streaming of LANZ data is not enabled by default. You must enable it on devices.
Secret configuration	If "enable secret" or "enable password" is configured, the secret must be the same as the Cloudvision user's password.

7.3 Features

The list the current supported and unsupported Telemetry platform features are provided in the following topics:

- Supported Features
- Unsupported Features

7.3.1 Supported Features

The CVP Telemetry Supported Features table lists the supported features. Review the supported features to ensure you are aware of the features available to you to monitor devices using Telemetry data.

Table 11: CVP Telemetry Supported Features

	Supported Feature
Real-time monitoring of devices	The Telemetry platform provides interfaces for viewing real-time updates about changes in device state as well as events. You can also view trends in device-state metrics and queries of historical device-state data.
Instant state change updates	Changes in the state of a device are instantly streamed to CVP.
Full state change data	All changes in device-state are captured and streamed to CVP for viewing. Types of device-state include: • All SysDB state (except state under /Sysdb/cell/*). • All SMASH tables. • Process and kernel data (for example, CPU and memory usage). • System log messages
Analytics engine	The Telemetry platform provides a robust analytics engine that aggregates the streamed device-state data across devices, monitors device state, and generates events to indicate issues. It also normalizes data so it is easier for other applications to use.
Telemetry events	Device-state and system environment event types are streamed to CVP: • Informational (updates about changes in device state). • Warning (for example, unsupported EOS version on a device) • Errors (data discards or input errors on interfaces, and more). • Critical (system environment issues such as overheating).
High performance database	The Telemetry platform utilizes a high performance Hbase database to store device-state data, including events. Data is stored in compressed format without a loss of resolution. • The data storage capacity is approximately: • 43200 records worth of raw data per path • 5 days of 10 second aggregated data • 4 weeks of 60 second aggregated data • 3 months worth of 15 minute aggregated data
Disk space protection	To prevent telemetry data from consuming too much disk space in the CVP cluster, the Telemetry platform automatically blocks the ingest port for the entire cluster if disk usage exceeds **85%** on any node of the cluster. Once the ingest port is blocked, it remains blocked until disk usage drops below **80%** on all nodes in the cluster.
Data management	To ensure that the most relevant data is given priority, the Telemetry platform provides automated data management, including: • Maximum time limit on stored device-state data (1 month). • Current and the most recent device-state updates are always stored (given priority over older state updates). Periodic clean-up jobs are executed weekly (Saturday at 11:00 P.M.). Old device-state data is purged.

Command support	Several commands are provided for: • Checking status of the Telemetry components. • Enabling and disabling of Telemetry platform components. • Starting and stopping Telemetry components. • Viewing the debug log for Telemetry components. • Troubleshooting the Telemetry components, including checking to see that logs are being created for the component. • To display granular information on disk space usage of telemetry data and delete telemetry data selectively.

7.3.2 Unsupported Features

The CVP Telemetry Unsupported Features table lists the unsupported features. Review the limitations to ensure you do not inadvertently attempt to configure or use unsupported Telemetry features.

Table 12: CVP Telemetry Unsupported Features

	Unsupported Feature
Streamed device-state data	Flexroute is not supported.

7.4 Telemetry Platform Components

Arista's streaming Telemetry platform consists of a set of components, all of which are essential to the proper operation of the platform.

The components of the Telemetry platform are:

- NetDB State Streaming Component
- CloudVision Analytics Engine Component
- REST and Websocket based APIs are available to programatically get data from the CloudVision Analytics Engine. Contact your Arista Sales Engineer for more information.

7.4.1 NetDB State Streaming Component

The NetDB State Streaming component is an agent that runs on Arista switches. It is the Telemetry platform component that streams device-state data from devices to the CloudVision Analytics Engine, which is the back-end component of platform.

7.4.2 CloudVision Analytics Engine Component

The CloudVision Analytics Engine is the back-end component of the Telemetry platform. It is a set of processes that run on CVP. Collectively, the processes perform the following operations:

- Receives all of the device-state data streamed by the NetDB State Streaming component from devices that have been configured to stream device-state data.
- Runs automated data analysis on the device-state data received from the NetDB State Streaming component. The analytics processes aggregate the device-state data across devices, monitor device state, and generate events if something goes wrong. The processes also normalize data so it is easier for other applications to use.
- Stores all of the streamed device-state data received from the NetDB State Streaming component, and then makes the stored data available in CloudVision.

- Provides CloudVision Analytics Engine Viewer, which is referred to as the Aeris Browser. You use it to directly view device-state data received from devices that have been configured to stream device-state data. The Aeris Browser enables you to view raw device-state data.
- REST and Websocket based APIs are available to programatically get data from the CloudVision Analytics Engine. Contact your Arista Sales Engineer for more information.

7.5 Supplementary Services: Splunk

For more information on the requirements for CVP to manage Splunk extensions on EOS devices, go to https://www.arista.com/en/support/software-download and download the PDF from **Extensions > Splunk > AristaTelemetry.pdf**.

Related topics:

- Requirement
- Installation
- Quick Start

7.5.1 Requirement

EOS 4.15.2 or later is required.

7.5.2 Installation

You can access the Splunk Telemetry App directly from CVP by completing the following steps. From your browser.

1. Copy the RPM to and install it on the switch.

```
show extensions
Name Version/Release Status RPMs
```

2. Install the Splunk Universal Forwarder RPM on EOS.

```
copy <source>/splunkforwarder-6.1.4-233537.i386.rpm extension:
extension splunkforwarder-6.1.4-233537.i386.rpm
```

3. Install the AristaAppForSplunk on EOS.

```
copy <source>/AristaAppForSplunk-1.3.2.swix extension:
extension AristaAppForSplunk-1.3.2.swix
```

Note: Extensions must be installed on all supervisors.

Restart the SuperServer agent.

```
(config)# agent SuperServer shutdown
(config-mgmt-api-http-cmds)# no agent SuperServer shutdown
```

4. Verify the extensions are loaded.

```
show extensions
Name Version/Release Status RPMs
------------------------------------------ ------------------------- ---
AristaAppForSplunk-<version>.swix <version>/1.fc14 A, I 3
splunkforwarder-6.1.4-233537.i386.rpm 6.1.4/233537 A, I 1
EosSdk-1.7.0-4.15.2F.i686.rpm 1.7.0/2692966.gaevanseoss A, I 1
A: available | NA: not available | I: installed | NI: not installed | F: f
```

7.5.3 Quick Start

1. Use the configuration to enable forwarding to the Splunk indexer. This assumes that a username/password and eAPI have been configured for the AristaAppForSplunk extension previously.

```
daemon SplunkForwarder
 exec /usr/bin/SplunkAgent
 no shutdown
```

2. Configure and turn on the desired indexes for data collection. The credentials must match 'username <name> secret <passphrase>' configured on the switch.

```
option eapi_username value <username>
 option eapi_password value 7 <encrypted-password>
 option eapi_protocol value https
```

3. Turn on desired indexes for data collection.

```
option index-inventory value on
 option index-interface-counters value on
 option index-lanz value on
 option index-topology value on
 option index-syslog value on
 option index-data value <index-name
```

4. Configure Splunk server IP and destination port.

```
option splunk-server value <Server-IP:Port>
```

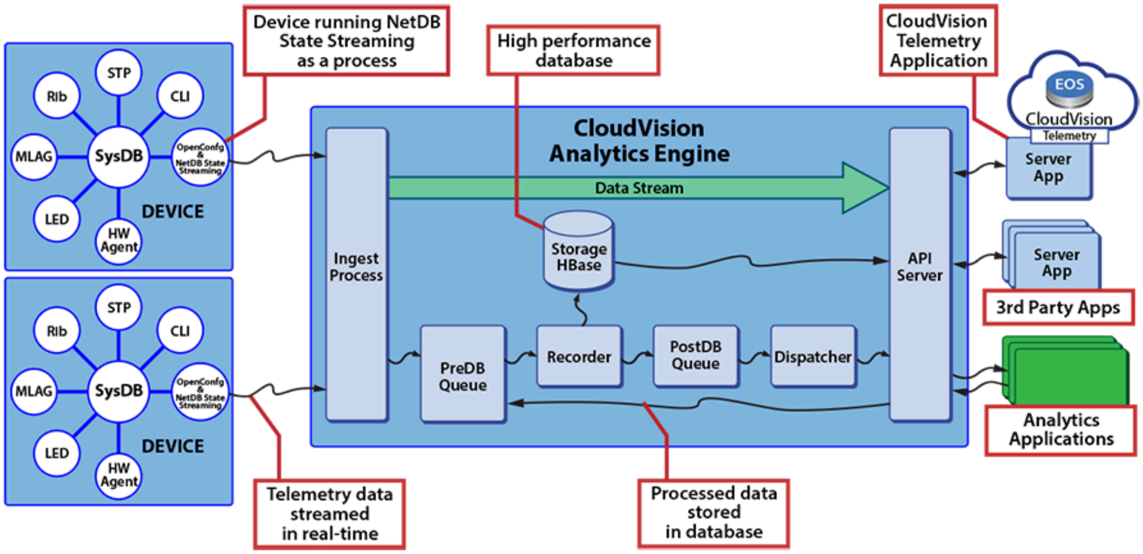
5. Start Splunk data forwarding.

```
option shutdown value off
```

7.6 Architecture

Telemetry Platform Architecture shows the architecture of the Telemetry platform, including all of the platform components and the data path of the streamed device-state data.

Figure 7-1: Telemetry Platform Architecture


Device running NetDB State Streaming as a process
High performance database
CloudVision Telemetry Application
EOS
CloudVision
Telemetry
STP
RIb
CLI
MLAG
SysDB
OpenConfig & NetDB State Streaming
LED
HW Agent
DEVICE
STP
RIb
CLI
MLAG
SysDB
OpenConfig & NetDB State Streaming
LED
HW Agent
DEVICE
CloudVision Analytics Engine
Data Stream
Ingest Process
Storage HBase
API Server
Server App
Server App
3rd Party Apps
PreDB Queue
Recorder
PostDB Queue
Dispatcher
Analytics Applications
Telemetry data streamed in real-time
Processed data stored in database

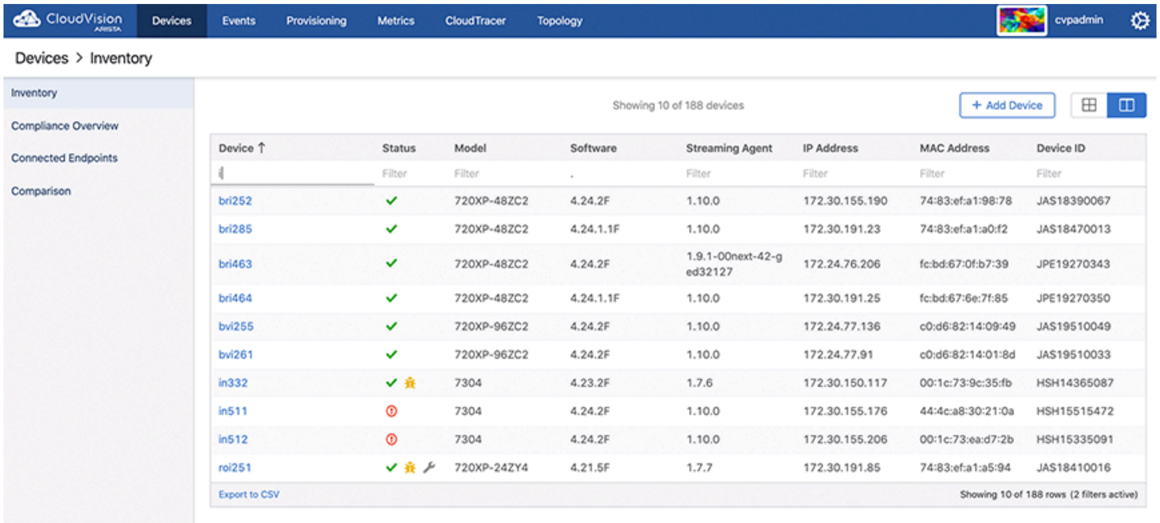
7.7 Accessing the Telemetry Browser Screen

You can access the CloudVision Telemetry Browser screen directly from CVP by completing the following steps. Open your browser.

1. Point your browser to the CVP IP address or hostname.
2. Login to CVP.

   The CVP Home screen appears.

   Figure 7-2: CVP Home Screen



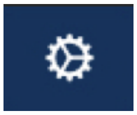
Showing 10 of 188 devices

Device ↑	Status	Model	Software	Streaming Agent	IP Address	MAC Address	Device ID
i	Filter	Filter	.	Filter	Filter	Filter	Filter
bri252	✓	720XP-48ZC2	4.24.2F	1.10.0	172.30.155.190	74:83:ef:a1:98:78	JAS18390067
bri285	✓	720XP-48ZC2	4.24.1.1F	1.10.0	172.30.191.23	74:83:ef:a1:a0:f2	JAS18470013
bri463	✓	720XP-48ZC2	4.24.2F	1.9.1-00next-42-ged32127	172.24.76.206	fc:bd:67:0f:b7:39	JPE19270343
bri464	✓	720XP-48ZC2	4.24.1.1F	1.10.0	172.30.191.25	fc:bd:67:6e:7f:85	JPE19270350
bvi255	✓	720XP-96ZC2	4.24.2F	1.10.0	172.24.77.136	c0:d6:82:14:09:49	JAS19510049
bvi261	✓	720XP-96ZC2	4.24.2F	1.10.0	172.24.77.91	c0:d6:82:14:01:8d	JAS19510033
in332	✓ 🐞	7304	4.23.2F	1.7.6	172.30.150.117	00:1c:73:9c:35:fb	HSH14365087
in511	ⓘ	7304	4.24.2F	1.10.0	172.30.155.176	44:4c:a8:30:21:0a	HSH15515472
in512	ⓘ	7304	4.24.2F	1.10.0	172.30.155.206	00:1c:73:ea:d7:2b	HSH15335091
roi251	✓ 🐞 🔧	720XP-24ZY4	4.21.5F	1.7.7	172.30.191.85	74:83:ef:a1:a5:94	JAS18410016

Showing 10 of 188 rows (2 filters active)

3. Click the gear icon at the upper right corner of the screen.

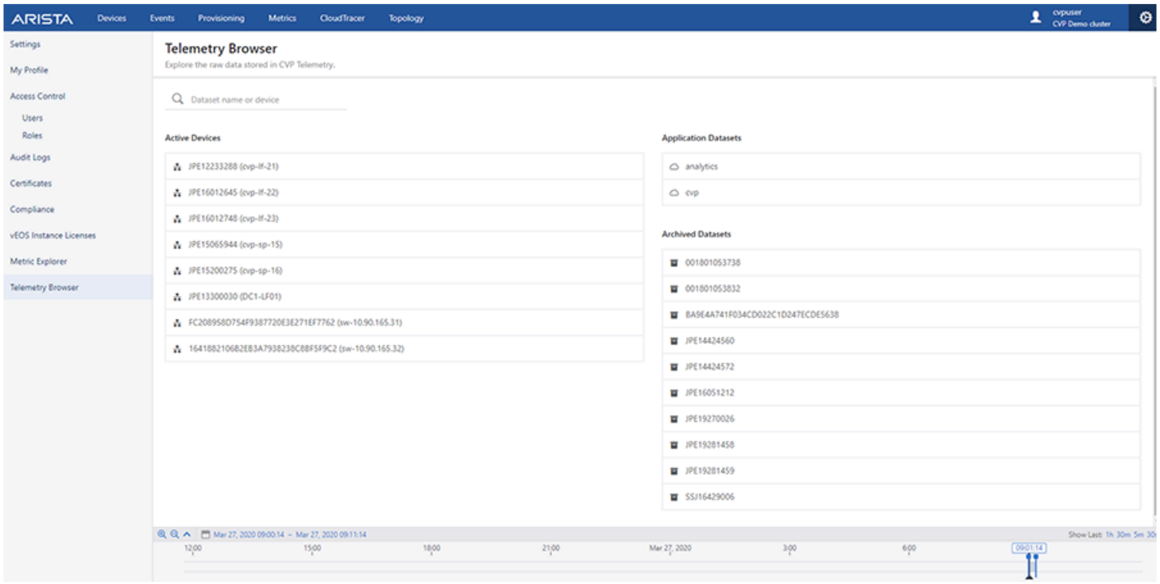
   Figure 7-3: Gear Icon



4. Click Telemetry Browser in the left pane.

The system opens the Telemetry Browser screen that allows exploring the raw data stored in CVP telemetry.

Figure 7-4: CloudVision Telemetry Browser Screen



Telemetry Browser

Explore the raw data stored in CVP Telemetry.

Active Devices

- JPE12233288 (cvp-lf-21)
- JPE16012645 (cvp-lf-22)
- JPE16012748 (cvp-lf-23)
- JPE15065944 (cvp-sp-15)
- JPE15200275 (cvp-sp-16)
- JPE13300030 (DC1-LF01)
- FC208958D754F9387720E3E271EF7762 (sw-10.90.165.31)
- 1641882106B2EB3A7938238C8BF5F9C2 (sw-10.90.165.32)

Application Datasets

- analytics
- cvp

Archived Datasets

- 001801053738
- 001801053832
- BA9E4A741F034CD022C1D247ECDE5638
- JPE14424560
- JPE14424572
- JPE16051212
- JPE19270026
- JPE19281458
- JPE19281459
- SSJ16429006

Mar 27, 2020 09:00:14 - Mar 27, 2020 09:11:14

12:00 15:00 18:00 21:00 Mar 27, 2020 3:00 6:00 09:01:14

7.8 Viewing Devices

You can quickly view information about devices that are currently configured to stream device-state data to CVP. Starting with *2018.2.0*, the inventory management screen is available under Devices in the CVP user interface.

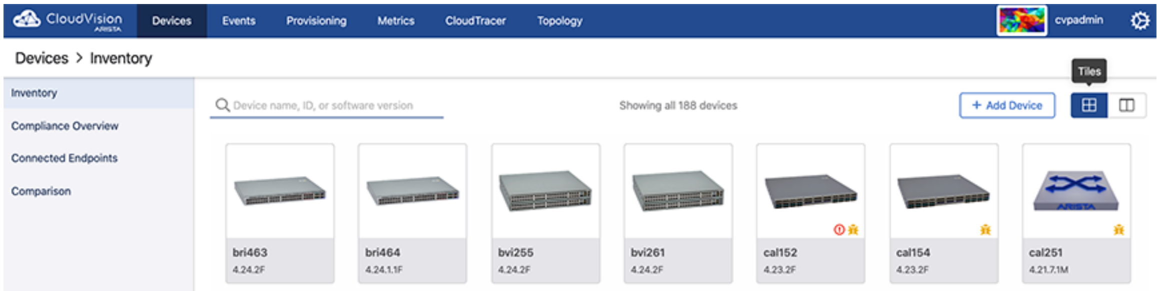
Related topics:

- Tiles View
- Tabular View

7.8.1 Tiles View

The tiles view allows search by device hostname, serial number, or EOS version. The screen updates to show all of the devices currently configured to stream device-state data to CVP. For each device, the name and the version of the EOS image are shown on the Devices screen.

Figure 7-5: Viewing Devices (View Showing all Devices)



bri463 4.24.2F

bri464 4.24.1.1F

bvi255 4.24.2F

bvi261 4.24.2F

cal152 4.23.2F

cal154 4.23.2F

cal251 4.21.7.1M

7.8.2 Tabular View

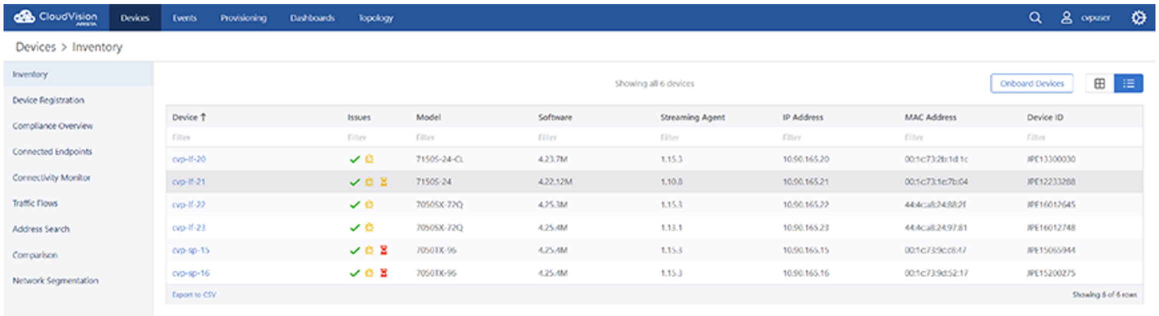
The tabular view lists device status, model, software, TerminAttr agent, IP address, MAC address, and serial number. You can search for devices based on device hostname, serial number, or EOS version.

Note: In the status column, hover the cursor over the following images for specified tasks:

- Check and exclamatory marks to view streaming status
- Bug image to view the count of available vulnerability updates
- Hourglass to view the End Of Life (EOL) status

  An amber hourglass signifies that the end of life is within 6 months, a red hourglass signifies that the End of Life has been reached.

Figure 7-6: Device Inventory



Device ↑	Issues	Model	Software	Streaming Agent	IP Address	MAC Address	Device ID
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
cvp-lf-20	✓ 🐞	7150S-24-CL	4.23.7M	1.15.3	10.90.165.20	00:1c:73:2b:1d:1c	JPE13300030
cvp-lf-21	✓ 🐞 ⌛	7150S-24	4.22.12M	1.10.8	10.90.165.21	00:1c:73:1e:7b:04	JPE12233288
cvp-lf-22	✓ 🐞	7050SX-72Q	4.25.3M	1.15.3	10.90.165.22	44:4c:a8:24:88:2f	JPE16012645
cvp-lf-23	✓ 🐞	7050SX-72Q	4.25.4M	1.13.1	10.90.165.23	44:4c:a8:24:97:81	JPE16012748
cvp-sp-15	✓ 🐞 ⌛	7050TX-96	4.25.4M	1.15.3	10.90.165.15	00:1c:73:9c:c8:47	JPE15065944
cvp-sp-16	✓ 🐞 ⌛	7050TX-96	4.25.4M	1.15.3	10.90.165.16	00:1c:73:9d:52:17	JPE15200275

Export to CSV

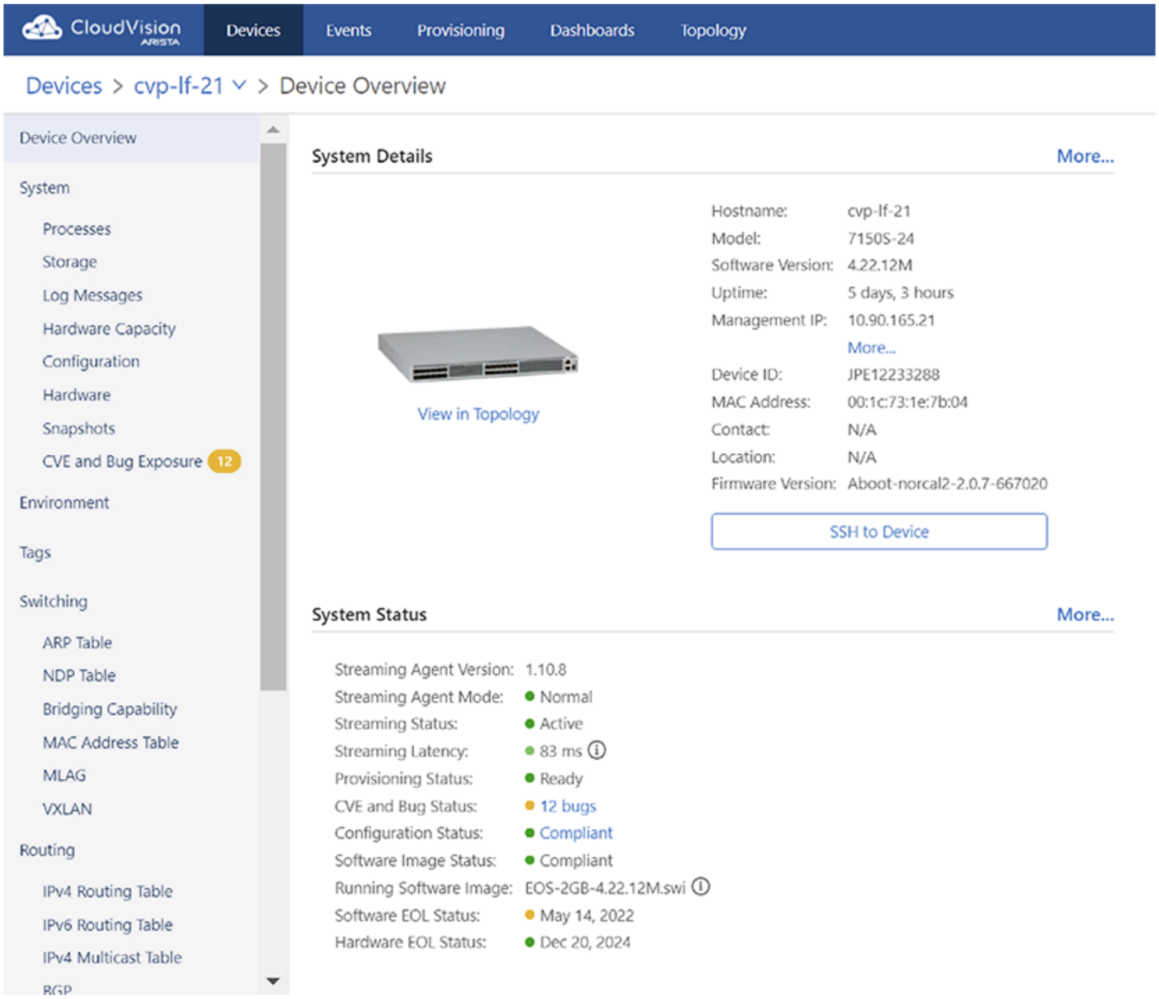
Showing 6 of 6 rows

7.9 Viewing Device Details

From the Inventory screen, you can quickly drill down to view details about a particular device by clicking the device icon. In the tabular view, click the device name to view the corresponding device details.

The screen refreshes to show the device-state data streamed from the device to CVP.

Figure 7-7: Viewing Devices Details (Single Device)



System Details

Hostname: cvp-lf-21
Model: 7150S-24
Software Version: 4.22.12M
Uptime: 5 days, 3 hours
Management IP: 10.90.165.21
More...
Device ID: JPE12233288
MAC Address: 00:1c:73:1e:7b:04
Contact: N/A
Location: N/A
Firmware Version: Aboot-norcal2-2.0.7-667020

System Status

Streaming Agent Version: 1.10.8
Streaming Agent Mode: ● Normal
Streaming Status: ● Active
Streaming Latency: ● 83 ms ⓘ
Provisioning Status: ● Ready
CVE and Bug Status: ● 12 bugs
Configuration Status: ● Compliant
Software Image Status: ● Compliant
Running Software Image: EOS-2GB-4.22.12M.swi ⓘ
Software EOL Status: ● May 14, 2022
Hardware EOL Status: ● Dec 20, 2024

Device details include the information on overview, system, compliance, environment, switching, routing, and interfaces.

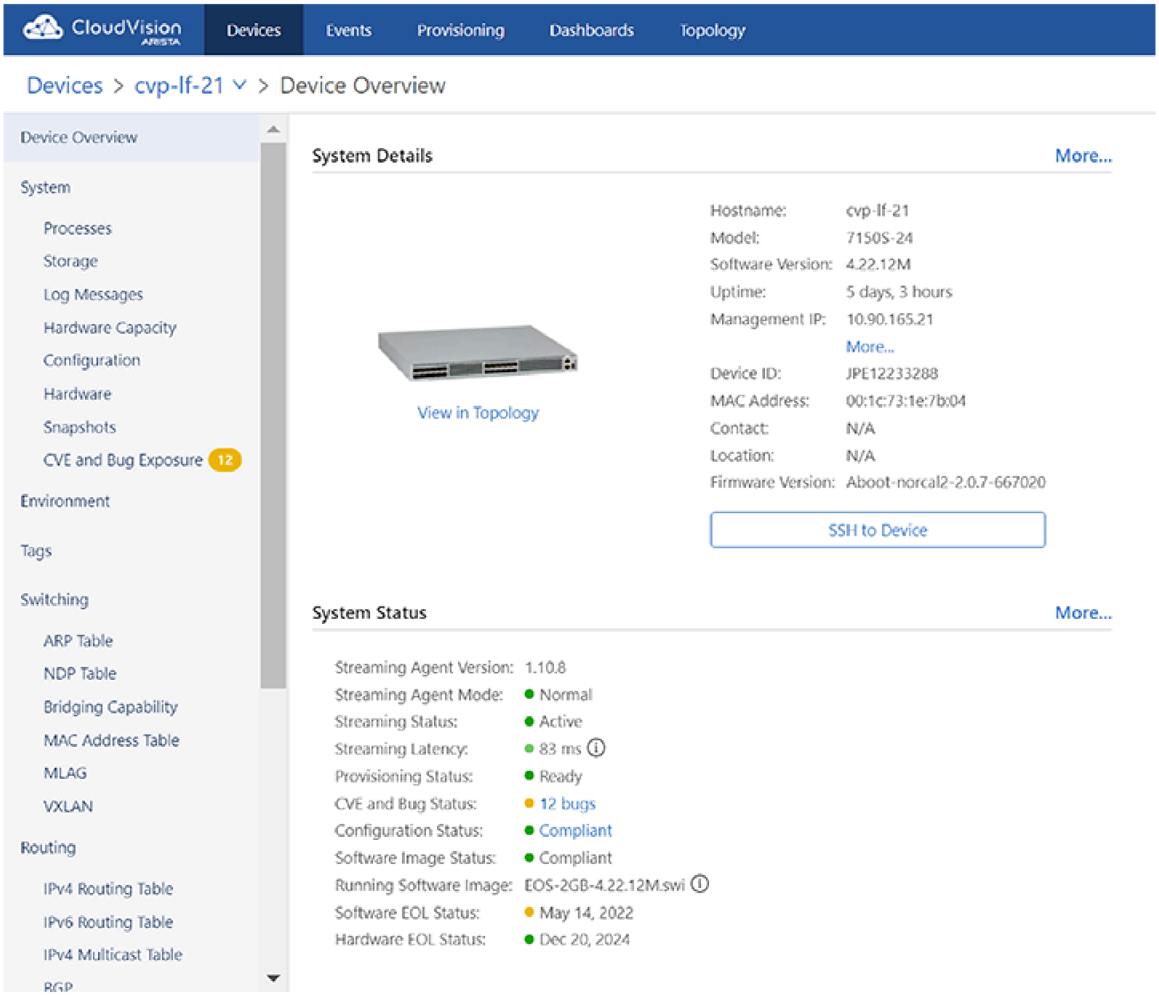
Related topics:

- Device Overview
- System Information
- Compliance
- Environment Details
- Switching Information
- Routing Information
- Status of Interfaces

7.9.1 Device Overview

The Device Overview section provides an overview of system details, telemetry status, and interface counts. Click **More** to reach corresponding sections for detailed information.

Figure 7-8: Device Overview Section



System Details

Hostname: cvp-lf-21
Model: 7150S-24
Software Version: 4.22.12M
Uptime: 5 days, 3 hours
Management IP: 10.90.165.21
More...
Device ID: JPE12233288
MAC Address: 00:1c:73:1e:7b:04
Contact: N/A
Location: N/A
Firmware Version: Aboot-norcal2-2.0.7-667020

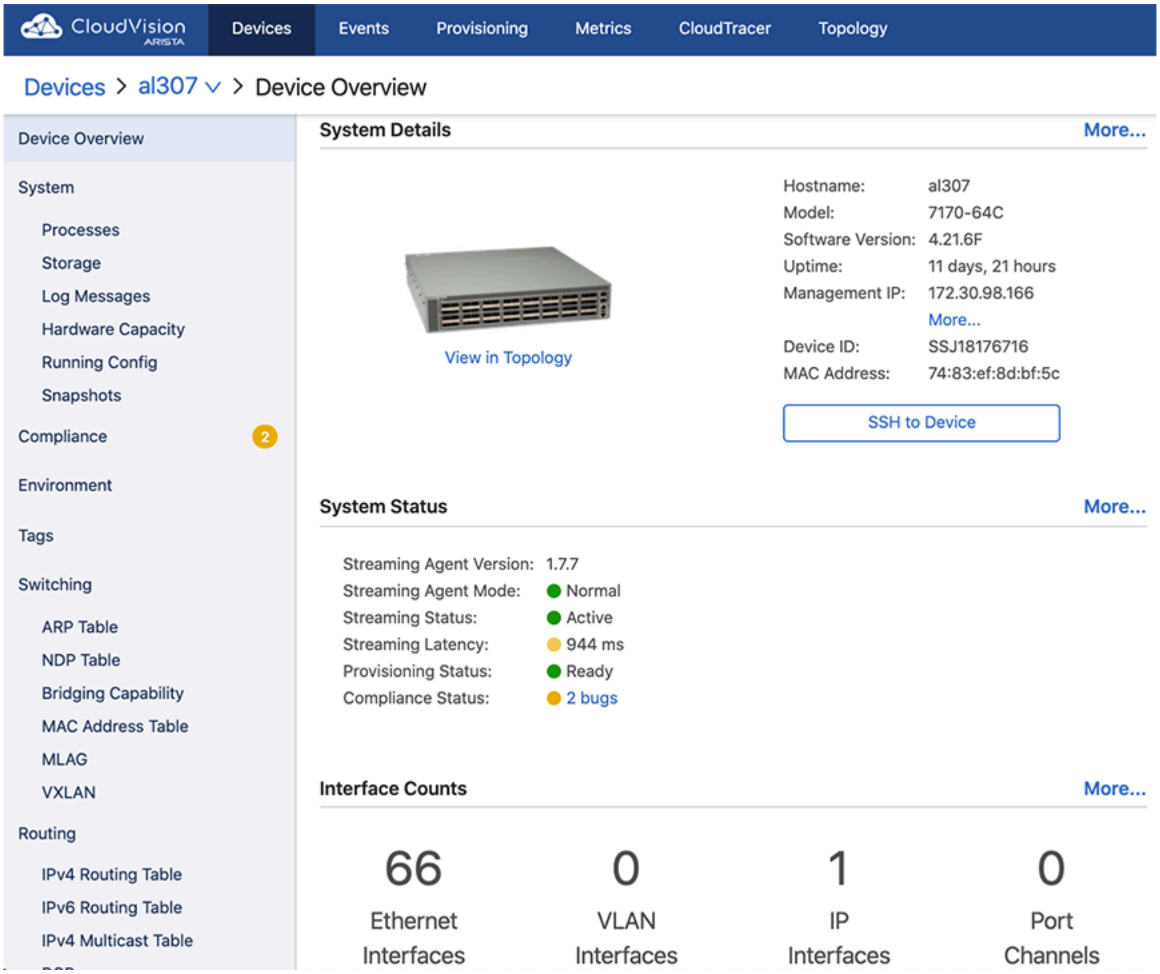
System Status

Streaming Agent Version: 1.10.8
Streaming Agent Mode: ● Normal
Streaming Status: ● Active
Streaming Latency: ● 83 ms ⓘ
Provisioning Status: ● Ready
CVE and Bug Status: ● 12 bugs
Configuration Status: ● Compliant
Software Image Status: ● Compliant
Running Software Image: EOS-2GB-4.22.12M.swi ⓘ
Software EOL Status: ● May 14, 2022
Hardware EOL Status: ● Dec 20, 2024

The Historical Comparison sub-section provides the information on EOS version, 5-minute CPU load average, MLAG status, IPv4 attached routes, IPV4 learned routes, configured BGP, IPv6 attached routes, IPV6 learned routes, and MAC addresses learned.

The system displays only Device Overview and System information for third-party devices.

Figure 7-9: Third-Party Device Overview



System Details

Hostname: al307
Model: 7170-64C
Software Version: 4.21.6F
Uptime: 11 days, 21 hours
Management IP: 172.30.98.166
More...
Device ID: SSJ18176716
MAC Address: 74:83:ef:8d:bf:5c

System Status

Streaming Agent Version: 1.7.7
Streaming Agent Mode: ● Normal
Streaming Status: ● Active
Streaming Latency: ● 944 ms
Provisioning Status: ● Ready
Compliance Status: ● 2 bugs

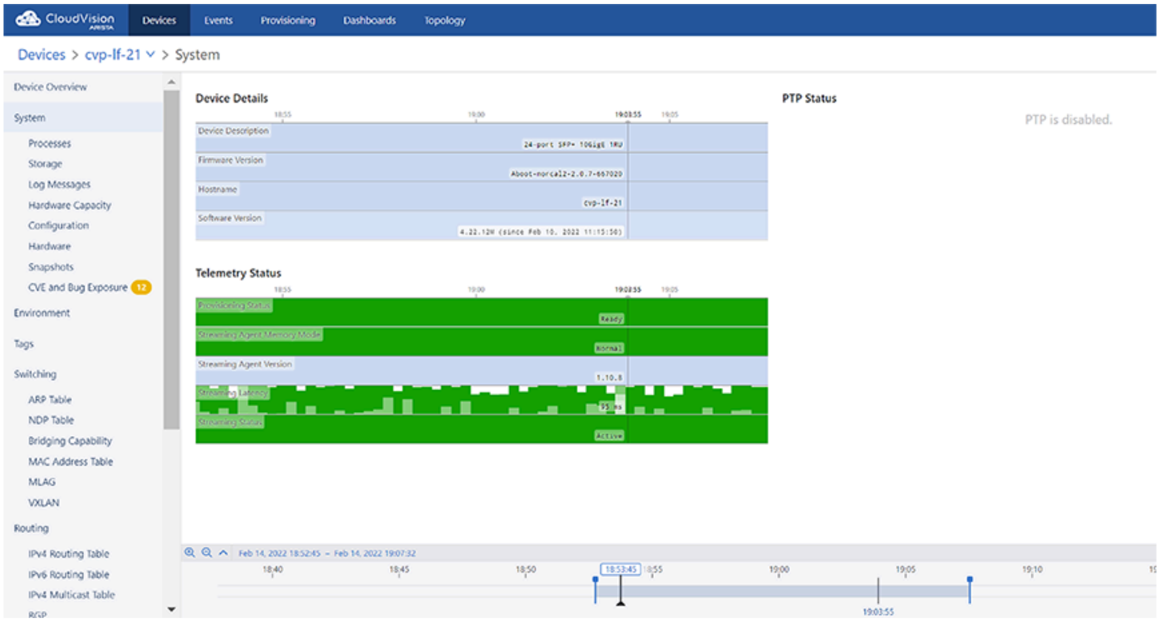
Interface Counts

66	0	1	0
Ethernet Interfaces	VLAN Interfaces	IP Interfaces	Port Channels

7.9.2 System Information

The System section provides an overview of device details, telemetry status, and PTP status.

Figure 7-10: System Section



Device Details

Device Description: 24-port SFP+ 10GigE 1RU
Firmware Version: Aboot-norcal2-2.0.7-667020
Hostname: cvp-lf-21
Software Version: 4.22.12M (since Feb 10, 2022 11:13:50)

Telemetry Status

Provisioning Status: Ready
Streaming Agent Memory Mode: Normal
Streaming Agent Version: 1.10.8
Streaming Latency: 95 ms
Streaming Status: Active

PTP Status

PTP is disabled.

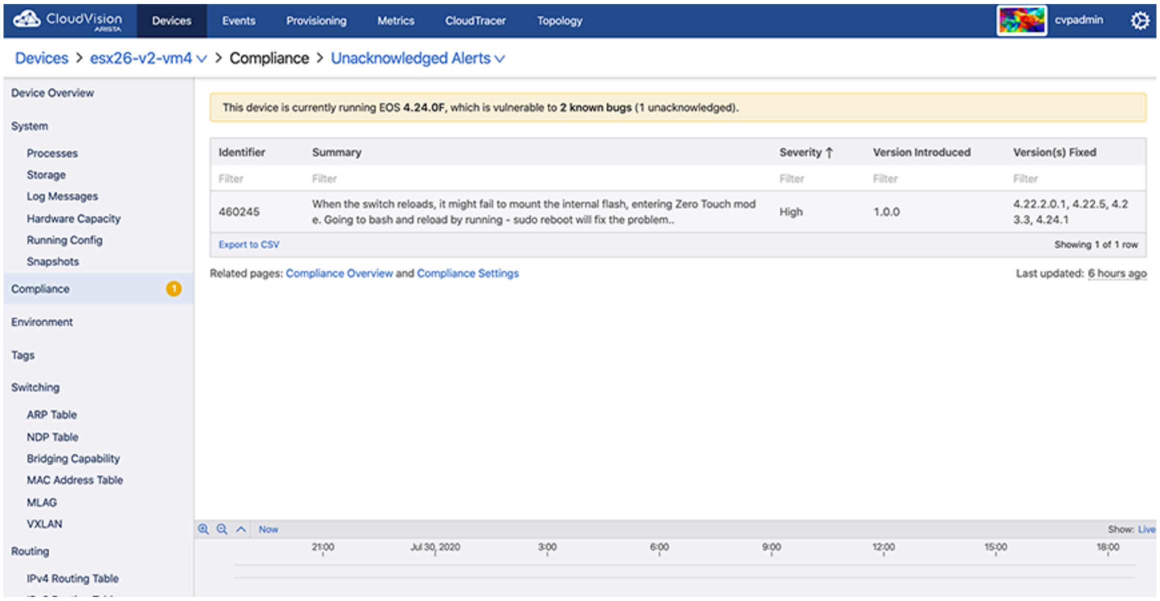
Feb 14, 2022 18:52:45 – Feb 14, 2022 19:07:32

Sub-sections provide information on processes, storage, log messages, hardware capacity, running config, and snapshots.

7.9.3 Compliance

The Compliance section provides information on vulnerability to known bugs.

Figure 7-11: Compliance Section



This device is currently running EOS **4.24.0F**, which is vulnerable to **2 known bugs** (1 unacknowledged).

Identifier	Summary	Severity ↑	Version Introduced	Version(s) Fixed
Filter	Filter	Filter	Filter	Filter
460245	When the switch reloads, it might fail to mount the internal flash, entering Zero Touch mode. Going to bash and reload by running - sudo reboot will fix the problem..	High	1.0.0	4.22.2.0.1, 4.22.5, 4.23.3, 4.24.1

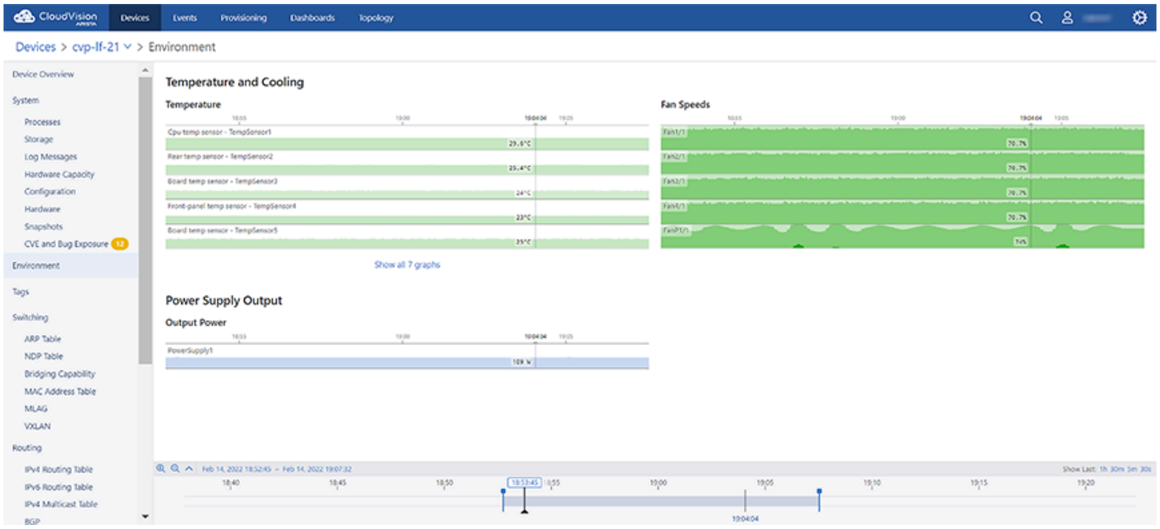
Export to CSV   Showing 1 of 1 row

Related pages: Compliance Overview and Compliance Settings   Last updated: 6 hours ago

7.9.4 Environment Details

The Environment section provides statistics on temperature, fan speeds, and output power.

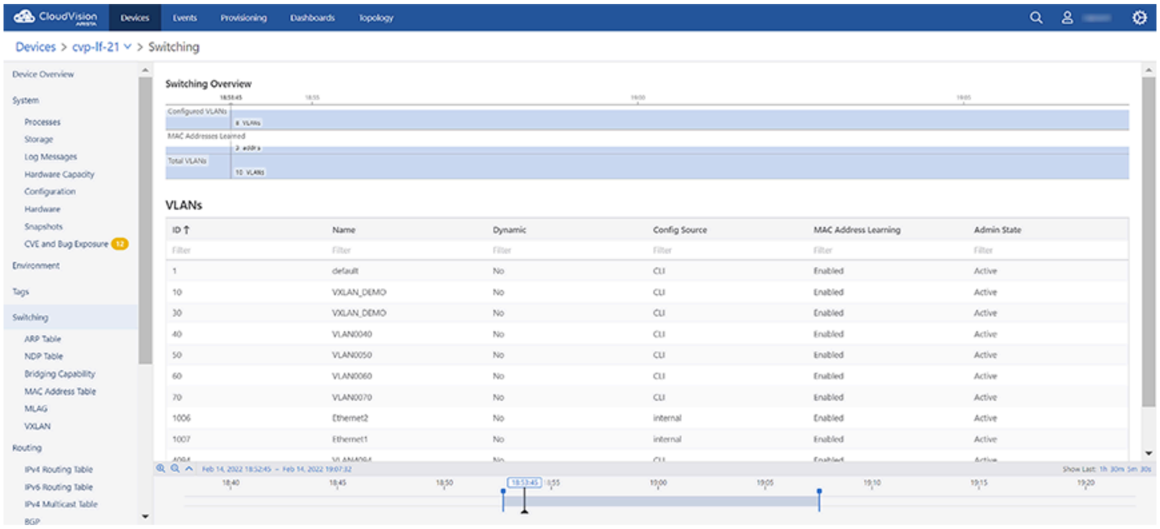
Figure 7-12: Environment Section



7.9.5 Switching Information

The Switching section provides the count of VLANs in which MAC address learning is enabled, count of total VLANs, count of configured VLANs, and detailed information on configured VLANs.

Figure 7-13: Switching Section



VLANs

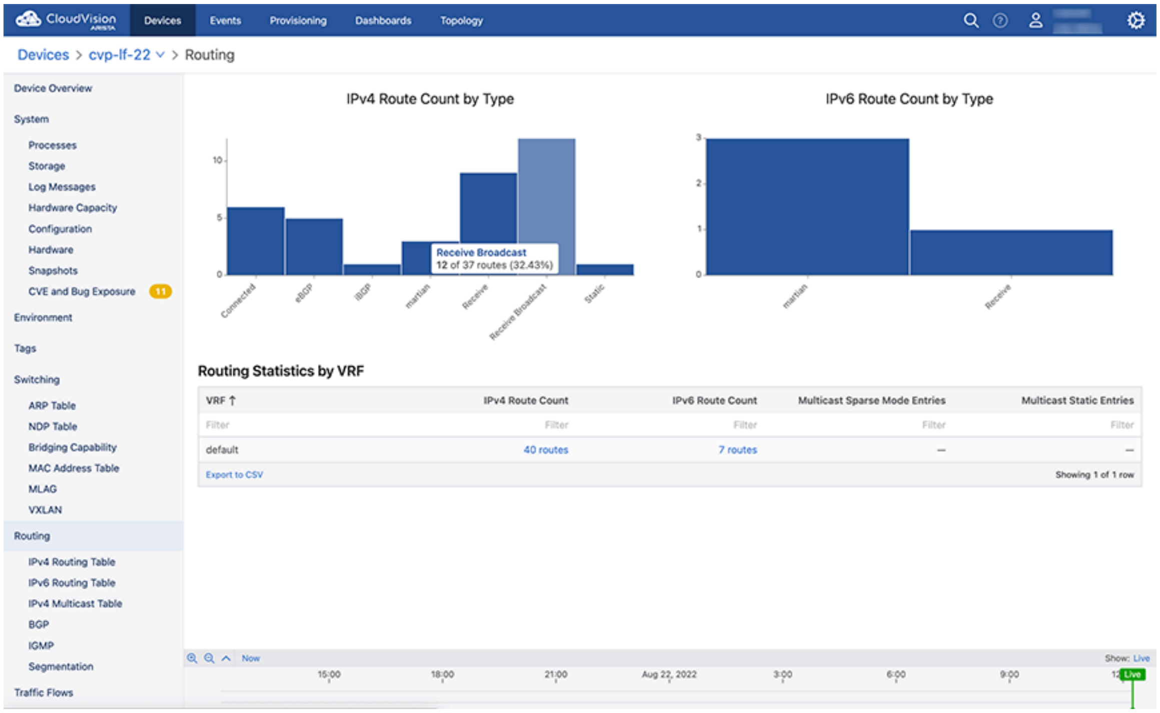
ID ↑	Name	Dynamic	Config Source	MAC Address Learning	Admin State
Filter	Filter	Filter	Filter	Filter	Filter
1	default	No	CLI	Enabled	Active
10	VXLAN_DEMO	No	CLI	Enabled	Active
30	VXLAN_DEMO	No	CLI	Enabled	Active
40	VLAN0040	No	CLI	Enabled	Active
50	VLAN0050	No	CLI	Enabled	Active
60	VLAN0060	No	CLI	Enabled	Active
70	VLAN0070	No	CLI	Enabled	Active
1006	Ethernet2	No	internal	Enabled	Active
1007	Ethernet1	No	internal	Enabled	Active
4094	VLAN4094	No	CLI	Enabled	Active

Sub-sections provide switching data like ARP table, NDP table, bridging capability, MAC address table, MLAG, and VXLAN.

7.9.6 Routing Information

The Routing section provides statistics on IPV4 route count by type, IPv6 route count by type, and routing statistics by VRF.

Figure 7-14: Routing Section



Routing Statistics by VRF

VRF ↑	IPv4 Route Count	IPv6 Route Count	Multicast Sparse Mode Entries	Multicast Static Entries
Filter	Filter	Filter	Filter	Filter
default	40 routes	7 routes	—	—

Export to CSV   Showing 1 of 1 row

Sub-sections provide routing data like IPv4 and IPv6 routing tables, routing table changes, multicast data like sparse mode PIM and static, and BGP information.

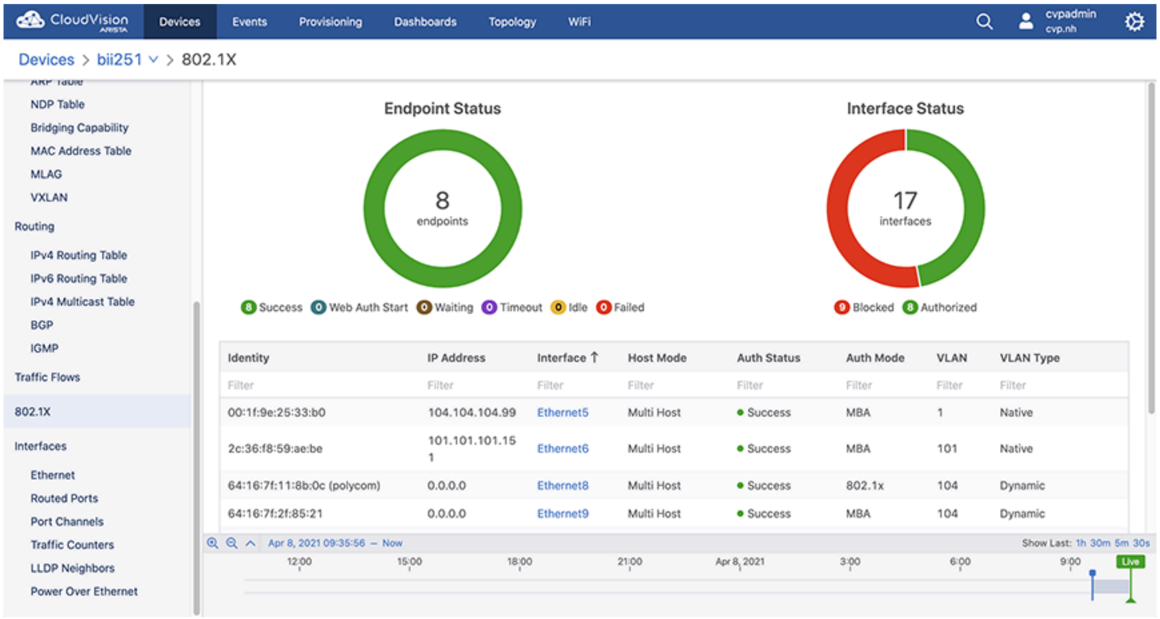
7.9.7 802.1X Metrics

802.1X information shows which endpoints have authenticated, are undergoing authentication, or have failed to authenticate to the network. This information is available to view primarily from the 802.1X page in the Devices application.

Accessing 802.1X Metrics

To access 802.1X Metrics From the Inventory screen in the **Devices** tab, select a device. In the scrolling menu on the left side of the page, select **801.X**. The 801.X Metrics page is displayed.

Figure 7-15: 802.1X Metrics



Identity	IP Address	Interface ↑	Host Mode	Auth Status	Auth Mode	VLAN	VLAN Type
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
00:1f:9e:25:33:b0	104.104.104.99	Ethernet5	Multi Host	● Success	MBA	1	Native
2c:36:f8:59:ae:be	101.101.101.151	Ethernet6	Multi Host	● Success	MBA	101	Native
64:16:7f:11:8b:0c (polycom)	0.0.0.0	Ethernet8	Multi Host	● Success	802.1x	104	Dynamic
64:16:7f:2f:85:21	0.0.0.0	Ethernet9	Multi Host	● Success	MBA	104	Dynamic

The graphs display the total number of interfaces and the status of each.

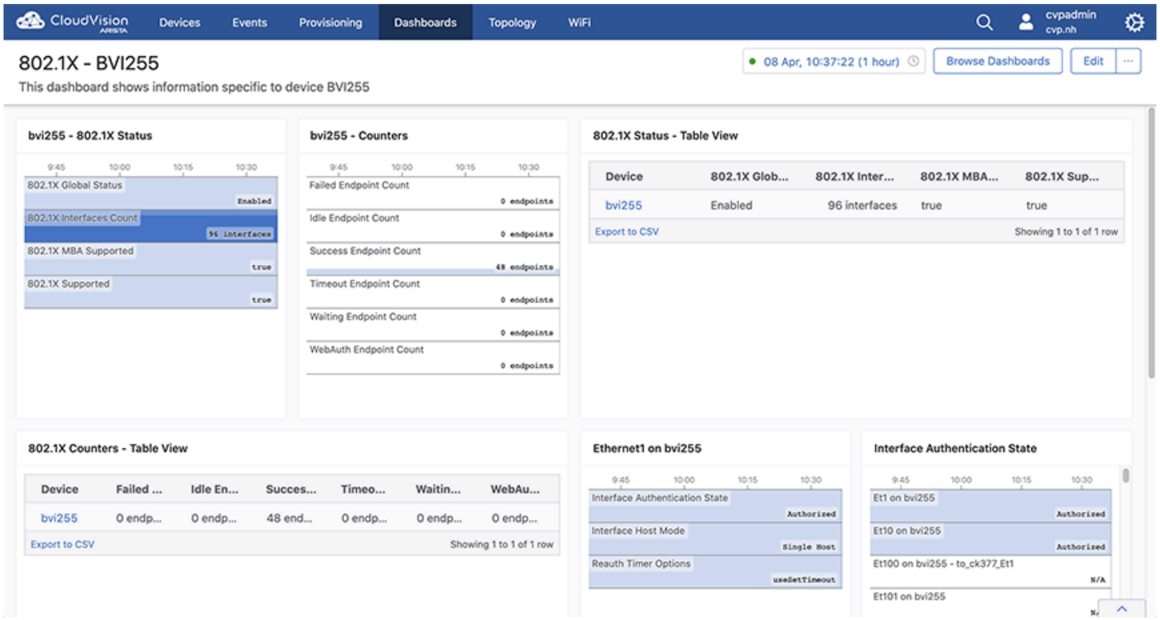
The table lists all of the endpoints with additional information. The columns show the following:

- **Identity**: the MAC address of the endpoint. The username, if provided, is displayed in parenthesis.
- **IP Address**: the IP address of the endpoint.
- **Interface**: which interface the endpoint is on. Selecting the interface will display a table showing all of the endpoints on that specific interface.
- **Host Mode**: the host mode of the endpoint (Single-Host, Multi-Host, Multi-Host Authenticated) with an optional Mac-Based VLAN Assignment. Place the cursor over Mac-Based VLAN Assignment to display the full name.
- **Auth Status**: the authentication status of the endpoint.
- **Auth Mode**: how the endpoint is authenticated.
- **VLAN**: the VLAN the endpoint is on.
- **VLAN Type**: the type of VLAN being used.

802.1X Dashboard View

802.1X metrics is also available from the Dashboard View. Refer to Dashboards for more information about creating a dashboard.

Figure 7-16: 802.1X Dashboard View



802.1X - BVI255

This dashboard shows information specific to device BVI255

802.1X Status - Table View

Device	802.1X Glob...	802.1X Inter...	802.1X MBA...	802.1X Sup...
bvi255	Enabled	96 interfaces	true	true

Export to CSV Showing 1 to 1 of 1 row

802.1X Counters - Table View

Device	Failed ...	Idle En...	Succes...	Timeo...	Waitin...	WebAu...
bvi255	0 endp...	0 endp...	48 end...	0 endp...	0 endp...	0 endp...

Export to CSV Showing 1 to 1 of 1 row

7.9.8 Viewing Traffic Flows

CloudVision lets you analyze the network traffic routed through a single device or through all devices that have flow tracking configured.

Note: Traffic flows return tunneled flows when the inner packet headers matches the user's query.

You can drill down into the details of global and device specific network flow activities using bar charts, stacked time series graphs, and tables of usage statistics. See Accessing the Global Traffic Flows Screen and Accessing the Device Specific Traffic Flows Screen.

Note: You can drill down the details of device specific network flow activities using heatmaps also.

To view the data on traffic flows, you must enable traffic flow tracking in devices to get data. See Enabling Traffic Flow Tracking.

7.9.8.1 Enabling Traffic Flow Tracking

Enabling flow tracking on a device allows CloudVision to provide a detailed breakdown of the forwarded network traffic. Traffic flow tracking is enabled through either of the following methods:

- Enable sFlow Sampling on a Device
- Enable Hardware Based IPFIX Flow Tracking

Enable sFlow Sampling on a Device

Arista switches provide a single sFlow agent instance that samples ingress traffic from all Ethernet and port channel interfaces.

Run the following commands to enable sFlow sampling on a device:

```
switch(config)#sflow sample <sampling rate>
switch(config)#sflow polling-interval <polling interval>
switch(config)#sflow destination 127.0.0.1
switch(config)#sflow source-interface <source interface>
switch(config)#sflow run
```

sFlow monitors a random sample of packets at the configured sampling rate. Reported bandwidth and packet measurements are scaled up using the sampling rate to provide estimates of actual bandwidth usage and packet counts.

Enable Hardware Based IPFIX Flow Tracking

Arista switches also allow exporting flow information using the IPFIX format.

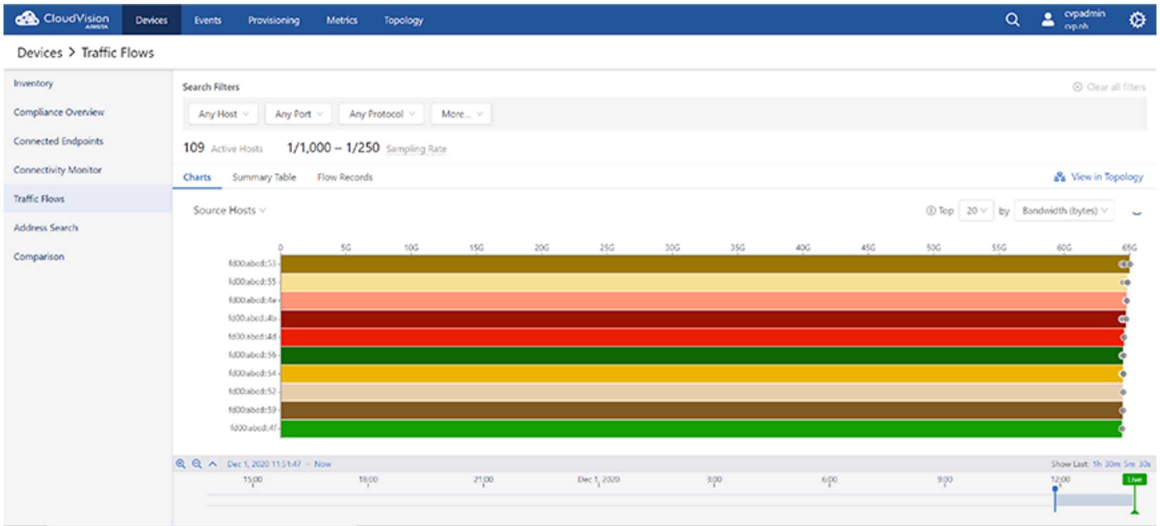
Run the following commands to enable hardware based IPFIX flow tracking:

```
switch(config)#flow tracking hardware
switch(config)#!
switch(config)#tracker <tracker name>
switch(config)#record export on inactive timeout <inactive timeout>
switch(config)#record export on interval <interval>
switch(config)#record format ipfix standard timestamps counters
switch(config)#!
switch(config)#exporter <exporter name>
switch(config)#collector <loopback interface ip>
switch(config)#local interface <loopback interface>
switch(config)#template interval <interval>
switch(config)#no shutdown
switch(config)#exit
switch(config)#interface <interface>
switch(config)#flow tracker hardware <tracker name>
switch(config)#no shutdown
```

7.9.8.2 Accessing the Global Traffic Flows Screen

To view the global traffic flows screen, navigate to **Devices** > **Traffic Flows** on the CloudVision portal. This screen displays information about traffic flows captured by all devices on the network with flow monitoring enabled. See the figure below.

Figure 7-17: Global Traffic Flows Screen



Note: This screen may present multiple values reported by different devices for the same flow or flow category.

Use the following search filters for customised presentation of the traffic flows data:

- Host filters
  - **Source Hosts**
    - **Show** autocomplete field - Provide hostnames, IP addresses, or subnets in CIDR notation of the source host that needs to be displayed
    - **Hide** autocomplete field - Provide hostnames, IP addresses, or subnets in CIDR notation of the source host that needs to be concealed
  - **Destination Hosts**
    - **Show** autocomplete field - Provide hostnames, IP addresses, or subnets in CIDR notation of the destination host that needs to be displayed
    - **Hide** autocomplete field - Provide hostnames, IP addresses, or subnets in CIDR notation of the destination host that needs to be concealed
  - **Bidirectional** checkbox - Select the checkbox to view the traffic flows between specified hosts.

    Note: When you select the **Bidirectional** checkbox, the **Source Hosts** and **Destination Hosts** fields change to **Hosts** and **To/From Hosts**.
- Port filters
  - **Source Ports** autocomplete field - Provide port numbers or service names of the source port
  - **Destination Ports** autocomplete field - Provide port numbers or service names of the destination port
  - **Show/Hide** dropdown - Select either **Show** or **Hide** to view or conceal the traffic flow data of specified source and destination ports respectively.
  - **Bidirectional** checkbox - Select the checkbox to view the traffic flows between specified ports.

    Note: When you select the **Bidirectional** checkbox, the **Source Ports** and **Destination Ports** fields change to **Ports** and **To/From Ports**.
- Protocol filter - Provide IP protocols of the required traffic flow data in the autocomplete field.

  Select either **Show** or **Hide** to view or conceal the traffic flow data of specified protocols respectively.
- More filters
  - **Locality** - Select **Public** and **Private** checkboxes to view traffic flows of corresponding networks
  - **Fragmentation** checkbox - Selecting the checkbox displays only flows with fragmented packets
- **Clear all filters** - Clears all specified filters
- **Top** dropdown menu - As per your selection, the top n items are displayed for each break down.
- **by** dropdown menu - Select the required method to measure traffic.

The global traffic flows dashboard provides the following display types for analyzing the flow data in different ways:

- Charts View
- Summary Table View
- Flow Records View

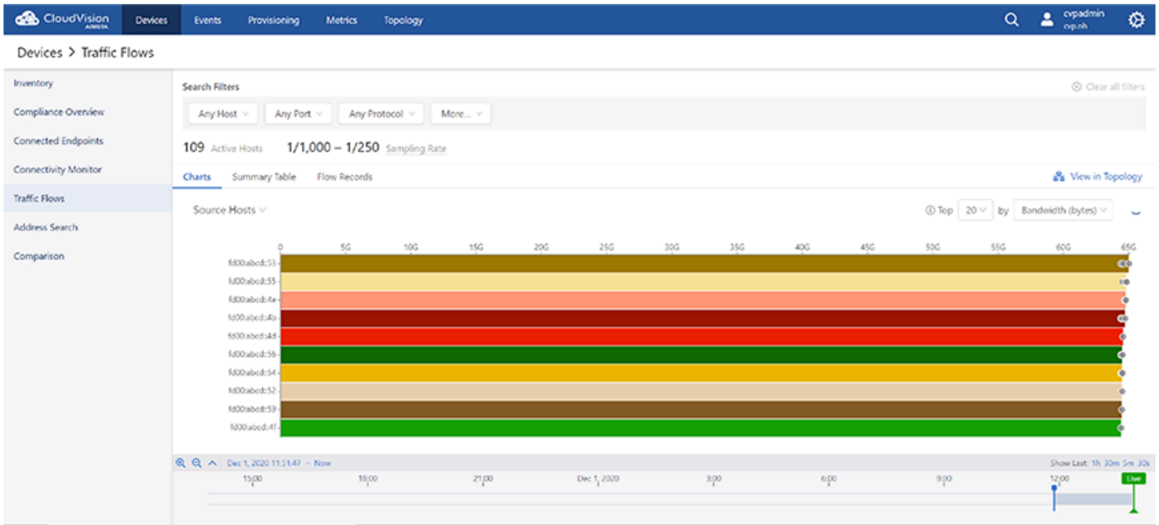
Note:

- Click the **View in Topology** link to see the data from the perspective of the topology flows view.
- The refresh icon provides countdown in seconds for refreshing the traffic flow data. The data in live mode gets updated every 30 seconds.

Charts View

The **Charts** display option presents the summary of global traffic flows in charts. The traffic flow data is arranged based on the breakdown selected from the dropdown list. See the figure below.

Figure 7-18: Global Traffic Flow Summary in Charts



Bar charts represent the device specific traffic flows over the selected time period. The bar length represents the traffic flow of a device with highest usage.

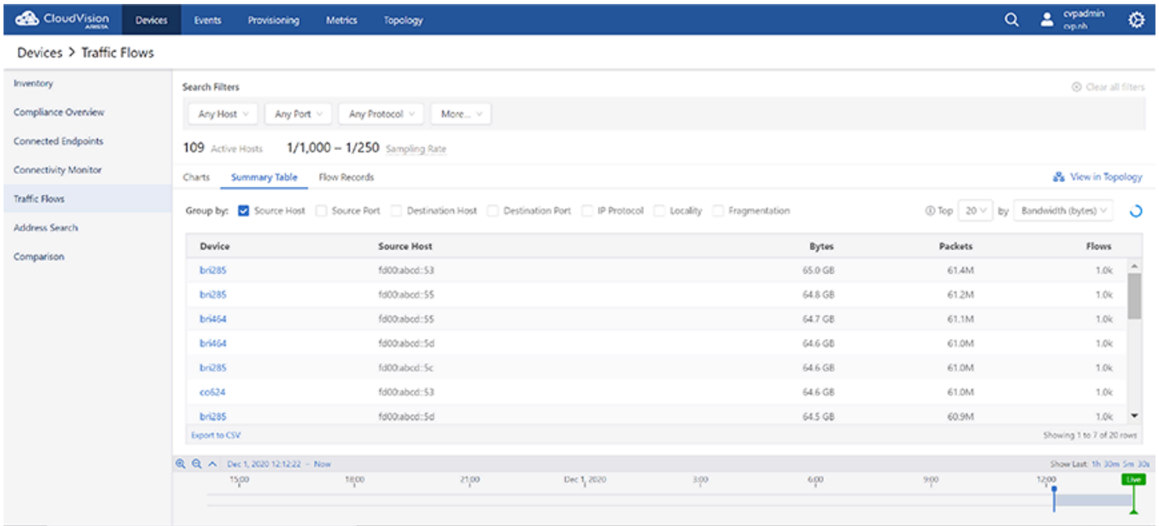
Note:

- Click on a bar in the bar chart in the stacked graph to set the clicked-on item as a filter wherever it is possible. For example, hosts or ports of source and destination.
- Hover the cursor on the dot in a bar to find the observing device.

Summary Table View

The **Summary Table** display option presents the summary of global traffic flows in a tabular format. See the figure below.

Figure 7-19: Global Traffic Flow Summary in Table



109 Active Hosts 1/1,000 – 1/250 Sampling Rate

Group by: ☑ Source Host □ Source Port □ Destination Host □ Destination Port □ IP Protocol □ Locality □ Fragmentation

Top 20 by Bandwidth (bytes)

Device	Source Host	Bytes	Packets	Flows
bri285	fd00:abcd::53	65.0 GB	61.4M	1.0k
bri285	fd00:abcd::55	64.8 GB	61.2M	1.0k
bri464	fd00:abcd::55	64.7 GB	61.1M	1.0k
bri464	fd00:abcd::5d	64.6 GB	61.0M	1.0k
bri285	fd00:abcd::5c	64.6 GB	61.0M	1.0k
co624	fd00:abcd::53	64.6 GB	61.0M	1.0k
bri285	fd00:abcd::5d	64.5 GB	60.9M	1.0k

Showing 1 to 7 of 20 rows

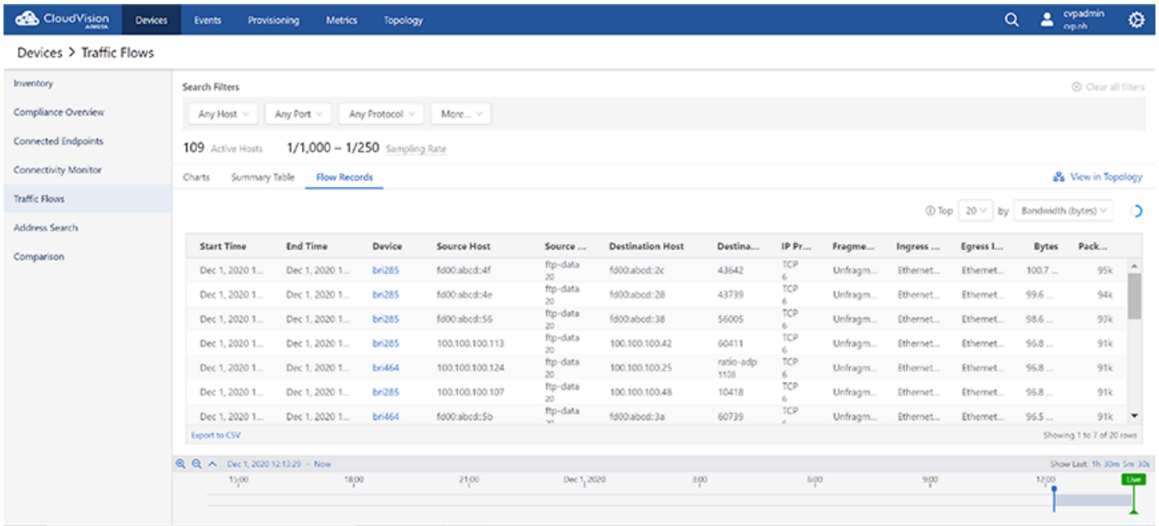
The traffic flow data is grouped based on the selected breakdowns. If multiple options are selected in the **Group By** field, the table displays a summary of usage statistics that is broken down according to the selected criteria. The summary can be sorted by bytes, packets, or flows in descending order.

Note: Click on a device name to view the traffic flows for the respective device.

Flow Records View

The **Flow Records** display option presents the record of all traffic flows in a tabular format. See the figure below.

Figure 7-20: Global Traffic Flow Record



109 Active Hosts 1/1,000 – 1/250 Sampling Rate

Top 20 by Bandwidth (bytes)

Start Time	End Time	Device	Source Host	Source ...	Destination Host	Destina...	IP Pr...	Fragme...	Ingress ...	Egress I...	Bytes	Pack...
Dec 1, 2020 1...	Dec 1, 2020 1...	bri285	fd00:abcd::4f	ftp-data 20	fd00:abcd::2c	43642	TCP 6	Unfragm...	Ethernet...	Ethernet...	100.7 ...	95k
Dec 1, 2020 1...	Dec 1, 2020 1...	bri285	fd00:abcd::4e	ftp-data 20	fd00:abcd::28	43739	TCP 6	Unfragm...	Ethernet...	Ethernet...	99.6 ...	94k
Dec 1, 2020 1...	Dec 1, 2020 1...	bri285	fd00:abcd::56	ftp-data 20	fd00:abcd::38	56005	TCP 6	Unfragm...	Ethernet...	Ethernet...	98.6 ...	93k
Dec 1, 2020 1...	Dec 1, 2020 1...	bri285	100.100.100.113	ftp-data 20	100.100.100.42	60411	TCP 6	Unfragm...	Ethernet...	Ethernet...	96.8 ...	91k
Dec 1, 2020 1...	Dec 1, 2020 1...	bri464	100.100.100.124	ftp-data 20	100.100.100.25	ratio-adp 1108	TCP 6	Unfragm...	Ethernet...	Ethernet...	96.8 ...	91k
Dec 1, 2020 1...	Dec 1, 2020 1...	bri285	100.100.100.107	ftp-data 20	100.100.100.48	10418	TCP 6	Unfragm...	Ethernet...	Ethernet...	96.8 ...	91k
Dec 1, 2020 1...	Dec 1, 2020 1...	bri464	fd00:abcd::5b	ftp-data 20	fd00:abcd::3a	60739	TCP 6	Unfragm...	Ethernet...	Ethernet...	96.5 ...	91k

Showing 1 to 7 of 20 rows

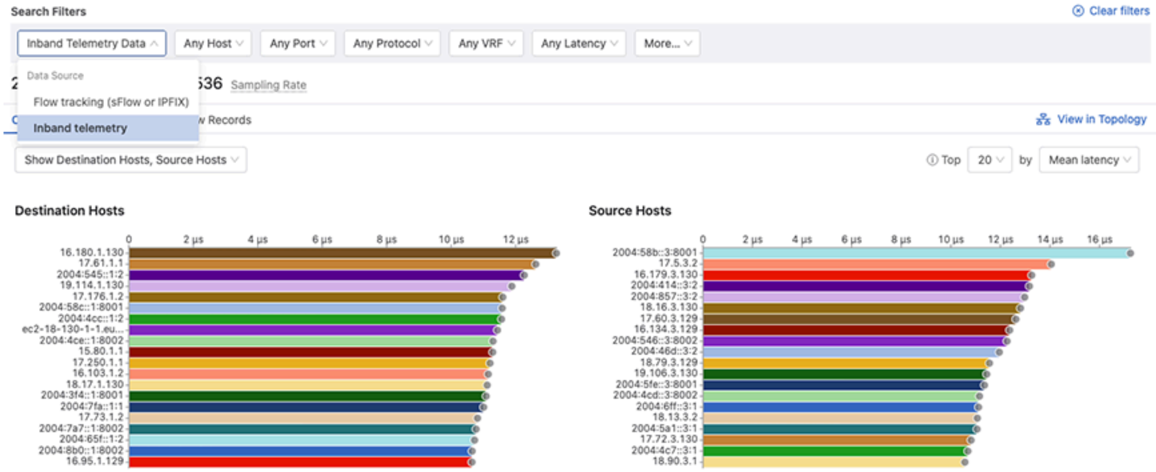
Dec 1, 2020 12:13:29 – Now

Note: Click on a device name to view the traffic flows for the respective device.

7.9.8.3 Accessing the Device Specific Traffic Flows Screen

On the CloudVision portal, navigate to **Devices** > **Inventory** > *Device_Name* > **Traffic Flows** to view the Traffic Flows screen. See the figure below.

Figure 7-21: Inband Telemetry



This screen displays the summary of flows, bandwidth, packets, active hosts, and sampling rate. Provide the following details to view custom information of traffic flows:

- Inband Telemetry Data
  - **Flow tracking (sFlow or IPFIX)**
  - **Inband telemetry**
- Host filters
  - **Source Hosts**
    - **Show** autocomplete field - Provide hostnames, IP addresses, or subnets in CIDR notation of the source host that needs to be displayed
    - **Hide** autocomplete field - Provide hostnames, IP addresses, or subnets in CIDR notation of the source host that needs to be concealed
  - **Destination Hosts**
    - **Show** autocomplete field - Provide hostnames, IP addresses, or subnets in CIDR notation of the destination host that needs to be displayed
    - **Hide** autocomplete field - Provide hostnames, IP addresses, or subnets in CIDR notation of the destination host that needs to be concealed
- Port filters
  - **Source Ports** autocomplete field - Provide port numbers or service names of the source port
  - **Destination Ports** autocomplete field - Provide port numbers or service names of the destination port
  - **Show/Hide** dropdown - Select either **Show** or **Hide** to view or conceal the traffic flow data of specified source and destination ports respectively.
- Protocol filter - Provide IP protocols of the required traffic flow data in the autocomplete field.

  Select either **Show** or **Hide** to view or conceal the traffic flow data of specified protocols respectively
- Interface filters
  - **Show** autocomplete field - Select the interfaces of which the traffic flow needs to be displayed
  - **Hide** autocomplete field - Select the interfaces of which the traffic flow needs to be concealed
- More filters
  - **Locality** - Select **Public** and **Private** checkboxes to view traffic flows of corresponding networks
  - **Fragmentation** checkbox - Selecting the checkbox displays only flows with fragmented packets
- **Clear all filters** - Clears all specified filters
- **Top** dropdown menu - As per your selection, the top n items are displayed for each break down.
- **by** dropdown menu - Select the required method to measure traffic.

The device specific traffic flows dashboard provides the following display types for analyzing the flow data in different ways:

- Figure 87: Device Specific Traffic Flow Summary in Charts
- Heatmap View
- Summary Table View
- Flow Records View

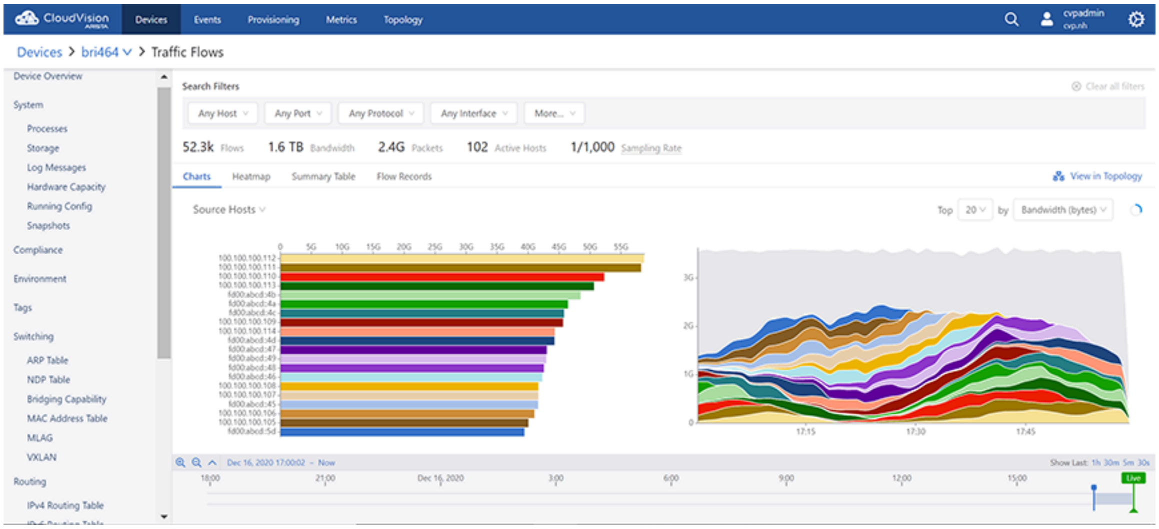
Note:

- Click the **View in Topology** link to see the data from the perspective of the topology flows view.
- The refresh icon provides countdown in seconds for refreshing the traffic flow data. The data in live mode gets updated every 30 seconds.

Charts View

The **Charts** display option presents the summary of device specific traffic flows in charts. The traffic flow data is arranged based on the breakdown selected from the dropdown list. See the figure below.

Figure 7-22: Device Specific Traffic Flow Summary in Charts



The following information is provided for each break down:

- Bar charts that display the total usage over the time period for items

  Note: Clicking on a bar in the bar chart or a time series in the stacked graph sets the clicked-on item as a filter wherever it is possible. For example, hosts or ports of source and destination.

- Stacked time series graphs that provide the following information:
  - The rate of usage vs. time

    Note: This information is provided only when the Sort By option is either Bandwidth (bytes) or Packets.

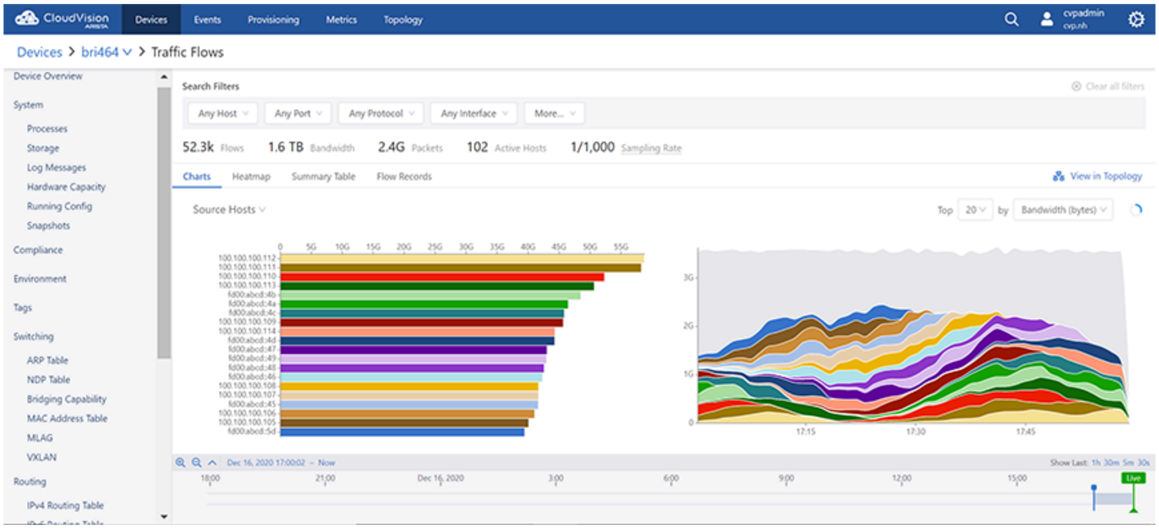
  - The number of flows active vs. time

    Note: This information is provided only when the Sort By option is Flow Count.

Charts View

The **Charts** display option presents the summary of device specific traffic flows in charts. The traffic flow data is arranged based on the breakdown selected from the dropdown list. See the figure below.

Figure 7-23: Device Specific Traffic Flow Summary in Charts



52.3k Flows 1.6 TB Bandwidth 2.4G Packets 102 Active Hosts 1/1,000 Sampling Rate

Top 20 by Bandwidth (bytes)

The following information is provided for each break down:

- Bar charts that display the total usage over the time period for items

  Note: Clicking on a bar in the bar chart or a time series in the stacked graph sets the clicked-on item as a filter wherever it is possible. For example, hosts or ports of source and destination.
- Stacked time series graphs that provide the following information:
  - The rate of usage vs. time

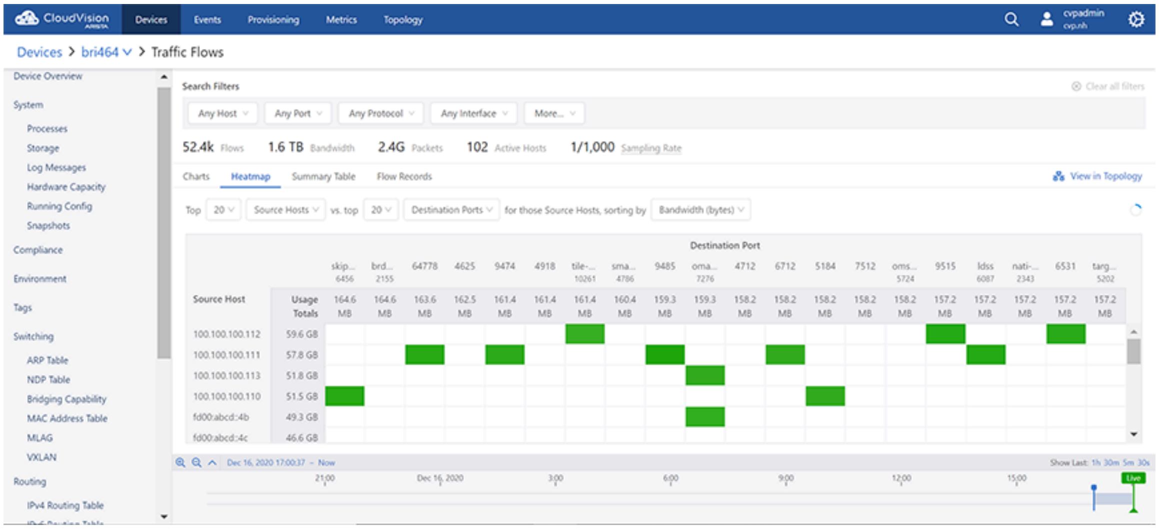
    Note: This information is provided only when the Sort By option is either Bandwidth (bytes) or Packets.
  - The number of flows active vs. time

    Note: This information is provided only when the Sort By option is Flow Count.

Heatmap View

The **Heatmap** display option presents the summary of device specific traffic flows in a heatmap. See the figure below.

Figure 7-24: Device Specific Traffic Flow Summary in Heatmap



52.4k Flows 1.6 TB Bandwidth 2.4G Packets 102 Active Hosts 1/1,000 Sampling Rate

Top 20 Source Hosts vs. top 20 Destination Ports for those Source Hosts, sorting by Bandwidth (bytes)

Destination Port

Source Host	Usage Totals	skip... 6456	brd... 2155	64778	4625	9474	4918	tile-... 10261	sma... 4786	9485	oma... 7276	4712	6712	5184	7512	oms... 5724	9515	ldss 6087	nati-... 2343	6531	targ... 5202
		164.6 MB	164.6 MB	163.6 MB	162.5 MB	161.4 MB	161.4 MB	161.4 MB	160.4 MB	159.3 MB	159.3 MB	158.2 MB	158.2 MB	158.2 MB	158.2 MB	158.2 MB	157.2 MB	157.2 MB	157.2 MB	157.2 MB	157.2 MB
100.100.100.112	59.6 GB							🟩									🟩			🟩	
100.100.100.111	57.8 GB			🟩		🟩				🟩			🟩					🟩			
100.100.100.113	51.8 GB										🟩										
100.100.100.110	51.5 GB	🟩												🟩							
fd00:abcd::4b	49.3 GB										🟩										
fd00:abcd::4c	46.6 GB																				

The heatmap plots two breakdowns against each other. For example, the user selects top 20 source hosts vs. top 20 destination hosts. The system displays the top 20 destination hosts that communicated with any of those top 20 source hosts.

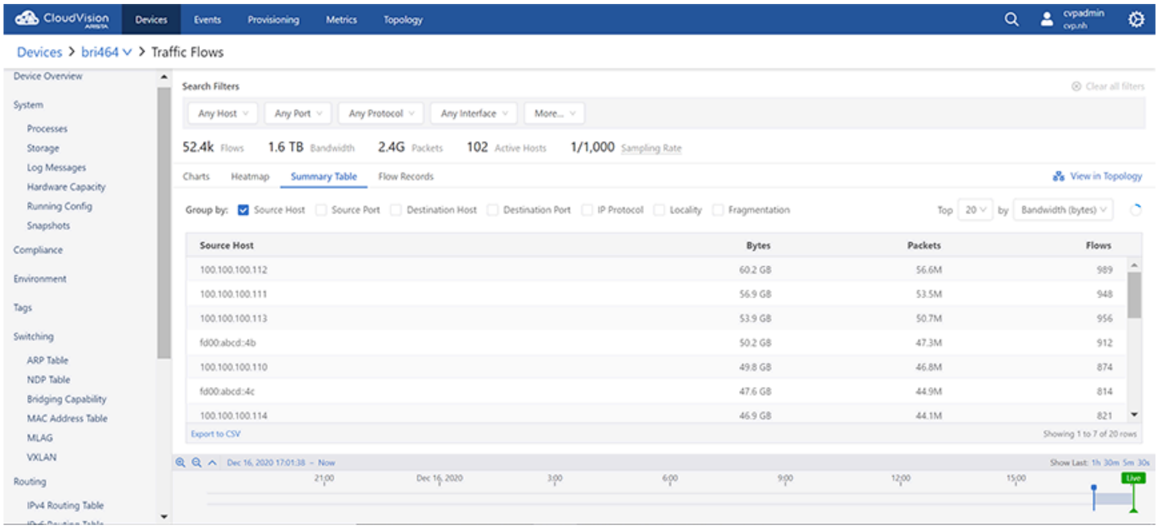
Each pairing of source host and destination host is shown as a cell in the grid. Cells are displayed in various shades of green based on their usage. The higher the usage, the darker the green shade.

Note: The system displays an empty cell if there is no usage.

Summary Table View

The **Summary Table** display option presents the summary of device specific traffic flows in a table. See the figure below.

Figure 7-25: Device Specific Traffic Flow Summary in Table



52.4k Flows 1.6 TB Bandwidth 2.4G Packets 102 Active Hosts 1/1,000 Sampling Rate

Group by: ☑ Source Host □ Source Port □ Destination Host □ Destination Port □ IP Protocol □ Locality □ Fragmentation Top 20 by Bandwidth (bytes)

Source Host	Bytes	Packets	Flows
100.100.100.112	60.2 GB	56.6M	989
100.100.100.111	56.9 GB	53.5M	948
100.100.100.113	53.9 GB	50.7M	956
fd00:abcd::4b	50.2 GB	47.3M	912
100.100.100.110	49.8 GB	46.8M	874
fd00:abcd::4c	47.6 GB	44.9M	814
100.100.100.114	46.9 GB	44.1M	821

Showing 1 to 7 of 20 rows

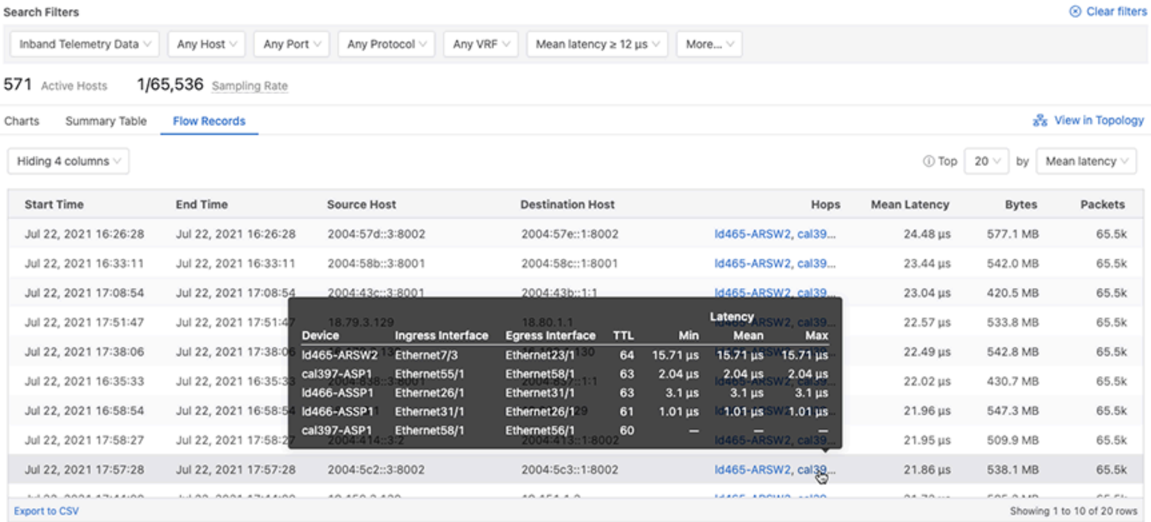
The traffic flow data is grouped based on the selected breakdowns. If multiple options are selected in the **Group By** field, the table displays a summary of usage statistics that is broken down according to the selected criteria. The summary can be sorted by bytes, packets, or flows in descending order.

Flow Records View

The **Flow Records** display option presents the record of device specific traffic flows in a tabular format. See the figure below.

When viewing individual flow records, the path of a flow, complete with ingress and egress interfaces, TTLs and latencies for each hop, can be inspected using the **Hops** column.

Figure 7-26: Flow Records View



Search Filters

Inband Telemetry Data | Any Host | Any Port | Any Protocol | Any VRF | Mean latency ≥ 12 µs | More...

Clear filters

571 Active Hosts 1/65,536 Sampling Rate

Charts | Summary Table | Flow Records

View in Topology

Hiding 4 columns

Top 20 by Mean latency

Start Time	End Time	Source Host	Destination Host	Hops	Mean Latency	Bytes	Packets
Jul 22, 2021 16:26:28	Jul 22, 2021 16:26:28	2004:57d::3:8002	2004:57e::1:8002	ld465-ARSW2, cal39...	24.48 µs	577.1 MB	65.5k
Jul 22, 2021 16:33:11	Jul 22, 2021 16:33:11	2004:58b::3:8001	2004:58c::1:8001	ld465-ARSW2, cal39...	23.44 µs	542.0 MB	65.5k
Jul 22, 2021 17:08:54	Jul 22, 2021 17:08:54	2004:43c::3:8001	2004:43b::1:1	ld465-ARSW2, cal39...	23.04 µs	420.5 MB	65.5k
Jul 22, 2021 17:51:47	Jul 22, 2021 17:51:47	18.79.3.129	18.80.1.1	...ARSW2, cal39...	22.57 µs	533.8 MB	65.5k
Jul 22, 2021 17:38:06	Jul 22, 2021 17:38:06	...13	...130	...ARSW2, cal39...	22.49 µs	542.8 MB	65.5k
Jul 22, 2021 16:35:33	Jul 22, 2021 16:35:33	2004:838::3:8001	2004:837::1:1	ld465-ARSW2, cal39...	22.02 µs	430.7 MB	65.5k
Jul 22, 2021 16:58:54	Jul 22, 2021 16:58:54	[illegible]	...29	ld...SW2...	21.96 µs	547.3 MB	65.5k
Jul 22, 2021 17:58:27	Jul 22, 2021 17:58:27	2004:414::3:2	2004:413::1:8002	ld465-ARSW2, cal39...	21.95 µs	509.9 MB	65.5k
Jul 22, 2021 17:57:28	Jul 22, 2021 17:57:28	2004:5c2::3:8002	2004:5c3::1:8002	ld465-ARSW2, cal39...	21.86 µs	538.1 MB	65.5k

				Latency		
Device	Ingress Interface	Egress Interface	TTL	Min	Mean	Max
ld465-ARSW2	Ethernet7/3	Ethernet23/1	64	15.71 µs	15.71 µs	15.71 µs
cal397-ASP1	Ethernet55/1	Ethernet58/1	63	2.04 µs	2.04 µs	2.04 µs
ld466-ASSP1	Ethernet26/1	Ethernet31/1	63	3.1 µs	3.1 µs	3.1 µs
ld466-ASSP1	Ethernet31/1	Ethernet26/1	61	1.01 µs	1.01 µs	1.01 µs
cal397-ASP1	Ethernet58/1	Ethernet56/1	60	—	—	—

Export to CSV

Showing 1 to 10 of 20 rows

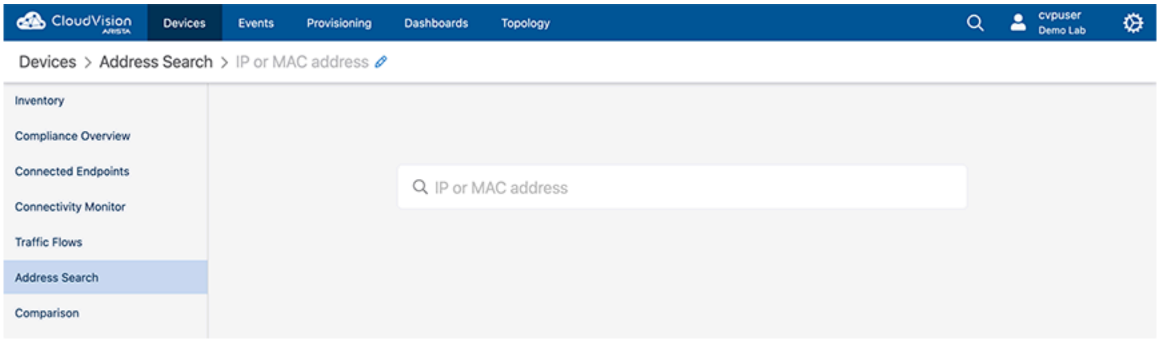
Note: Filters and fields related to packet fragmentation, tunnelling, and user identity are not available for inband telemetry data.

7.9.9 Address Search

Address Search supports searching MAC addresses, IP addresses of all formats, device IDs, and hostnames of inventory devices.

The Address Search page can be found in the primary Devices view on the sidebar. Navigating to it will open the Address Search page.

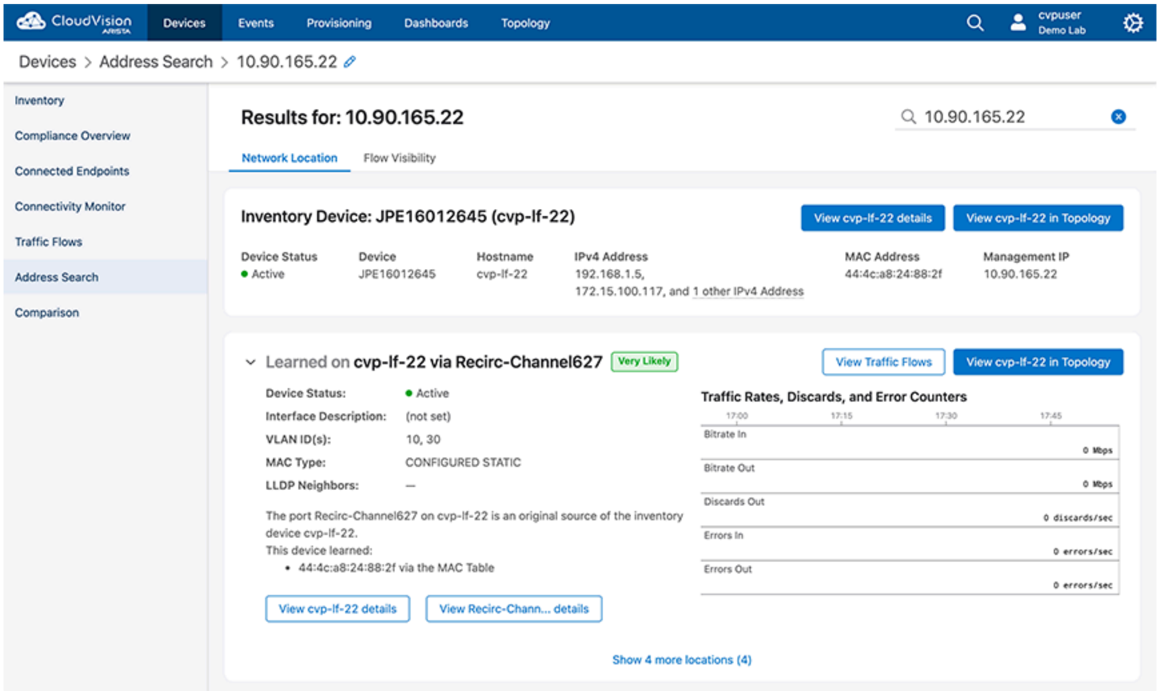
Figure 7-27: Address Search Page



Devices > Address Search > IP or MAC address

Enter the search information and press **Enter** to view the search results.

Figure 7-28: Address Search Results



Results for: 10.90.165.22

Inventory Device: JPE16012645 (cvp-lf-22)

Device Status	Device	Hostname	IPv4 Address	MAC Address	Management IP
● Active	JPE16012645	cvp-lf-22	192.168.1.5, 172.15.100.117, and 1 other IPv4 Address	44:4c:a8:24:88:2f	10.90.165.22

Learned on cvp-lf-22 via Recirc-Channel627

Device Status:	● Active
Interface Description:	(not set)
VLAN ID(s):	10, 30
MAC Type:	CONFIGURED STATIC
LLDP Neighbors:	—

The port Recirc-Channel627 on cvp-lf-22 is an original source of the inventory device cvp-lf-22.
This device learned:

- 44:4c:a8:24:88:2f via the MAC Table

Traffic Rates, Discards, and Error Counters

Bitrate In	0 Mbps
Bitrate Out	0 Mbps
Discards Out	0 discards/sec
Errors In	0 errors/sec
Errors Out	0 errors/sec

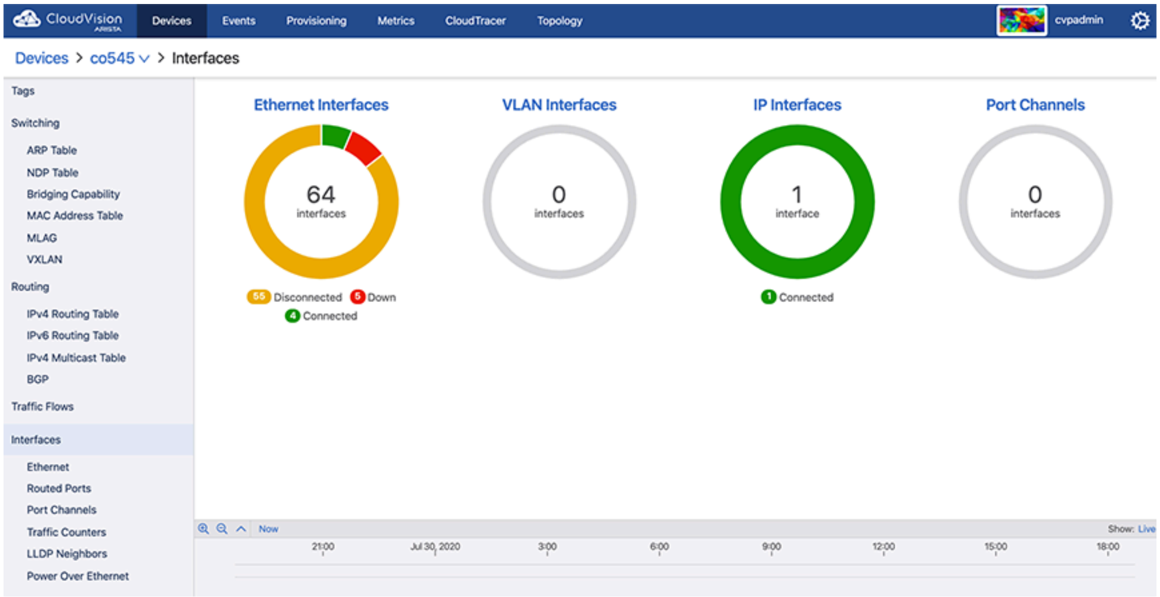
There are two tabs available in the search results view.

- Network Location is the default view. This view displays detailed information from the MAC, ARP, and LLDP Tables.
- Flow Visibility view displays the traffic that is being sent and received by all IP addresses associated with the search result.

7.9.10 Status of Interfaces

The Interfaces section provides status of Ethernet interfaces, VLAN interfaces, IP interfaces, and port channels.

Figure 7-29: Interfaces Section



Sub-sections provide detailed information on Ethernet interfaces, routed ports, port channels, traffic counters, LLDP neighbors, and Power Over Ethernet.

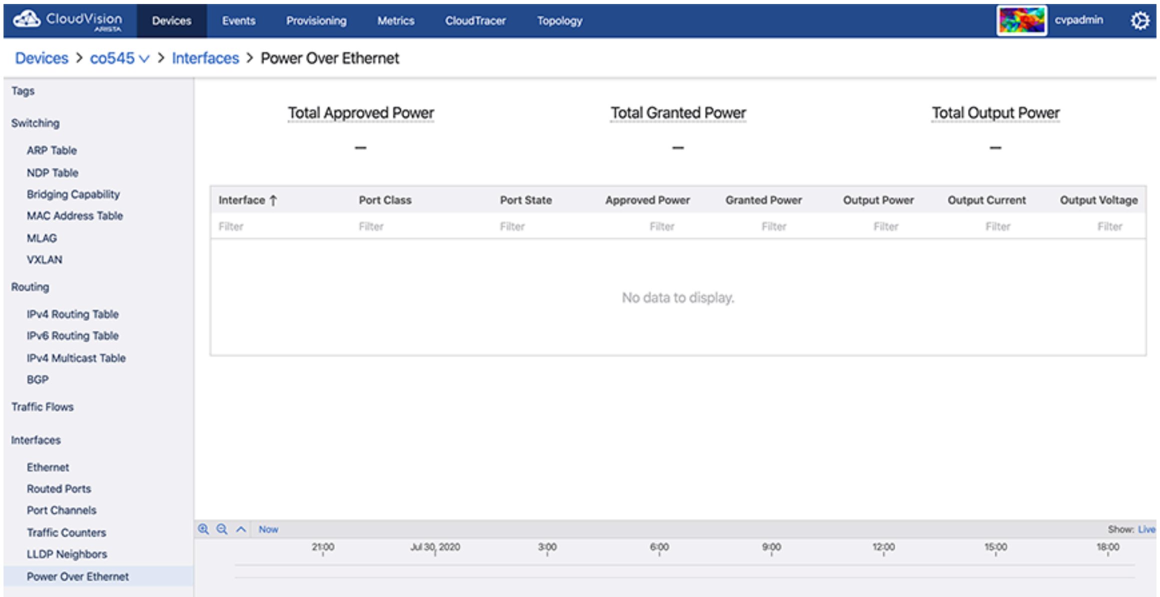
7.9.10.1 Power Over Ethernet

Power Over Ethernet (PoE) is a technology for delivering electrical power along with network data over physical Ethernet connections. Some benefits of PoE are provided below:

- Reduces the need of extension cables and additional outlets
- Provides a reliable power source on difficult terrain
- Prevents data transmission hiccups
- Substantial reductions in space usage, cost, and time

In CloudVision, the Power Over Ethernet screen provides a summary of all interfaces along with information on each interface.

Figure 7-30: Power Over Ethernet Screen



Interface ↑	Port Class	Port State	Approved Power	Granted Power	Output Power	Output Current	Output Voltage
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter

No data to display.

The Power Over Ethernet screen displays the following information:

- Summary of All Interfaces
  - Total Approved Power - Sum of the approved maximum power amounts configured for each Ethernet port
  - Total Granted Power - Sum of the approved power amounts minus power loss to transmission over Ethernet cables
  - Total Output Power - Sum of actual power amounts delivered to each powered Ethernet device
- Information on Individual Interfaces
  - Interface - Interface name
  - Port Class - Maximum power in watts (W)
  - Port State - Operational status of a PoE device connected to the port
  - Approved Power - Configured maximum power output in watts (W) for the interface
  - Granted Power - Maximum power available to the device
  - Output Power - Power drawn by the device
  - Output Current - Current available on the PoE link in milliamps (mA)
  - Output Voltage - Voltage available over the PoE link in volts (V)

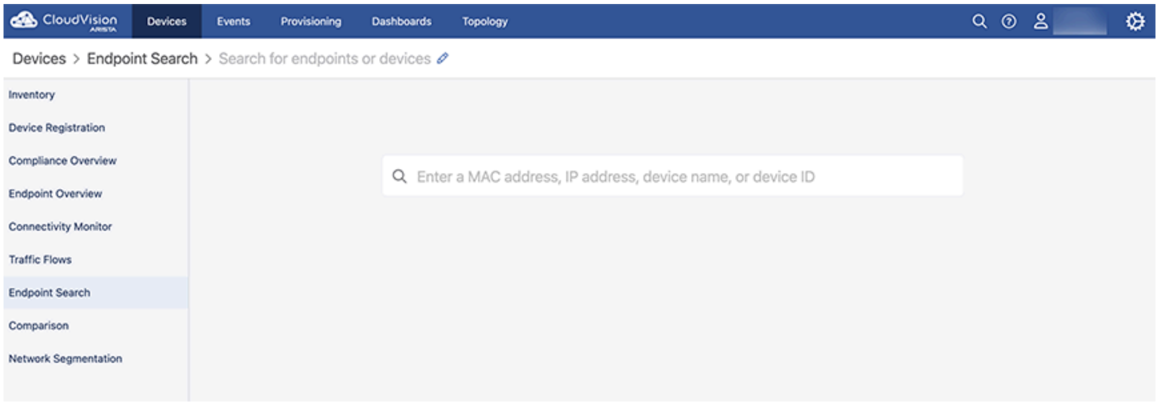
Note: PoE metrics are also available in the Metrics Explorer and can be built into custom metrics dashboards. Data on individual interfaces is available under the Interfaces metric type.

7.9.11 Viewing 802.1x Details for Endpoint Search

From the 2023.2.0 release onward, you can view additional functionality (Endpoint Authentication tab) when you search for the device details using the **Devices** > **Endpoint Search** page from the CloudVision portal.

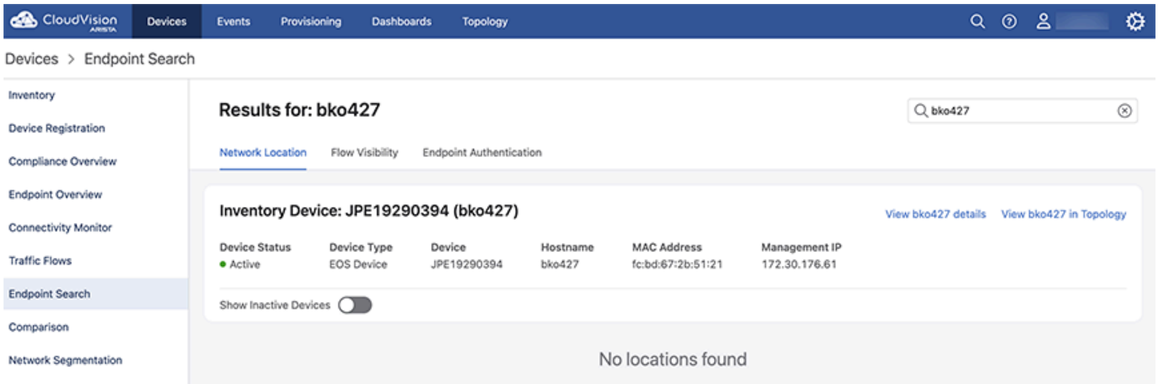
You can view the device details by entering the MAC address, IP address, device name, or device ID in the search window. For example:

Figure 7-31: Search Window



Based on the configuration, the device details are displayed, with three tabs: Network Location, Flow Visibility, and Endpoint Authentication. For details on **Network Location** and **Flow Visibility**, see the Address Search sections. From the 2023.2.0 release onward, the Endpoint Authentication tab is also visible as in the example here:

Figure 7-32: Endpoint Search Results



Results for: bko427

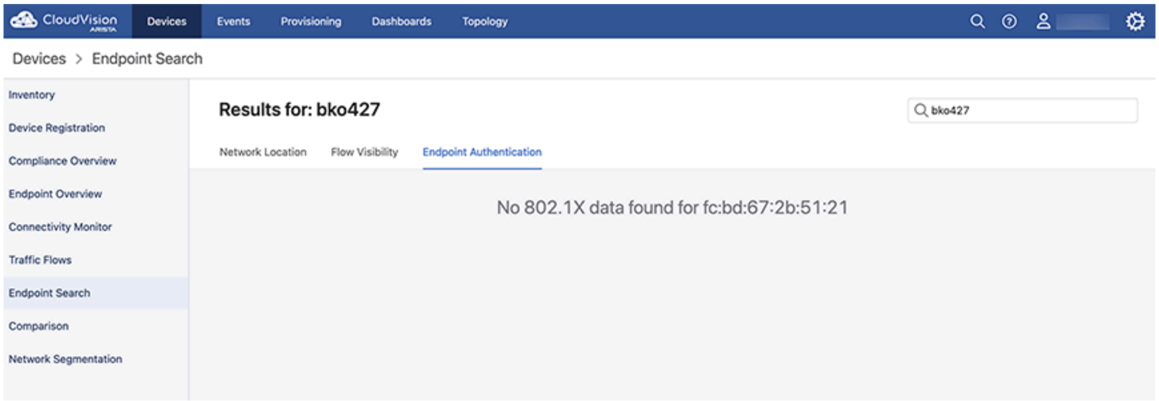
Inventory Device: JPE19290394 (bko427)

Device Status	Device Type	Device	Hostname	MAC Address	Management IP
● Active	EOS Device	JPE19290394	bko427	fc:bd:67:2b:51:21	172.30.176.61

No locations found

The Endpoint Authentication tab displays 802.1x information for the MAC addresses associated with the searched device or endpoint. If there is no 802.1x information for the searched MAC Addresses, a "No data found" page is displayed as here:

Figure 7-33: Endpoint Authentication Tab

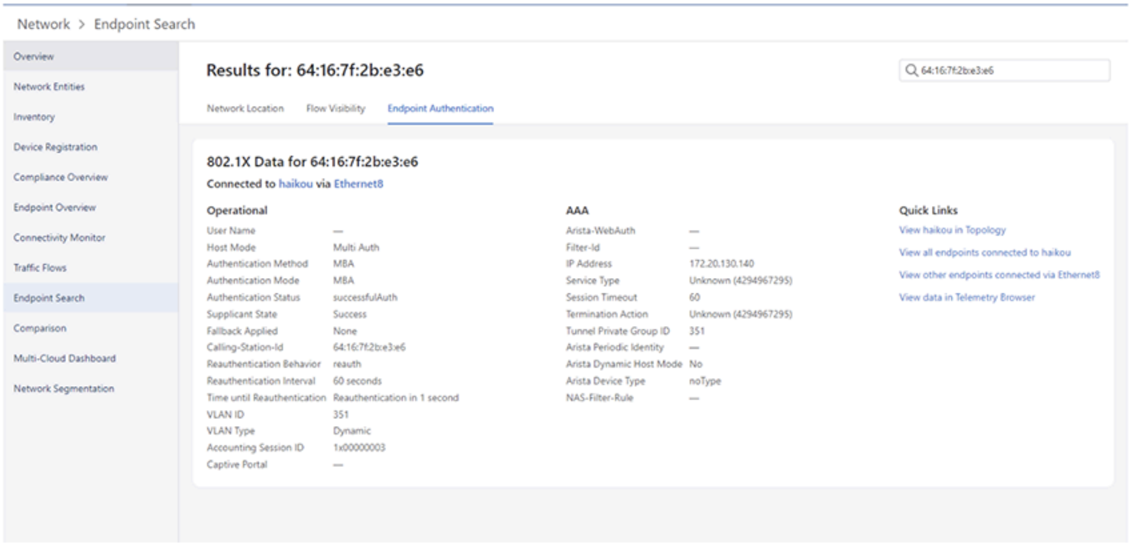


Results for: bko427

No 802.1X data found for fc:bd:67:2b:51:21

If there is 802.1x information associated with the searched MAC address, a card with Operational, AAA, and Quick Links are displayed for that MAC address as in the example here.

Figure 7-34: Endpoint_Authentication_Results



Results for: 64:16:7f:2b:e3:e6

802.1X Data for 64:16:7f:2b:e3:e6

Connected to haikou via Ethernet8

Operational

User Name	—
Host Mode	Multi Auth
Authentication Method	MBA
Authentication Mode	MBA
Authentication Status	successfulAuth
Supplicant State	Success
Fallback Applied	None
Calling-Station-Id	64:16:7f:2b:e3:e6
Reauthentication Behavior	reauth
Reauthentication Interval	60 seconds
Time until Reauthentication	Reauthentication in 1 second
VLAN ID	351
VLAN Type	Dynamic
Accounting Session ID	1x00000003
Captive Portal	—

AAA

Arista-WebAuth	—
Filter-Id	—
IP Address	172.20.130.140
Service Type	Unknown (4294967295)
Session Timeout	60
Termination Action	Unknown (4294967295)
Tunnel Private Group ID	351
Arista Periodic Identity	—
Arista Dynamic Host Mode	No
Arista Device Type	noType
NAS-Filter-Rule	—

Quick Links

View haikou in Topology

View all endpoints connected to haikou

View other endpoints connected via Ethernet8

View data in Telemetry Browser

The following 802.1x details are displayed for the searched device or endpoint:

- **Operational** tab
  - User Name
  - Authentication Method
  - Authentication Mode
  - Authentication Status
  - Supplicant State
  - Fallback Applied
  - Calling-Station-Id
  - Reauthentication Behavior
  - Reauthentication Interval
  - Time until Reauthentication
  - VLAN ID
  - VLAN Type
  - Accounting Session ID
  - Captive Portal
- **AAA** tab
  - Arista-WebAuth
  - Filter-Id
  - IP Address
  - NAS-Filter-Rule
  - Service Type
  - Session Timeout
  - Termination Action
  - Tunnel Private Group ID
  - Arista Periodic Identity
  - Arista Dynamic Host Mode
  - Arista Device Type
- **Quick Links** tab

- Link to the associated device in Topology
- Link to the Dot1x sections for the associated device
- Link to the Dot1x sections via Ethernet for the associated interface
- Link to the Telemetry Browser to view the additional fields that are not displayed in Endpoint Search

7.10 Viewing Connected Endpoints

Connected Endpoints are identified by DHCP collector. By default, the DHCP collector is enabled in TerminAttr. You must enable it on VLANs where you would like to identify connected endpoints. See Enabling DHCP Collector.

Once it is enabled, the Connected Endpoints summary screen provides information on all connected endpoints. See Accessing the Connected Endpoints Summary Screen.

Enabling DHCP Collector

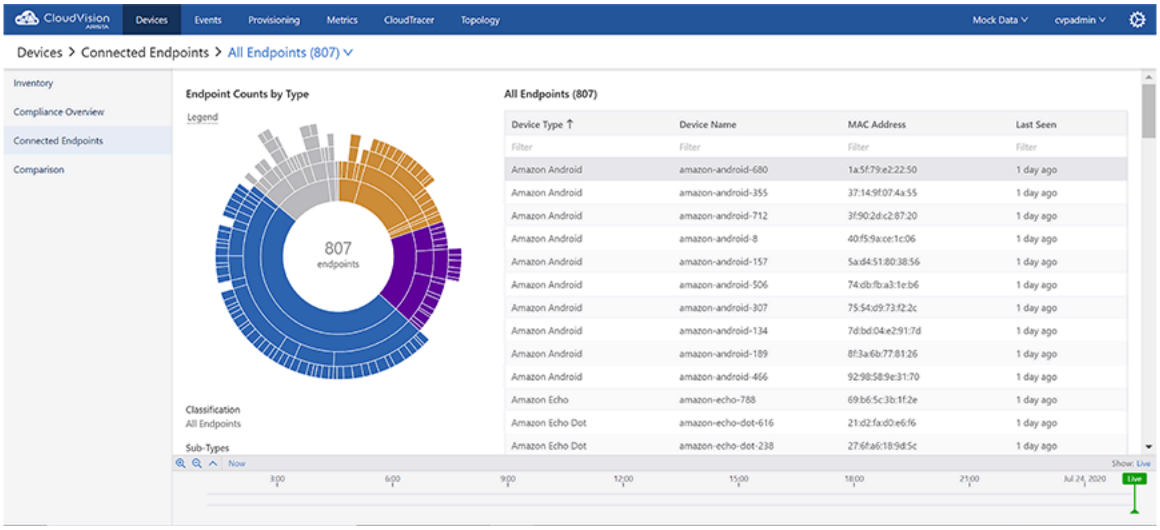
As of TerminAttr v.1.6.0, the ECO DHCP Collector is enabled by default and listens on 127.0.0.1:67 for UDP traffic. Add 127.0.0.1 as an IP helper address on VLANs to capture device identification.

```
switch(config)# interface vlan100
switch(config-if-Vl100)# ip helper-address dhcp_server_address
switch(config-if-Vl100)# ip helper-address 127.0.0.1
switch(config-if-Vl100)# exit
switch(config)# ip dhcp snooping
switch(config)# ip dhcp snooping information option
switch(config)# ip dhcp snooping vlan 100
```

Accessing the Connected Endpoints Summary Screen

On the CloudVision portal, navigate to **Devices** > **Connected Endpoints** to view the Connected Endpoints Summary screen.This screen provides the classified summary of all endpoints along with the detailed information of each endpoint. See the figure below.

Figure 7-35: Connected Endpoints Summary Screen



All Endpoints (807)

Device Type ↑	Device Name	MAC Address	Last Seen
Filter	Filter	Filter	Filter
Amazon Android	amazon-android-680	1a:5f:79:e2:22:50	1 day ago
Amazon Android	amazon-android-355	37:14:9f:07:4a:55	1 day ago
Amazon Android	amazon-android-712	3f:90:2d:c2:87:20	1 day ago
Amazon Android	amazon-android-8	40:f5:9a:ce:1c:06	1 day ago
Amazon Android	amazon-android-157	5a:d4:51:80:38:56	1 day ago
Amazon Android	amazon-android-506	74:db:fb:a3:1e:b6	1 day ago
Amazon Android	amazon-android-307	75:54:d9:73:f2:2c	1 day ago
Amazon Android	amazon-android-134	7d:bd:04:e2:91:7d	1 day ago
Amazon Android	amazon-android-189	8f:3a:6b:77:81:26	1 day ago
Amazon Android	amazon-android-466	92:98:58:9e:31:70	1 day ago
Amazon Echo	amazon-echo-788	69:b6:5c:3b:1f:2e	1 day ago
Amazon Echo Dot	amazon-echo-dot-616	21:d2:fa:d0:e6:f6	1 day ago
Amazon Echo Dot	amazon-echo-dot-238	27:6f:a6:18:9d:5c	1 day ago

Note: To reset to all endpoints, click the refresh icon (next to selected endpoint in breadcrumbs) that is displayed after selecting a particular endpoint.

This screen provides the following functionalities:

- Classification drop-down menu - Click and select the required classification.
- Endpoints Counts by Type pane - This pane provides a summary of the selected classification through the following groups:
  - Legend - Hover the cursor on Legend to view color classifications used for various categories.
  - Sunburst graph - Provides the summarized view of all endpoints in various categories, hierarchies, and counts.

    Note: Clicking on a category sets the appropriate category as the new active classification.
  - Classification - Displays selected classification in bread crumbs

    Note: Clicking a breadcrumb link sets the appropriate classification as the new active classification.
  - Sub-Types (Optional) - Displays the count of sub-types under classification

    Note: Clicking a sub-type link sets the appropriate sub-type as the new active classification
- All selected classification Endpoints pane - This pane provides the specified information of each endpoint in selected classification under the following categories:
  - Device Type
  - Device Name
  - MAC Address
  - Last Seen

7.11 Connectivity Monitor and CloudTracer

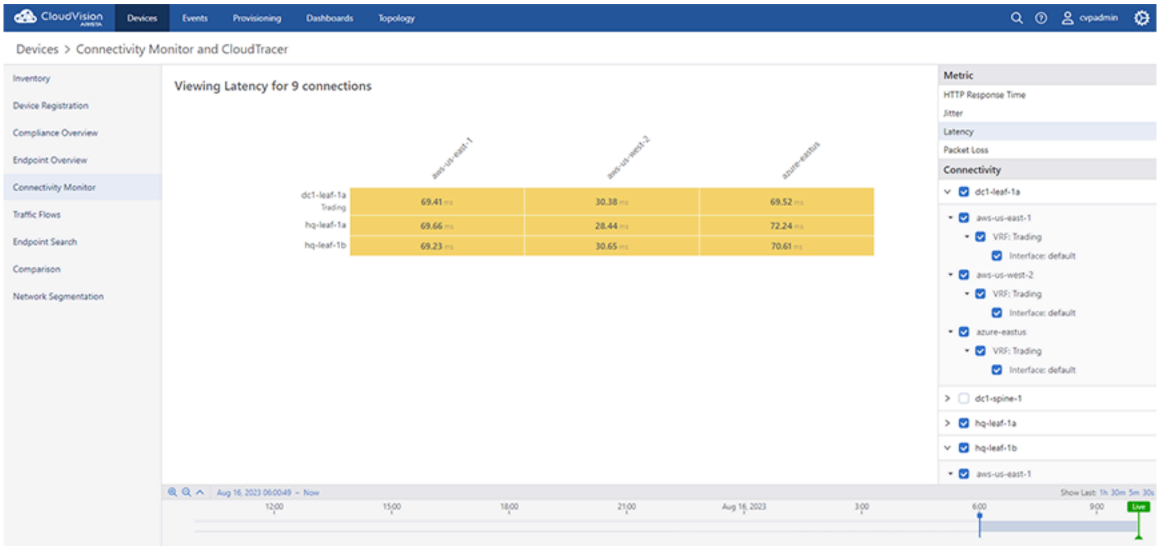
The Connectivity Monitor includes Cloud Tracer to monitor metrics streamed from EOS devices. This section includes:

- Accessing the CloudTracer Screen
- Connectivity Monitor with VRF Support

7.11.1 Accessing the Connectivity Monitor and CloudTracer Screen

To view data metrics, open to the Connectivity Monitor and CloudTracer by selecting the **Devices** tab and selcting **Connectivity Monitor** from the left-side menu bar.

Figure 7-36: Connectivity Monitor and CloudTracer Screen



Viewing Latency for 9 connections

	aws-us-east-1	aws-us-west-2	azure-eastus
dc1-leaf-1a Trading	69.41 ms	30.38 ms	69.52 ms
hq-leaf-1a	69.66 ms	28.44 ms	72.24 ms
hq-leaf-1b	69.23 ms	30.65 ms	70.61 ms

- ☑ dc1-leaf-1a
  - ☑ aws-us-east-1
    - ☑ VRF: Trading
      - ☑ Interface: default
  - ☑ aws-us-west-2
    - ☑ VRF: Trading
      - ☑ Interface: default
  - ☑ azure-eastus
    - ☑ VRF: Trading
      - ☑ Interface: default
- □ dc1-spine-1
- ☑ hq-leaf-1a
- ☑ hq-leaf-1b
  - ☑ aws-us-east-1

This screen is divided into the following two panels:

- Right Panel of the CloudTracer Screen
- Left Panel of the CloudTracer Screen

7.11.1.1 Right Panel of the CloudTracer Screen

This panel provides the following metric options:

- **Metric** pane - Click any of the following entities to view the corresponding current metric for n connections where n is the count of selected devices and hosts:
  - HTTP Response Time
  - Jitter
  - Latency
  - Packet Loss
- **Connections** pane
  - Device or host search string - Type the device or host name for a quick search
  - Configured devices - Select the required devices and hosts to view corresponding metrics

7.11.1.2 Left Panel of the CloudTracer Screen

This panel displays metrics of selected options in the following ways:

- Current information of the selected metric type from selected devices and hosts

  Note: Metrics are streamed whenever data is gathered on EOS switches. The default interval to query metrics data is five seconds.
- Click on a metric to view detailed information.
- Double click on a metric to view a graph of a selected metric. From the graph you can select to view:
  - Metric History
  - Data Table

- Data Paths
- Statistics
- Related Metrics

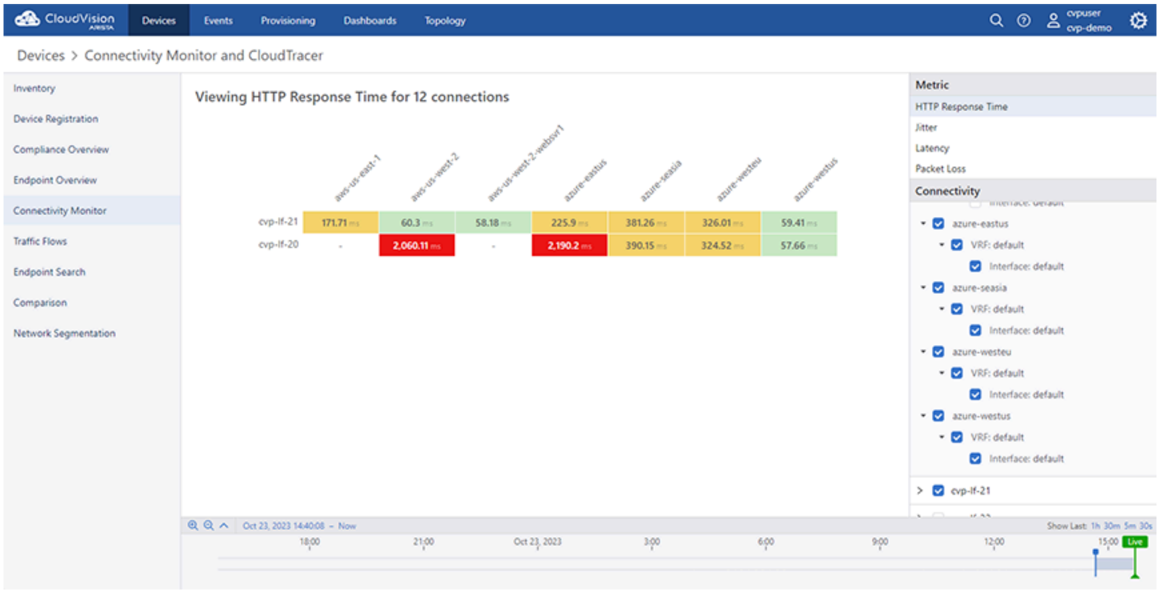
7.11.2 Connectivity Monitor with VRF Support

Connectivity Monitor with VRF support allows you to configure multiple VRFs for each host and multiple source interfaces within each host on each device.

Viewing Connectivity Monitor with VRF Support

To view Connectivity Monitor with VRF Support, select **Connectivity Monitor** from the **Devices** tab.

Figure 7-37: Viewing VRF Results in Connectivity Monitor



Viewing HTTP Response Time for 12 connections

	aws-us-east-1	aws-us-west-2	aws-us-west-2-websvr1	azure-eastus	azure-seasia	azure-westeu	azure-westus
cvp-lf-21	171.71 ms	60.3 ms	58.18 ms	225.9 ms	381.26 ms	326.01 ms	59.41 ms
cvp-lf-20	-	2,060.11 ms	-	2,190.2 ms	390.15 ms	324.52 ms	57.66 ms

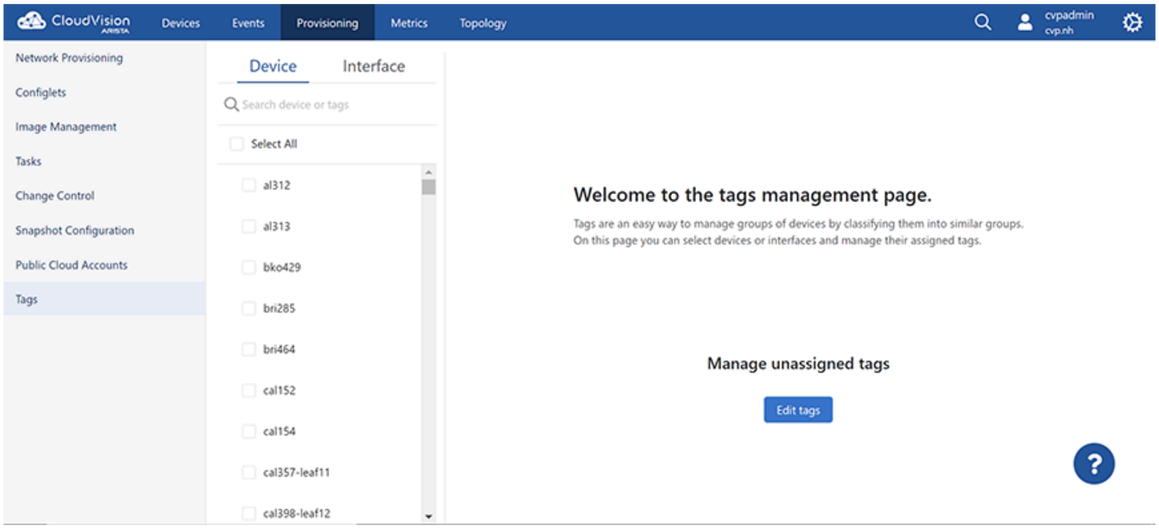
You can select individual host/VRF/interface combinations to view latency/jitter etc. information for just the selection. Selection options include:

- Selecting the checkbox next to a VRF name will select all source interfaces on the VRF.
- Selecting the checkbox next to the name of the host will select all VRFs and all source interfaces within each VRF.
- Selecting the checkbox next to the device name will select every host configuration available on the device.

7.12 Managing Tags

On the CloudVision portal, navigate to **Provisioning** > **Tags** to view the Tags Management screen. See the figure below.

Figure 7-38: Tags Management Screen



Welcome to the tags management page.

Tags are an easy way to manage groups of devices by classifying them into similar groups. On this page you can select devices or interfaces and manage their assigned tags.

This screen provides the following functionalities:

- **Search device or tags** field under the **Devices** column **-** Type either the required device name, tags category, or tag name for a quick search of devices and tags.
- **Search device, interface, or tags** field under the **Interface** column **-** Type either the required device name, tags category, tag name, or interface name for a quick search of device, interface, or tags.
- **Select All** checkbox - Select the checkbox to choose all devices simultaneously.
- **Edit tags** button - Click to delete unassigned tags. See Deleting Unassigned Tags.

7.12.1 Creating and Assigning Tags

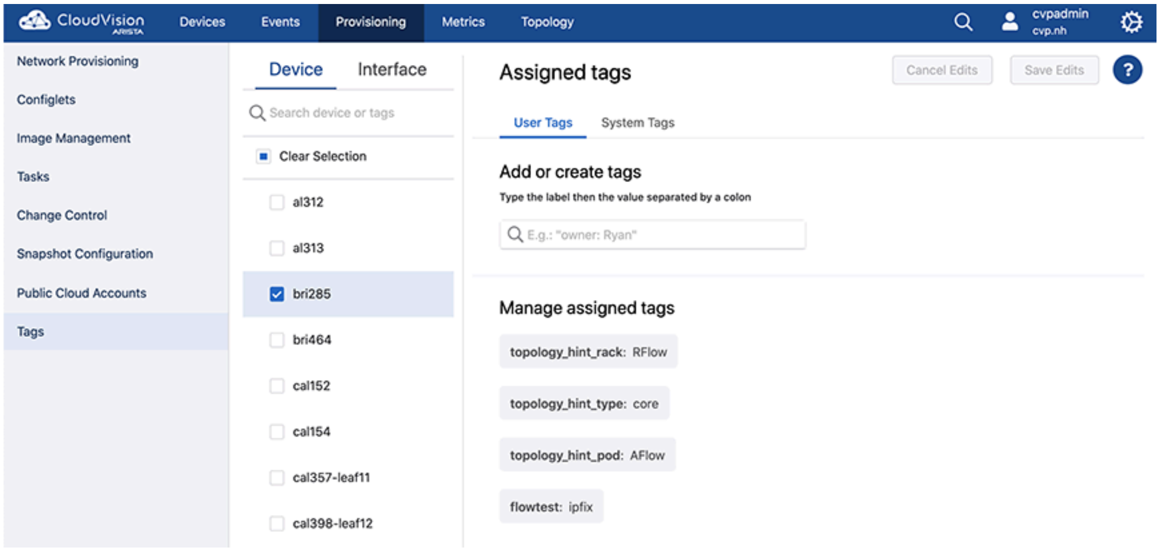
Perform the following steps to create and assign a tag to a device:

1. On CVP, click **Provisioning** > **Tags**.

   The system displays the tags screen.
2. On the **Device** pane, select device(s) to which you want to create and assign a tag.

The system opens the **Assigned tags** pane. See the figure below.

Figure 7-39: Create and Assign



Note:

- Optionally, use the search bar for searching required devices.
- To manage interface tags, click the **Interface** tab and perform required tasks.

3. Type the new tag in the search field under **User Tags** > **Add or create tags** > **Type the label then the value separated by a colon**.

   Note:

   - Tags should be of the form <*label*>: <*value*>. For example, owner: Bill.
   - The **System Tags** pane displays tags that are automatically created and assigned by the system.

4. Click **Create and Assign**.

   Note: If you had selected multiple devices, the new tag will be simultaneously assigned to all selected devices.

   The new tag is displayed under **Manage assigned tags**.

7.12.2 Deleting Assigned Tags

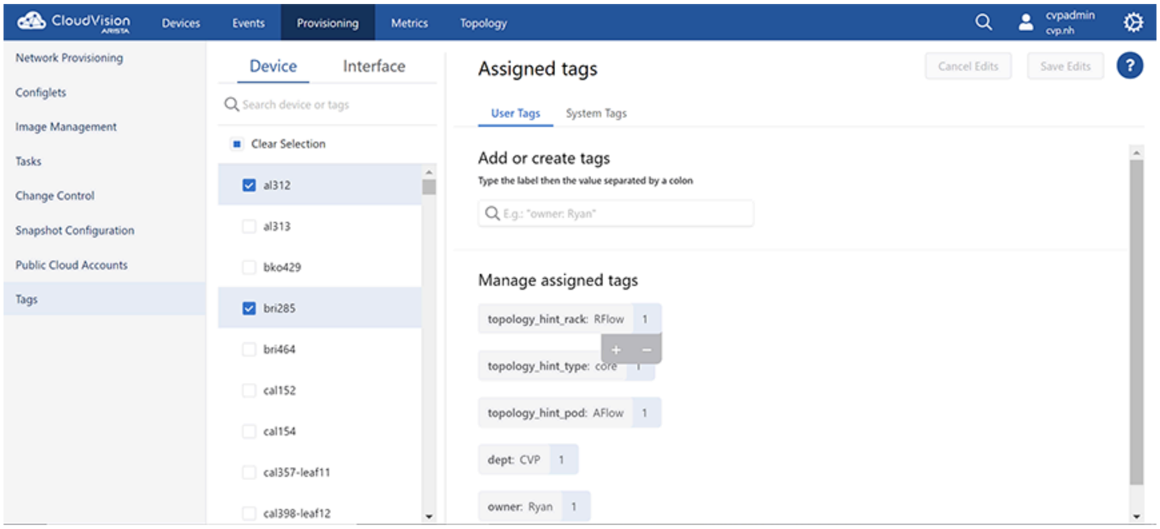
Perform the following steps to delete an assigned tag:

1. On CVP, click **Provisioning** > **Tags**.

   The system displays the tags screen.
2. On the **Device** pane, select the device(s) which is associated with the tag that needs to be removed.

The system displays all tags assiged to the selected device(s) under **Manage assigned tags**.

Figure 7-40: Associated with Selected Devices



Note:

- Optionally, use the search bar for searching required devices or tags.
- Hovering the cursor on the number next to the tag name, lists the devices to which the current tag is assigned.

3. Click the tag that needs to be removed.

   The system displays plus and minus signs when the tag is clicked.
4. Click the minus sign to delete the selected tag.
5. Click **Save Edits**.

7.12.3 Adding Tags to Multiple Devices

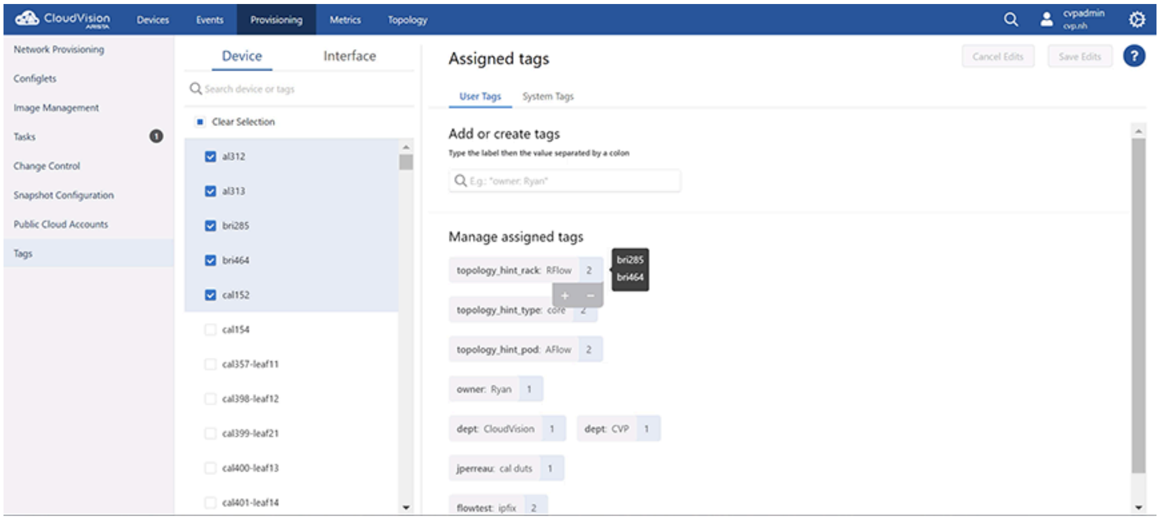
Perform the following steps to add a tag to multiple devices simultaneously:

1. On the main pane of the tags screen, select the device to which the tag has already been assigned to; and new devices to which the tag needs to be assigned.

   Under **Manage Assigned Tags** on the right pane, CVP lists tags that are assigned to selected devices.

Note: Hovering the cursor on the number next to the tag name, lists the devices to which the current tag is assigned. See the figure below.

Figure 7-41: Tag Assigned to Multiple Devices



2. Click the desired tag.

   The system pops up plus and minus signs beneath the tag.
3. Click the plus sign to add this tag to all selected devices.
4. Click **Save Edits**.

7.12.4 Removing Tags from Multiple Devices

Perform the following steps to remove a tag from multiple device simultaneously:

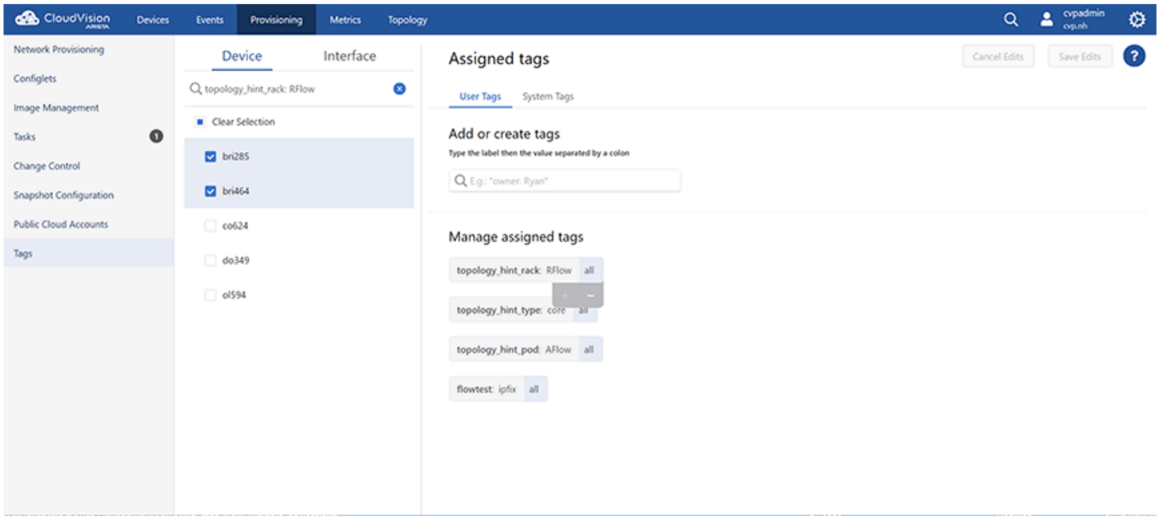
1. On the main pane of the tags screen, select devices that are assigned with the tag that needs to be removed.

   Note: Alternatively, search the tag that needs to be removed. CVP lists all devices to which the tag is assigned to. To remove the tag from few devices, select only devices from which the tag needs to be removed. If you select all devices, the tag will be removed from all devices.

   Under **Manage Assigned Tags** on the right pane, the system lists tags that are assigned to selected devices.
2. Click the tag that needs to be removed.

The system pops up plus and minus signs beneath the tag. See the figure below.

Figure 7-42: Remove Tag from Multiple Devices



Search: topology_hint_rack: RFlow

☑ bri285
☑ bri464
□ co624
□ do349
□ ol594

topology_hint_rack: RFlow	all
topology_hint_type: core	all
topology_hint_pod: AFlow	all
flowtest: ipfix	all

3. Click the minus sign to remove the tag from all selected devices.
4. Click **Save edits**.

7.12.5 Deleting Unassigned Tags

Perform the following steps to manage unassigned tags:

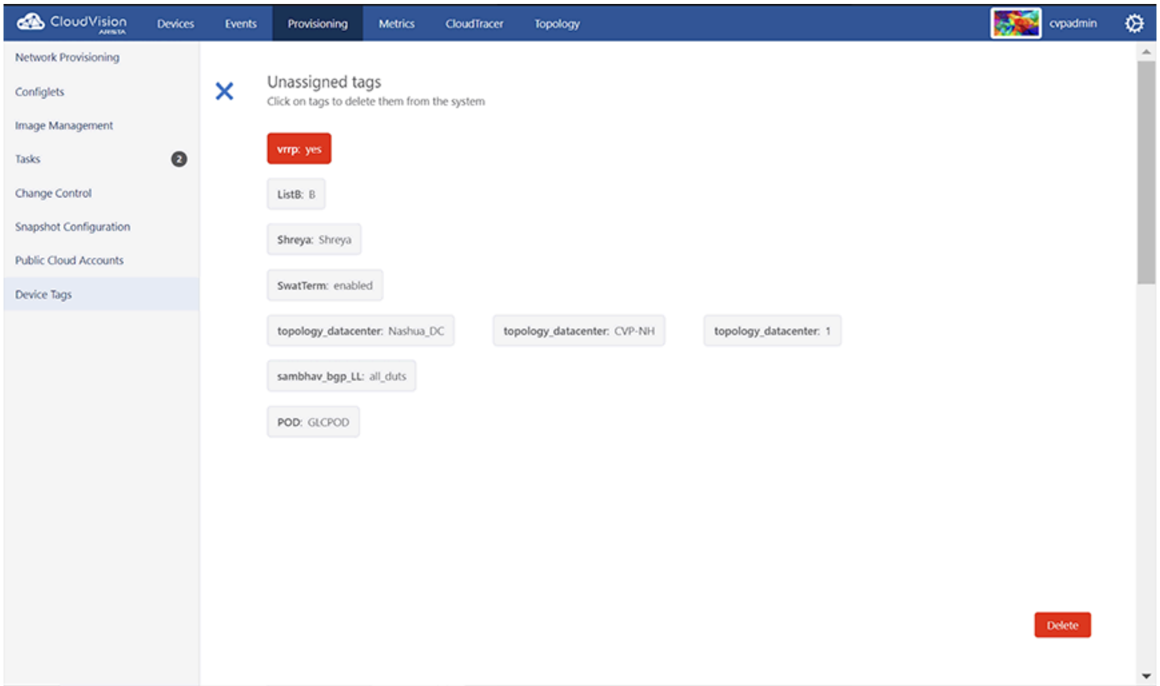
1. On CVP, click **Provisioning** > **Tags**.

   The system displays the tags screen.
2. On the main pane of the tags screen, click **Edit tags**.

   The system lists all unassigned tags.
3. Click the tag that needs to be removed.

The clicked tag turns to red.

Figure 7-43: Delete Unassigned Tags



Unassigned tags

Click on tags to delete them from the system

vrrp: yes

ListB: B

Shreya: Shreya

SwatTerm: enabled

topology_datacenter: Nashua_DC

topology_datacenter: CVP-NH

topology_datacenter: 1

sambhav_bgp_LL: all_duts

POD: GLCPOD

4. Click **Delete**.

   The system deletes the tag from CVP.

7.13 Accessing Dashboards

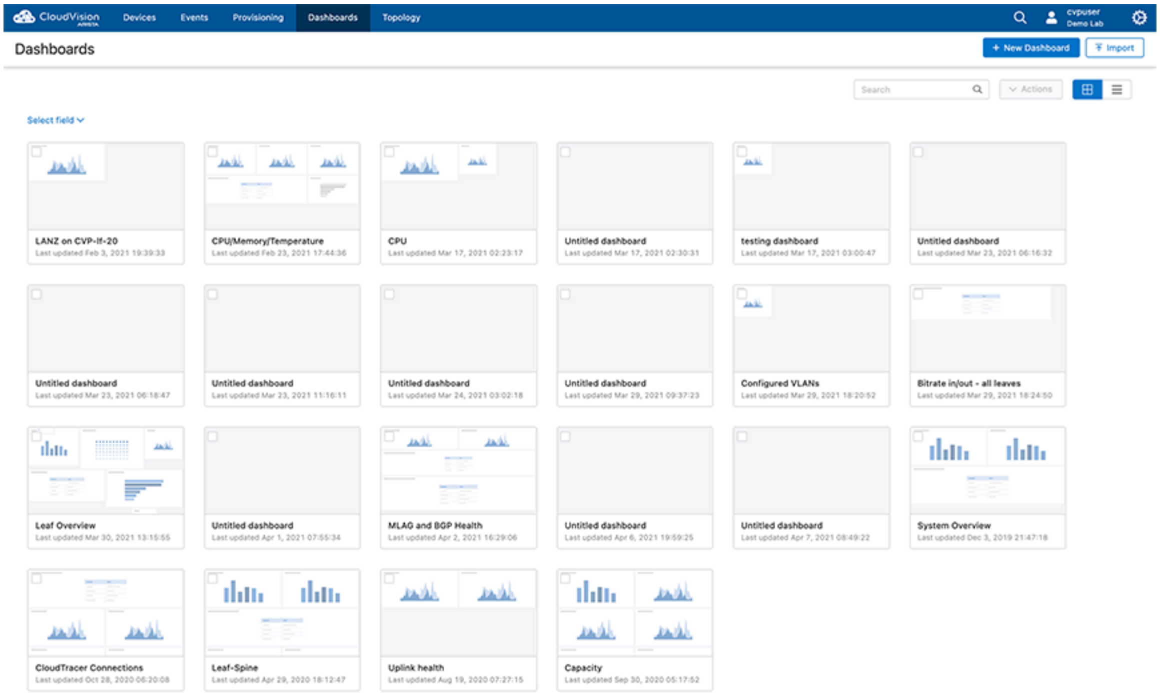
The Dashboards application allows you to create customizable dashboards consisting of multiple metrics across various datasets in different views. You can quickly resize and drag widgets on the grid to accommodate various custom layouts views. Data gathered from devices configured for streaming telemetry data to CVP.

- Dashboard Manager
- Editing and Creating Dashboards

7.13.1 Dashboard Manager

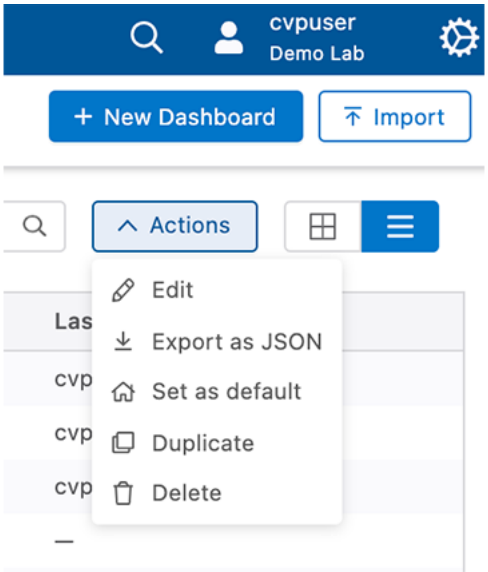
Dashboards Manager is where you are presented with the list of available dashboards. This screen can be viewed in either a grid or table format.

Figure 7-44: Dashboard Manager


CloudVision
Devices
Events
Provisioning
Dashboards
Topology
cvpuser
Demo Lab
Dashboards
+ New Dashboard
Import
Search
Actions
Select field
LANZ on CVP-lf-20
Last updated Feb 3, 2021 19:39:33
CPU/Memory/Temperature
Last updated Feb 23, 2021 17:44:36
CPU
Last updated Mar 17, 2021 02:23:17
Untitled dashboard
Last updated Mar 17, 2021 02:30:31
testing dashboard
Last updated Mar 17, 2021 03:00:47
Untitled dashboard
Last updated Mar 23, 2021 06:16:32
Untitled dashboard
Last updated Mar 23, 2021 06:18:47
Untitled dashboard
Last updated Mar 23, 2021 11:16:11
Untitled dashboard
Last updated Mar 24, 2021 03:02:18
Untitled dashboard
Last updated Mar 29, 2021 09:37:23
Configured VLANs
Last updated Mar 29, 2021 18:20:52
Bitrate in/out - all leaves
Last updated Mar 29, 2021 18:24:50
Leaf Overview
Last updated Mar 30, 2021 13:15:55
Untitled dashboard
Last updated Apr 1, 2021 07:55:34
MLAG and BGP Health
Last updated Apr 2, 2021 16:29:06
Untitled dashboard
Last updated Apr 6, 2021 19:59:25
Untitled dashboard
Last updated Apr 7, 2021 08:49:22
System Overview
Last updated Dec 3, 2019 21:47:18
CloudTracer Connections
Last updated Oct 28, 2020 06:20:08
Leaf-Spine
Last updated Apr 29, 2020 18:12:47
Uplink health
Last updated Aug 19, 2020 07:27:15
Capacity
Last updated Sep 30, 2020 05:17:52

Each dashboard on the grid provides the dashboard name, description, and an approximate layout of the dashboard. To perform actions on any of the dashboards, select one or more dashboards by selecting the checkbox associated with each dashboard.

Figure 7-45: Dashboard Actions Menu



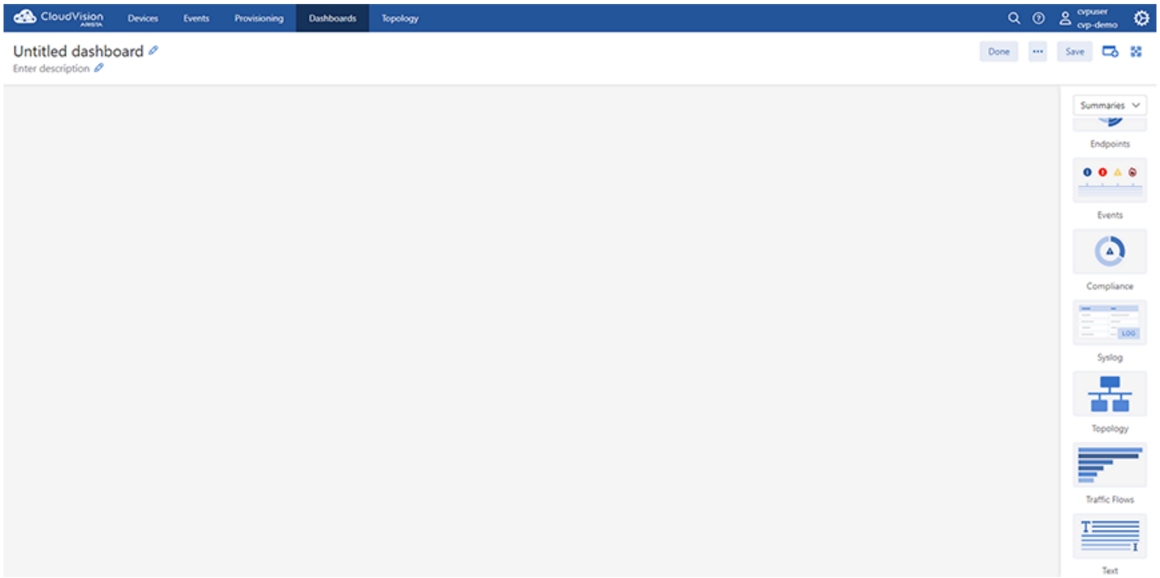
7.13.2 Editing and Creating Dashboards

Creating a Dashboard

Perform the following steps to create a dashboard.

1. Select **New Dashboard** from the Dashboard Manager page.
2. Select one or more widgets to display information.

Figure 7-46: Dashboard Widgets



3. Select the widget in the main screen to configure and label the widget.
4. Enter a title and description of the new dashboard.
5. Select **Save Changes** to save the new dashboard.

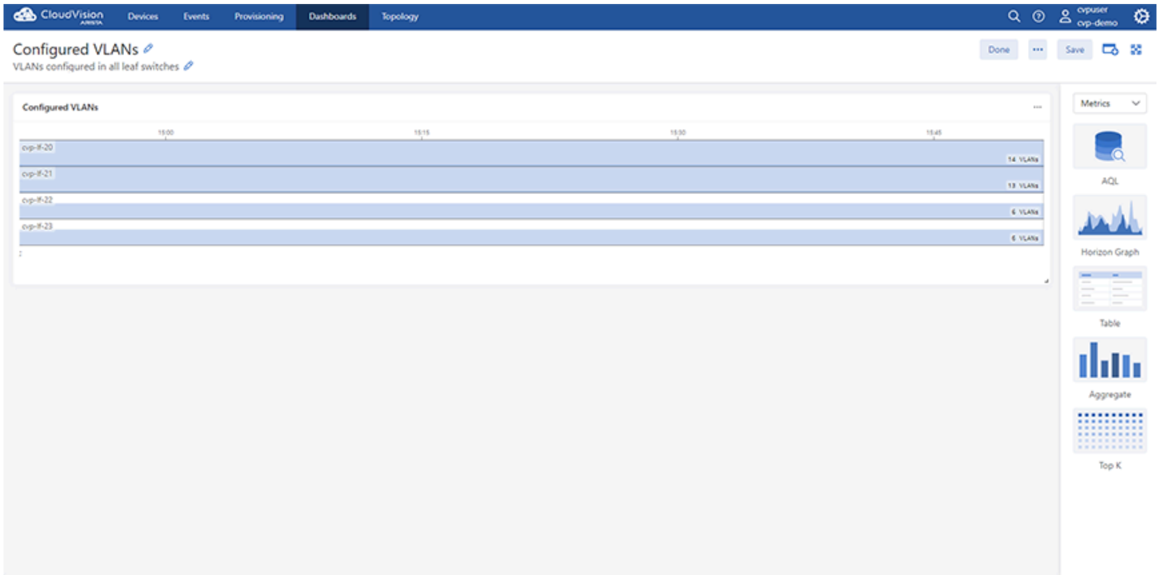
Editing a Dashboard

Perform the following steps to edit a dashboard. Dashboard widgets can be added, removed, or configured while in editing mode.

1. Select a dashboard to display from the Dashboard Manager page.

2. Select **Edit Dashboard** from the Dashboard Manager page.

Figure 7-47: Editing a Dashboard



3. Select a currently displayed widget in the main screen to edit or configure as needed.
4. To add a new widget, select from widgets tab.
5. To change the inputs, select the Inputs tab to configure as needed.
6. Select the pencil icons to edit the dashboard title and description.
7. Select **Save Changes** to save the changes.

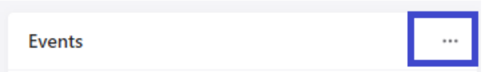
7.13.3 Dashboard Panel Appearance Settings

Every panel has four configurable appearance settings. The available settings include:

- **Show Title:** Select whether to display the title or not.
- **Title Size:** Select a size for the title of the panel.
- **Show Headline Divider:** Hide the separator between the panel title and the panel contents.
- **Show Panel Background Color:** Enable or disable the panel background color.

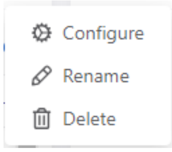
1. Click the ellipse to the right of the dashboard title.

Figure 7-48: Accessing Edit Dashboard Appearance



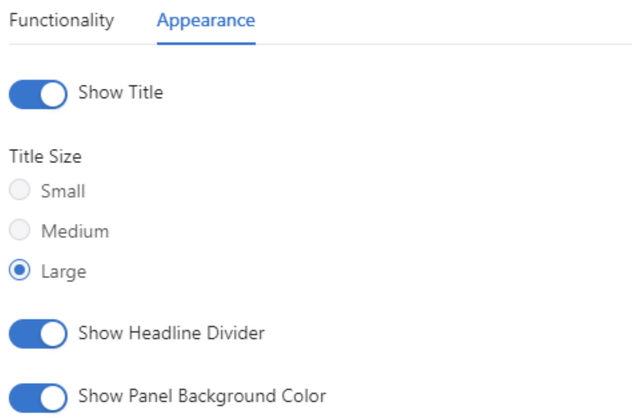
2. Click **Configure** in the dashboard configuration menu.

Figure 7-49: Dashboard Configuration Menu



3. Select the appearance settings for your dashboard.

Figure 7-50: Dashboard Appearance Menu



Functionality | Appearance

● Show Title

Title Size

○ Small

○ Medium

● Large

● Show Headline Divider

● Show Panel Background Color

7.13.4 Syslog Panel

The Syslog panel is a dashboard element that allows to you view log messages for the devices both in real-time or a selected timeframe.

7.13.4.1 Creating a Syslog Panel

1. Create a new dashboard or edit an existing dashboard.
2. On the sidebar, select the **Summaries** category and select the **Syslog panel** .

7.13.4.2 Configuring a Syslog Panel

Follow this procedure to Filter log messages by tags (Optional). A single tag filter input is associated with one tag. This can be a single device, or it could include many devices that grouped within a single tag.

1. On the sidebar, select **Input** category, and select **Single Tag Filter**.
2. Click on the ellipsis of the input and select **Configure**.
3. On the Settings Drawer, define a name for the input (Optional).
4. Select device input type.
5. Choose the tag label.
6. Close the settings drawer.
7. Click on the input to select its specific value. Select a tag value from the dropdown.
8. Click on the ellipsis of the Syslog panel and select **Configure**.
9. On the Settings Drawer, click on the **Dashboard Inputs** field to select the name of the single tag filter.
10. Close the settings drawer.

Log messages in the syslog panel will be now filtered by the specified tag.

7.13.5 Dashboards with Custom Query Language widget

The AQL panel is a dashboard element that allows you to create custom data displays using the CloudVision Advanced Query Language (AQL). This gives you complete control over what data the panel displays and how it displays it. You define the inputs and write the AQL query that feeds data to the panel. Further customization is available through creating a color mapping for the panel’s display, defining units, and decimal places among other options. You can create custom dashboards with AQL panels that are acutely relevant to your organization.

There are three elements:

- Inputs: These are used by the AQL query to feed data to the AQL panel AQL
- Panel: This is the display item within your dashboard and which uses the AQL query and any inputs to render a display AQL
- Panel Visualization: The AQL panel has five ways to display the data fed to it (Table, Single Value, Bar Graph, Line Graph, and Donut), which each requires that the AQL query be formatted in a particular way. Each visualization can be further customized to change how it displays its data

The AQL panel is currently in beta and needs to be enabled as a setting. To enable the AQL panel, go to **General Settings** and turn on the toggle **Beta Widgets** under **Features**.

The Arista Support page titled Dashboards with Custom Query Language widget provides detailed configuration instructions and a tutorial about CloudVision Advanced Query Language (AQL).

7.13.6 Dashboard Preview

You can preview dashboards from the main dashboards screen. A windowed version of the selected dashboard can be viewed.

Preview any dashboard by accessing Dashboards and hover over the preview symbol to see a preview of a dashboard. In the preview, you can hover over relevant information to obtain details. Select any part of the preview to close the preview and load that dashboard.

7.14 Topology View

You can view the network hierarchy for the devices and subnetwork in real-time. The topology view is available for devices running on LLDP including Arista switches and connected neighbors.

Related topics:

- Setup
- Overlays
- Custom Topology Views
- Changing the Node Type
- Nodes and Features

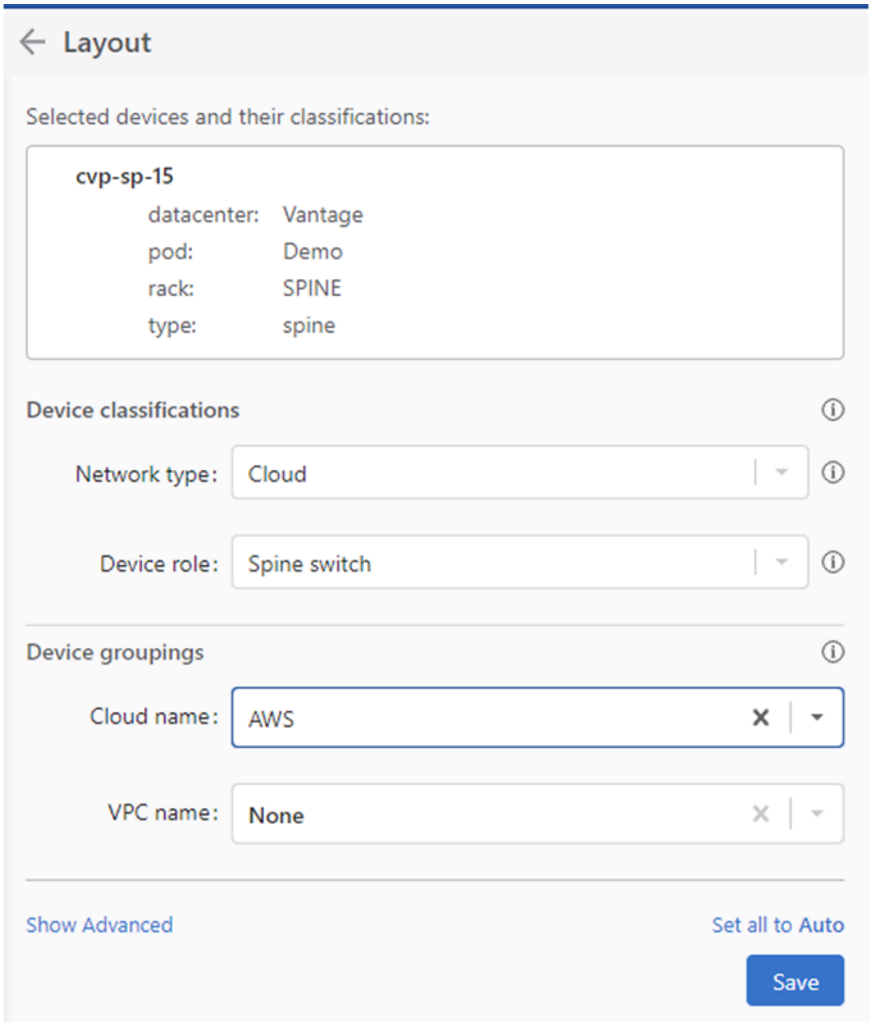
7.14.1 Setup

You can customize the topology by completing the following steps.

1. Click the **Topology** tab to view your network.
2. To enter layout hints, click on a device in the topology view and then click on the layout tab.

Following example shows the detail of a device.

Figure 7-51: CVP Detail Layout



Layout

Selected devices and their classifications:

cvp-sp-15

datacenter:	Vantage
pod:	Demo
rack:	SPINE
type:	spine

Device classifications

Network type: Cloud

Device role: Spine switch

Device groupings

Cloud name: AWS

VPC name: None

7.14.2 Overlays

You can superimpose link-level metrics overlay onto the network topology. Use the Layers Panel to view these overlays and color-codes based on the severity of that metric. Following are the overlays supported in this release.

The following table lists the Overlays supported in this release.

Table 13: Supported Overlays

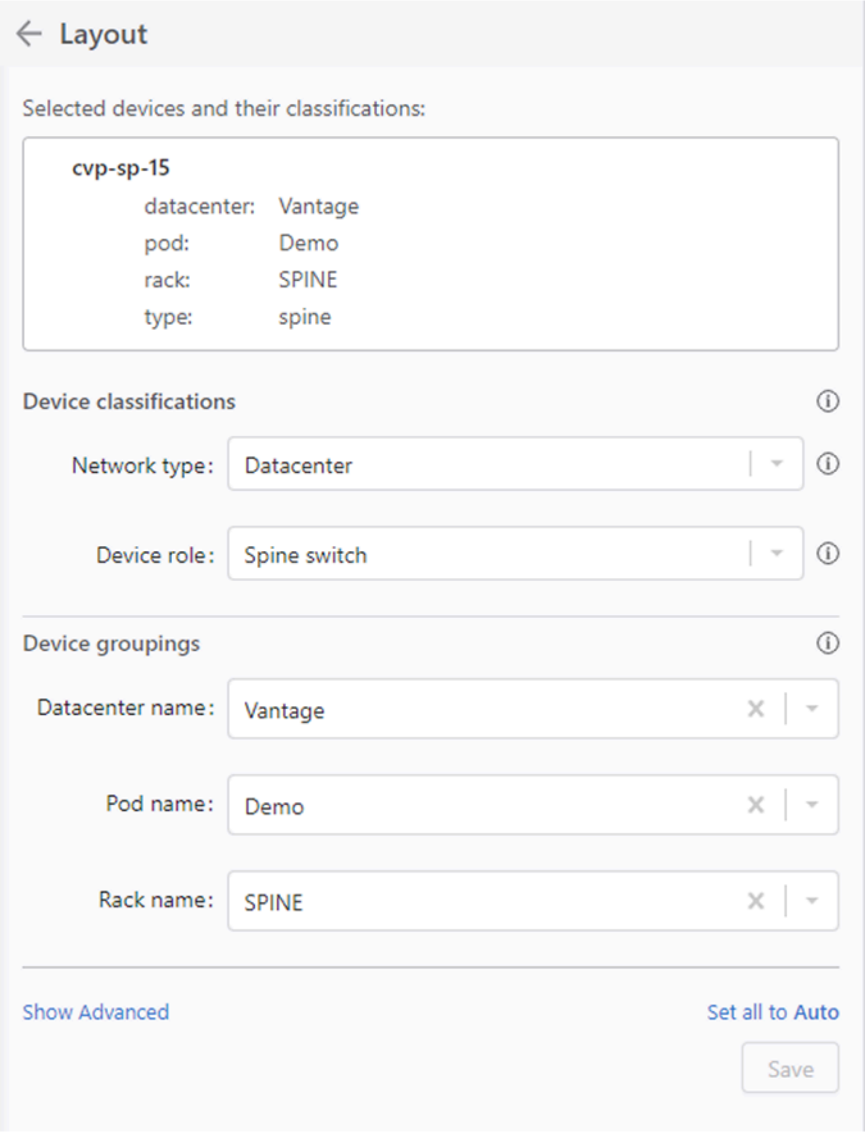
Overlay	Description
Bandwidth Utilization	Shows the bitrate as a percentage of the speed of the link. It uses the maximum bitrate in either direction on the link, averaged out over a one-minute window. Light green indicates a small percent of the link is being used, while darker greens indicate higher usage. Beyond 80% utilization, the links show up in yellow or red.
Traffic Throughput	Shows the bitrate of a link as an absolute number. Darker blues indicate higher utilization.
Error Rates	Show if either end of a link is registering input or output errors (for example, CRC Errors). It uses a one-minute window, and displays severity in increasingly dark reds.
Discard Rates	Indicate that a link is dropping packets, likely due to congestion. Links discarding more packets in a one-minute window are shown in darker red.
None	Turns off all colors.

7.14.3 Custom Topology Views

From the Topology tab, you can perform the following steps to customize a view:

1. To move a rack to a different pod use the Pod field. For example, the switch called cv-demo-sw3 is set to be in a pod 1.

Figure 7-52: User Layout Hints



Layout

Selected devices and their classifications:

cvp-sp-15

datacenter: Vantage
pod: Demo
rack: SPINE
type: spine

Device classifications

Network type: Datacenter

Device role: Spine switch

Device groupings

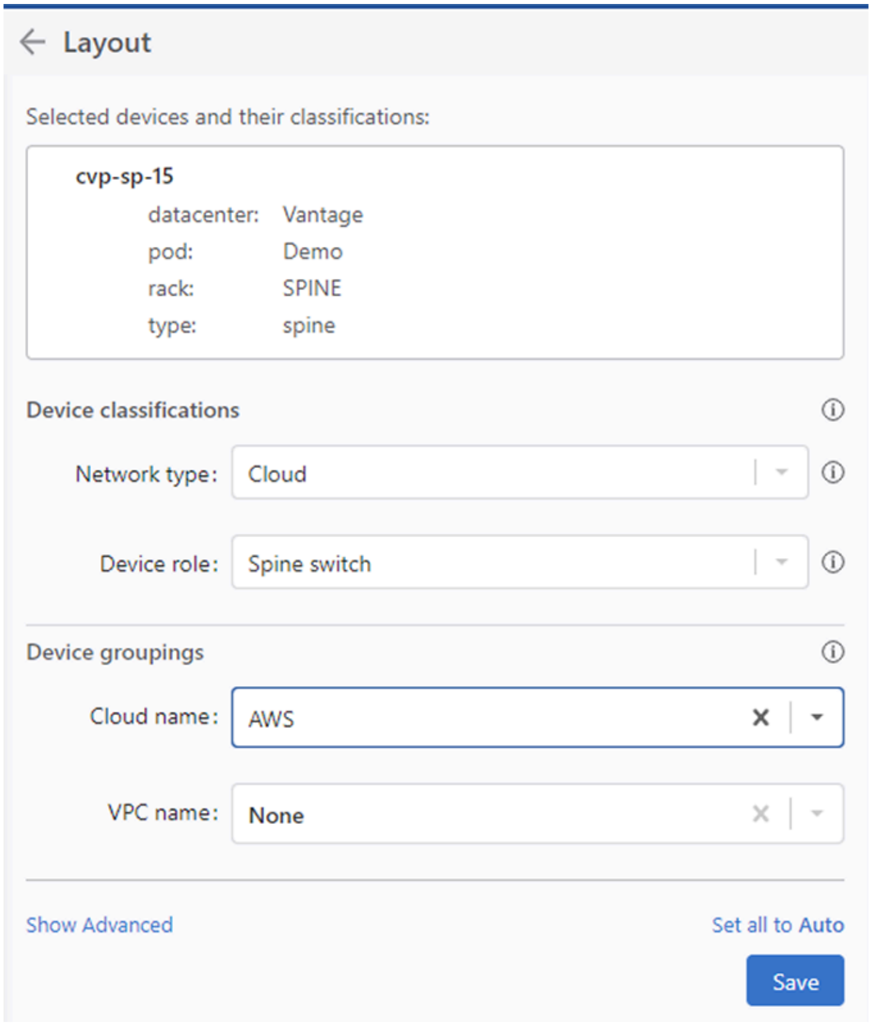
Datacenter name: Vantage

Pod name: Demo

Rack name: SPINE

2. To setup the pod or rack names, apply a layout hint for switch with alternate name or pod hint for the spine switch to rename the pod. Following example shows the top-of-rack switch cv-demo-sw3 default name change via the rack layout hint.

Figure 7-53: Device Details in Layout



Layout

Selected devices and their classifications:

cvp-sp-15

datacenter:	Vantage
pod:	Demo
rack:	SPINE
type:	spine

Device classifications

Network type: Cloud

Device role: Spine switch

Device groupings

Cloud name: AWS

VPC name: None

7.14.4 Changing the Node Type

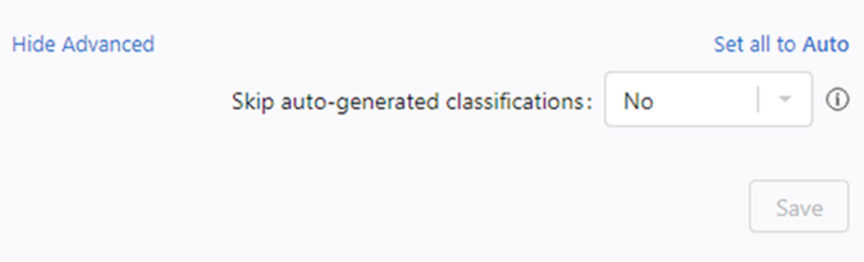
The following table lists the node types supported by the Topology view.

Table 14: Supported Node Type

Node Type	Description
Edge Device	The device is an edge device, for example, leading to the Internet or another network, or a similar function device.
Core Switch	The device is at the core level switch (above spines) or similar function device.
Spine Switch	The device is a pod level (spine or aggregation) switch or similar function device.
Leaf Switch	The device is a top of rack switch or similar function device.
Endpoint Device	The device is a server or similar endpoint device.

Setting the **Node Type** layout hint gives the **Topology** view of the type of device selected. Selecting **skip auto-generating** forces the auto tagger to ignore the device and not assign or modify any of the hints.

Figure 7-54: Changing Node Type



Skip auto-generated classifications: No

7.14.5 Nodes and Features

Nodes are arranged in clusters. To expand a cluster, click on the representative **Cluster-node**. To collapse a cluster, click on the minus (**-**) icon.

You can select various overlays on the graph for color coding links.

To see details about a node and its neighbors, click on the **Node**. You can also see the immediate neighbors of the device and the metrics related to particular physical links between devices by clicking **Neighbors List**.

7.15 Topology Hierarchy Manager

Using Topology Hierarchy Manager you can construct a custom topology frameworks for your network. This allows you to customize the topology layout and how devices are mapped. A custom hierarchy is constructed in a tree-like formation consisting of layers. Each layer is associated with a tag label or value, which can be assigned in Topology using Topology Tags and Hints. Multiple hierarchies can be used in the same CloudVision cluster, so you can display different areas of your network differently.

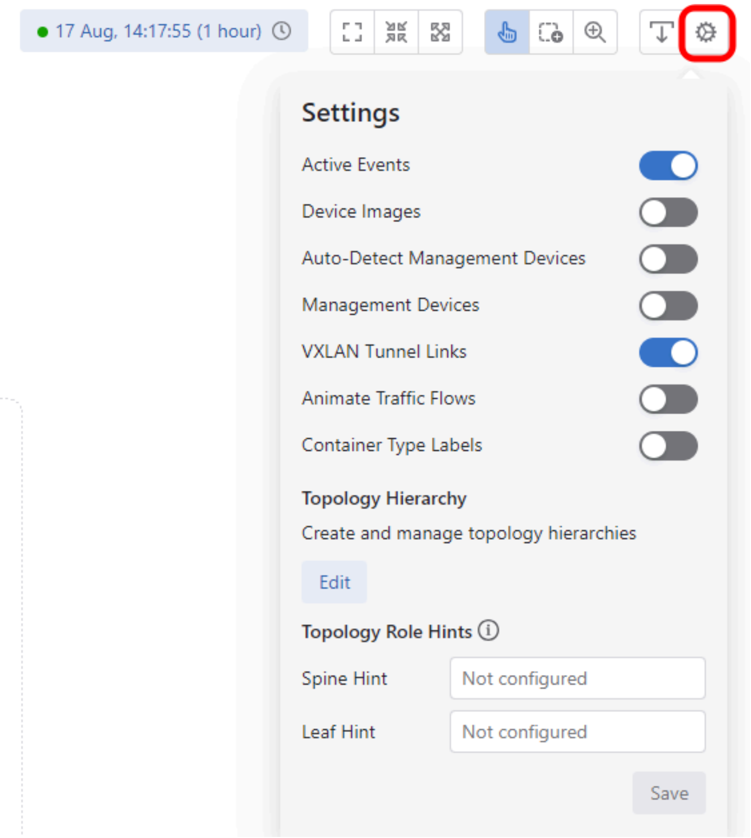
- Accessing Topology Hierarchy Manager
- Topology Hierarchy Manager Layout
- Configuring a Topology Hierarchy
- Configuring Layer Properties
- Using a Custom Topology Hierarchy

7.15.1 Accessing Topology Hierarchy Manager

To Access Topology Hierarchy Manager go to the Topologoly tab.

1. Click the **Topology Settings** icon.

   Figure 7-55: Accessing Topology Hierarchy Manager



17 Aug, 14:17:55 (1 hour)

Settings

- Active Events ☑
- Device Images ☐
- Auto-Detect Management Devices ☐
- Management Devices ☐
- VXLAN Tunnel Links ☑
- Animate Traffic Flows ☐
- Container Type Labels ☐

Topology Hierarchy

Create and manage topology hierarchies

Edit

Topology Role Hints ⓘ

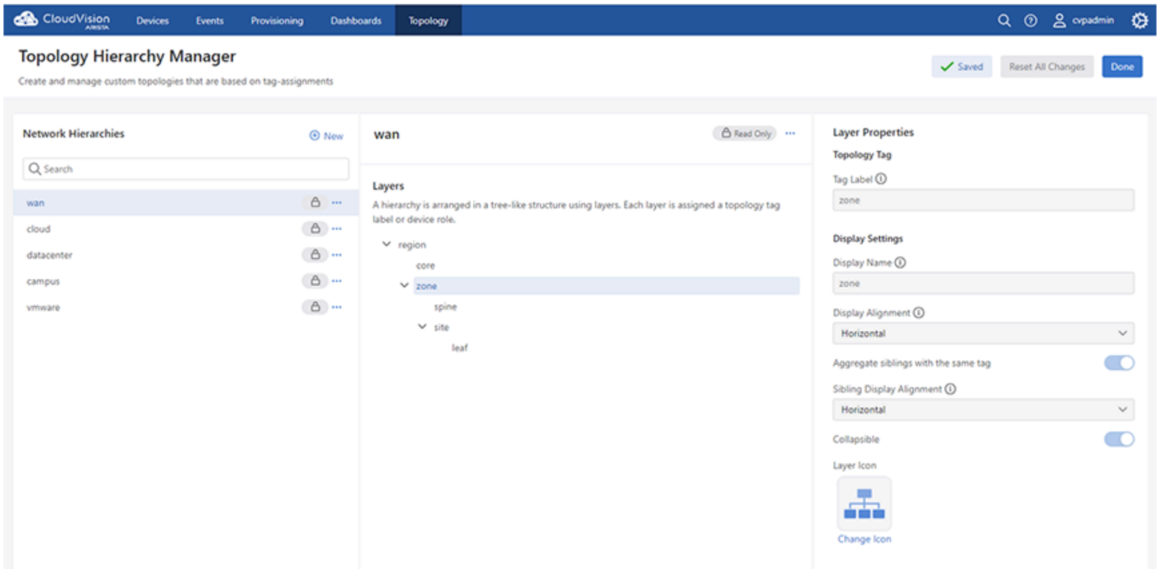
Spine Hint: Not configured

Leaf Hint: Not configured

Save

2. Click **Edit** under Topology Hierarchy. The Topology Hierarchy Manager opens.

   Figure 7-56: Topology Hierarchy Manager



Topology Hierarchy Manager

Create and manage custom topologies that are based on tag-assignments

✓ Saved | Reset All Changes | Done

Network Hierarchies ⊕ New

Search

- wan
- cloud
- datacenter
- campus
- vmware

wan Read Only

Layers

A hierarchy is arranged in a tree-like structure using layers. Each layer is assigned a topology tag label or device role.

```
region
  core
  zone
    spine
    site
      leaf
```

Layer Properties

Topology Tag

Tag Label ⓘ: zone

Display Settings

Display Name ⓘ: zone

Display Alignment ⓘ: Horizontal

Aggregate siblings with the same tag ☑

Sibling Display Alignment ⓘ: Horizontal

Collapsible ☑

Layer Icon

Change Icon

7.15.2 Topology Hierarchy Manager Layout

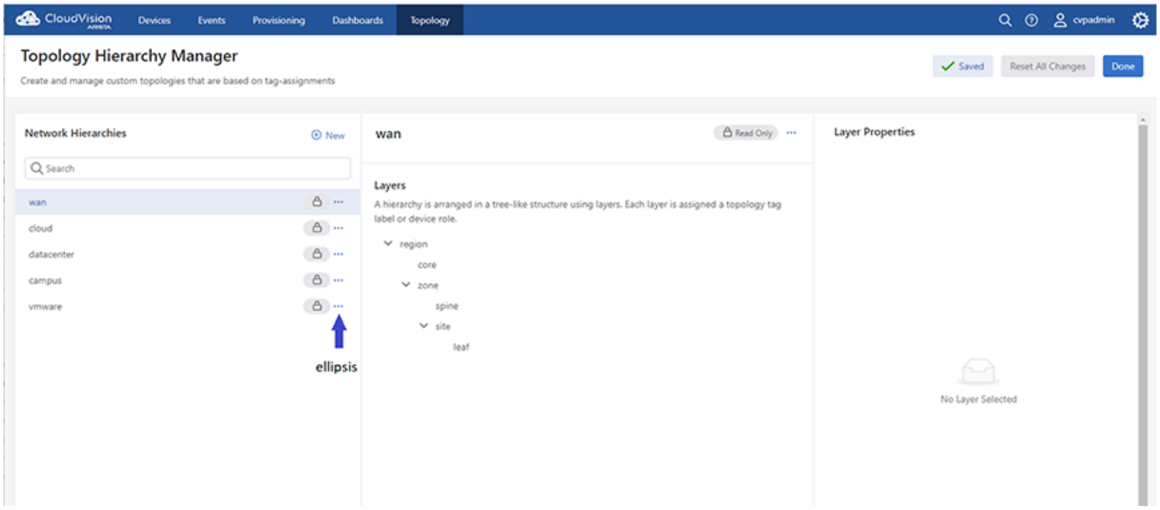
The Topology Hierarchy Manager has three key areas, which perform different functions when configuring a custom topology hierarchy.

- **Network Hierarchies:** Lists all hierarchies available to use. Those with lock icons are built-in hierarchies and cannot be edited.
- **Selected Hierarchy:** The center panel displays the layers of a selected hierarchy, which can be edited when it is a custom hierarchy.
- **Layer Properties:** The third panel displays the properties of a selected layer.

7.15.3 Configuring a Topology Hierarchy

1. Click **New**.

Figure 7-57: Topology Hierarchy Manager



Topology Hierarchy Manager

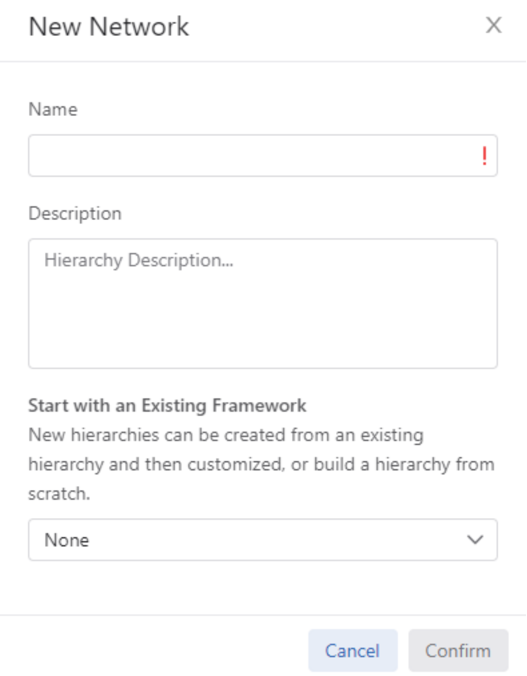
Create and manage custom topologies that are based on tag-assignments

Layers

A hierarchy is arranged in a tree-like structure using layers. Each layer is assigned a topology tag label or device role.

2. Enter the hierarchy details.

Figure 7-58: Topology Hierarchy Manager - New Network



New Network

Name

Description

Hierarchy Description...

Start with an Existing Framework

New hierarchies can be created from an existing hierarchy and then customized, or build a hierarchy from scratch.

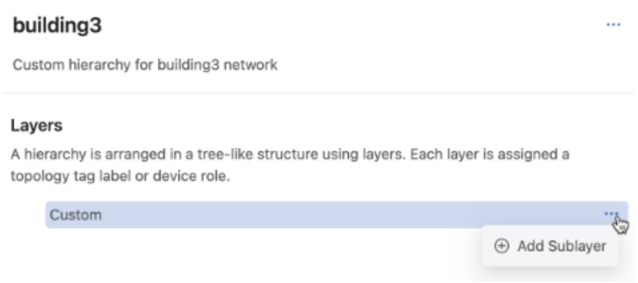
None

- **Name:** Enter a name for the hierarchy.
- **Description:** Add a description to explain the purpose of this hierarchy.
- **Existing Framework:** You can duplicate an existing hierarchy or set this option to None to start with a blank hierarchy.

3. Click **…** (ellipsis) on the root layer and select **Add Sublayer**.

   Note: You must hover over the layer name before you will see the **Options …**

   Figure 7-59: Add Sublayer

   building3

   Custom hierarchy for building3 network

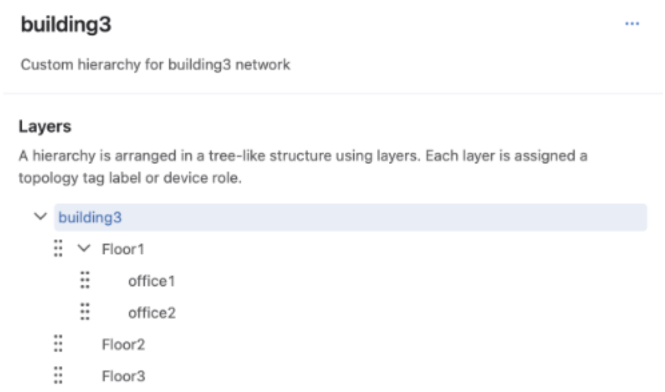
   Layers

   A hierarchy is arranged in a tree-like structure using layers. Each layer is assigned a topology tag label or device role.

   The root layer is the top layer of the hierarchy. You can change its name by configuring its layer properties.

4. Continue to add layers to match the layout of the hierarchy.

   Figure 7-60: Continue to Add Layers

   building3

   Custom hierarchy for building3 network

   Layers

   A hierarchy is arranged in a tree-like structure using layers. Each layer is assigned a topology tag label or device role.

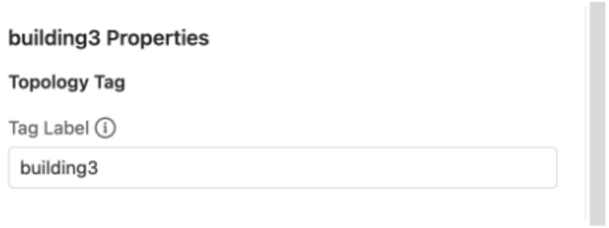
   Layer names and their display managed and when configuring a layer's properties. When your topology is mapped out and each layer's properties configured, you can use the custom hierarchy.

7.15.4 Configuring Layer Properties

The properties of a layer determine how devices map to it and how it is displayed in the topology.

1. Enter a tag label or device role.

   Figure 7-61: Enter a Tag Label

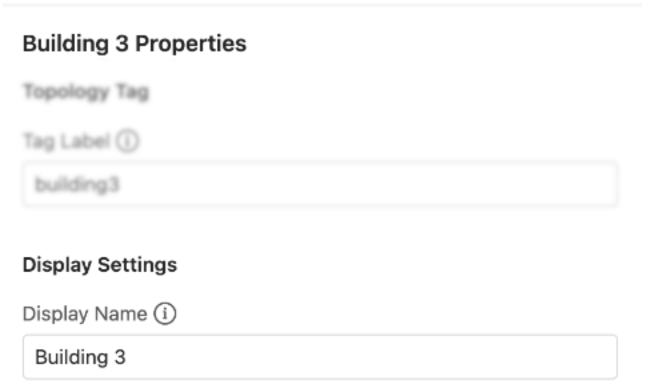
   building3 Properties

   Topology Tag

   Tag Label: building3

   The name of this input dynamically changes depending on whether it has children or not. A layer without children will accept a device role, which is a tag value. Any parent layer will accept a tag label. Tag labels are used to provide hints, which will map devices with device tags that match. A tag is a label:value pair. So assigning a tag label to a parent layer and a device role to child will create a label:value pair, like **DC1:leaf**.
2. Enter an optional display name.

   Figure 7-62: Enter an Optional Display Name

   Building 3 Properties

   Topology Tag

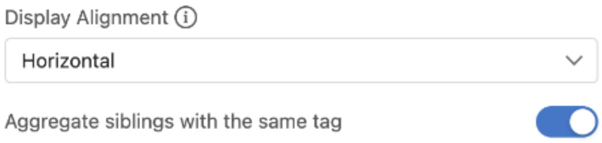
   Tag Label: building3

   Display Settings

   Display Name: Building 3

   The default display name is the tag name or device role.
3. Select a display alignment.

   Figure 7-63: Select a Display Alignment

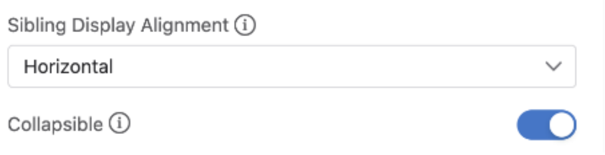
   Display Alignment: Horizontal

   Aggregate siblings with the same tag ☑
4. Enable or disable **Aggregate Siblings with the Same Tag**.

   Option only available on parent layers..

5. Select a sibling display alignment.

Figure 7-64: Select Sibling Display Alignment



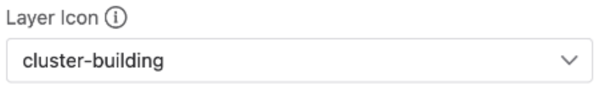
Sibling Display Alignment ⓘ

Horizontal

Collapsible ⓘ ●

6. Enable or disable **Collapsible**.
7. Select a cluster icon.

Figure 7-65: Select a Cluster Icon



Layer Icon ⓘ

cluster-building

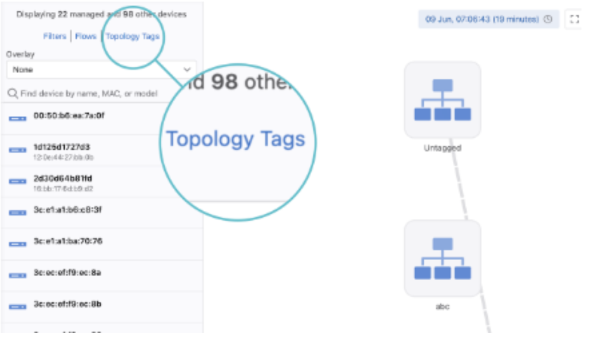
The layer icon is displayed for the container or devices matching this layer. Once the hierarchy layers have been arranged and their properties configured, you can use the custom hierarchy for your topology.

7.15.5 Using a Custom Topology Hierarchy

Custom hierarchies can be used with Topology Tags and Hints to configure your network. Topology Tags are used to assign and match existing devices and containers with child layers in the custom hierarchy. Hints use the parent’s tag label and child’s device role to automatically assign devices with matching user tags.

1. Click **Topology Tags**.

Figure 7-66: Click Topology Tags



Displaying 22 managed and 98 other devices

Overlay

None

Find device by name, MAC, or model

00:50:b6:ea:7a:0f

1d125d1727d3
12:0e:44:27:bb:0b

2d30d64b81fd
16:bb:17:6d:b9:d2

3c:e1:a1:b6:c8:3f

3c:e1:a1:ba:70:76

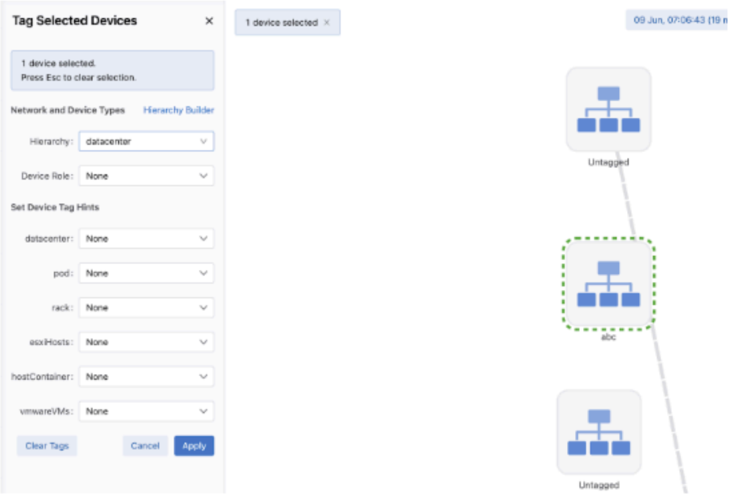
3c:ec:ef:f9:ec:8a

3c:ec:ef:f9:ec:8b

09 Jun, 07:06:43 (19 minutes)

2. Select one or more devices or containers.

Figure 7-67: Select One or More Devices or Containers



Tag Selected Devices

1 device selected.
Press Esc to clear selection.

Network and Device Types

Hierarchy: datacenter

Device Role: None

Set Device Tag Hints

datacenter: None

pod: None

rack: None

esxiHosts: None

hostContainer: None

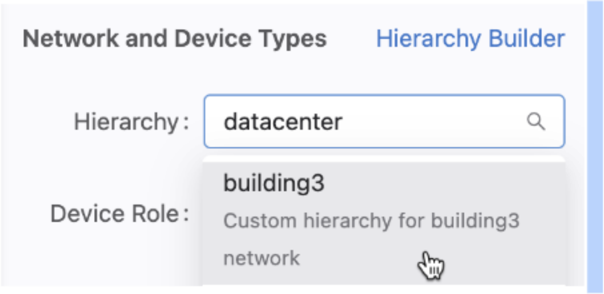
vmwareVMs: None

1 device selected

09 Jun, 07:06:43 (19 m

3. Select the custom hierarchy from the Hierarchy dropdown.

Figure 7-68: Select the Custom Hierarchy



Network and Device Types

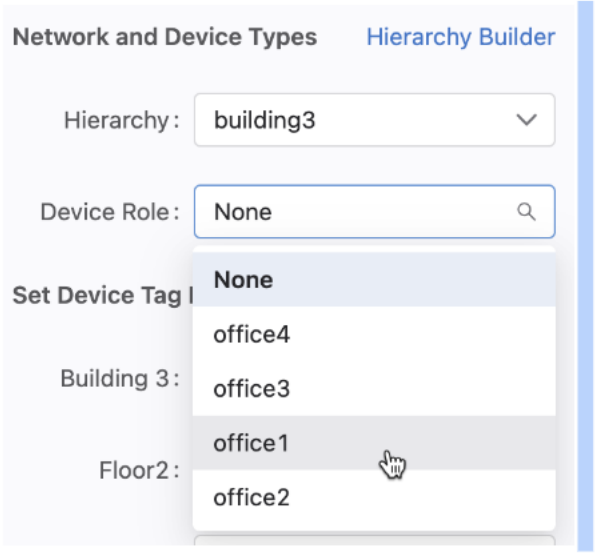
Hierarchy: datacenter

Device Role:

building3
Custom hierarchy for building3 network

4. Select a device role in the Device Role dropdown.

Figure 7-69: Select a Device Role



Network and Device Types

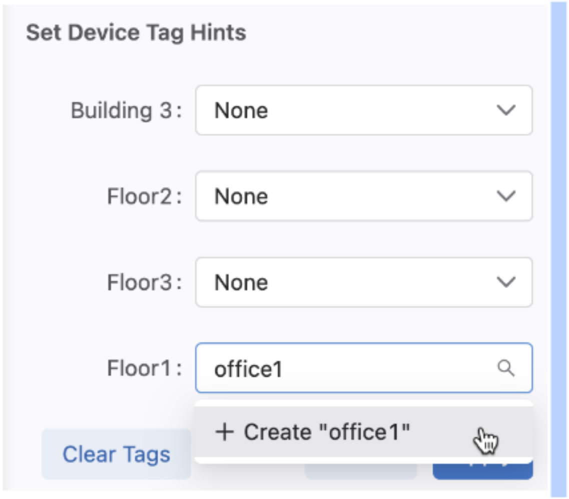
Hierarchy: building3

Device Role: None

Devices in this selected container are now assigned the layer properties of office1 in hierarchy building3..

5. Optionally provide tag hints for parent layers.

Figure 7-70: Provide Tag Hints



Set Device Tag Hints

Building 3: None

Floor2: None

Floor3: None

Floor1: office1

When a device with a user tag matching the parent layer tag label and one of that parent's children's device roles, it will be automatically positioned in the topology. In this example, if a device has the tag **Floor1:office1** it will occupy the same position in the topology as what we assigned to the above container.

6. Click **Apply**.

The selected devices or containers will now apply the layer properties to all affected devices.

7.16 Topology Filter Builder

A filter is used to exclude devices from the topology view. When a filter is enabled, a notification will be displayed in the topology view.

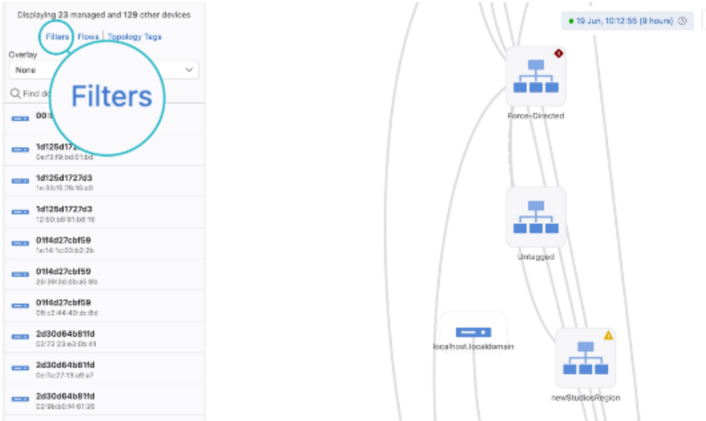
You can create permanent filters, which are saved in the Filters section of Topology. These filters can be enabled or disabled at any time. Filters are useful for only showing selected VLANs, VXLANs, or tagged devices in your topology.

7.16.1 Managing Topology Filters

You can access your filters when you want to enable or disable a filter, create a new filter, or delete an existing filter.

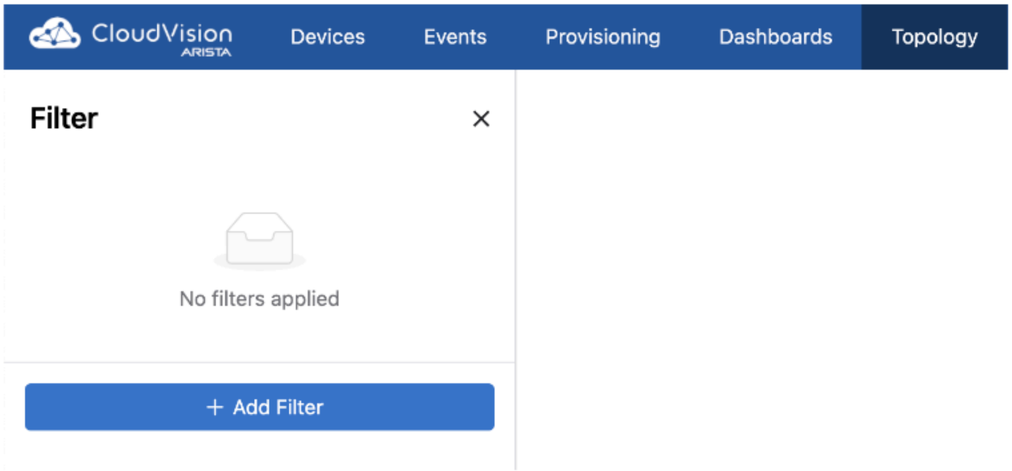
1. In the Topology tab select **Filters**.

   Figure 7-71: Accessing Topology Filters



2. Click **Add Filter**.

   Figure 7-72: Add Filter

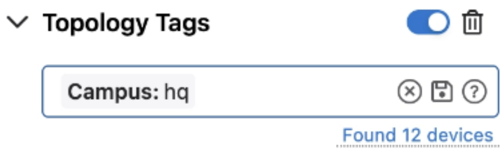


3. Edit the value of an existing filter or click **Delete** to delete a filter.
4. If adding a new filter, select a filter type from the dropdown menu.

   There are three filters to choose from:

- Topology Tags: Enter a tag query to only display devices with matching tags.

  Figure 7-73: Topology Tags Filter

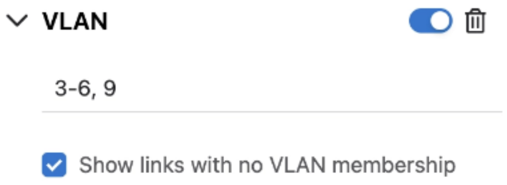
  Topology Tags

  Campus: hq

  Found 12 devices

- VLAN: Enter a VLAN ID or range to limit the display to devices in one or more VLANs.

  Figure 7-74: VLAN Filter

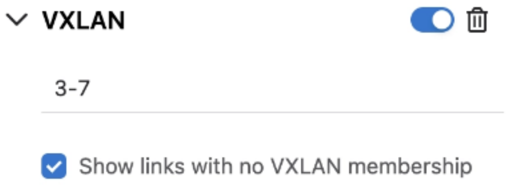
  VLAN

  3-6, 9

  ☑ Show links with no VLAN membership

- VXLAN: Enter a VNI or range to view devices belonging to a selected VXLAN or VXLANs.

  Figure 7-75: VXLAN Filter

  VXLAN

  3-7

  ☑ Show links with no VXLAN membership

  Filtering by VLAN and VXLAN membership also allows you to show or hide links that do not belong to a VLAN or VXLAN. To show links that do not belong to a VLAN or VXLAN, select the appropriate checkbox. Disable it to hide them from the display.

5. Press **Enter** if defining a VLAN or VXLAN filter. The values are saved to the filter.

You can enable and disable filters by toggling them on or off. Filters can be deleted at any time by clicking **Delete**.

7.17 Accessing Events

You can access the following events screens:

- Events Summary Screen
- Event Details Screen

Related topics:

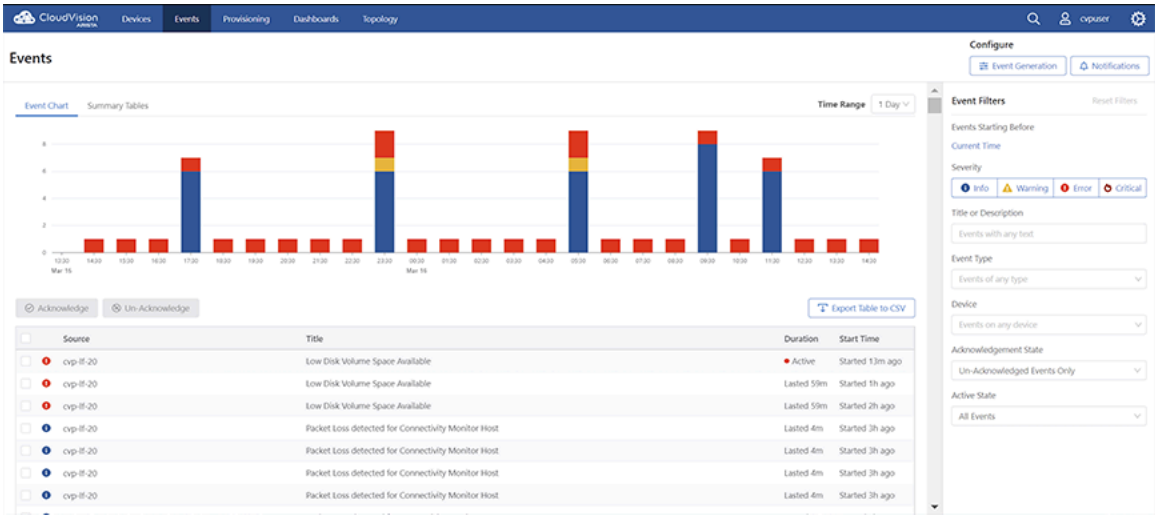
- Events Summary Screen
- Event Details Screen
- Configuring Event Generations
- Managing Events
  - Disabling All Events of the Selected Type

  - Disabling All Events of the Selected Type with Exceptions
- Acknowledging Events
- Configuring Notifications
  - Configuring Status
  - Configuring Platforms
  - Configuring Receivers
  - Configuring Rules

7.17.1 Events Summary Screen

The events summary screen displays all events, and configures alerts and event generation. To view this screen, click **Events** on the CloudVision portal. The figure below displays the events summary screen.

Figure 7-76: Events Summary Screen



Source	Title	Duration	Start Time
cvp-lf-20	Low Disk Volume Space Available	● Active	Started 13m ago
cvp-lf-20	Low Disk Volume Space Available	Lasted 59m	Started 1h ago
cvp-lf-20	Low Disk Volume Space Available	Lasted 59m	Started 2h ago
cvp-lf-20	Packet Loss detected for Connectivity Monitor Host	Lasted 4m	Started 3h ago
cvp-lf-20	Packet Loss detected for Connectivity Monitor Host	Lasted 4m	Started 3h ago
cvp-lf-20	Packet Loss detected for Connectivity Monitor Host	Lasted 4m	Started 3h ago
cvp-lf-20	Packet Loss detected for Connectivity Monitor Host	Lasted 4m	Started 3h ago

Events Starting Before: Current Time
Severity
Title or Description: Events with any text
Event Type: Events of any type
Device: Events on any device
Acknowledgement State: Un-Acknowledged Events Only
Active State: All Events

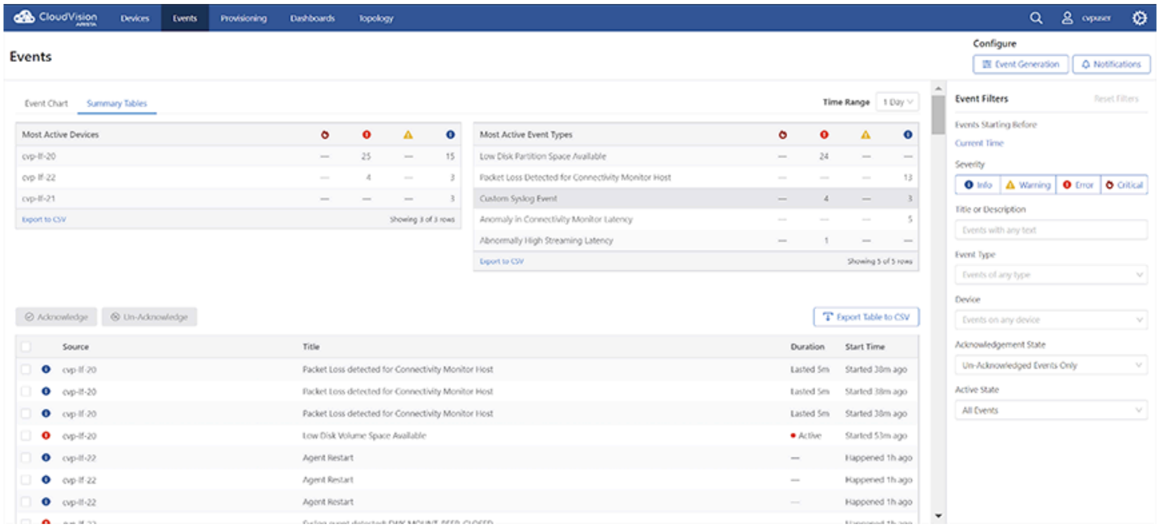
The **Events** screen provides the following information and functionalities:

- Click the **Event Generation** button to configure generating new events. Refer to Configuring Event Generations.
- Click the **Notifications** button to configure notifications. Refer to Configuring Notifications
- Left Pane
  - **Event Chart** and **Summary Tables** tabs
    - The **Event Chart** tab displays the bar graphs of all events.

      Note: Hover the cursor over the different segments of the bar graph to view the count of severity events.

- The **Summary Tables** tab displays **Most Active Devices** and **Most Active Event Types** in tabular formats. See the figure below.

Figure 7-77: Event Summary Screen - Summary Tables



Time Range: 1 Day

Most Active Devices	●	●	⚠	ⓘ
cvp-lf-20	—	25	—	15
cvp-lf-22	—	4	—	3
cvp-lf-21	—	—	—	3

Export to CSV — Showing 3 of 3 rows

Most Active Event Types	●	●	⚠	ⓘ
Low Disk Partition Space Available	—	24	—	—
Packet Loss Detected for Connectivity Monitor Host	—	—	—	13
Custom Syslog Event	—	4	—	3
Anomaly in Connectivity Monitor Latency	—	—	—	5
Abnormally High Streaming Latency	—	1	—	—

Export to CSV — Showing 5 of 5 rows

□		Source	Title	Duration	Start Time
□	ⓘ	cvp-lf-20	Packet Loss detected for Connectivity Monitor Host	Lasted 5m	Started 30m ago
□	ⓘ	cvp-lf-20	Packet Loss detected for Connectivity Monitor Host	Lasted 5m	Started 38m ago
□	ⓘ	cvp-lf-20	Packet Loss detected for Connectivity Monitor Host	Lasted 5m	Started 30m ago
□	●	cvp-lf-20	Low Disk Volume Space Available	● Active	Started 53m ago
□	ⓘ	cvp-lf-22	Agent Restart	—	Happened 1h ago
□	ⓘ	cvp-lf-22	Agent Restart	—	Happened 1h ago
□	ⓘ	cvp-lf-22	Agent Restart	—	Happened 1h ago

Events Starting Before: Current Time

Severity

Title or Description: Events with any text

Event Type: Events of any type

Device: Events on any device

Acknowledgement State: Un-Acknowledged Events Only

Active State: All Events

Note: The severity levels include critical, error, warning, and info.

- The **Time Range** dropdown menu to select the time span of events.
- The **Acknowledge** button to acknowledges selected events.
- The **Un-Acknowledge** button to renounce selected events.
- A list of all events with selection checkboxes in a tabular format.
- Click the **Export Table to CSV** button to download the table in csv format to your local drive.

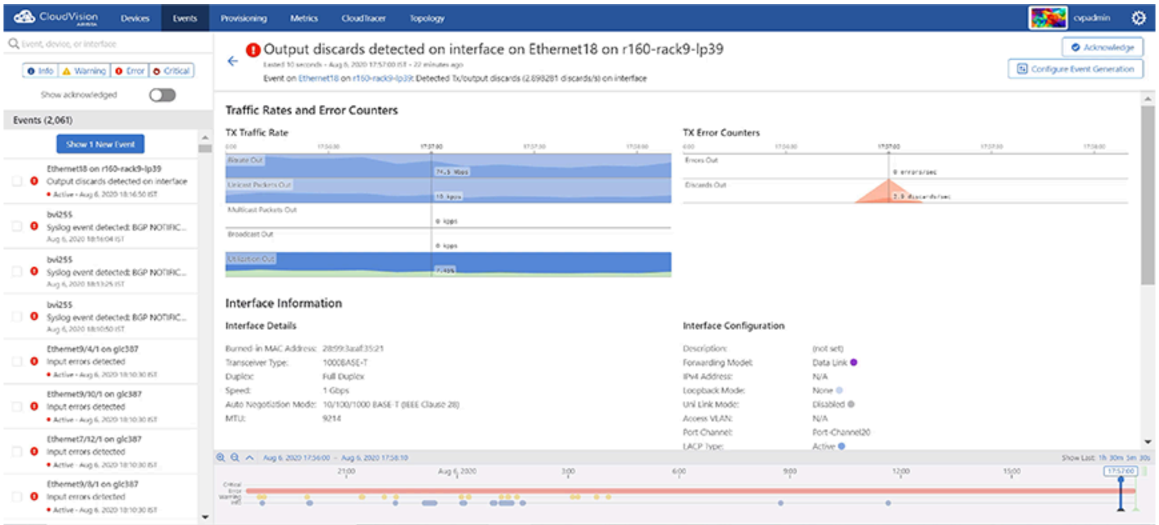
- Right Pane

  - The **Reset Filters** button to clear all filtering options.
  - The **Current Time** date picker to select the event start date.
  - Search field based on **Title or Description** and dropdown menus based on **Event Type**, **Device**, **Acknowlegement State**, and **Active State**.
  - Buttons to perform a search based on severity levels (**Info**, **Warning**, **Error**, and **Critical**)

7.17.2 Event Details Screen

An event details screen displays appropriate event details, acknowledges the event, and configures event generation. To view this screen, click one of the events listed on the **Events** screen.

Figure 7-78: Event Details Screen



Events (2,061)

- Ethernet18 on r160-rack9-lp39
  Output discards detected on interface
  Active - Aug 6, 2020 18:16:50 IST
- bvi255
  Syslog event detected: BGP NOTIFIC...
  Aug 6, 2020 18:16:04 IST
- bvi255
  Syslog event detected: BGP NOTIFIC...
  Aug 6, 2020 18:13:25 IST
- bvi255
  Syslog event detected: BGP NOTIFIC...
  Aug 6, 2020 18:10:50 IST
- Ethernet9/4/1 on glc387
  Input errors detected
  Active - Aug 6, 2020 18:10:30 IST
- Ethernet9/30/1 on glc387
  Input errors detected
  Active - Aug 6, 2020 18:10:30 IST
- Ethernet7/12/1 on glc387
  Input errors detected
  Active - Aug 6, 2020 18:10:30 IST
- Ethernet9/8/1 on glc387
  Input errors detected
  Active - Aug 6, 2020 18:10:30 IST

Output discards detected on interface on Ethernet18 on r160-rack9-lp39

Lasted 10 seconds - Aug 6, 2020 17:57:00 IST - 22 minutes ago

Event on Ethernet18 on r160-rack9-lp39: Detected Tx/output discards (2.898281 discards/s) on interface

Traffic Rates and Error Counters

TX Traffic Rate

TX Error Counters

Interface Information

Interface Details

Burned-in MAC Address:	28:99:3a:af:35:21
Transceiver Type:	1000BASE-T
Duplex:	Full Duplex
Speed:	1 Gbps
Auto Negotiation Mode:	10/100/1000 BASE-T (IEEE Clause 28)
MTU:	9214

Interface Configuration

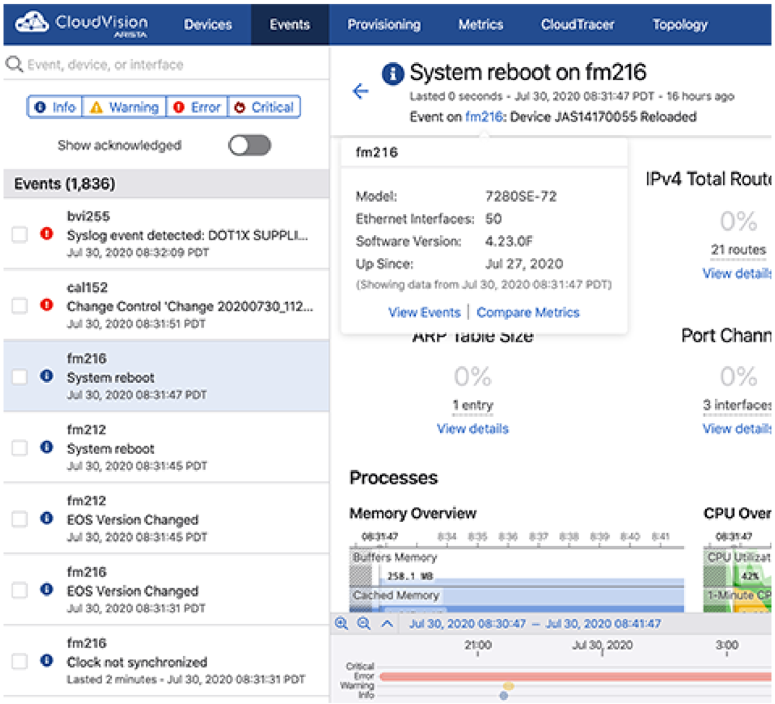
Description:	(not set)
Forwarding Model:	Data Link ●
IPv4 Address:	N/A
Loopback Mode:	None ●
Uni Link Mode:	Disabled ●
Access VLAN:	N/A
Port Channel:	Port-Channel20
LACP Type:	Active ●

This screen provides the following information and functionalities in the right pane:

- Left arrow to return to the events summary screen
- Click the **Event Generation** button to configure generating new events. Refer to Configuring Event Generations.
- Click the **Notifications** button to configure notifications. Refer to Configuring Notifications
- Displays the event description
- Time when event details were captured

- Hover the cursor on the event name. The system displays a popup window with event details.

Figure 7-79: Event Name Popup Window



Events (1,836)

bvi255
Syslog event detected: DOT1X SUPPLI...
Jul 30, 2020 08:32:09 PDT

cal152
Change Control 'Change 20200730_112...
Jul 30, 2020 08:31:51 PDT

fm216
System reboot
Jul 30, 2020 08:31:47 PDT

fm212
System reboot
Jul 30, 2020 08:31:45 PDT

fm212
EOS Version Changed
Jul 30, 2020 08:31:45 PDT

fm216
EOS Version Changed
Jul 30, 2020 08:31:31 PDT

fm216
Clock not synchronized
Lasted 2 minutes - Jul 30, 2020 08:31:31 PDT

System reboot on fm216
Lasted 0 seconds - Jul 30, 2020 08:31:47 PDT - 16 hours ago
Event on fm216: Device JAS14170055 Reloaded

fm216

Model: 7280SE-72
Ethernet Interfaces: 50
Software Version: 4.23.0F
Up Since: Jul 27, 2020
(Showing data from Jul 30, 2020 08:31:47 PDT)

View Events | Compare Metrics

IPv4 Total Route
0%
21 routes
View details

ARP Table Size
0%
1 entry
View details

Port Chann
0%
3 interfaces
View details

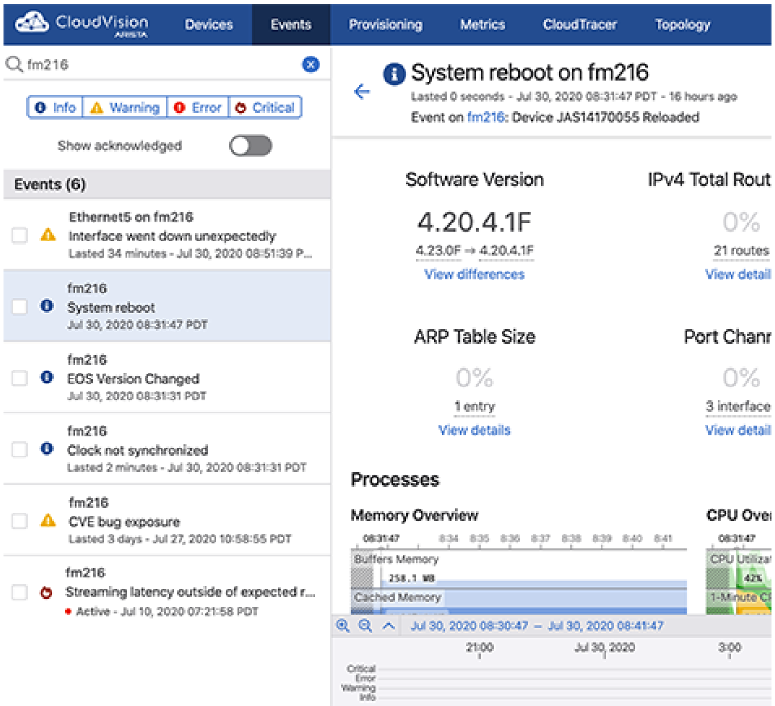
Processes

Memory Overview
CPU Over

The popup window provides the following options:

- Click **View Events** to view search results with the same event name.

Figure 7-80: Search Results with the Same Event Name



fm216

Events (6)

Ethernet5 on fm216
Interface went down unexpectedly
Lasted 34 minutes - Jul 30, 2020 08:51:39 P...

fm216
System reboot
Jul 30, 2020 08:31:47 PDT

fm216
EOS Version Changed
Jul 30, 2020 08:31:31 PDT

fm216
Clock not synchronized
Lasted 2 minutes - Jul 30, 2020 08:31:31 PDT

fm216
CVE bug exposure
Lasted 3 days - Jul 27, 2020 10:58:55 PDT

fm216
Streaming latency outside of expected r...
Active - Jul 10, 2020 07:21:58 PDT

System reboot on fm216
Lasted 0 seconds - Jul 30, 2020 08:31:47 PDT - 16 hours ago
Event on fm216: Device JAS14170055 Reloaded

Software Version
4.20.4.1F
4.23.0F → 4.20.4.1F
View differences

IPv4 Total Rout
0%
21 routes
View detail

ARP Table Size
0%
1 entry
View details

Port Chanr
0%
3 interface
View detail

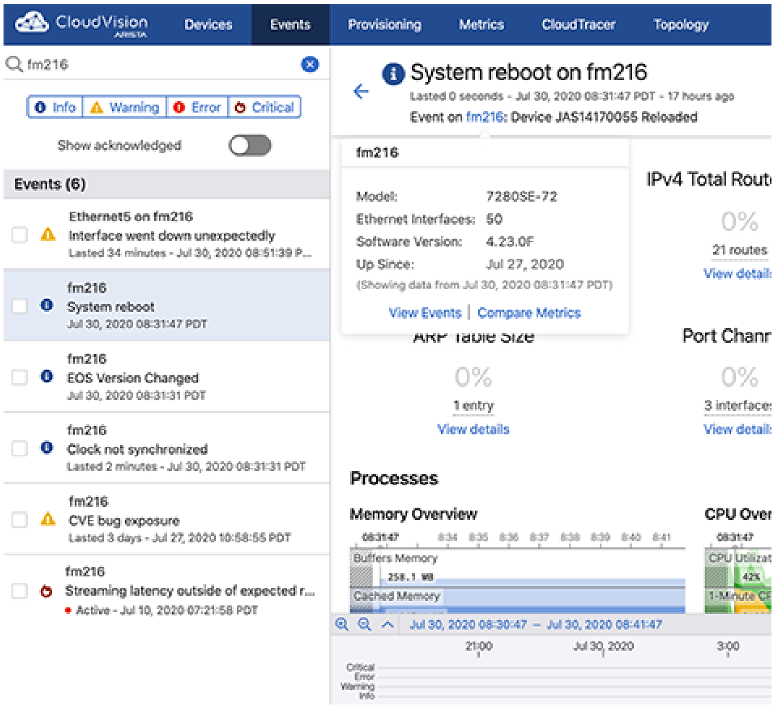
Processes

Memory Overview
CPU Over

- Click **Compare Metrics** to navigate to the **Explorer** tab in Metrics app.

- Hover the cursor on the event name. The system displays a popup window with device details in that location.

Figure 7-81: Location Name Popup Window



Events (6)

- Ethernet5 on fm216
Interface went down unexpectedly
Lasted 34 minutes - Jul 30, 2020 08:51:39 P...
- fm216
System reboot
Jul 30, 2020 08:31:47 PDT
- fm216
EOS Version Changed
Jul 30, 2020 08:31:31 PDT
- fm216
Clock not synchronized
Lasted 2 minutes - Jul 30, 2020 08:31:31 PDT
- fm216
CVE bug exposure
Lasted 3 days - Jul 27, 2020 10:58:55 PDT
- fm216
Streaming latency outside of expected r...
• Active - Jul 10, 2020 07:21:58 PDT

System reboot on fm216

Lasted 0 seconds - Jul 30, 2020 08:31:47 PDT - 17 hours ago

Event on fm216: Device JAS14170055 Reloaded

fm216

Model:	7280SE-72
Ethernet Interfaces:	50
Software Version:	4.23.0F
Up Since:	Jul 27, 2020

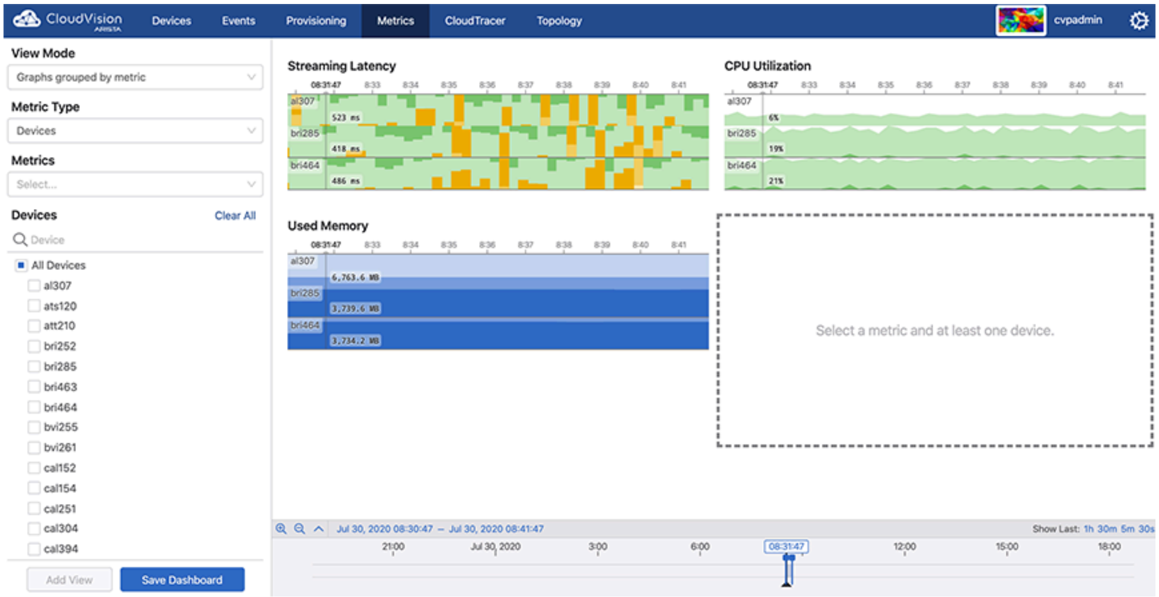
(Showing data from Jul 30, 2020 08:31:47 PDT)

View Events | Compare Metrics

The popup window provides the following options:

- Click **View Events** to view search results with the same location name.

Figure 7-82: Search Results with the Same Location Name



View Mode: Graphs grouped by metric

Metric Type: Devices

Metrics: Select...

Devices Clear All

Device

- ■ All Devices
- □ al307
- □ ats120
- □ att210
- □ bri252
- □ bri285
- □ bri463
- □ bri464
- □ bvi255
- □ bvi261
- □ cal152
- □ cal154
- □ cal251
- □ cal304
- □ cal394

Select a metric and at least one device.

- Click **Compare Metrics** to navigate to the **Explorer** tab under **Metrics**.
- The **Acknowledge** button to acknowledge the appropriate event.
- The **Configure Event Generation** button to configure the generation of appropriate event.
- Metric details of the event

- A chronological history of all errors (shown at the bottom of the screen)

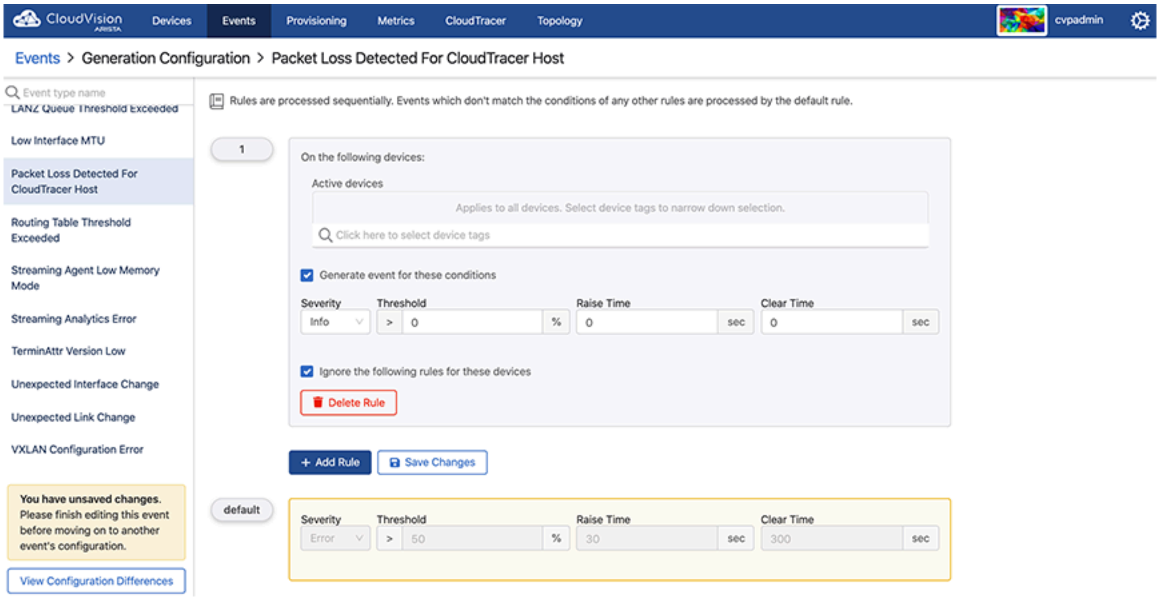
7.17.3 Configuring Event Generations

Configure rules and conditions to customize event generation.

Perform the following steps to configure the settings for generating events:

1. On the CloudVision portal, click the **Events** tab. The system displays the **Events** screen.
2. Click **Configure Event Generation** at the upper right corner of the **Events** section. The system displays the **Generation Configuration** screen with all configurable events listed in the left pane.

Figure 7-83: Generation Configuration Screen


CloudVision
ARISTA
Devices
Events
Provisioning
Metrics
CloudTracer
Topology
cvpadmin
Event type name
LANZ Queue Threshold Exceeded
Low Interface MTU
Packet Loss Detected For CloudTracer Host
Routing Table Threshold Exceeded
Streaming Agent Low Memory Mode
Streaming Analytics Error
TerminAttr Version Low
Unexpected Interface Change
Unexpected Link Change
VXLAN Configuration Error
View Configuration Differences
1
Delete Rule
+ Add Rule
Save Changes
default

Events > Generation Configuration > Packet Loss Detected For CloudTracer Host

Rules are processed sequentially. Events which don't match the conditions of any other rules are processed by the default rule.

You have unsaved changes. Please finish editing this event before moving on to another event's configuration.

On the following devices:

Active devices

Applies to all devices. Select device tags to narrow down selection.

Click here to select device tags

☑ Generate event for these conditions

Severity	Threshold	Raise Time	Clear Time
Info	> 0 %	0 sec	0 sec

☑ Ignore the following rules for these devices

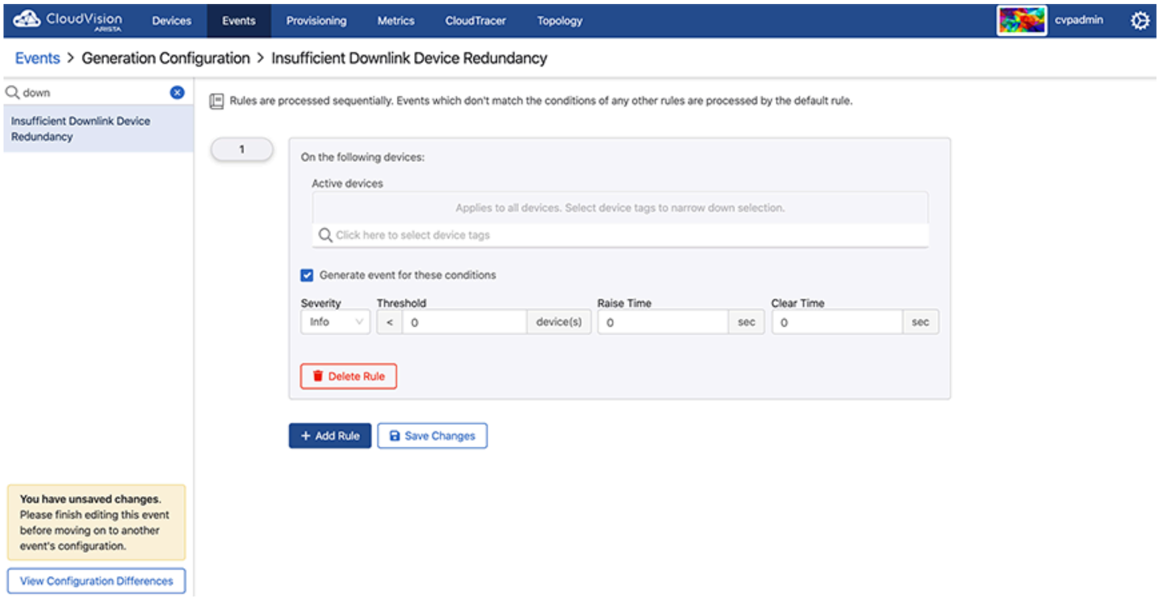
Severity	Threshold	Raise Time	Clear Time
Error	> 50 %	30 sec	300 sec

Note: Alternatively, you can go to an event details screen and click **Configure Event Generation** to configure rules for generating events.

3. Click the required event in the left pane.

4. Click **Add Rule** in the lower end of right pane. A new **Condition** pane is displayed on the screen.

Figure 7-84: Add Rule Pane in Generation Configuration


CloudVision
ARISTA
Devices
Events
Provisioning
Metrics
CloudTracer
Topology
cvpadmin
Events > Generation Configuration > Insufficient Downlink Device Redundancy
down
Insufficient Downlink Device Redundancy
1
On the following devices:
Active devices
Click here to select device tags
☑ Generate event for these conditions
Severity
Threshold
Raise Time
Clear Time
Delete Rule
+ Add Rule
Save Changes
View Configuration Differences

Rules are processed sequentially. Events which don't match the conditions of any other rules are processed by the default rule.

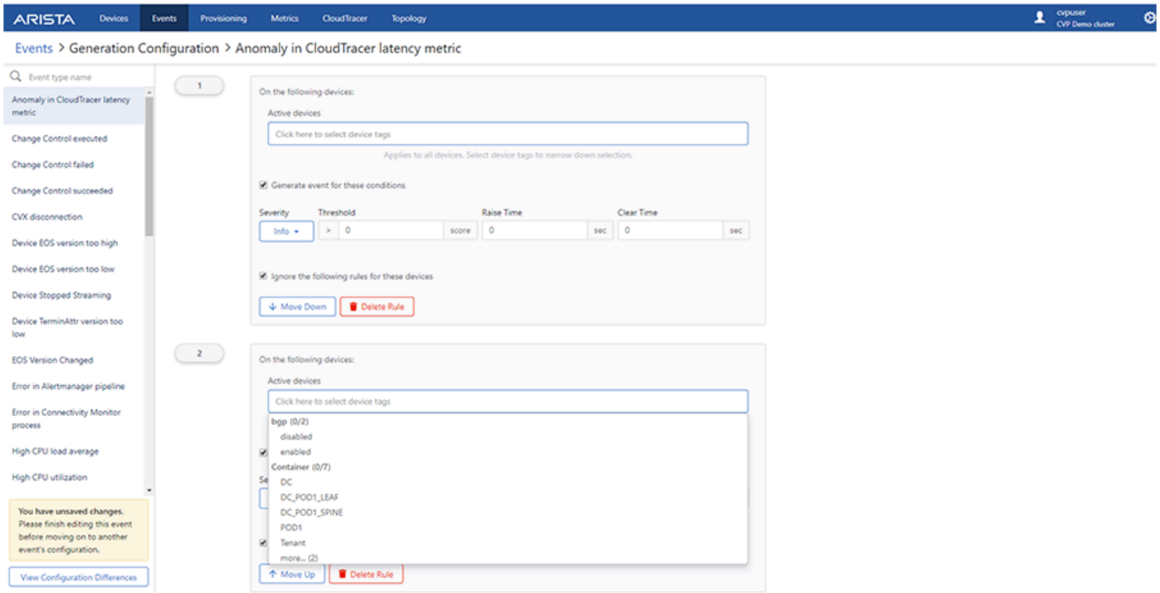
Applies to all devices. Select device tags to narrow down selection.

Severity: Info; Threshold: < 0 device(s); Raise Time: 0 sec; Clear Time: 0 sec

You have unsaved changes. Please finish editing this event before moving on to another event's configuration.

5. In the **Condition** pane, click on the search field. The system displays the list of configured devices tags.

Figure 7-85: List of Configured Device Tags


ARISTA
Devices
Events
Provisioning
Metrics
CloudTracer
Topology
cvpuser
CVP Demo cluster
Events > Generation Configuration > Anomaly in CloudTracer latency metric
Event type name
Anomaly in CloudTracer latency metric
Change Control executed
Change Control failed
Change Control succeeded
CVX disconnection
Device EOS version too high
Device EOS version too low
Device Stopped Streaming
Device TerminAttr version too low
EOS Version Changed
Error in Alertmanager pipeline
Error in Connectivity Monitor process
High CPU load average
High CPU utilization
1
On the following devices:
Active devices
Click here to select device tags
☑ Generate event for these conditions
Severity
Threshold
Raise Time
Clear Time
☑ Ignore the following rules for these devices
Move Down
Delete Rule
2
On the following devices:
Active devices
Click here to select device tags
bgp (0/2)
disabled
enabled
Container (0/7)
DC
DC_POD1_LEAF
DC_POD1_SPINE
POD1
Tenant
more... (2)
Move Up
Delete Rule
View Configuration Differences

Applies to all devices. Select device tags to narrow down selection.

Severity: Info; Threshold: > 0 score; Raise Time: 0 sec; Clear Time: 0 sec

You have unsaved changes. Please finish editing this event before moving on to another event's configuration.

Note: Alternatively, you can type the required device tag in the search field for a quick search.

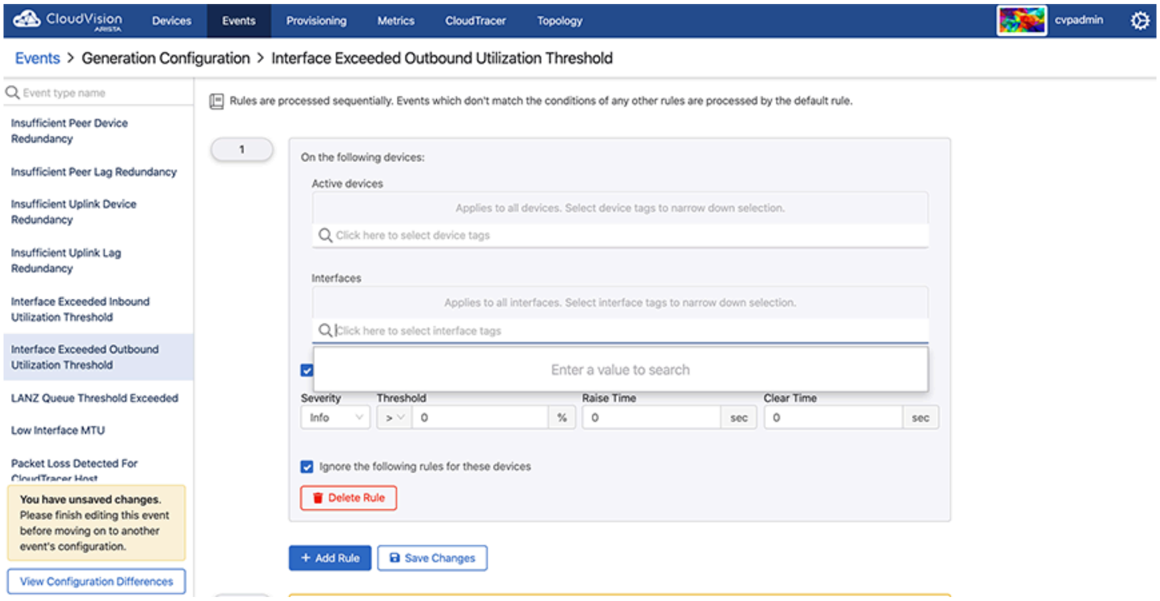
6. Select preferred devices tags from the displayed list.

Note: After you have selected the device, the system displays the count of matched devices. The rule is applicable to all devices when you do not select any device tag.

7. Click on the **Interfaces** search field (available only for interface events).

The system displays the list of configured interface tags..

Figure 7-86: List of Configured Interface Tags


CloudVision ARISTA
Devices
Events
Provisioning
Metrics
CloudTracer
Topology
cvpadmin
Event type name
Insufficient Peer Device Redundancy
Insufficient Peer Lag Redundancy
Insufficient Uplink Device Redundancy
Insufficient Uplink Lag Redundancy
Interface Exceeded Inbound Utilization Threshold
Interface Exceeded Outbound Utilization Threshold
LANZ Queue Threshold Exceeded
Low Interface MTU
Packet Loss Detected For CloudTracer Host
View Configuration Differences
1
Delete Rule
Add Rule
Save Changes

Events > Generation Configuration > Interface Exceeded Outbound Utilization Threshold

Rules are processed sequentially. Events which don't match the conditions of any other rules are processed by the default rule.

On the following devices:

Active devices

Applies to all devices. Select device tags to narrow down selection.

Click here to select device tags

Interfaces

Applies to all interfaces. Select interface tags to narrow down selection.

Click here to select interface tags

Enter a value to search

Severity: Info | Threshold: > 0 % | Raise Time: 0 sec | Clear Time: 0 sec

☑ Ignore the following rules for these devices

You have unsaved changes. Please finish editing this event before moving on to another event's configuration.

8. Select preferred interface tags from the displayed list.

   Note: After you have selected an interface tag, the system displays the count of matching interfaces. The rule is applicable to all interfaces when you do not select any interface tag.

9. Provide the following criteria required to generate events:

   - **Severity** - Select the severity type from the drop-down menu. Options include **Info**, **Warning**, **Critical**, and **Error**.
   - **Threshold** (applicable only to threshold events) **-** Type the threshold value.
   - **Raise Time -** Type the preferred wait time (seconds) to create an event after reaching the threshold limit.
   - **Clear Time -** Type the precise time (seconds) to delete an event after the current value goes below the threshold limit.

   Note: Select the **Stop generating events** and checking rules checkbox if you do not want to apply further rules for selected tags. If no tags are selected, further rules are not applicable to any device.

10. Click **Move up** if you prefer to move this rule up in the priority list.

    Note: Rules are processed sequentially. The default rule is applied only when an event does not match any other rules. Click **Delete** rule to delete the corresponding rule. Click **Move down** in configured rules to move the corresponding rule down in the priority list.

11. Click **Save** in the left pane.

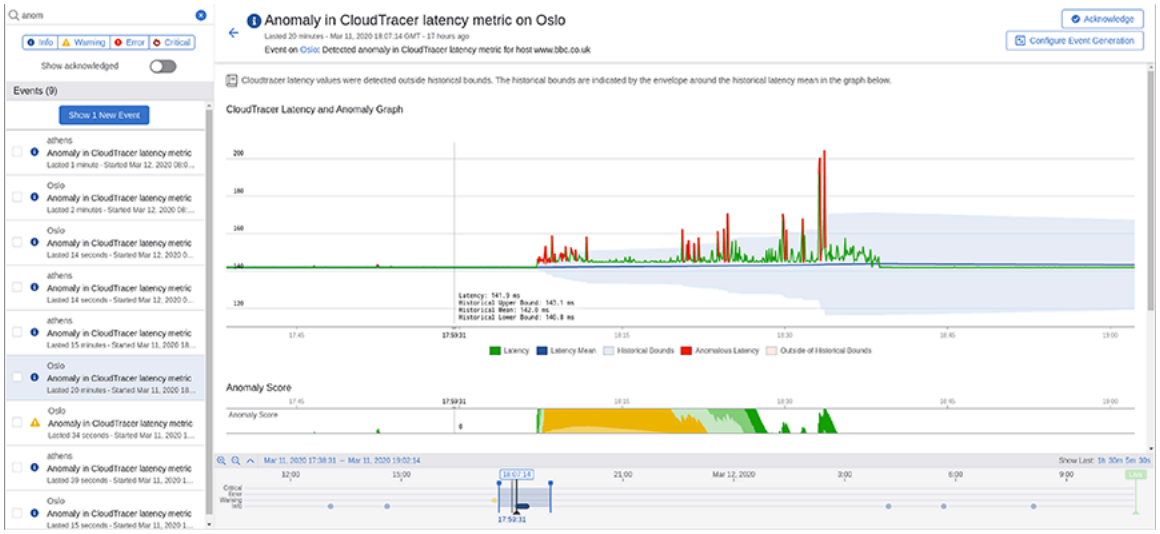
    Note: Click **View Configuration Differences** in the lower left pane to view differences in event configurations.

7.17.3.1 Anomaly in Connectivity Monitor Latency

From the Events tab, select Anomaly in Connectivity Monitor Latency to configure event generation for latency events between devices and configured hosts. The events are designed to alert the user when the latency between a device and a configured host is outside of recent historical bounds.

Figure 151: Anomaly Event View is a sample event view for one of these events between the device with hostname `Oslo` and the cloudtracer host endpoint `www.bbc.co.uk`.

Figure 7-87: Anomaly Event View



Anomaly in CloudTracer latency metric on Oslo

Lasted 20 minutes - Mar 11, 2020 18:07:14 GMT - 17 hours ago

Event on Oslo: Detected anomaly in CloudTracer latency metric for host www.bbc.co.uk

Cloudtracer latency values were detected outside historical bounds. The historical bounds are indicated by the envelope around the historical latency mean in the graph below.

CloudTracer Latency and Anomaly Graph

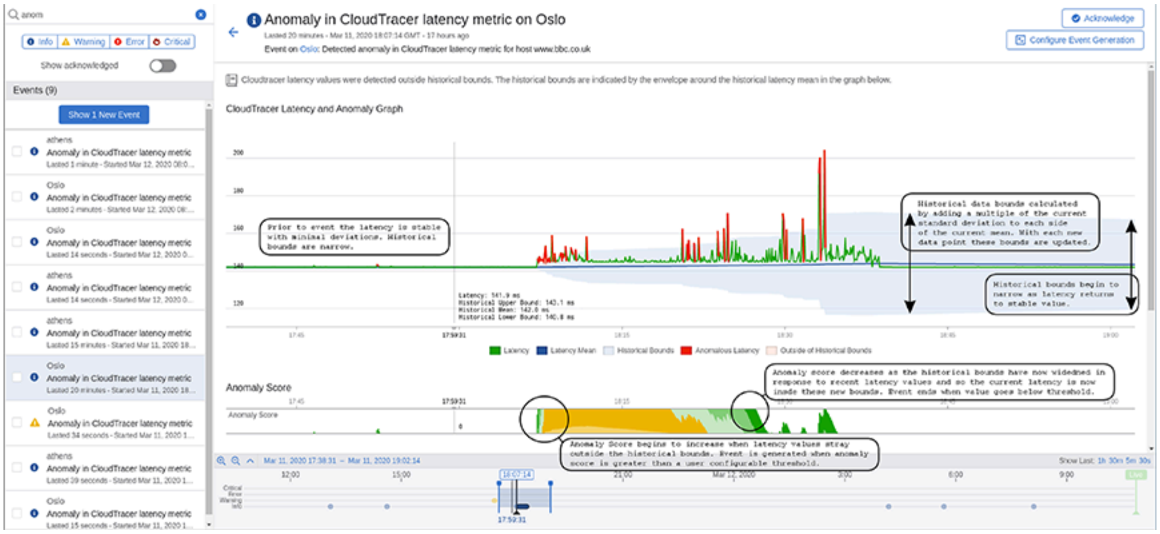
Latency: 141.9 ms
Historical Upper Bound: 143.1 ms
Historical Mean: 142.0 ms
Historical Lower Bound: 140.8 ms

Events (9)

- athens — Anomaly in CloudTracer latency metric — Lasted 1 minute - Started Mar 12, 2020 08:0...
- Oslo — Anomaly in CloudTracer latency metric — Lasted 2 minutes - Started Mar 12, 2020 08:...
- Oslo — Anomaly in CloudTracer latency metric — Lasted 14 seconds - Started Mar 12, 2020 0...
- athens — Anomaly in CloudTracer latency metric — Lasted 14 seconds - Started Mar 12, 2020 0...
- athens — Anomaly in CloudTracer latency metric — Lasted 15 minutes - Started Mar 11, 2020 18...
- Oslo — Anomaly in CloudTracer latency metric — Lasted 20 minutes - Started Mar 11, 2020 18...
- Oslo — Anomaly in CloudTracer latency metric — Lasted 34 seconds - Started Mar 11, 2020 1...
- athens — Anomaly in CloudTracer latency metric — Lasted 29 seconds - Started Mar 11, 2020 1...
- Oslo — Anomaly in CloudTracer latency metric — Lasted 15 seconds - Started Mar 11, 2020 1...

Figure 152: Anomaly Event View Overlay explains various stages of this event.

Figure 7-88: Anomaly Event View Overlay



Prior to event the latency is stable with minimal deviations. Historical bounds are narrow.

Historical data bounds calculated by adding a multiple of the current standard deviation to each side of the current mean. With each new data point these bounds are updated.

Historical bounds begin to narrow as latency returns to stable value.

Anomaly score decreases as the historical bounds have now widedned in response to recent latency values and so the current latency is now inside these new bounds. Event ends when value goes below threshold.

Anomaly Score begins to increase when latency values stray outside the historical bounds. Event is generated when anomaly score is greater than a user configurable threshold.

Anomaly in CloudTracer latency metric on Oslo

Lasted 20 minutes - Mar 11, 2020 18:07:14 GMT - 17 hours ago

Event on Oslo: Detected anomaly in CloudTracer latency metric for host www.bbc.co.uk

Cloudtracer latency values were detected outside historical bounds. The historical bounds are indicated by the envelope around the historical latency mean in the graph below.

CloudTracer Latency and Anomaly Graph

Latency: 141.9 ms
Historical Upper Bound: 143.1 ms
Historical Mean: 142.0 ms
Historical Lower Bound: 140.8 ms

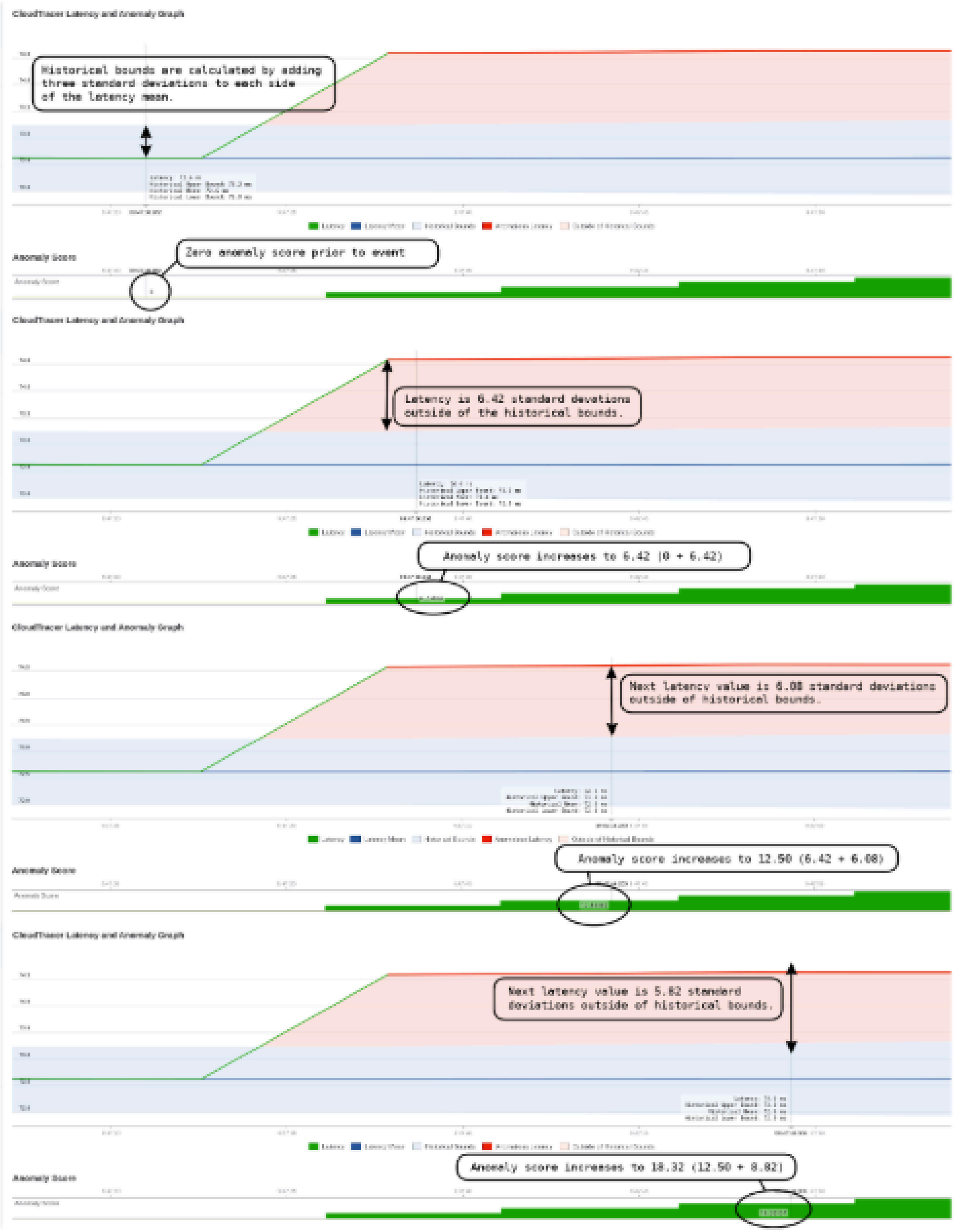
Prior to this event in Figure 152: Anomaly Event View Overlay, the latency metric (green line in upper graph) is stable with minimal deviations. The historical bounds (blue shaded region) that determine when the metric is in a normal state has a small range with both the upper and lower bounds near the historical mean (dark blue line). The historical bounds are computed by adding and subtracting a fixed multiple of the current latency standard deviation to the current mean.

The anomaly score starts to increase from zero when the latency value strays outside of the historical bounds. The latency values that are outside the bounds are highlighted in red. The anomaly score is the total number of standard deviations outside the historical bounds. The anomaly score is the positive cumulative sum of the number of standard deviations outside of the historical bounds. For example, if the bounds are set as 3 standard deviations outside of the mean and we get a value of the latency that is 5 times the standard deviation away from the mean, the anomaly score will increase by 2. If the next latency value was 1.5 times the standard deviation outside of then mean then we would subtract 1.5 from the anomaly score.

The anomaly score therefore keeps track of the cumulative deviation of the latency outside of the historical bounds. It is bounded below by zero.

Figure 153: Anomaly Score Computation provides a detailed explanation on computing the anomaly score.

Figure 7-89: Anomaly Score Computation



CloudTracer Latency and Anomaly Graph
Historical bounds are calculated by adding three standard deviations to each side of the latency mean.
Anomaly Score
Zero anomaly score prior to event
CloudTracer Latency and Anomaly Graph
Latency is 6.42 standard devations outside of the historical bounds.
Anomaly Score
Anomaly score increases to 6.42 (0 + 6.42)
CloudTracer Latency and Anomaly Graph
Next latency value is 6.08 standard deviations outside of historical bounds.
Anomaly Score
Anomaly score increases to 12.50 (6.42 + 6.08)
CloudTracer Latency and Anomaly Graph
Next latency value is 5.82 standard deviations outside of historical bounds.
Anomaly Score
Anomaly score increases to 18.32 (12.50 + 5.82)

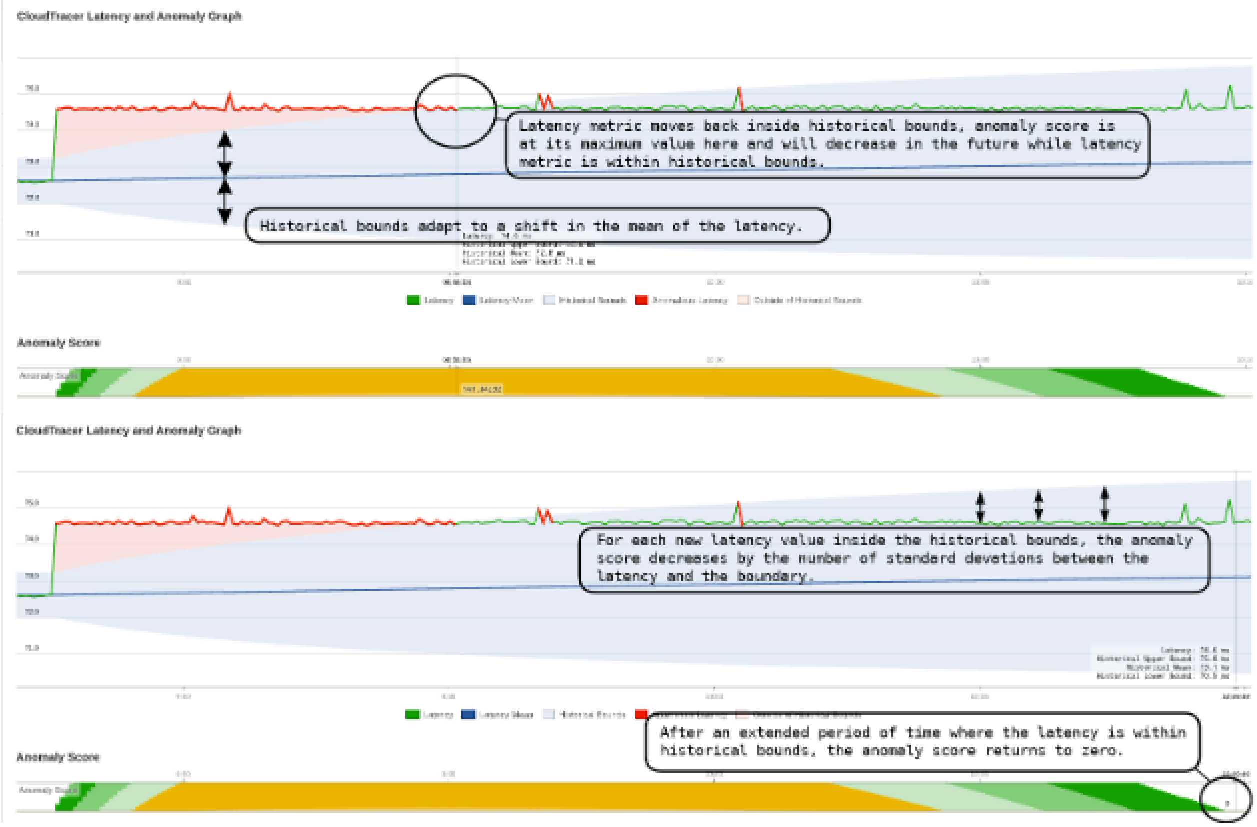
The event is generated when the anomaly score exceeds a threshold for a set period of time.

Note: You can configure the threshold and time duration in the event configuration rules.

The anomaly score starts to decrease when the latency values are inside the historical bounds. The historical bounds have increased based on recent deviations in latency which makes the system less sensitive than prior to the event. The event ends when the anomaly score is below the threshold for a set period of time.

Figure 154: Decreasing of Anomaly Score provides a detailed explanation of the anomaly score decreasing when an event ends.

Figure 7-90: Decreasing of Anomaly Score



Latency metric moves back inside historical bounds, anomaly score is at its maximum value here and will decrease in the future while latency metric is within historical bounds.

Historical bounds adapt to a shift in the mean of the latency.

For each new latency value inside the historical bounds, the anomaly score decreases by the number of standard devations between the latency and the boundary.

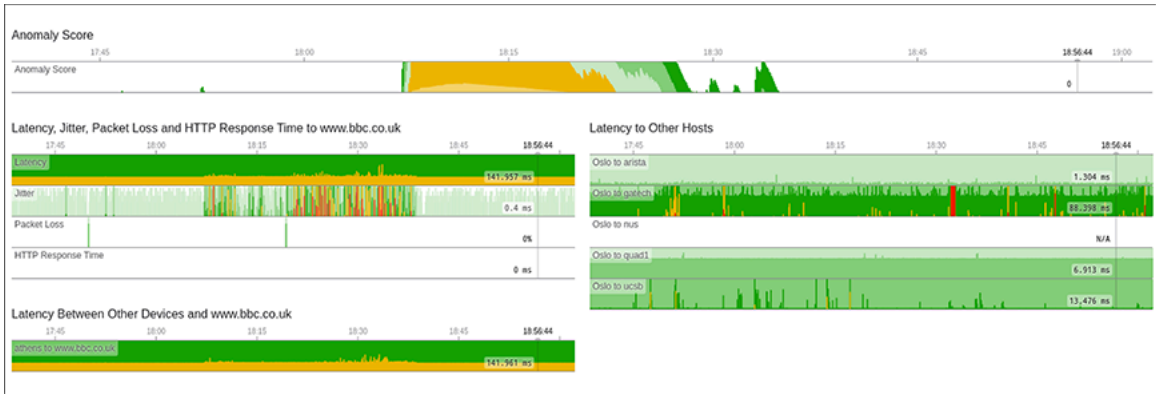
After an extended period of time where the latency is within historical bounds, the anomaly score returns to zero.

At the end of the time range, historical bounds are narrowing as the latency has now returned to a stable value with minimum deviations. The history needs approximately six hours to have negligible impact on the statistics and bounds.

This screen also provides the following additional metrics of this event (see Figure 155: CloudTracer Event Additional View):

- The other CloudTracer metrics are displayed for this device and host pair
- The latency metric between other devices and this host
- The latency metric between this device and other hosts

Figure 7-91: CloudTracer Event Additional View



7.17.4 Custom Syslog Events

The **Custom Syslog Event** creates syslog message events based on rule conditions. To end all similar active events, you must update the configuration as per the recommended action provided in the EOS System Message Guide.

An EOS System Message Guide is published with every EOS release. In the guide, you can find all the common system messages generated by devices, including the syslog facility, mnemonic, severity, and log message format. To download the guide, click https://www.arista.com/en/support/software-download and look for SysMsgGuide under EOS release Docs.

Note: Rules are processed sequentially. Events that don't match user created rule conditions are processed by default rule(s).

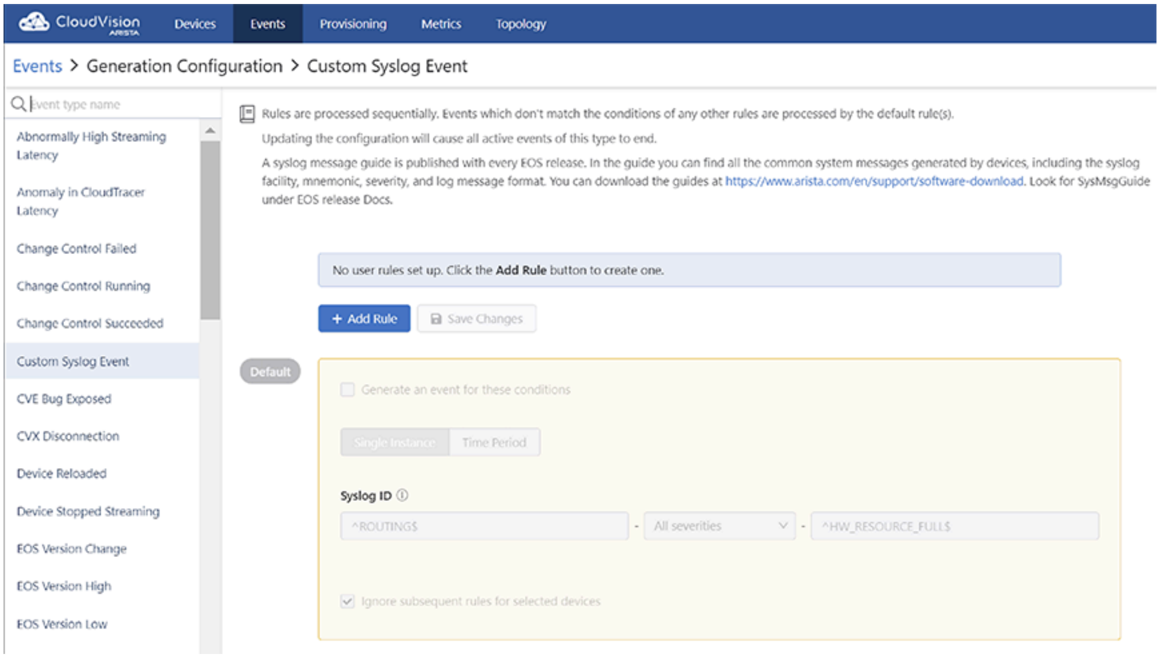
Perform the following steps to create a rule for generating syslog events:

1. On the CloudVision portal, click the **Events** tab. The system displays the Events screen.
2. Click **Configure Event Generation** at the upper right corner of the **Events** section.

   Note: Alternatively, you can go to an event details screen and click **Configure Event Generation** to configure rules for generating events.

   The system displays the Generation Configuration screen with all configurable event types listed in the left pane.
3. Click **Custom Syslog Event**.

   Figure 7-92: Custom Syslog Event Screen



Rules are processed sequentially. Events which don't match the conditions of any other rules are processed by the default rule(s).

Updating the configuration will cause all active events of this type to end.

A syslog message guide is published with every EOS release. In the guide you can find all the common system messages generated by devices, including the syslog facility, mnemonic, severity, and log message format. You can download the guides at https://www.arista.com/en/support/software-download. Look for SysMsgGuide under EOS release Docs.

No user rules set up. Click the **Add Rule** button to create one.

☐ Generate an event for these conditions

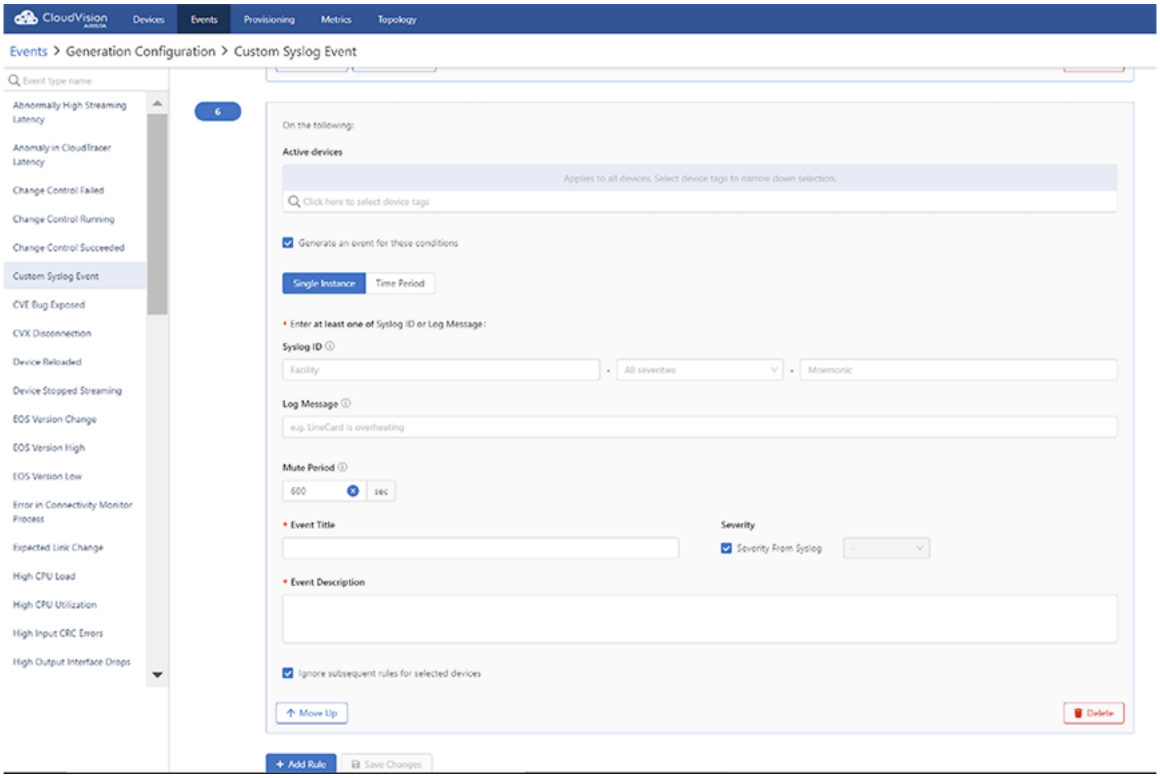
Syslog ID: ^ROUTING$ - All severities - ^HW_RESOURCE_FULL$

☑ Ignore subsequent rules for selected devices

4. Click **+Add Rule** in the right pane.

A new condition pane is displayed on the screen.

Figure 7-93: Conditions Pane for the Custom Syslog Event Rule



On the following:

Active devices

Applies to all devices. Select device tags to narrow down selection.

Click here to select device tags

☑ Generate an event for these conditions

Single Instance | Time Period

* Enter at least one of Syslog ID or Log Message:

Syslog ID ⓘ

Facility · All severities · Mnemonic

Log Message ⓘ

e.g. LineCard is overheating

Mute Period ⓘ

600 sec

* Event Title

Severity

☑ Severity From Syslog -

* Event Description

☑ Ignore subsequent rules for selected devices

5. Provide the following information in specified fields:
   - **Active devices** autocomplete field -
   - **Generate an event for these conditions** checkbox -
6. Choose either **Single Instance Events** or **Time Period Events** using the toggle button.
7. Based on your choice between single instance events and time period events, provide the following relevant conditions for generating a rule:
   - Configuring Single Instance Events
   - Configuring Time Period Events

   Note: The corresponding fields appear after you choose the required event type.
8. **Save Changes** button - Click to save specified changes.

7.17.4.1 Configuring Single Instance Events

CVP creates a single instance event whenever either the specified syslog ID matches with the device syslog ID or the specified syslog message matches with the device syslog message. See Figure 157: Conditions Pane for the Custom Syslog Event Rule.

Provide the following information in specified fields to configure a single instance event:

- **Syslog ID** - Provide facility, severity, and mnemonic of a syslog with regular expressions in the following fields:
  - **Facility** field - Type the facility of syslog in either simple string or regular expression.
  - **All severities** field - Select the severity of the device.

    Note: If no severity is selected, CVP considers all available severities.

    - **Mnemonic** field - CVP creates a single instance event when the log message specified in this field matches with a device syslog message.
- **Log Message** field - The log message to match against the device syslog message.

  Note: You must mandatorily configure either a syslog ID or a log message.

- **Mute Period** field - CVP does not create another similar event using this rule on a given device until the time period specified in this field expires for the ongoing event.

  Note: This prevents a large number of events generated for the same device within a short period of time due to a repetitive syslog message.

- **Event Title** field - Type the event title.
- **Severity From Syslog** checkbox - Select the checkbox if you prefer CVP to select the severity of the generated event to be derived from the syslog message severity.

  Note: CVP uses the following syslog message severities to event severities:

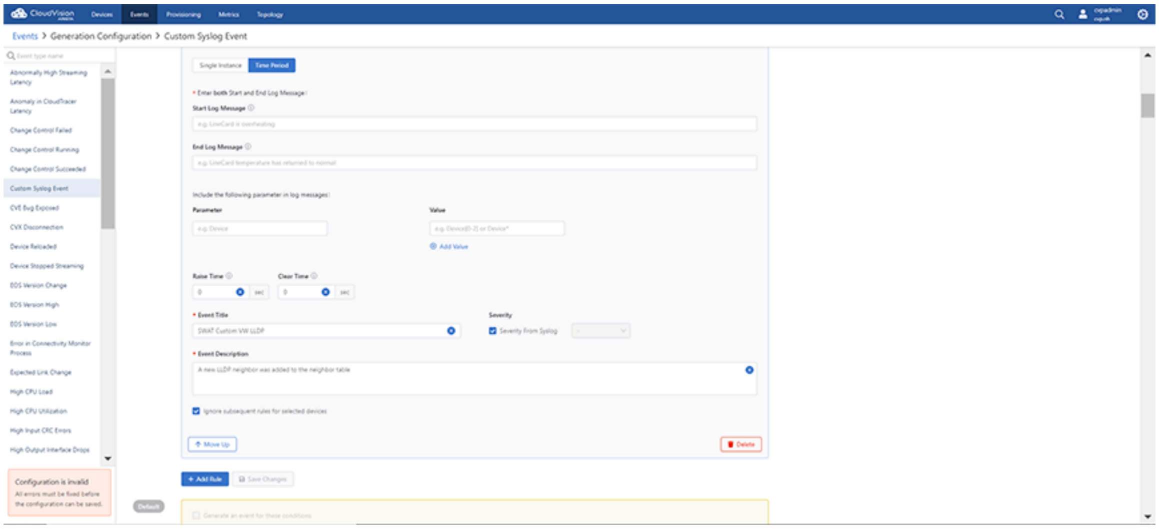
  - [0, 1, 2] - Critical event
  - [3] - Error event
  - [4] - Warning event
  - [5,6,7,...] - Info event
- **Severity** dropdown menu - Select the preferred severity of the generated event. Severity is configurable only when **Severity From Syslog** checkbox is not selected.
- **Event Description** field - Provide the event description.
- **Ignore subsequent rules for selected devices** checkbox - Select the checkbox to suppress generating events for a specific syslog or override upcoming configurations.
- **Move Up** / **Move Down** buttons - Use this button to manage the sequence of configured syslog event rules.
- **Delete** button - Click to delete the corresponding rule.

Note: Syslogs with high severities like 0 (Emergency), 1 (Alert), 2 (Critical), and 3 (Error) generate events by default unless they are ignored by user configured rules.

7.17.4.2 Configuring Time Period Events

Events can also be configured to be time period events that remain active between the syslog message that creates it and the syslog message that ends the event. See the figure below.

Figure 7-94: Configuring Time Period Event



Events > Generation Configuration > Custom Syslog Event

Event Title: SWAT Custom VW LLDP

Severity: ☑ Severity From Syslog

Event Description: A new LLDP neighbor was added to the neighbor table

☑ Ignore subsequent rules for selected devices

Configuration is invalid
All errors must be fixed before the configuration can be saved.

Provide the following information in specified fields to configure a time period event:

- **Start Log Message** field - CVP starts a time period event when the start log message specified in this field matches with a device syslog message.

  Note: The start log message must be a string without special characters.

- **End Log Message** field - CVP ends a time period event when the end log message specified in this field matches with a device syslog message.

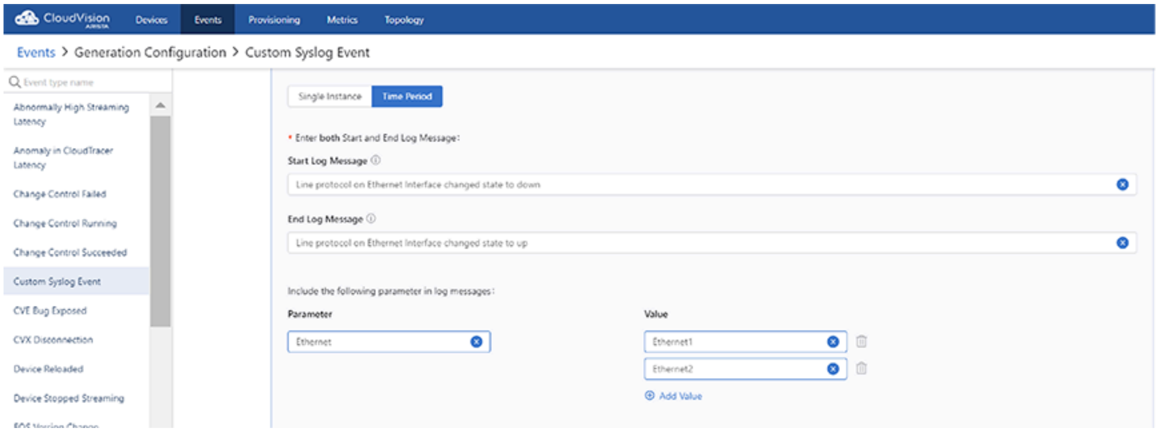
  Note: The end log message must be a string without special characters.

- **Parameter** field - Type the variable that must be configured in log messages specified in the **Start Log Message** and **End Log Message** fields.
  - **Value** field - Type a variable for the specified parameter in either a simple string or a regular expression.
  - **Add Value** - Click to add another variable for the specified parameter.

Ethernet is a parameter with values as *Ethernet1* and *Ethernet2*. See the figure below.

In this case, the specified log messages matches with Ethernet1 and Ethernet2 values for either starting or ending an event.

Figure 7-95: Example1 of Parameter Variables



* Enter both Start and End Log Message:

Start Log Message: Line protocol on Ethernet Interface changed state to down

End Log Message: Line protocol on Ethernet Interface changed state to up

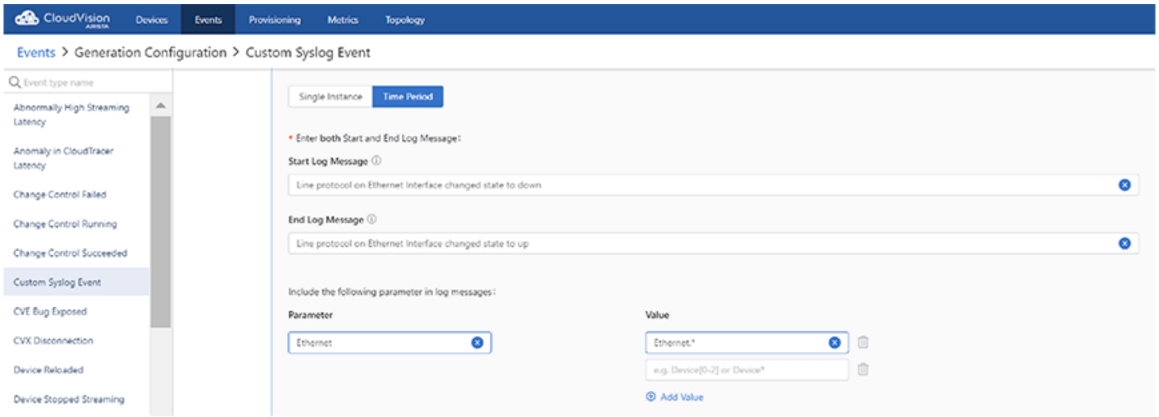
Include the following parameter in log messages:

Parameter	Value
Ethernet	Ethernet1
	Ethernet2

Ethernet is a parameter with a value as *Ethernet.**. See the figure below.

In this case, the specified log messages matches with all ethernet values like Ethernet1, Ethernet1/2, Ethernet1/3, and so on for either starting or ending an event.

Figure 7-96: Example2 of Parameter Variables



* Enter both Start and End Log Message:

Start Log Message: Line protocol on Ethernet Interface changed state to down

End Log Message: Line protocol on Ethernet Interface changed state to up

Include the following parameter in log messages:

Parameter	Value
Ethernet	Ethernet.*
	e.g. Device[0-2] or Device*

- **Raise Time** field - After a start rule matches, the starting of an event is delayed for the duration specified in this field.

  Note: If the end event log message arrives before this delay elapses, the event is not generated. This option is useful in situations where you wish to generate an event only when a syslog condition has persisted for at least some set period of time.
- **Clear Time** field - After an end rule matches, the ending of the ongoing event is delayed for the duration specified in this field.

  Note: If the start event log message arrives before this delay elapses, the event is not ended and will continue as an active event. This option is useful in situations where you wish to generate a long single event which may encompass several start/end conditions being met during a set period of time.
- **Event Title** field - Type the event title.
- **Severity From Syslog** checkbox - Select the checkbox if you prefer CVP to select the severity of the generated event to be derived from the syslog message severity.

  Note: CVP uses the following syslog message severities to event severities:

  - [0, 1, 2] - Critical event
  - [3] - Error event
  - [4] - Warning event
  - [5,6,7,...] - Info event
- **Severity** dropdown menu - Select the preferred severity of the generated event. Severity is configurable only when **Severity From Syslog** checkbox is not selected.
- **Event Description** field - Provide the event description.
- **Ignore subsequent rules for selected devices** checkbox - Select the checkbox to suppress generating events for a specific syslog or override upcoming configurations.
- **Move Up** / **Move Down** buttons - Use this button to manage the sequence of configured syslog event rules.
- **Delete** button - Click to delete the corresponding rule.

Note: A configuration change in the current rule ends all ongoing events.

7.17.4.3 Rule Labels

Rule Labels are optional conditions in Event Notifications for sending notifications to receiver platforms. Using rule labels allows you to create more complex notification rules in relation to generated events. An event can be generated with a rule label, which is configured and created in Event Generation. That label can be added as a condition to a rule in Event Notifications for sending an alert to a platform receiver.

Related Topics:

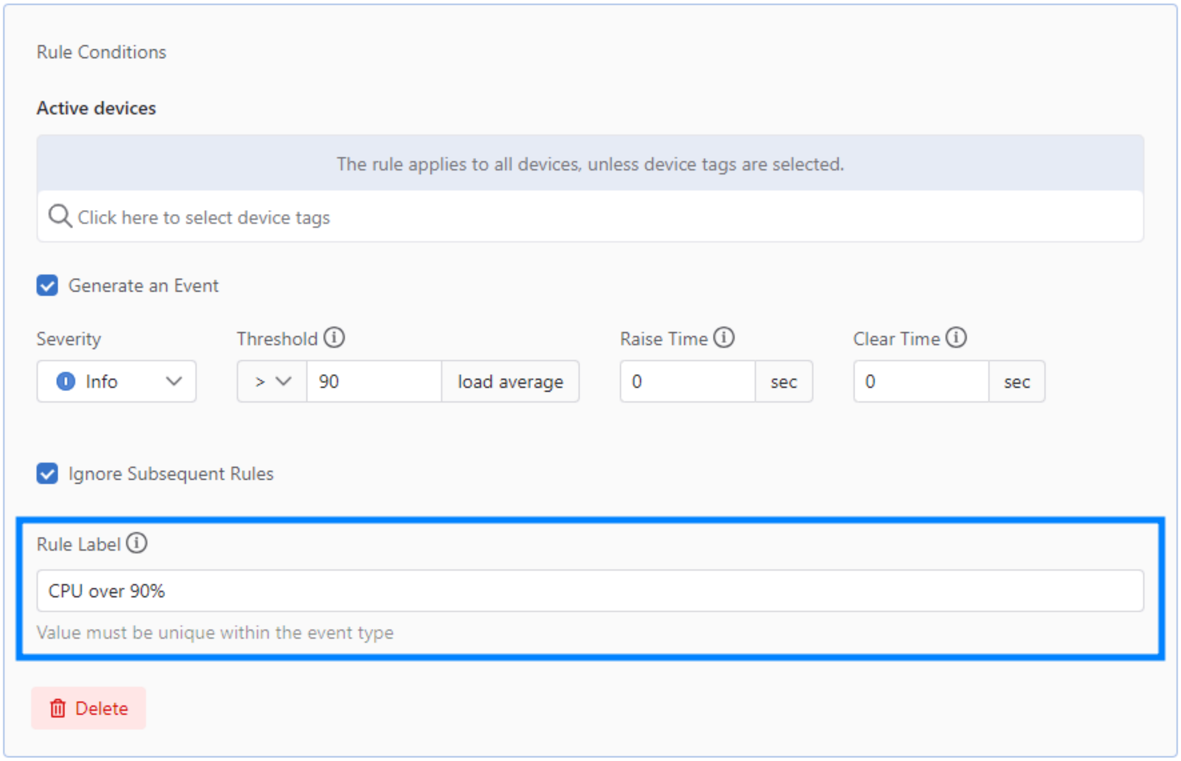
- Creating a Rule Label
- Assigning a Rule Label
- Platform Settings Overrides
- Compliance Events

7.17.4.3.1 Creating a Rule Label

A rule label is created in Event Generation, which creates events in CloudVision. The label can be assigned as a condition in a rule for Event Notifications.

1. Add or select a rule in Event Generation.

Figure 7-97: Add Rule Label



Rule Conditions

Active devices

The rule applies to all devices, unless device tags are selected.

Click here to select device tags

☑ Generate an Event

Severity: Info

Threshold: > 90 load average

Raise Time: 0 sec

Clear Time: 0 sec

☑ Ignore Subsequent Rules

Rule Label: CPU over 90%

Value must be unique within the event type

2. Add a rule label in the Rule Label field.

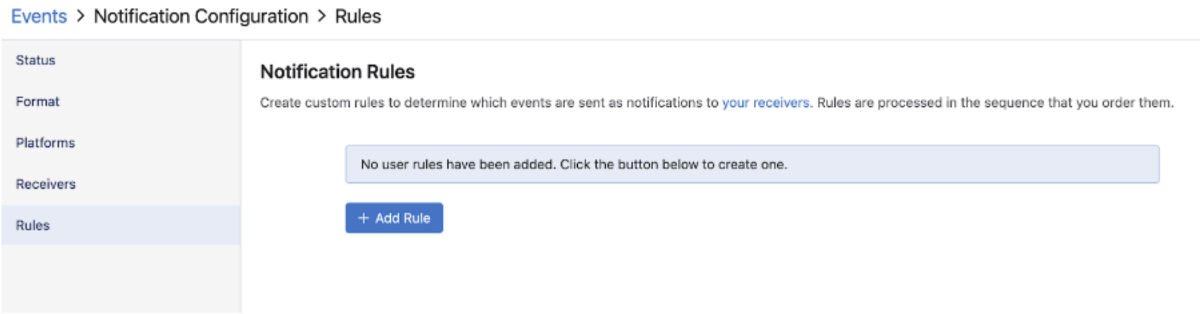
7.17.4.3.2 Assigning a Rule Label

You can assign rule labels that have been created in Event Generation to rules in Notifications. When an event is generated with a rule label, notifications will only be sent if the rule label matches the event generated rule label.

The notification rule will only generate an event that has a rule with a label that matches the selected rule label.

1. Add or select a rule in Event Notifications.

Figure 7-98: Assigning a Rule Label



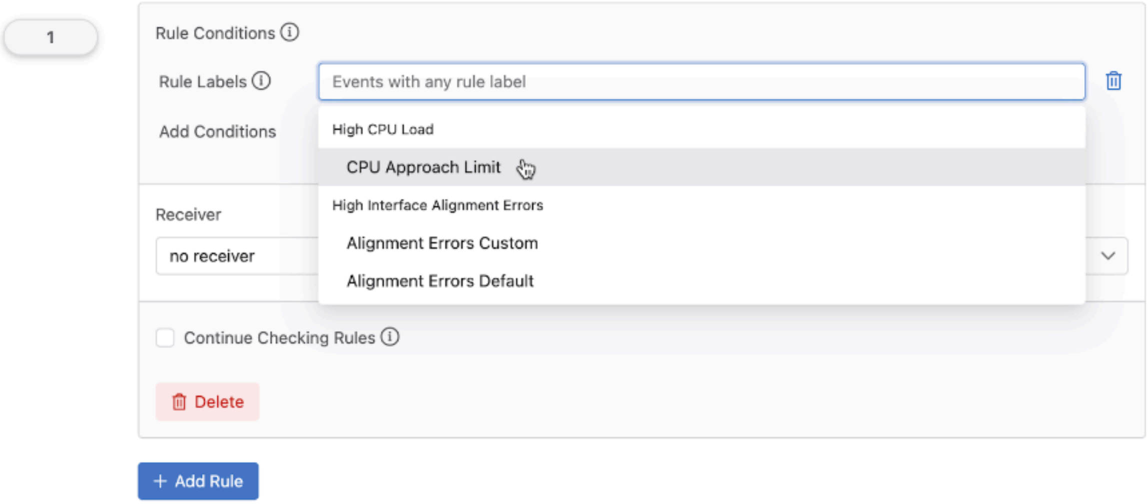
Notification Rules

Create custom rules to determine which events are sent as notifications to your receivers. Rules are processed in the sequence that you order them.

No user rules have been added. Click the button below to create one.

2. Click **Rule Labels** and select one or more existing rule label.

Figure 7-99: Notification Rues



1

Rule Conditions ⓘ

Rule Labels ⓘ Events with any rule label

Add Conditions

High CPU Load

CPU Approach Limit

High Interface Alignment Errors

Alignment Errors Custom

Alignment Errors Default

Receiver

no receiver

□ Continue Checking Rules ⓘ

Delete

+ Add Rule

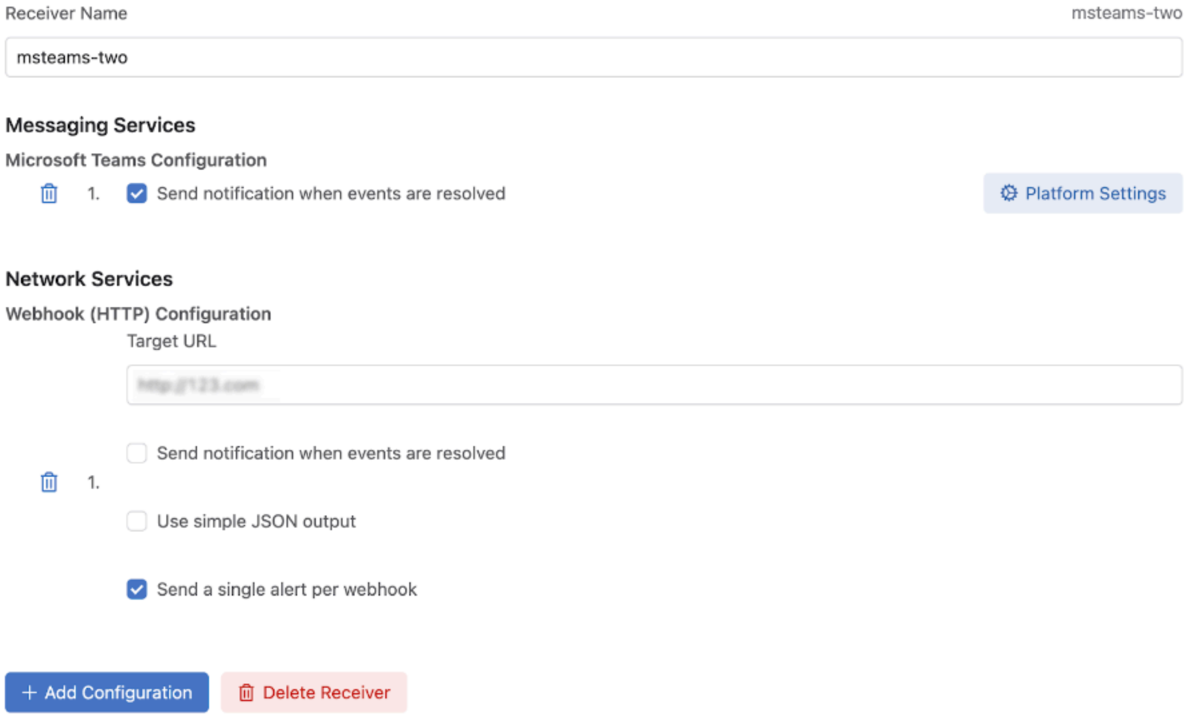
7.17.4.3.3 Platform Settings Overrides

When adding a receiver in Event Notifications, you can override existing platform settings in Platforms. This allows you to add default platform settings in Platforms and then use different settings when creating a receiver. You can have multiple settings for the same platform on a per-receiver basis.

Upon completion for the following steps, the receiver will use the override settings instead of the default settings created in Platforms.

1. Add or select an existing receiver.

Figure 7-100: Add or Select an Existing Receiver



Receiver Name msteams-two

msteams-two

Messaging Services

Microsoft Teams Configuration

1. ☑ Send notification when events are resolved

⚙ Platform Settings

Network Services

Webhook (HTTP) Configuration

Target URL

[redacted]

1.

□ Send notification when events are resolved

□ Use simple JSON output

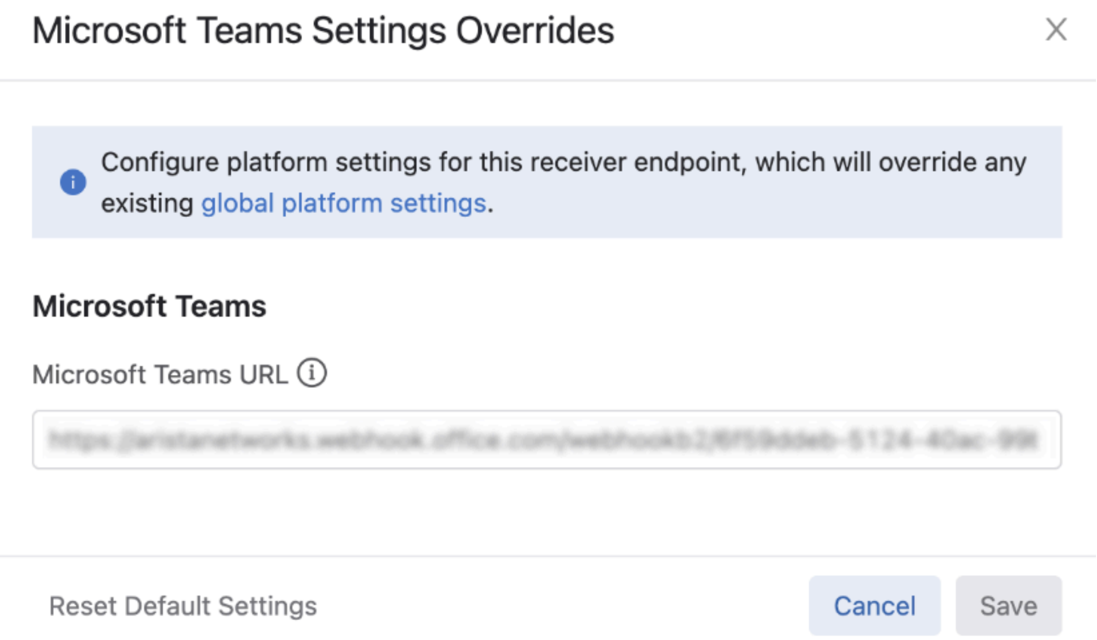
☑ Send a single alert per webhook

+ Add Configuration

Delete Receiver

2. Click **Platform Settings.**
3. Enter custom settings for the selected platform.

Figure 7-101: Custom Settings for Selected Platform



Microsoft Teams Settings Overrides

Configure platform settings for this receiver endpoint, which will override any existing global platform settings.

Microsoft Teams

Microsoft Teams URL

4. Click **Save**.

7.17.4.3.4 Compliance Events

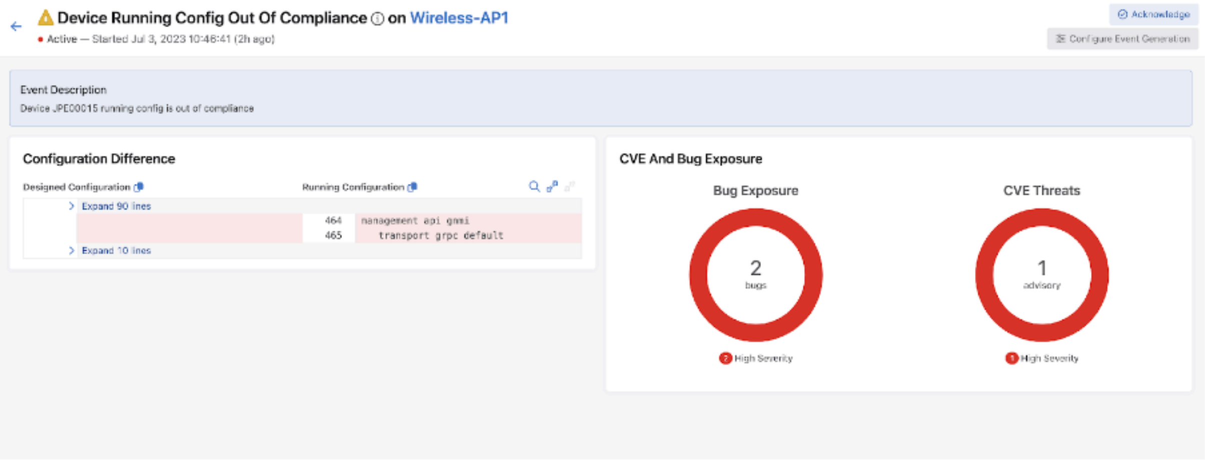
Events will be generated when a provisioned device's running configuration or image is out of sync with the designed configuration or image on CloudVision via the system's continuous compliance checker. This can occur when configuration or an image is pushed to a device outside of CloudVision, which prevents CloudVision from being the source of truth for device configuration.

Alerts will continue to be shown in Inventory, Compliance Overview, and Network Provisioning when a device is non-compliant.

Device Running Config Out of Compliance

A Device Running Config Out Of Compliance event is generated when CloudVision detects that a device's running config is out of sync with its designed config on CloudVision. The event layout will show the running and designed configuration, along with related information about the compliance of the device, including the bug/security advisory exposure of the device.

Figure 7-102: Device Running Config Out of Compliance



Device Running Config Out Of Compliance on Wireless-AP1

● Active — Started Jul 3, 2023 10:46:41 (2h ago)

Event Description

Device JPE00015 running config is out of compliance

Configuration Difference

```
Designed Configuration          Running Configuration
  > Expand 90 ines
                                464  management api gnmi
                                465     transport grpc default
  > Expand 10 ines
```

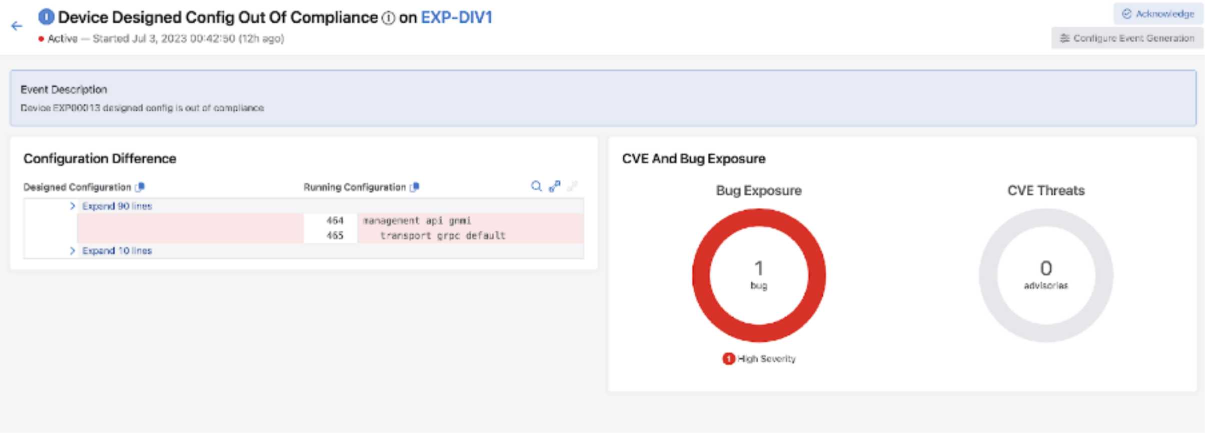
CVE And Bug Exposure

The event has a Warning severity.

Device Designed Config Out of Compliance

A Device Designed Config Out of Compliance event is generated when the designed configuration for a device is out of sync with a device's running configuration. This occurs when configuration created on CloudVision has not been pushed to a device.

Figure 7-103: Device Designed Config Out of Compliance



Device Designed Config Out Of Compliance on EXP-DIV1

● Active — Started Jul 3, 2023 00:42:50 (12h ago)

Event Description

Device EXP00013 designed config is out of compliance

Configuration Difference

```
Designed Configuration          Running Configuration
  > Expand 90 lines
                                464  management api gnmi
                                465     transport grpc default
  > Expand 10 lines
```

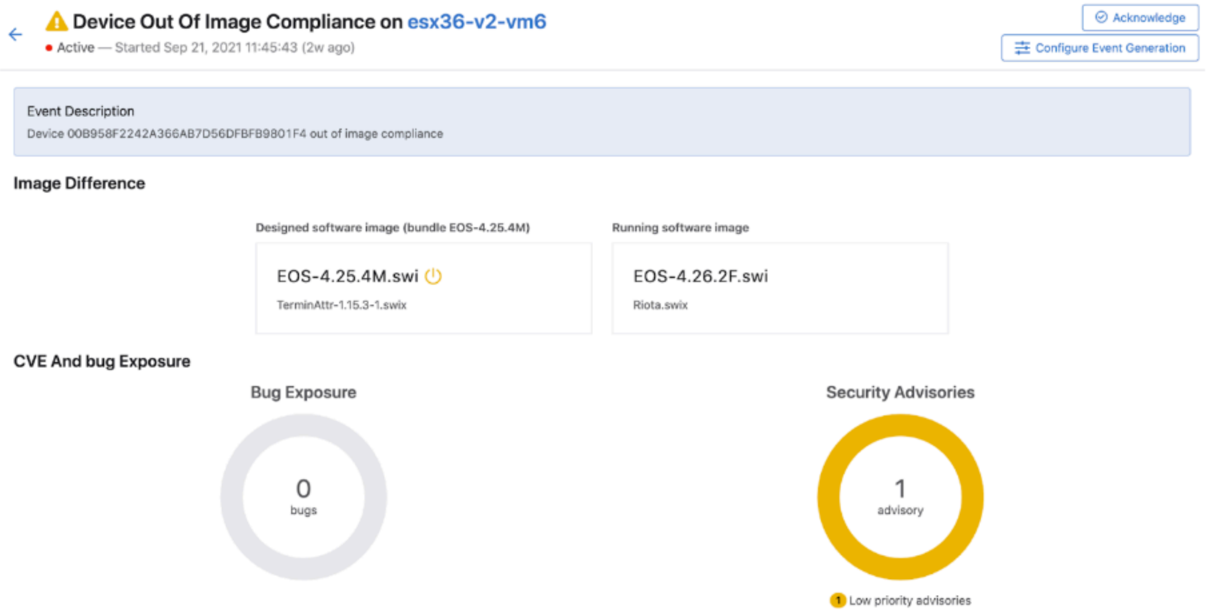
CVE And Bug Exposure

The event has an Info severity.

Device Image Compliance

A Device Image Compliance event is generated when a device's designed and running image are out of sync. You will need to upgrade the correct image for the device on CloudVision and, if required, push the image to the device.

Figure 7-104: Device Image Compliance



Device Out Of Image Compliance on esx36-v2-vm6

● Active — Started Sep 21, 2021 11:45:43 (2w ago)

Event Description

Device 00B958F2242A366AB7D56DFBFB9801F4 out of image compliance

Image Difference

Designed software image (bundle EOS-4.25.4M)	Running software image
EOS-4.25.4M.swi TerminAttr-1.15.3-1.swix	EOS-4.26.2F.swi Riota.swix

CVE And bug Exposure

The event has a Warning severity.

7.17.5 Managing Events

You can manage an event by customizing event rules differently. Refer to the following examples:

- Disabling All Events of the Selected Type
- Disabling All Events of the Selected Type with Exception

7.17.5.1 Disabling All Events of the Selected Type

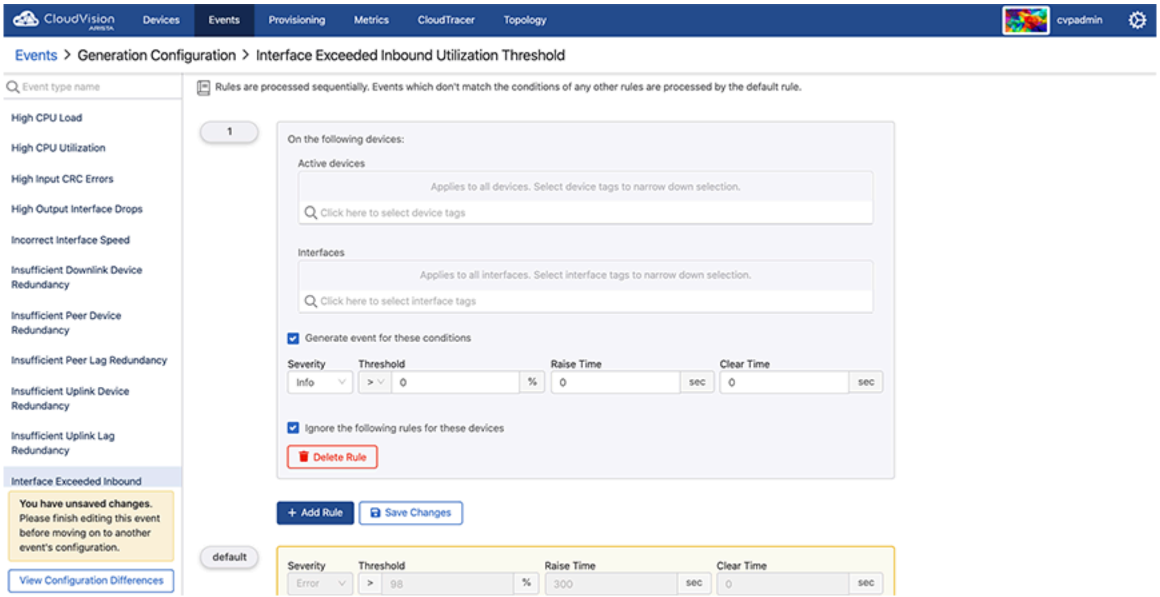
Perform the following steps to disable all events of the selected type:

1. Navigate to the **Generation Configuration** screen.
2. Click the required event type in the left pane.
3. In the right pane, Click the **+ Add Rule** button.

   Note: Retain only one rule with no values defined. To disable the event only for selected datasets, select appropriate devices tags in the **Devices** field.
4. Select the **Stop generating events** and checking rules checkbox.

The system disables all events of the selected event type.

Figure 7-105: Disable All Events of the Selected Type



Events > Generation Configuration > Interface Exceeded Inbound Utilization Threshold

Event type name

- High CPU Load
- High CPU Utilization
- High Input CRC Errors
- High Output Interface Drops
- Incorrect Interface Speed
- Insufficient Downlink Device Redundancy
- Insufficient Peer Device Redundancy
- Insufficient Peer Lag Redundancy
- Insufficient Uplink Device Redundancy
- Insufficient Uplink Lag Redundancy
- Interface Exceeded Inbound

You have unsaved changes. Please finish editing this event before moving on to another event's configuration.

View Configuration Differences

Rules are processed sequentially. Events which don't match the conditions of any other rules are processed by the default rule.

1

On the following devices:

Active devices

Applies to all devices. Select device tags to narrow down selection.

Click here to select device tags

Interfaces

Applies to all interfaces. Select interface tags to narrow down selection.

Click here to select interface tags

☑ Generate event for these conditions

Severity	Threshold	Raise Time	Clear Time
Info	> 0 %	0 sec	0 sec

☑ Ignore the following rules for these devices

Delete Rule

+ Add Rule   Save Changes

default

Severity	Threshold	Raise Time	Clear Time
Error	> 98 %	300 sec	0 sec

5. Click **Save** in the left pane.

7.17.5.2 Disabling All Events of the Selected Type with Exception

Perform the following steps to disable all events of the selected type with exceptions:

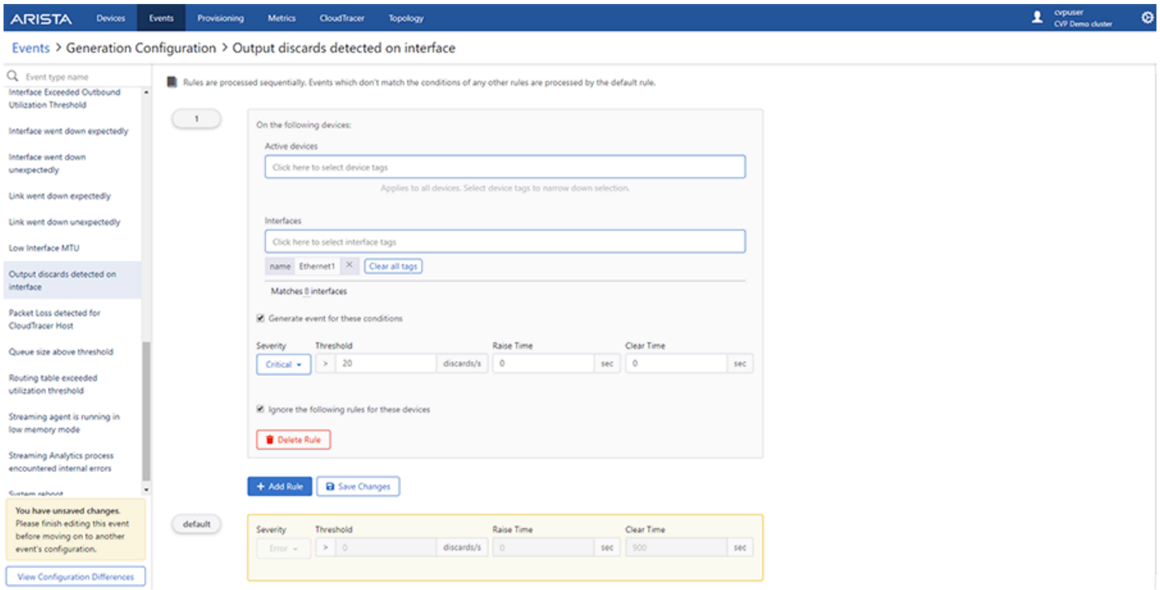
1. Navigate to the **Generation Configuration** screen.
2. Click the required event type in the left pane.
3. In the right pane, Click the **+ Add Rule** button.
4. In the **Conditions** pane, provide the device tags that you still want to generate an event for. The system creates rule 1.

   Note: If you need devices with different conditions, add another rule by repeating steps 3 and 4.

5. Click the **+ Add Rule** button.
6. In the appropriate **Conditions** pane, select the Stop generating events and checking rules checkbox. The system creates rule 3.

Note: If you skip steps 5 and 6, the system applies default rules to all device tags except the ones that are defined in rules 1 and 2.

Figure 7-106: Disable All Events of the Selected Type with Exception


ARISTA
Devices
Events
Provisioning
Metrics
CloudTracer
Topology
cvpuser
CVP Demo cluster
Event type name
Interface Exceeded Outbound Utilization Threshold
Interface went down expectedly
Interface went down unexpectedly
Link went down expectedly
Link went down unexpectedly
Low Interface MTU
Output discards detected on interface
Packet Loss detected for CloudTracer Host
Queue size above threshold
Routing table exceeded utilization threshold
Streaming agent is running in low memory mode
Streaming Analytics process encountered internal errors
System reboot
View Configuration Differences
1
Click here to select device tags
Click here to select interface tags
Clear all tags
Delete Rule
Add Rule
Save Changes
default

Events > Generation Configuration > Output discards detected on interface

Rules are processed sequentially. Events which don't match the conditions of any other rules are processed by the default rule.

You have unsaved changes. Please finish editing this event before moving on to another event's configuration.

On the following devices:

Active devices

Applies to all devices. Select device tags to narrow down selection.

Interfaces: name Ethernet1

Matches 8 interfaces

☑ Generate event for these conditions

Severity: Critical; Threshold: > 20 discards/s; Raise Time: 0 sec; Clear Time: 0 sec

☑ Ignore the following rules for these devices

Severity: Error; Threshold: > 0 discards/s; Raise Time: 0 sec; Clear Time: 900 sec

The system disables all events of the selected type except the ones that are defined in rules 1 and 2.

7.17.6 Acknowledging Events

Acknowledging an event confirms that you are aware of the corresponding event and its consequences. By default, acknowledged events are hidden and do not send alerts.

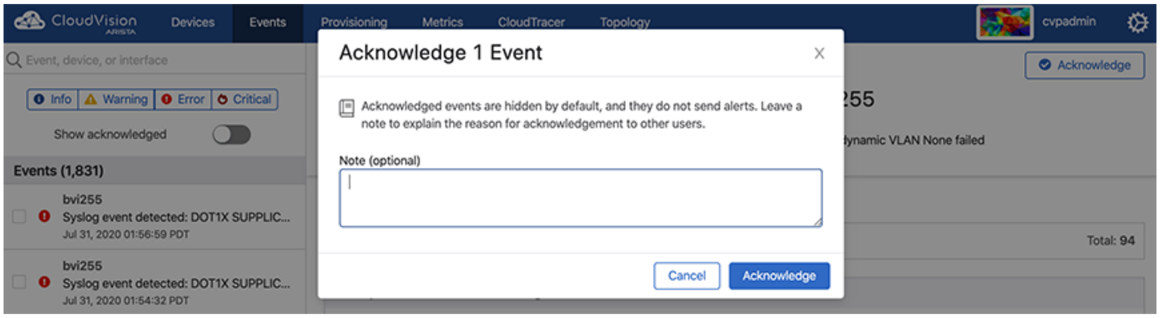
Perform the following steps to acknowledge an event:

1. Click the **Events** tab. The system displays the **Events** screen.
2. Select preferred event(s) in the side panel.
3. Click **Acknowledge *n*** in the upper right corner of the side panel.

Note: ***n*** represents the count of selected events.

The system displays the **Acknowledgment Event** window.

Figure 7-107: Acknowledgment Event Pop-Up



Events (1,831)

bvi255
Syslog event detected: DOT1X SUPPLIC...
Jul 31, 2020 01:56:59 PDT

bvi255
Syslog event detected: DOT1X SUPPLIC...
Jul 31, 2020 01:54:32 PDT

Acknowledge 1 Event

Acknowledged events are hidden by default, and they do not send alerts. Leave a note to explain the reason for acknowledgement to other users.

Note (optional)

4. (Optional) Type a note for other users explaining the reason for the acknowledgment.
5. Click **Acknowledge *n* events** where ***n*** represents the count of selected events.

Note: For acknowledged events, the system replaces the **Acknowledge** button with **Un-Acknowledge** button. To undo the acknowledgment activity, Click **Un-Acknowledge** in the side panel of the acknowledged event.

7.17.7 Configuring Notifications

The event alerting system sends notifications for CVP events as they alert operating platforms that you have set up. Once you have customized the topology view for your network, provide the required information to configure the monitoring of notifications.

Perform the following steps to configure event alerts:

1. Click the **Events** tab.
2. Click **Configure Notifications** at the upper right corner of the Events section. The system displays the Notification Configuration screen.
3. Configure the following entities:
   - Configuring Status
   - Configuring Platforms
   - Configuring Receivers
   - Configuring Rules
4. Click **Save** in the left pane

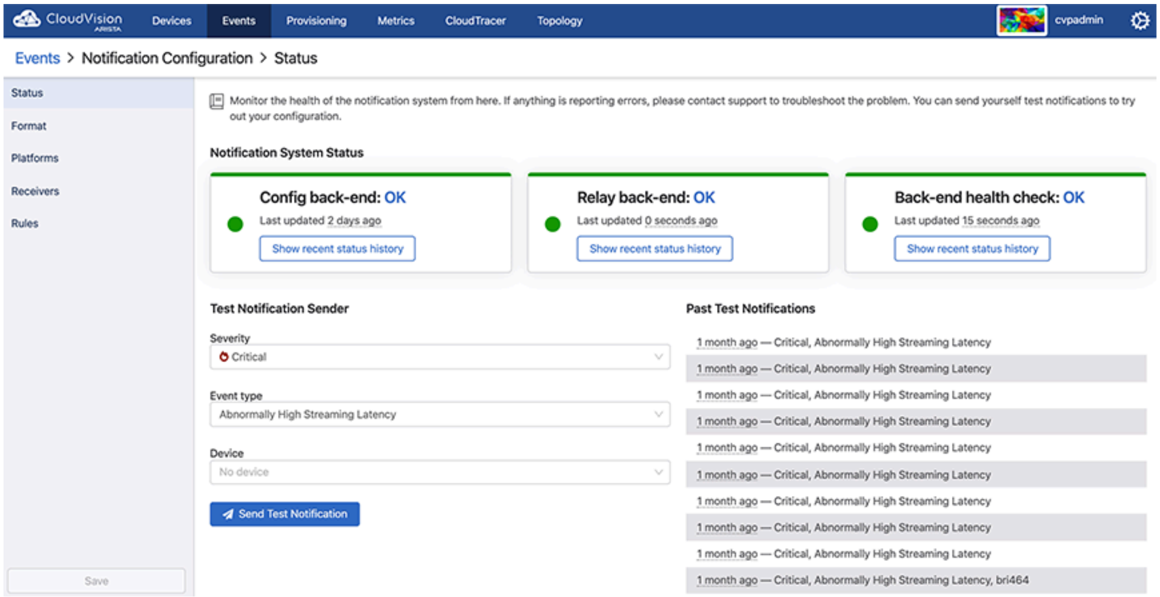
7.17.7.1 Configuring Status

The **Status** section configures monitoring the health of notification system.

Perform the following steps to configure the notification criteria:

1. Click **Status**. The system displays the **Status** screen.

Figure 7-108: Status Screen of Notification Configuration



Monitor the health of the notification system from here. If anything is reporting errors, please contact support to troubleshoot the problem. You can send yourself test notifications to try out your configuration.

Notification System Status

Config back-end: OK
Last updated 2 days ago

Relay back-end: OK
Last updated 0 seconds ago

Back-end health check: OK
Last updated 15 seconds ago

Test Notification Sender

Severity: Critical

Event type: Abnormally High Streaming Latency

Device: No device

Past Test Notifications

1 month ago — Critical, Abnormally High Streaming Latency
1 month ago — Critical, Abnormally High Streaming Latency
1 month ago — Critical, Abnormally High Streaming Latency
1 month ago — Critical, Abnormally High Streaming Latency
1 month ago — Critical, Abnormally High Streaming Latency
1 month ago — Critical, Abnormally High Streaming Latency
1 month ago — Critical, Abnormally High Streaming Latency
1 month ago — Critical, Abnormally High Streaming Latency
1 month ago — Critical, Abnormally High Streaming Latency
1 month ago — Critical, Abnormally High Streaming Latency, bri464

2. On the **Test Alert Sender** pane, provide the required criterion in **Severity**, **Event type**, and **Device** drop-down menus.
3. If required, click **Send Test Notification** to verify current configuration.

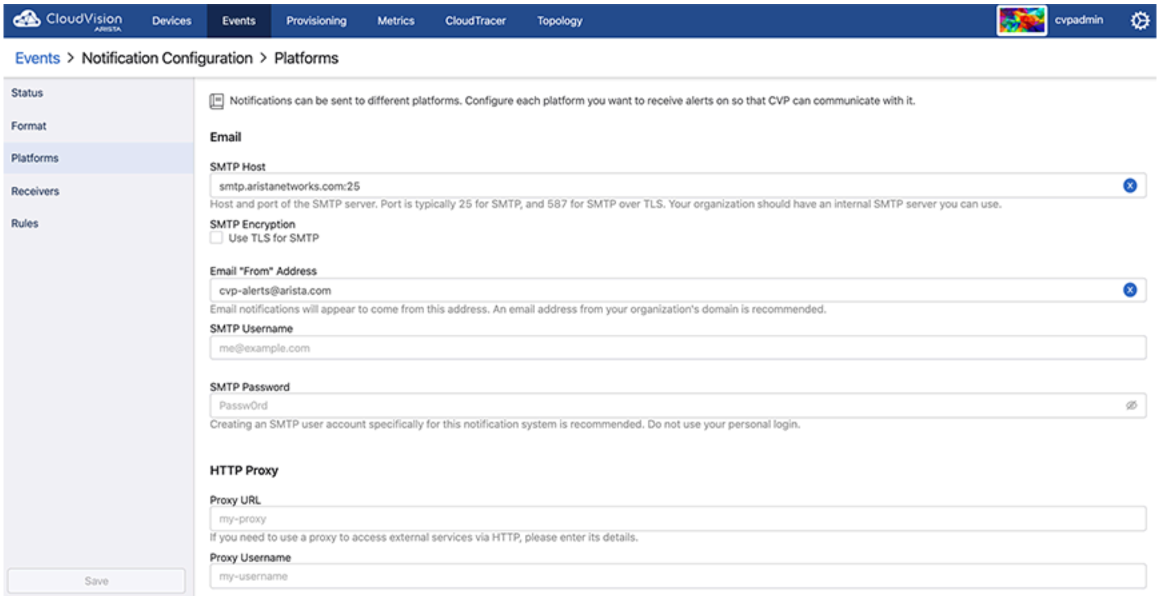
7.17.7.2 Configuring Platforms

The Platforms section specifies what platforms will receive notifications.

Perform the following steps to configure preferred platforms:

1. Click **Platforms**. The system displays the **Platforms** screen.

   Figure 7-109: Platforms Screen of Notification Configuration



Notifications can be sent to different platforms. Configure each platform you want to receive alerts on so that CVP can communicate with it.

Email

SMTP Host: smtp.aristanetworks.com:25

Host and port of the SMTP server. Port is typically 25 for SMTP, and 587 for SMTP over TLS. Your organization should have an internal SMTP server you can use.

SMTP Encryption

☐ Use TLS for SMTP

Email "From" Address: cvp-alerts@arista.com

Email notifications will appear to come from this address. An email address from your organization's domain is recommended.

SMTP Username: me@example.com

SMTP Password: Passw0rd

Creating an SMTP user account specifically for this notification system is recommended. Do not use your personal login.

HTTP Proxy

Proxy URL: my-proxy

If you need to use a proxy to access external services via HTTP, please enter its details.

Proxy Username: my-username

2. Configure any of the following platforms through which you prefer to receive notifications from CVP:

   - **Email**

     Provide the following information to receive email notifications:

     - Type your SMTP servers hostname and port number separated by a colon in the **SMTP Hos**t field.

       Note: Typically, the port numbers of SMTP and SMTP over TLS are 25 and 587.

     - Select the **Use TLS for SMT**P checkbox if you prefer to encrypt notifications received from and sent to the SMTP server.
     - Type the email address that you prefer to display as a sender in the **Email "From" Address** field.

       Note: We recommend an email address with the domain of your organization.

     - Type the username of your SMTP account in the **SMTP Username** field.
     - Type the password of your SMTP account in the **SMTP Password** field.
   - **Slack**

     Create a custom integration through the Incoming WebHooks Slack application and type the Webhook URL in the **Slack Webhook URL** field.
   - **VictorOps**
     - In your **VictorOp**s settings, add a new alert integration for Prometheus and type the Service API Key in the **VictorOps API Key** field.
     - If required, type a custom API URL in the **VictorOps API URL** field.
   - **PagerDuty**

     If required, type a custom API URL in the **PagerDuty URL** field.
   - **OpsGenie**
     - Create an API integration for your OpsGenie team and type the API key in the **OpsGenie API Key** field.
     - If required, type a custom API URL in the **OpsGenie API URL** field.
   - **Google Chat**

In Google Chat the Alerter will send a message containing one or more alerts and related information. Follow the steps in the Google Chat for Developers Guide to create a webhook, use the webhook URL to configure the Google Chat platform on CloudVision.

- **Microsoft Teams**

  In MS Teams the Alerter will send a message containing one or more alerts and related information. Follow the steps in the Microsoft Teams - Create Incoming Webhooks - document to create a webhook, use the webhook URL to configure the Microsoft Teams platform on CloudVision.
- **Zoom**

  In Zoom the Alerter will send a message containing one or more alerts and related information. Add webhooks and get configuration information using the guide Using Zoom's Incoming Webhook Chatbot, once you have the URL and verification token you can enter them into the Zoom platforms settings on CloudVision.
- **Sendgrid**

  Sendgrid is also available as an alternative to email. On CVaaS, Sendgrid requires no configuration, while for on-prem installations Sendgrid requires an API key and from address. It uses the same content templates as Email.
- **Syslog**

  The Alerter will send a syslog message for each CVP event. The syslog facility must be set in the configuration. The syslog priority is mapped from the CVP severity and this mapping may be customized in the configuration.

  Syslog messages are formatted with the following values:

  - Timestamp: The time that the event fired/was resolved.
  - Hostname: a comma-separated list of device hostnames from the devices the event is related to.
  - Facility: from user configuration.
  - Severity: mapped from CVP severity according to user configuration.
  - Appname: tag from user configuration.
  - Message: $devices: $eventType - $description, $time
- **SNMP**

  The Alerter will send an SNMP trap for each CVP event, this supports SNMPv1, SNMPv2c and SNMPv3. The OID of the SNMP Trap will use an OID from an Arista CloudVision Alerter specific MIB ARISTA-CV-MIB.txt, the message is a string message containing the necessary information.

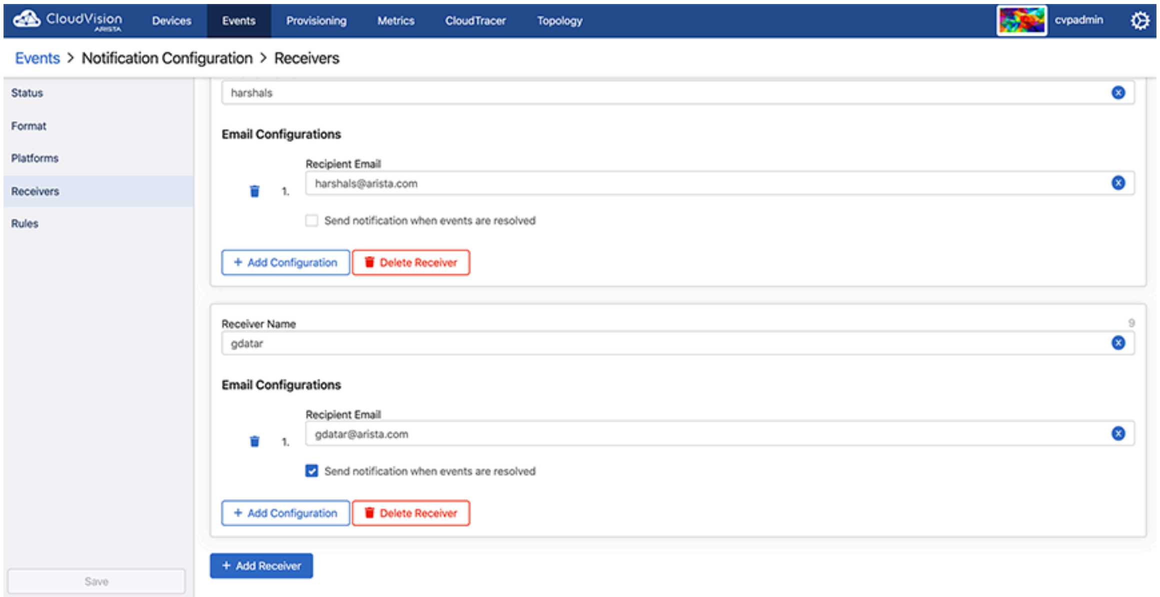
7.17.7.3 Configuring Receivers

The Receivers section configures a receiver for each preferred team to send notifications and link receivers to notification platforms.

Perform the following steps to add new receivers:

1. Click **Receivers**. The system displays the Receivers screen.

Figure 7-110: Receivers Screen of Notification Configuration



harshals

Email Configurations

Recipient Email

1. harshals@arista.com

☐ Send notification when events are resolved

Receiver Name 9

gdatar

Email Configurations

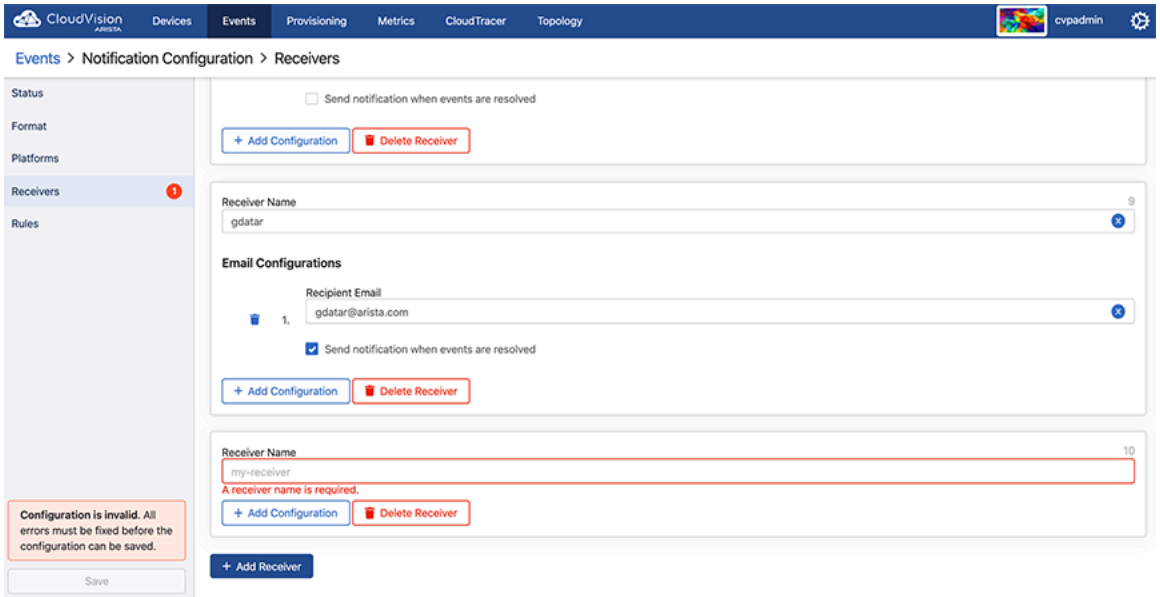
Recipient Email

1. gdatar@arista.com

☑ Send notification when events are resolved

2. Click **Add Receivers** at the end of the screen.
3. Type receiver's name in the **Receiver Name** field.

Figure 7-111: Add Receiver Pane



☐ Send notification when events are resolved

Receiver Name 9

gdatar

Email Configurations

Recipient Email

1. gdatar@arista.com

☑ Send notification when events are resolved

Receiver Name 10

my-receiver

A receiver name is required.

Configuration is invalid. All errors must be fixed before the configuration can be saved.

4. Click the **Add Configuration** drop-down menu.
5. Select any of the options in following table and provide the required information to link alert receivers with alerting platforms.

Table 15: Configuration Options

Configuration Options	Required Information
Add Email Configuration	• Type recipient's email address in the **Recipient Email** field. • If required, select the **Send alert when events are resolved** checkbox.
Add VictorOps Configuration	• Type a routing key in the **Routing Key** field. • If required, select the **Send alert when events are resolved** checkbox.
Add PagerDuty Configuration	• Type a routing key in the **Integration Key** field. • If required, select the **Send alert when events are resolved** checkbox.
Add OpsGenie Configuration	Select the **Send alert when events are resolved** checkbox.
Add Slack Configuration	• Type a channel in the **Channel** field. • If required, select the **Send alert when events are resolved** checkbox.
Add Pushover Configuration	• Type a recipient's user key in the **Recipient User Key** field. • Type a pushover API token in the **Application API Token** field. • If required, select the **Send alert when events are resolved** checkbox.
Add Webhook Configuration	• Type the URL where you prefer to post event alerts in the **Target URL** field. • If required, select the **Send alert when events are resolve**d checkbox

Note: Click the recycle bin icon at the right end of corresponding fields if you prefer to delete that configuration. Click **Delete Receiver** next to **Add Configuration** if you prefer to delete the corresponding receiver.

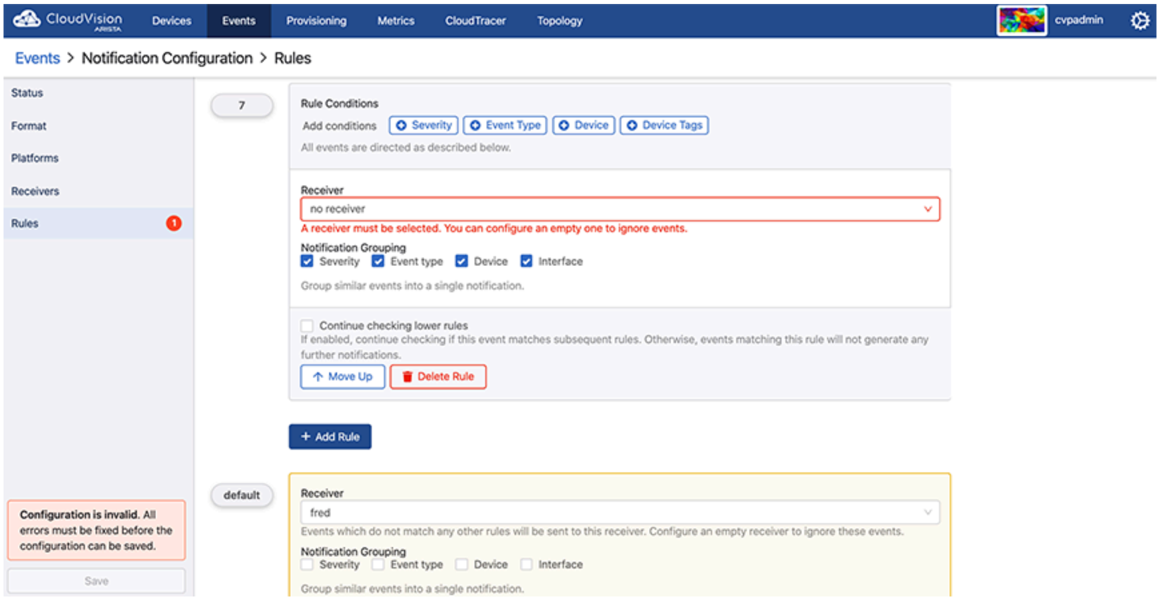
7.17.7.4 Configuring Rules

The Rules section customizes notifications that are sent to receivers.

Perform the following steps to add a new rule:

1. Click **Rules**. The system displays the Rules screen.

Figure 7-112: Rules Screen of Notification Configuration



Rule Conditions

Add conditions

All events are directed as described below.

Receiver: no receiver

A receiver must be selected. You can configure an empty one to ignore events.

Notification Grouping: ☑ Severity ☑ Event type ☑ Device ☑ Interface

Group similar events into a single notification.

□ Continue checking lower rules

If enabled, continue checking if this event matches subsequent rules. Otherwise, events matching this rule will not generate any further notifications.

Receiver: fred

Events which do not match any other rules will be sent to this receiver. Configure an empty receiver to ignore these events.

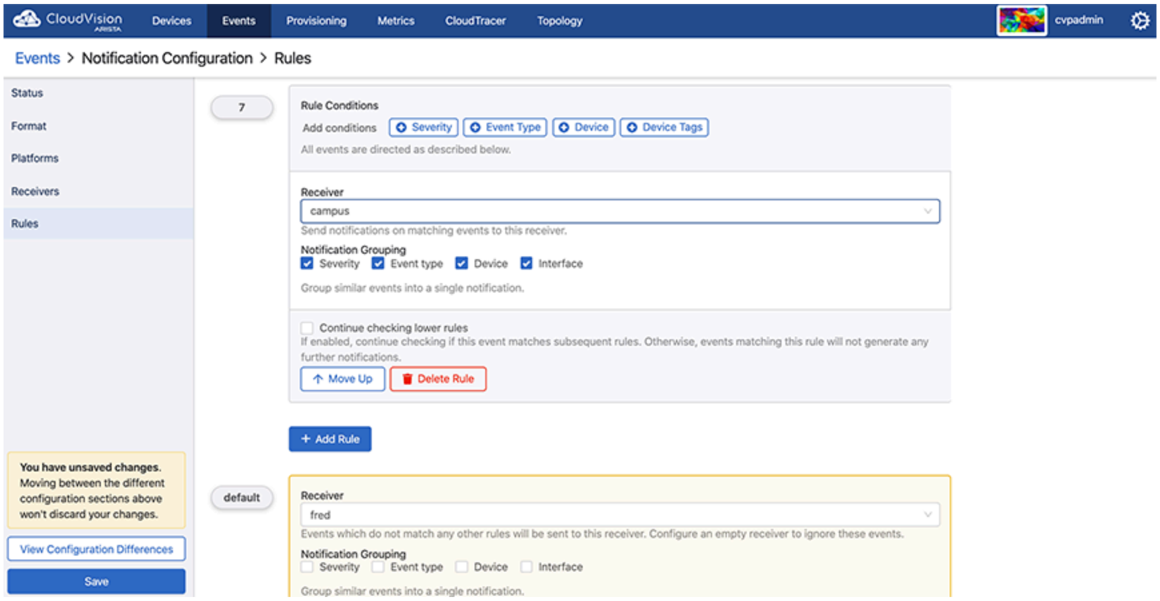
Notification Grouping: □ Severity □ Event type □ Device □ Interface

Group similar events into a single notification.

Configuration is invalid. All errors must be fixed before the configuration can be saved.

2. Click **Add Rules**. A new Rules Conditions pane is displayed on the screen.

Figure 7-113: Rule Conditions Pane



Rule Conditions

Add conditions

All events are directed as described below.

Receiver: campus

Send notifications on matching events to this receiver.

Notification Grouping: ☑ Severity ☑ Event type ☑ Device ☑ Interface

Group similar events into a single notification.

□ Continue checking lower rules

If enabled, continue checking if this event matches subsequent rules. Otherwise, events matching this rule will not generate any further notifications.

Receiver: fred

Events which do not match any other rules will be sent to this receiver. Configure an empty receiver to ignore these events.

Notification Grouping: □ Severity □ Event type □ Device □ Interface

Group similar events into a single notification.

You have unsaved changes. Moving between the different configuration sections above won't discard your changes.

3. Next to **Add Conditions**, click **Severity**, **Event Type**, **Device**, and **Device Tags** to provide the criteria that are used for monitoring the health of the alerting system.

   Note: Click **Remove** at the end of a field to delete that configuration.

4. Select the required receiver from the **Receiver** drop-down menu.
5. Select required checkboxes among Severity, Event Type, Device, and Interface to group similar events into a single alert.
6. Select the **Continue checking lower rules** checkbox to continue checking for alerts if this event matches subsequent rules.
7. Click **Move up** if you prefer to move this rule up in the priority list.

Note: Rules are processed sequentially. The default rule is applied only when an event does not match any other rules. Click **Delete rule** to delete the corresponding rule. Click **Move down** in configured rules to move the corresponding rule down in the priority list.

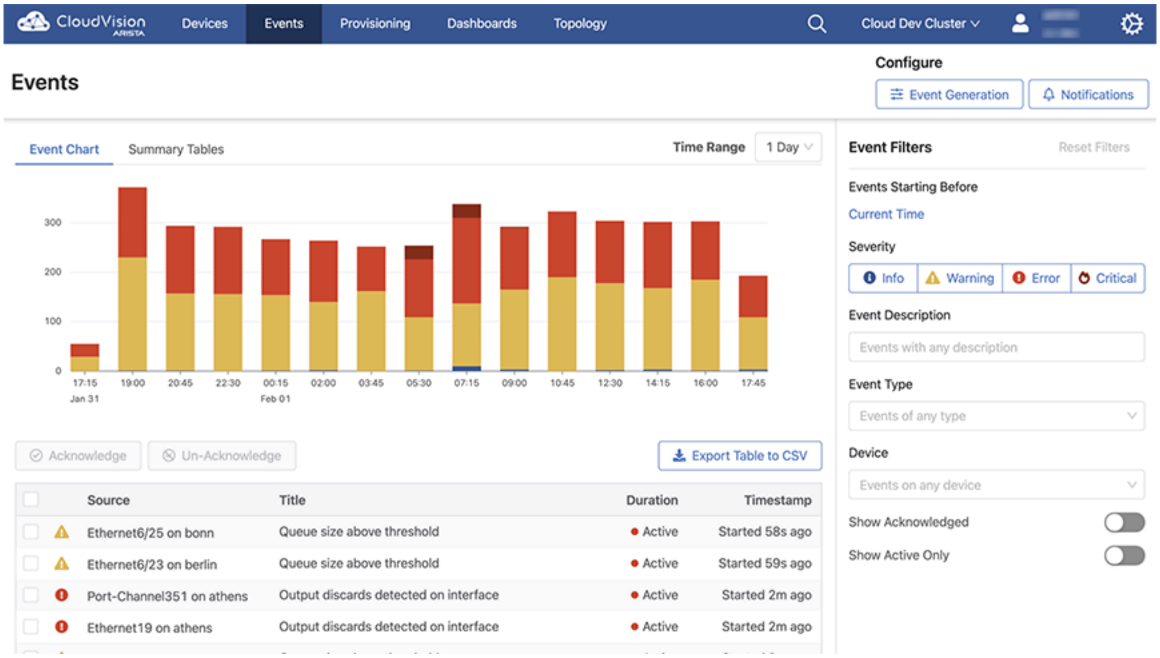
7.18 Events App

The Events app provides fast filtering results that are loaded 100 events at a time, improving loading times and responsiveness compared to the existing Events app.

7.18.1 Event Summary

At the top of the app is the event summary. The summary has two tabs for the Event Chart and the Summary Tables. There is also a time range duration picker that selects the start of the time range for the summary results. The filters in the app sidebar also affect the summary views, allowing the request of specific summary queries.

Figure 7-114: New Events App



Events Starting Before: Current Time

Severity: Info | Warning | Error | Critical

Event Description: Events with any description

Event Type: Events of any type

Device: Events on any device

Show Acknowledged

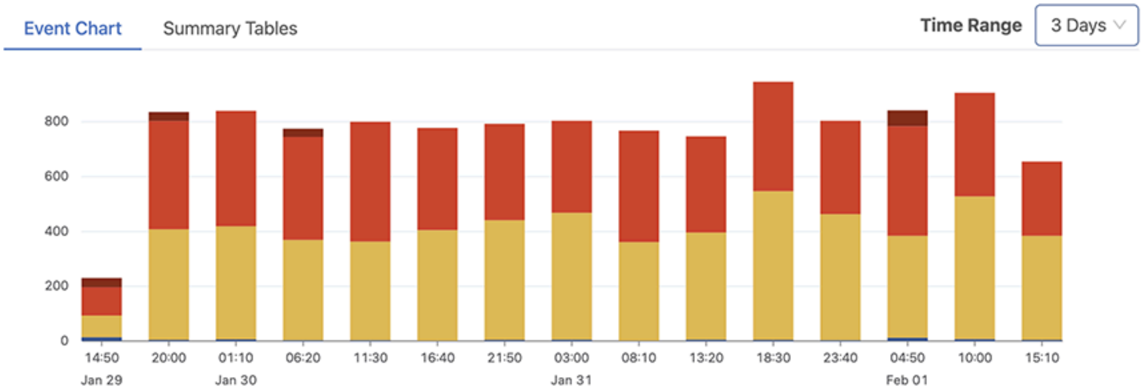
Show Active Only

☐		Source	Title	Duration	Timestamp
☐	⚠	Ethernet6/25 on bonn	Queue size above threshold	● Active	Started 58s ago
☐	⚠	Ethernet6/23 on berlin	Queue size above threshold	● Active	Started 59s ago
☐	❗	Port-Channel351 on athens	Output discards detected on interface	● Active	Started 2m ago
☐	❗	Ethernet19 on athens	Output discards detected on interface	● Active	Started 2m ago

Event Chart

The default summary view is the Events Chart. This chart displays the number of events that were created in a time range, broken down by severity. Hovering over a colored section of a bar shows how many events occurred with that given severity. A bar represents the events that were created within time range for that bar. . The amount of time represented by a bar is dependent on the selected time range. Larger time ranges will group more events into a single bar.

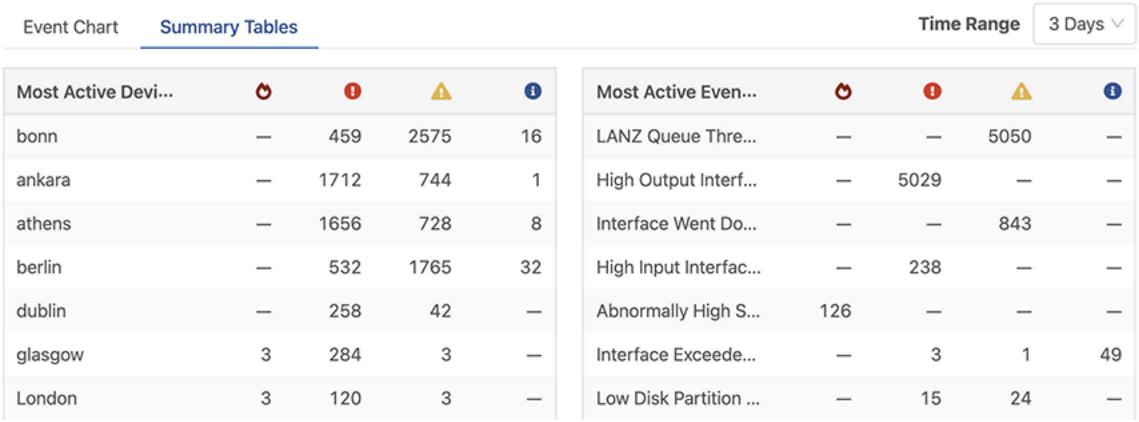
Figure 7-115: Event Chart Summary



Summary Tables

The Summary Tables tab displays the events of the Events Chart in a table format. Results can be filtered by severity value, device, or event-type.

Figure 7-116: Summary Tables



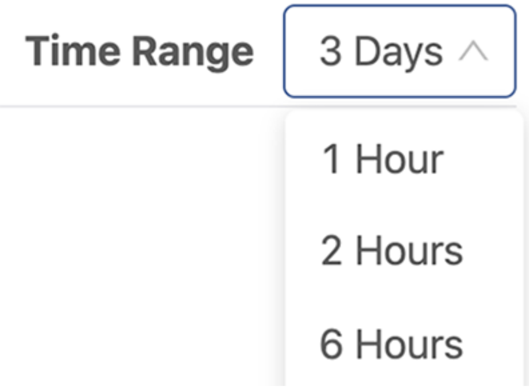
Most Active Devi...	🔥	❗	⚠	ℹ
bonn	—	459	2575	16
ankara	—	1712	744	1
athens	—	1656	728	8
berlin	—	532	1765	32
dublin	—	258	42	—
glasgow	3	284	3	—
London	3	120	3	—

Most Active Even...	🔥	❗	⚠	ℹ
LANZ Queue Thre...	—	—	5050	—
High Output Interf...	—	5029	—	—
Interface Went Do...	—	—	843	—
High Input Interfac...	—	238	—	—
Abnormally High S...	126	—	—	—
Interface Exceede...	—	3	1	49
Low Disk Partition ...	—	15	24	—

Summary Time Picker

In the top-right corner of the summary there is a time range picker. This affects the summaries only. The end-time of the summary window is determined by the **Events Starting Before** filter in the sidebar. The start-time is derived from the chosen time range. The range picker has a minimum duration of one hour and a maximum of one week.

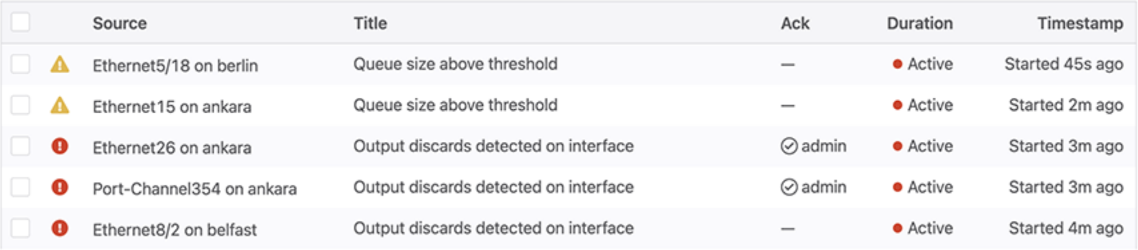
Figure 7-117: Summary Time Picker



7.18.2 Events Table

Events matching the selected filters are displayed in the table below the summary.

Figure 7-118: Events Tables



□		Source	Title	Ack	Duration	Timestamp
□	⚠	Ethernet5/18 on berlin	Queue size above threshold	—	● Active	Started 45s ago
□	⚠	Ethernet15 on ankara	Queue size above threshold	—	● Active	Started 2m ago
□	❗	Ethernet26 on ankara	Output discards detected on interface	✓ admin	● Active	Started 3m ago
□	❗	Port-Channel354 on ankara	Output discards detected on interface	✓ admin	● Active	Started 3m ago
□	❗	Ethernet8/2 on belfast	Output discards detected on interface	—	● Active	Started 4m ago

The newest 100 events are initially loaded. Subsequent events are fetched via automatic pagination. The **Ack**(Acknowledgement) column only appears if the **Show Acknowledged** filter toggle is on. This allows other columns to expand when acknowledgment information is not required.

Events Table Functionality

- When scrolling down through the table of events, older events are automatically fetched.
- If there are no events matching the selected filters, the events table will display an empty data message.
- To update the display with events that may have occurred while viewing the Events Table, select the **Show New Events** button. The screen will be updated with the new data.
- To export the currently-loaded events, select the **Export Table to CSV** button.

Certificate Expiration Event

When the CloudVision SSL certificate is expiring an event will alert users 90 days in advance of certificate expiration. Clicking on the event will provide further information. To clear the event, the SSL certificate must be replaced.

7.18.3 Event Filters

Filter options are located in the sidebar. The selected filters affect the results in both the events summary and the events table. Multiple filters can be selected to refine the results shown in these sections. Filters are automatically applied as they are changed in the sidebar.

Events Starting Before

The **Events Starting Before** time selector defines the end cutoff time filter for events. Events that are created after the selected time will not be shown. By default, the filter is set to the current time.

Select this filter to open the date-time picker, allowing an older time to be selected. Select **Apply** to update with this new time filter. Select **Use current time** to show live events.

Severity

Selecting an event severity will display only the selected severity level.

Event Description

The **Event Description** filter allows events to be searched by arbitrary text in the event description field.

Event Type

When selected, the **Event Types** filter presents a list of all available event types. Selecting one or more options filters the results to events of the selected types.

Device

When Selected, the **Device** filter presents a list of all streaming devices. Selecting one or more devices will display events that occurred on the selected devices.

Show Acknowledged

Select **Show Acknowledged** to view events which have been previously acknowledged.

Active Events Only

Select **Show Active Only** to view events which are still active.

Resetting Filters

Select the **Reset Filters** button to place all Event filters to their default values.

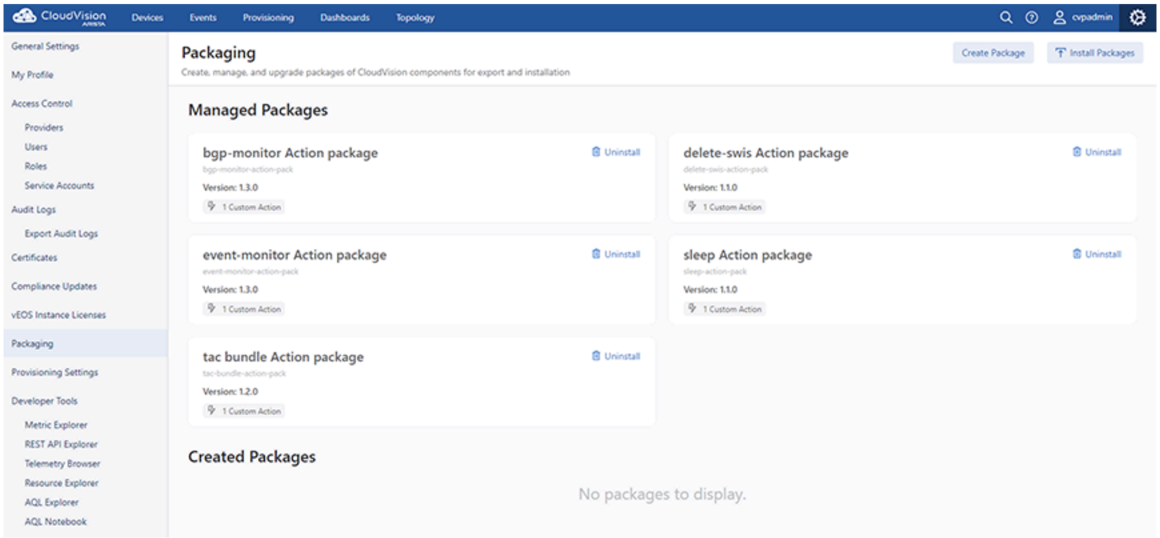
7.19 Packaging

The Packaging feature is used to export custom change control actions from one CloudVision cluster and install them in another. Package IDs and version numbers can be used to update existing packages with version control.

Accessing Packaging

The Packaging feature is available under Settings tab in the navigation bar.

Figure 7-119: Accessing Packaging



Packaging

Create, manage, and upgrade packages of CloudVision components for export and installation

Managed Packages

bgp-monitor Action package
bgp-monitor-action-pack
Version: 1.3.0
1 Custom Action

delete-swis Action package
delete-swis-action-pack
Version: 1.1.0
1 Custom Action

event-monitor Action package
event-monitor-action-pack
Version: 1.3.0
1 Custom Action

sleep Action package
sleep-action-pack
Version: 1.1.0
1 Custom Action

tac bundle Action package
tac-bundle-action-pack
Version: 1.2.0
1 Custom Action

Created Packages

No packages to display.

From the Packaging screen, you can create, install, and review packages. There are two main sections when managing packages: Managed Packages and Created Packages.

Managed Packages have been imported from another CloudVision cluster and installed. Hover over the package to review the description. The only available function is to unistall the selected package.

Created Packages are editable and available for export to another CloudVision cluster.

Note: Packages can only be edited and exported from,the cluster where they were created.

7.19.1 Create a Package

When creating a package you can select the components to be included. You can select studios, actions, and dashboards to bundle and export. Additional actions to manage the installation and uninstallation of packages and components can be added.

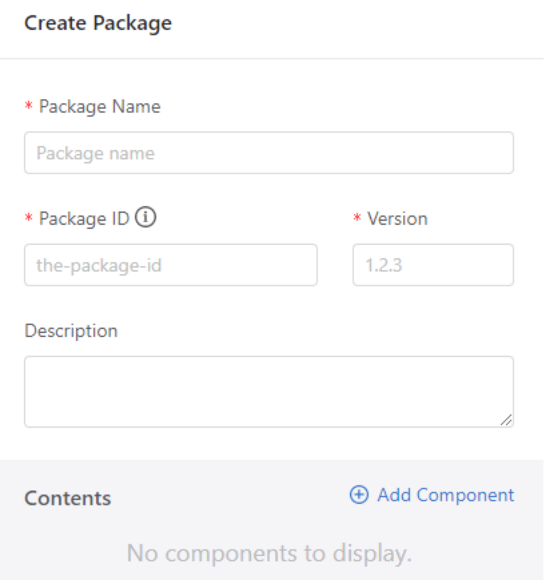
Creating a Package

1. From the Packaing screen, select **Create Package**.
2. Enter a package name.
3. Create a unique Package ID and enter a version number. The Package ID should be human readable. The version number must be three digits (x.x.x).

   Note: Make sure that the ID does not match the Package ID of an existing package, otherwise an existing package may be overwriten.

4. Enter a description of the package.

Figure 7-120: Creating a Package



Create Package

* Package Name

Package name

* Package ID ⓘ

the-package-id

* Version

1.2.3

Description

Contents

No components to display.

5. Click **Add Component** and use the dropdown to select actions to include in the package. Selected actions will appear under Contents

> **Note:** Actions may be executed at different speeds. Limit the number of components in a package to those that are related and likely to change together, such as a pair of actions that run before and after a process.

6. (Optional) Click **Edit** below any component name to create a unique Component ID.
7. Click **Create Package**. The package will appear under Created Packages.
8. Click **Export** on the package to download the .tar package file.
9. Save the file to the appropriate repository so that it can easily be located for import and installation in another CloudVision cluster.

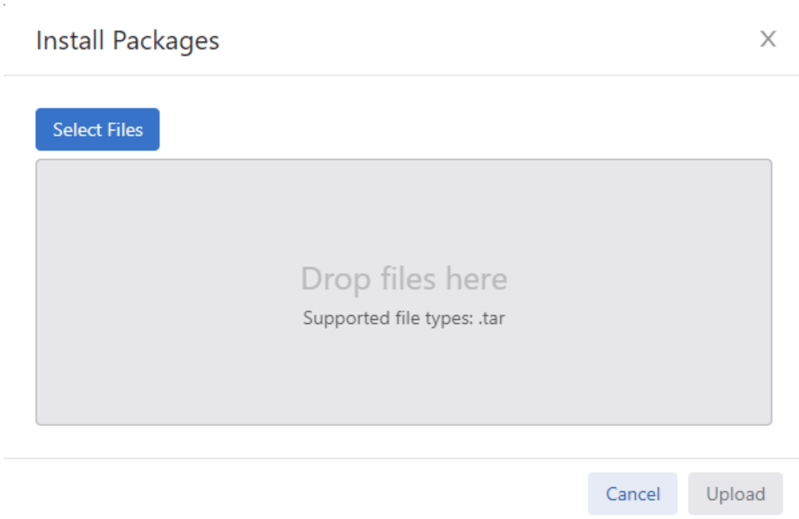
7.19.2 Installing a Package

Packages that have been exported as .tar files from another CloudVision cluster can be imported and installed.

1. In the cluster that a packege is to be installed, open the Packaging screen and click **Install Packages**.
2. Select or drag-and-drop the appropriate .tar file into the modal. Multiple packages may be selected and installed at the same time.

Note: Check the version number and Package ID before installation to avoid overwriting an existing package.

Figure 7-121: Installing Packages



Install Packages

Drop files here

Supported file types: .tar

3. Select **Upload**.

7.19.3 Updating a Package

Updating a package will overwrite an existing package.

1. Export the package to be overwritten.
2. If the package to be overwritten is listed under Created Packages it must be deleted.
3. Create a new package using the same name as the package to be updated.
4. Enter the package ID with the same package ID of the original package.
5. Increase the version number of the original package sequentially.
6. Proceed to follow the steps for uploading and installing a package,

Note: Before installing an updated package, verify that you select the .tar file with the appropriate version number.

7.20 Troubleshooting

A number of commands are provided with the Telemetry platform that you can use to troubleshoot the Telemetry platform components. The types of troubleshooting you can perform using the Telemetry platform commands are:

- General Troubleshooting
- Troubleshooting the NetDB State Streaming Agent
- Checking the Status of the Ingest Port

7.20.1 General Troubleshooting

Telemetry commands are provided that enable you to troubleshoot the Telemetry platform components. By default, debug log files are available for all of the Telemetry platform components, which you can view using Telemetry commands. You can also use standard CVP commands to check the status of Telemetry components and applications.

7.20.1.1 Viewing Debug Log Files

You can view debug log files for all platform components in a single log file, or for a particular platform component.

Note: To use the commands, you must login as **cvp** user. You must also login as **cvp** user to execute `su cvp`.

To view debug log files for all platform components in a single log file

Use the `cvpi logs all` command.

To view the location of debug log files for a particular platform component

Use the `cvpi logs <component>` command.

You must specify the component using the name of the component as it is specified in the component's yaml file definition.

To create a zip archive (.tgz) containing debugging information

Use the `cvpi debug` command.

This command creates a .tgz archive on each CVP node that contains debugging information. The archive is automatically saved to the /data/debug directory on each node. Files need to be collected manually.

7.20.1.2 Checking CVPI Status

You can use commands to check status of the Telemetry components and applications, and to check the status of the entire CVP environment.

To check the status of CVPI

Use the `cvpi status all` command.

This command checks the status of CVPI, including the Telemetry components and applications.

To check the status of CVP environment

Use the `cvpi check all` command.

This command runs a check to ensure that the CVP environment is setup correctly. In a multi-node setup, it checks to make sure that the nodes can communicate with to each other and have the same environments and configuration.

7.20.2 Troubleshooting the NetDB State Streaming Agent

The Telemetry platform component provides commands you can use to troubleshoot issues you may encounter with the installation or performance of the NetDB State Streaming Agent.

The commands enable you to:

- Inspect the agent's configuration
- Restart the agent
- View the agent's logs

7.20.2.1 Inspect the agent’s configuration

Run the following commands to view the agent’s configuration:

```
switch> enable
switch# config
switch (config)# daemon TerminAttr
switch (config-daemon-TerminAttr)# show active
```

```
daemon TerminAttr
     exec /usr/bin/TerminAttr -ingestgrpcurl=172.28.131.84:9910 -ingestauth=k
ey,ab27cf35f73543d2afe3b4c15c12e6a3 -taillogs
     no shutdown
```

7.20.2.2 Restart the agent

Run the following commands to toggle the shutdown attribute:

```
switch (config-daemon-TerminAttr)# shutdown
switch (config-daemon-TerminAttr)# no shutdown
```

7.20.2.3 View the agent’s logs

On the switch or using the CLI shortcut, run the following command:

```
bash cat /var/log/agents/TerminAttr-`pidof TerminAttr`
```

7.20.3 Checking the Status of the Ingest Port

The Telemetry platform automatically blocks the ingest port for the entire CVP cluster if the disk usage on any node of the cluster exceeds 85%. This feature prevents the potential for telemetry data to consume too much disk space in the CVP cluster.

You can easily check to see if the ingest port is blocked using the cvpi status ingest-port command.

Example

```
[cvp@cvp109 bin]$ cvpi status ingest-port
[ingest-port:status] Executing...
[ingest-port:status] FAILED

COMPONENT    ACTION   NODE    STATUS     ERROR


ingest-port   status    primary  NOT RUNNING  command: Error running  '/cvpi/
bin/ingest-port.sh status'...
ingest-port       status       secondary     NOT RUNNING     command: Error
 running '/cvpi/bin/ingest-port.sh status': exit status 1
ingest-port       status       tertiary      NOT RUNNING     command: Error
 running '/cvpi/bin/ingest-port.sh status': exit status 1
[cvp@cvp109 bin]$
```

Chapter 8

Device Comparison Application

To gain valuable insights into the state of your devices, such as state changes and comparison with another device, you can manage your inventory for real-time status updates.

The device comparison application gives information about the configuration running on the devices, the VXLAN table, MAC addresses of the devices, IPv4 and IPv6 routing tables, etc.

- Comparison Dashboard
- Running Configuration
- Snapshots
- ARP Table
- Comparing NDP Table
- MAC Address Table
- VXLAN table
- Viewing Device IPv4 Routing Table
- Viewing Device IPv6 Routing Table
- Comparing IPv4 Multicast Table

8.1 Comparison Dashboard

The Comparison Dashboard from the Device tab explores the difference between devices or changes that happened to devices over time. You can compare devices in the following categories:

- Two devices: Two devices at current time with live updates
- Two times: The state of a single device at two chosen times
- Advanced: Two devices at two chosen times

- Accessing the Comparison Browser Screen

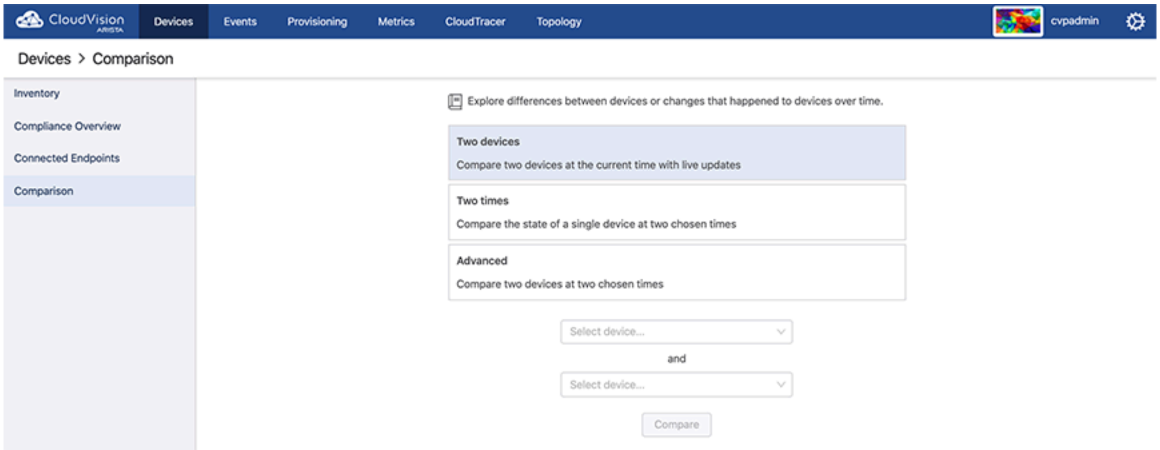
8.1.1 Accessing the Comparison Browser Screen

You can access the Cloud Vision Telemetry Browser screen directly from CVP by completing the following steps. Open your browser.

1. Point your browser to the CVP IP address or hostname.
2. Login to CVP. The CVP Home screen appears.
3. Click **Devices**.

4. Click **Comparison**.

Figure 8-1: Start page for comparison of devices



Explore differences between devices or changes that happened to devices over time.

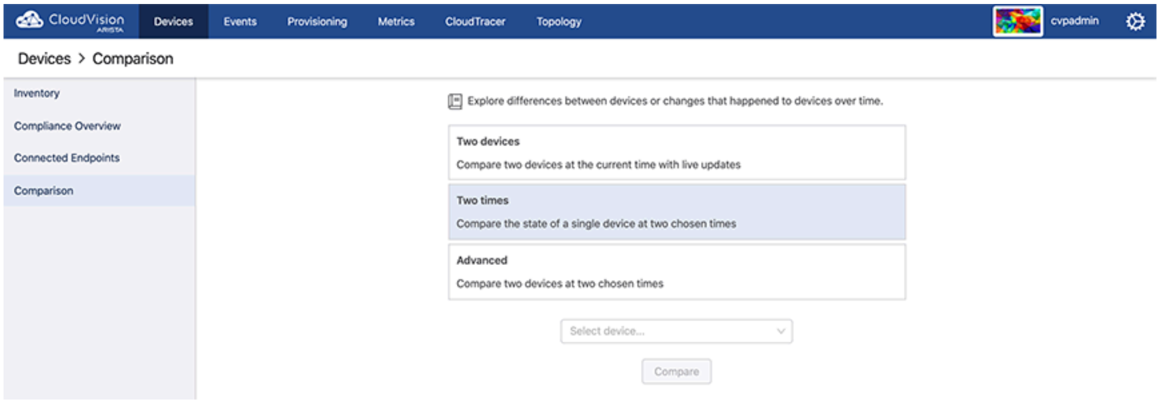
Two devices
Compare two devices at the current time with live updates

Two times
Compare the state of a single device at two chosen times

Advanced
Compare two devices at two chosen times

For a particular device with two chosen times, select the Two times option.

Figure 8-2: Comparison of device at two chosen times



Explore differences between devices or changes that happened to devices over time.

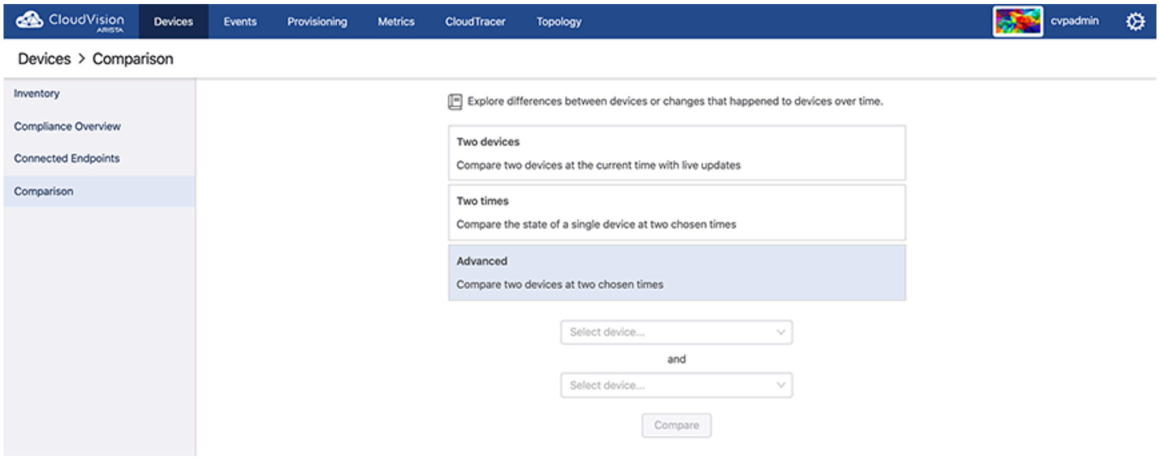
Two devices
Compare two devices at the current time with live updates

Two times
Compare the state of a single device at two chosen times

Advanced
Compare two devices at two chosen times

Comparing two devices at two chosen times, select the Advanced option:

Figure 8-3: Comparison of device advanced



Explore differences between devices or changes that happened to devices over time.

Two devices
Compare two devices at the current time with live updates

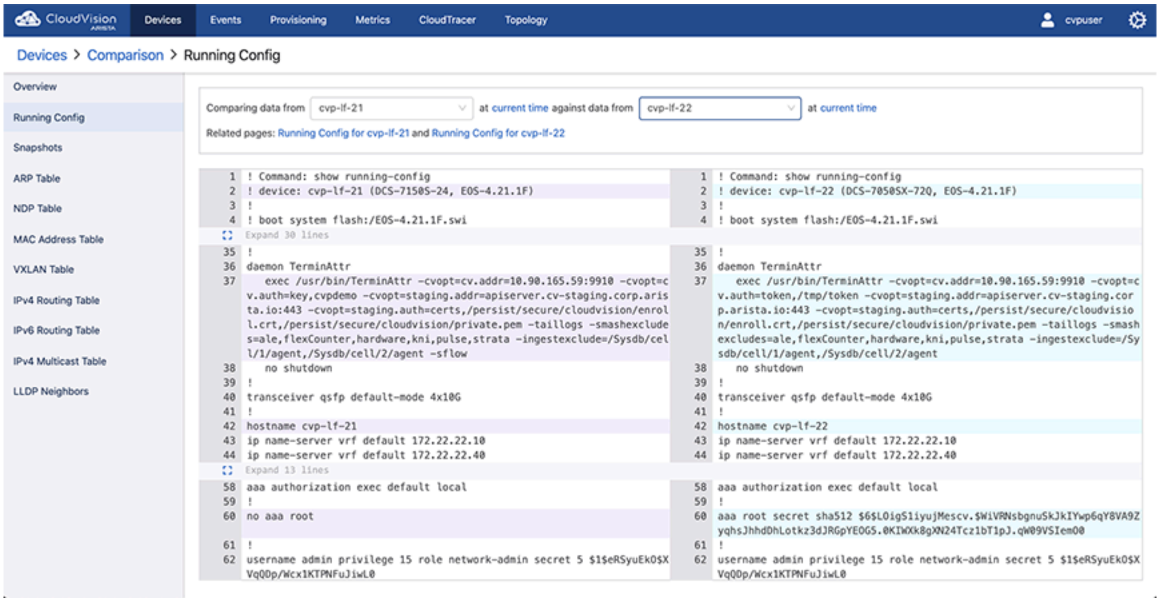
Two times
Compare the state of a single device at two chosen times

Advanced
Compare two devices at two chosen times

8.2 Running Configuration

To compare the data for the Running configuration for different devices, select **Running Config**. You have an option for current time comparison or chosen times comparison.

Figure 8-4: Comparison of Running configuration for two devices



Comparing data from cvp-lf-21 at current time against data from cvp-lf-22 at current time

Related pages: Running Config for cvp-lf-21 and Running Config for cvp-lf-22

```
! Command: show running-config
! device: cvp-lf-21 (DCS-7150S-24, EOS-4.21.1F)
!
! boot system flash:/EOS-4.21.1F.swi
!
daemon TerminAttr
   exec /usr/bin/TerminAttr -cvopt=cv.addr=10.90.165.59:9910 -cvopt=cv.auth=key,cvpdemo -cvopt=staging.addr=apiserver.cv-staging.corp.arista.io:443 -cvopt=staging.auth=certs,/persist/secure/cloudvision/enroll.crt,/persist/secure/cloudvision/private.pem -taillogs -smashexcludes=ale,flexCounter,hardware,kni,pulse,strata -ingestexclude=/Sysdb/cell/1/agent,/Sysdb/cell/2/agent -sflow
   no shutdown
!
transceiver qsfp default-mode 4x10G
!
hostname cvp-lf-21
ip name-server vrf default 172.22.22.10
ip name-server vrf default 172.22.22.40
aaa authorization exec default local
!
no aaa root
!
username admin privilege 15 role network-admin secret 5 $1$eRSyuEkO$XVqQDp/Wcx1KTPNFuJiwL0
```

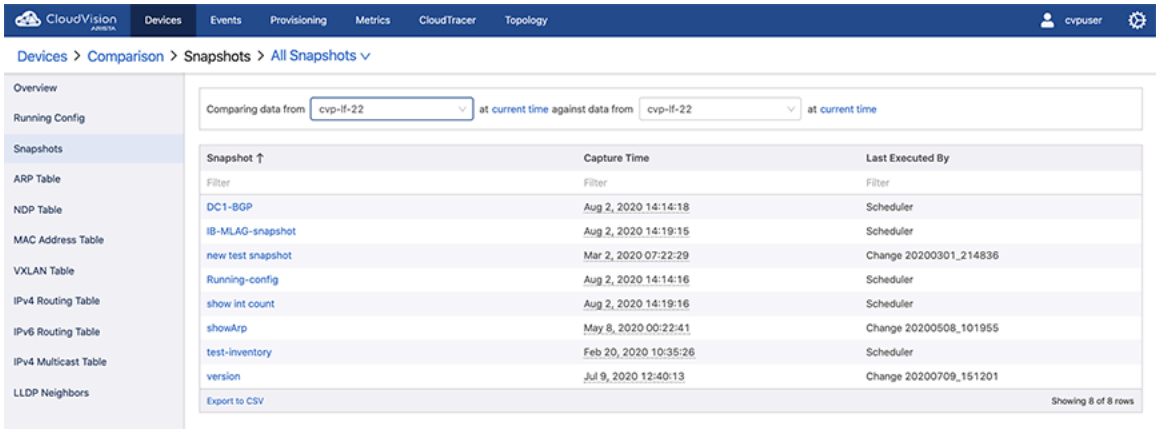
```
! Command: show running-config
! device: cvp-lf-22 (DCS-7050SX-72Q, EOS-4.21.1F)
!
! boot system flash:/EOS-4.21.1F.swi
!
daemon TerminAttr
   exec /usr/bin/TerminAttr -cvopt=cv.addr=10.90.165.59:9910 -cvopt=cv.auth=token,/tmp/token -cvopt=staging.addr=apiserver.cv-staging.corp.arista.io:443 -cvopt=staging.auth=certs,/persist/secure/cloudvision/enroll.crt,/persist/secure/cloudvision/private.pem -taillogs -smashexcludes=ale,flexCounter,hardware,kni,pulse,strata -ingestexclude=/Sysdb/cell/1/agent,/Sysdb/cell/2/agent
   no shutdown
!
transceiver qsfp default-mode 4x10G
!
hostname cvp-lf-22
ip name-server vrf default 172.22.22.10
ip name-server vrf default 172.22.22.40
aaa authorization exec default local
!
aaa root secret sha512 $6$LOigS1iyujMescv.$WiVRNsbgnuSkJkIYwp6qY8VA9ZyqhsJhhdDhLotkz3dJRGpYEOGS.0KIWXk8gXN24Tcz1bT1pJ.qW09VSIem00
!
username admin privilege 15 role network-admin secret 5 $1$eRSyuEkO$XVqQDp/Wcx1KTPNFuJiwL0
```

- Supported Snapshots

8.2.1 Supported Snapshots

All Snapshots give the list of snapshots, its capture time and its last executioner in the following figure.

Figure 8-5: All Snapshots options



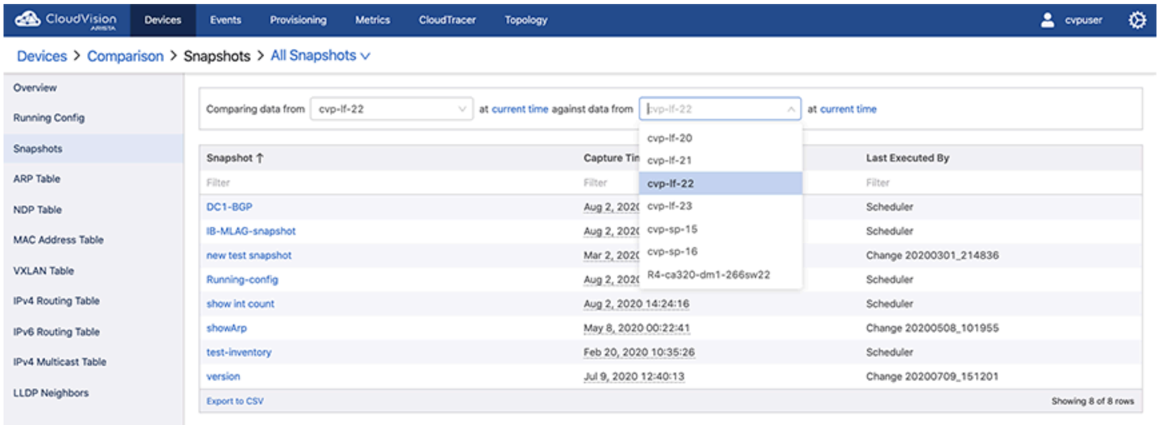
Comparing data from cvp-lf-22 at current time against data from cvp-lf-22 at current time

Snapshot ↑	Capture Time	Last Executed By
DC1-BGP	Aug 2, 2020 14:14:18	Scheduler
IB-MLAG-snapshot	Aug 2, 2020 14:19:15	Scheduler
new test snapshot	Mar 2, 2020 07:22:29	Change 20200301_214836
Running-config	Aug 2, 2020 14:14:16	Scheduler
show int count	Aug 2, 2020 14:19:16	Scheduler
showArp	May 8, 2020 00:22:41	Change 20200508_101955
test-inventory	Feb 20, 2020 10:35:26	Scheduler
version	Jul 9, 2020 12:40:13	Change 20200709_151201

8.3 Snapshots

On the CloudVision portal, navigate to **Devices > Comparison** to **Snapshots** to view the snapshot for the device.

Figure 8-6: Comparing snapshots



Comparing data from cvp-lf-22 at current time against data from cvp-lf-22 at current time

Snapshot ↑	Capture Tin	Last Executed By
Filter	Filter	Filter
DC1-BGP	Aug 2, 202	Scheduler
IB-MLAG-snapshot	Aug 2, 202	Scheduler
new test snapshot	Mar 2, 202	Change 20200301_214836
Running-config	Aug 2, 202	Scheduler
show int count	Aug 2, 2020 14:24:16	Scheduler
showArp	May 8, 2020 00:22:41	Change 20200508_101955
test-inventory	Feb 20, 2020 10:35:26	Scheduler
version	Jul 9, 2020 12:40:13	Change 20200709_151201

Showing 8 of 8 rows

The screen provides the following functionalities:

- All Snapshots: Displays all current snapshots options
- Snapshots Filter: Select the required snapshot filter

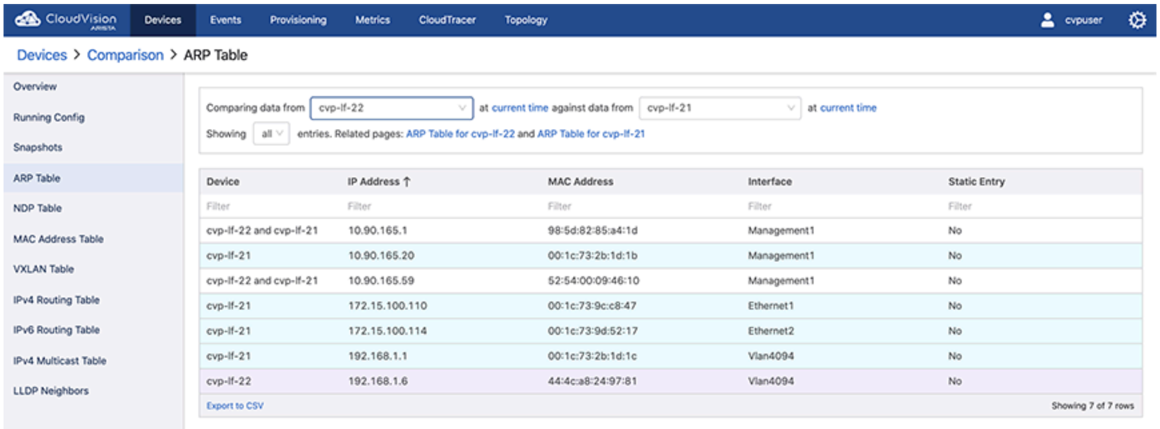
8.4 ARP Table

On the Cloud Vision portal, navigate to **Devices > Comparison** to ARP Table to view the information about ARP. Arista's device comparison platform for ARP table compares data between two devices at the same time and at different time settings.

You can compare the following:

- Device's IP Address
- Device's MAC Address
- Interface

Figure 8-7: Comparing ARP table



Comparing data from cvp-lf-22 at current time against data from cvp-lf-21 at current time

Showing all entries. Related pages: ARP Table for cvp-lf-22 and ARP Table for cvp-lf-21

Device	IP Address ↑	MAC Address	Interface	Static Entry
Filter	Filter	Filter	Filter	Filter
cvp-lf-22 and cvp-lf-21	10.90.165.1	98:5d:82:85:a4:1d	Management1	No
cvp-lf-21	10.90.165.20	00:1c:73:2b:1d:1b	Management1	No
cvp-lf-22 and cvp-lf-21	10.90.165.59	52:54:00:09:46:10	Management1	No
cvp-lf-21	172.15.100.110	00:1c:73:9c:c8:47	Ethernet1	No
cvp-lf-21	172.15.100.114	00:1c:73:9d:52:17	Ethernet2	No
cvp-lf-21	192.168.1.1	00:1c:73:2b:1d:1c	Vlan4094	No
cvp-lf-22	192.168.1.6	44:4c:a8:24:97:81	Vlan4094	No

Showing 7 of 7 rows

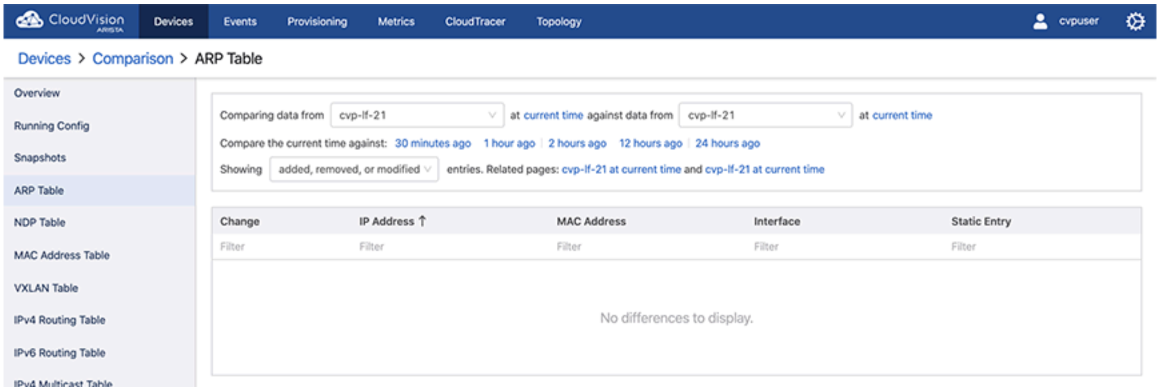
8.5 Comparing NDP Table

On the Cloud Vision portal, navigate to **Devices > Comparison** to NDP Table to view the information about NDP. Arista's device comparison platform for NDP table compares data between two devices at the same time and at different time settings.

The components of the comparison are as follows:

- Device's IP Address
- Device's MAC Address
- Interface
- Static entry

Figure 8-8: Comparing NDP table



Devices > Comparison > ARP Table

Comparing data from cvp-lf-21 at current time against data from cvp-lf-21 at current time

Compare the current time against: 30 minutes ago | 1 hour ago | 2 hours ago | 12 hours ago | 24 hours ago

Showing added, removed, or modified entries. Related pages: cvp-lf-21 at current time and cvp-lf-21 at current time

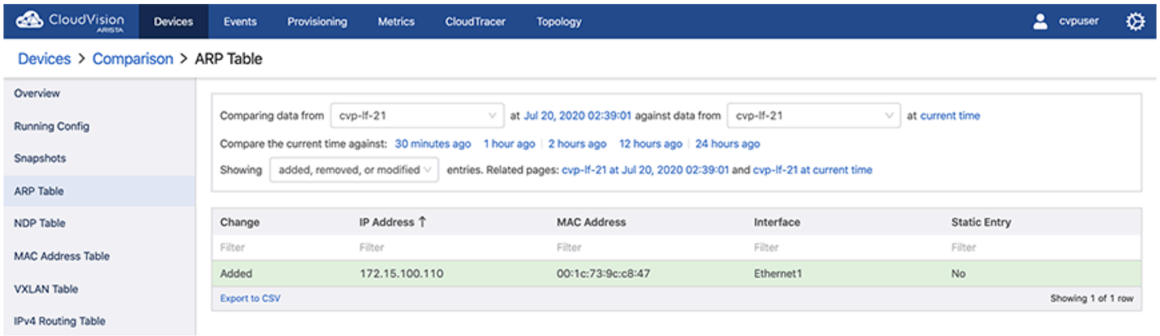
Change	IP Address ↑	MAC Address	Interface	Static Entry
Filter	Filter	Filter	Filter	Filter

No differences to display.

You can compare the status at the current time against the following times:

- 30 minutes
- 1 hour
- 2 hours
- 12 hours and
- 24 hours ago.

Figure 8-9: Comparing same device for NDP table for different times



Devices > Comparison > ARP Table

Comparing data from cvp-lf-21 at Jul 20, 2020 02:39:01 against data from cvp-lf-21 at current time

Compare the current time against: 30 minutes ago | 1 hour ago | 2 hours ago | 12 hours ago | 24 hours ago

Showing added, removed, or modified entries. Related pages: cvp-lf-21 at Jul 20, 2020 02:39:01 and cvp-lf-21 at current time

Change	IP Address ↑	MAC Address	Interface	Static Entry
Filter	Filter	Filter	Filter	Filter
Added	172.15.100.110	00:1c:73:9c:c8:47	Ethernet1	No

Export to CSV Showing 1 of 1 row

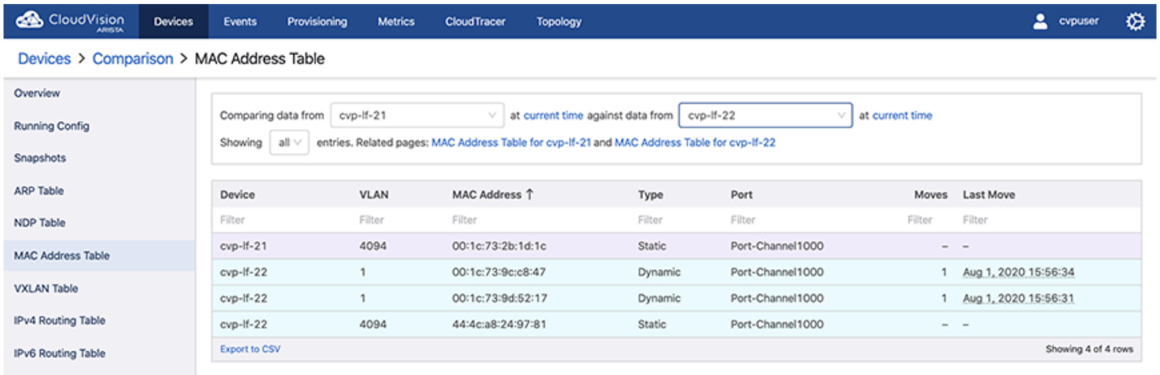
8.6 MAC Address Table

On the Cloud Vision portal, navigate to **Devices > Comparison** to MAC AddressTable to view the information about MAC addresses for the devices. Arista's device comparison platform for MAC Address table compares data between two devices at the same time and at different time settings.

The components of the comparison are as follows:

- VLAN
- Device's MAC Address
- Type of the VLAN
- Port
- Number of moves on the Port
- Timing for last movement

Figure 8-10: Comparing MAC Address table for current time for two devices



Devices > Comparison > MAC Address Table

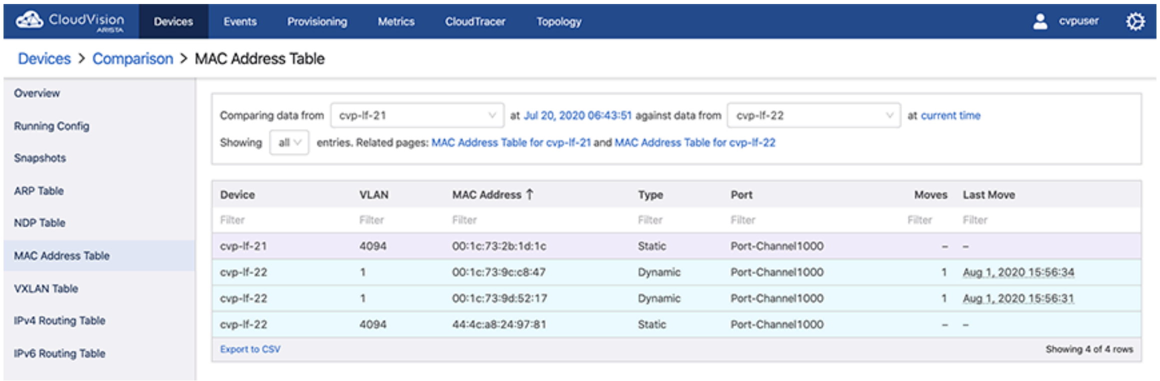
Comparing data from cvp-lf-21 at current time against data from cvp-lf-22 at current time

Showing all entries. Related pages: MAC Address Table for cvp-lf-21 and MAC Address Table for cvp-lf-22

Device	VLAN	MAC Address ↑	Type	Port	Moves	Last Move
cvp-lf-21	4094	00:1c:73:2b:1d:1c	Static	Port-Channel1000	–	–
cvp-lf-22	1	00:1c:73:9c:c8:47	Dynamic	Port-Channel1000	1	Aug 1, 2020 15:56:34
cvp-lf-22	1	00:1c:73:9d:52:17	Dynamic	Port-Channel1000	1	Aug 1, 2020 15:56:31
cvp-lf-22	4094	44:4c:a8:24:97:81	Static	Port-Channel1000	–	–

Showing 4 of 4 rows

Figure 8-11: Comparing MAC Address table for different times for two devices



Devices > Comparison > MAC Address Table

Comparing data from cvp-lf-21 at Jul 20, 2020 06:43:51 against data from cvp-lf-22 at current time

Showing all entries. Related pages: MAC Address Table for cvp-lf-21 and MAC Address Table for cvp-lf-22

Device	VLAN	MAC Address ↑	Type	Port	Moves	Last Move
cvp-lf-21	4094	00:1c:73:2b:1d:1c	Static	Port-Channel1000	–	–
cvp-lf-22	1	00:1c:73:9c:c8:47	Dynamic	Port-Channel1000	1	Aug 1, 2020 15:56:34
cvp-lf-22	1	00:1c:73:9d:52:17	Dynamic	Port-Channel1000	1	Aug 1, 2020 15:56:31
cvp-lf-22	4094	44:4c:a8:24:97:81	Static	Port-Channel1000	–	–

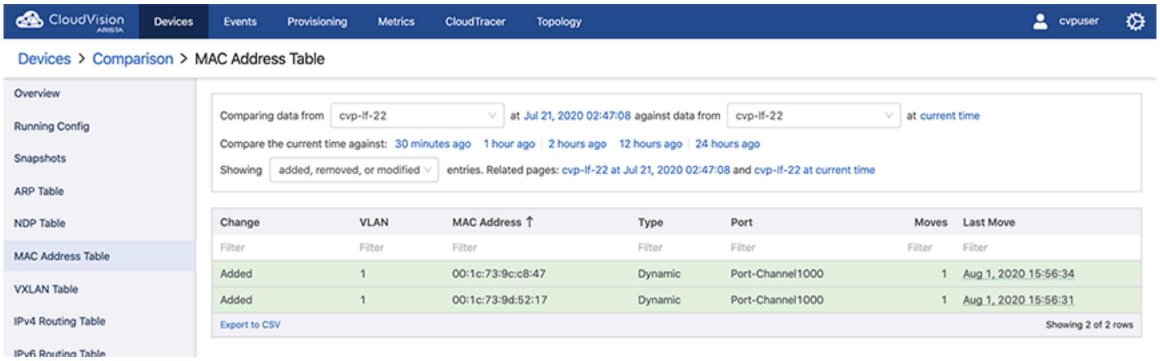
Showing 4 of 4 rows

You can compare the status at the current time against the following times:

- 30 minutes
- 1 hour
- 2 hours
- 12 hours and
- 24 hours ago.

Status is shown by added, removed and modified entries.

Figure 8-12: Comparing same device for different times and status



Devices > Comparison > MAC Address Table

Comparing data from cvp-lf-22 at Jul 21, 2020 02:47:08 against data from cvp-lf-22 at current time

Compare the current time against: 30 minutes ago | 1 hour ago | 2 hours ago | 12 hours ago | 24 hours ago

Showing added, removed, or modified entries. Related pages: cvp-lf-22 at Jul 21, 2020 02:47:08 and cvp-lf-22 at current time

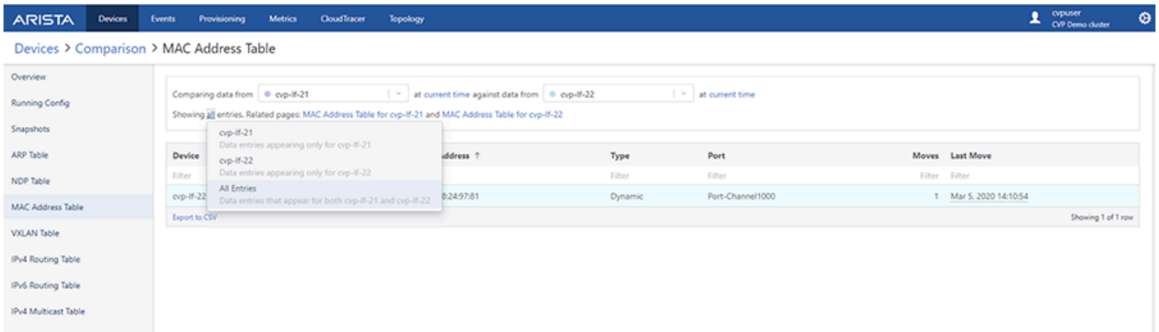
Change	VLAN	MAC Address ↑	Type	Port	Moves	Last Move
Filter	Filter	Filter	Filter	Filter	Filter	Filter
Added	1	00:1c:73:9c:c8:47	Dynamic	Port-Channel1000	1	Aug 1, 2020 15:56:34
Added	1	00:1c:73:9d:52:17	Dynamic	Port-Channel1000	1	Aug 1, 2020 15:56:31

Export to CSV

Showing 2 of 2 rows

To show all entries for the devices, Click ALL.

Figure 8-13: Showing all entries for the Devices for MAC Address table



Devices > Comparison > MAC Address Table

Comparing data from cvp-lf-21 at current time against data from cvp-lf-22 at current time

Showing all entries. Related pages: MAC Address Table for cvp-lf-21 and MAC Address Table for cvp-lf-22

cvp-lf-21
Data entries appearing only for cvp-lf-21
cvp-lf-22
Data entries appearing only for cvp-lf-22
All Entries
Data entries that appear for both cvp-lf-21 and cvp-lf-22

Device	ddress ↑	Type	Port	Moves	Last Move
Filter		Filter	Filter	Filter	Filter
cvp-lf-22	8:24:97:81	Dynamic	Port-Channel1000	1	Mar 5, 2020 14:10:54

Export to CSV

Showing 1 of 1 row

8.7 VXLAN Table

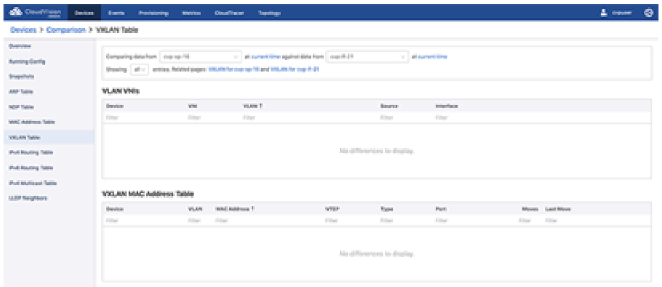
On the Cloud Vision portal, navigate to **Devices > Comparison** to VXLAN Table to view the information about MAC addresses for the devices.

The components of the comparison are as follows:

- VLAN VNIs

- VXLAN MAC Address

Figure 8-14: Comparing VXLAN table for current time for two devices



Comparing data from cvp-sp-16 at current time against data from cvp-lf-21 at current time

Showing all entries. Related pages: VXLAN for cvp-sp-16 and VXLAN for cvp-lf-21

VLAN VNIs

Device	VNI	VLAN ↑	Source	Interface
Filter	Filter	Filter	Filter	Filter

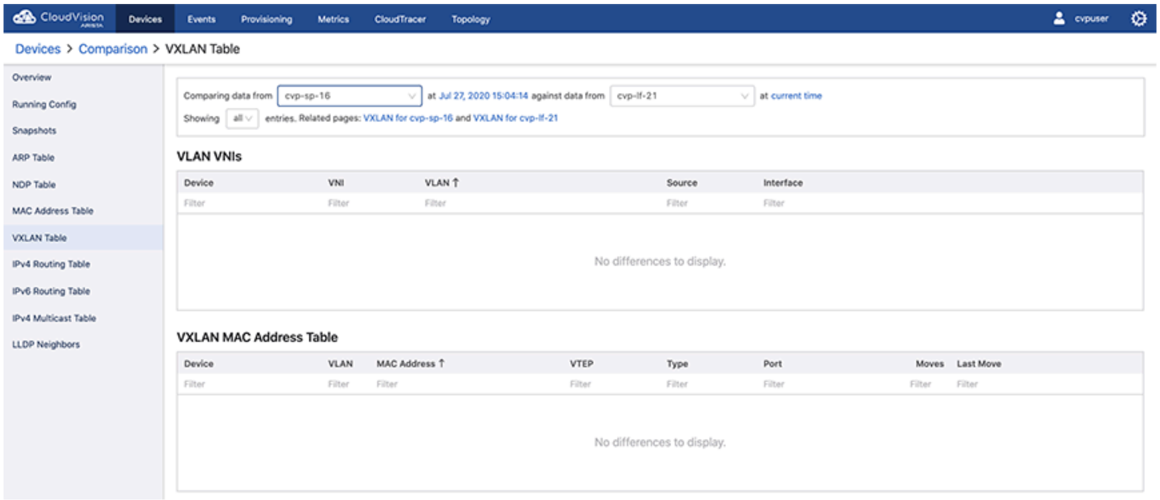
No differences to display.

VXLAN MAC Address Table

Device	VLAN	MAC Address ↑	VTEP	Type	Port	Moves	Last Move
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter

No differences to display.

Figure 8-15: Comparing VXLAN table for different times for two devices



Comparing data from cvp-sp-16 at Jul 27, 2020 15:04:14 against data from cvp-lf-21 at current time

Showing all entries. Related pages: VXLAN for cvp-sp-16 and VXLAN for cvp-lf-21

VLAN VNIs

Device	VNI	VLAN ↑	Source	Interface
Filter	Filter	Filter	Filter	Filter

No differences to display.

VXLAN MAC Address Table

Device	VLAN	MAC Address ↑	VTEP	Type	Port	Moves	Last Move
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter

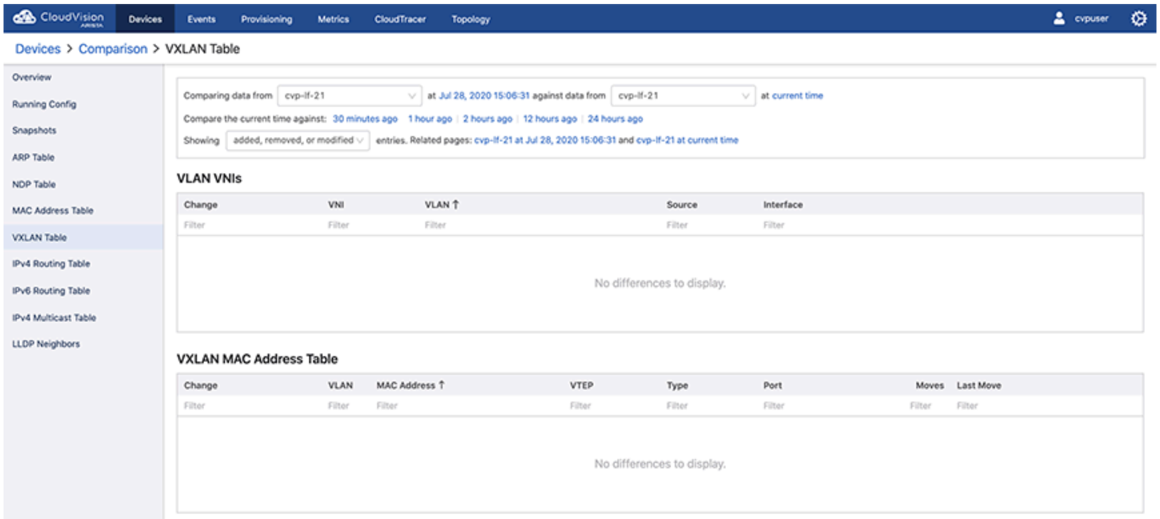
No differences to display.

You can compare the status at the current time against the following times:

- 30 minutes
- 1 hour
- 2 hours
- 12 hours and
- 24 hours ago.

Status is shown by added, removed and modified entries.

Figure 8-16: Comparing same device for different times and status



Devices > Comparison > VXLAN Table

Comparing data from cvp-lf-21 at Jul 28, 2020 15:06:31 against data from cvp-lf-21 at current time

Compare the current time against: 30 minutes ago | 1 hour ago | 2 hours ago | 12 hours ago | 24 hours ago

Showing added, removed, or modified entries. Related pages: cvp-lf-21 at Jul 28, 2020 15:06:31 and cvp-lf-21 at current time

VLAN VNIs

Change	VNI	VLAN ↑	Source	Interface
Filter	Filter	Filter	Filter	Filter

No differences to display.

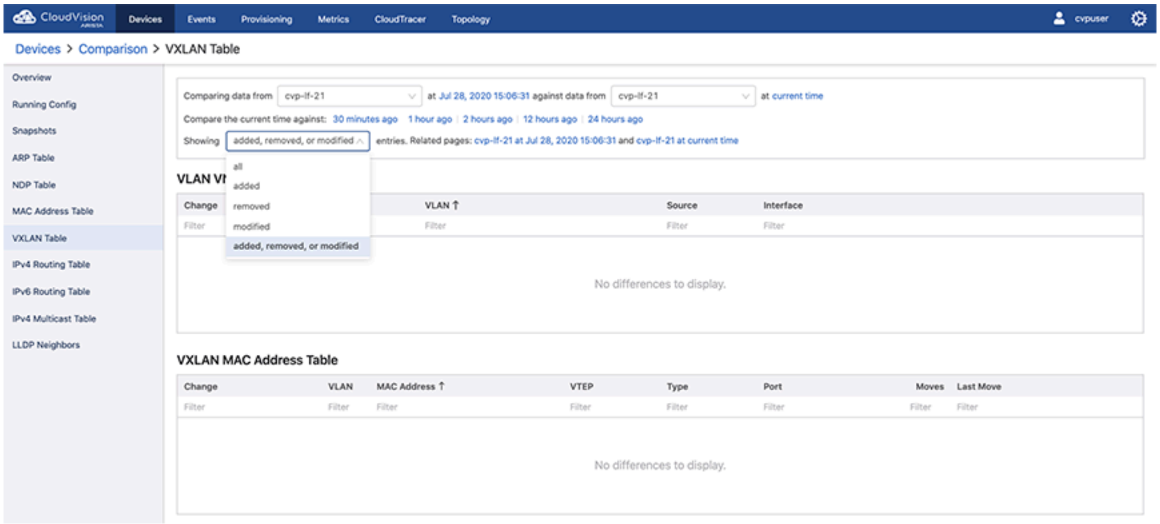
VXLAN MAC Address Table

Change	VLAN	MAC Address ↑	VTEP	Type	Port	Moves	Last Move
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter

No differences to display.

To show all entries for the devices, Click ALL.

Figure 8-17: Showing all entries for the Devices for VXLAN table



Devices > Comparison > VXLAN Table

Comparing data from cvp-lf-21 at Jul 28, 2020 15:06:31 against data from cvp-lf-21 at current time

Compare the current time against: 30 minutes ago | 1 hour ago | 2 hours ago | 12 hours ago | 24 hours ago

Showing added, removed, or modified entries. Related pages: cvp-lf-21 at Jul 28, 2020 15:06:31 and cvp-lf-21 at current time

VLAN VNIs

Change	VNI	VLAN ↑	Source	Interface
Filter	Filter	Filter	Filter	Filter

No differences to display.

VXLAN MAC Address Table

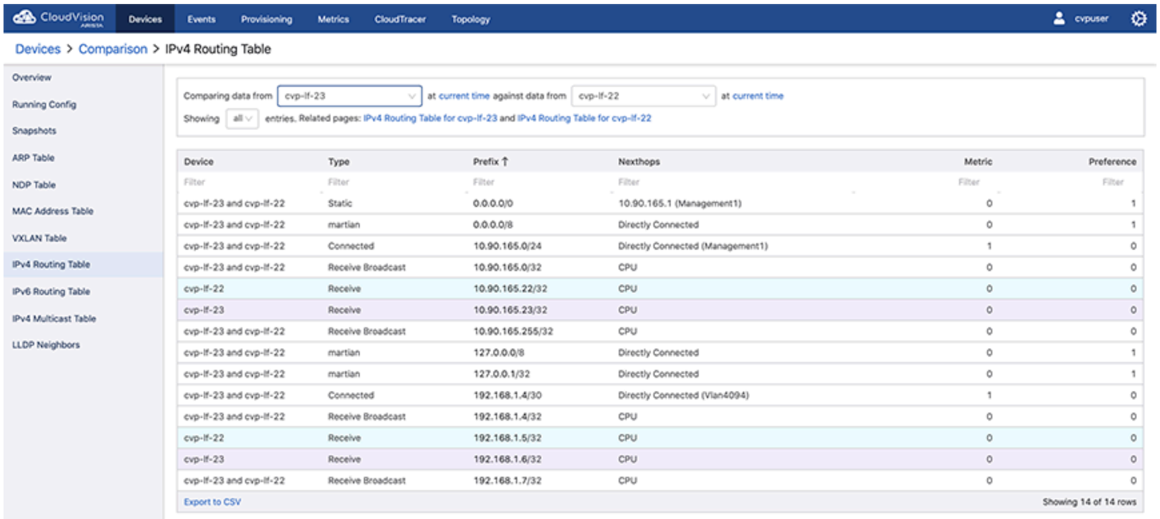
Change	VLAN	MAC Address ↑	VTEP	Type	Port	Moves	Last Move
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter

No differences to display.

8.8 Viewing Device IPv4 Routing Table

From the Comparison screen, you can quickly drill down to view details about IPv4 Routing from different devices. In tabular view, click the device names to compare the corresponding device details.

Figure 8-18: Comparing IPv4 routing table for different devices



Comparing data from cvp-lf-23 at current time against data from cvp-lf-22 at current time

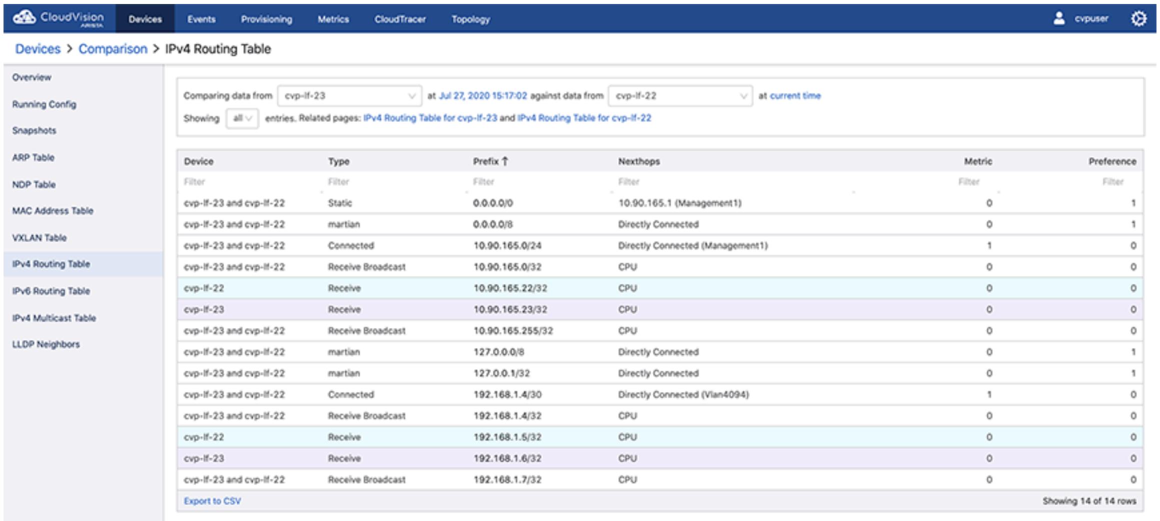
Showing all entries. Related pages: IPv4 Routing Table for cvp-lf-23 and IPv4 Routing Table for cvp-lf-22

Device	Type	Prefix ↑	Nexthops	Metric	Preference
Filter	Filter	Filter	Filter	Filter	Filter
cvp-lf-23 and cvp-lf-22	Static	0.0.0.0/0	10.90.165.1 (Management1)	0	1
cvp-lf-23 and cvp-lf-22	martian	0.0.0.0/8	Directly Connected	0	1
cvp-lf-23 and cvp-lf-22	Connected	10.90.165.0/24	Directly Connected (Management1)	1	0
cvp-lf-23 and cvp-lf-22	Receive Broadcast	10.90.165.0/32	CPU	0	0
cvp-lf-22	Receive	10.90.165.22/32	CPU	0	0
cvp-lf-23	Receive	10.90.165.23/32	CPU	0	0
cvp-lf-23 and cvp-lf-22	Receive Broadcast	10.90.165.255/32	CPU	0	0
cvp-lf-23 and cvp-lf-22	martian	127.0.0.0/8	Directly Connected	0	1
cvp-lf-23 and cvp-lf-22	martian	127.0.0.1/32	Directly Connected	0	1
cvp-lf-23 and cvp-lf-22	Connected	192.168.1.4/30	Directly Connected (Vlan4094)	1	0
cvp-lf-23 and cvp-lf-22	Receive Broadcast	192.168.1.4/32	CPU	0	0
cvp-lf-22	Receive	192.168.1.5/32	CPU	0	0
cvp-lf-23	Receive	192.168.1.6/32	CPU	0	0
cvp-lf-23 and cvp-lf-22	Receive Broadcast	192.168.1.7/32	CPU	0	0

Showing 14 of 14 rows

The screen refreshes to show the status, IP address and functions it does for Nexthop. Status is generally shown by Static, Martian, Connected, Receive and Receive Broadcast.

Figure 8-19: Comparing IPv4 Routing table for different times for two devices



Comparing data from cvp-lf-23 at Jul 27, 2020 15:17:02 against data from cvp-lf-22 at current time

Showing all entries. Related pages: IPv4 Routing Table for cvp-lf-23 and IPv4 Routing Table for cvp-lf-22

Device	Type	Prefix ↑	Nexthops	Metric	Preference
Filter	Filter	Filter	Filter	Filter	Filter
cvp-lf-23 and cvp-lf-22	Static	0.0.0.0/0	10.90.165.1 (Management1)	0	1
cvp-lf-23 and cvp-lf-22	martian	0.0.0.0/8	Directly Connected	0	1
cvp-lf-23 and cvp-lf-22	Connected	10.90.165.0/24	Directly Connected (Management1)	1	0
cvp-lf-23 and cvp-lf-22	Receive Broadcast	10.90.165.0/32	CPU	0	0
cvp-lf-22	Receive	10.90.165.22/32	CPU	0	0
cvp-lf-23	Receive	10.90.165.23/32	CPU	0	0
cvp-lf-23 and cvp-lf-22	Receive Broadcast	10.90.165.255/32	CPU	0	0
cvp-lf-23 and cvp-lf-22	martian	127.0.0.0/8	Directly Connected	0	1
cvp-lf-23 and cvp-lf-22	martian	127.0.0.1/32	Directly Connected	0	1
cvp-lf-23 and cvp-lf-22	Connected	192.168.1.4/30	Directly Connected (Vlan4094)	1	0
cvp-lf-23 and cvp-lf-22	Receive Broadcast	192.168.1.4/32	CPU	0	0
cvp-lf-22	Receive	192.168.1.5/32	CPU	0	0
cvp-lf-23	Receive	192.168.1.6/32	CPU	0	0
cvp-lf-23 and cvp-lf-22	Receive Broadcast	192.168.1.7/32	CPU	0	0

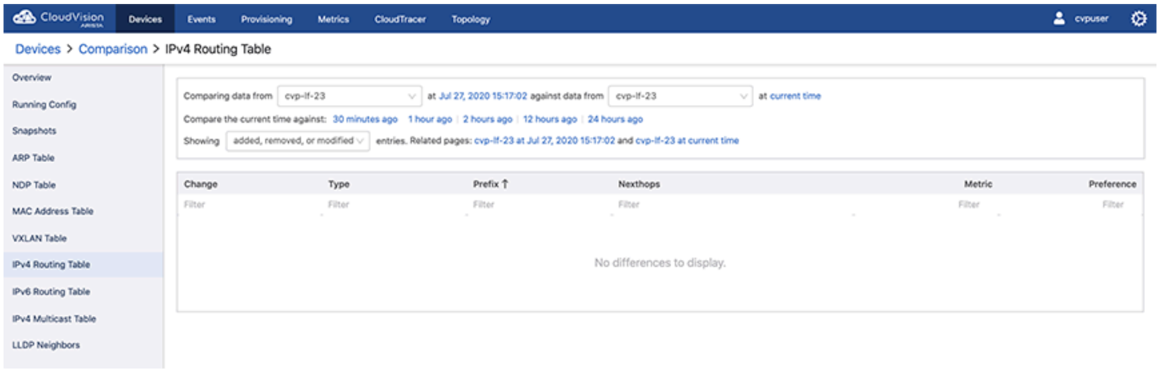
Showing 14 of 14 rows

You can compare the status at the current time against the following times:

- 30 minutes
- 1 hour
- 2 hours
- 12 hours and
- 24 hours ago.

Status is shown by added, removed and modified entries.

Figure 8-20: Comparing same device for different times and status



Comparing data from cvp-lf-23 at Jul 27, 2020 15:17:02 against data from cvp-lf-23 at current time

Compare the current time against: 30 minutes ago | 1 hour ago | 2 hours ago | 12 hours ago | 24 hours ago

Showing added, removed, or modified entries. Related pages: cvp-lf-23 at Jul 27, 2020 15:17:02 and cvp-lf-23 at current time

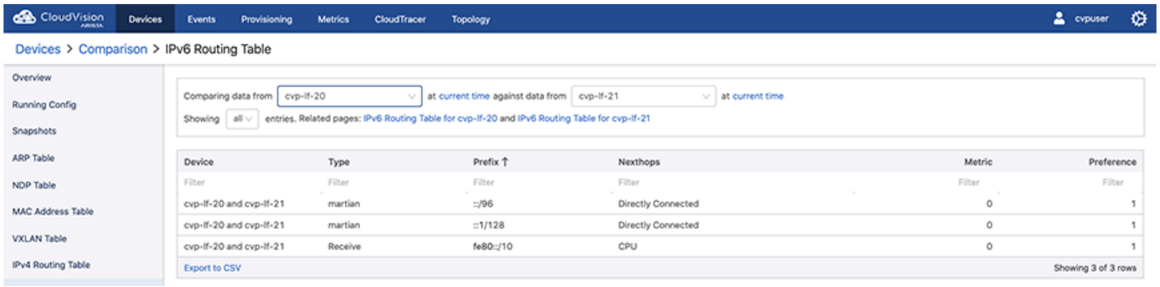
Change	Type	Prefix ↑	Nexthops	Metric	Preference
Filter	Filter	Filter	Filter	Filter	Filter

No differences to display.

8.9 Viewing Device IPv6 Routing Table

From the Comparison screen, you can quickly drill down to view details about IPv6 Routing from different devices. In tabular view, click the device names to compare the corresponding device details.

Figure 8-21: Comparing IPv6 routing table for different devices



Comparing data from cvp-lf-20 at current time against data from cvp-lf-21 at current time

Showing all entries. Related pages: IPv6 Routing Table for cvp-lf-20 and IPv6 Routing Table for cvp-lf-21

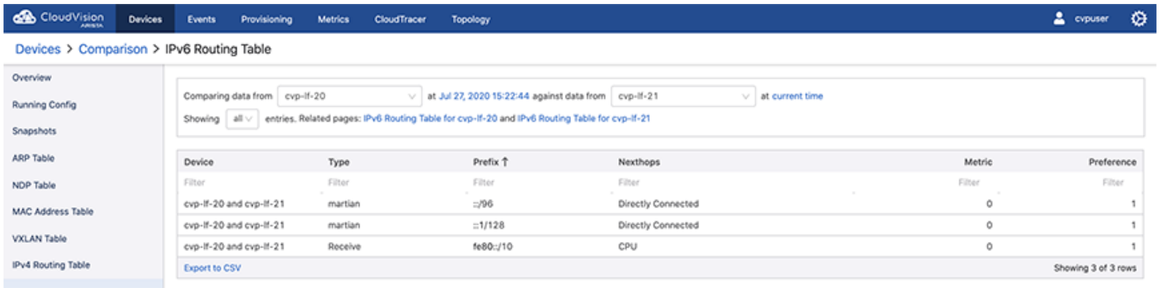
Device	Type	Prefix ↑	Nexthops	Metric	Preference
Filter	Filter	Filter	Filter	Filter	Filter
cvp-lf-20 and cvp-lf-21	martian	::/96	Directly Connected	0	1
cvp-lf-20 and cvp-lf-21	martian	::1/128	Directly Connected	0	1
cvp-lf-20 and cvp-lf-21	Receive	fe80::/10	CPU	0	1

Export to CSV

Showing 3 of 3 rows

The screen refreshes to show the status, IP address and functions it does for Nexthop. Status is generally shown by Static, Martian, Connected, Receive and Receive Broadcast.

Figure 8-22: Comparing IPv6 Routing table for different times for two devices



Comparing data from cvp-lf-20 at Jul 27, 2020 15:22:44 against data from cvp-lf-21 at current time

Showing all entries. Related pages: IPv6 Routing Table for cvp-lf-20 and IPv6 Routing Table for cvp-lf-21

Device	Type	Prefix ↑	Nexthops	Metric	Preference
Filter	Filter	Filter	Filter	Filter	Filter
cvp-lf-20 and cvp-lf-21	martian	::/96	Directly Connected	0	1
cvp-lf-20 and cvp-lf-21	martian	::1/128	Directly Connected	0	1
cvp-lf-20 and cvp-lf-21	Receive	fe80::/10	CPU	0	1

Export to CSV

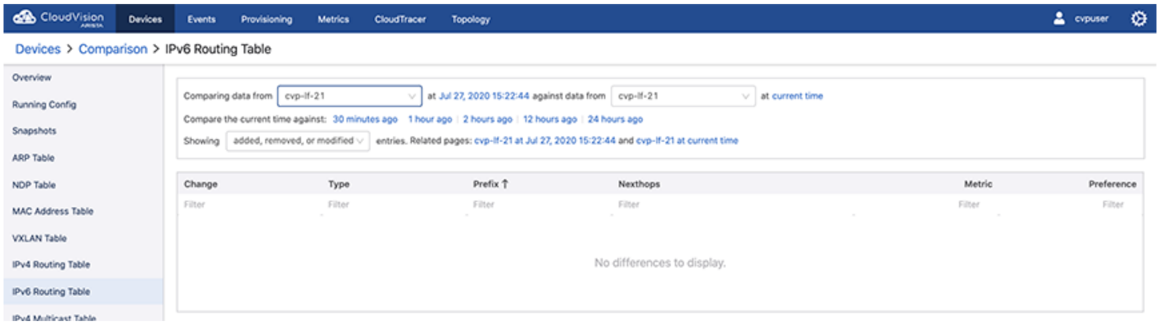
Showing 3 of 3 rows

You can compare the status at the current time against the following times:

- 30 minutes
- 1 hour
- 2 hours
- 12 hours and
- 24 hours ago.

Status is shown by added, removed and modified entries.

Figure 8-23: Comparing same device for different times and status



Devices > Comparison > IPv6 Routing Table

Comparing data from cvp-lf-21 at Jul 27, 2020 15:22:44 against data from cvp-lf-21 at current time

Compare the current time against: 30 minutes ago | 1 hour ago | 2 hours ago | 12 hours ago | 24 hours ago

Showing added, removed, or modified entries. Related pages: cvp-lf-21 at Jul 27, 2020 15:22:44 and cvp-lf-21 at current time

Change	Type	Prefix ↑	Nexthops	Metric	Preference
Filter	Filter	Filter	Filter	Filter	Filter

No differences to display.

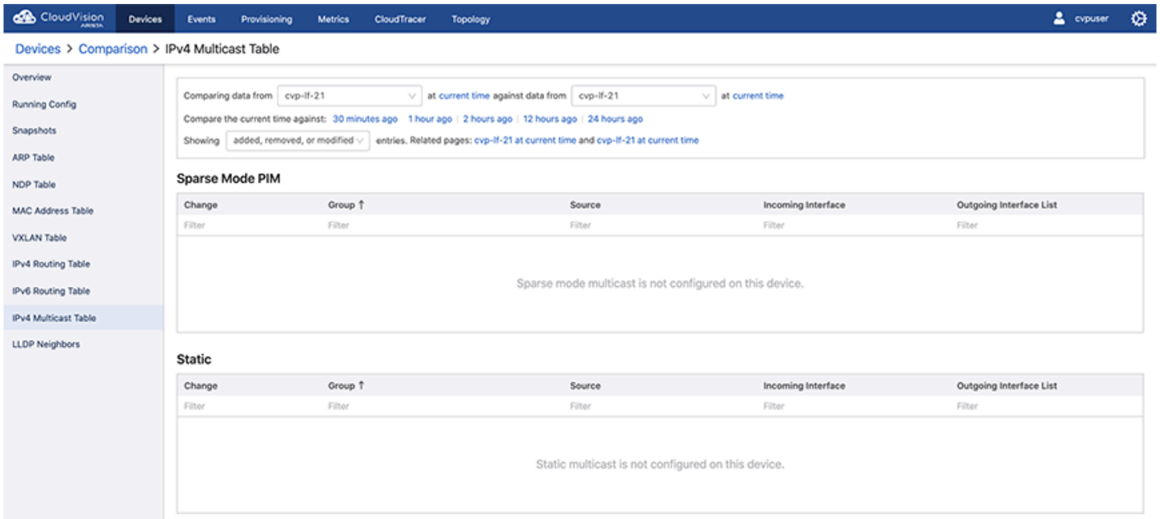
8.10 Comparing IPv4 Multicast Table

On the Cloud Vision portal, navigate to **Devices > Comparison to IPv4 Multicast Table** to view the information about Multicast. Arista's device comparison platform for IPv4 Multicast table compares data between two devices at the same time and at different time settings.

The components of the comparison are as follows:

- Sparse Mode PIM
- Static

Figure 8-24: Comparing IPv4 Multicast table



Devices > Comparison > IPv4 Multicast Table

Comparing data from cvp-lf-21 at current time against data from cvp-lf-21 at current time

Compare the current time against: 30 minutes ago | 1 hour ago | 2 hours ago | 12 hours ago | 24 hours ago

Showing added, removed, or modified entries. Related pages: cvp-lf-21 at current time and cvp-lf-21 at current time

Sparse Mode PIM

Change	Group ↑	Source	Incoming Interface	Outgoing Interface List
Filter	Filter	Filter	Filter	Filter

Sparse mode multicast is not configured on this device.

Static

Change	Group ↑	Source	Incoming Interface	Outgoing Interface List
Filter	Filter	Filter	Filter	Filter

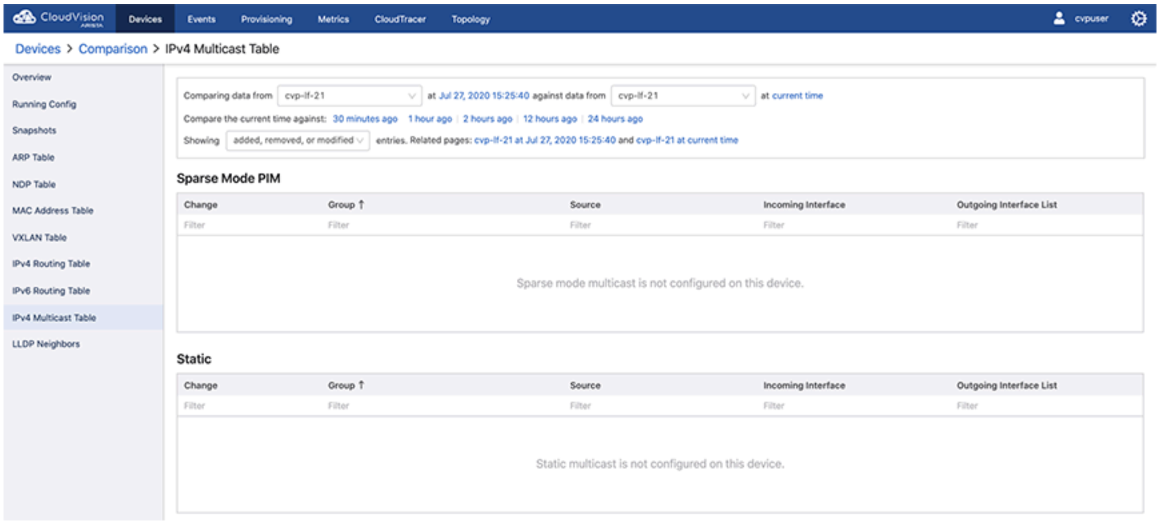
Static multicast is not configured on this device.

You can compare the status at the current time against the following times:

- 30 minutes
- 1 hour
- 2 hours
- 12 hours and

- 24 hours ago.

Figure 8-25: Comparing same device for IPv4 Multicast table for different times



Comparing data from cvp-lf-21 at Jul 27, 2020 15:25:40 against data from cvp-lf-21 at current time

Compare the current time against: 30 minutes ago | 1 hour ago | 2 hours ago | 12 hours ago | 24 hours ago

Showing added, removed, or modified entries. Related pages: cvp-lf-21 at Jul 27, 2020 15:25:40 and cvp-lf-21 at current time

Sparse Mode PIM

Change	Group ↑	Source	Incoming Interface	Outgoing Interface List
Filter	Filter	Filter	Filter	Filter

Sparse mode multicast is not configured on this device.

Static

Change	Group ↑	Source	Incoming Interface	Outgoing Interface List
Filter	Filter	Filter	Filter	Filter

Static multicast is not configured on this device.

Chapter 9

Network Compliance (CVP)

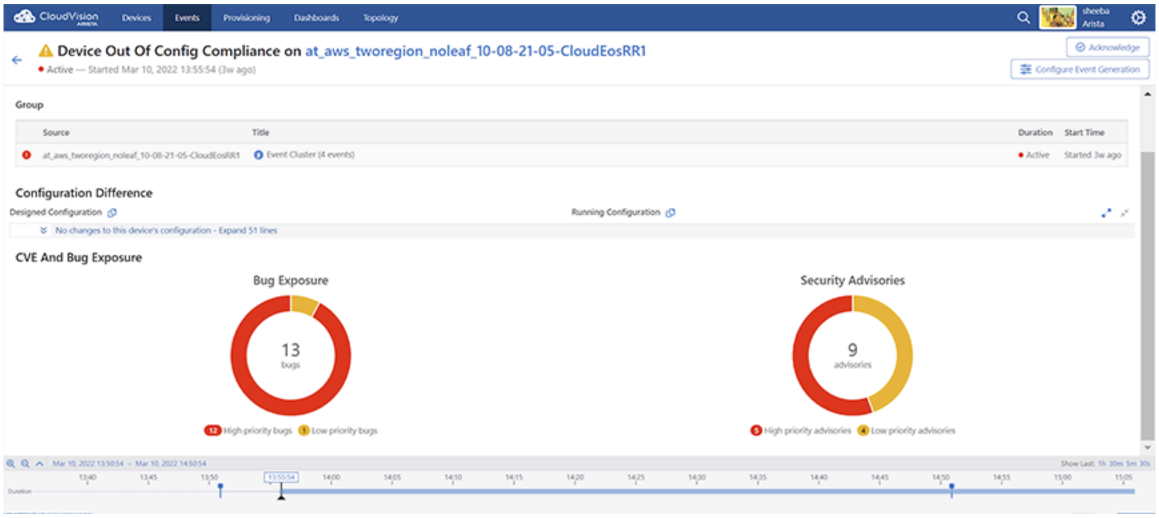
CloudVision continuously computes image and configuration compliances. If a device is either configuration, image, or extension non-compliant, CVP automatically generates a non-compliant event on the **Compliance** dashboard and flags the device as non-compliant on the **Inventory** screen.

Note: The event layout displays the running and designed configuration, related information about the device compliance, and the device bug/security advisory exposure.

A device configuration compliance is triggered in the following circumstances:

- A configlet is assigned to either a device or Container
- Configlet content changes affect all devices to which the configlet has been mapped
- A device restarts streaming after you make the changes mentioned above
- A device is edited

Figure 9-1: Device Out of Config Compliance Event



Device Out Of Config Compliance on at_aws_tworegion_noleaf_10-08-21-05-CloudEosRR1

● Active — Started Mar 10, 2022 13:55:54 (3w ago)

Group

Source	Title	Duration	Start Time
at_aws_tworegion_noleaf_10-08-21-05-CloudEosRR1	Event Cluster (4 events)	● Active	Started 3w ago

Configuration Difference

Designed Configuration | Running Configuration

No changes to this device's configuration - Expand 51 lines

CVE And Bug Exposure

Bug Exposure: 13 bugs — 12 High priority bugs, 1 Low priority bugs

Security Advisories: 9 advisories — 5 High priority advisories, 4 Low priority advisories

Compliance statuses of image and switch configuration are computed when the following entities are edited:

- Running or designed configurations
- Extensions or EOS versions

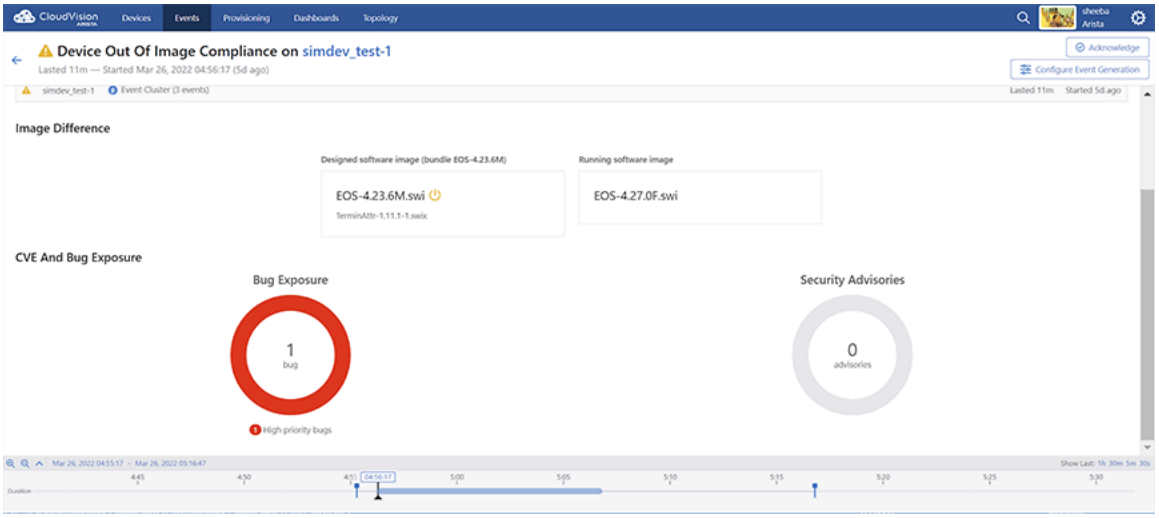
Note: The compliance status of device and parent container icons update automatically.

An image configuration compliance is triggered in the following circumstances:

- An image bundle is either applied or removed from either device or container
- An image bundle content is edited
- EOS version is edited

- EOS image version changes due to an image upgrade or downgrade

Figure 9-2: Device Out of Image Compliance Event



Device Out Of Image Compliance on simdev_test-1

Lasted 11m — Started Mar 26, 2022 04:56:17 (5d ago)

simdev_test-1 Event Cluster (3 events) Lasted 11m Started 5d ago

Image Difference

Designed software image (bundle EOS-4.23.6M): EOS-4.23.6M.swi TerminAttr-1.11.1-1.swix

Running software image: EOS-4.27.0F.swi

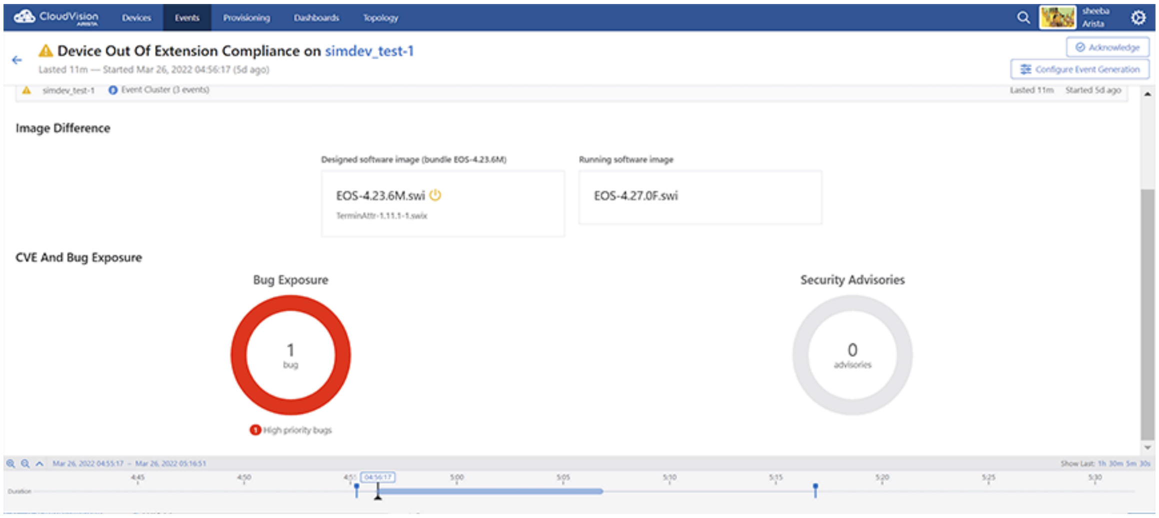
CVE And Bug Exposure

Bug Exposure: 1 bug — 1 High priority bugs

Security Advisories: 0 advisories

An extension configuration compliance is triggered when extensions are edited.

Figure 9-3: Device Out of Extension Compliance Event



Device Out Of Extension Compliance on simdev_test-1

Lasted 11m — Started Mar 26, 2022 04:56:17 (5d ago)

simdev_test-1 Event Cluster (3 events) Lasted 11m Started 5d ago

Image Difference

Designed software image (bundle EOS-4.23.6M): EOS-4.23.6M.swi TerminAttr-1.11.1-1.swix

Running software image: EOS-4.27.0F.swi

CVE And Bug Exposure

Bug Exposure: 1 bug — 1 High priority bugs

Security Advisories: 0 advisories

The Compliance Overview dashboard from the **Devices** tab presents the number of devices and their compliance status in the following categories:

- Bug Exposure
- Security Advisories
- Configuration Compliance
- Image Compliance

Sections in this chapter include:

- Device Compliance
- Notifications for Container-level Compliance Checks and Reconciles
- Compliance Dashboard
- Print Compliance Dashboard
- Setup for Automatic Sync of Compliance Bug Database

9.1 Device Compliance

In CloudVision Portal (CVP), devices have a compliance status which indicates whether the running configuration and image of a device is different from the designed (managed) configuration and image for the device.

The possible device compliance statuses are:

- **Compliant:** Devices in which the running configuration and image are identical to the designed configuration and image for the device.
- **Non-compliant:** Devices in which the running configuration or image are different from the designed configuration or image for the device

When you edit running and designed configurations of provisioned devices, CloudVision automatically computes the difference and updates the compliance status in response to changes in the network. CVP provides device compliance status indicators to easily identify non-compliant devices and the functionality required to bring non-compliant devices into compliance. One process used to resolve the difference in running and designed configuration is referred to as reconciling.

For more information, see:

- Device Compliance Status Indicators
- Device Compliance Checks

9.1.1 Device Compliance Status Indicators

CloudVision Portal (CVP) provides device compliance status information in both the **Network Provisioning** screen and the **Inventory** screen (list view).

9.1.1.1 Network Provisioning Screen Compliance Status Indicators

The **Network Provisioning** screen (topology view) utilizes color coding to indicate the presence of compliance alerts on devices. A compliance alert on a device indicates that the running configuration or image is different from the designed configuration or image for the device. This feature enables you to easily see if a device has a compliance alert.

In addition to using color codes for device icons, CVP also uses color codes for container icons to indicate that a device within the container has a compliance alert. If a device within a container has an active alert, the container inherits the alert color of the device. For example, if a device within a container has a configuration mismatch, the container inherits the alert color used to indicate a configuration mismatch.

This feature enables you to easily see if a device within a container has an alert, even if the device is not visible. It also prevents you from having to open a container to see if a device within it has an alert.

Note: Containers only inherit the alert color of a device if the device is directly underneath the container in the hierarchy. If the device is not directly underneath the container in the hierarchy, the container does not show the alert notification color of the device.

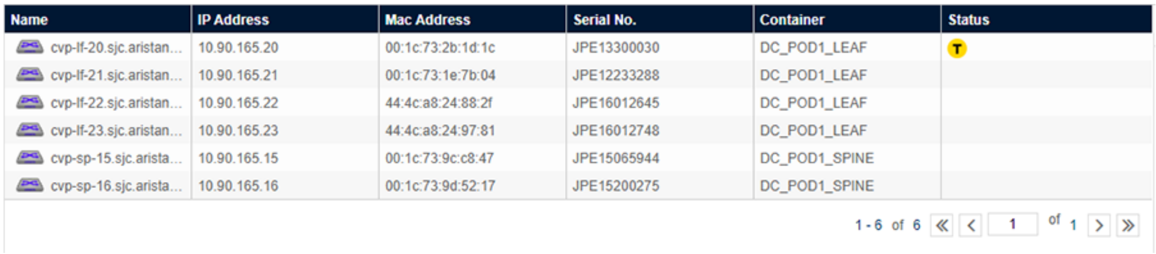
For descriptions of the color codes used to indicate compliance status, see:

- Device Icon Compliance Status Color Codes
- Container Icon Compliance Status Color Codes

9.1.1.2 Representation Under Show All Devices

The image below shows the representation of device compliance status information for devices that are only visible by accessing **Show all devices**. The statuses shown are the same as those shown using device icons in the topology view.

Figure 9-4: Show All Devices display of device compliance status

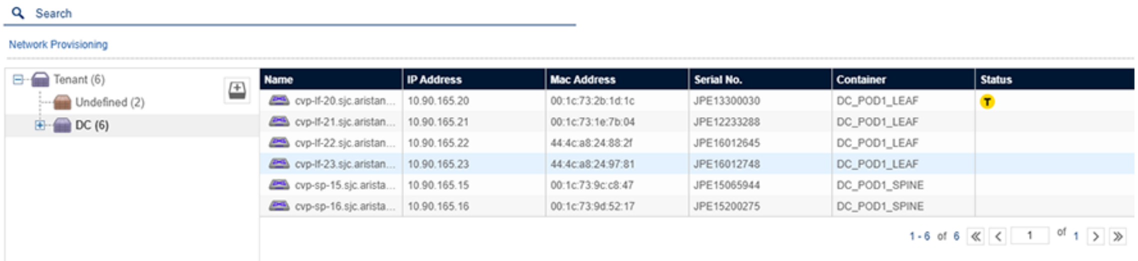


Name	IP Address	Mac Address	Serial No.	Container	Status
cvp-lf-20.sjc.aristan...	10.90.165.20	00:1c:73:2b:1d:1c	JPE13300030	DC_POD1_LEAF	T
cvp-lf-21.sjc.aristan...	10.90.165.21	00:1c:73:1e:7b:04	JPE12233288	DC_POD1_LEAF	
cvp-lf-22.sjc.aristan...	10.90.165.22	44:4c:a8:24:88:2f	JPE16012645	DC_POD1_LEAF	
cvp-lf-23.sjc.aristan...	10.90.165.23	44:4c:a8:24:97:81	JPE16012748	DC_POD1_LEAF	
cvp-sp-15.sjc.arista...	10.90.165.15	00:1c:73:9c:c8:47	JPE15065944	DC_POD1_SPINE	
cvp-sp-16.sjc.arista...	10.90.165.16	00:1c:73:9d:52:17	JPE15200275	DC_POD1_SPINE	

9.1.1.3 Representation in List View

The image below shows the representation of device compliance status information when using the **List View**. The statuses shown are the same as those shown using device icons in the **Topology** view.

Figure 9-5: List View display of device compliance status



Name	IP Address	Mac Address	Serial No.	Container	Status
cvp-lf-20.sjc.aristan...	10.90.165.20	00:1c:73:2b:1d:1c	JPE13300030	DC_POD1_LEAF	T
cvp-lf-21.sjc.aristan...	10.90.165.21	00:1c:73:1e:7b:04	JPE12233288	DC_POD1_LEAF	
cvp-lf-22.sjc.aristan...	10.90.165.22	44:4c:a8:24:88:2f	JPE16012645	DC_POD1_LEAF	
cvp-lf-23.sjc.aristan...	10.90.165.23	44:4c:a8:24:97:81	JPE16012748	DC_POD1_LEAF	
cvp-sp-15.sjc.arista...	10.90.165.15	00:1c:73:9c:c8:47	JPE15065944	DC_POD1_SPINE	
cvp-sp-16.sjc.arista...	10.90.165.16	00:1c:73:9d:52:17	JPE15200275	DC_POD1_SPINE	

9.1.1.4 Removing Compliance Indicators

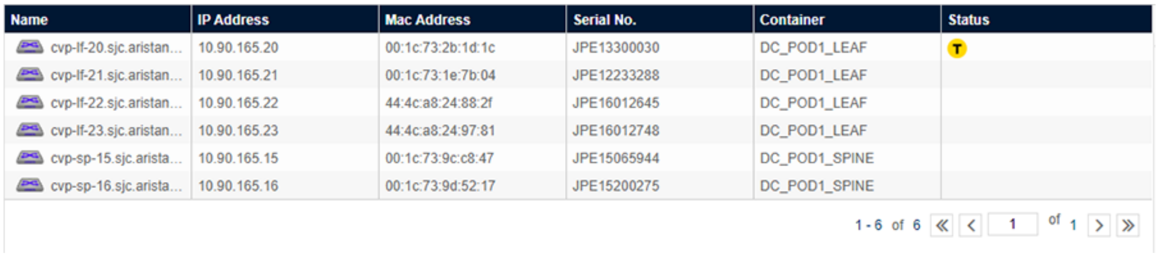
The **Network Provisioning** screen shows non-compliance whenever there is a mismatch between the running configuration or image and designed configuration or image of devices in the topology. To remove compliance indicators, reconcile the configuration of any devices that have a configuration mismatch.

Note: Compliance indicators are removed from the display only when there is no configuration mismatch.

9.1.1.5 Representation Under Show All Devices

The image below shows the representation of device compliance status information for devices that are only visible by accessing **Show all devices**. The statuses shown are the same as those shown using device icons in the topology view.

Figure 9-6: Show All Devices display of device compliance status



Name	IP Address	Mac Address	Serial No.	Container	Status
cvp-lf-20.sjc.aristan...	10.90.165.20	00:1c:73:2b:1d:1c	JPE13300030	DC_POD1_LEAF	T
cvp-lf-21.sjc.aristan...	10.90.165.21	00:1c:73:1e:7b:04	JPE12233288	DC_POD1_LEAF	
cvp-lf-22.sjc.aristan...	10.90.165.22	44:4c:a8:24:88:2f	JPE16012645	DC_POD1_LEAF	
cvp-lf-23.sjc.aristan...	10.90.165.23	44:4c:a8:24:97:81	JPE16012748	DC_POD1_LEAF	
cvp-sp-15.sjc.arista...	10.90.165.15	00:1c:73:9c:c8:47	JPE15065944	DC_POD1_SPINE	
cvp-sp-16.sjc.arista...	10.90.165.16	00:1c:73:9d:52:17	JPE15200275	DC_POD1_SPINE	

1 - 6 of 6 « < 1 of 1 > »

9.1.1.6 Device Icon Compliance Status Color Codes

The color of the device icon indicates the compliance status of the device. This table lists and describes the device icon color codes:

Icon	Description
	Gray The compliance status is normal (no compliance alert).
	Orange (no task) The device has a configuration mismatch (the running configuration or image are different from the designed configuration or image for the device). No task to resolve the mismatch is associated with the device.
T	**Orange (with task)** The device has a configuration mismatch (the running configuration or image are different from the designed configuration or image for the device). A task to resolve the mismatch is associated with the device.

See Representation Under Show All Devices for how this status is shown when using the **Show All Devices** option.

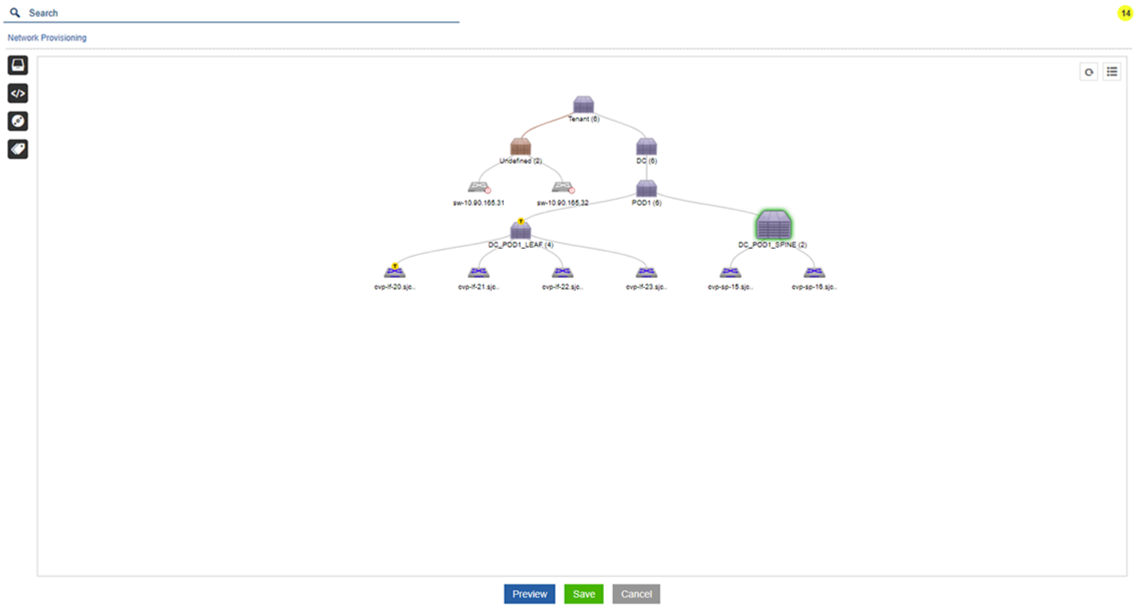
9.1.1.7 Container Icon Compliance Status Color Codes

The figure below shows a container that has a device within it that has an alert. In this example, the alert color is yellow, which indicates one of the following:

- A device within the container has a configuration mismatch.

- A device within the container has a configuration mismatch, and there is a task associated with the device to resolve the mismatch.

Figure 9-7: Container showing alert color



9.1.2 Device Compliance Checks

CloudVision Portal (CVP) enables you to see if devices are non-compliant by performing compliance checks at the device level and at the container level.

9.1.3 Device Access Alerts

The **Network Provisioning** screen shows device access alerts whenever a device is no longer reachable by CVP. This enables you to easily identify unreachable devices in the screen. Any device that is no longer reachable is represented on the screen using a color coded device icon.

This table lists and describes the color codes used for unreachable devices:

Icon	Description
🟥	**Red** The device is unreachable (CVP cannot connect to the device).

Like device compliance status alerts, CVP also uses color codes for container icons to indicate that a device within the container is unreachable. If a device within a container has an access alert, the container inherits the alert color of the device (red).

This feature enables you to easily see if a device within a container has an alert, even if the device is not visible. It also prevents you from having to open a container to see if a device within it has an alert.

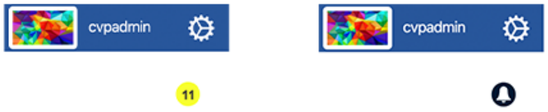
Note: Containers only inherit the alert color of a device if the device is directly underneath the container in the hierarchy. If the device is not directly underneath the container in the hierarchy, the container does not show the alert notification color of the device.

9.2 Notifications for Container-level Compliance Checks and Reconciles

CloudVision Portal (CVP) provides notifications for container-level compliance checks and reconciles. When a container-level compliance check or reconcile is completed, CVP automatically generates a notification message, indicating that the action has occurred.

Because container-level compliance check or reconciles are not tracked by tasks, you track them using automated notifications. The notifications can be accessed directly from the **Network Provisioning** screen by clicking the **Notifications** icon. The presentation of the icon indicates whether there are unread notifications.

Figure 9-8: Read and Unread Notification Icons

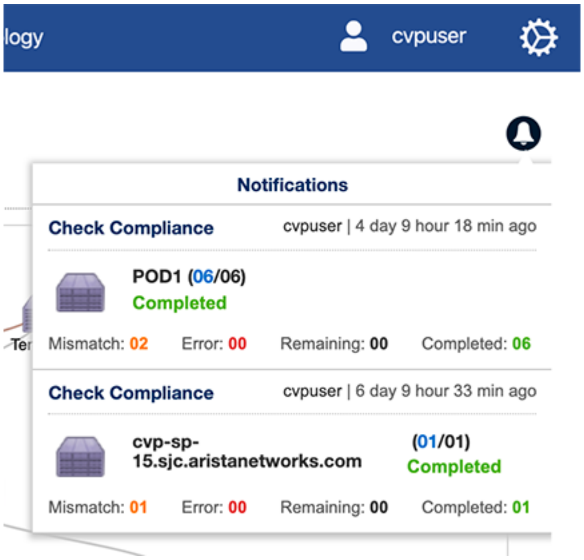


The notification list provides the following information:

- Current actions in progress, with a progress bar.
- Unread notifications (shaded in blue).
- Previously viewed notifications (no shading). These are shown at the bottom of the list.

The type of action (Check **Compliance** or **Reconcile**) is indicated for each notification.

Figure 9-9: List of Notifications



Notifications

Check Compliance cvpuser | 4 day 9 hour 18 min ago

POD1 (06/06)
Completed

Mismatch: 02 Error: 00 Remaining: 00 Completed: 06

Check Compliance cvpuser | 6 day 9 hour 33 min ago

cvp-sp-15.sjc.aristanetworks.com (01/01)
Completed

Mismatch: 01 Error: 00 Remaining: 00 Completed: 01

Note: To view notifications for the previous CVP session, click the bell icon and choose **View History**.

For information on container-level compliance checks and reconciles, see:

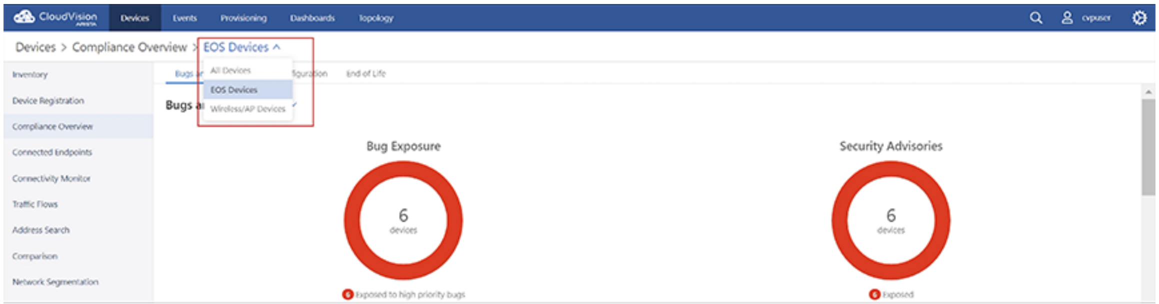
- Device Compliance Checks

9.3 Compliance Dashboard

When you edit running and designed configurations of provisioned devices, CloudVision automatically computes the difference and updates the compliance status in response to changes in the network.

The Compliance dashboard displays the real-time summary view of image, configuration, and security compliances for all managed devices. You can filter devices using **All Devices**, **EOS Devices**, and **Wireless/AP Devices** dropdown options available next to breadcrumbs. See the figure below:

Figure 9-10: Compliance Dashboard - Managed Devices



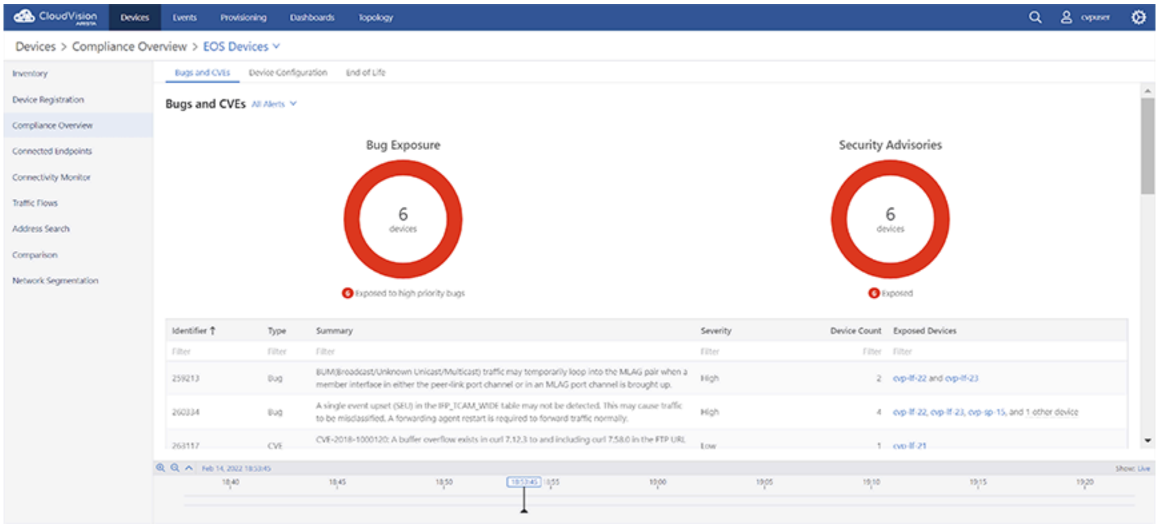
The assessment uses bug details published on https://www.arista.com and leverages the network wide database to compute the exposure based on hardware and software versions. The ***CVP 2020.2.0*** release comes packaged with a file named **`AlertBase.json`** which contains information about software defects and security vulnerabilities.

The compliance dashboard table consists of **Bugs and CVEs**, **Device Configuration**, and **End Of Life** tabs.

Bugs and CVEs

The **Bugs and CVEs** tab displays graphical and tabular presentation of bug alerts. See the image below:

Figure 9-11: Compliance Dashboard- Bugs and CVEs



Identifier ↑	Type	Summary	Severity	Device Count	Exposed Devices
Filter	Filter	Filter	Filter	Filter	Filter
259213	Bug	BUM(Broadcast/Unknown Unicast/Multicast) traffic may temporarily loop into the MLAG pair when a member interface in either the peer-link port channel or in an MLAG port channel is brought up.	High	2	cvp-lf-22 and cvp-lf-23
260334	Bug	A single event upset (SEU) in the IFP_TCAM_WIDE table may not be detected. This may cause traffic to be misclassified. A forwarding agent restart is required to forward traffic normally.	High	4	cvp-lf-22, cvp-lf-23, cvp-sp-15, and 1 other device
263117	CVE	CVE-2018-1000120: A buffer overflow exists in curl 7.12.3 to and including curl 7.58.0 in the FTP URL	Low	1	cvp-lf-21

Note: You can filter bug alerts using **All Alerts**, **Unacknowleged Alerts**, and **Acknowledged Alerts** dropdown options available next to the tab title.

The donuts display the count of devices exposed to bugs and security and advisories where green signifies secured devices and red signifies exposed devices. Hover the cursor on the donut ring to view the count of devices exposed, total count of devices, and the percentile of exposed devices.

The table provides the following information:

- **Identifier**: Bug number for issues tracked.

  Note: The checkmark next to identifier ID signifies acknowledged bugs.

- **Type**: Identifies the type of bug. Security vulnerabilities are tracked by type **CVE**. Software defects are tracked by type **Bug**. This field can be used to filter on either of these types.
- **Summary**: Provides a description of the software defect/security vulnerability.
- **Severity**: Calls out the severity of the software defect.
- **Device Count**: Lists the number of devices impacted by the tracked issue.

  Note:

  - If a device is acknowledged in tracked issues, this count is decreased by one.
  - If the bug is acknowledged, CVP displays zero.
  - Unacknowledged actions undo these results.

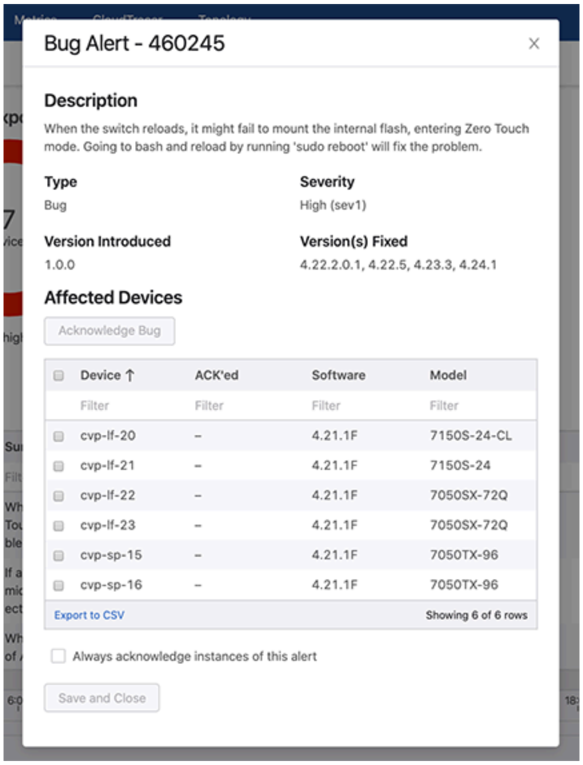
- **Exposed Devices**: Lists the names of devices impacted by the software defect or security vulnerability.

  Note:

  - If a device is acknowledged in tracked issues, CVP does not list its name.
  - If a bug is acknowledged, CVP displays **None**.
  - Unacknowledged actions undo these results.
  - CVP generates events for CVE bugs that are exposed on device(s). These events last until the bug either is resolved on the device or is acknowledged.

Click the listed bug alert to view more details from the corresponding **Bug Alert -** *Identifier ID* pop-window. See the figure below.

Figure 9-12: Bug Alert Pop-Up Window



Bug Alert - 460245

Description

When the switch reloads, it might fail to mount the internal flash, entering Zero Touch mode. Going to bash and reload by running 'sudo reboot' will fix the problem.

Type: Bug

Severity: High (sev1)

Version Introduced: 1.0.0

Version(s) Fixed: 4.22.2.0.1, 4.22.5, 4.23.3, 4.24.1

Affected Devices

□	Device ↑	ACK'ed	Software	Model
	Filter	Filter	Filter	Filter
□	cvp-lf-20	–	4.21.1F	7150S-24-CL
□	cvp-lf-21	–	4.21.1F	7150S-24
□	cvp-lf-22	–	4.21.1F	7050SX-72Q
□	cvp-lf-23	–	4.21.1F	7050SX-72Q
□	cvp-sp-15	–	4.21.1F	7050TX-96
□	cvp-sp-16	–	4.21.1F	7050TX-96

Showing 6 of 6 rows

□ Always acknowledge instances of this alert

You can fix listed bugs through one of the following ways:

- Upgrading your device to versions mentioned under **Version(s) Fixed**

- Installing the hotfix available at https://www.arista.com/en/support/advisories-notices as either a part of an image bundle or directly using the EOS CLI.

  Note: You can search for hotfixes via identifier IDs.

Click the **Acknowledge Bug on *n* Device(s) and Close** button to hide the corresponding bug from bug info in selected devices.

Note:

- ***n*** presents the count of selected devices.
- (Optional) Provide reasons for acknowledgement in the text box.
- To undo the acknowledgement, reopen the bug to select acknowledged devices and click the **Unacknowledge Bug on *n* Device(s) and Close** button.

To acknowledge a bug for all current and future devices, select **Always acknowledge instances of this alert** checkbox and click **Save and Close** button.

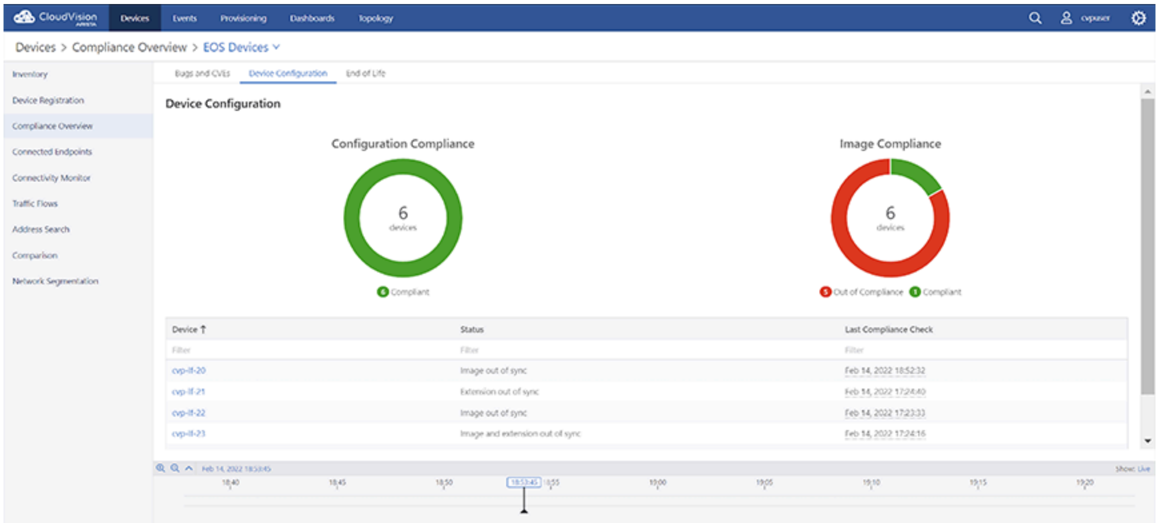
Note:

- (Optional) Provide reasons for acknowledgement in the text box.
- To undo the acknowledgement, reopen the bug, unselect the checkbox, and click **Save and Close**.

Device Configuration

The **Device Configuration** tab displays graphical and tabular presentation of image and configuration compliances. See the image below:

Figure 9-13: Compliance Dashboard - Device Configuration



Device ↑	Status	Last Compliance Check
Filter	Filter	Filter
cvp-lf-20	Image out of sync	Feb 14, 2022 18:52:32
cvp-lf-21	Extension out of sync	Feb 14, 2022 17:24:40
cvp-lf-22	Image out of sync	Feb 14, 2022 17:23:33
cvp-lf-23	Image and extension out of sync	Feb 14, 2022 17:24:16

The donuts display the total count of devices available for image and configuration compliances where green signifies compliant devices and red signifies non-compliant devices. Hover the cursor on the donut ring to view the count of non-compliant devices, total count of devices, and the percentile of non-compliant devices..

The table displays the following information:

- **Device** - Lists the hostnames of devices.

  Note: Clicking on a device name opens the **Running Configuration** screen.

- **Status** - Displays the device status on configuration compliance.

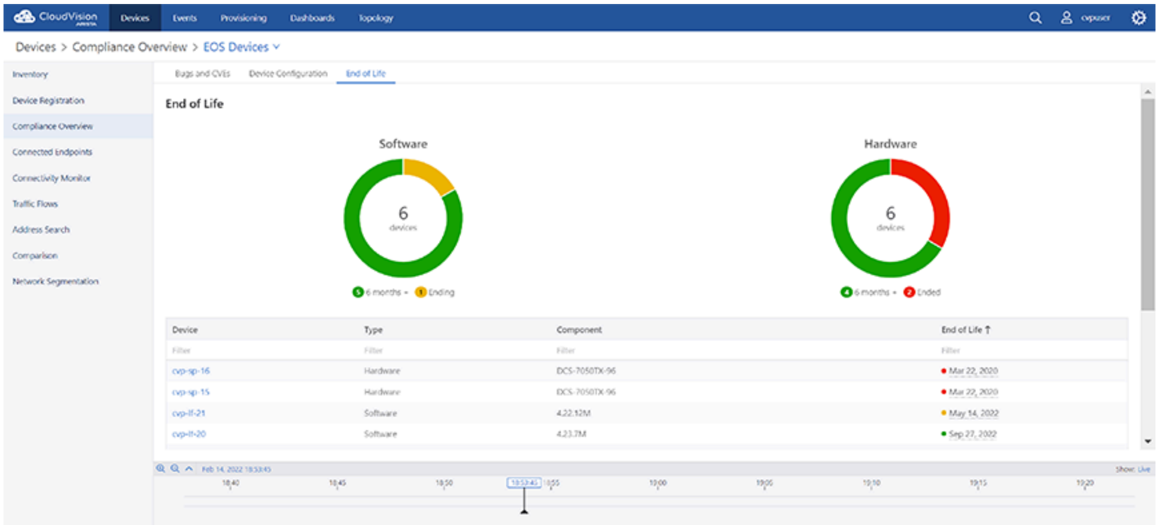
  Note: CVP tracks out of sync status for configuration, image, and extensions.

- **Last Compliance Check** - Displays the timestamp of the last compliance check.

End of Life

The **End of Life** tab displays graphical and tabular presentation of End Of Life (EOL) of devices . See the image below:

Figure 9-14: Compliance Dashboard - End of Life



Device	Type	Component	End of Life ↑
Filter	Filter	Filter	Filter
cvp-sp-16	Hardware	DCS-7050TX-96	🟥 Mar 22, 2020
cvp-sp-15	Hardware	DCS-7050TX-96	🟥 Mar 22, 2020
cvp-lf-21	Software	4.22.12M	🟨 May 14, 2022
cvp-lf-20	Software	4.23.7M	🟩 Sep 27, 2022

The donuts display the total count of devices where green signifies the percentile of devices with more than 6 months of life, amber signifies the percentile of devices that are approaching EOL, and red signifies the percentile of devices that reached EOL. Hover the cursor on the donut ring to view the count and percentile of devices with more than six months of life.

The table displays the following information:

- **Device**: Lists the hostnames of devices.

  Note: Clicking on a device name displays the hardware inventory details of child devices.

- **Type**: Lists whether the device is a hardware or software.
- **Component**: List the device model numbers for hardware devices and version numbers for software devices.
- **End of Life**: Lists the earliest date of EOL.

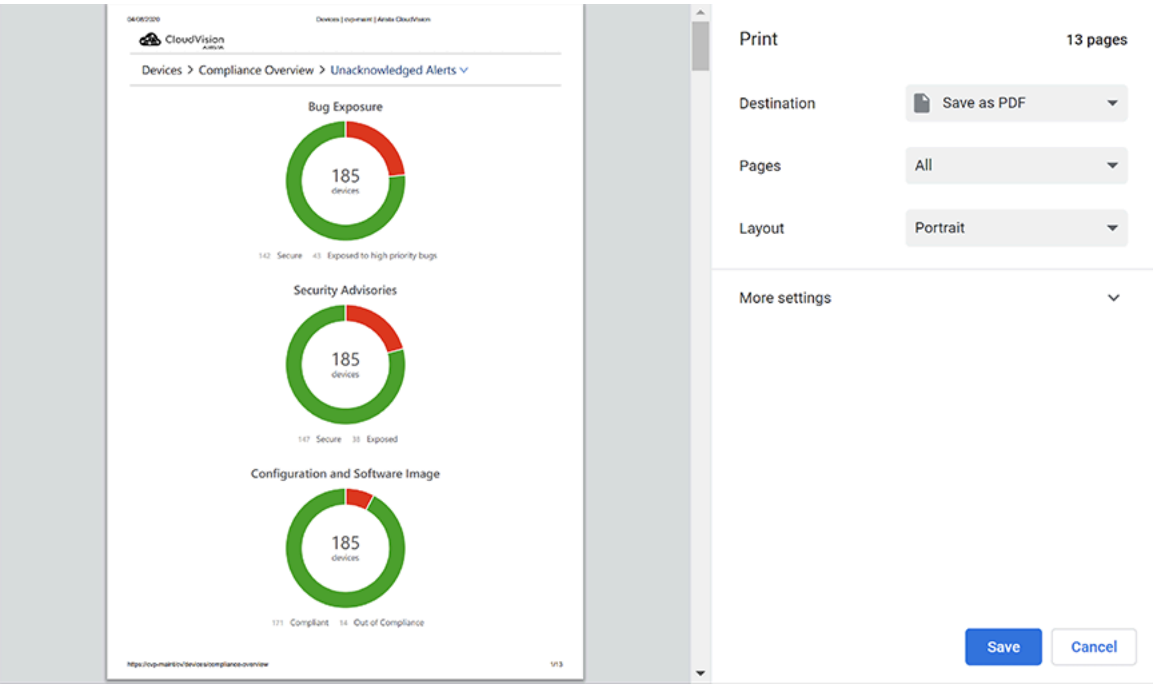
9.4 Print Compliance Dashboard

Perform the following steps to print the Compliance dashboard:

1. Select **Print** from the browser menu.

CVP displays the Print pop-up window. See the figure below.

Figure 9-15: Print Pop-Up Window


CloudVision
Devices > Compliance Overview > Unacknowledged Alerts
Bug Exposure
185 devices
142 Secure 43 Exposed to high priority bugs
Security Advisories
185 devices
147 Secure 38 Exposed
Configuration and Software Image
185 devices
171 Compliant 14 Out of Compliance
1/13
Save
Cancel

Print 13 pages

Destination: Save as PDF

Pages: All

Layout: Portrait

More settings

2. Select your printer from the **Destination** dropdown menu to print the screen.

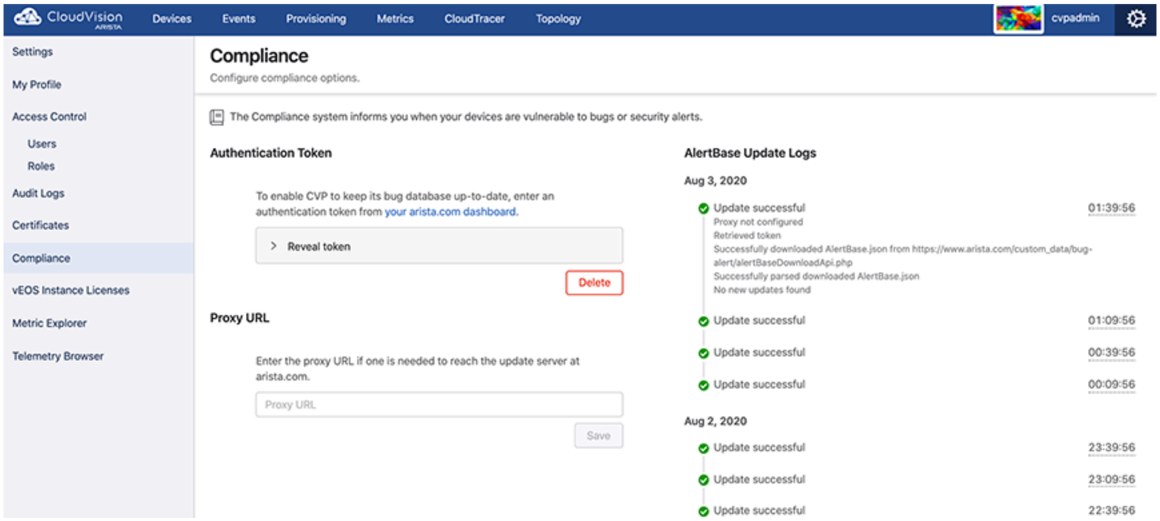
Note: To save a print-friendly version of the screen, select **Save as PDF** from the **Destination** dropdown menu. This PDF contains all rows of the compliance table.

3. Click **Save**.

9.5 Setup for Automatic Sync of Compliance Bug Database

In order to keep the bug database up to date and receive real-time assessments on exposure to software defects and security vulnerabilities, an automated sync can be configured between CVP and https://www.arista.com using a token-based authentication and proxy URL.

Figure 9-16: Configuring Compliance Settings



Compliance

Configure compliance options.

The Compliance system informs you when your devices are vulnerable to bugs or security alerts.

Authentication Token

To enable CVP to keep its bug database up-to-date, enter an authentication token from your arista.com dashboard.

Proxy URL

Enter the proxy URL if one is needed to reach the update server at arista.com.

Proxy URL

AlertBase Update Logs

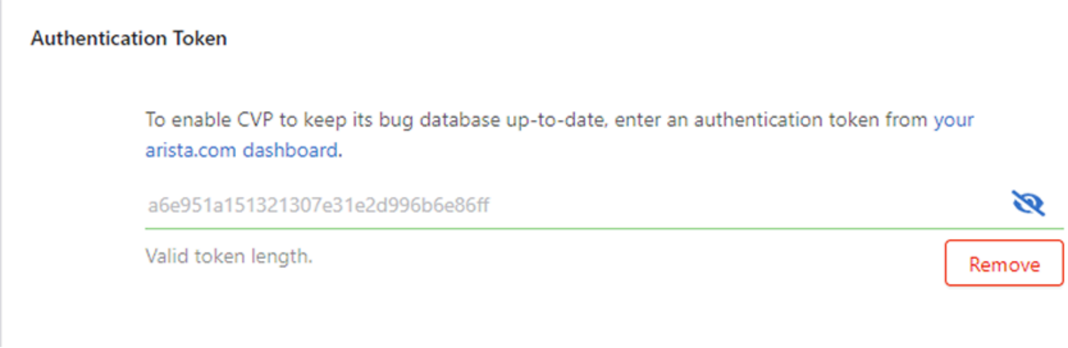
```
Aug 3, 2020
Update successful                                                   01:39:56
Proxy not configured
Retrieved token
Successfully downloaded AlertBase.json from https://www.arista.com/custom_data/bug-
alert/alertBaseDownloadApi.php
Successfully parsed downloaded AlertBase.json
No new updates found
Update successful                                                   01:09:56
Update successful                                                   00:39:56
Update successful                                                   00:09:56
Aug 2, 2020
Update successful                                                   23:39:56
Update successful                                                   23:09:56
Update successful                                                   22:39:56
```

The Compliance screen has a compliance section that accepts the following information:

- An authentication token generated by www.arista.com to enable CVP to keep its bug database up-to-date.
- Proxy URL to reach the update server at www.arista.com.

This token is generated per user and can be obtained from the user profile screen under the Portal Access section on www.arista.com.

Figure 9-17: Compliance Portal Access



Authentication Token

To enable CVP to keep its bug database up-to-date, enter an authentication token from your arista.com dashboard.

a6e951a151321307e31e2d996b6e86ff

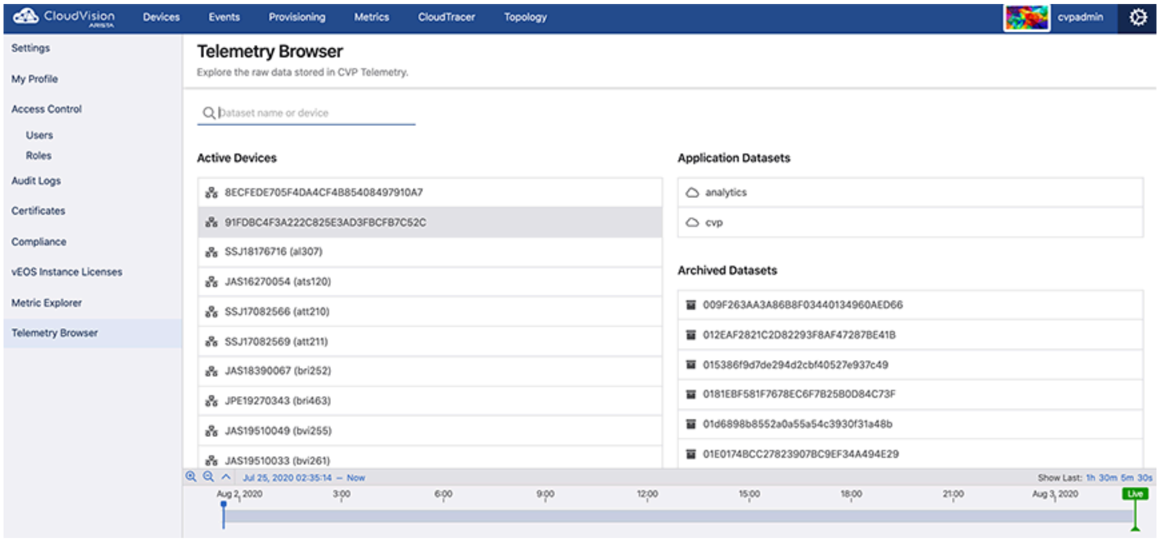
Valid token length.

When this token is provided in the Compliance settings screen, it allows CVP to download the latest version of the https://www.arista.com/en/login file that is available on the Software downloads page.

Note: To leverage automatic updates of the compliance bug database, connectivity to www.arista.com should be ensured from the CVP VM.

The version and release date of the compliance bug database in use can be viewed in the **Settings** screen under **Telemetry Browser > analytics > BugAlerts > update**.

Figure 9-18: Telemetry Browser Screen



Telemetry Browser

Explore the raw data stored in CVP Telemetry.

Dataset name or device

Active Devices

- 8ECFEDE705F4DA4CF4B85408497910A7
- 91FDBC4F3A222C825E3AD3FBCFB7C52C
- SSJ18176716 (al307)
- JAS16270054 (ats120)
- SSJ17082566 (att210)
- SSJ17082569 (att211)
- JAS18390067 (bri252)
- JPE19270343 (bri463)
- JAS19510049 (bvi255)
- JAS19510033 (bvi261)

Application Datasets

- analytics
- cvp

Archived Datasets

- 009F263AA3A86B8F03440134960AED66
- 012EAF2821C2D82293F8AF47287BE41B
- 015386f9d7de294d2cbf40527e937c49
- 0181EBF581F7678EC6F7B2580D84C73F
- 01d6898b8552a0a55a54c3930f31a48b
- 01E0174BCC27823907BC9EF34A494E29

Jul 25, 2020 02:35:14 – Now

Chapter 10

Network Provisioning (CVP)

The Network Provisioning Screen presents a hierarchical view of the network configuration.

It is not a network topology; it is a configuration tree view. The switches at the bottom of the tree inherit the configuration specified in the containers above them as well as the configuration that is specific to them. The containers and switches all have sub menus that are accessed by right mouse clicking on them. The main features of the screen are described below.

Note: Switches that have been added to the network from new will ZTP boot using generic details from CVP and appear in the Undefined container.

10.1 Network Provisioning View

The topology view of the Network Provisioning screen is a tree structure that consists of containers and devices. This view represents the current groupings of devices (devices grouped by container) as well individual devices.

By default, two types of containers are available in the topology view.

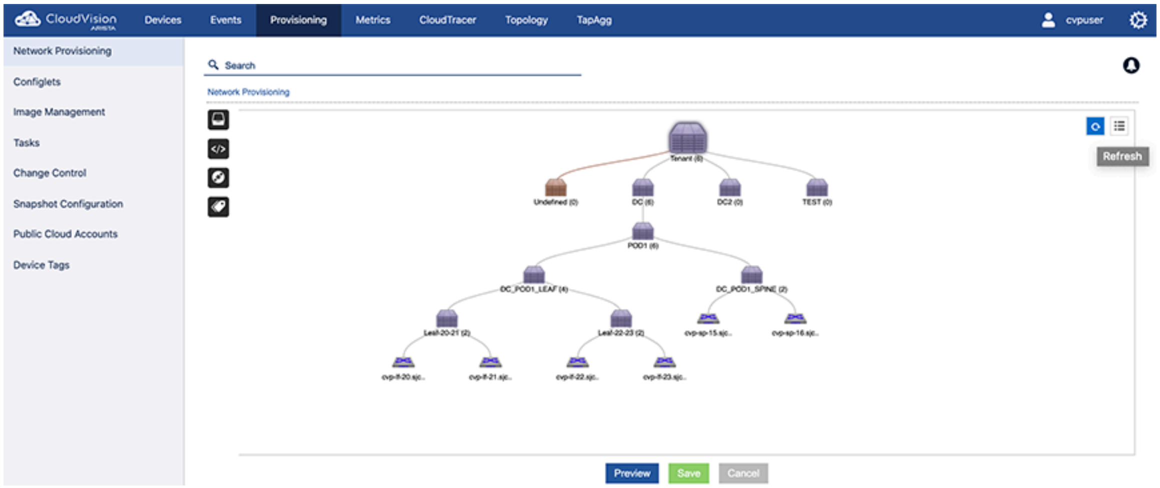
- **Tenant**: Top-most container.
- **Undefined**: Container for all devices that have registered themselves with the CloudVision Portal using Zero Touch Provisioning (ZTP) and are awaiting configuration. Undefined containers are shown in the view in a different color than defined containers.

The example shown below includes:

- One tenant container (there is always only one tenant container).
- Three containers under the tenant container (one of the three is an undefined container).

- Seven devices (one is under the undefined container, and 6are grouped under the container named Vantage-DC (6)).

Figure 10-1: Network provisioning view showing tree structure



Note: Different color icons are used to indicate that devices have compliance alerts or access alerts.

For more information, see:

- Network Provisioning Screen Options
- Changing Between Network Provisioning View and List View

Related topics:

- Container Level Actions
- Device-level Actions
- Viewing Containers and Devices

10.1.1 Network Provisioning Screen Options

The following options are available from the **Network Provisioning** screen.

- **Device Management** Lists all the switches that reside below the selected container level, these could belong to the selected container or reside in containers within the selected container.
- **Configlet Management** Lists the configlets associated with the selected container or if a switch is selected all of the configlets applied to it both directly and inherited.
- **Image Management** Lists the EOS or vEOS software image associated with a container or switch. Switches below the container selected will be loaded with this image.
- **Label Management** Lists the system or custom labels associated with the selected container or switch.
- **Refresh and Listview** Refresh the current screen to show any updates or changes to the switches or devices. Listview changes the display from **Topology View** and displays the switches in a list.
- **Containers** Containers are the basic logical construct of the topology view. They are used to used group devices and to apply configurations and deploy images to the device groups.

Container Right Click Options:

- **Show From Here** Changes the display to show only the containers and switches below the selected container.
- **Expand / Collapse** toggles between shrinking or growing the tree topology below the selected container.
- **Show All Devices** Lists the switches that are associated with that specific container. The container turns blue if it contains more than five switches and will only display 25 of the total number of switches in the topology structure.

- **Container: Add / Delete** Create or remove a container that from the selected container.
- **Device: Add / Manage** Add a device to the selected container or manage the switches already associated with the container. The manage option displays a list of switches which can be selected by enabling the tick box on the left-hand side. The selected switches can then be moved to another container, reset (returned to a ZTP boot state and associated with the undefined container), or removed from CVP completely.
- **Manage: Configlet / Image Bundle** Allocate or remove a configlet or Image to or from a switch or container.
- **View Config** View the configuration created from the combined configlets. At the container level this shows the combined configlet configuration associated with that container.
- **Check Compliance** - To initiate a compliance check on all devices under the container.
- **Reconcile** - To initiate configuration reconcile on all devices under the container.

Device Right Click Options:

- **Manage: Configlet / Image Bundle** Allocate or remove a configlet or Image to or from a switch or container.
- **Labels** Lists / assigns the user created labels associated with the selected switch.
- **View Config** View the configuration created from the combined configlets. At the switch level the entire configuration that will be applied to the switch is shown.
- **Check Compliance** Compares the current running configuration on the switch against the designed configuration in CVP. If they are out of sync the device change to an orange color.
- **Move** Allows a user to move a switch from one container to another.
- **Factory Reset** Erases the configuration on the switch then ZTP boots it. This will return it to the undefined container on the provisioning screen.
- **Remove** Removes the switch from CVP. This stops CVP making changes to it and tracking its configuration. The switch is left running with its current configuration on it.
- **Replace** - To perform a Zero Touch Replacement (ZTR) of the selected device.

Related topics:

- Changing Between Network Provisioning View and List View
- Container Level Actions
- Device-level Actions
- Viewing Containers and Devices

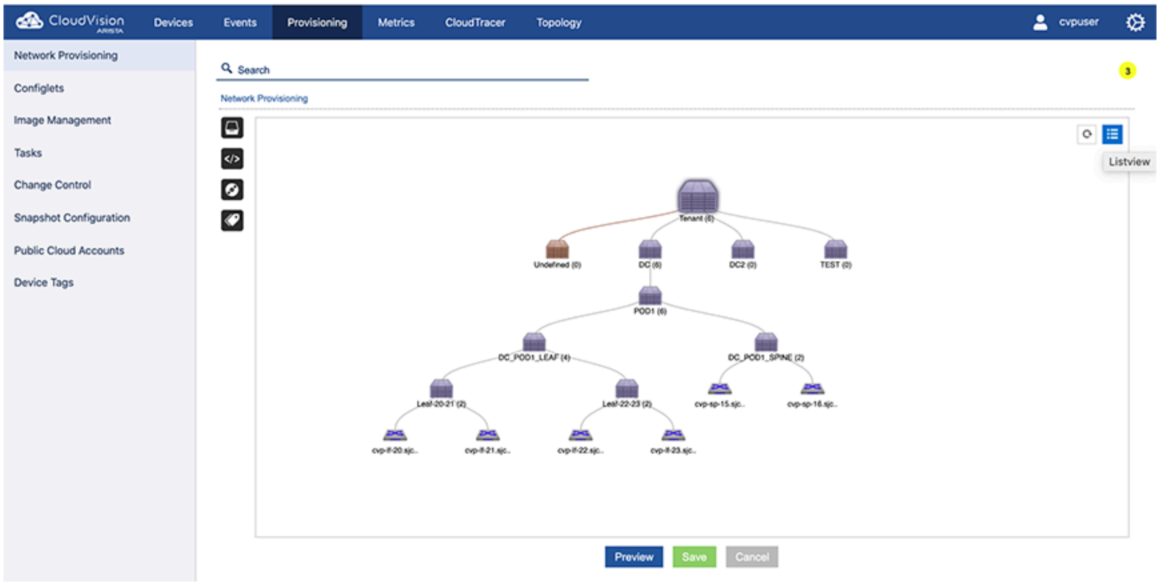
10.1.2 Changing Between Network Provisioning View and List View

Click the icons to toggle between the topology view and the list view of the Network Provisioning screen.

Changing to List View

Click the **List** icon for a list view.

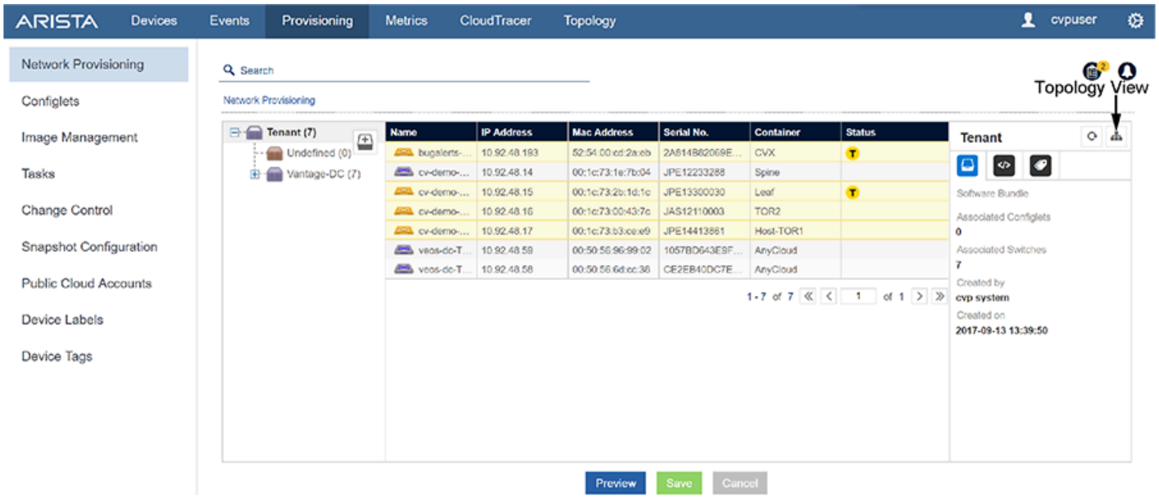
Figure 10-2: Changing to List View



Changing to Topology View

Click the **Topology** icon for a topology view.

Figure 10-3: Changing to Topology View



Name	IP Address	Mac Address	Serial No.	Container	Status
bugalerts-...	10.92.48.193	52:54:00:cd:2a:eb	2A614B82069E...	CVX	T
cv-demo-...	10.92.48.14	00:1c:73:1e:7b:04	JPE12233288	Spine	
cv-demo-...	10.92.48.15	00:1c:73:2b:1d:1c	JPE13300030	Leaf	T
cv-demo-...	10.92.48.16	00:1c:73:00:43:7c	JAS12110003	TOR2	
cv-demo-...	10.92.48.17	00:1c:73:b3:ce:e9	JPE14413861	Host-TOR1	
veos-dc-T...	10.92.48.59	00:50:56:96:99:02	1057BD643E9F...	AnyCloud	
veos-dc-T...	10.92.48.58	00:50:56:6d:cc:38	CE2EB40DC7E...	AnyCloud	

Tenant

Software Bundle

Associated Configlets
0

Associated Switches
7

Created by
cvp system

Created on
2017-09-13 13:39:50

Related topics:

- Network Provisioning Screen Options
- Container Level Actions
- Device-level Actions
- Viewing Containers and Devices

10.2 Container Level Actions

Containers are a logical entity used to group network devices and to define a hierarchy to which configurations can be applied. When you apply a configlet to a container, the configlet is automatically applied to all of the devices in the container's hierarchy.

Simple container implementations:

- Create a container for every datacenter.
- Within each datacenter container, create a container for every POD (leaf-spine deployment).
- Add devices that belong to each POD to the POD container. Tenant: Top-most container.

For details on how to create, rename, and delete containers, see:

- Creating a Container
- Deleting a Container
- Renaming a Container

Related topics:

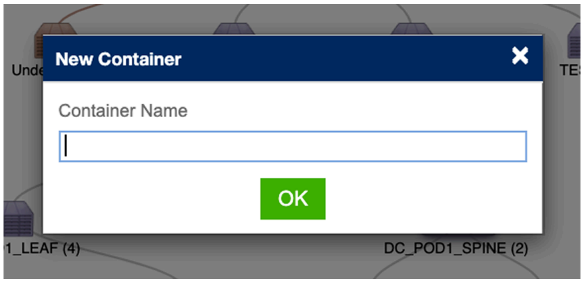
- Device-level Actions
- Viewing Containers and Devices

10.2.1 Creating a Container

To create a container:

1. Select a parent container (the container to which you want to add a new container).
2. Right-click the container and choose **Add > Container**. The **New Container** dialog appears:

Figure 10-4: New Container Dialog



New Container

Container Name

3. Enter the name of the new container and select **OK** to create the container.
4. Click **Save** to apply the changes.

10.2.2 Deleting a Container

Note: Only empty containers can be deleted.

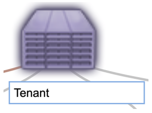
1. Locate the container to be deleted.
2. Right-click the container and click **Remove**.

10.2.3 Renaming a Container

To rename a container in a topology:

1. Double-click the name field of the container to open the name field editor.
2. Enter a new, unique name for the container and click **Enter** to rename the container.

Figure 10-5: Rename Container



Tenant

10.3 Device Bootstrap Process

The device bootstrap process is a process that automatically makes un-provisioned devices available for configuration through CVP. Un-provisioned devices automatically boot up in Zero Touch Provisioning mode and register themselves with the CloudVision Portal (CVP). Once they are registered with CVP, devices become available for configuration in the Undefined Container.

1. Un-provisioned devices boot into Zero Touch Provisioning mode and send out a DHCP request.
2. The DHCP server then assigns the device an IP Address and returns a URL pointing to the CloudVision portal in the bootfile-name option. The URL with IP address will be like this **//ipaddress/ztp/bootstrap** .
3. The device executes this bootstrap script and registers itself with the CloudVision Portal. At this point, the device is available in the Undefined Container.

   You can now add the device to the destination container of your choice and apply the correct image and configuration to the device.

   Related topics:

   - Device-level Actions
   - Viewing Containers and Devices

10.4 Device-level Actions

CloudVision Portal (CVP) enables you to provision devices as needed based on your current networking requirements. Some examples of the types of actions you can perform include:

- Adding devices (use this action to add devices from the undefined container to defined containers)
- Moving devices (used this action to move devices from one defined container to another defined container)
- Removing devices (removing devices from the CVP topology)
- Reset devices
- Replace devices

For details on the steps you use to perform these device level actions, see:

- Adding Devices (from Undefined Container)
- Registering Devices
- Moving Devices from one Container to Another Container
- Removing a Device from a Container
- Device Factory Reset

When resetting a device:

- The device will be removed from the parent container.
- The running configuration of the device will be flushed.
- Device will reboot with ZTP mode enabled.
- Device will be identified under undefined container.

There are three options you can use to move devices. They are:

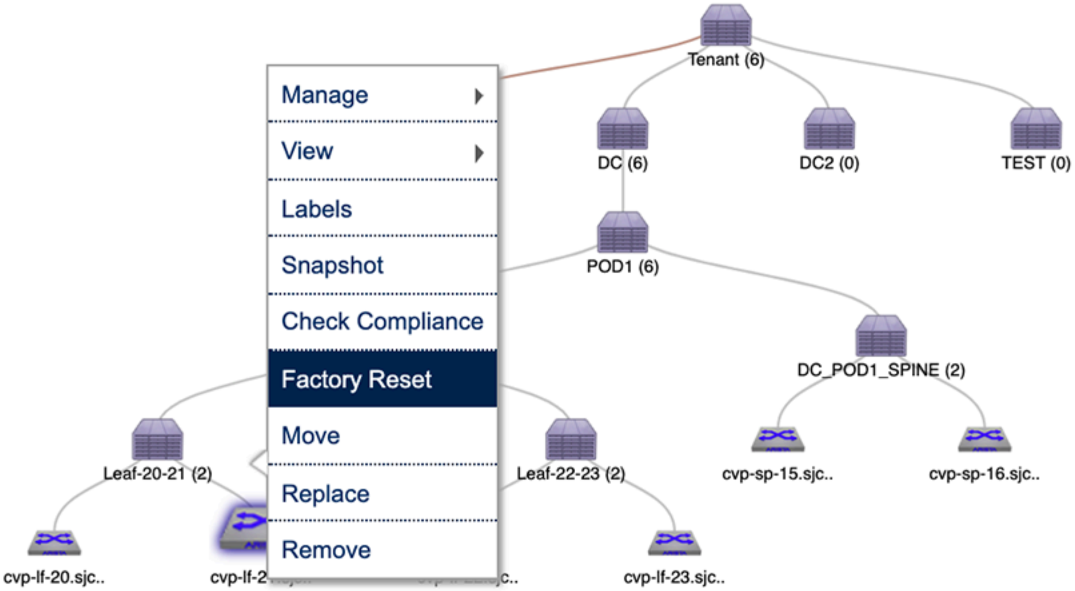
- Option 1
- Option 2
- Option 3

Option 1:

1. Locate the device.

2. Right-click the device and choose **Factory Reset**.

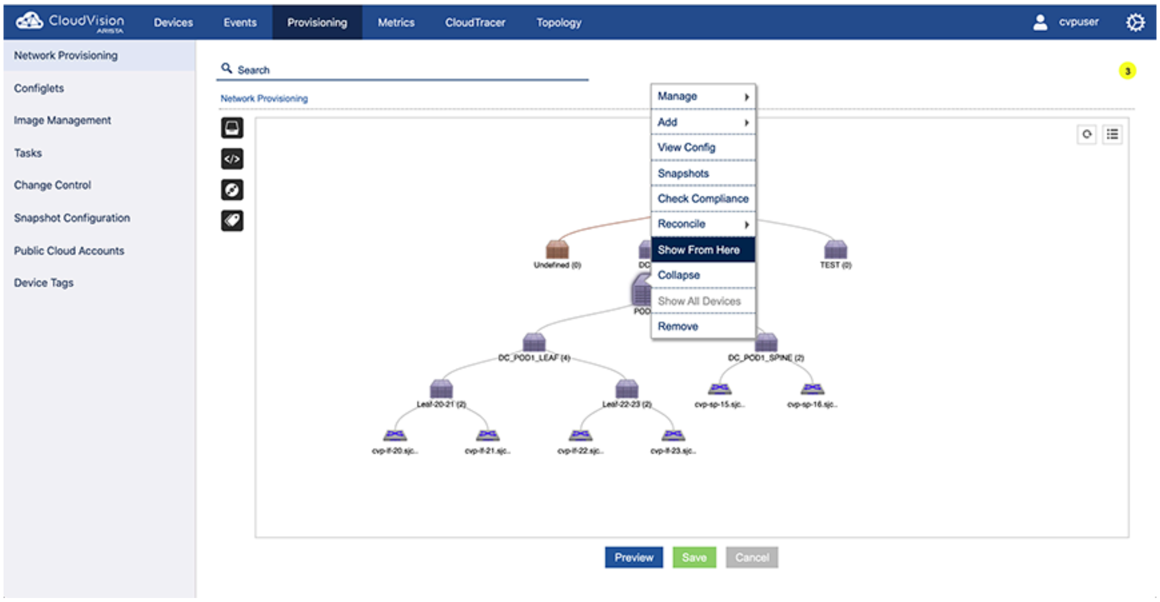
Figure 10-6: Resetting the Device (option 1)



Option 2:

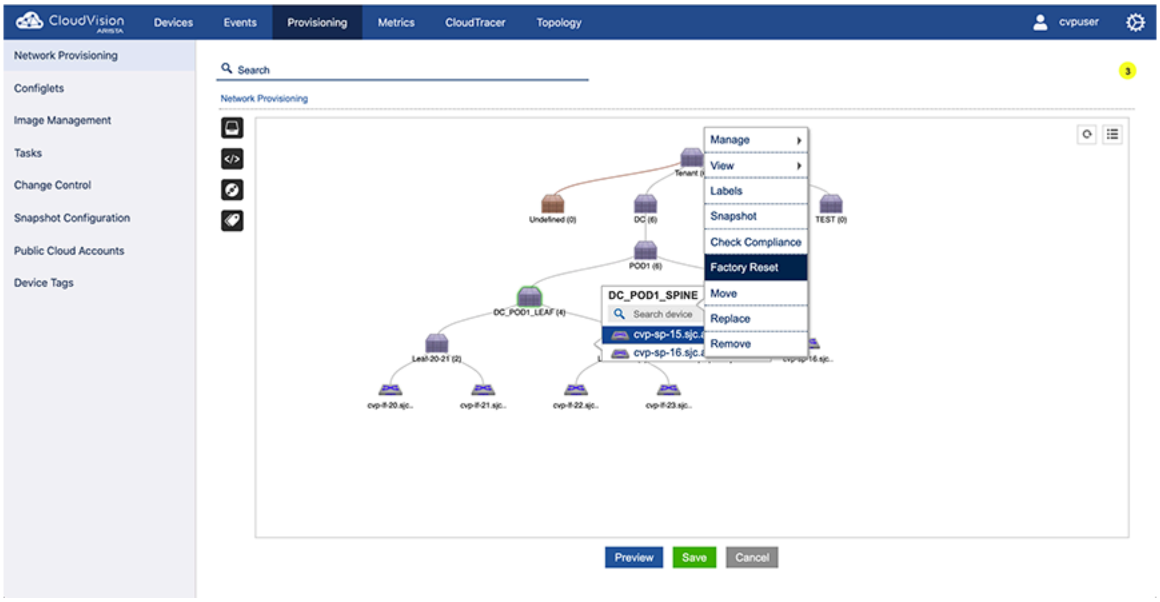
1. Locate the parent container.
2. Right-click the container and choose **Show All Devices.** This will list all the devices under the container.

Figure 10-7: Showing all devices during factory reset (option 2)



3. Right-click the device and choose **Factory Reset**.

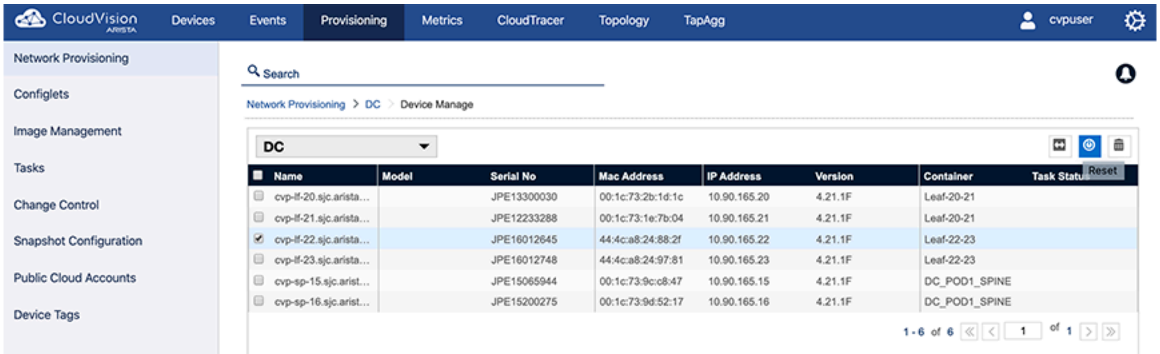
Figure 10-8: Resetting the device (option 2)



Option 3:

1. Locate the parent container.
2. Right-click the container and choose **Manage > Device**. This will load the inventory of all the child devices under the container.
3. Select the checkbox of the device to be reset, and click the reset icon.

Figure 10-9: Selecting the device and resetting it (option 3)



☐ Name	Model	Serial No	Mac Address	IP Address	Version	Container	Task Status
☐ cvp-lf-20.sjc.arista...		JPE13300030	00:1c:73:2b:1d:1c	10.90.165.20	4.21.1F	Leaf-20-21	
☐ cvp-lf-21.sjc.arista...		JPE12233288	00:1c:73:1e:7b:04	10.90.165.21	4.21.1F	Leaf-20-21	
☑ cvp-lf-22.sjc.arista...		JPE16012645	44:4c:a8:24:88:2f	10.90.165.22	4.21.1F	Leaf-22-23	
☐ cvp-lf-23.sjc.arista...		JPE16012748	44:4c:a8:24:97:81	10.90.165.23	4.21.1F	Leaf-22-23	
☐ cvp-sp-15.sjc.arist...		JPE15065944	00:1c:73:9c:c8:47	10.90.165.15	4.21.1F	DC_POD1_SPINE	
☐ cvp-sp-16.sjc.arist...		JPE15200275	00:1c:73:9d:52:17	10.90.165.16	4.21.1F	DC_POD1_SPINE	

On saving the session, a task will be spawned to reset the selected device.

10.4.1 Adding Devices (from Undefined Container)

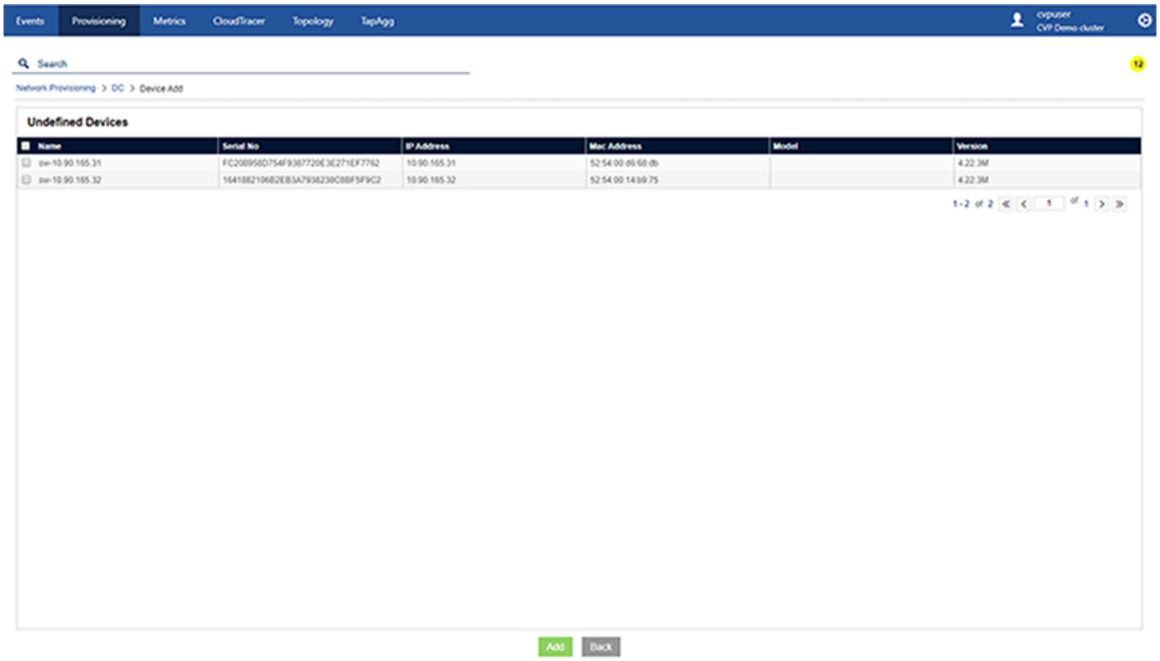
Adding devices from the undefined container is the most common method for adding devices to a container in the CVP topology. This method involves adding devices that are not part of the hierarchy of devices to defined containers in the CVP topology. Containers that receive the added devices are called destination containers.

Complete the following steps to add a device from the undefined container to a destination container:

1. Locate the container to which you want to add a device.

2. Right-click the container and choose **Add > Device**. The current inventory of undefined devices for the selected container appears.

Figure 10-10: Adding a device



Undefined Devices

□ Name	Serial No	IP Address	Mac Address	Model	Version
□ sw-10.90.165.31	FC208958D754F9387720E3E271EF7762	10.90.165.31	52:54:00:d6:68:db		4.22.3M
□ sw-10.90.165.32	1641882106B2EB3A7938238C8BF5F9C2	10.90.165.32	52:54:00:14:b9:75		4.22.3M

3. Select the device and click **Add**.
4. Save the session.
5. Execute the **Device Add** task using the **Task Management** module to add the device to destination container.

10.4.2 Deploying vEOS Routers

CVP deploys and provisions vEOS routers from cloud and datacenter to Amazon Web Services (AWS) and Microsoft Azure. Based on the requirement in vEOS deployment, configlets are assigned for push EOS configuration along with deployment parameters such as AWS Virtual Private Cloud (VPC), subnets, and security groups.

Note: When CVP is deployed behind NAT devices, the vEOS telemetry configuration needs to be updated. You can view telemetry data coming from the deployed device when you configure the public IP address of CVP.

Related Topics:

- Prerequisites
- Adding IPsec and vEOS Licenses
- Adding AWS to Public Cloud Accounts
- Deploying the vEOS Router to AWS
- Adding Microsoft Azure to Public Cloud Accounts
- Deploying a vEOS Router to Microsoft Azure

10.4.2.1 Prerequisites

The prerequisites to deploy vEOS routers within a cloud are:

- vEOS version *4.21.1.1F* or later
- *CVP 2018.2.0*
- vEOS license

- Cloud (AWS/Microsoft Azure) credentials
- vEOS deployment parameters including VPC within which the vEOS has to be deployed, subnets and security groups associated with vEOS
- IP connectivity from deployed vEOS to CVP

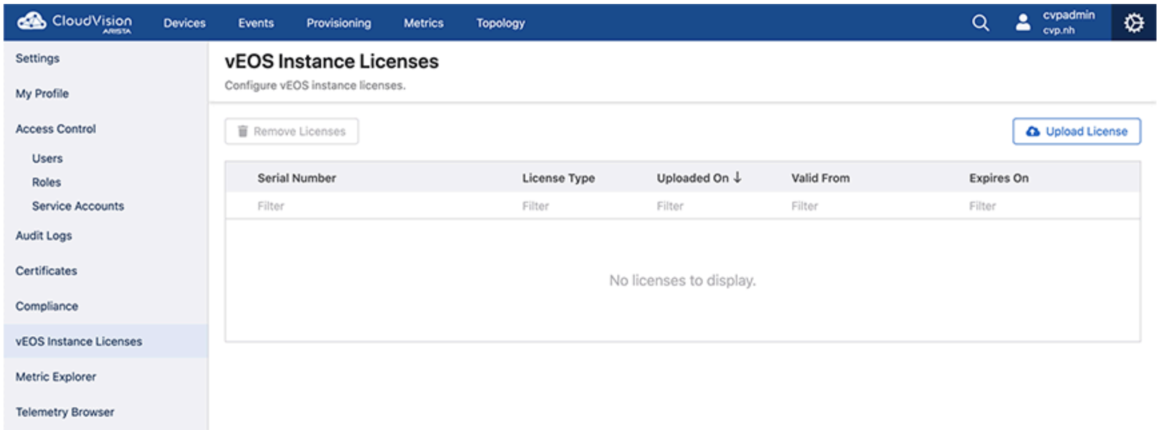
10.4.2.2 Adding IPSec and vEOS Licenses

The addition of an IPSec license is optional based on the deployment.

Perform the following steps to add IPSec and vEOS licenses:

1. Click the gear icon at the upper right corner of the CVP. The system displays the **Settings** screen.
2. Click **EOS Feature Licenses** in the left pane. The system displays the **EOS Feature Licenses** screen.

Figure 10-11: EOS Feature Licenses Screen



vEOS Instance Licenses

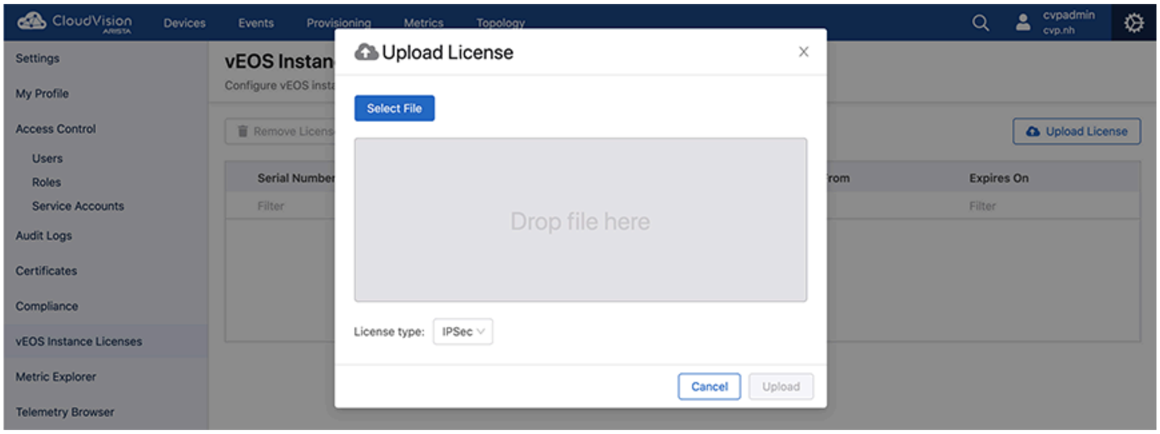
Configure vEOS instance licenses.

Serial Number	License Type	Uploaded On ↓	Valid From	Expires On
Filter	Filter	Filter	Filter	Filter

No licenses to display.

3. Click **Add License** in the right pane. The system displays the **Add License** window.

Figure 10-12: Add License Window

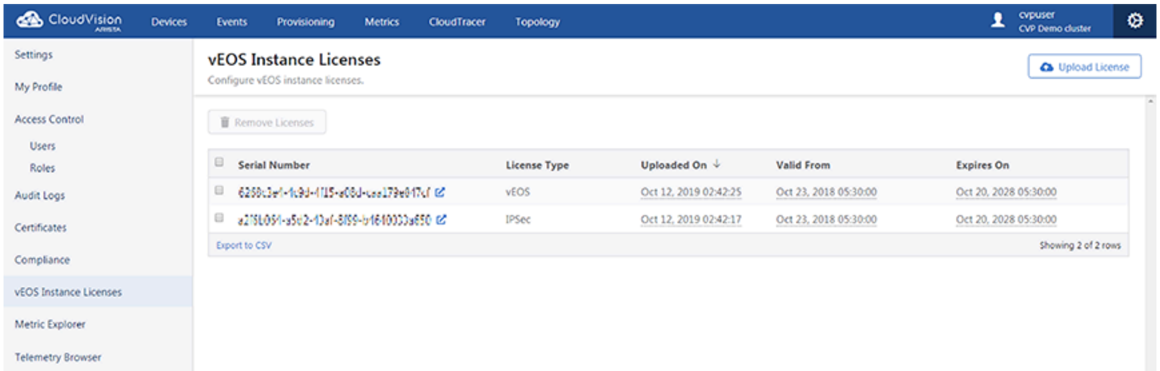


License type: IPSec

4. Click **Select license file**. The system displays the Windows Explorer.
5. Navigate to the required location and select the license.
6. Click **Open**.
7. Select the required option from the **License type** drop-down menu.

8. Click **Upload**. The system lists uploaded licenses in the **EOS Feature Licenses** screen.

Figure 10-13: Licenses Listed in EOS Feature Licenses Screen



vEOS Instance Licenses

Configure vEOS instance licenses.

□	Serial Number	License Type	Uploaded On ↓	Valid From	Expires On
□	6250c3e1-1c9d-4115-a08d-caa179e047cf	vEOS	Oct 12, 2019 02:42:25	Oct 23, 2018 05:30:00	Oct 20, 2028 05:30:00
□	a2f5b051-a5c2-43af-8f99-b1610033a650	IPSec	Oct 12, 2019 02:42:17	Oct 23, 2018 05:30:00	Oct 20, 2028 05:30:00

Showing 2 of 2 rows

10.4.2.3 Adding AWS to Public Cloud Accounts

AWS Security Token Service (STS) is required when adding an AWS account to public cloud accounts.

AWS STS gives CVP temporary access to your AWS environment with proper permissions. This allows CVP to deploy the vEOS router and related resources in your AWS VPC.

CVP calls certain AWS APIs to query VPC information and creates a vEOS router Virtual Machine (VM) in VPC. It needs an AWS IAM (Identity and Access Management) role with permissions as listed in the code below .

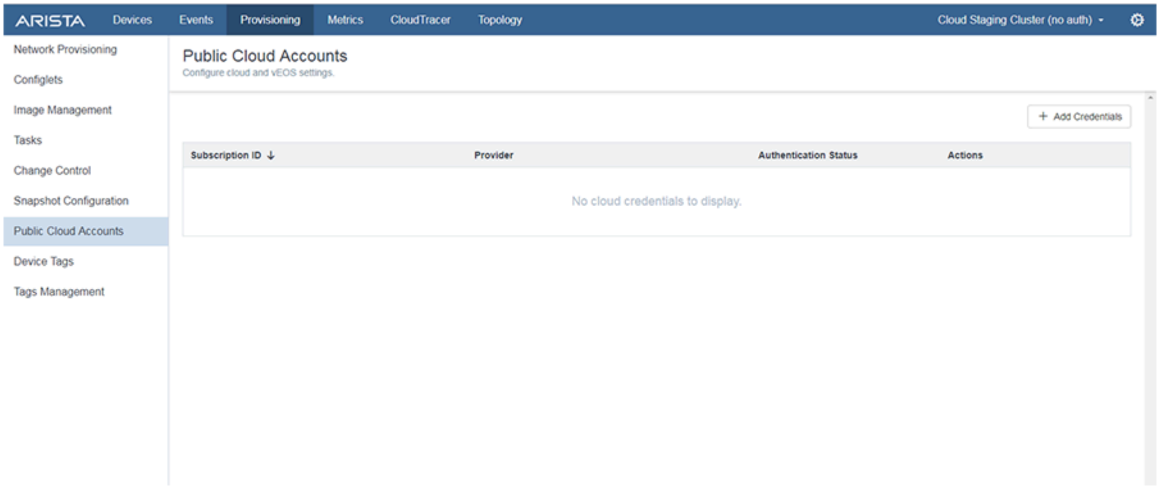
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeRegions",
                "ec2:DescribeVpcs",
                "ec2:DescribeImages",
                "ec2:DescribeAddresses",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeNetworkInterfaces",
                "ec2:CreateNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DetachNetworkInterface",
                "ec2:DeleteNetworkInterface",
                "ec2:AllocateAddress",
                "ec2:AssociateAddress",
                "ec2:DisassociateAddress",
                "ec2:ReleaseAddress",
                "ec2:RunInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*"
        }
    ]
}
```

Note: You receive the STS token after the IAM role is created.

Perform the following steps to add a AWS account to public cloud accounts:

1. Click **Provisioning**. The system displays the **Network Provisioning** screen.
2. Click **Public Cloud Accounts** in the left pane. The system displays the **Public Cloud Accounts** screen.

Figure 10-14: Public Cloud Accounts Screen



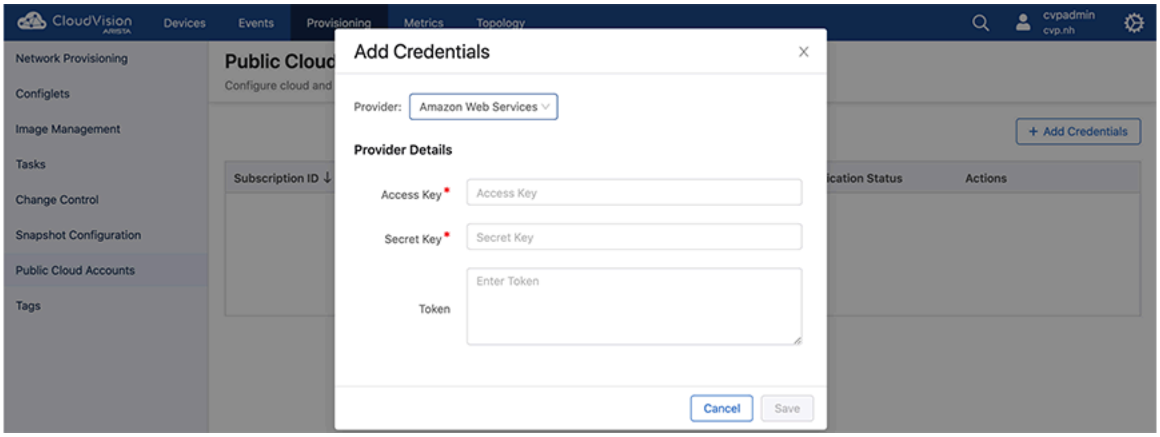
Public Cloud Accounts

Configure cloud and vEOS settings.

Subscription ID ↓	Provider	Authentication Status	Actions
No cloud credentials to display.			

3. Click **Add Credentials** in the upper right corner of the right pane. The system displays the **Add Credentials** window.
4. Select **Amazon Web Services** from the **Provider** drop-down menu.

Figure 10-15: Add Credentials Window for AWS



Add Credentials

Provider: Amazon Web Services

Provider Details

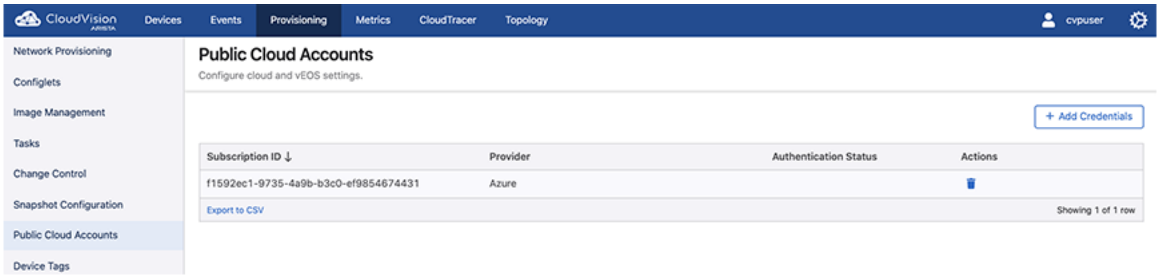
Access Key* Access Key

Secret Key* Secret Key

Token Enter Token

5. On the **Provider Details** pane, provide the access key, secret key, and token details in the corresponding fields.
6. Click **Save**. The system displays the configured AWS account in the **Public Cloud Accounts** screen.

Figure 10-16: AWS Configured in Public Cloud Accounts



Public Cloud Accounts

Configure cloud and vEOS settings.

Subscription ID ↓	Provider	Authentication Status	Actions
f1592ec1-9735-4a9b-b3c0-ef9854674431	Azure		🗑

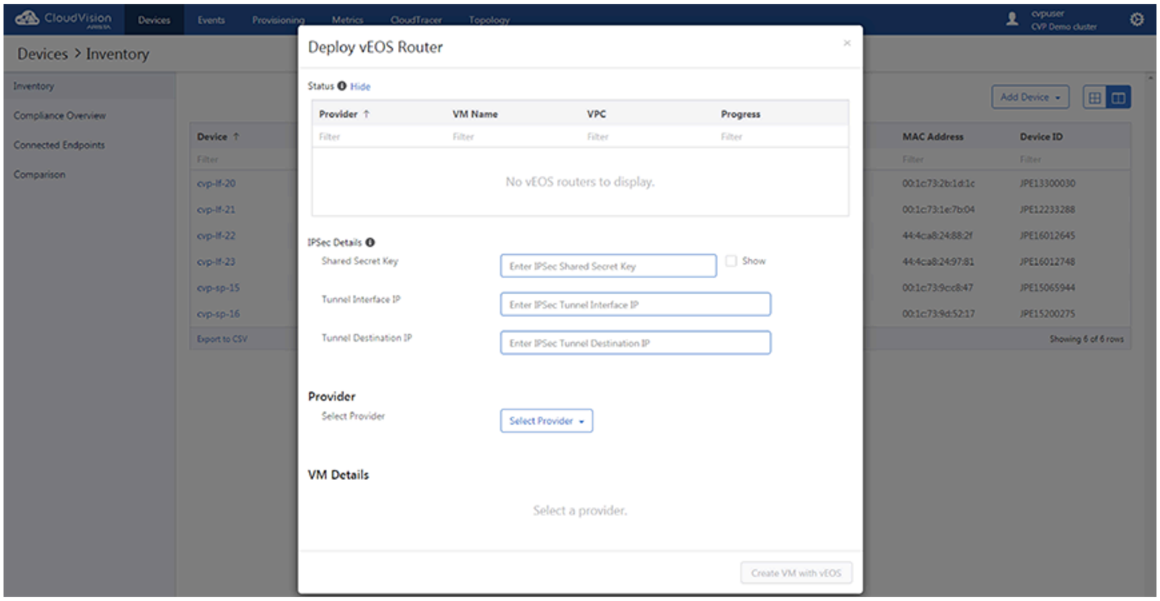
Showing 1 of 1 row

10.4.2.4 Deploying the vEOS Router to AWS

Perform the following steps to deploy the vEOS router to AWS:

1. Click **Devices**. The system displays the Inventory screen.
2. Click the **Add Devices** drop-down menu at the upper right corner of the right pane.
3. Select **Deploy vEOS Router**. The system displays the **Deploy vEOS Router** window.

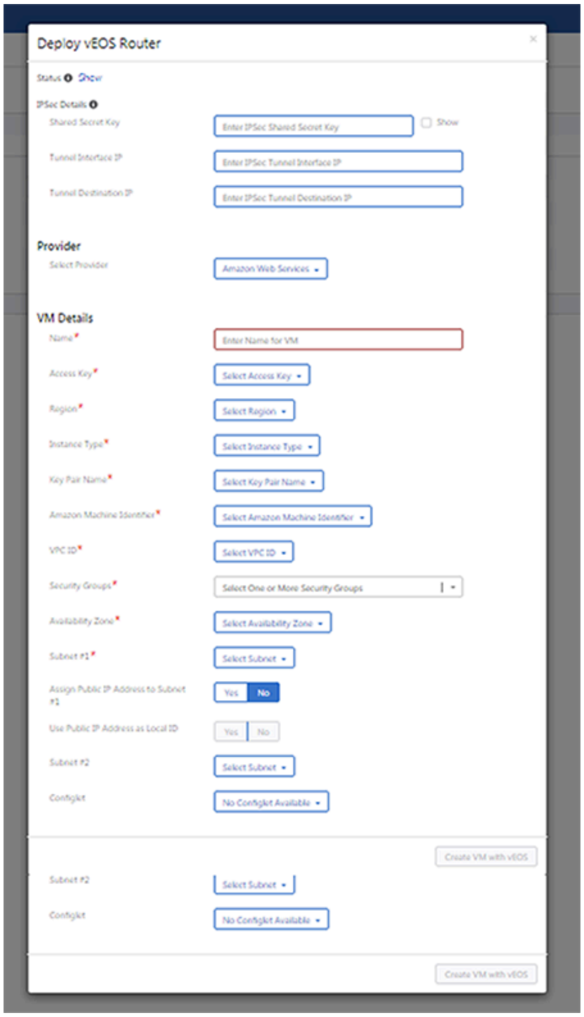
Figure 10-17: Deploy vEOS Router Window



4. Provide the following IPSec details in the appropriate fields:
   - **Shared Secret Key (optional)** - Pre-shared key for IPSec profile
   - **Tunnel Interface IP (optional)** - IP address under tunnel interface
   - **Tunnel#1 Destination IP (optional)** - Peer's (tunnel destination) IP address

5. Click the **Select Provider** drop-down menu and select **AWS**.

Figure 10-18: VM Details for AWS



Deploy vEOS Router

Status Show

IPSec Details

Shared Secret Key: Enter IPSec Shared Secret Key □ Show

Tunnel Interface IP: Enter IPSec Tunnel Interface IP

Tunnel Destination IP: Enter IPSec Tunnel Destination IP

Provider

Select Provider: Amazon Web Services

VM Details

Name*: Enter Name for VM

Access Key*: Select Access Key

Region*: Select Region

Instance Type*: Select Instance Type

Key Pair Name*: Select Key Pair Name

Amazon Machine Identifier*: Select Amazon Machine Identifier

VPC ID*: Select VPC ID

Security Groups*: Select One or More Security Groups

Availability Zone*: Select Availability Zone

Subnet #1*: Select Subnet

Assign Public IP Address to Subnet #1: Yes [✓ No]

Use Public IP Address as Local ID: Yes No

Subnet #2: Select Subnet

Configlet: No Configlet Available

Subnet #2: Select Subnet

Configlet: No Configlet Available

6. Provide the following VM details in the appropriate fields:

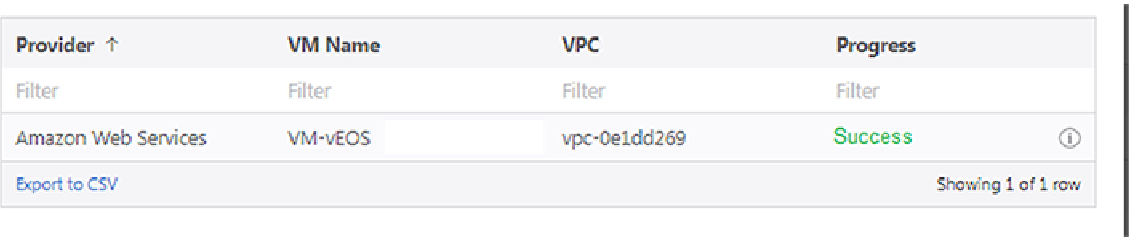
- **Name -** The name of the vEOS router instance
- **Access Key -** The access key used in the public cloud account
- **Region -** The region that the vEOS router will be deployed in
- **Instance Type -** The type of vEOS router that the instance will run on
- **Key Pair Name -** The Elastic Compute Cloud (EC2) keypair used to log in to the vEOS router
- **Amazon Machine Identifier -** The vEOS AMIs on the AWS marketplace
- **VPC ID -** The VPC that the vEOS router will be deployed to
- **Security Group -** The security group that will be associated with the vEOS interface
- **Availability Zone -** The availability zone that vEOS will be deployed in
- **Subnet #1 -** The first subnet that vEOS puts Ethernet1 in
- **Assign Public IP Address to Subnet #1 -** Select Yes if you need a public IP address assigned to the vEOS router; otherwise, select No
- **Use Public IP Address as Local ID -** The public IP address of the vEOS router

  Note: The system displays the public IP address of the vEOS router after the VM is created.

- **Subnet #2 (optional) -** The second subnet that vEOS puts Ethernet2 in
- **Configlet (optional) -** The configlet to configure vEOS once it is active

7. Click **Create VM with vEOS**. The system displays the status of vEOS deployment under the `Progress` column on the **Status** pane.

Figure 10-19: Status of vEOS Deployment to AWS



Provider ↑	VM Name	VPC	Progress
Filter	Filter	Filter	Filter
Amazon Web Services	VM-vEOS	vpc-0e1dd269	Success ⓘ

You can also check the VM deployment process on your AWS Portal. Hover the mouse over the corresponding information icon to view detailed information about the vEOS router deployment. After the successful deployment of the vEOS router to AWS, you can use your AWS SSH Privacy Enhanced Mail (PEM) key to login to vEOS.

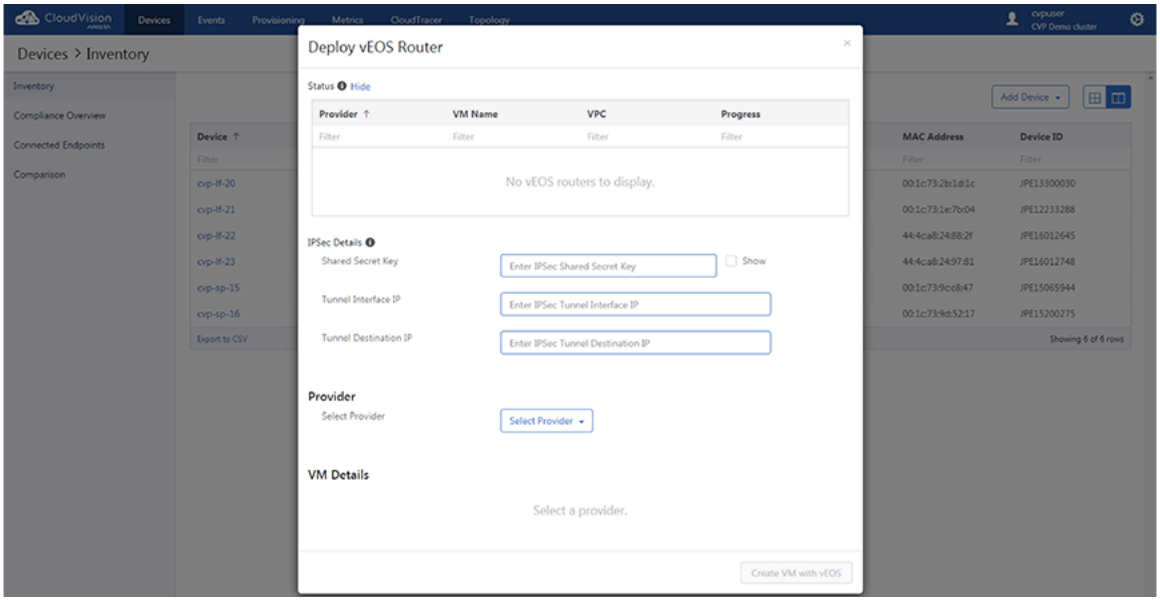
Note: To make CVP manage vEOS routers, register this device using the instructions in Registering Devices. Ensure that the AWS security group associated with vEOS router VM has an ingress rule of allowing TCP port 9910 from CVP's IP address. You must configure AWS for the vEOS router to function as a VPC gateway using the instructions in Using vEOS Router on the AWS Platform.

10.4.2.5 Deploying a vEOS Router to Microsoft Azure

Perform the following steps to deploy a vEOS router to the Azure VNET:

1. Click **Devices**. The system displays the **Inventory** screen.
2. Click the **Add Devices** drop-down menu at the upper right corner of the right pane.
3. Select **Deploy vEOS Router**. The system displays the **Deploy vEOS Router** window.
4. Provide the following IPSec details in the appropriate fields:
   - **Shared Secret Key** (optional) - Pre-shared key for IPSec profile
   - **Tunnel Interface IP** (optional) - IP address under tunnel interface
   - **Tunnel#1 Destination IP** (optional) - Peer's (tunnel destination) IP address
5. Select **Azure** from the **Select Provider** drop-down menu.

Figure 10-20: VM Details for Microsoft Azure



Device ↑	MAC Address	Device ID
Filter	Filter	Filter
cvp-lf-20	00:1c:73:2b:1d:1c	JPE13300030
cvp-lf-21	00:1c:73:1e:7b:04	JPE12233288
cvp-lf-22	44:4c:a8:24:88:2f	JPE16012645
cvp-lf-23	44:4c:a8:24:97:81	JPE16012748
cvp-sp-15	00:1c:73:9c:c8:47	JPE15065944
cvp-sp-16	00:1c:73:9d:52:17	JPE15200275

Deploy vEOS Router

Status Hide

Provider ↑	VM Name	VPC	Progress
Filter	Filter	Filter	Filter

No vEOS routers to display.

IPSec Details

Shared Secret Key: Enter IPSec Shared Secret Key □ Show

Tunnel Interface IP: Enter IPSec Tunnel Interface IP

Tunnel Destination IP: Enter IPSec Tunnel Destination IP

Provider

Select Provider: Select Provider ▾

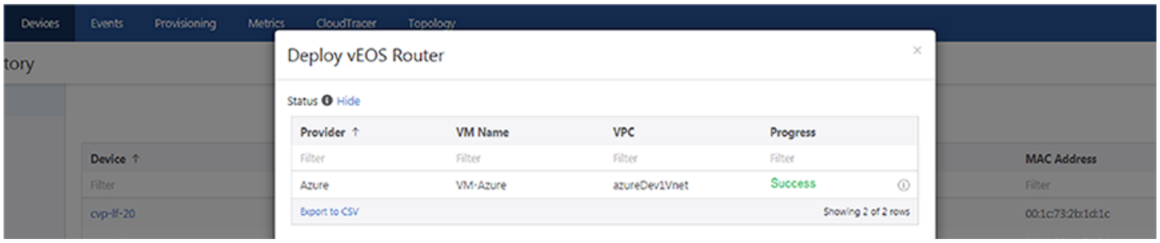
VM Details

Select a provider.

6. Provide the following VM details in the appropriate fields:
   - **Name** - The name of the vEOS router instance.
   - **Subscription ID** - The subscription that the vEOS router will be deployed to.
   - **Instance Size** - The size of vEOS router that the instance will run on.
   - **Resource Group** - The resource group that the vEOS router will be deployed to.
   - **Location** - The Azure region that contains the VNET.
   - **Security Group** - The network security group that will be associated with the vEOS interface.
   - **Virtual Network** - The VNET that vEOS will be deployed in.
   - **Subnet #1** - The first subnet that vEOS puts Ethernet1 in.
   - **Assign Public IP Address to Subnet #1** - Select Yes if you need a public IP address assigned to vEOS router, else select No.
   - **Use Public IP Address as Local ID** - The public IP address of vEOS Router.

     Note: The system displays the public IP address of vEOS router after the VM is created.
   - **Subnet #2** - The second subnet that vEOS puts Ethernet2 in.
   - **Configlet** - The configlet to configure vEOS once it is up.
   - **EOS Image** - The vEOS images on Azure marketplace.
7. Click **Create VM with vEOS**. The system displays the status of vEOS deployment under the Progress column in the Status pane.

   Figure 10-21: Status of vEOS Deployment to Microsoft Azure



Deploy vEOS Router

Status Hide

Provider ↑	VM Name	VPC	Progress
Filter	Filter	Filter	Filter
Azure	VM-Azure	azureDev1Vnet	Success

Export to CSV — Showing 2 of 2 rows

You can also check the VM deployment process on your Microsoft Azure Portal. Hover the mouse over the corresponding information icon to view detailed information about the vEOS router's deployment. It contains the initial login credentials you can use to login to vEOS router, you can change the credentials after logging into the device.

Note: To make CVP manage vEOS routers, register this device using the instructions in Registering Devices. Ensure that the Azure network security group associated with vEOS router VM has an ingress rule of allowing TCP port 9910 from CVP's IP address. You must configure Microsoft Azure for the vEOS router to function as VNET gateway using the instructions in **Using the vEOS Router on Microsoft Azure**.

10.4.2.6 Adding Microsoft Azure to Public Cloud Accounts

You need a subscription ID, a tenant ID, a client ID, and client server details in order to an azure account to public cloud accounts.

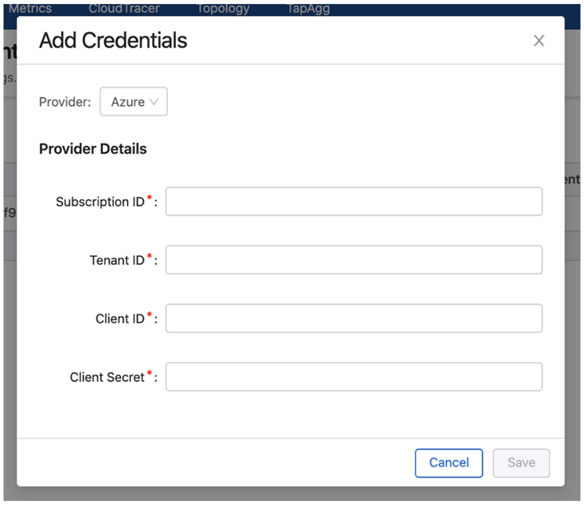
To get these details, you must create an application in the Azure active directory and assign proper permissions to CVP for authentication with Microsoft Azure environment to make API calls. CVP uses a few APIs to create a vEOS router. Therefore, you must add a contributor role to the resource group that has either Virtual Network Protocol (VNET) or the whole subscription.

Perform the following steps for adding the Microsoft Azure account to public cloud accounts:

1. Click **Provisioning**. The system displays the **Network Provisioning** screen.
2. Click **Public Cloud Accounts** in the left pane. The system displays the **Public Cloud Accounts** screen.

3. Click **Add Credentials** in the upper right corner of the right pane. The system displays the **Add Credentials** window.

Figure 10-22: Add Credentials Window for Microsoft Azure



Provider: Azure

Provider Details

Subscription ID*:

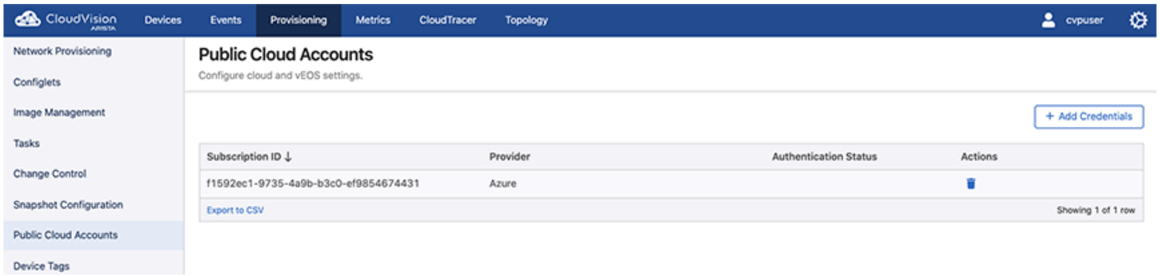
Tenant ID*:

Client ID*:

Client Secret*:

4. Select **Azure** from the **Provider** drop-down menu.
5. Under the **Provider Details** pane, provide the subscription ID, tenant ID, client ID, and client server details in the appropriate fields.
6. Click **Save**. The system displays the configured Microsoft Azure account in the **Public Cloud Accounts** screen.

Figure 10-23: Microsoft Azure Configured in Public Cloud Accounts



Public Cloud Accounts

Configure cloud and vEOS settings.

Subscription ID ↓	Provider	Authentication Status	Actions
f1592ec1-9735-4a9b-b3c0-ef9854674431	Azure		🗑

Showing 1 of 1 row

10.4.3 Registering Devices

Registering is the method used for adding devices to CVP. As a part of registering devices, CloudVision automatically enables streaming of the registered devices' state to the cluster by installing and configuring the TerminAttr agent. Newly registered devices are always placed under an undefined container.

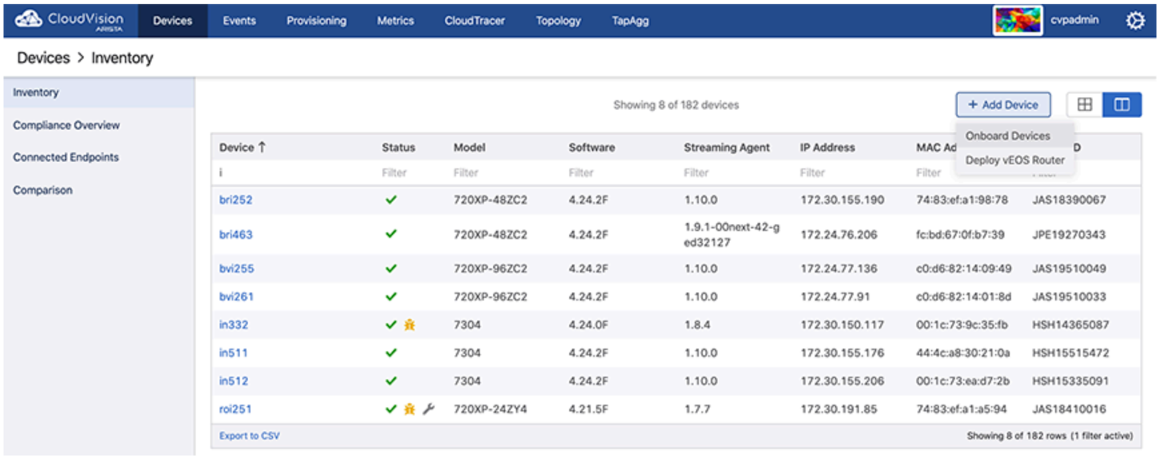
Note: Manual installation or configuration of streaming telemetry is not required prior to registration.

Complete the following steps to register devices with CVP:

1. Navigate to the **Inventory** screen.

2. Click the **Add Device** drop-down menu and select **Register Existing Device**. The **Device Registration** pop-up window appears.

Figure 10-24: Add Device for Registration



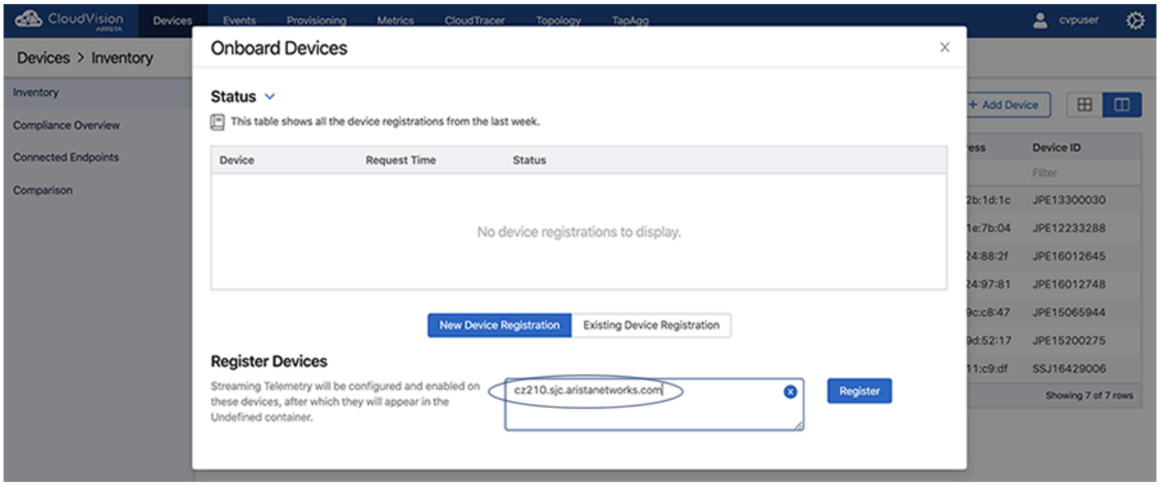
Showing 8 of 182 devices

Device ↑	Status	Model	Software	Streaming Agent	IP Address	MAC Ad	D
bri252	✓	720XP-48ZC2	4.24.2F	1.10.0	172.30.155.190	74:83:ef:a1:98:78	JAS18390067
bri463	✓	720XP-48ZC2	4.24.2F	1.9.1-00next-42-g ed32127	172.24.76.206	fc:bd:67:0f:b7:39	JPE19270343
bvi255	✓	720XP-96ZC2	4.24.2F	1.10.0	172.24.77.136	c0:d6:82:14:09:49	JAS19510049
bvi261	✓	720XP-96ZC2	4.24.2F	1.10.0	172.24.77.91	c0:d6:82:14:01:8d	JAS19510033
in332	✓	7304	4.24.0F	1.8.4	172.30.150.117	00:1c:73:9c:35:fb	HSH14365087
in511	✓	7304	4.24.2F	1.10.0	172.30.155.176	44:4c:a8:30:21:0a	HSH15515472
in512	✓	7304	4.24.2F	1.10.0	172.30.155.206	00:1c:73:ea:d7:2b	HSH15335091
roi251	✓	720XP-24ZY4	4.21.5F	1.7.7	172.30.191.85	74:83:ef:a1:a5:94	JAS18410016

Showing 8 of 182 rows (1 filter active)

3. Enter the host name or IPv4 addresses of the device(s) to be registered; and click **Register**.

Figure 10-25: Selecting Device for Registering



Onboard Devices

Status

This table shows all the device registrations from the last week.

Device	Request Time	Status

No device registrations to display.

Register Devices

Streaming Telemetry will be configured and enabled on these devices, after which they will appear in the Undefined container.

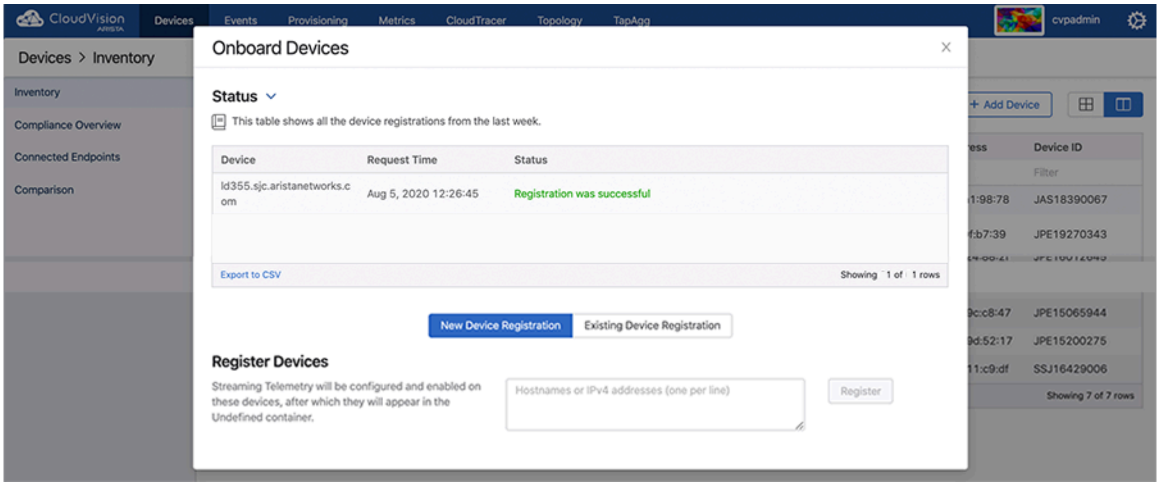
cz210.sjc.aristanetworks.com

ess	Device ID
2b:1d:1c	JPE13300030
1e:7b:04	JPE12233288
24:88:2f	JPE16012645
24:97:81	JPE16012748
9c:c8:47	JPE15065944
9d:52:17	JPE15200275
11:c9:df	SSJ16429006

Showing 7 of 7 rows

The following figures show the device registration status through the registration process.

Figure 10-26: Registration Status



Onboard Devices

Status

This table shows all the device registrations from the last week.

Device	Request Time	Status
ld355.sjc.aristanetworks.com	Aug 5, 2020 12:26:45	Registration was successful

Export to CSV — Showing 1 of 1 rows

New Device Registration | Existing Device Registration

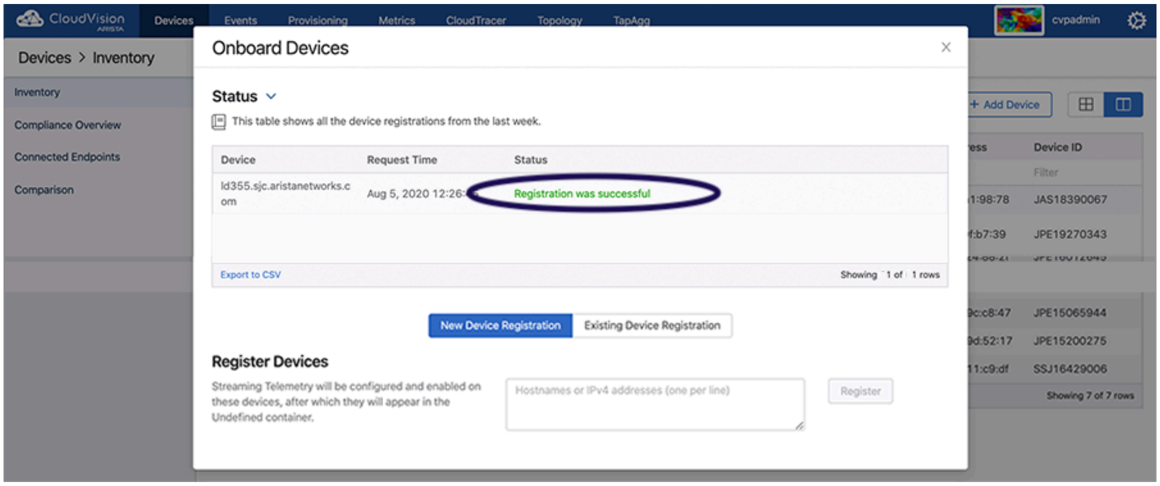
Register Devices

Streaming Telemetry will be configured and enabled on these devices, after which they will appear in the Undefined container.

Hostnames or IPv4 addresses (one per line)

Register

Figure 10-27: Registration Successful



Onboard Devices

Status

This table shows all the device registrations from the last week.

Device	Request Time	Status
ld355.sjc.aristanetworks.com	Aug 5, 2020 12:26:45	Registration was successful

Export to CSV — Showing 1 of 1 rows

New Device Registration | Existing Device Registration

Register Devices

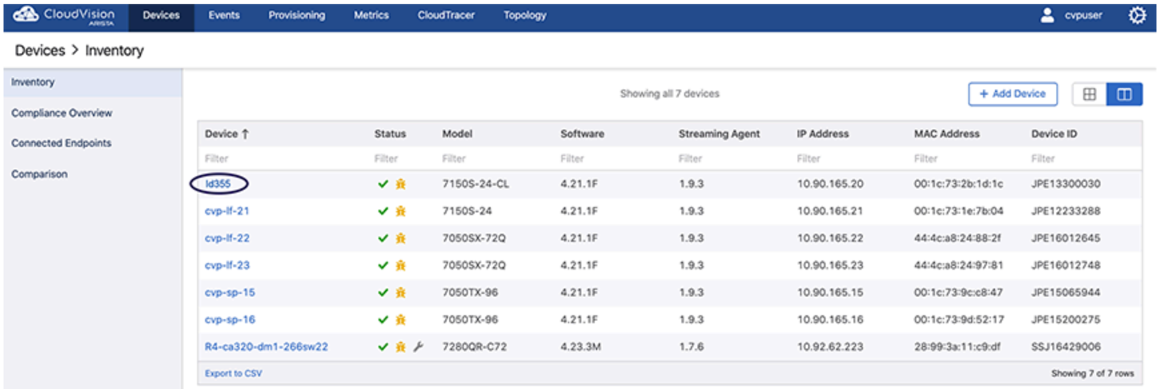
Streaming Telemetry will be configured and enabled on these devices, after which they will appear in the Undefined container.

Hostnames or IPv4 addresses (one per line)

Register

The newly registered devices are now shown in the inventory.

Figure 10-28: List of Registered Devices



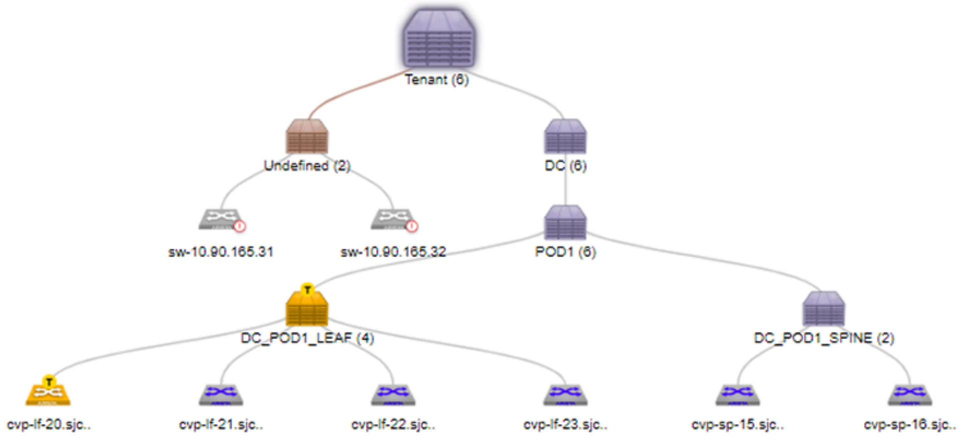
Showing all 7 devices

Device ↑	Status	Model	Software	Streaming Agent	IP Address	MAC Address	Device ID
ld355	✓	7150S-24-CL	4.21.1F	1.9.3	10.90.165.20	00:1c:73:2b:1d:1c	JPE13300030
cvp-lf-21	✓	7150S-24	4.21.1F	1.9.3	10.90.165.21	00:1c:73:1e:7b:04	JPE12233288
cvp-lf-22	✓	7050SX-72Q	4.21.1F	1.9.3	10.90.165.22	44:4c:a8:24:88:2f	JPE16012645
cvp-lf-23	✓	7050SX-72Q	4.21.1F	1.9.3	10.90.165.23	44:4c:a8:24:97:81	JPE16012748
cvp-sp-15	✓	7050TX-96	4.21.1F	1.9.3	10.90.165.15	00:1c:73:9c:c8:47	JPE15065944
cvp-sp-16	✓	7050TX-96	4.21.1F	1.9.3	10.90.165.16	00:1c:73:9d:52:17	JPE15200275
R4-ca320-dm1-266sw22	✓	7280QR-C72	4.23.3M	1.7.6	10.92.62.223	28:99:3a:11:c9:df	SSJ16429006

Export to CSV — Showing 7 of 7 rows

The newly registered devices are shown in the undefined container in the **Network Provisioning** view.

Figure 10-29: Registered Devices in the Network Provisioning View



10.4.4 Moving Devices from one Container to Another Container

Moving devices from one defined container to another is a method you can use to add devices to a container in the CVP topology. You use this method when you want to add devices to a container, and the device you want to add is currently under another container in the CVP topology. This method involves locating the device to be moved, and then moving it to the destination container. Containers that receive the imported devices are called destination containers.

There are three options you can use to move devices. They are:

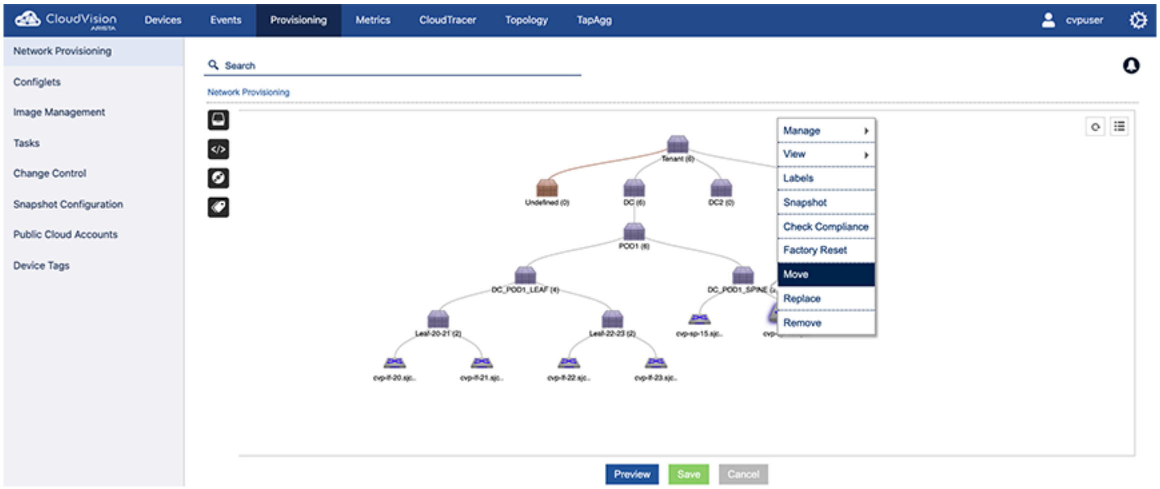
- Option 1
- Option 2
- Option 3

10.4.4.1 Option 1

1. Locate the device.

2. Right-click the device and choose **Move**.

Figure 10-30: Selecting the device to be moved (option 1)

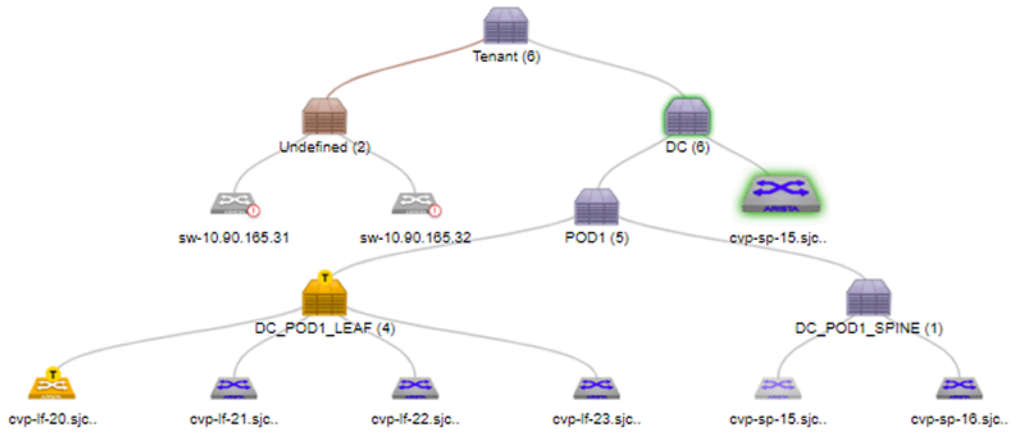


3. Select the destination container from the drop-down menu.
4. Save the session to move the device to the destination container.

10.4.4.2 Option 2

1. Locate the container that has the device you want to move.
2. Right-click the container and choose **Show All Devices**. This will load the inventory of all the devices under the container.
3. Locate the device to be moved.
4. Right-click the device and choose **Move**. After moving there will be a "T" icon to indicate the move has been tasked. (The task won't automatically be executed.)

Figure 10-31: Device with pending move task (option 2)



5. Go to Tasks and explicitly execute the move task. After the task has been executed, the "T" icon is removed.

10.4.4.3 Option 3

1. Locate the container that has the device you want to move.
2. Right-click the container and choose **Manage > Device**. This will load the inventory of all the devices under the container.
3. Select the device to be moved and click **<â€“>** to choose the destination container.
4. From the popup menu, select the destination container and click **OK**. This will provision a move for the device

10.4.5 Removing a Device from a Container

A device can be removed from a container. Removing a device from the container will:

- Remove the device from parent container.
- Clear all information about the device in the CloudVision Portal.
- Stop any monitoring of the device.

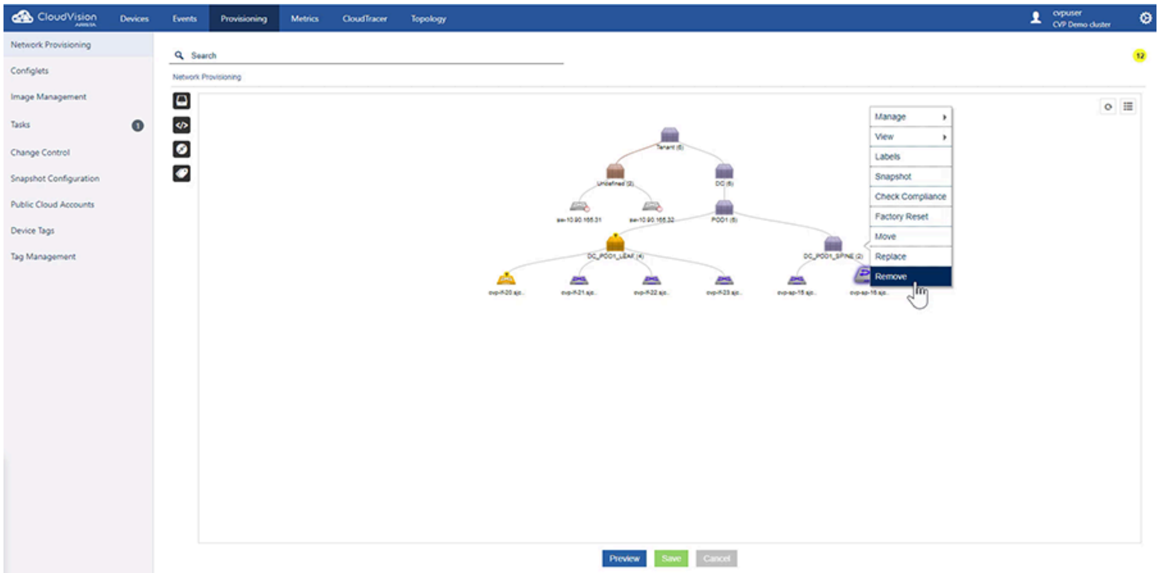
There are three options you can use to remove devices. They are:

- Option 1
- Option 2
- Option 3

10.4.5.1 Option 1

1. Locate the device.
2. Right-click the device and choose **Remove**.

Figure 10-32: Removing a device (option 1)



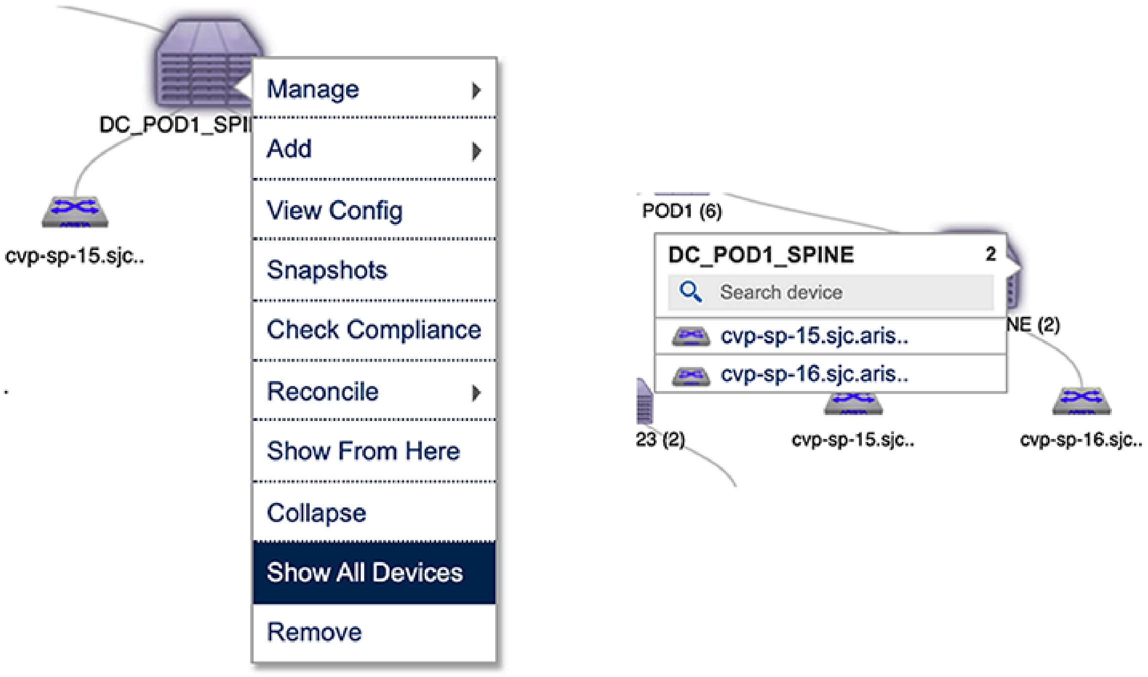
10.4.5.2 Option 2

This option is available only for topology views.

1. Locate the parent container.

2. Right-click the container and choose **Show All Devices**. All the devices under the container are listed.

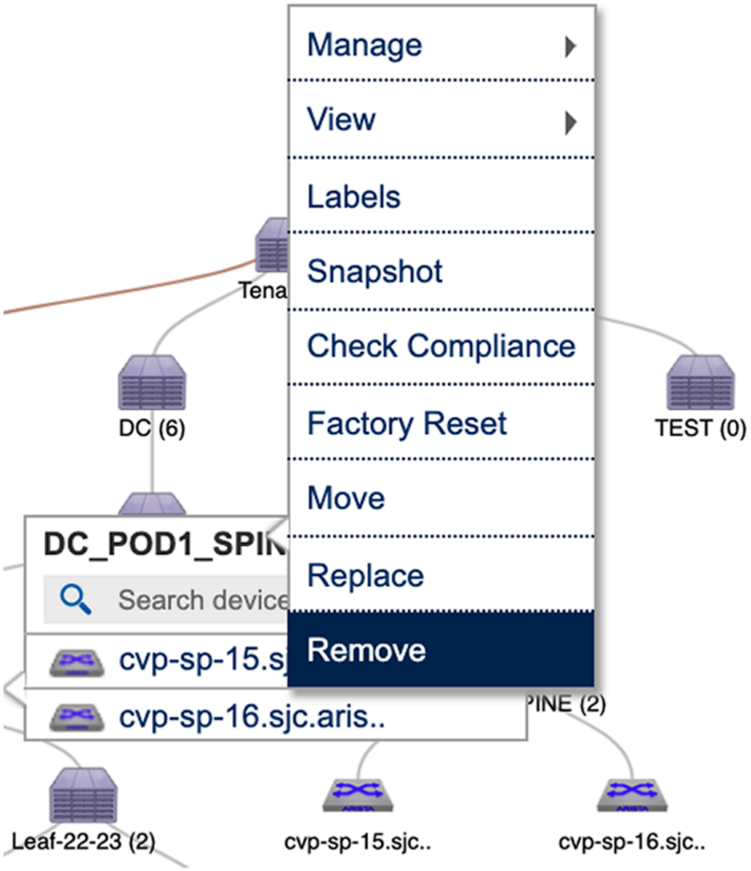
Figure 10-33: Selecting the device to be removed (option 2)



3. Select the device you want to remove.

4. Right-click the device and choose **Remove**. The device is removed from the Network Provisioning view.

Figure 10-34: Removing the device (option 2)

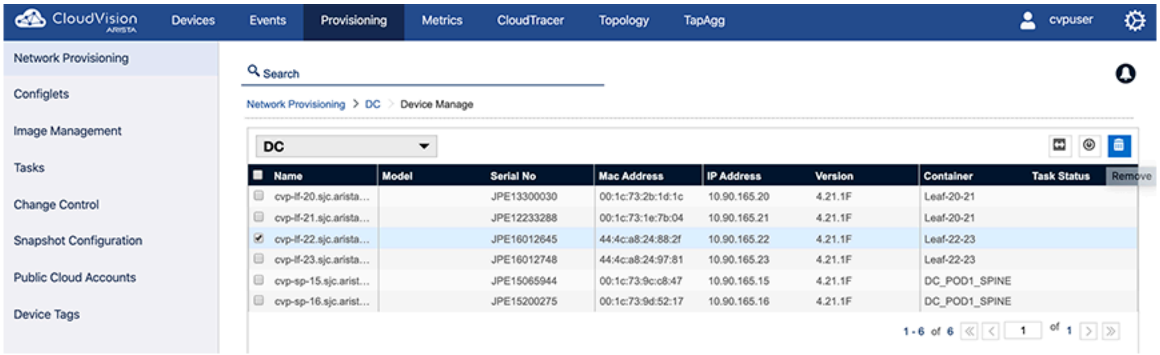


10.4.5.3 Option 3

This option is available only for the list view of the Network Provisioning screen.

1. Locate the parent container.
2. Right-click the container and choose **Manage > Device**. This will load the inventory of all the child devices under the container.

Figure 10-35: Remove device from the container (option 3)



	Name	Model	Serial No	Mac Address	IP Address	Version	Container	Task Status
□	cvp-lf-20.sjc.arista...		JPE13300030	00:1c:73:2b:1d:1c	10.90.165.20	4.21.1F	Leaf-20-21	
□	cvp-lf-21.sjc.arista...		JPE12233288	00:1c:73:1e:7b:04	10.90.165.21	4.21.1F	Leaf-20-21	
☑	cvp-lf-22.sjc.arista...		JPE16012645	44:4c:a8:24:88:2f	10.90.165.22	4.21.1F	Leaf-22-23	
□	cvp-lf-23.sjc.arista...		JPE16012748	44:4c:a8:24:97:81	10.90.165.23	4.21.1F	Leaf-22-23	
□	cvp-sp-15.sjc.arist...		JPE15065944	00:1c:73:9c:c8:47	10.90.165.15	4.21.1F	DC_POD1_SPINE	
□	cvp-sp-16.sjc.arist...		JPE15200275	00:1c:73:9d:52:17	10.90.165.16	4.21.1F	DC_POD1_SPINE	

3. Select the device you want to remove and then click **Remove**. On saving the session, a task will be spawned to reset the selected device.

10.4.6 Device Factory Reset

When resetting a device:

- The device will be removed from the parent container.
- The running configuration of the device will be flushed.
- Device will reboot with ZTP mode enabled.
- Device will be identified under undefined container.

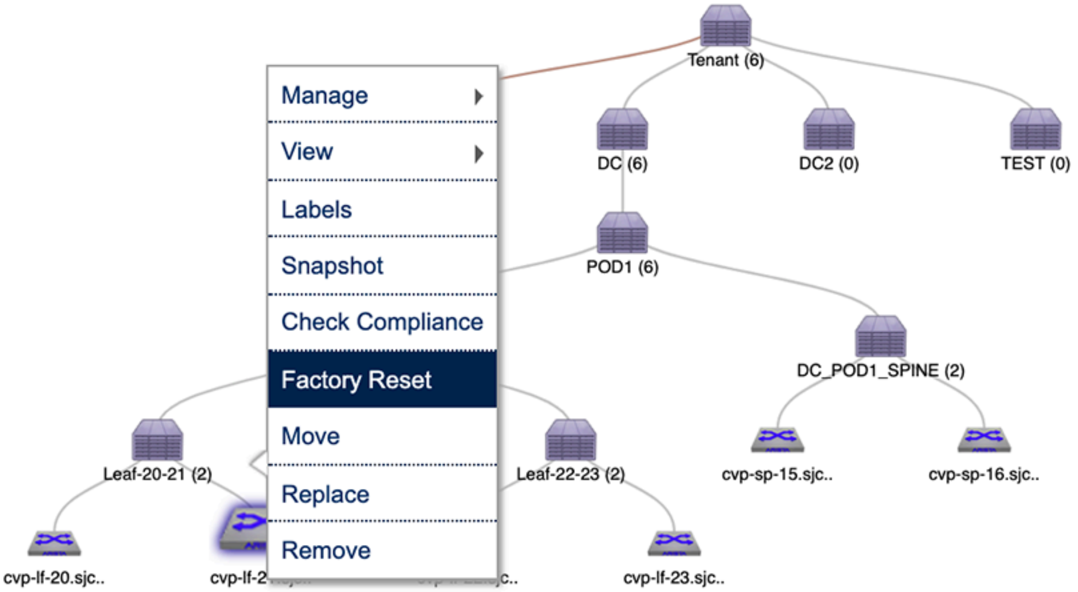
There are three options you can use to move devices. They are:

- Option 1
- Option 2
- Option 3

10.4.6.1 Option 1

1. Locate the device.
2. Right-click the device and choose **Factory Reset**.

Figure 10-36: Resetting the device (option 1)

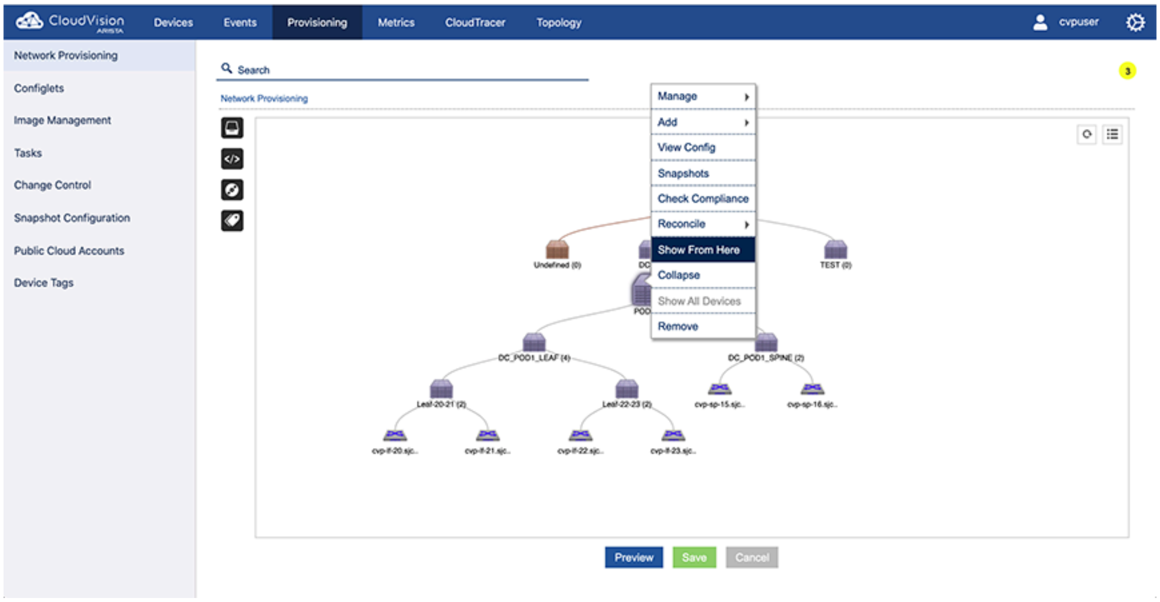


10.4.6.2 Option 2

1. Locate the parent container.

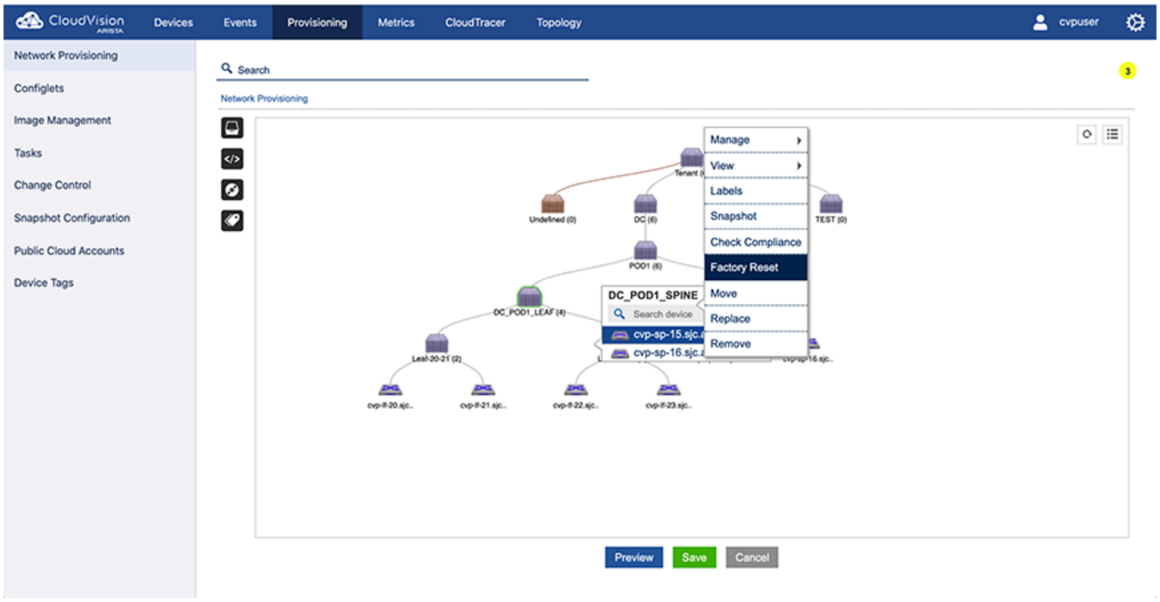
2. Right-click the container and choose **Show All Devices**. This will list all the devices under the container.

Figure 10-37: Showing all devices during factory reset (option 2)



3. Right-click the device and choose **Factory Reset**.

Figure 10-38: Resetting the device (option 2)

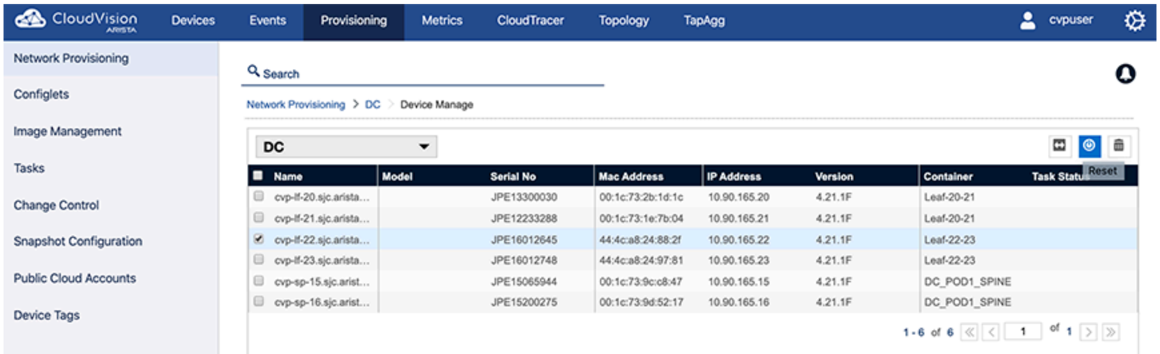


10.4.6.3 Option 3

1. Locate the parent container.
2. Right-click the container and choose **Manage > Device**. This will load the inventory of all the child devices under the container.

3. Select the checkbox of the device to be reset, and click the **reset** icon. On saving the session, a task will be spawned to reset the selected device.

Figure 10-39: Selecting the device and resetting it (option 3)



☐	Name	Model	Serial No	Mac Address	IP Address	Version	Container	Task Status
☐	cvp-lf-20.sjc.arista...		JPE13300030	00:1c:73:2b:1d:1c	10.90.165.20	4.21.1F	Leaf-20-21	
☐	cvp-lf-21.sjc.arista...		JPE12233288	00:1c:73:1e:7b:04	10.90.165.21	4.21.1F	Leaf-20-21	
☑	cvp-lf-22.sjc.arista...		JPE16012645	44:4c:a8:24:88:2f	10.90.165.22	4.21.1F	Leaf-22-23	
☐	cvp-lf-23.sjc.arista...		JPE16012748	44:4c:a8:24:97:81	10.90.165.23	4.21.1F	Leaf-22-23	
☐	cvp-sp-15.sjc.arist...		JPE15065944	00:1c:73:9c:c8:47	10.90.165.15	4.21.1F	DC_POD1_SPINE	
☐	cvp-sp-16.sjc.arist...		JPE15200275	00:1c:73:9d:52:17	10.90.165.16	4.21.1F	DC_POD1_SPINE	

10.5 Replacing Switches Using the ZTR Feature

The Zero Touch Replacement (ZTR) feature enables you to replace switches without having to configure the new switch. When you replace a switch using this feature, the new switch assumes the identity (IP), image, and configuration of the old switch. You use the Network Provisioning screen to replace switches using the (ZTR) feature.

Pre-requisites: Before you can begin the process to replace a switch using ZTR, make you must complete the following steps:

1. Make sure that the old switch is physically powered down and is not physically connected to the network.
2. Physically connect the new switch to the network exactly as the old switch was connected.
3. Power on the new switch.
4. Make sure the new switch comes up using ZTP, and that it shows up in the undefined container as an available resource. The new switch must have a different IP address from the switch that is being replaced at this point in the process.

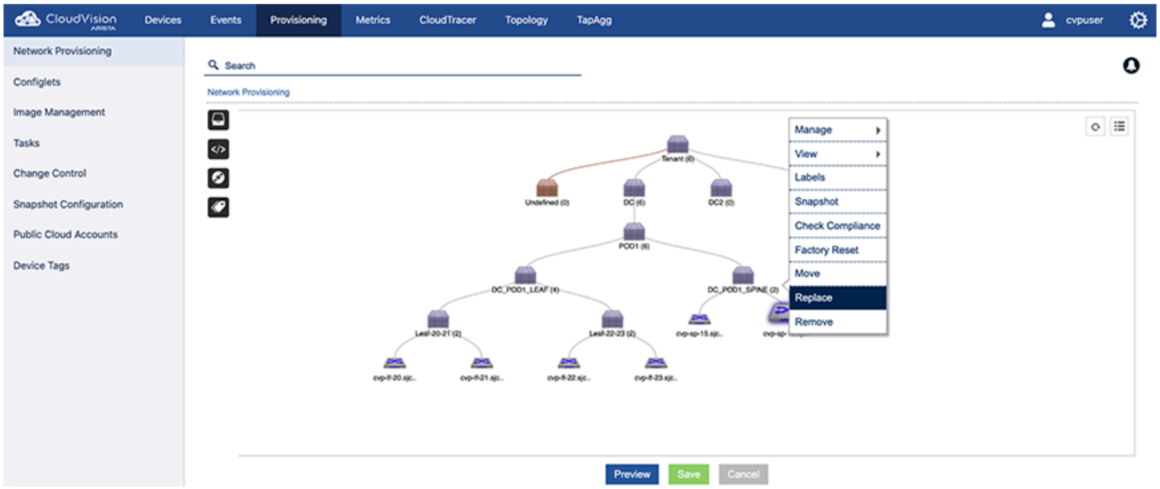
Note: Verify the new switch has a different IP address from the switch that is being replaced.

Complete these steps to replace a switch using ZTP:

1. Go to the **Network Provisioning** screen.

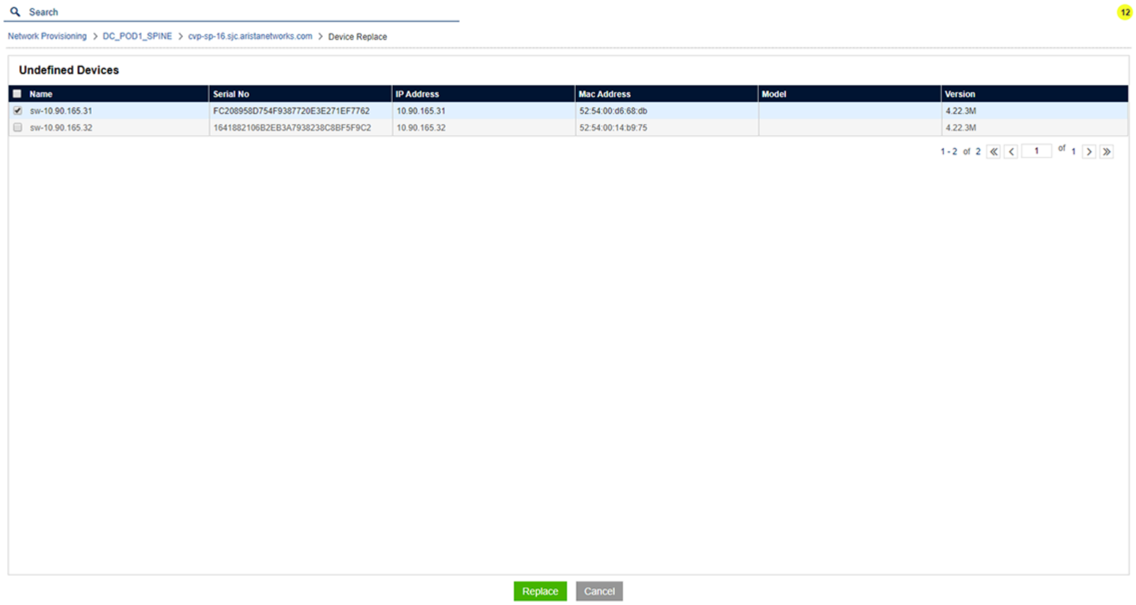
2. Right-click on the old switch, and select **Replace**. This initiates ZTR, and opens the **Undefined Device** screen.

Figure 10-40: Selecting the switch to be replaced



3. Select the new switch by checking the checkbox next to the Serial No. column, and then click **Replace**.

Figure 10-41: Selecting the new device and replacing the old device



Search

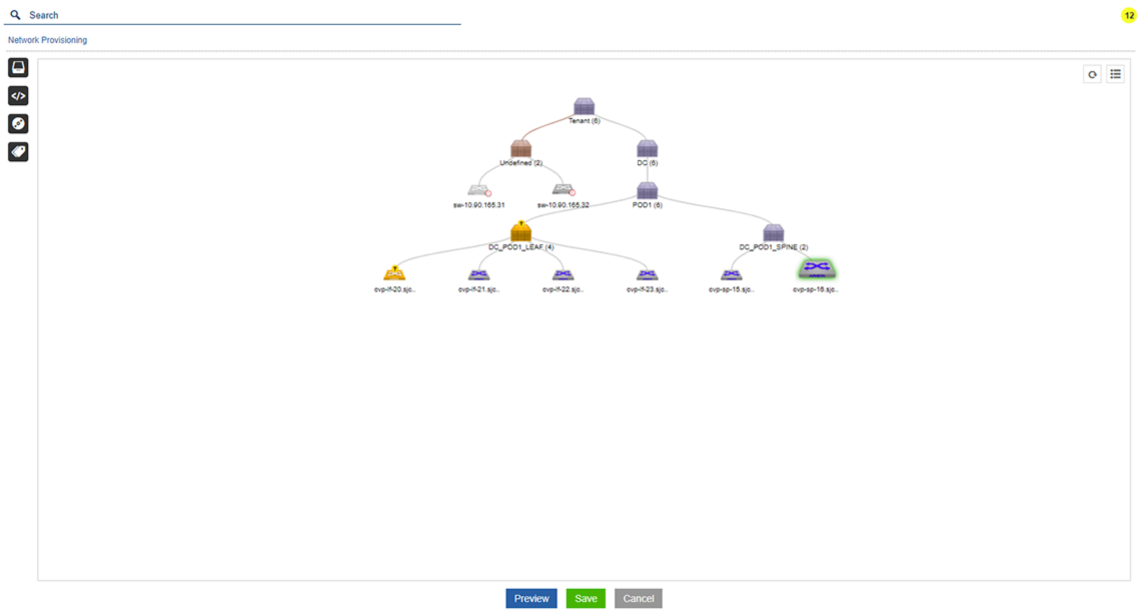
Network Provisioning > DC_POD1_SPINE > cvp-sp-16.sjc.aristanetworks.com > Device Replace

Undefined Devices

□	Name	Serial No	IP Address	Mac Address	Model	Version
☑	sw-10.90.165.31	FC208958D754F9387720E3E271EF7762	10.90.165.31	52:54:00:d6:68:db		4.22.3M
□	sw-10.90.165.32	1641882106B2EB3A7938238C8BF5F9C2	10.90.165.32	52:54:00:14:b9:75		4.22.3M

4. In the Network Provisioning screen, click **Save**. A task icon **T** shows on the old switch, indicating that a task to replace it has been scheduled. Also, an **R** icon shows on the new switch, indicating that it is the replacement switch for a scheduled ZTR task.

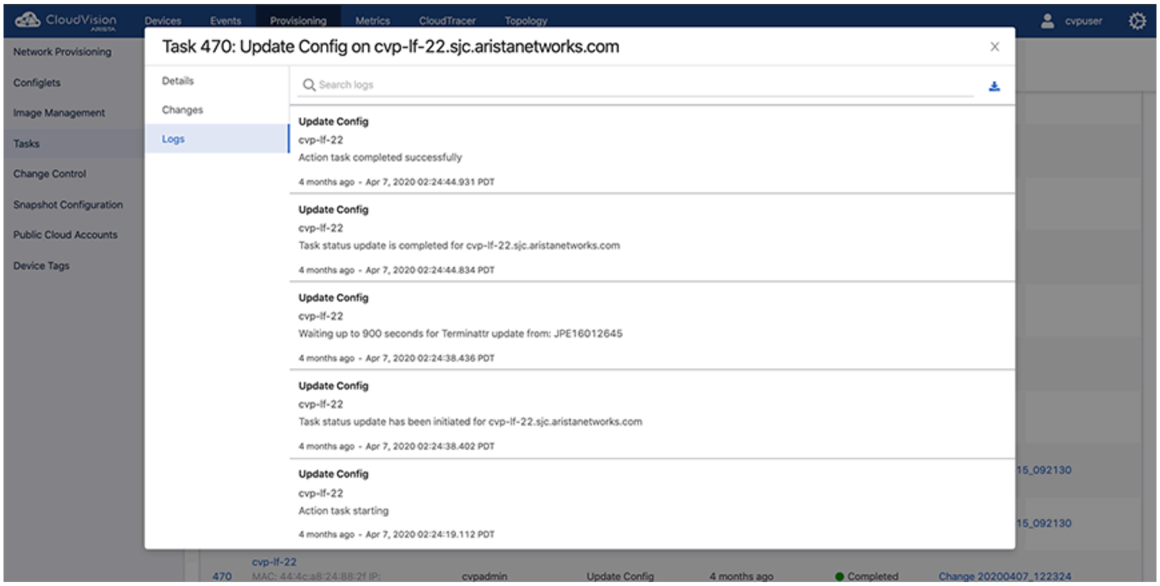
Figure 10-42: Topology view showing device with pending replace task



5. Go to the **Tasks** screen.
6. Select the task and click the play icon to execute the task.

While the task is executing, you can open the logs for the task to view how ZTR manages the replacement. ZTR first pushes the old switches image and configuration to the new replacement switch, and then initiates the reboot.

Figure 10-43: Task log showing processing of device replacement



Task 470: Update Config on cvp-lf-22.sjc.aristanetworks.com

```
Update Config
cvp-lf-22
Action task completed successfully
4 months ago • Apr 7, 2020 02:24:44.931 PDT

Update Config
cvp-lf-22
Task status update is completed for cvp-lf-22.sjc.aristanetworks.com
4 months ago • Apr 7, 2020 02:24:44.834 PDT

Update Config
cvp-lf-22
Waiting up to 900 seconds for Terminattr update from: JPE16012645
4 months ago • Apr 7, 2020 02:24:38.436 PDT

Update Config
cvp-lf-22
Task status update has been initiated for cvp-lf-22.sjc.aristanetworks.com
4 months ago • Apr 7, 2020 02:24:38.402 PDT

Update Config
cvp-lf-22
Action task starting
4 months ago • Apr 7, 2020 02:24:19.112 PDT
```

470	cvp-lf-22 MAC: 44:4c:a8:24:88:2f IP:	cvpadmin	Update Config	4 months ago	● Completed	Change 20200407_122324

10.6 Managing Configurations

CloudVision Portal (CVP) enables you to manage configurations by assigning configurations to containers and to devices. Configurations that you assign to containers are applied to all devices under the container's hierarchy. CVP also enables you to easily view the configuration currently assigned to containers and devices.

- Applying Configurations to Containers
- Viewing the Configuration Applied to Devices
- Applying Configurations to a Device

10.6.1 Applying Configurations to Containers

Applying configurations to containers involves adding Configlets to containers or removing Configlets from containers.

Adding Configlets

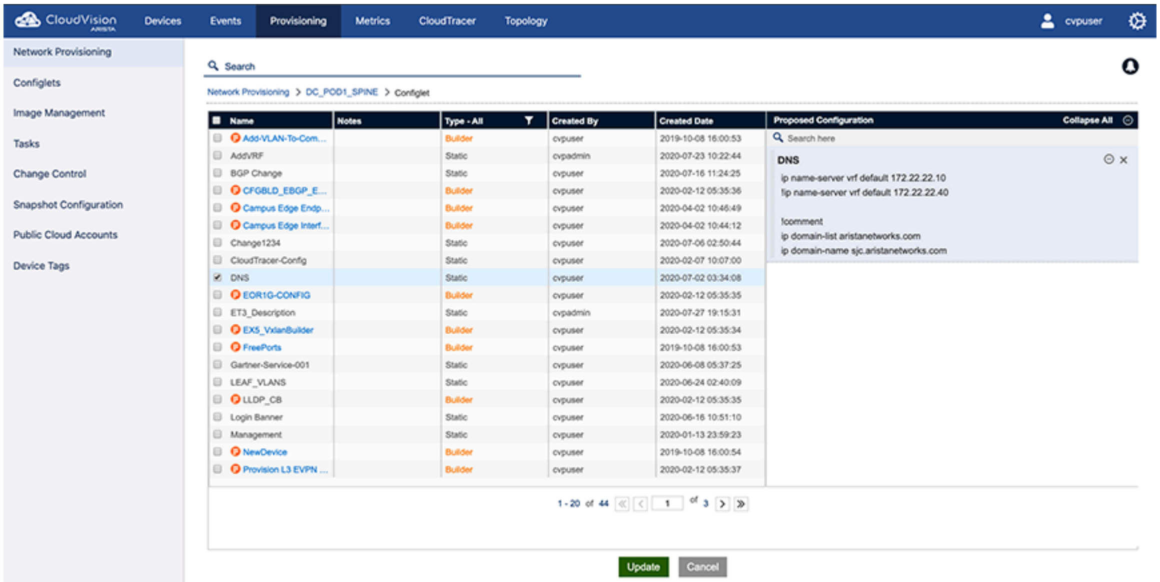
1. Locate the container.
2. Right-click the container and choose **Manage >Configlet**. This will open the window display the inventory of configlets.
3. Select the configlet and click **Update**. This will provision configlet add for the container and all the devices under it.

Removing Configlets

To remove the configlet inventory from a container.

1. Locate the container.
2. Right-click the container and choose **Manage>Configlet** .
3. Remove the configlets.
4. Click **Update**.

Figure 10-44: Remove the configlet and select Update



□ Name	Notes	Type - All	Created By	Created Date
□ Add-VLAN-To-Com...		Builder	cvpuser	2019-10-08 16:00:53
□ AddVRF		Static	cvpadmin	2020-07-23 10:22:44
□ BGP Change		Static	cvpuser	2020-07-16 11:24:25
□ CFGBLD_EBGP_E...		Builder	cvpuser	2020-02-12 05:35:36
□ Campus Edge Endp...		Builder	cvpuser	2020-04-02 10:46:49
□ Campus Edge Interf...		Builder	cvpuser	2020-04-02 10:44:12
□ Change1234		Static	cvpuser	2020-07-06 02:50:44
□ CloudTracer-Config		Static	cvpuser	2020-02-07 10:07:00
☑ DNS		Static	cvpuser	2020-07-02 03:34:08
□ EOR1G-CONFIG		Builder	cvpuser	2020-02-12 05:35:35
□ ET3_Description		Static	cvpadmin	2020-07-27 19:15:31
□ EX5_VxlanBuilder		Builder	cvpuser	2020-02-12 05:35:34
□ FreePorts		Builder	cvpuser	2019-10-08 16:00:53
□ Gartner-Service-001		Static	cvpuser	2020-06-08 05:37:25
□ LEAF_VLANS		Static	cvpuser	2020-06-24 02:40:09
□ LLDP_CB		Builder	cvpuser	2020-02-12 05:35:35
□ Login Banner		Static	cvpuser	2020-06-16 10:51:10
□ Management		Static	cvpuser	2020-01-13 23:59:23
□ NewDevice		Builder	cvpuser	2019-10-08 16:00:54
□ Provision L3 EVPN ...		Builder	cvpuser	2020-02-12 05:35:37

DNS

```
ip name-server vrf default 172.22.22.10
!ip name-server vrf default 172.22.22.40


!comment
ip domain-list aristanetworks.com
ip domain-name sjc.aristanetworks.com
```

10.6.2 Applying Configurations to a Device

Applying configurations to devices involves adding Configlets to devices.

Note: When you update a device configuration using configlets, CVP replaces the entire device configuration with the Designed Configuration for the device. For new devices with pre-existing configurations added into CVP, you must explicitly perform a one-time reconciliation to save the desired device-specific running configuration in CVP. If you do not, that configuration may be lost, or the configuration update task may fail (see Reconciling Device Configurations at the Device Level).

Adding Configlets

1. Select the device and choose **Manage > Configlets**.

   This loads the configlet inventory screen.
2. Select the configlets.

   You are required to validate the configuration.
3. To validate the configurations, select **Validate**.

   The validation screen will be loaded.
4. Select **Save** to propose a Config Assign action.

   When saving the session, this will spawn a Config Assign task.

10.6.3 Viewing the Configuration Applied to Devices

CloudVision Portal (CVP) enables you to use the **Network Provisioning** screen to view the configuration (Confliglets) currently assigned to devices. When you view the Configlets, you can also see which Configlets are inherited from Containers, and which are applied directly to the device.

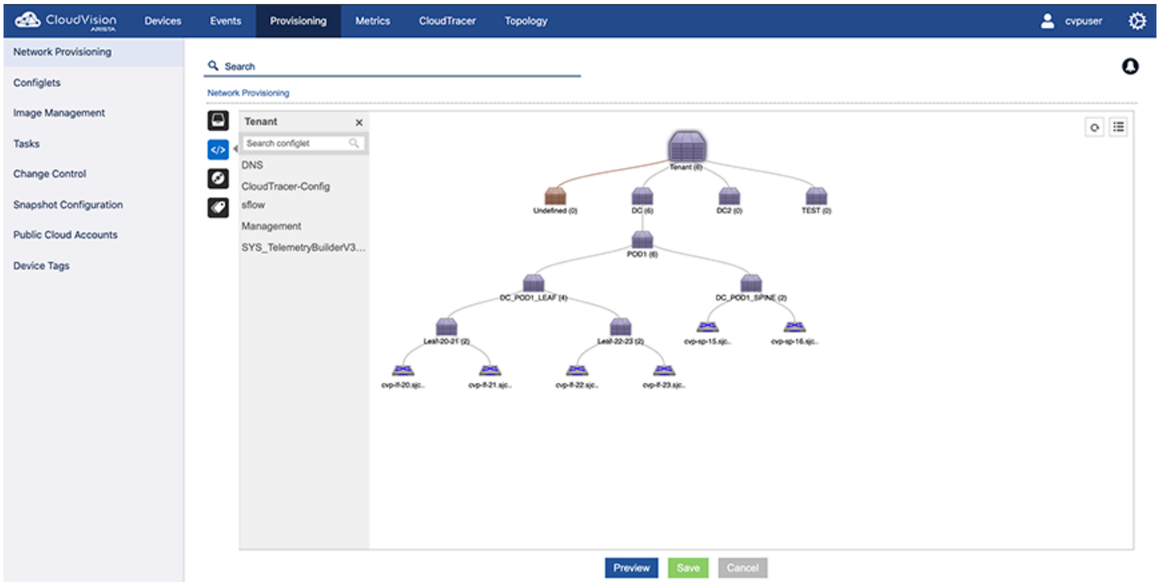
Complete the following steps to view the Configlets applied to a device.

1. Go to the **Network Provisioning** screen.
2. Make sure you are using the topology view, not the list view.
3. Click on the device in the topology.
4. Click the Configlet icon.

   The Configlets applied to the device are listed in a drop-down list.

   - If a Configlet is inherited from a Container to which the device belongs, the Container icon appears in front of the Configlet name.
   - If a Configlet is directly applied to the device, no Container icon is shown next to the Configlet name.

Figure 10-45: Viewing the Configlets applied to a device



10.6.4 Rolling Back Configurations Assigned to a Device

CloudVision's Network Rollbacks feature enables you to restore a previous configuration to devices. You can apply the rollback to all the devices in a container, or to single devices. When you rollback a container or device, you select the date and time for the rollback and whether you want to rollback the configuration or EOS image (or both).

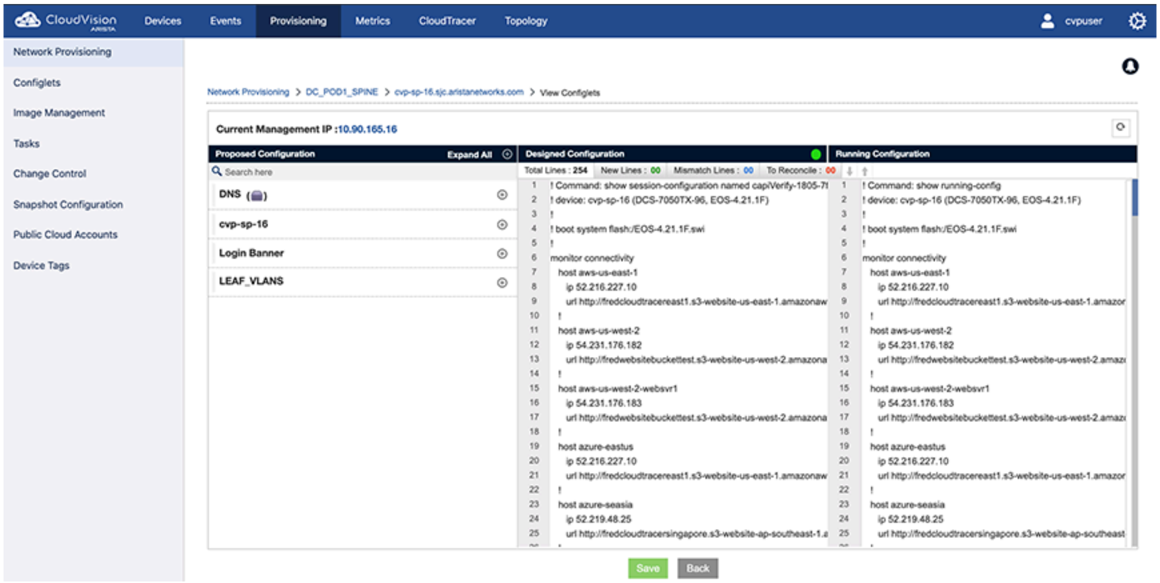
See Rolling Back Images and Configurations for details.

10.7 Configuration Validation

The validation screen consists of three panes.

- Pane 1: Shows the proposed configuration.
- Pane 2: Shows the designed configuration. (This shows how a resulting running configuration will look like after successful configuration push.)
- Pane 3: Shows the current running configuration of a device.

Figure 10-46: Validating your configurations



Current Management IP :10.90.165.16

Total Lines : 254 New Lines : 00 Mismatch Lines : 00 To Reconcile : 00

```
! Command: show session-configuration named capiVerify-1805-7t
! device: cvp-sp-16 (DCS-7050TX-96, EOS-4.21.1F)
!
! boot system flash:/EOS-4.21.1F.swi
!
monitor connectivity
  host aws-us-east-1
    ip 52.216.227.10
    url http://fredcloudtracereast1.s3-website-us-east-1.amazonaw
  !
  host aws-us-west-2
    ip 54.231.176.182
    url http://fredwebsitebuckettest.s3-website-us-west-2.amazona
  !
  host aws-us-west-2-websvr1
    ip 54.231.176.183
    url http://fredwebsitebuckettest.s3-website-us-west-2.amazona
  !
  host azure-eastus
    ip 52.216.227.10
    url http://fredcloudtracereast1.s3-website-us-east-1.amazonaw
  !
  host azure-seasia
    ip 52.219.48.25
    url http://fredcloudtracersingapore.s3-website-ap-southeast-1.a
```

```
! Command: show running-config
! device: cvp-sp-16 (DCS-7050TX-96, EOS-4.21.1F)
!
! boot system flash:/EOS-4.21.1F.swi
!
monitor connectivity
  host aws-us-east-1
    ip 52.216.227.10
    url http://fredcloudtracereast1.s3-website-us-east-1.amazor
  !
  host aws-us-west-2
    ip 54.231.176.182
    url http://fredwebsitebuckettest.s3-website-us-west-2.amaz
  !
  host aws-us-west-2-websvr1
    ip 54.231.176.183
    url http://fredwebsitebuckettest.s3-website-us-west-2.amaz
  !
  host azure-eastus
    ip 52.216.227.10
    url http://fredcloudtracereast1.s3-website-us-east-1.amazor
  !
  host azure-seasia
    ip 52.219.48.25
    url http://fredcloudtracersingapore.s3-website-ap-southeast
```

10.8 Using Hashed Passwords for Configuration Tasks

Some EOS commands take a password or a secret key as a parameter. There are usually two ways of passing EOS command parameters:

- As plain text.
- As a hashed string.

Note: Because EOS always returns the hashed version of the command in its running configuration, using the plain text version of commands in Configlets results in the following issues:

- CVP shows that there are configuration differences that need reconciling, even if there are none.
- Compliance checks show devices to be out of compliance.

To avoid these issues, you should use the hashed version of EOS commands in Configlets (for example, use `ntp authentication-key 11 md5 7 <key>` instead of `ntp authentication-key 11 md5 0 <key>`). Using the hashed versions of commands also keeps the real password hidden.

10.9 Reconciling Configuration Differences

CloudVision enables you to reconcile differences between the designed (managed) configuration and running configuration on devices so that CVP is maintaining the full configuration of each device.

Related topics:

- Key Terms
- Reconciling Device Configurations at the Device Level
- Reconciling Device Configuration Differences at the Container Level

10.9.1 Key Terms

Reconcilable differences	Configuration differences between the designed configuration and the running configuration, which do not conflict with the configuration in any configlets, other than the reconcile configlet.
Reconcile configlet	A specially marked device configlet that is system generated and used to store reconcilable differences in order for the designed configuration to match the running configuration.

Reconciling device configuration differences does not require a task, because there is no configuration to be pushed out to the device. Reconcilable differences are only adjusted in the reconcile configlet, to match the running configuration. Because of this, there is no task pushed to change the running configuration.

When you reconcile device configuration differences, you add the reconcilable differences found in the running configuration to the reconcile configlet of the designed configuration.

For details on reconciling device configuration differences, see:

- Reconciling Device Configurations at the Device Level
- Reconciling Device Configuration Differences at the Container Level

10.9.2 Reconciling Device Configurations Differences at the Container Level

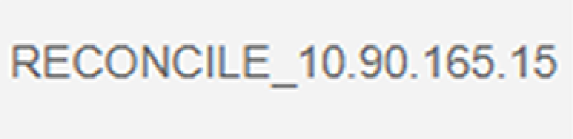
CloudVision enables you to reconcile device configuration differences for all devices under the hierarchy of a selected container, instead of having to initiate this device by device.

Note: The designed configurations of devices in the container that do not have reconcilable differences are not changed.

For devices that have reconcilable differences, the lines or commands on the device that are not present in the designed configuration are pulled into the reconcile configlet for that device in one of two ways:

- Using the existing reconcile configlet that is specific to that device.
- Creating a new reconcile configlet that is specific to that device. This is done when there is no existing reconcile configlet specific for the device. The system automatically creates a unique name for the configlet.

A green checkmark beside the configlet indicates it as the reconcile configlet for the device.



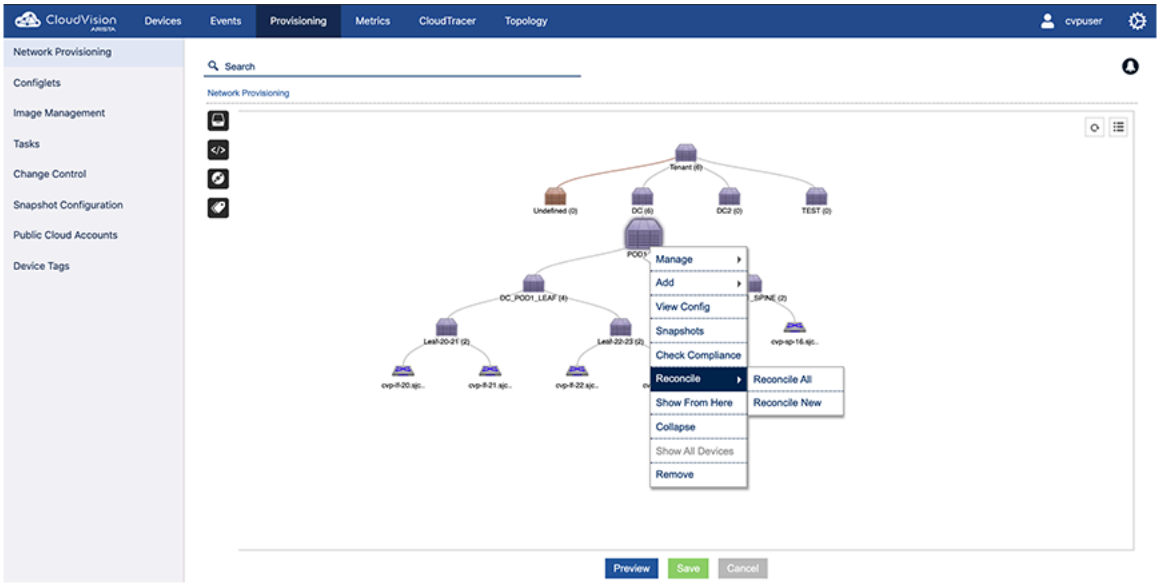
RECONCILE_10.90.165.15

Complete the following steps to reconcile device configuration differences for a container:

1. Go to the **Network Provisioning** screen.

2. Locate the container in the topology where you want to reconcile the configurations of all devices under that container hierarchy.
3. Right-click the container, hover the cursor on Reconcile, and click either **Reconcile All** or **Reconcile New**.

Figure 10-47: Device configuration reconciliation at the container level



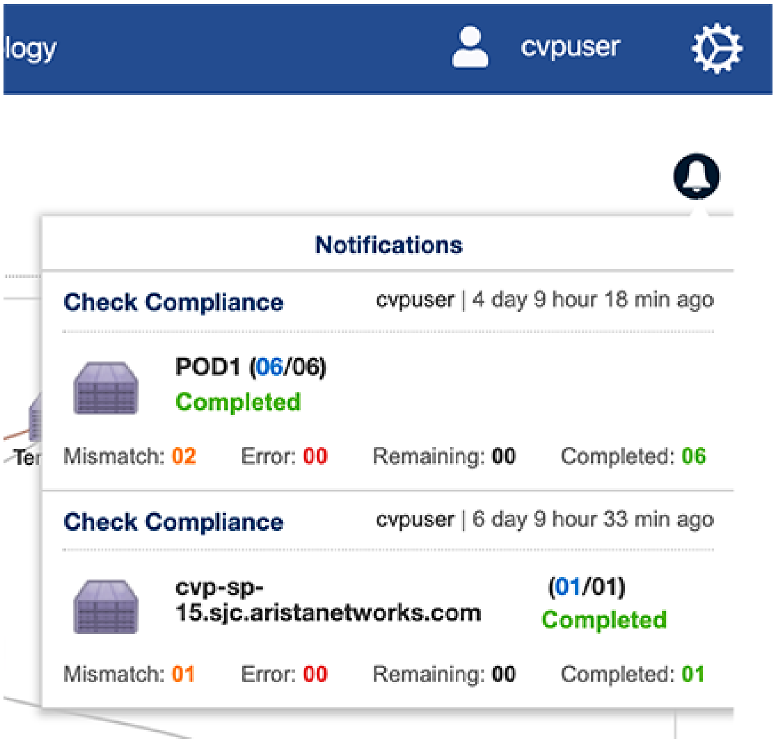
The **Reconcile New** option reconciles only the configuration lines that exist on the device, but not in the designed configuration.

The **Reconcile All** option reconciles new lines and also lines that differ in designed and running configurations. This usually brings the device into compliance because the resulting designed configuration will be identical to running configuration. However, there can be cases where in spite of reconciling device configuration lines, the designed configuration may not end up identical to running configuration. In these cases, no changes are made to the reconcile configlet. Arista recommends to go through the device-level reconcile process (See Reconciling Device Configurations at the Device Level), and select the desired lines.

Note: The bell icon in the upper right corner turns yellow to indicate unread notifications.

4. (Optional) To view the notification for the reconciliation, click the bell icon. The notification list appears showing the container-level configuration reconciliation, and any other unread notifications.

Figure 10-48: List of unread notifications



Notifications

Check Compliance cvpuser | 4 day 9 hour 18 min ago

POD1 (06/06)
Completed

Mismatch: 02 Error: 00 Remaining: 00 Completed: 06

Check Compliance cvpuser | 6 day 9 hour 33 min ago

cvp-sp-15.sjc.aristanetworks.com (01/01)
Completed

Mismatch: 01 Error: 00 Remaining: 00 Completed: 01

10.9.3 Reconciling Device Configurations at the Device Level

CloudVision enables you to reconcile device configuration differences at the device level (specific, individual devices). Configuration differences at the device level occur when there are reconcilable differences in the running configuration of the device.

The **Configuration Validation** screen shows details of the configuration differences. When the system identifies a reconcilable difference, the Reconcile option becomes available, and the extra reconcilable configuration is listed in a text editor on the screen.

Reconcile Configlets

You use a type of configlet called a reconcile configlet to reconcile device configuration differences at the device level. A reconcile configlet is a configlet for a single specific device, and is explicitly marked as the reconcile configlet for that device. The reconcile configlet for a device contains the additional running configuration for that device.

Note: There is only one reconcile configlet for any device. It is the only configlet that contains the additional running configuration for the device.

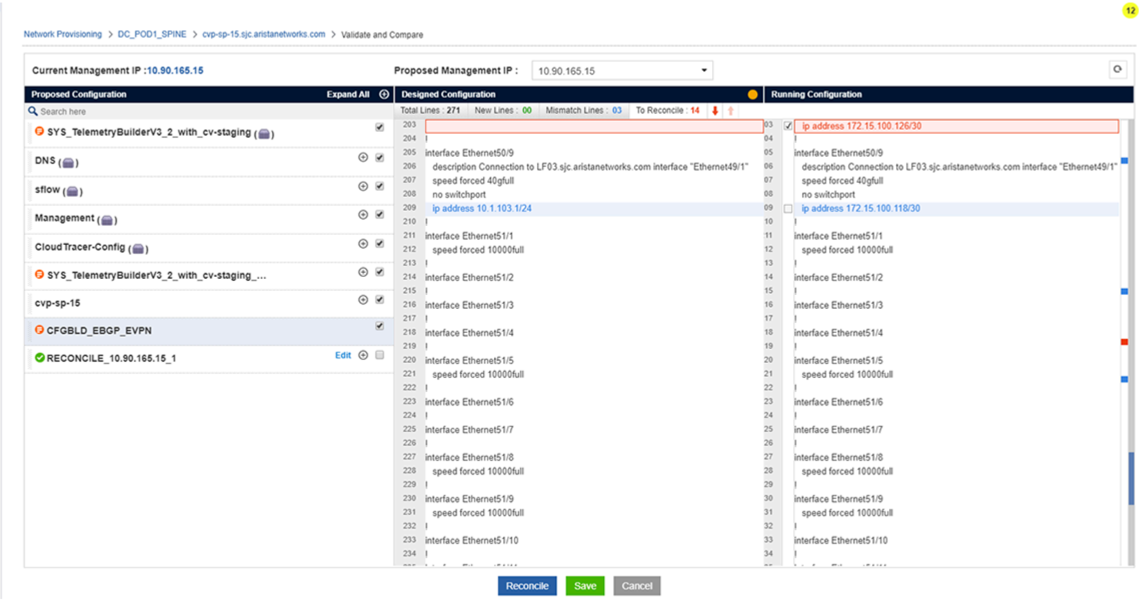
Every time a device-level or a container-level reconcile is performed, the reconcile configlet for each device included in the reconcile action is modified to include the extra running configuration.

To reconcile device level configuration, perform the following steps:

1. If required, select additional lines from running configuration to reconcile.

2. Click the blue **Reconcile** button to add the reconcilable configuration in the running configuration to the reconcile configlet of the designed configuration.

Figure 10-49: Configuration validation screen showing device-level configuration differences



Network Provisioning > DC_POD1_SPINE > cvp-sp-15.sjc.aristanetworks.com > Validate and Compare

Current Management IP :10.90.165.15

Proposed Management IP : 10.90.165.15

Proposed Configuration — Expand All

- SYS_TelemetryBuilderV3_2_with_cv-staging ☑
- DNS ☑
- sflow ☑
- Management ☑
- CloudTracer-Config ☑
- SYS_TelemetryBuilderV3_2_with_cv-staging_... ☑
- cvp-sp-15 ☑
- CFGBLD_EBGP_EVPN ☑
- RECONCILE_10.90.165.15_1 Edit □

Designed Configuration

Total Lines : 271 New Lines : 00 Mismatch Lines : 03 To Reconcile : 14

```

!
interface Ethernet50/9
  description Connection to LF03.sjc.aristanetworks.com interface "Ethernet49/1"
  speed forced 40gfull
  no switchport
  ip address 10.1.103.1/24
!
interface Ethernet51/1
  speed forced 10000full
!
interface Ethernet51/2
!
interface Ethernet51/3
!
interface Ethernet51/4
!
interface Ethernet51/5
  speed forced 10000full
!
interface Ethernet51/6
!
interface Ethernet51/7
!
interface Ethernet51/8
  speed forced 10000full
!
interface Ethernet51/9
  speed forced 10000full
!
interface Ethernet51/10
!
```

Running Configuration

```
☑ ip address 172.15.100.126/30
!
interface Ethernet50/9
  description Connection to LF03.sjc.aristanetworks.com interface "Ethernet49/1"
  speed forced 40gfull
  no switchport
□ ip address 172.15.100.118/30
!
interface Ethernet51/1
  speed forced 10000full
!
interface Ethernet51/2
!
interface Ethernet51/3
!
interface Ethernet51/4
!
interface Ethernet51/5
  speed forced 10000full
!
interface Ethernet51/6
!
interface Ethernet51/7
!
interface Ethernet51/8
  speed forced 10000full
!
interface Ethernet51/9
  speed forced 10000full
!
interface Ethernet51/10
!
```

3. (Optional) Click **Edit** next to the configlet name to edit or rename the reconciled configlet.
4. (Optional) Click the reconcile disk icon next to the configlet name to save the reconciled configlet with the extra commands present in the running configuration.

Figure 10-50: Reconcile Disk icon

RECONCILE_10.90.165.15

Note: CVP will not execute pushing a configuration that causes CVP to lose connectivity with the device if the management interface or IP is missing in the configuration. When the task is executed, it will fail.

5. Click **Save**.

10.10 Managing EOS Images Applied to Devices

CloudVision enables you to efficiently manage the EOS images of devices by assigning image bundles to containers or devices in the current CloudVision network topology. An image bundle assigned to containers are automatically applied to all devices under that container.

The image bundle you want to apply must already exist in the set of current EOS image bundles.

The following tasks are involved in managing the EOS image bundles assigned to devices:

- Applying an Image Bundle to a Container
- Viewing the Image Bundle Assigned to Devices
-
- Applying an Image Bundle to a Device
- Setting up an Image Bundle as the default for ZTP

10.10.1 Applying an Image Bundle to a Container

An image bundle can be added to, or removed from a container.

1. Select the container and choose **Manage > Image Bundle**. This will load image bundle inventory in topology.

   Figure 10-51: Image bundle inventory

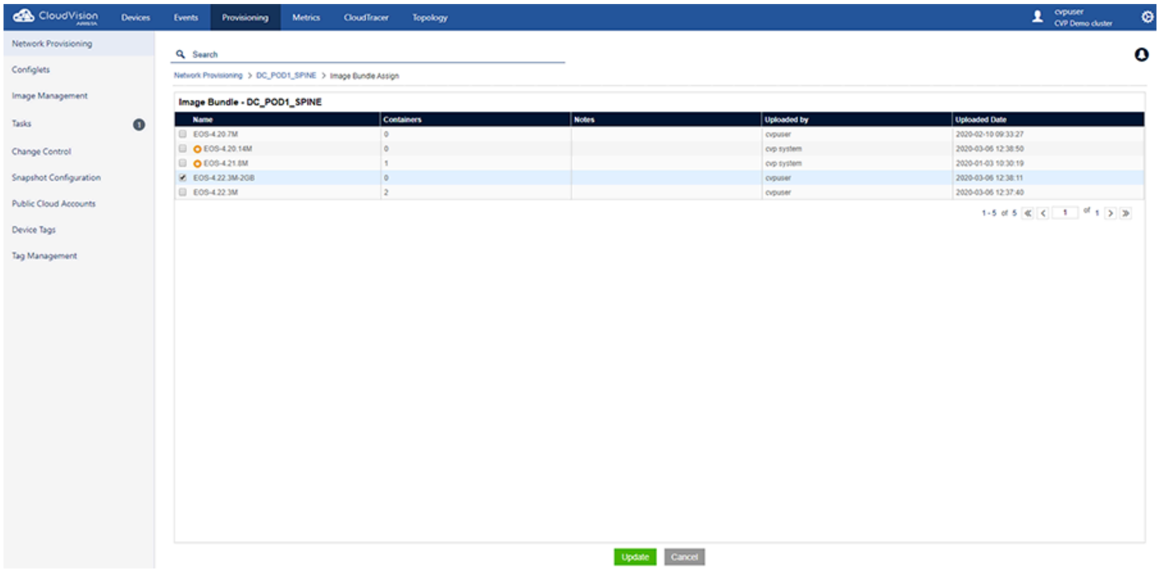


Image Bundle - DC_POD1_SPINE

	Name	Containers	Notes	Uploaded by	Uploaded Date
□	EOS-4.20.7M	0		cvpuser	2020-02-10 09:33:27
□	○ EOS-4.20.14M	0		cvp system	2020-03-06 12:38:50
□	○ EOS-4.21.8M	1		cvp system	2020-01-03 10:30:19
☑	EOS-4.22.3M-2GB	0		cvpuser	2020-03-06 12:38:11
□	EOS-4.22.3M	2		cvpuser	2020-03-06 12:37:40

2. Select the bundle to be assigned to the container.
3. Click **Update** to provision the bundle add for the container. This action will cause a task to be created for each device in the container to upgrade it to the specified image bundle.

10.10.2 Viewing the Image Bundle Assigned to Devices

CloudVision Portal (CVP) enables you to use the **Network Provisioning** screen to view the image bundle currently assigned to a device. You can also see if the image bundle is inherited from a Container or assigned directly to the device.

Complete the following steps to view the image bundle applied to a device.

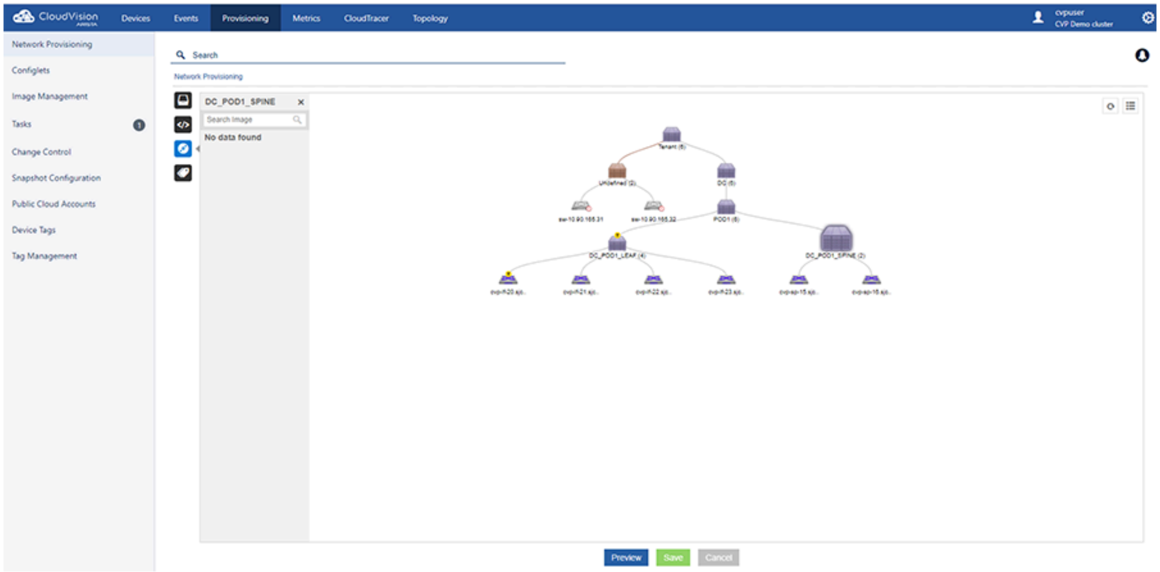
1. Go to the **Network Provisioning** screen.
2. Make sure you are using the topology view, not the list view.
3. Click on the **device** in the topology.
4. Click the image icon in the left pane.

   The image bundle assigned to the device is shown in a pop-up box.

   - If the image bundle is inherited from a Container to which the device belongs, the Container icon appears in front of the image bundle name.

- If the image bundle is assigned directly to the device, there is no Container icon in front of the image bundle name.

Figure 10-52: Viewing the Image Bundle assigned to a device



10.10.3 Applying an Image Bundle to a Device

1. Right-click the device, then choose Manage > Image Bundle. This will open the window display the inventory of Image bundles.

   Note: Only one image bundle can be selected and assigned to a device at a time.

2. Select the bundle to be assigned to the device.
3. Click **Update** to provision the bundle add for the device.

   This action will cause a task to be created for that device to upgrade it to the specified image bundle.

10.10.4 Setting up an Image Bundle as the default for ZTP

Since all devices must run this image, you must apply the image at the tenant level.

1. Go to the **Network Provisioning** screen.
2. Right-click the **Tenant** container and choose **Manage > Image Bundle**.
3. Select the bundle you created and click **Update**.
4. Click **Preview** to verify the changes before saving the changes.
5. Click **Save** to apply the changes.

10.11 Rolling Back Images and Configurations

CloudVision Network Rollbacks feature enables you to restore a previous EOS image and configuration to containers and devices. You can apply the rollback to all the devices in a container, or to single devices. When you rollback a container or device, you select the date and time for the rollback and whether you want to rollback the EOS image or configuration (or both).

CloudVision supports rollback to any previous point in time irrespective of captured snapshots. However, rollback is possible to a point that is far beyond the CloudVision Cluster update to *2018.2.0* only when your devices are upgraded to TerminAttr 1.4+ long before that.

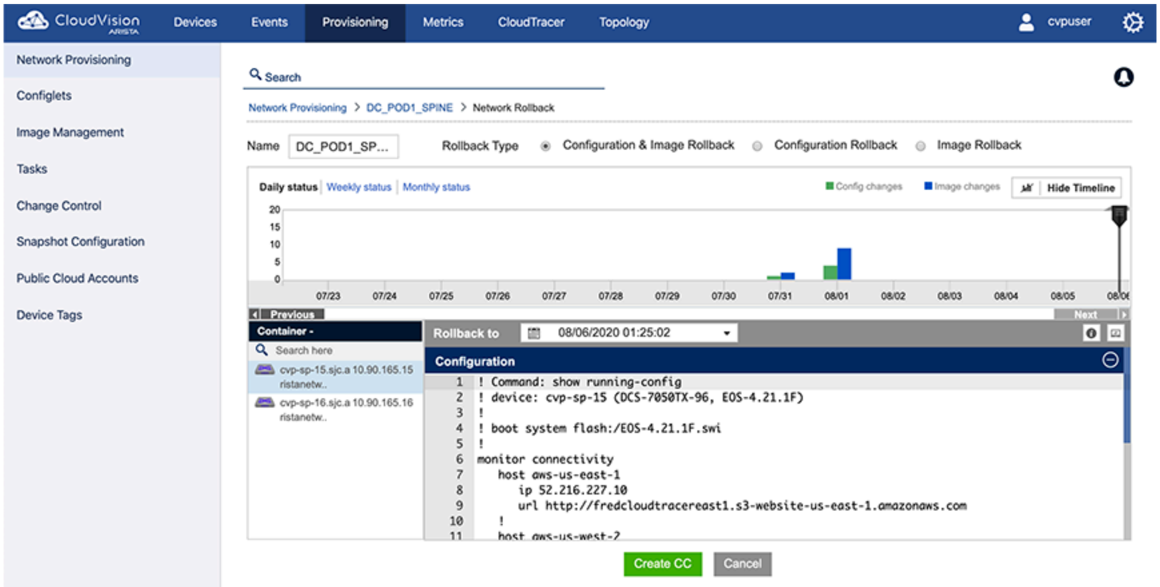
Note: To help you select the desired rollback destination day and time, you can compare the image and running configuration differences between current and rollback times of all effected devices. The potential destination rollback date and time in the comparison is based on the destination rollback date and time you select.

10.11.1 Rolling Back Container Images and Configurations

Complete the following steps to apply a network rollback in containers:

1. Go to the **Network Provisioning** screen.
2. Right-click on the container you want to rollback, and then choose **Manage > Network Rollback**.

Figure 10-53: Network Rollback Screen



Name DC_POD1_SP...

Rollback Type ● Configuration & Image Rollback ○ Configuration Rollback ○ Image Rollback

Rollback to 08/06/2020 01:25:02

```
! Command: show running-config
! device: cvp-sp-15 (DCS-7050TX-96, EOS-4.21.1F)
!
! boot system flash:/EOS-4.21.1F.swi
!
monitor connectivity
   host aws-us-east-1
      ip 52.216.227.10
      url http://fredcloudtracereast1.s3-website-us-east-1.amazonaws.com
   !
   host aws-us-west-2
```

3. Using the Rollback Type: options near the top of the screen, select the type of rollback. The options are:
   - Configuration & Image Rollback (both the configuration and EOS image are rolled back)
   - Configuration Rollback (only the configuration is rolled back)
   - Image Rollback (only the EOS image is rolled back)
4. Either drag the vertical slider on the timeline to the desired date and select the time for rollback; or use the Rollback to menu for selecting rollback date and time (directly above the configuration pane on the left side).
5. Click the telemetry icon (directly above the configuration pane on the right side) for viewing the running configuration differences between current and rollback times.
6. If required, change the destination date and time for the rollback.
7. Click **Create CC** to create a Change Control (CC) record for the network rollback. CloudVision automatically creates a rollback task for each device in the rollback; and makes them part of CC.

   Note: Rollback Change Controls are automatically assigned a unique name. You can rename the Change Control record by editing the Change Control record. Once the Change Control is created, it can be executed like any other Change Control.

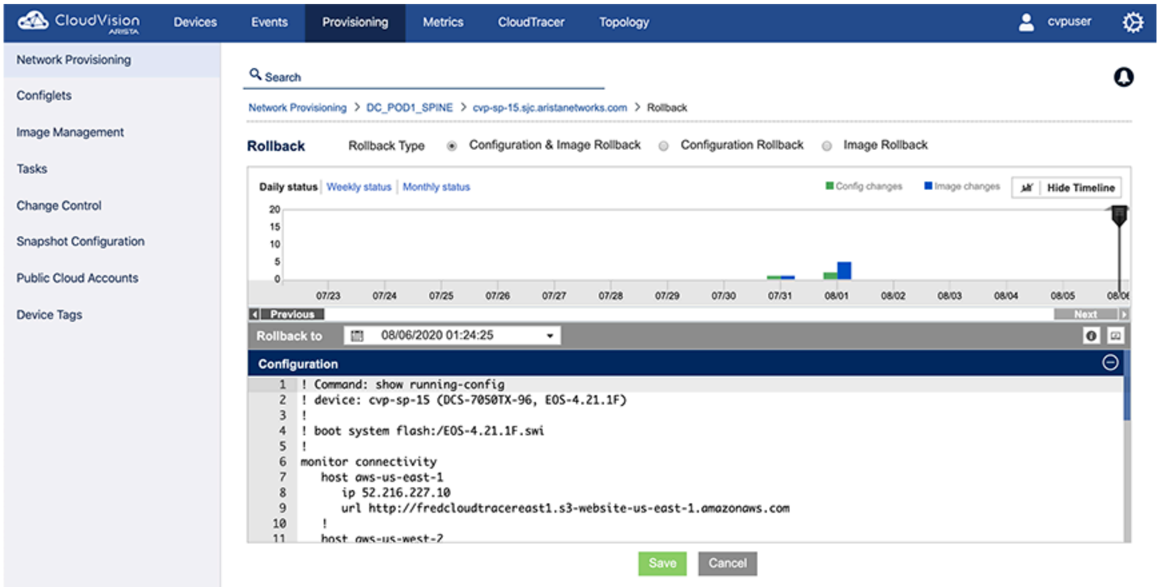
10.11.2 Rolling Back Device Images and Configurations

Complete the following steps to apply a rollback in devices:

1. Go to the **Network Provisioning** screen.

2. Right-click on the device you want to rollback, and then choose **Manage > Rollback**.

   Figure 10-54: Device Rollback Screen



Rollback   Rollback Type ● Configuration & Image Rollback ○ Configuration Rollback ○ Image Rollback

Rollback to 08/06/2020 01:24:25

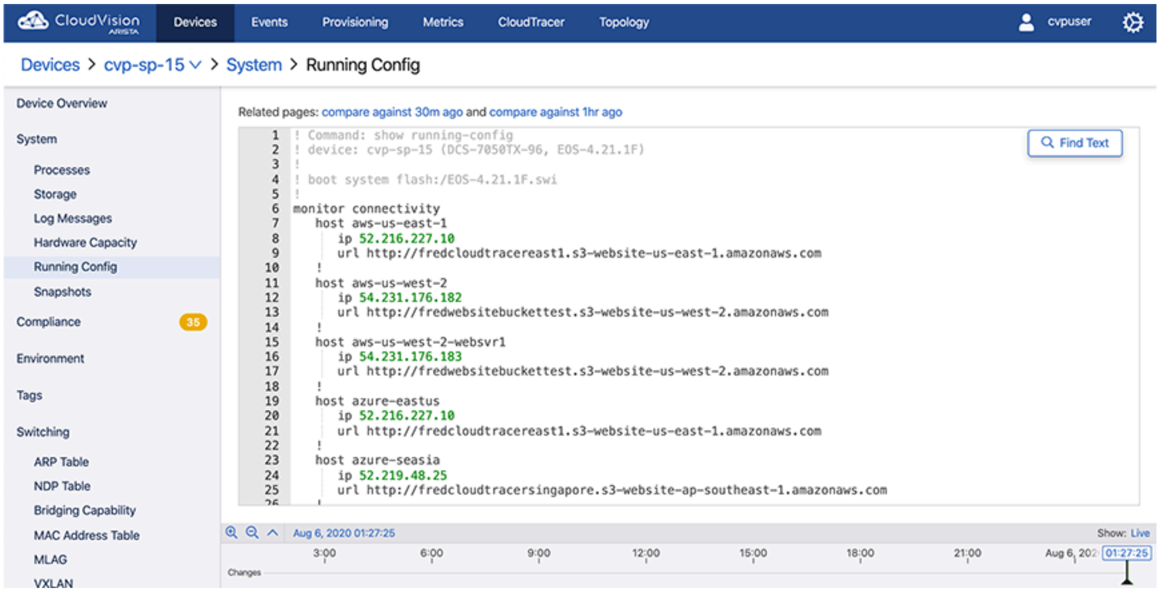
```
! Command: show running-config
! device: cvp-sp-15 (DCS-7050TX-96, EOS-4.21.1F)
!
! boot system flash:/EOS-4.21.1F.swi
!
monitor connectivity
   host aws-us-east-1
      ip 52.216.227.10
      url http://fredcloudtracereast1.s3-website-us-east-1.amazonaws.com
   !
   host aws-us-west-2
```

3. Using the **Rollback Type**: options near the top of the screen, select the type of rollback. The options are:

   - Configuration & Image Rollback (both the configuration and EOS image are rolled back)
   - Configuration Rollback (only the configuration is rolled back)
   - Image Rollback (only the EOS image is rolled back)

4. Either drag the vertical slider on the timeline to the desired date and select the time for rollback; or use the **Rollback to** menu for selecting rollback date and time (directly above the **configuration** pane on the left side).
5. Click the telemetry icon (directly above the **configuration** pane on the right side) for viewing the running configuration differences between current and rollback times.

   Figure 10-55: Differences in Running Configuration



Related pages: compare against 30m ago and compare against 1hr ago

```
! Command: show running-config
! device: cvp-sp-15 (DCS-7050TX-96, EOS-4.21.1F)
!
! boot system flash:/EOS-4.21.1F.swi
!
monitor connectivity
   host aws-us-east-1
      ip 52.216.227.10
      url http://fredcloudtracereast1.s3-website-us-east-1.amazonaws.com
   !
   host aws-us-west-2
      ip 54.231.176.182
      url http://fredwebsitebuckettest.s3-website-us-west-2.amazonaws.com
   !
   host aws-us-west-2-websvr1
      ip 54.231.176.183
      url http://fredwebsitebuckettest.s3-website-us-west-2.amazonaws.com
   !
   host azure-eastus
      ip 52.216.227.10
      url http://fredcloudtracereast1.s3-website-us-east-1.amazonaws.com
   !
   host azure-seasia
      ip 52.219.48.25
      url http://fredcloudtracersingapore.s3-website-ap-southeast-1.amazonaws.com
   !
```

   The **Unified** tab displays running configuration differences in a single window with differences highlighted. The **Split** tab displays running configurations in different windows with differences highlighted.

6. If required, change the destination date and time for the rollback.

7. Click **Save** to create a task for the device rollback.

10.11.3 Rolling Back Configurations Assigned to a Device

CloudVision's Network Rollbacks feature enables you to restore a previous configuration to devices. You can apply the rollback to all the devices in a container, or to single devices. When you rollback a container or device, you select the date and time for the rollback and whether you want to rollback the configuration or EOS image (or both).

See Rolling Back Images and Configurations for details.

10.12 Device Labels

A label is simply defined as Text Tags. There are two types of label:

- System labels: Assigned automatically by the system.
- Custom labels: Defined and assigned by the user.
    - Users can assign custom labels to devices from the **Network Provisioning** screen.
    - A device can be tagged with one or more custom labels.
    - Labels can be used to filter the devices in the **Network Provisioning** screen.

10.12.1 System Labels

System labels are defined by the system and are automatically applied to and removed from devices based on the following characteristics of that device:

- Software version
- Software bundle
- Product model and family
- Assigned configlet name
- DANZ enabled
- MLAG enabled
- Parent container name

Note: System labels cannot be modified or removed by the user.

10.12.2 Custom Device Labels

You can create custom device labels and assign them to devices. The device labels you assign to a device show on the **Network Provisioning** screen next to the device.

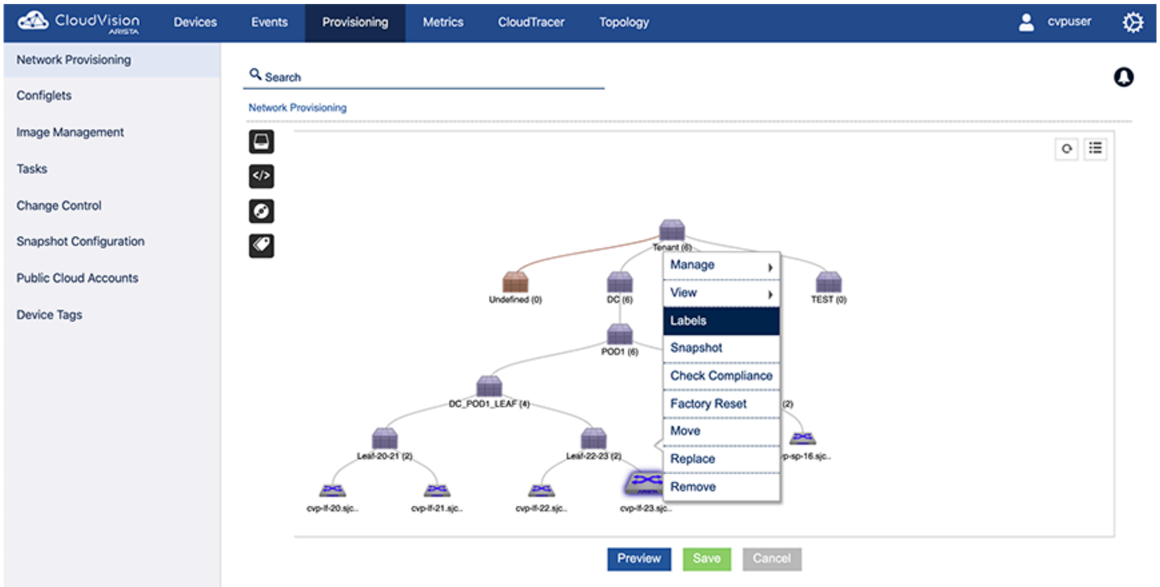
10.12.2.1 Assigning an Existing Label to a Device

Complete these steps to assign an existing label to a device.

1. Select the device to be labeled.

2. Right-click the device and choose **Labels**.

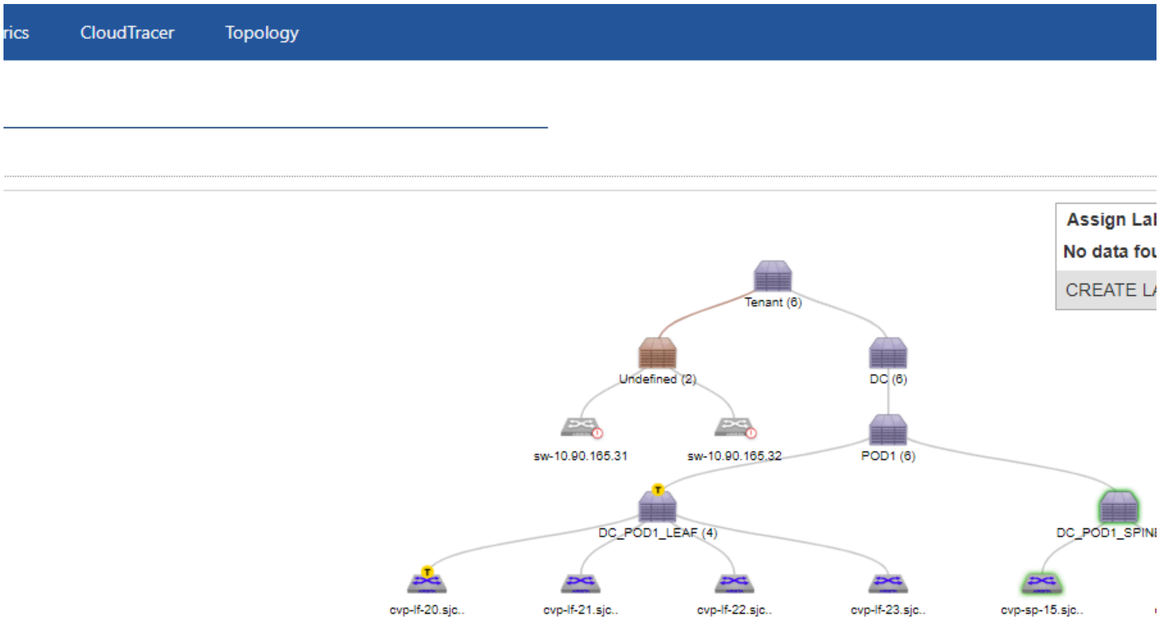
Figure 10-56: Choose Labels



The **Assign Label** pop-up menu appears, showing the available device labels.

3. Select the label to be applied and click **Save**.

Figure 10-57: Assign Label



The selected label will be applied to the device.

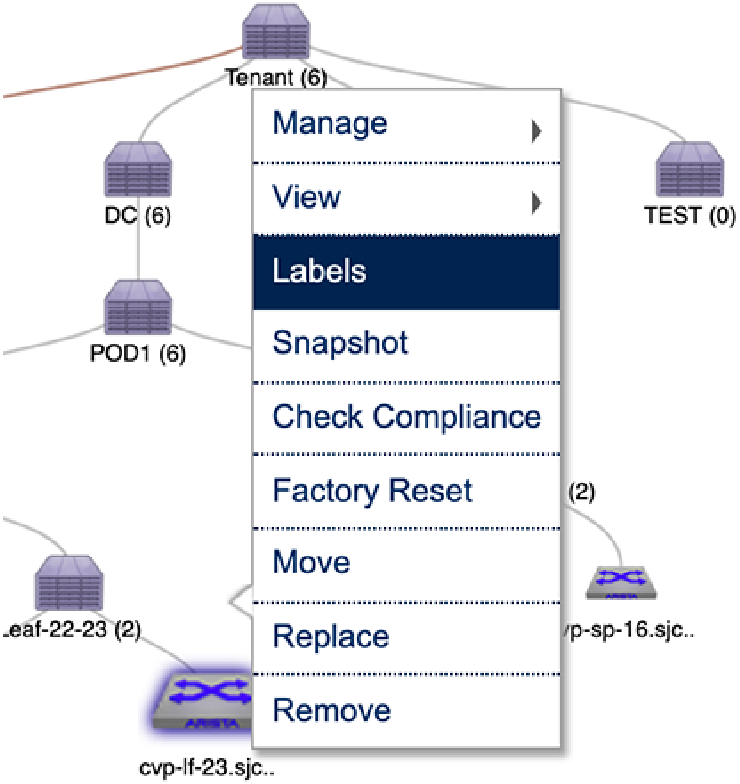
10.12.2.2 Creating a Custom Label for a Device

Complete these steps to create a new, custom label to a device.

1. Select the device for which you want to create a new, custom label.

2. Right-click the device and choose **Labels.**

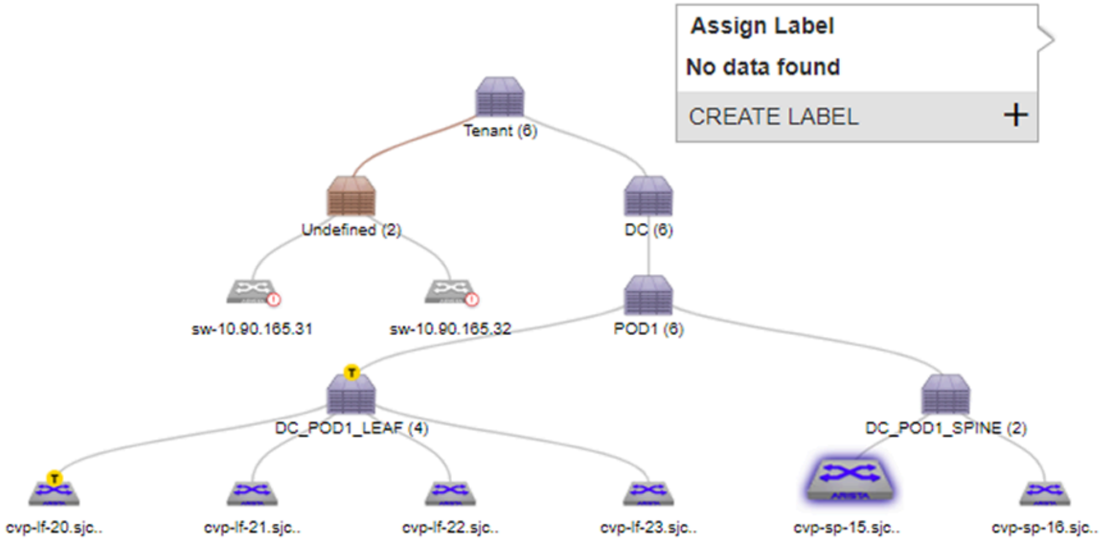
Figure 10-58: Choose Labels



The Assign Label pop-up menu appears, showing the available device labels.

3. In the pop-up menu, click on **CREATE LABEL**.

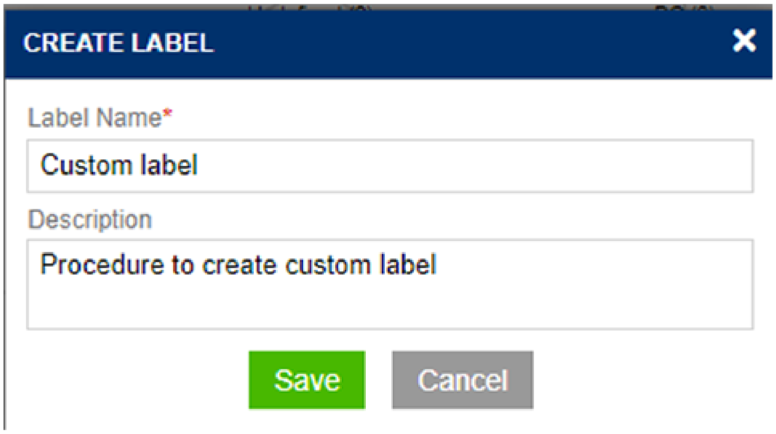
Figure 10-59: Create label Pop-up



The Create Label dialog appears.

4. Type the new, custom label for the device, then click **Save**.

Figure 10-60: Create Label



CREATE LABEL

Label Name*

Custom label

Description

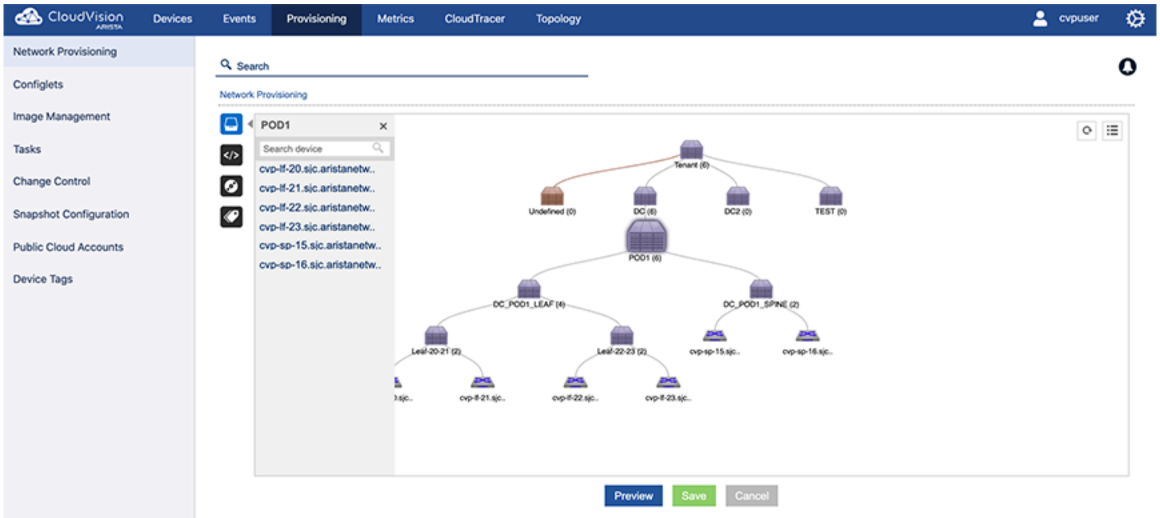
Procedure to create custom label

The new label is created and is assigned to the device.

10.12.3 Left Pane Behavior in Network Provisioning View

The left pane in the topology view is used to display information on the resources assigned to a given device or container.

Figure 10-61: Left pane view



Opening and Closing the Left Pane

1. Double click the container or device to open the left pane.
2. Click the **X** button to close it.

10.13 Viewing Containers and Devices

The Network Provisioning screen provides you with various options that enable you to easily control the topology view so that you can view containers and devices based on your needs.

The options you use are:

- **Expand / Collapse** (see Expanding and Collapsing Containers).

- **Show From Here** (see Show From Here).
- **Show Full Topology** (see Show Full Topology).

CloudVision Portal uses color coded icons to indicate compliance or access issues with devices.

10.13.1 Expanding and Collapsing Containers

Containers can be expanded and collapsed within the Network Provisioning topology view so that you can change the view as needed based on your needs.

You use the **Show From Here** and **Show Full Topology** options to expand or collapse containers shown in the **Network Provisioning** screen.

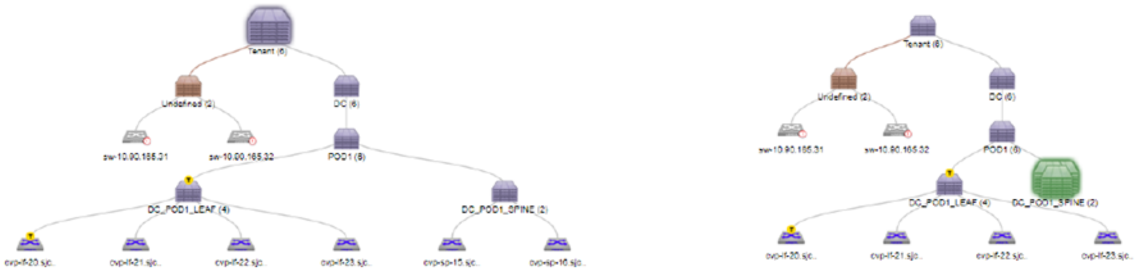
The **Expand and Collapse** option is only available for the **Network Provisioning** view. It is not available for the List view.

The default view mode for containers is expanded. When you choose **Expand/Collapse** option for a container, one of the following occurs, depending on the current view mode:

- A container currently in expanded (normal) view is collapsed.
- A container currently in collapsed mode is returned to expanded view mode (the default).

Complete these steps to expand or collapse a container view from the **Network Provisioning** screen.

Figure 10-62: Expanded and collapsed view of a container



1. Select a container.
2. Right-click it and select the **Expand/Collapse** option.

10.13.2 Show From Here

The **Show From Here** option displays the topology with the selected container as the root. The hierarchy above the selected container will be hidden from the view allowing the user to only focus on the chosen container and the tree below it.

1. Select a container.
2. Right click **Show From Here** to display the option. The hierarchy from the selected container will be displayed.

10.13.3 Show Full Topology

The **Show Full Topology** option allows the user to get back to the full topology view. This option will be enabled for a particular container once the user uses the show from here option on it.

1. Select a container.
2. Right-click **Show Full Topology** to view the option.

10.14 Network Search

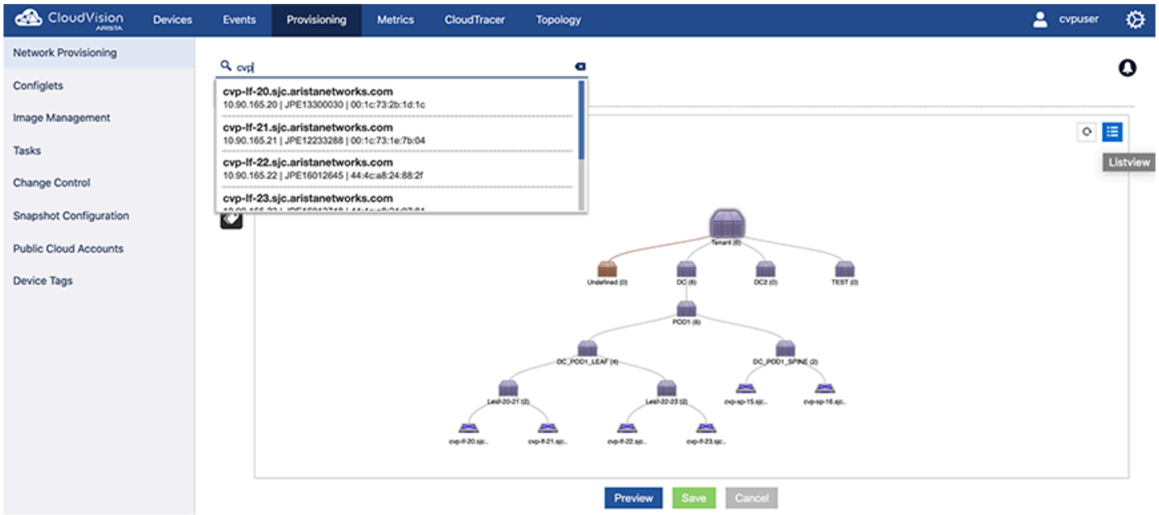
In the **Network Provisioning** module, the user can use the search bar at the top of the module to find a given device or container.

10.14.1 Search Behavior in Topology and List View

This search is very different from rest of other search options available in topology. On user starts to type, the list of possible matches will be displayed below as an auto suggestion.

10.14.2 Topology Search

Figure 10-63: Using search



cvp|

cvp-lf-20.sjc.aristanetworks.com
10.90.165.20 | JPE13300030 | 00:1c:73:2b:1d:1c

cvp-lf-21.sjc.aristanetworks.com
10.90.165.21 | JPE12233288 | 00:1c:73:1e:7b:04

cvp-lf-22.sjc.aristanetworks.com
10.90.165.22 | JPE16012645 | 44:4c:a8:24:88:2f

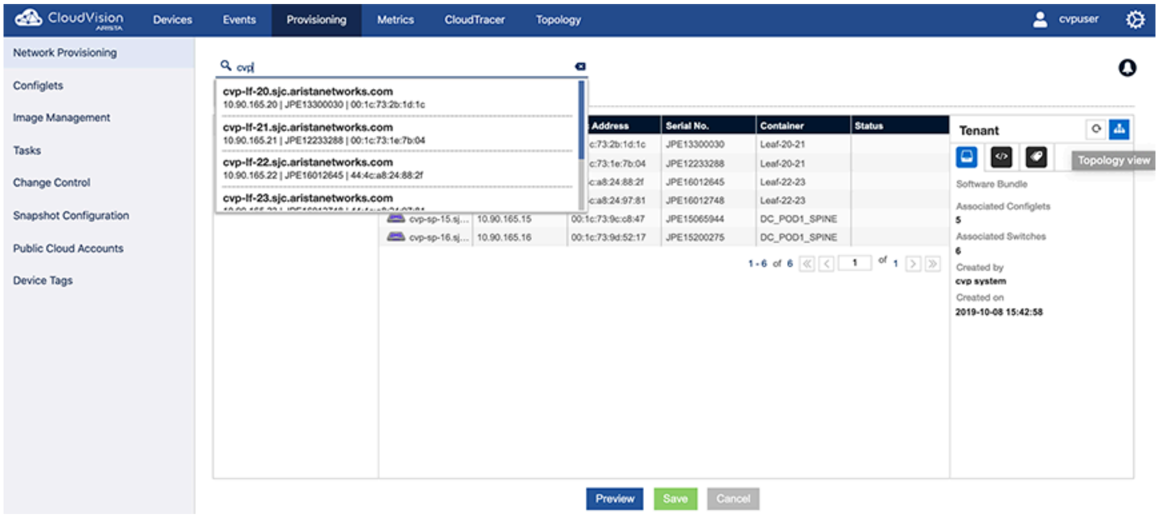
cvp-lf-23.sjc.aristanetworks.com

10.14.3 List View Search

The search behaves similar to the topology search.

For a single device search, the selected device will be listed in the grid.

Figure 10-64: List view search



cvp|

cvp-lf-20.sjc.aristanetworks.com
10.90.165.20 | JPE13300030 | 00:1c:73:2b:1d:1c

cvp-lf-21.sjc.aristanetworks.com
10.90.165.21 | JPE12233288 | 00:1c:73:1e:7b:04

cvp-lf-22.sjc.aristanetworks.com
10.90.165.22 | JPE16012645 | 44:4c:a8:24:88:2f

cvp-lf-23.sjc.aristanetworks.com

		Address	Serial No.	Container	Status
		c:73:2b:1d:1c	JPE13300030	Leaf-20-21	
		c:73:1e:7b:04	JPE12233288	Leaf-20-21	
		c:a8:24:88:2f	JPE16012645	Leaf-22-23	
		c:a8:24:97:81	JPE16012748	Leaf-22-23	
cvp-sp-15.sj...	10.90.165.15	00:1c:73:9c:c8:47	JPE15065944	DC_POD1_SPINE	
cvp-sp-16.sj...	10.90.165.16	00:1c:73:9d:52:17	JPE15200275	DC_POD1_SPINE	

Tenant

Software Bundle

Associated Configlets
5

Associated Switches
6

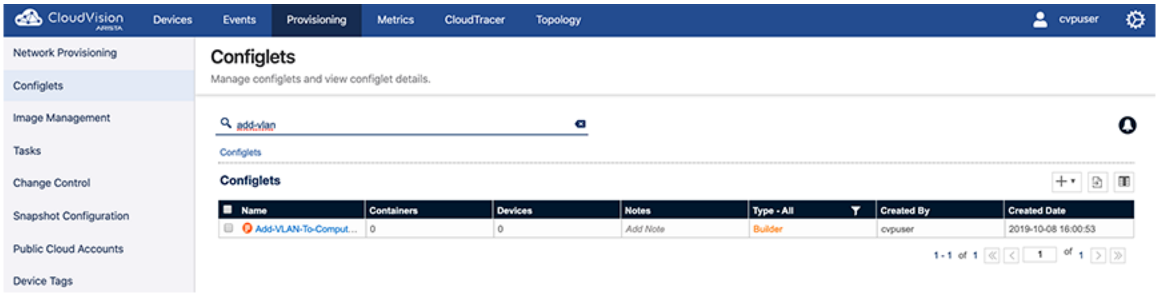
Created by
cvp system

Created on
2019-10-08 15:42:58

10.14.4 Search in Other Grids

During a grid search, the user will not be provided with an auto suggest option. Only the records matching the specified data entered will be filtered and displayed in the grid.

Figure 10-65: Grid searches



Configlets

Manage configlets and view configlet details.

add-vlan

Configlets

Configlets

Name	Containers	Devices	Notes	Type - All	Created By	Created Date
Add-VLAN-To-Comput...	0	0	Add Note	Builder	cvpuser	2019-10-08 16:00:53

1 - 1 of 1 1 of 1

10.14.5 Label Search

Use the search bar from the Network Provisioning screen to filter the devices based on labels.

This is a contextual search.

To search a label:

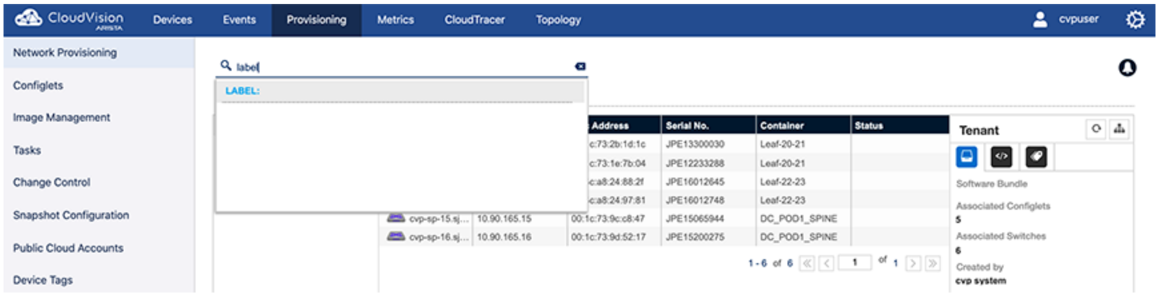
1. Use the keyword Label: followed by the label name.

10.14.5.1 AND Operation

Lists all the devices which has both the labels present on it in the hierarchy.

Label: <*Label Name*> AND Label: <*Label Name*>

Figure 10-66: Search AND operation



label

LABEL:

		Address	Serial No.	Container	Status
		c:73:2b:1d:1c	JPE13300030	Leaf-20-21	
		c:73:1e:7b:04	JPE12233288	Leaf-20-21	
		c:a8:24:88:2f	JPE16012645	Leaf-22-23	
		c:a8:24:97:81	JPE16012748	Leaf-22-23	
cvp-sp-15.sj...	10.90.165.15	00:1c:73:9c:c8:47	JPE15065944	DC_POD1_SPINE	
cvp-sp-16.sj...	10.90.165.16	00:1c:73:9d:52:17	JPE15200275	DC_POD1_SPINE	

1 - 6 of 6 1 of 1

Tenant

Software Bundle

Associated Configlets
5

Associated Switches
6

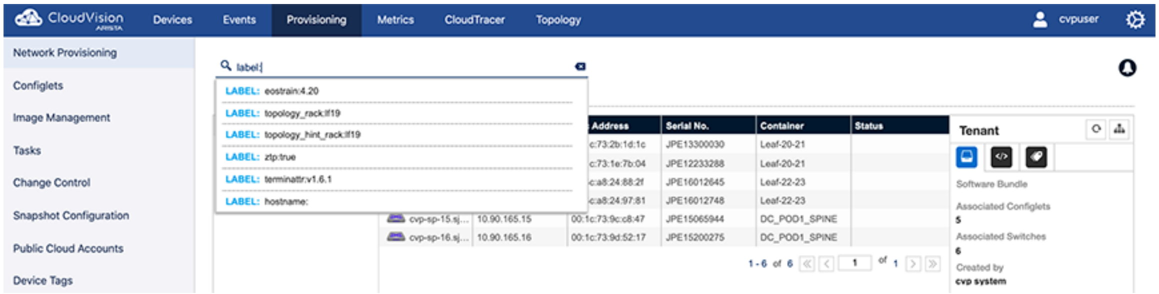
Created by
cvp system

10.14.5.2 OR Operation

Lists all the devices which has either one of the labels present on it in the hierarchy.

Label: <Label Name> OR Label: <Label Name>

Figure 10-67: Search OR operation



label:|

- LABEL: eostrain:4.20
- LABEL: topology_rack:lf19
- LABEL: topology_hint_rack:lf19
- LABEL: ztp:true
- LABEL: terminattr:v1.6.1
- LABEL: hostname:

		Address	Serial No.	Container	Status
		c:73:2b:1d:1c	JPE13300030	Leaf-20-21	
		c:73:1e:7b:04	JPE12233288	Leaf-20-21	
		c:a8:24:88:2f	JPE16012645	Leaf-22-23	
		c:a8:24:97:81	JPE16012748	Leaf-22-23	
cvp-sp-15.sj...	10.90.165.15	00:1c:73:9c:c8:47	JPE15065944	DC_POD1_SPINE	
cvp-sp-16.sj...	10.90.165.16	00:1c:73:9d:52:17	JPE15200275	DC_POD1_SPINE	

1 - 6 of 6 « ‹ 1 of 1 › »

Associated Configlets: 5

Associated Switches: 6

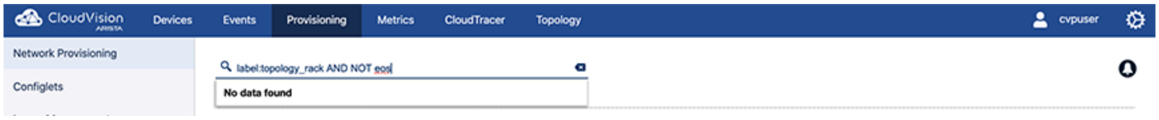
Created by: cvp system

10.14.5.3 NOT Operation

Lists all the devices which has first label one the labels present on it in the hierarchy.

Label: ***Label Name*** AND NOT Label: ***Label Name***

Figure 10-68: Search AND NOT operation



label:topology_rack AND NOT eos|

No data found

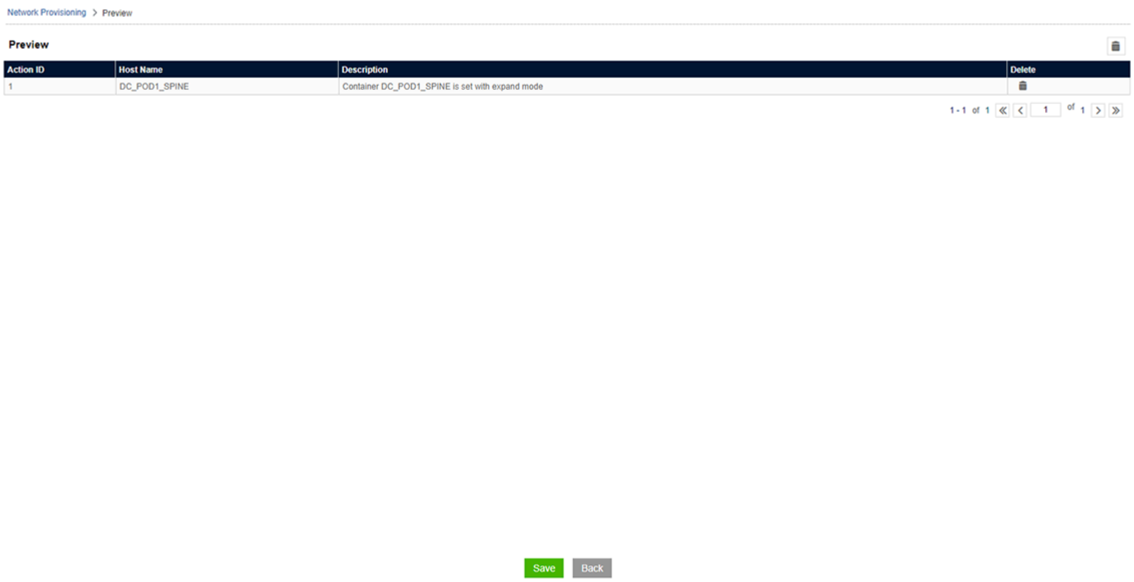
10.14.6 Preview Option

All the actions performed in **Network Provisioning** module can be previewed before saving the changes.

To access the preview screen:

1. Select the “Preview” button.

Figure 10-69: Preview option display



Preview

Action ID	Host Name	Description	Delete
1	DC_POD1_SPINE	Container DC_POD1_SPINE is set with expand mode	🗑

1 - 1 of 1 « ‹ 1 of 1 › »

10.15 Management IP

The CloudVision Portal tracks the Management IP of each device to use in connecting to it. When this IP address changes, the device becomes unreachable by the portal. You can manually change the IP address used by the portal to communicate with a given device.

10.15.1 Changing A Device's Management IP

The management IP address of a device may change for one of the following reasons:

Reason 1:

When a device is provisioned using Zero Touch Provisioning, it may have been assigned a temporary IP address via DHCP. The CloudVision Portal will use this IP address to provision the device. Once the configuration is pushed and the device reboots, this IP address may change.

Reason 2:

1If you change the device IP address directly via the switch console, CloudVision cannot record the change, and the device will become unreachable. **Current management IP** and **proposed management IP** can be used to mitigate this potential issue.

Option 1:

Current Management IP: The IP address used by CloudVision to communicate with a device.

1. Set the proposed IP address before pushing the configlet. This way CloudVision will try to reach the device with this IP address once configuration is pushed.

Option 2:

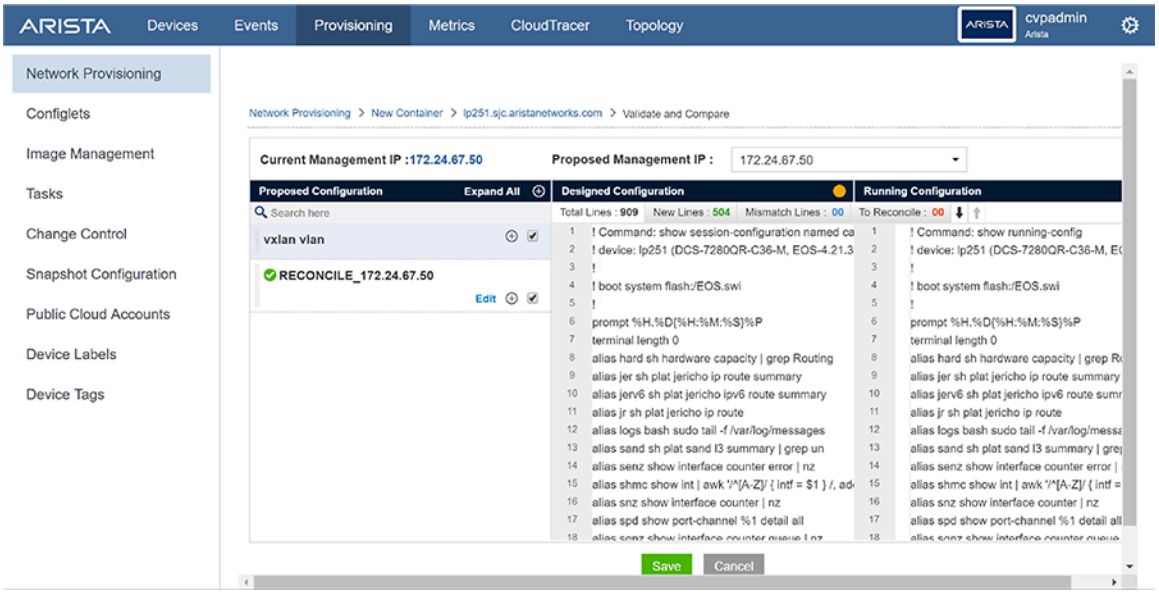
Proposed Management IP: The IP address that CloudVision uses after pushing the configlet.

1. In the Inventory Management screen and the topology, update the Management IP address. For any unreachable device, set the IP address to bring it back to the network.

10.15.2 Setting Proposed Management IP

You can set the Proposed Management IP while adding configlets to the device using the Proposed Management IP menu.

Figure 10-70: Location of menu for setting Proposed Management IP



Current Management IP :172.24.67.50

Proposed Management IP : 172.24.67.50

vxlan vlan

RECONCILE_172.24.67.50

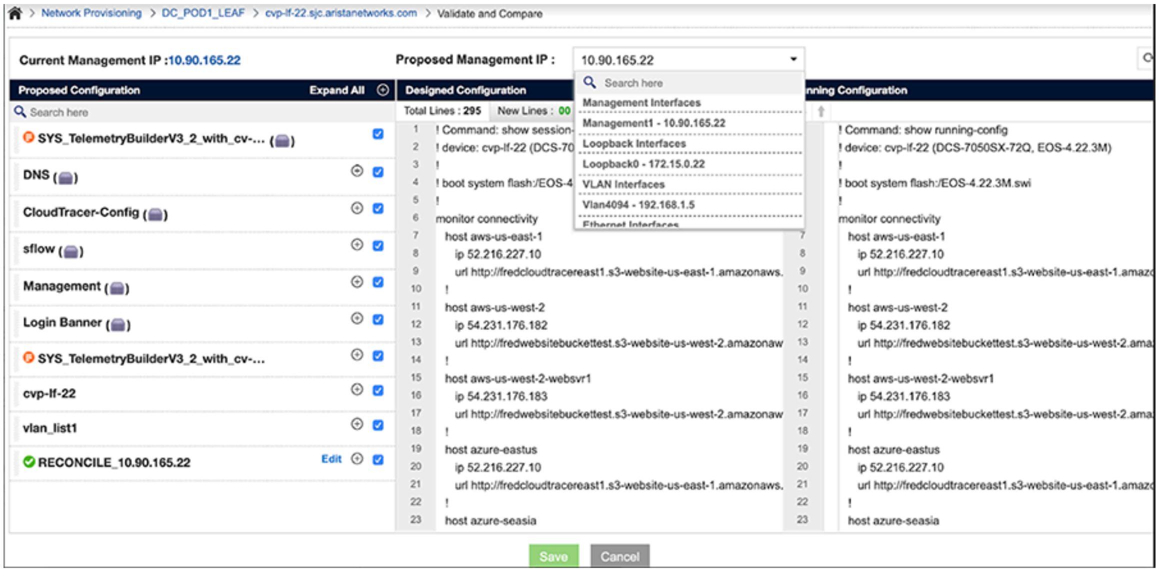
Total Lines : 909 New Lines : 504 Mismatch Lines : 00 To Reconcile : 00

```
! Command: show session-configuration named ca
! device: lp251 (DCS-7280QR-C36-M, EOS-4.21.3
!
! boot system flash:/EOS.swi
!
prompt %H.%D{%H:%M:%S}%P
terminal length 0
alias hard sh hardware capacity | grep Routing
alias jer sh plat jericho ip route summary
alias jerv6 sh plat jericho ipv6 route summary
alias jr sh plat jericho ip route
alias logs bash sudo tail -f /var/log/messages
alias sand sh plat sand l3 summary | grep un
alias senz show interface counter error | nz
alias shmc show int | awk '/^[A-Z]/ { intf = $1 } /, ad
alias snz show interface counter | nz
alias spd show port-channel %1 detail all
alias sqnz show interface counter queue | nz
```

```
! Command: show running-config
! device: lp251 (DCS-7280QR-C36-M, E
!
! boot system flash:/EOS.swi
!
prompt %H.%D{%H:%M:%S}%P
terminal length 0
alias hard sh hardware capacity | grep R
alias jer sh plat jericho ip route summary
alias jerv6 sh plat jericho ipv6 route sumr
alias jr sh plat jericho ip route
alias logs bash sudo tail -f /var/log/messa
alias sand sh plat sand l3 summary | gre
alias senz show interface counter error |
alias shmc show int | awk '/^[A-Z]/ { intf =
alias snz show interface counter | nz
alias spd show port-channel %1 detail all
alias sqnz show interface counter queue
```

If you do not set the Proposed Management IP, you cannot save the configuration as not setting Proposed Management IP.

Figure 10-71: Setting the Proposed Management IP



Current Management IP :10.90.165.22

Proposed Management IP : 10.90.165.22

SYS_TelemetryBuilderV3_2_with_cv-... ( )
DNS ( )
CloudTracer-Config ( )
sflow ( )
Management ( )
Login Banner ( )
SYS_TelemetryBuilderV3_2_with_cv-...
cvp-lf-22
vlan_list1
RECONCILE_10.90.165.22

Total Lines : 295 New Lines : 00

```
! Command: show session-
! device: cvp-lf-22 (DCS-70
!
! boot system flash:/EOS-4
!
monitor connectivity
   host aws-us-east-1
      ip 52.216.227.10
      url http://fredcloudtracereast1.s3-website-us-east-1.amazonaws.
   !
   host aws-us-west-2
      ip 54.231.176.182
      url http://fredwebsitebuckettest.s3-website-us-west-2.amazonaw
   !
   host aws-us-west-2-websvr1
      ip 54.231.176.183
      url http://fredwebsitebuckettest.s3-website-us-west-2.amazonaw
   !
   host azure-eastus
      ip 52.216.227.10
      url http://fredcloudtracereast1.s3-website-us-east-1.amazonaws.
   !
   host azure-seasia
```

```
! Command: show running-config
! device: cvp-lf-22 (DCS-7050SX-72Q, EOS-4.22.3M)
!
! boot system flash:/EOS-4.22.3M.swi
!
monitor connectivity
   host aws-us-east-1
      ip 52.216.227.10
      url http://fredcloudtracereast1.s3-website-us-east-1.amaz
   !
   host aws-us-west-2
      ip 54.231.176.182
      url http://fredwebsitebuckettest.s3-website-us-west-2.ama
   !
   host aws-us-west-2-websvr1
      ip 54.231.176.183
      url http://fredwebsitebuckettest.s3-website-us-west-2.ama
   !
   host azure-eastus
      ip 52.216.227.10
      url http://fredcloudtracereast1.s3-website-us-east-1.amaz
   !
   host azure-seasia
```

1. Select the Proposed Management IP using the drop-down menu.

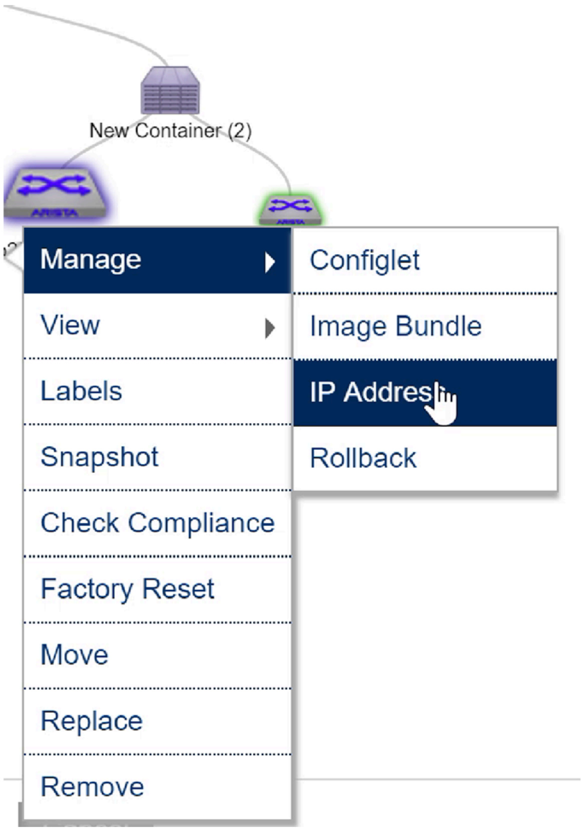
   CloudVision lists the available Management IP, Loop back IP, VLAN IP, and Routed Ethernet IP.
2. Select the desired IP address.
3. Click **Save**.

   A task is spawned to assign the new Proposed Management IP.

10.15.3 Changing Current Management IP

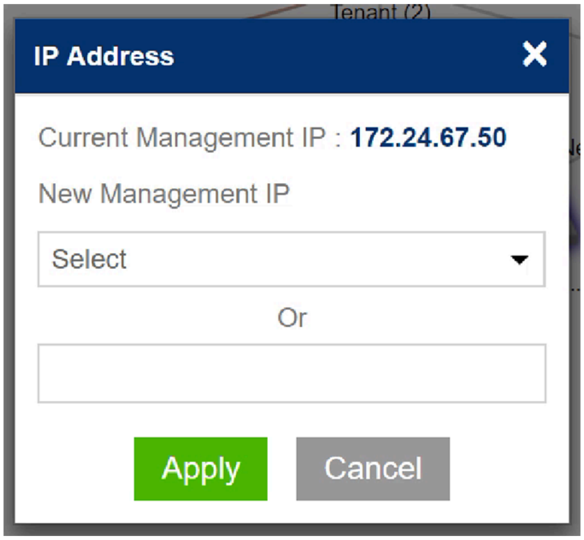
1. Go to the **Network Provisioning** screen.
2. Select a device from topology/list view.
3. Right-click the device and choose **Manage > IP Address**

Figure 10-72: Change Management IP



4. A pop up will appear allowing you to manually add a new IP address.

Figure 10-73: Change IP Address

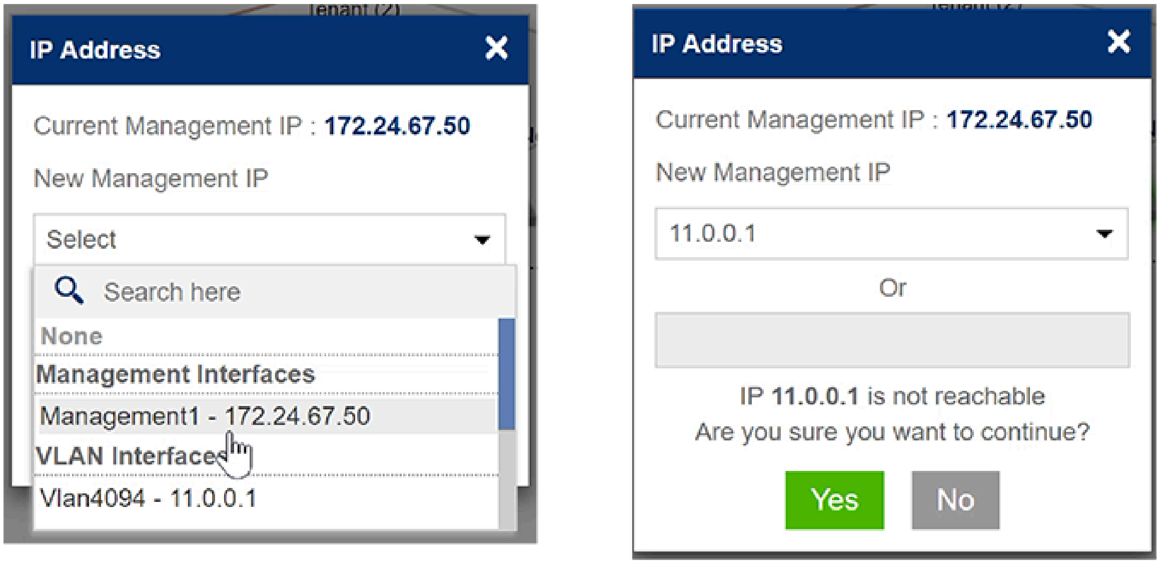


Current Management IP : **172.24.67.50**

New Management IP

5. Verify the reachability of new IP address.

Figure 10-74: Verify IP Address



IP Address

Current Management IP : **172.24.67.50**

New Management IP

Select

IP Address

Current Management IP : **172.24.67.50**

New Management IP

11.0.0.1

Or

IP **11.0.0.1** is not reachable
Are you sure you want to continue?

Chapter 11

Configlet Management (CVP)

Configlets are portion of configuration that CloudVision user codes and maintains independently under Configlet Management inventory. These Configlets can be later applied to devices or containers in the topology.

Sections in this chapter include:

- Creating Configlets
- Configlet Information Page
- Editing Configlets
- Tips for Applying Profiles to the Interfaces
- Deleting Configlets
- Importing and Exporting Configlets

11.1 Creating Configlets

CloudVision Portal (CVP) enables you to create Configlets using two different methods. You can create Configlets using the CVP Configlet Builder feature, or you can create them manually. You should use the method that is best suited to your intended use of the Configlet.

Note: The Configlet Builder feature is designed to help you create Configlets dynamically based on variables.

For more information, see:

- About the Configlet Builder Feature
- Creating Configlets Using the Configlet Builder
- Using the Provided Configlet Builder Examples
- Python Execution Environment
- Creating Configlets Manually

11.1.1 About the Configlet Builder Feature

The Configlet Builder feature enables you to programatically create device configurations (Configlets) for devices that have relatively dynamic configuration requirements. This helps to prevent you from having to manually code Configlets.

The Configlet Builder feature is essentially a set of user interface (UI) widgets and a python script, that when used together, programatically generate Configlets for a device. The python script is embedded into a python interpreter, which is the component that generates Configlets. The UI widgets are essential if you want to use the feature to generate Configlets with user input.

Note: Using UI widgets associated with a Configlet Builder are optional. If the UI widgets are used, the generated Configlets require user input to be created.

The Configlet Builder can be used to create Configlets for both devices or containers, in the same way that static Configlets can be used with devices or containers. Configlets that are created using the Configlet Builder are executed (including the generation of Configlets) at the point when the Configlet Builder is applied to a device or container, or when a device is added to a container that contains a Configlet Builder.

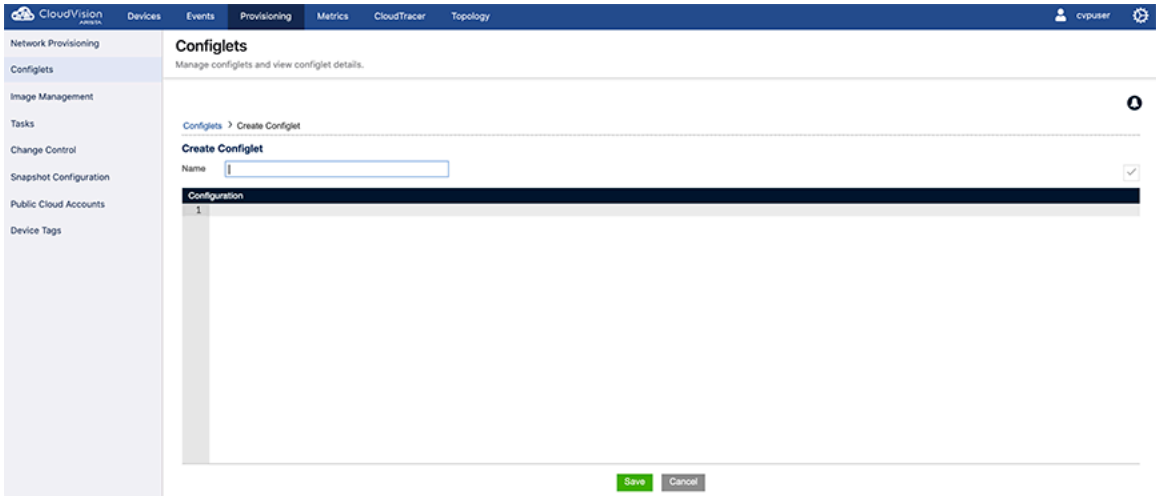
11.1.2 Creating Configlets Using the Configlet Builder

The Configlet Builder enables you to create Configlets (device configurations). The following Configlet Builder example configures the management interface based on input from the use of UI widgets.

Complete the following steps to create Configlets using the Configlet Builder:

1. Create a Configlet Builder from the Configlet page.

Figure 11-1: Creating a Configlet Builder



Configlets
Manage configlets and view configlet details.

Configlets > Create Configlet

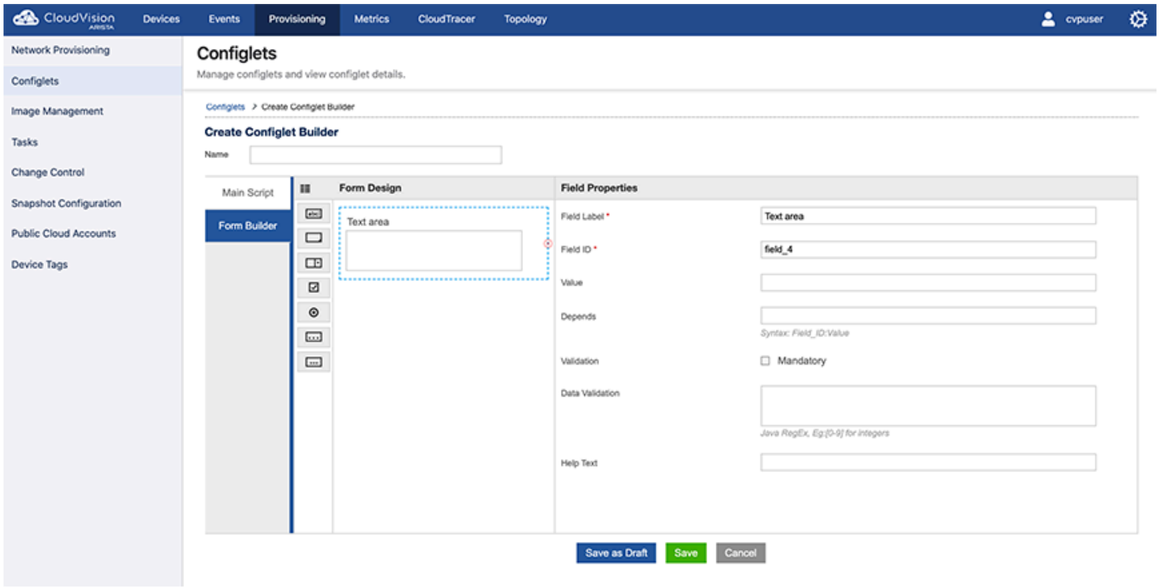
Create Configlet

Name

Configuration

2. (Optional) Define the UI widgets to be associated with the Configlet Builder.

Figure 11-2: Configlet UI Widgets



Configlets
Manage configlets and view configlet details.

Configlets > Create Configlet Builder

Create Configlet Builder

Name

Form Design

Text area

Field Properties

Field Label * Text area

Field ID * field_4

Value

Depends

Syntax: Field_ID:Value

Validation □ Mandatory

Data Validation

Java RegEx, Eg:[0-9] for integers

Help Text

The widget types are:

- **Text Box** – Use for single line text entries (for example, descriptions, host name).
- **Text Area** – Use for multiple lines of text (for example, MOTD, or login banner).
- **Drop Down** – Use to select a value from a menu as defined in the Value Field.
- **Tick Box** – Use to select a value from a tick list as defined in the Value Field.
- **Radio Button** – Use to select one option from a set of options as defined in Value Field.
- **IP Address** – Use to specify an IP address (this is a Dotted Decimal Address field).

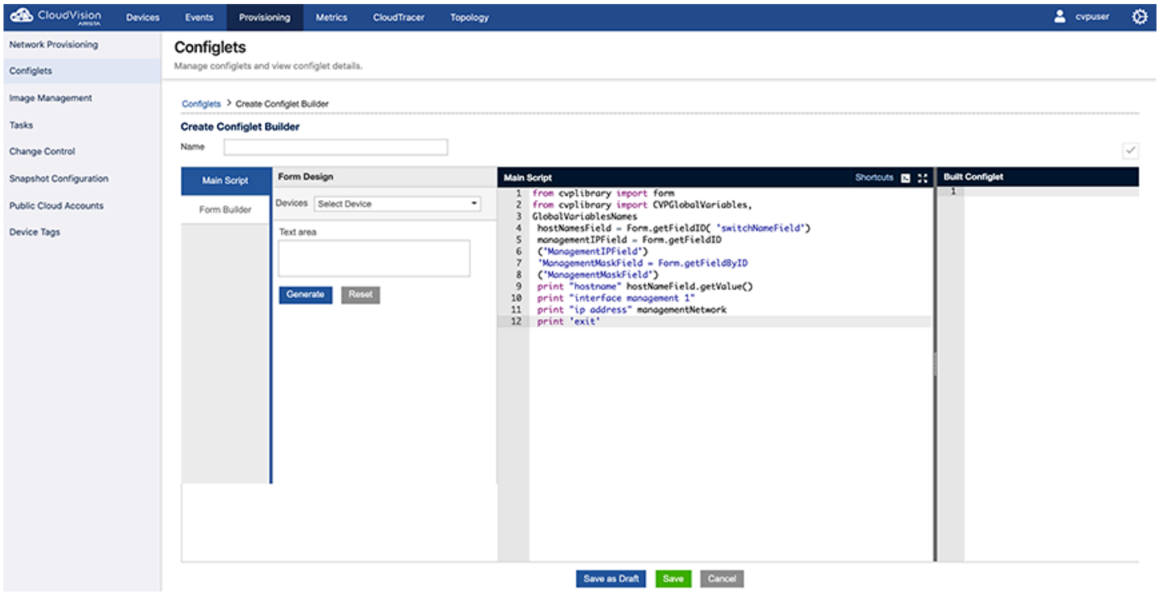
- **Password** – Use to specify a single line of text (characters are hidden as they are entered).

3. Write a Python script that reads the inputs you entered in the previous step and then generates the Configlet.

Note: The figures listed in this table show examples of the steps involved in writing a script, including an example of use of standard Python syntax to build components of the Configlet.

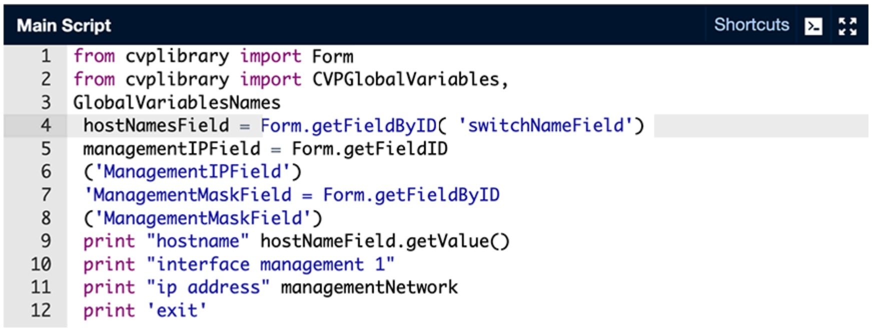
Figure	**Example of**	**Description**
Example (Showing Import of CVP-Specific Internal Libraries)	Importing CVP-specific internal libraries into the script	The CVP-specific internal libraries are used by the script to access form fields and CVP variables.
Example (Showing Specification of Field IDs Defined in the Form Builder)	Specification of field IDs defined in the Form Builder	You must specify the IDs of fields you defined in the Form Builder in **Step 2**. The fields you specify are included in the Configlet content generated by the script.
Example (Showing Use Of Standard Python Script Syntax)	Use of standard Python syntax	The Configlet Builder supports the use of standard Python syntax to build parts of the Configlet. You can also make calls to external files and database.
Example (Showing Print Output)	Print output (Configlet content)	The script automatically produces print output from the CVP internal libraries you imported and the fields you have defined in the script. The print output is the content of the Configlet.

Figure 11-3: Example (Showing Import of CVP-Specific Internal Libraries)



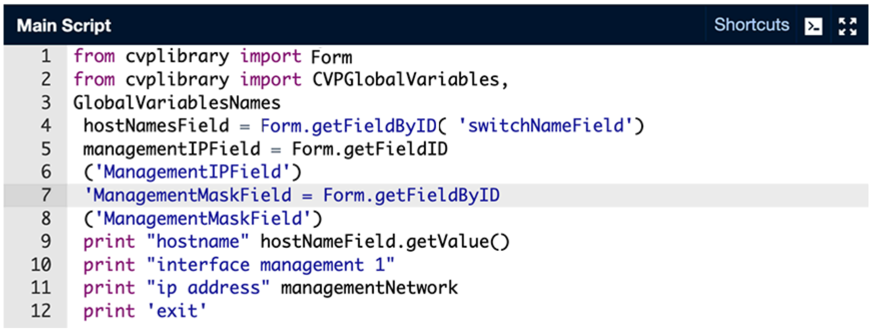
```
from cvplibrary import form
from cvplibrary import CVPGlobalVariables,
GlobalVariablesNames
 hostNamesField = Form.getFieldID( "switchNameField")
 managementIPField = Form.getFieldID
 ("ManagementIPField")
 'ManagementMaskField = Form.getFieldByID
 ("ManagementMaskField")
 print "hostname" hostNameField.getValue()
 print "interface management 1"
 print "ip address" managementNetwork
 print 'exit'
```

Figure 11-4: Example (Showing Specification of Field IDs Defined in the Form Builder)



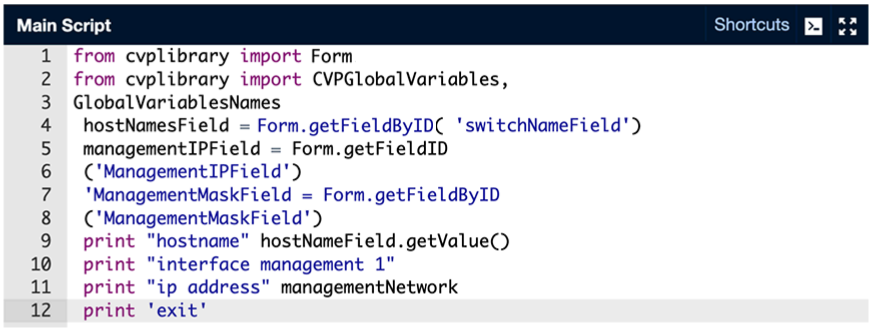
```
from cvplibrary import Form
from cvplibrary import CVPGlobalVariables,
GlobalVariablesNames
 hostNamesField = Form.getFieldByID( 'switchNameField')
 managementIPField = Form.getFieldID
 ('ManagementIPField')
 'ManagementMaskField = Form.getFieldByID
 ('ManagementMaskField')
 print "hostname" hostNameField.getValue()
 print "interface management 1"
 print "ip address" managementNetwork
 print 'exit'
```

Figure 11-5: Example (Showing Use Of Standard Python Script Syntax)



```
from cvplibrary import Form
from cvplibrary import CVPGlobalVariables,
GlobalVariablesNames
 hostNamesField = Form.getFieldByID( 'switchNameField')
 managementIPField = Form.getFieldID
 ('ManagementIPField')
 'ManagementMaskField = Form.getFieldByID
 ('ManagementMaskField')
 print "hostname" hostNameField.getValue()
 print "interface management 1"
 print "ip address" managementNetwork
 print 'exit'
```

Figure 11-6: Example (Showing Print Output)

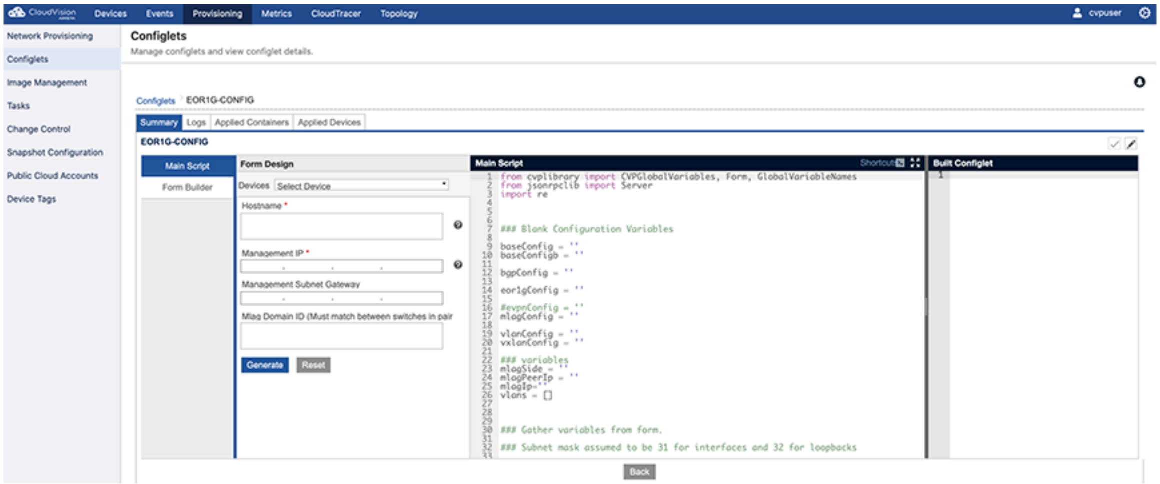


```
from cvplibrary import Form
from cvplibrary import CVPGlobalVariables,
GlobalVariablesNames
 hostNamesField = Form.getFieldByID( 'switchNameField')
 managementIPField = Form.getFieldID
 ('ManagementIPField')
 'ManagementMaskField = Form.getFieldByID
 ('ManagementMaskField')
 print "hostname" hostNameField.getValue()
 print "interface management 1"
 print "ip address" managementNetwork
 print 'exit'
```

Note: Complete steps 4 and 5 to test the script to make sure it can generate Configlet content.

4. Fill in the Form Design fields.

Figure 11-7: Filling in the Design Fields



Devices: Select Device

Hostname *

Management IP *

Management Subnet Gateway

Mlag Domain ID (Must match between switches in pair

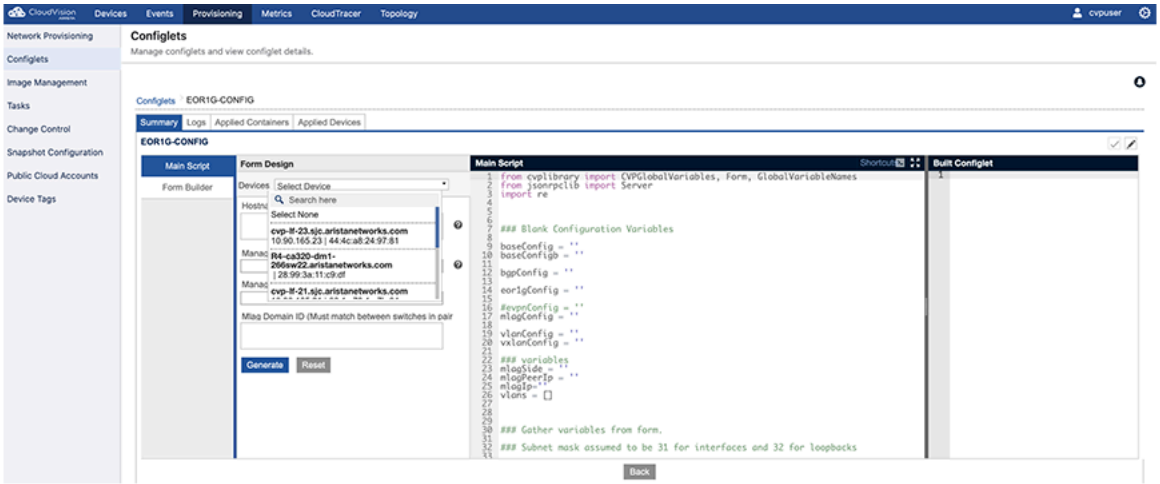
```
from cvplibrary import CVPGlobalVariables, Form, GlobalVariableNames
from jsonrpclib import Server
import re



### Blank Configuration Variables

baseConfig = ''
baseConfigb = ''

bgpConfig = ''

eor1gConfig = ''

#evpnConfig = ''
mlagConfig = ''

vlanConfig = ''
vxlanConfig = ''

### variables
mlagSide = ''
mlagPeerIp = ''
mlagIp=''
vlans = []



### Gather variables from form.

### Subnet mask assumed to be 31 for interfaces and 32 for loopbacks

```

5. Click **Generate.**

The Configlet content is generated and shows in the **Built Configlet** pane.

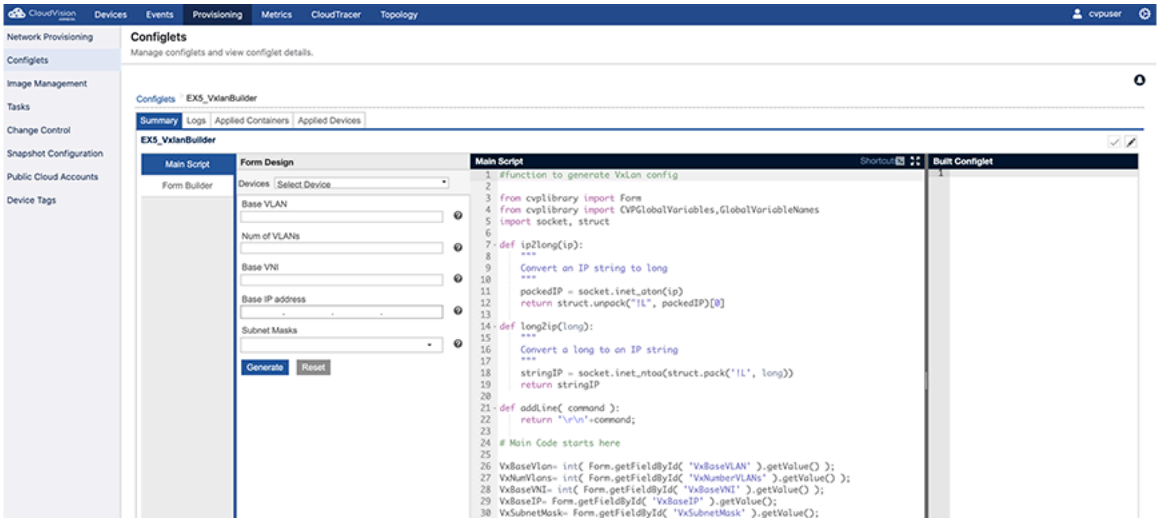
Note: If it is necessary to select a device to generate the Configlet, then select a device from the list of devices under Form Design.

Figure 11-8: Selecting a Device from the List of Devices Under Form Design



```
from cvplibrary import CVPGlobalVariables, Form, GlobalVariableNames
from jsonrpclib import Server
import re



### Blank Configuration Variables

baseConfig = ''
baseConfigb = ''

bgpConfig = ''

eor1gConfig = ''

#evpnConfig = ''
mlagConfig = ''

vlanConfig = ''
vxlanConfig = ''

### variables
mlagSide = ''
mlagPeerIp = ''
mlagIp=''
vlans = []



### Gather variables from form.

### Subnet mask assumed to be 31 for interfaces and 32 for loopbacks
```

Figure 11-9: Example (Generating Configlet Content)



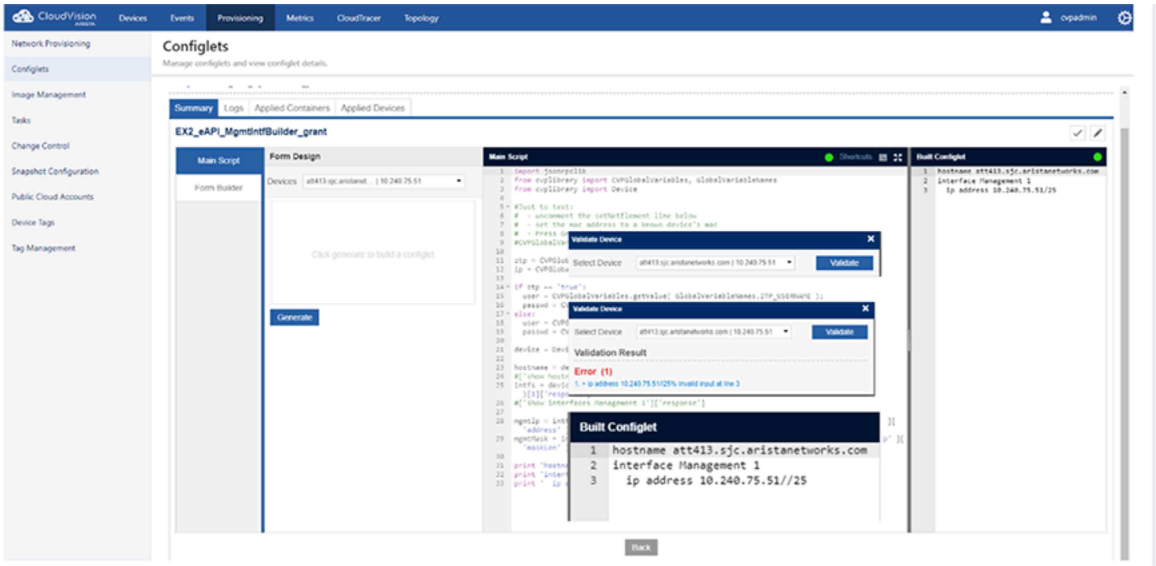
```
#function to generate Vxlan config

from cvplibrary import Form
from cvplibrary import CVPGlobalVariables,GlobalVariableNames
import socket, struct

def ip2long(ip):
    """
    Convert an IP string to long
    """
    packedIP = socket.inet_aton(ip)
    return struct.unpack("!L", packedIP)[0]

def long2ip(long):
    """
    Convert a long to an IP string
    """
    stringIP = socket.inet_ntoa(struct.pack('!L', long))
    return stringIP

def addLine( command ):
    return '\r\n'+command;

# Main Code starts here

VxBaseVlan= int( Form.getFieldById( 'VxBaseVLAN' ).getValue() );
VxNumVlans= int( Form.getFieldById( 'VxNumberVLANs' ).getValue() );
VxBaseVNI= int( Form.getFieldById( 'VxBaseVNI' ).getValue() );
VxBaseIP= Form.getFieldById( 'VxBaseIP' ).getValue();
VxSubnetMask= Form.getFieldById( 'VxSubnetMask' ).getValue();
```

6. Validate the generated Configlet on the device by clicking the **Tick** icon at the upper-right of the page.

   The Validate Device dialog appears.

7. In the Validate Device pop-up dialog, click Validate.

Figure 11-10: Example Script (Validating Device)



Configlets

Manage configlets and view configlet details.

EX2_eAPI_MgmtIntfBuilder_grant

Devices: att413.sjc.aristanet... | 10.240.75.51

Validate Device

Select Device: att413.sjc.aristanetworks.com | 10.240.75.51 [Validate]

Validation Result

Error (1)

1. > ip address 10.240.75.51//25% invalid input at line 3

Built Configlet

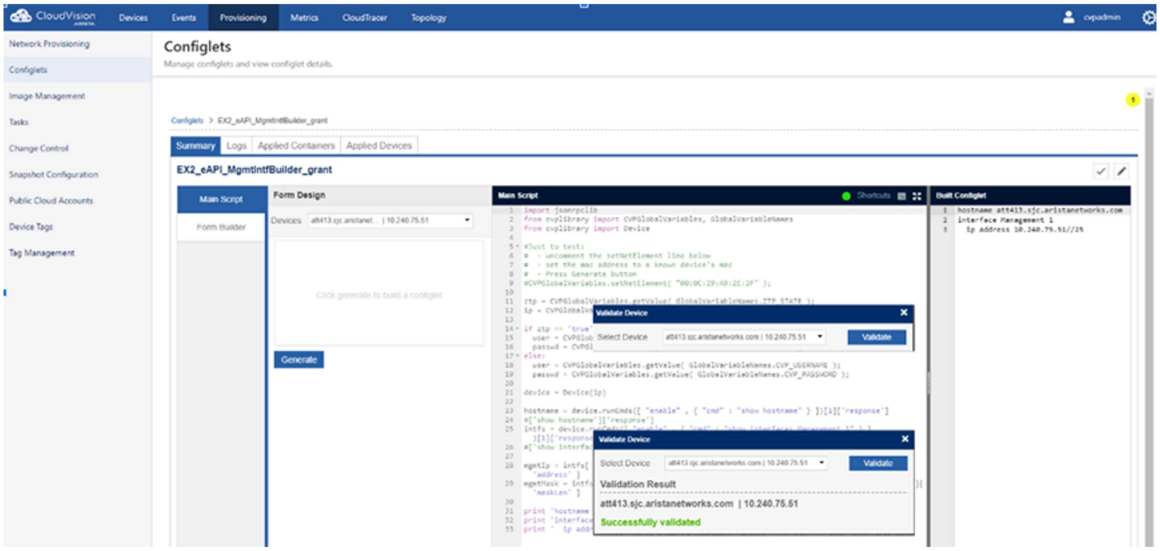
```
1  hostname att413.sjc.aristanetworks.com
2  interface Management 1
3    ip address 10.240.75.51//25
```

If the device cannot be validated, the error (or errors) are listed in the Validate Device dialog.

8. (If needed) Correct any errors and repeat step 7 to validate the device.

The Validate Device dialog shows a message to indicate a successful validation.

Figure 11-11: Example Script (Re-Validating Device after Correction)



Configlets

Manage configlets and view configlet details.

EX2_eAPI_MgmtIntfBuilder_grant

Devices: att413.sjc.aristanet... | 10.240.75.51

Validate Device

Select Device: att413.sjc.aristanetworks.com | 10.240.75.51 [Validate]

Validation Result

att413.sjc.aristanetworks.com | 10.240.75.51

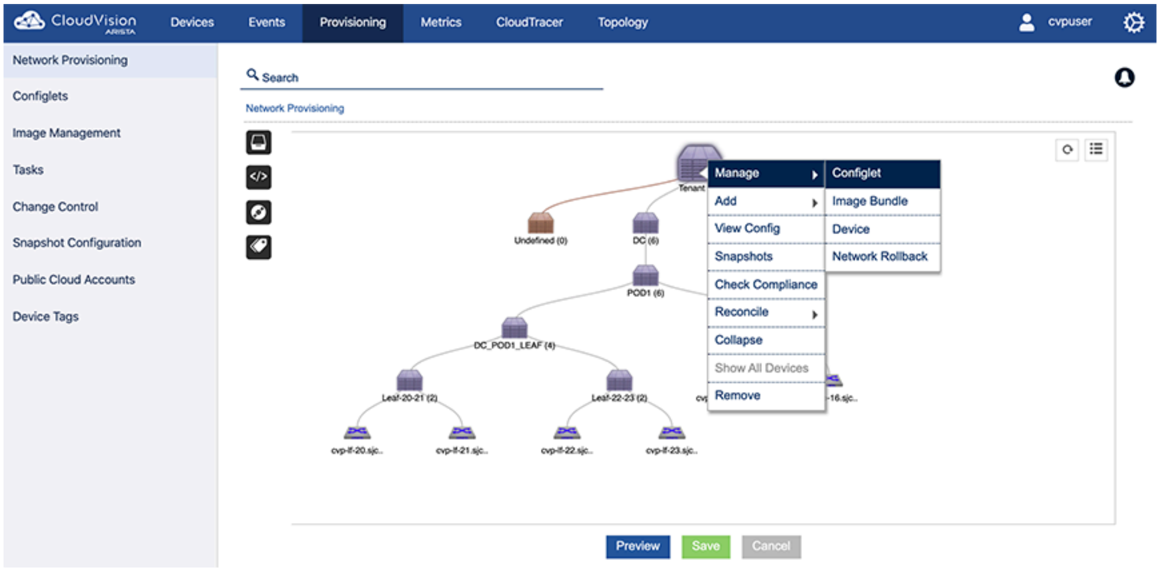
Successfully validated

9. To apply the new Configlet to the container, do the following:

   a. Go the Network Provisioning page.

b. Right-click the container and choose **Manage > Configlet**.

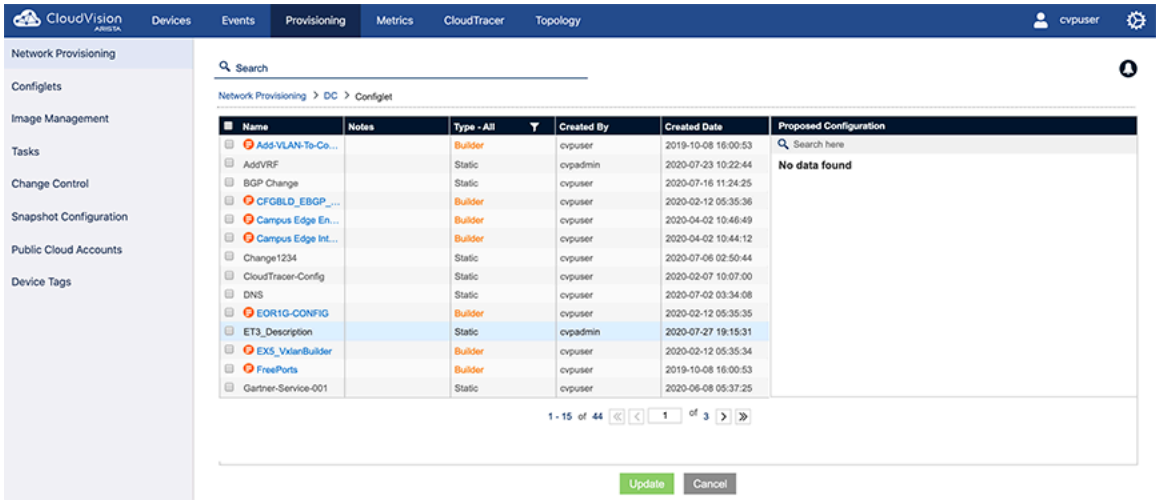
Figure 11-12: Select the Container to Apply the New Configlet



The list of available Configlets appears on the Configlet page.

10. Select the Configlet to apply to the device by clicking the checkbox next to the name of the Configlet.

Figure 11-13: Select Configlet on Configlet Page



Name	Notes	Type - All	Created By	Created Date
□ Add-VLAN-To-Co...		Builder	cvpuser	2019-10-08 16:00:53
□ AddVRF		Static	cvpadmin	2020-07-23 10:22:44
□ BGP Change		Static	cvpuser	2020-07-16 11:24:25
□ CFGBLD_EBGP_...		Builder	cvpuser	2020-02-12 05:35:36
□ Campus Edge En...		Builder	cvpuser	2020-04-02 10:46:49
□ Campus Edge Int...		Builder	cvpuser	2020-04-02 10:44:12
□ Change1234		Static	cvpuser	2020-07-06 02:50:44
□ CloudTracer-Config		Static	cvpuser	2020-02-07 10:07:00
□ DNS		Static	cvpuser	2020-07-02 03:34:08
□ EOR1G-CONFIG		Builder	cvpuser	2020-02-12 05:35:35
□ ET3_Description		Static	cvpadmin	2020-07-27 19:15:31
□ EX5_VxlanBuilder		Builder	cvpuser	2020-02-12 05:35:34
□ FreePorts		Builder	cvpuser	2019-10-08 16:00:53
□ Gartner-Service-001		Static	cvpuser	2020-06-08 05:37:25

Proposed Configuration

Search here

No data found

1 - 15 of 44 « ‹ 1 of 3 › »

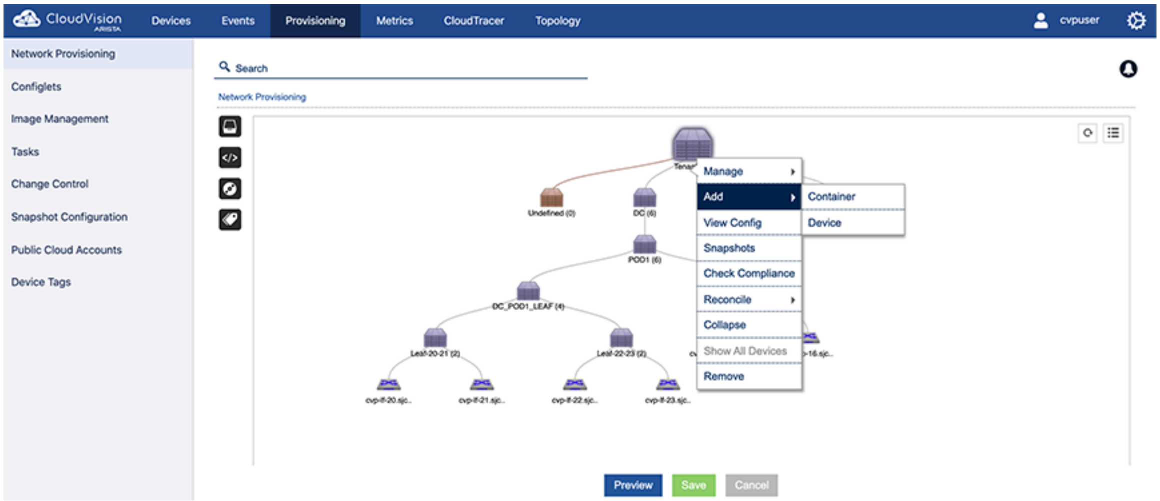
Update Cancel

11. To add devices to the container, do the following:

a. Go the **Network Provisioning** page.

b. Right-click the container and choose **Device > Add**.

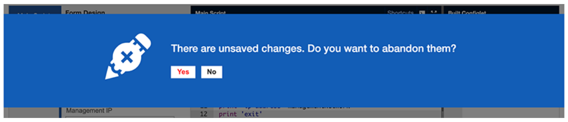
Figure 11-14: Adding Devices to the Container



12. Do one of the following:

- Click **Yes** to apply the Configlet you selected to all of the devices in the hierarchy.
- Click **No** if you do not want to apply the Configlet you selected to all of the devices in the hierarchy.

Figure 11-15: Message Indicating Selection of Hierarchical Container

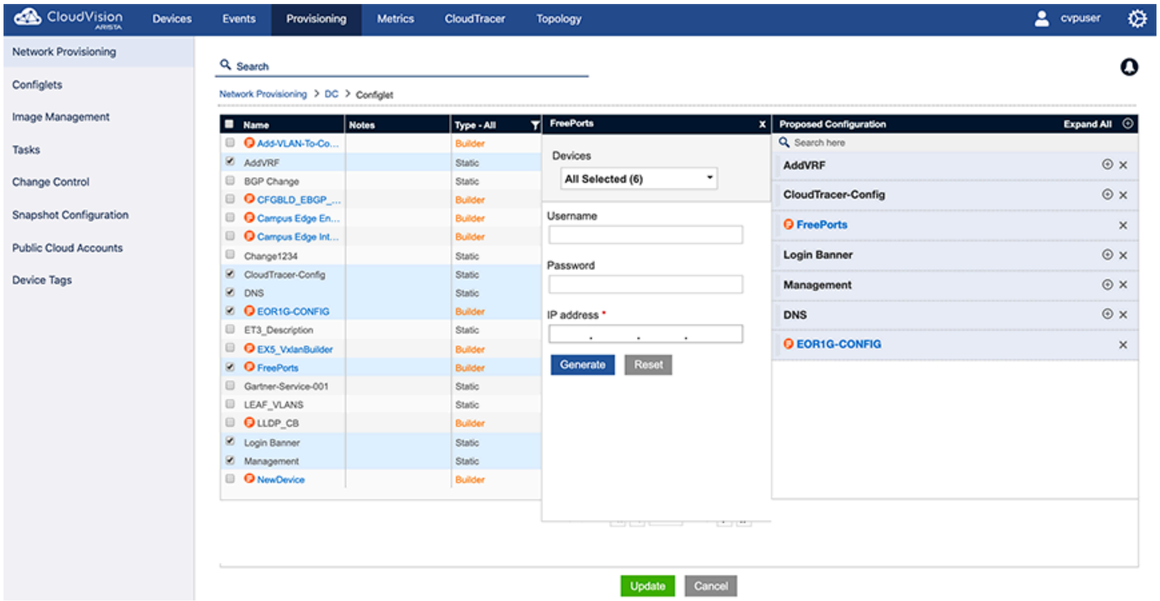


There are unsaved changes. Do you want to abandon them?

The Configlet page appears showing the Configlet you selected to apply to the container.

13. To assign the Configlet Builder to the container you selected, select (click) the **Configlet Builder**.

Figure 11-16: Selecting the Configlet to Assign to the Container



■	Name	Notes	Type - All
□	Add-VLAN-To-Co...		Builder
☑	AddVRF		Static
□	BGP Change		Static
□	CFGBLD_EBGP_...		Builder
□	Campus Edge En...		Builder
□	Campus Edge Int...		Builder
□	Change1234		Static
☑	CloudTracer-Config		Static
☑	DNS		Static
☑	EOR1G-CONFIG		Builder
□	ET3_Description		Static
□	EX5_VxlanBuilder		Builder
☑	FreePorts		Builder
□	Gartner-Service-001		Static
□	LEAF_VLANS		Static
□	LLDP_CB		Builder
☑	Login Banner		Static
☑	Management		Static
□	NewDevice		Builder

FreePorts

Devices: All Selected (6)

Username

Password

IP address *

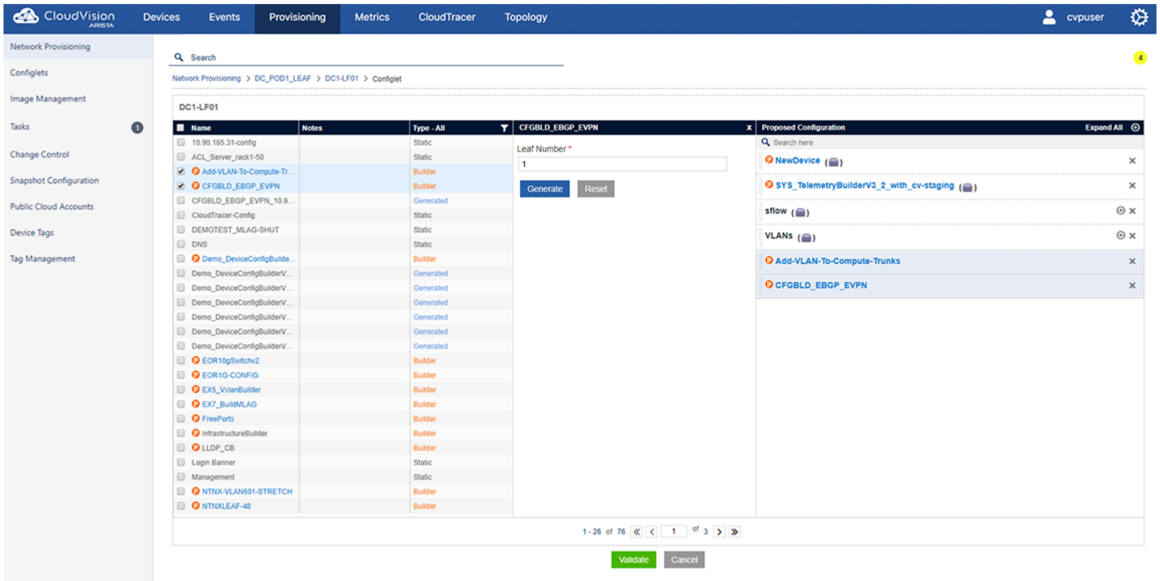
Proposed Configuration — Expand All

Search here

- AddVRF
- CloudTracer-Config
- FreePorts
- Login Banner
- Management
- DNS
- EOR1G-CONFIG

The page loads a form.

Figure 11-17: Form Loaded on Page after you Select the Configlet Builder



Network Provisioning > DC_POD1_LEAF > DC1-LF01 > Configlet

DC1-LF01

	Name	Notes	Type - All
□	10.90.165.31-config		Static
□	ACL_Server_rack1-50		Static
☑	Add-VLAN-To-Compute-Tr...		Builder
☑	CFGBLD_EBGP_EVPN		Builder
□	CFGBLD_EBGP_EVPN_10.9...		Generated
□	CloudTracer-Config		Static
□	DEMOTEST_MLAG-SHUT		Static
□	DNS		Static
□	Demo_DeviceConfigBuilde...		Builder
□	Demo_DeviceConfigBuilderV...		Generated
□	Demo_DeviceConfigBuilderV...		Generated
□	Demo_DeviceConfigBuilderV...		Generated
□	Demo_DeviceConfigBuilderV...		Generated
□	Demo_DeviceConfigBuilderV...		Generated
□	Demo_DeviceConfigBuilderV...		Generated
□	EOR10gSwitchv2		Builder
□	EOR1G-CONFIG		Builder
□	EX5_VxlanBuilder		Builder
□	EX7_BuildMLAG		Builder
□	FreePorts		Builder
□	InfrastructureBuilder		Builder
□	LLDP_CB		Builder
□	Login Banner		Static
□	Management		Static
□	NTNX-VLAN601-STRETCH		Builder
□	NTNXLEAF-48		Builder

CFGBLD_EBGP_EVPN ×

Leaf Number *

1

Generate   Reset

Proposed Configuration   Expand All

Search here

- NewDevice ×
- SYS_TelemetryBuilderV3_2_with_cv-staging ×
- sflow ×
- VLANs ×
- Add-VLAN-To-Compute-Trunks ×
- CFGBLD_EBGP_EVPN ×

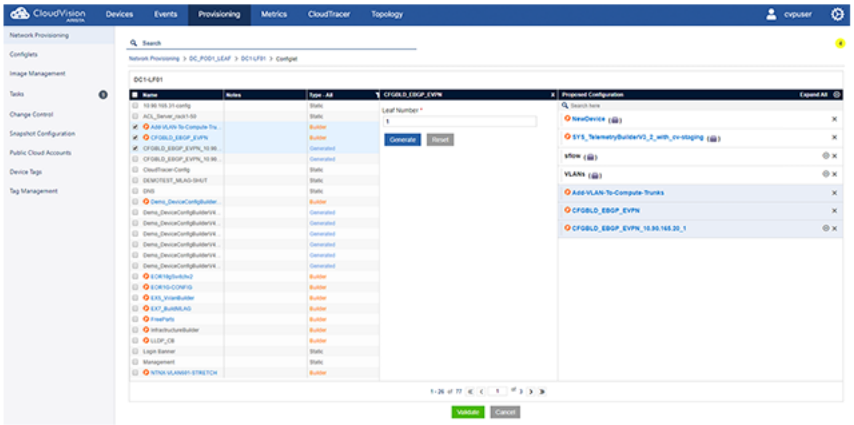
1 - 26 of 76 « ‹ 1 of 3 › »

Validate   Cancel

14. Complete (fill in) the form and then click **Generate**.

The Configlet Builder creates the new, device-specific Configlet, and the Configlet is shown in the **Built Configlet** pane.

Figure 11-18: Configlet Page Showing New, Device-Specific Configlet



Network Provisioning > DC_POD1_LEAF > DC1-LF01 > Configlet

DC1-LF01

	Name	Notes	Type - All
□	10.90.165.31-config		Static
□	ACL_Server_rack1-50		Static
☑	Add-VLAN-To-Compute-Tru...		Builder
☑	CFGBLD_EBGP_EVPN		Builder
☑	CFGBLD_EBGP_EVPN_10.90...		Generated
□	CFGBLD_EBGP_EVPN_10.90...		Generated
□	CloudTracer-Config		Static
□	DEMOTEST_MLAG-SHUT		Static
□	DNS		Static
□	Demo_DeviceConfigBuilder...		Builder
□	Demo_DeviceConfigBuilderV4...		Generated
□	Demo_DeviceConfigBuilderV4...		Generated
□	Demo_DeviceConfigBuilderV4...		Generated
□	Demo_DeviceConfigBuilderV4...		Generated
□	Demo_DeviceConfigBuilderV4...		Generated
□	Demo_DeviceConfigBuilderV4...		Generated
□	EOR10gSwitchv2		Builder
□	EOR1G-CONFIG		Builder
□	EX5_VxlanBuilder		Builder
□	EX7_BuildMLAG		Builder
□	FreePorts		Builder
□	InfrastructureBuilder		Builder
□	LLDP_CB		Builder
□	Login Banner		Static
□	Management		Static
□	NTNX-VLAN601-STRETCH		Builder

CFGBLD_EBGP_EVPN ×

Leaf Number *

1

Generate   Reset

Proposed Configuration   Expand All

Search here

- NewDevice ×
- SYS_TelemetryBuilderV3_2_with_cv-staging ×
- sflow ×
- VLANs ×
- Add-VLAN-To-Compute-Trunks ×
- CFGBLD_EBGP_EVPN ×
- CFGBLD_EBGP_EVPN_10.90.165.20_1 ×

1-26 of 77 « ‹ 1 of 3 › »

Validate   Cancel

11.1.3 Using the Provided Configlet Builder Examples

CloudVision Portal (CVP) provides some Configlet Builder examples to help you get started using this feature.

You can load the examples to your CVP instance using the following commands:

- Log into the primary node's Linux shell as root user.
- Change directory to */cvpi/tools* and import the example Configlets using the cvptool.

```
./cvptool.py --host <host> --user <user> --password <pass> --objects
 Configlets --action restore --tarFile examples.tar.
```

The provided examples include:

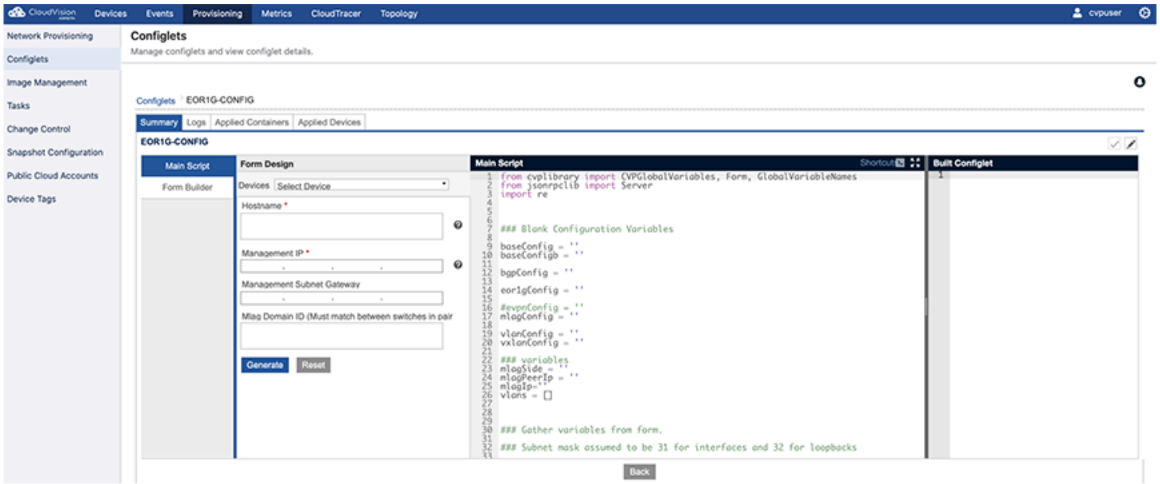
- Example 1: Form-based management interface Configlet Builder

- Example 2: eAPI-based management interface Configlet Builder
- Example 3: SSH-based management interface Configlet Builder
- Example 4: MySQL-based management interface Configlet Builder
- Example 5: Device library based management interface Configlet Builder

11.1.3.1 Example 1: Form-based management interface Configlet Builder

This example uses the form to input the management interface configuration, and generates a new Configlet to preserve the configuration.

Figure 11-19: Example 1



Devices: Select Device

Hostname *

Management IP *

Management Subnet Gateway

Mlag Domain ID (Must match between switches in pair

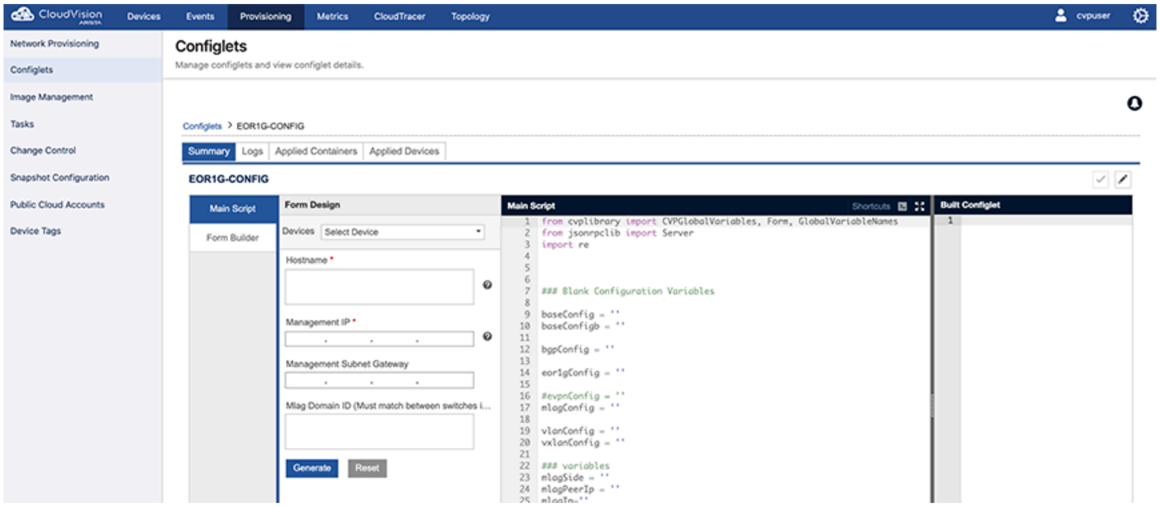
```
from cvplibrary import CVPGlobalVariables, Form, GlobalVariableNames
from jsonrpclib import Server
import re



### Blank Configuration Variables

baseConfig = ''
baseConfigb = ''

bgpConfig = ''

eor1gConfig = ''

#evpnConfig = ''
mlagConfig = ''

vlanConfig = ''
vxlanConfig = ''

### variables
mlagSide = ''
mlagPeerIp = ''
mlagIp=''
vlans = []



### Gather variables from form.

### Subnet mask assumed to be 31 for interfaces and 32 for loopbacks
```

11.1.3.2 Example 2: eAPI-based management interface Configlet Builder

This example uses eAPI to read the management interface configuration that the device received from the DHCP server during the ZTP boot, and generates a new Configlet to preserve the configuration.

Note: No UI widgets are associated with the Configlet Builder in this example.

Figure 11-20: Example 2



Devices: Select Device

Hostname *

Management IP *

Management Subnet Gateway

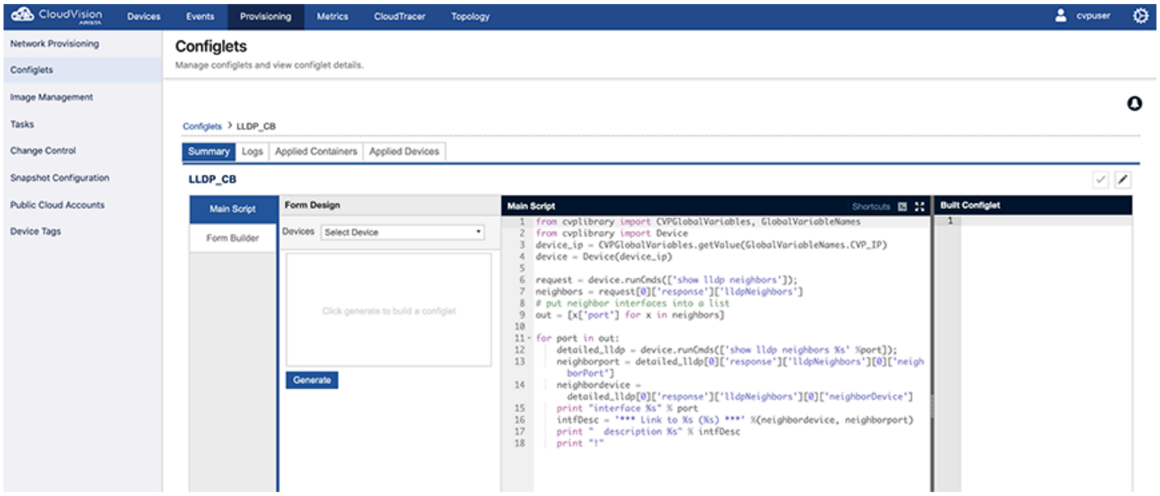
Mlag Domain ID (Must match between switches i...

```
from cvplibrary import CVPGlobalVariables, Form, GlobalVariableNames
from jsonrpclib import Server
import re



### Blank Configuration Variables

baseConfig = ''
baseConfigb = ''

bgpConfig = ''

eor1gConfig = ''

#evpnConfig = ''
mlagConfig = ''

vlanConfig = ''
vxlanConfig = ''

### variables
mlagSide = ''
mlagPeerIp = ''
mlagIp=''
```

11.1.3.3 Example 3: SSH-based management interface Configlet Builder

This example uses SSH to read the management interface configuration that the device received from the DHCP server during the ZTP boot, and generates a new Configlet to preserve the configuration.

Figure 11-21: Example 3



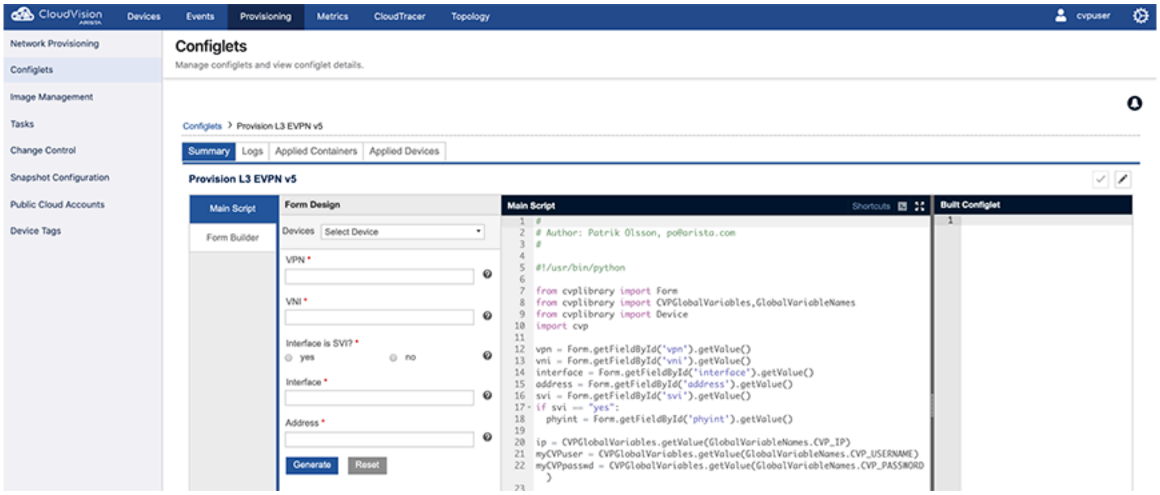
```
from cvplibrary import CVPGlobalVariables, GlobalVariableNames
from cvplibrary import Device
device_ip = CVPGlobalVariables.getValue(GlobalVariableNames.CVP_IP)
device = Device(device_ip)

request = device.runCmds(['show lldp neighbors']);
neighbors = request[0]['response']['lldpNeighbors']
# put neighbor interfaces into a list
out = [x['port'] for x in neighbors]

for port in out:
    detailed_lldp = device.runCmds(['show lldp neighbors %s' %port]);
    neighborport = detailed_lldp[0]['response']['lldpNeighbors'][0]['neigh
      borPort']
    neighbordevice =
      detailed_lldp[0]['response']['lldpNeighbors'][0]['neighborDevice']
    print "interface %s" % port
    intfDesc = '*** Link to %s (%s) ***' %(neighbordevice, neighborport)
    print "  description %s" % intfDesc
    print "!"
```

11.1.3.4 Example 4: MySQL-based management interface Configlet Builder

In this example, the Configlet Builder uses the device’s MAC address to lookup up its Management IP address, netmask, default route, and host name, which are stored on external MySQL server, and generates a new Configlet to preserve the configuration.

Note: No UI widgets are associated with the Configlet Builder in this example.

Figure 11-22: Example 4

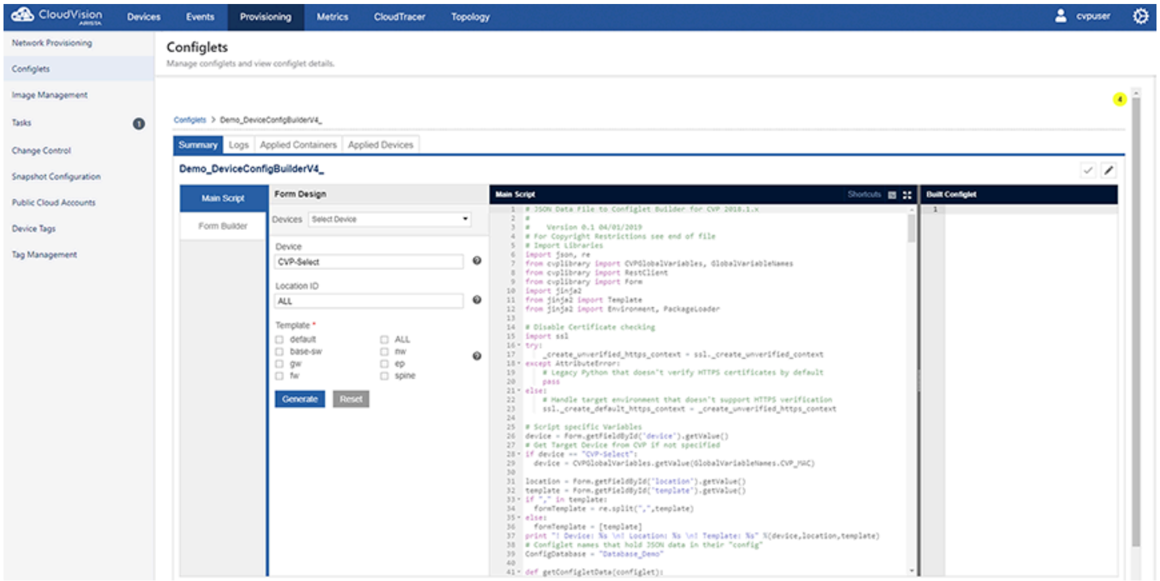


```
#
# Author: Patrik Olsson, po@arista.com
#

#!/usr/bin/python

from cvplibrary import Form
from cvplibrary import CVPGlobalVariables,GlobalVariableNames
from cvplibrary import Device
import cvp

vpn = Form.getFieldById('vpn').getValue()
vni = Form.getFieldById('vni').getValue()
interface = Form.getFieldById('interface').getValue()
address = Form.getFieldById('address').getValue()
svi = Form.getFieldById('svi').getValue()
if svi == "yes":
  phyint = Form.getFieldById('phyint').getValue()

ip = CVPGlobalVariables.getValue(GlobalVariableNames.CVP_IP)
myCVPuser = CVPGlobalVariables.getValue(GlobalVariableNames.CVP_USERNAME)
myCVPpasswd = CVPGlobalVariables.getValue(GlobalVariableNames.CVP_PASSWORD
  )
```

11.1.3.5 Example 5: Device library based management interface Configlet Builder

This example uses Device library to read the management interface configuration that the device received from the DHCP server during the ZTP boot, and generates a new Configlet to preserve the configuration.

Figure 11-23: Example 5



Devices: Select Device

Device: CVP-Select

Location ID: ALL

Template *

□ default □ ALL
□ base-sw □ mw
□ gw □ ep
□ fw □ spine

Generate Reset

```
# JSON Data File to Configlet Builder for CVP 2018.1.x
#
#    Version 0.1 04/01/2019
# For Copyright Restrictions see end of file
# Import Libraries
import json, re
from cvplibrary import CVPGlobalVariables, GlobalVariableNames
from cvplibrary import RestClient
from cvplibrary import Form
import jinja2
from jinja2 import Template
from jinja2 import Environment, PackageLoader

# Disable Certificate checking
import ssl
try:
    _create_unverified_https_context = ssl._create_unverified_context
except AttributeError:
    # Legacy Python that doesn't verify HTTPS certificates by default
    pass
else:
    # Handle target environment that doesn't support HTTPS verification
    ssl._create_default_https_context = _create_unverified_https_context

# Script specific Variables
device = Form.getFieldById('device').getValue()
# Get Target Device from CVP if not specified
if device == "CVP-Select":
  device = CVPGlobalVariables.getValue(GlobalVariableNames.CVP_MAC)

location = Form.getFieldById('location').getValue()
template = Form.getFieldById('template').getValue()
if "," in template:
  formTemplate = re.split(",",template)
else:
  formTemplate = [template]
print "! Device: %s \n! Location: %s \n! Template: %s" %(device,location,template)
# Configlet names that hold JSON data in their "config"
ConfigDatabase = "Database_Demo"

def getConfigletData(configlet):
```

1

11.1.4 Python Execution Environment

The CloudVision Portal (CVP) python execution is supported by several CVP-specific libraries. These libraries provide access to the various CVP services and device state.

11.1.4.1 CVP Form

This library provides access to the user interface (UI) widgets that can be associated with a Configlet Builder (see the provided examples for usage details).

The supported methods are:

```
from cvplibrary import Form
obj =  Form.getFieldById( ‘id' );
print obj.getValue()

obj.getFieldById( ‘id' ); - Used to get the UI widget by id
obj.getValue() - To get the value
obj.getFieldID() - To get the unique id
obj.isMandatory() - Gets whether the field is mandatory or not
obj.getHelpText() - To get the help text
obj.getDependsOn() - To get the depends on
obj.getType() - To get the type (TextBox, Dropdown,etc)
obj.getDataValidation() - To get the Data validation
```

11.1.4.2 CVP Global Variables and Supported Methods

This library give access to the current execution context for Configlet Builders (see the provided examples for usage details).

The supplied global variables are:

```
from cvplibrary import CVPGlobalVariables, GlobalVariableNames
```

```
CVPGlobalVariables.getValue(GlobalVariableNames.CVP_USERNAME)

Supported GlobalVariableNames:
   CVP_USERNAME - Username of the current user
   CVP_PASSWORD - Password of the current user
   CVP_IP - IP address of the current device
   CVP_MAC - MAC of the current device
   CVP_SERIAL - Serial number of the current device
   CVP_SESSION_ID - Session id of current cvp user
   ZTP_STATE - ZTP state of the device (true/false)
   ZTP_USERNAME - Default username to login to ztp enabled device
   ZTP_PASSWORD - Password to login to ztp enabled device
   CVP_ALL_LABELS - Labels associated to current device
   CVP_CUSTOM_LABELS - Custom labels associated to current device
   CVP_SYSTEM_LABELS - System/Auto generated labels associated to current
 device
```

11.1.4.3 CVP Rest Client

This library allows a Configlet Builder to access any CVP API endpoint. The following is an example:

```
from cvplibrary import RestClient
url='http://localhost/cvpservice/inventory/devices';
method= 'GET';
client= RestClient(url,method);
if client.connect():
    print client.getResponse()
```

If no certificates are installed on the server, then add the following lines to ignore ssl warnings:

```
import ssl
ssl._create_default_https_context = ssl._create_unverified_contex
```

11.1.5 Creating Configlets Manually

CloudVision Portal (CVP) enables you to create Configlet manually. This method should be used to create Configlets that are relatively static.

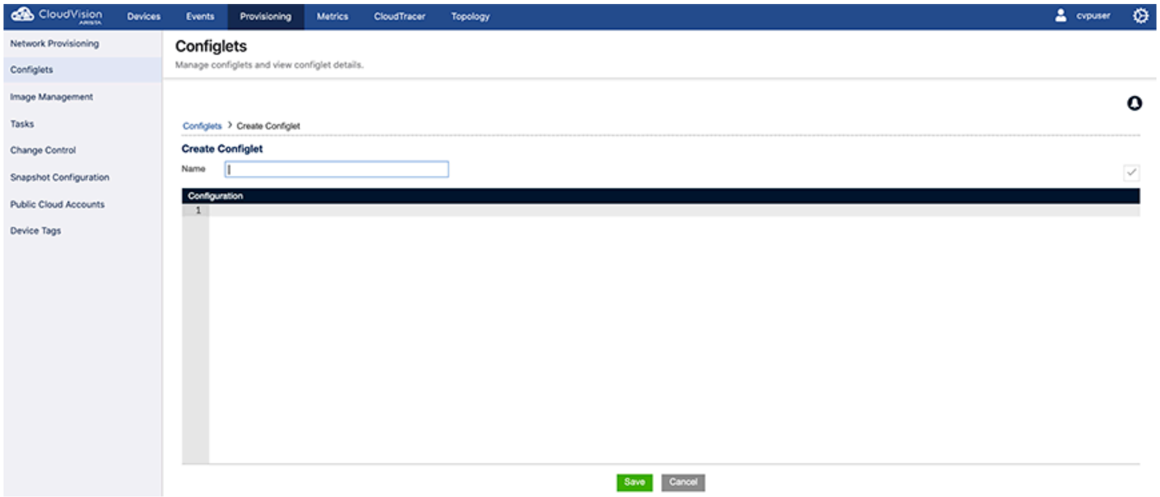
Note: If you need to create Configlets that require less user input, you may want to use the Configlet Builder feature.

Complete these steps to manually create Configlets:

1. Select the “**+**” icon in the grid.

2. The **Create Configlet** page appears.

Figure 11-24: Create Configlet Page



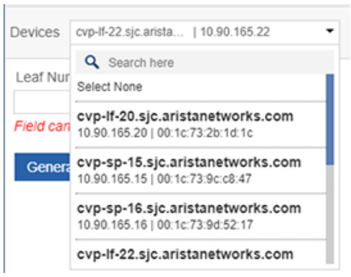
3. Click **Save** to save the Configlet.
4. This will list the Configlet in the Configlet Management grid.

11.1.5.1 Validating a Configlet During Creation

CloudVision provides a facility to enter the Configlet code and validate it before saving the codes.

1. Enter the Configlet codes in the field provided.
2. On the right pane, there is a drop-down menu listing all the switches in CloudVision.
3. Search for the device to be validated.

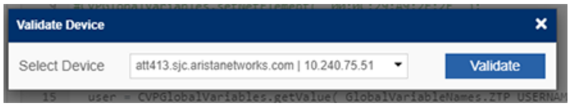
Figure 11-25: Validate-Search Device


Devices: cvp-lf-22.sjc.arista... | 10.90.165.22

Leaf Nur
Field can
Genera
Search here
Select None
cvp-lf-20.sjc.aristanetworks.com
10.90.165.20 | 00:1c:73:2b:1d:1c
cvp-sp-15.sjc.aristanetworks.com
10.90.165.15 | 00:1c:73:9c:c8:47
cvp-sp-16.sjc.aristanetworks.com
10.90.165.16 | 00:1c:73:9d:52:17
cvp-lf-22.sjc.aristanetworks.com

4. Select the switch to validate.

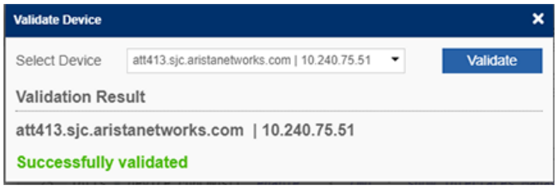
Figure 11-26: Select Device


Select Device: att413.sjc.aristanetworks.com | 10.240.75.51

5. Select **Validate**.

On successful validation, the message Successfully Validated is displayed.

Figure 11-27: Validate-Success



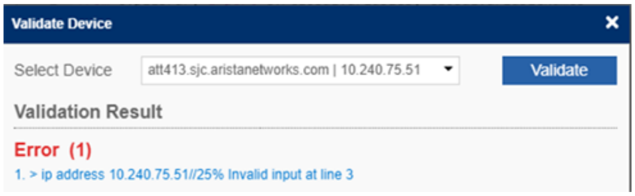
Validation Result

att413.sjc.aristanetworks.com | 10.240.75.51

Successfully validated

When an error occurs, the message error will be displayed.

Figure 11-28: Validation Error



Validation Result

Error (1)

1. > ip address 10.240.75.51//25% Invalid input at line 3

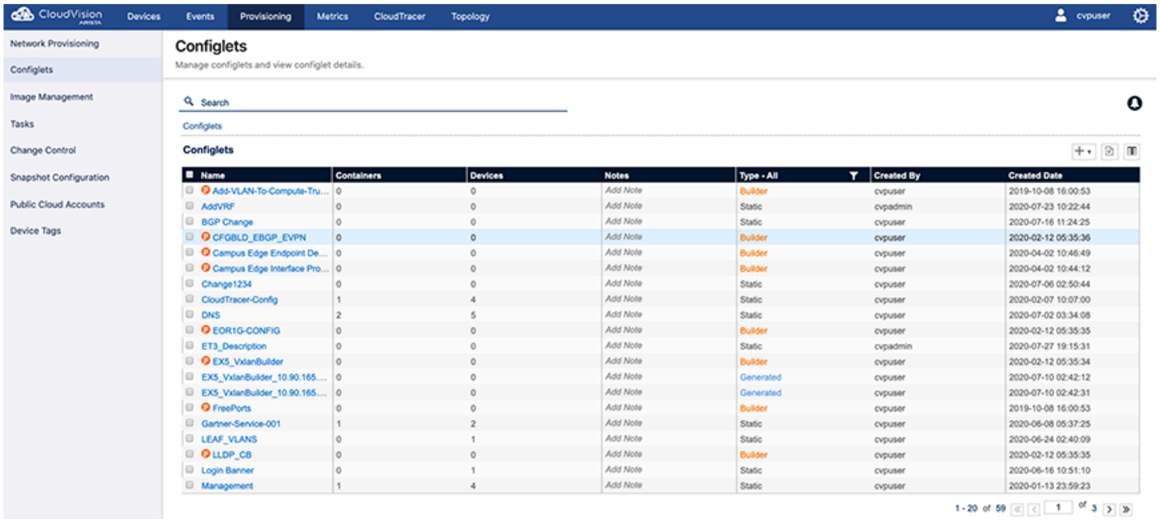
Related topics:

- Configlet Information Page
- Editing Configlets
- Deleting Configlets
- Importing and Exporting Configlets

11.2 Configlet Information Page

1. Select the name of the Configlet from the grid to access the Configlet information page.

Figure 11-29: Configlet Information Page



Configlets

Manage configlets and view configlet details.

Configlets

Configlets

Name	Containers	Devices	Notes	Type - All	Created By	Created Date
Add-VLAN-To-Compute-Tru...	0	0	Add Note	Builder	cvpuser	2019-10-08 16:00:53
AddVRF	0	0	Add Note	Static	cvpadmin	2020-07-23 10:22:44
BGP Change	0	0	Add Note	Static	cvpuser	2020-07-16 11:24:25
CFGBLD_EBGP_EVPN	0	0	Add Note	Builder	cvpuser	2020-02-12 05:35:36
Campus Edge Endpoint De...	0	0	Add Note	Builder	cvpuser	2020-04-02 10:46:49
Campus Edge Interface Pro...	0	0	Add Note	Builder	cvpuser	2020-04-02 10:44:12
Change1234	0	0	Add Note	Static	cvpuser	2020-07-06 02:50:44
CloudTracer-Config	1	4	Add Note	Static	cvpuser	2020-02-07 10:07:00
DNS	2	5	Add Note	Static	cvpuser	2020-07-02 03:34:08
EOR1G-CONFIG	0	0	Add Note	Builder	cvpuser	2020-02-12 05:35:35
ET3_Description	0	0	Add Note	Static	cvpadmin	2020-07-27 19:15:31
EX5_VxlanBuilder	0	0	Add Note	Builder	cvpuser	2020-02-12 05:35:34
EX5_VxlanBuilder_10.90.165....	0	0	Add Note	Generated	cvpuser	2020-07-10 02:42:12
EX5_VxlanBuilder_10.90.165....	0	0	Add Note	Generated	cvpuser	2020-07-10 02:42:31
FreePorts	0	0	Add Note	Builder	cvpuser	2019-10-08 16:00:53
Gartner-Service-001	1	2	Add Note	Static	cvpuser	2020-06-08 05:37:25
LEAF_VLANS	0	1	Add Note	Static	cvpuser	2020-06-24 02:40:09
LLDP_CB	0	0	Add Note	Builder	cvpuser	2020-02-12 05:35:35
Login Banner	0	1	Add Note	Static	cvpuser	2020-06-16 10:51:10
Management	1	4	Add Note	Static	cvpuser	2020-01-13 23:59:23

1 - 20 of 59 « ‹ 1 of 3 › »

11.2.1 Tabs in Configlet Information Page

The Configlet Information page consists of:

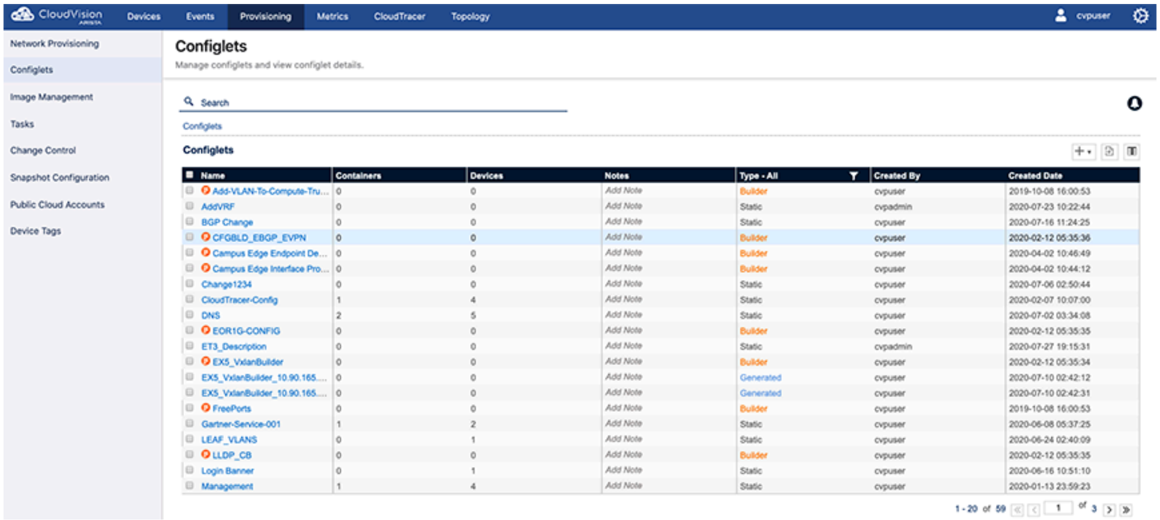
- Summary Tab

- Logs Tab
- Change History Tab
- Applied Containers Tab
- Applied Devices Tab

11.2.1.1 Summary Tab

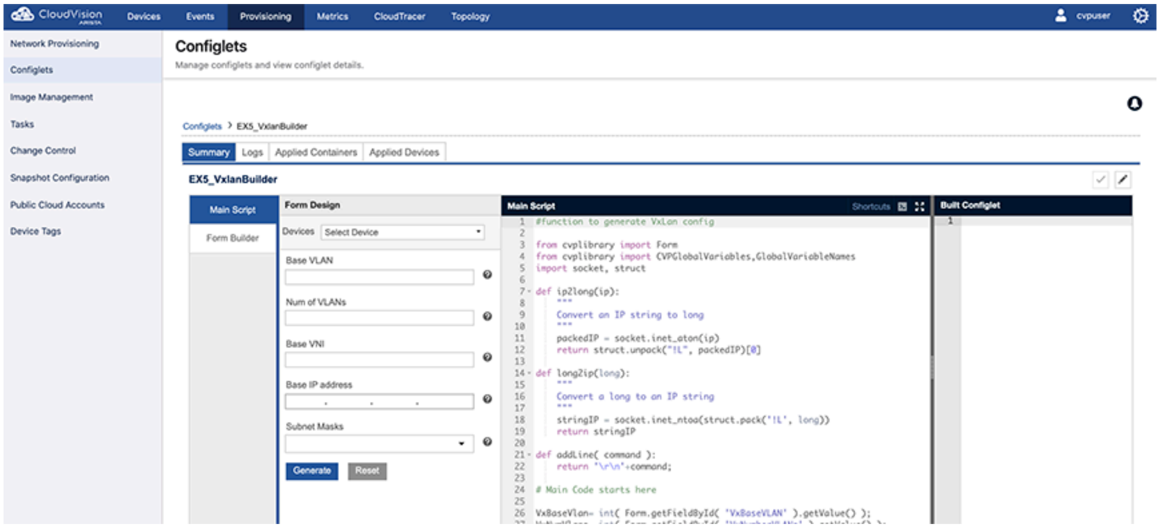
The Configlet “Summary” tab provides information about the Configlet. This tab is used to show static Configlets, and Configlet Builder Configlets.

Figure 11-30: Summary Tab Page for Static Configlets



Name	Containers	Devices	Notes	Type - All	Created By	Created Date
Add-VLAN-To-Compute-Tru...	0	0	Add Note	Builder	cvpuser	2019-10-08 16:00:53
AddVRF	0	0	Add Note	Static	cvpadmin	2020-07-23 10:22:44
BGP Change	0	0	Add Note	Static	cvpuser	2020-07-16 11:24:25
CFGBLD_EBGP_EVPN	0	0	Add Note	Builder	cvpuser	2020-02-12 05:35:36
Campus Edge Endpoint De...	0	0	Add Note	Builder	cvpuser	2020-04-02 10:46:49
Campus Edge Interface Pro...	0	0	Add Note	Builder	cvpuser	2020-04-02 10:44:12
Change1234	0	0	Add Note	Static	cvpuser	2020-07-06 02:50:44
CloudTracer-Config	1	4	Add Note	Static	cvpuser	2020-02-07 10:07:00
DNS	2	5	Add Note	Static	cvpuser	2020-07-02 03:34:08
EOR1G-CONFIG	0	0	Add Note	Builder	cvpuser	2020-02-12 05:35:35
ET3_Description	0	0	Add Note	Static	cvpadmin	2020-07-27 19:15:31
EX5_VxlanBuilder	0	0	Add Note	Builder	cvpuser	2020-02-12 05:35:34
EX5_VxlanBuilder_10.90.165....	0	0	Add Note	Generated	cvpuser	2020-07-10 02:42:12
EX5_VxlanBuilder_10.90.165....	0	0	Add Note	Generated	cvpuser	2020-07-10 02:42:31
FreePorts	0	0	Add Note	Builder	cvpuser	2019-10-08 16:00:53
Gartner-Service-001	1	2	Add Note	Static	cvpuser	2020-06-08 05:37:25
LEAF_VLANS	0	1	Add Note	Static	cvpuser	2020-06-24 02:40:09
LLDP_CB	0	0	Add Note	Builder	cvpuser	2020-02-12 05:35:35
Login Banner	0	1	Add Note	Static	cvpuser	2020-06-16 10:51:10
Management	1	4	Add Note	Static	cvpuser	2020-01-13 23:59:23

Figure 11-31: Configlet Summary Tab Page for Configlet Builder

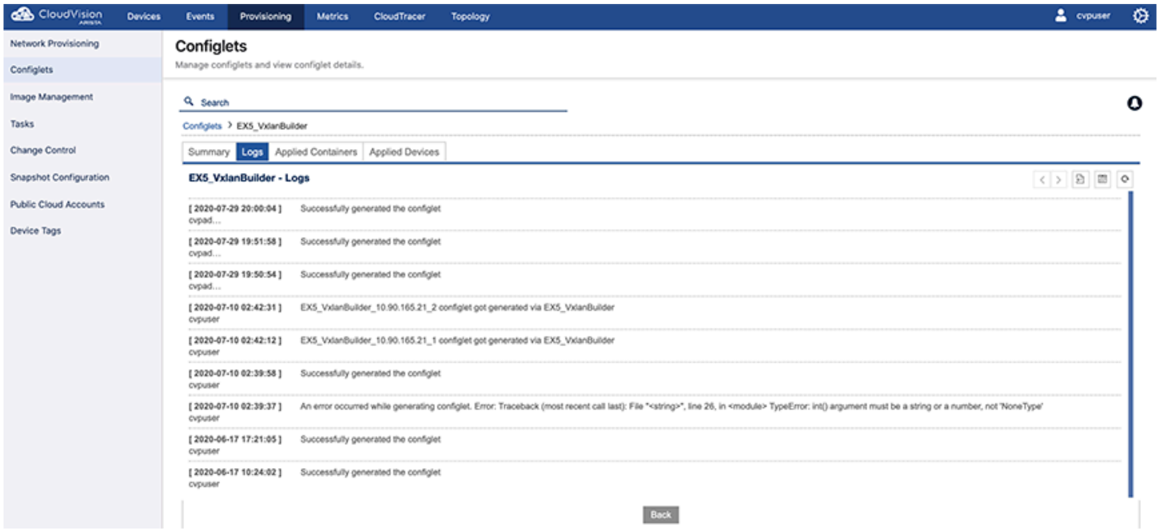


```
#function to generate VxLan config

from cvplibrary import Form
from cvplibrary import CVPGlobalVariables,GlobalVariableNames
import socket, struct

def ip2long(ip):
    """
    Convert an IP string to long
    """
    packedIP = socket.inet_aton(ip)
    return struct.unpack("!L", packedIP)[0]

def long2ip(long):
    """
    Convert a long to an IP string
    """
    stringIP = socket.inet_ntoa(struct.pack('!L', long))
    return stringIP

def addLine( command ):
    return "\r\n"+command;

# Main Code starts here

VxBaseVlan= int( Form.getFieldById( 'VxBaseVLAN' ).getValue() );
```

11.2.1.2 Logs Tab

The “Logs” tab provides complete information on the Configlet assignment to devices and execution details.

Figure 11-32: Configlet Logs Page



```
[ 2020-07-29 20:00:04 ]   Successfully generated the configlet
cvpad...
[ 2020-07-29 19:51:58 ]   Successfully generated the configlet
cvpad...
[ 2020-07-29 19:50:54 ]   Successfully generated the configlet
cvpad...
[ 2020-07-10 02:42:31 ]   EX5_VxlanBuilder_10.90.165.21_2 configlet got generated via EX5_VxlanBuilder
cvpuser
[ 2020-07-10 02:42:12 ]   EX5_VxlanBuilder_10.90.165.21_1 configlet got generated via EX5_VxlanBuilder
cvpuser
[ 2020-07-10 02:39:58 ]   Successfully generated the configlet
cvpuser
[ 2020-07-10 02:39:37 ]   An error occurred while generating configlet. Error: Traceback (most recent call last): File "<string>", line 26, in <module> TypeError: int() argument must be a string or a number, not 'NoneType'
cvpuser
[ 2020-06-17 17:21:05 ]   Successfully generated the configlet
cvpuser
[ 2020-06-17 10:24:02 ]   Successfully generated the configlet
cvpuser
```

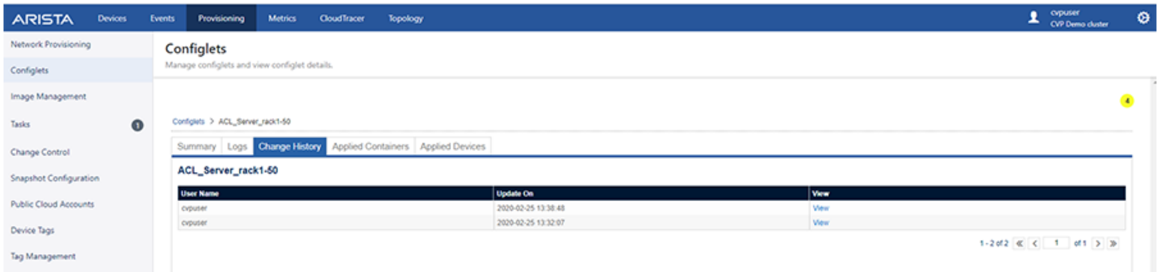
11.2.1.3 Change History Tab

Any change in the Configlets will be recorded in the **History** tab.

1. Select the **View** option.

   A popup window is opened comparing the last version of the Configlet with the edited version (Figure 335: Configlet History Page).

   Figure 11-33: Configlet History Page



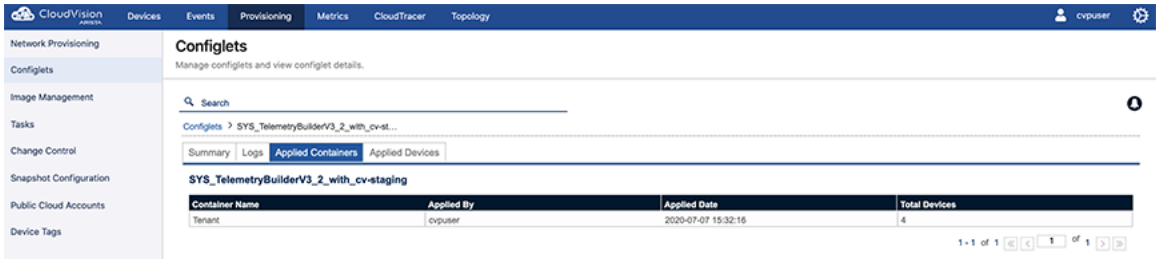
ACL_Server_rack1-50

User Name	Update On	View
cvpuser	2020-02-25 13:38:48	View
cvpuser	2020-02-25 13:32:07	View

11.2.1.4 Applied Containers Tab

This tab gives the details on the containers to which the Configlet is assigned. This also shows the name of the user who made the assignment (Figure 336: Applied Container Page).

Figure 11-34: Applied Container Page



Configlets

Manage configlets and view configlet details.

Configlets > SYS_TelemetryBuilderV3_2_with_cv-st...

SYS_TelemetryBuilderV3_2_with_cv-staging

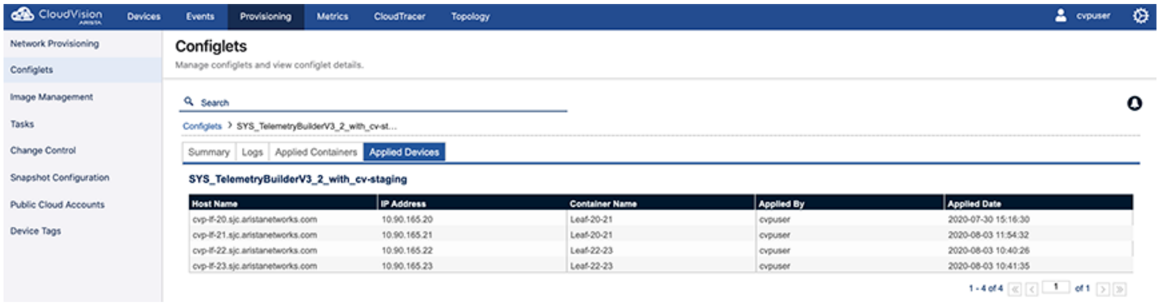
Container Name	Applied By	Applied Date	Total Devices
Tenant	cvpuser	2020-07-07 15:32:16	4

1 - 1 of 1 1 of 1

11.2.1.5 Applied Devices Tab

The **Applied Devices** tab displays the details on the devices to which the Configlet is associated in addition to other information such as **Parent container**, **Applied by**, and **Applied date**.

Figure 11-35: Applied Devices Page



Configlets

Manage configlets and view configlet details.

Configlets > SYS_TelemetryBuilderV3_2_with_cv-st...

SYS_TelemetryBuilderV3_2_with_cv-staging

Host Name	IP Address	Container Name	Applied By	Applied Date
cvp-lf-20.sjc.aristanetworks.com	10.90.165.20	Leaf-20-21	cvpuser	2020-07-30 15:16:30
cvp-lf-21.sjc.aristanetworks.com	10.90.165.21	Leaf-20-21	cvpuser	2020-08-03 11:54:32
cvp-lf-22.sjc.aristanetworks.com	10.90.165.22	Leaf-22-23	cvpuser	2020-08-03 10:40:26
cvp-lf-23.sjc.aristanetworks.com	10.90.165.23	Leaf-22-23	cvpuser	2020-08-03 10:41:35

1 - 4 of 4 1 of 1

When a Configlet is removed from any device through the Network Provisioning module, the device will be removed from the list.

Related topics:

- Editing Configlets
- Deleting Configlets
- Importing and Exporting Configlets
- Creating Configlets

11.3 Editing Configlets

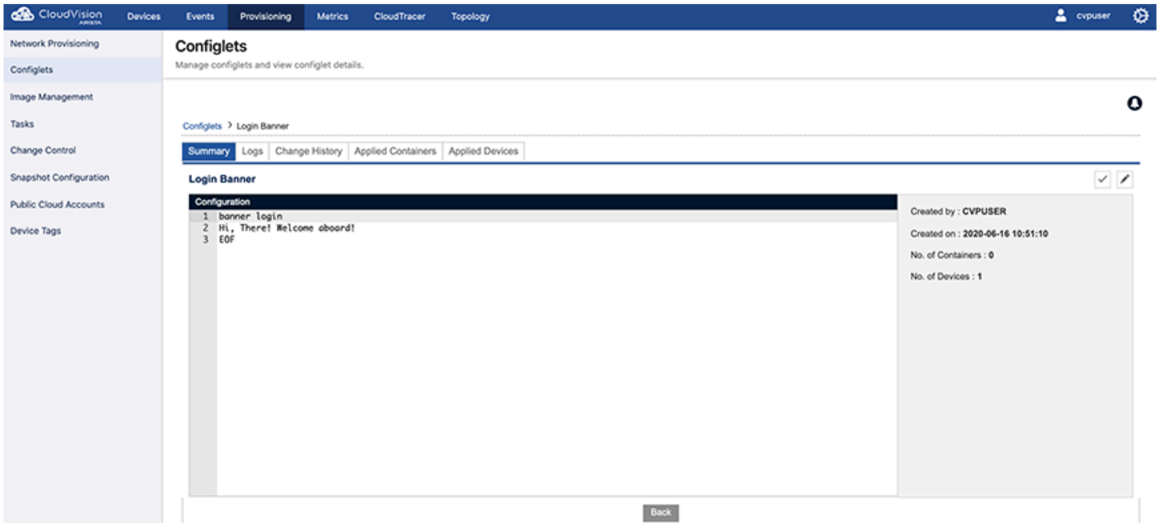
You edit Configlets through the Configlet “Summary” page. When you save the edited Configlet, it will update the all the associated tasks and devices in CloudVision.

- Configuration assign tasks which are waiting to be executed in task management that are using the edited Configlet are considered as associated tasks.
- Saving the edited Configlet affects all the associated tasks as follows:

Pending tasks:	Tasks in pending state are auto updated. The spawned configuration points to the updated Configlet.
Failed tasks:	Tasks in a failed state are auto canceled. A new configuration push task is spawned.
Save As:	The edited Configlet can be saved as a new Configlet. Give the new Configlet a unique name.

1. Select the **Edit** (pen) icon in the page.

Figure 11-36: Configlet Summary Page



```
banner login
Hi, There! Welcome aboard!
EOF
```

Created by : **CVPUSER**

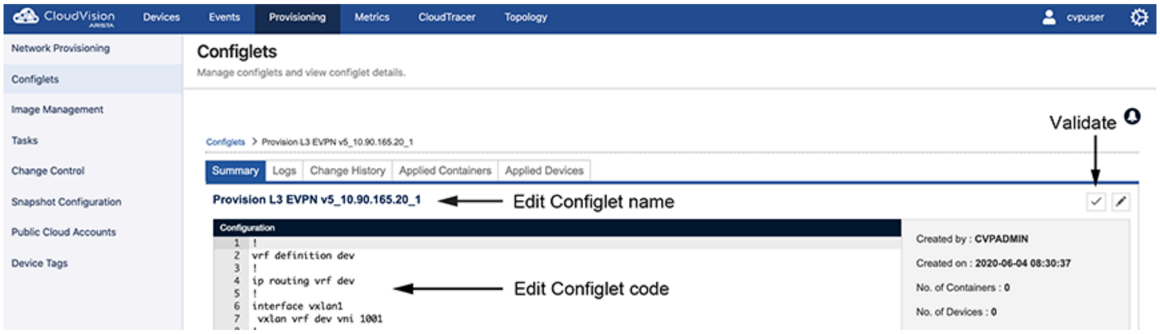
Created on : **2020-06-16 10:51:10**

No. of Containers : **0**

No. of Devices : **1**

2. Validate the Configlet with the **Validation** pane.

Figure 11-37: Edit Configlet Summary



Validate

Edit Configlet name

Edit Configlet code

```
!
vrf definition dev
!
ip routing vrf dev
!
interface vxlan1
 vxlan vrf dev vni 1001
```

Created by : **CVPADMIN**

Created on : **2020-06-04 08:30:37**

No. of Containers : **0**

No. of Devices : **0**

3. Do one of the following:

- Click **Save** to save the edited configlet.
- Click **Save As** to save the edited configlet as a new Configlet (the name Configlet).

Related topics:

- Deleting Configlets
- Importing and Exporting Configlets
- Creating Configlets
- Configlet Information Page

11.4 Tips for Applying Profiles to the Interfaces

When interface profiles are added to configlets, the user should ensure the interface profiles are first applied to all the interfaces, and only after that the interface profile is completed.

Apply empty profiles to the interface first and then fill out the profile. The commands should look similar to the following:

~~~
```
interface et1-49
profile test
!
interface profile test
command description test
```
~~~

Note: If the profile is created first and then applied to the interfaces, the config validation and commit can take several minutes as opposed to just a few seconds if the profile is first applied and then created.

11.5 Deleting Configlets

Only unused Configlets can be deleted. If a Configlet is assigned to a device or a container, it cannot be deleted from the inventory. To delete a specific Configlet, its association should be removed from the devices and container.

1. Select a Configlet in the grid. A “trash can” icon will appear.
2. Click the **Trash** icon to delete the Configlet.

   Related topics:

   - Importing and Exporting Configlets
   - Creating Configlets
   - Configlet Information Page
   - Editing Configlets

11.6 Importing and Exporting Configlets

You can import and export Configlets using the CloudVision graphical user interface (GUI). This enables you to easily share Configlets with others and back up specific Configlets.

For Configlets shared with you by another system user, you import Configlets from your desktop. When you share Configlets with another system user, you export Configlets to your desktop. You use the Configlets page to import and export Configlets or Configlet Builders.

Note: Both Configlets and Configlet Builders can be imported and exported using the GUI.

For more information, see:

- Protection from Overwriting Configlets or Configlet Builders
- Importing Configlets or Configlet Builders
- Exporting Configlets or Configlet Builders

11.6.1 Protection from Overwriting Configlets or Configlet Builders

CloudVision provides protection from accidentally overwriting exiting Configlets or Configlet Builders when importing a Configlet or Configlet Builder.

If you import a file that contains one or more Configlets or Configlet Builders that are named the same as Configlets or Configlet Builders already in CVP, the system automatically adds a suffix to the names of the items you are importing. The suffix that is added is in the format of “<number>”.

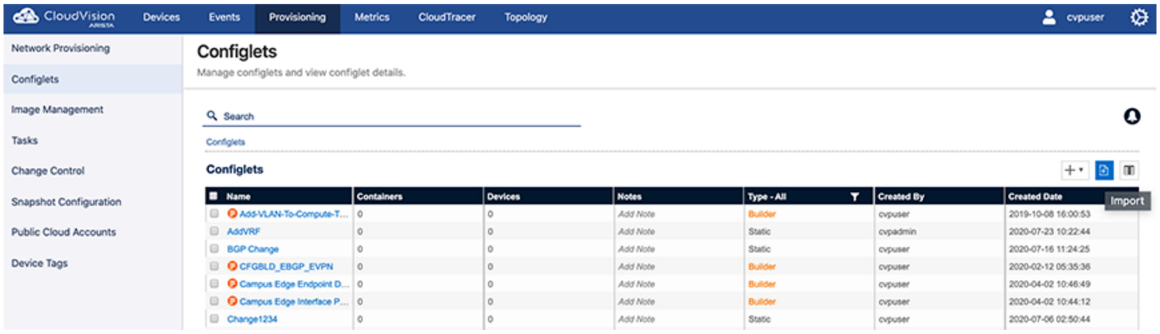
11.6.2 Importing Configlets or Configlet Builders

You import Configlets or Configlet Builders into CVP when another system user has shared a Configlet or Configlet Builder with you. Once you import Configlets or Configlet Builders, the imported items are available for use in CVP. You import Configlets or Configlet Builders from your desktop using the Configlets page.

Complete the following steps to import Configlets or Configlet Builders.

1. Open the Configlets page.
2. Click the Import icon, located in the upper right of the page.

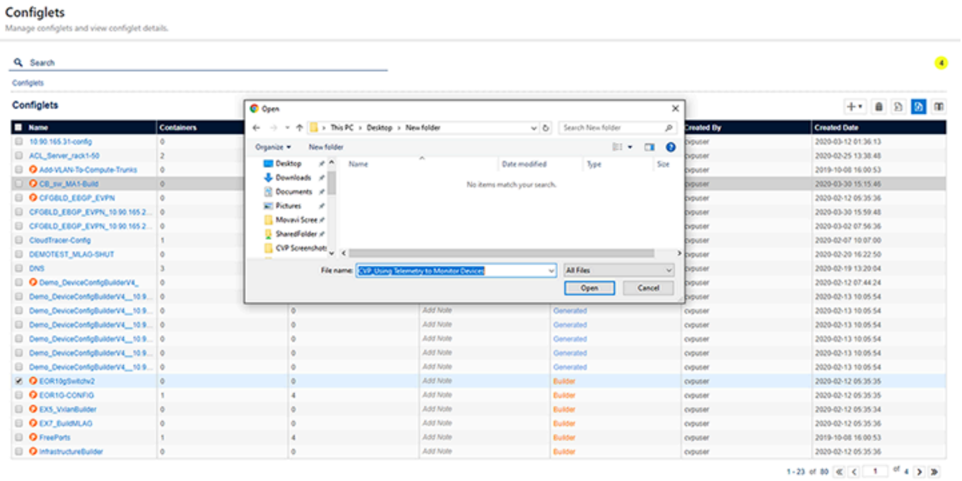
Figure 11-38: Configlets Page Showing Import Icon



☐	Name	Containers	Devices	Notes	Type - All	Created By	Created Date
☐	Add-VLAN-To-Compute-T...	0	0	Add Note	Builder	cvpuser	2019-10-08 16:00:53
☐	AddVRF	0	0	Add Note	Static	cvpadmin	2020-07-23 10:22:44
☐	BGP Change	0	0	Add Note	Static	cvpuser	2020-07-16 11:24:25
☐	CFGBLD_EBGP_EVPN	0	0	Add Note	Builder	cvpuser	2020-02-12 05:35:36
☐	Campus Edge Endpoint D...	0	0	Add Note	Builder	cvpuser	2020-04-02 10:46:49
☐	Campus Edge Interface P...	0	0	Add Note	Builder	cvpuser	2020-04-02 10:44:12
☐	Change1234	0	0	Add Note	Static	cvpuser	2020-07-06 02:50:44

A dialog appears that you use to select the file that contains the Configlets or Configlet Builders you want to import.

Figure 11-39: Selecting Configlets or Configlet Builders to be Imported



☐	Name	Containers				Created By	Created Date
☐	10.90.165.31-config	0				cvpuser	2020-03-12 01:36:13
☐	ACL_Server_rack1-50	2				cvpuser	2020-02-25 13:38:48
☐	Add-VLAN-To-Compute-Trunks	0				cvpuser	2019-10-08 16:00:53
☐	CB_sw_MA1-Build	0				cvpuser	2020-03-30 15:15:46
☐	CFGBLD_EBGP_EVPN	0				cvpuser	2020-02-12 05:35:36
☐	CFGBLD_EBGP_EVPN_10.90.165.2...	0				cvpuser	2020-03-30 15:59:48
☐	CFGBLD_EBGP_EVPN_10.90.165.2...	0				cvpuser	2020-03-02 07:56:36
☐	CloudTracer-Config	1				cvpuser	2020-02-07 10:07:00
☐	DEMOTEST_MLAG-SHUT	0				cvpuser	2020-02-20 16:22:50
☐	DNS	3				cvpuser	2020-02-19 13:20:04
☐	Demo_DeviceConfigBuilderV4_	0				cvpuser	2020-02-12 07:44:24
☐	Demo_DeviceConfigBuilderV4__10.9...	0				cvpuser	2020-02-13 10:05:54
☐	Demo_DeviceConfigBuilderV4__10.9...	0	0	Add Note	Generated	cvpuser	2020-02-13 10:05:54
☐	Demo_DeviceConfigBuilderV4__10.9...	0	0	Add Note	Generated	cvpuser	2020-02-13 10:05:54
☐	Demo_DeviceConfigBuilderV4__10.9...	0	0	Add Note	Generated	cvpuser	2020-02-13 10:05:54
☐	Demo_DeviceConfigBuilderV4__10.9...	0	0	Add Note	Generated	cvpuser	2020-02-13 10:05:54
☐	Demo_DeviceConfigBuilderV4__10.9...	0	0	Add Note	Generated	cvpuser	2020-02-13 10:05:54
☑	EOR10gSwitchv2	0	0	Add Note	Builder	cvpuser	2020-02-12 05:35:35
☐	EOR10-CONFIG	1	4	Add Note	Builder	cvpuser	2020-02-12 05:35:35
☐	EX5_VxlanBuilder	0	0	Add Note	Builder	cvpuser	2020-02-12 05:35:34
☐	EX7_BuildMLAG	0	0	Add Note	Builder	cvpuser	2020-02-12 05:35:36
☐	FreePorts	1	4	Add Note	Builder	cvpuser	2019-10-08 16:00:53
☐	InfrastructureBuilder	0	0	Add Note	Builder	cvpuser	2020-02-12 05:35:36

3. Select the file that contains the items you want to import.
4. Click **Open**.

The Configlets or Configlet Builders in the file you selected are imported into CVP.

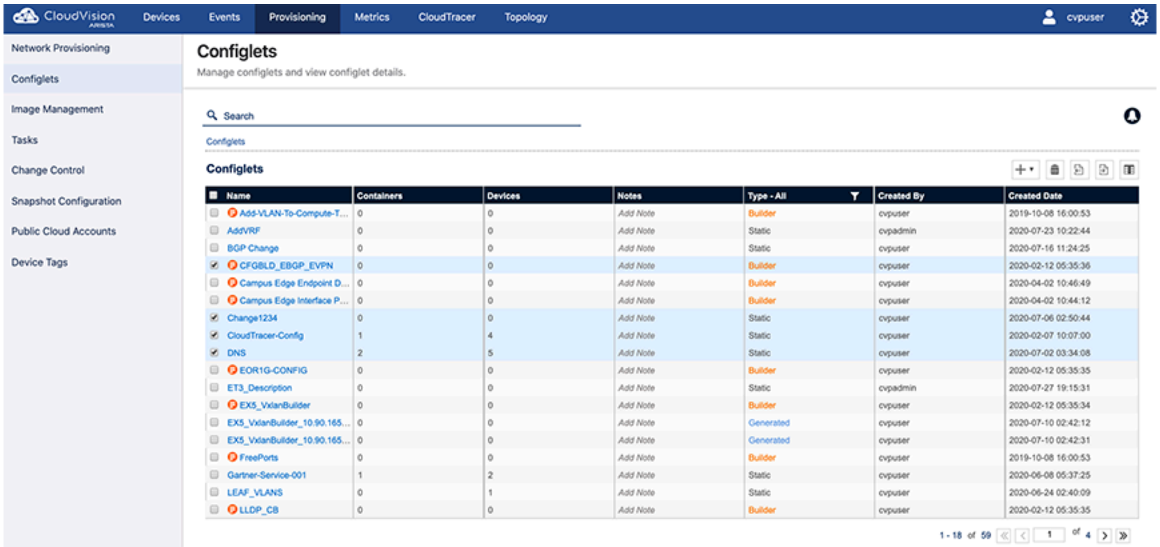
11.6.3 Exporting Configlets or Configlet Builders

You export Configlets or Configlet Builders when you want to share them with another system user. Once you export Configlets or Configlet Builders, the exported items are available to be sent to and then imported by the other system user. You export Configlets or Configlet Builders to your desktop using the Configlets page.

Complete the following steps to export Configlets or Configlet Builders.

1. Open the **Configlets** page.
2. Select the checkbox of each Configlet and Configlet Builder you want to export.

Figure 11-40: Configlets Page Showing Items Selected to be Exported



Configlets

Manage configlets and view configlet details.

Search

Configlets

Configlets

☐	Name	Containers	Devices	Notes	Type - All	Created By	Created Date
☐	Add-VLAN-To-Compute-T...	0	0	Add Note	Builder	cvpuser	2019-10-08 16:00:53
☐	AddVRF	0	0	Add Note	Static	cvpadmin	2020-07-23 10:22:44
☐	BGP Change	0	0	Add Note	Static	cvpuser	2020-07-16 11:24:25
☑	CFGBLD_EBGP_EVPN	0	0	Add Note	Builder	cvpuser	2020-02-12 05:35:36
☐	Campus Edge Endpoint D...	0	0	Add Note	Builder	cvpuser	2020-04-02 10:46:49
☐	Campus Edge Interface P...	0	0	Add Note	Builder	cvpuser	2020-04-02 10:44:12
☑	Change1234	0	0	Add Note	Static	cvpuser	2020-07-06 02:50:44
☑	CloudTracer-Config	1	4	Add Note	Static	cvpuser	2020-02-07 10:07:00
☑	DNS	2	5	Add Note	Static	cvpuser	2020-07-02 03:34:08
☐	EOR1G-CONFIG	0	0	Add Note	Builder	cvpuser	2020-02-12 05:35:35
☐	ET3_Description	0	0	Add Note	Static	cvpadmin	2020-07-27 19:15:31
☐	EX5_VxlanBuilder	0	0	Add Note	Builder	cvpuser	2020-02-12 05:35:34
☐	EX5_VxlanBuilder_10.90.165...	0	0	Add Note	Generated	cvpuser	2020-07-10 02:42:12
☐	EX5_VxlanBuilder_10.90.165...	0	0	Add Note	Generated	cvpuser	2020-07-10 02:42:31
☐	FreePorts	0	0	Add Note	Builder	cvpuser	2019-10-08 16:00:53
☐	Gartner-Service-001	1	2	Add Note	Static	cvpuser	2020-06-08 05:37:25
☐	LEAF_VLANS	0	1	Add Note	Static	cvpuser	2020-06-24 02:40:09
☐	LLDP_CB	0	0	Add Note	Builder	cvpuser	2020-02-12 05:35:35

1 - 18 of 59 « ‹ 1 of 4 › »

3. Click the **Export** icon (located in the upper right of the page).

   A single file (.zip archive) that contains all of the items you selected is automatically downloaded to your desktop.
4. (Optional) You can rename the downloaded file and make a copy of it before sharing it.
5. Share the file with one or more system users.

   Note: The items you share can be imported only on systems that support the import of Configlets and Configlet Builders (the Import icon on the Configlets page indicates support for this feature).

Related topics:

- Creating Configlets
- Configlet Information Page
- Editing Configlets
- Deleting Configlets

Chapter 12

Image Management (CVP)

The Extensible Operating System (EOS) used by the switches are uploaded into CloudVision, and details about them are maintained in the Image Management Inventory.

The main purpose of the Image Management module is to enable you to manage the EOS operating system images across the devices in your current CloudVision environment. It provides you with the functionality required to:

- Validate images
- Upload EOS images to CloudVision
- Maintain the inventory of available EOS images
- Assign images to devices in your CloudVision environment

Sections in this chapter include:

- Image Management Page
- Validating Images
- Upgrading Extensible Operating System (EOS) Images
- Creating Image Bundles
- The Bundle Information Page

12.1 Image Management Page

The Image Management page shows the current operating system images that are available for upload to CloudVision. Once uploaded, they can be assigned to devices.

You can navigate to the Image Management page through Provisioning > Image Management.

Figure 12-1: Image Management page

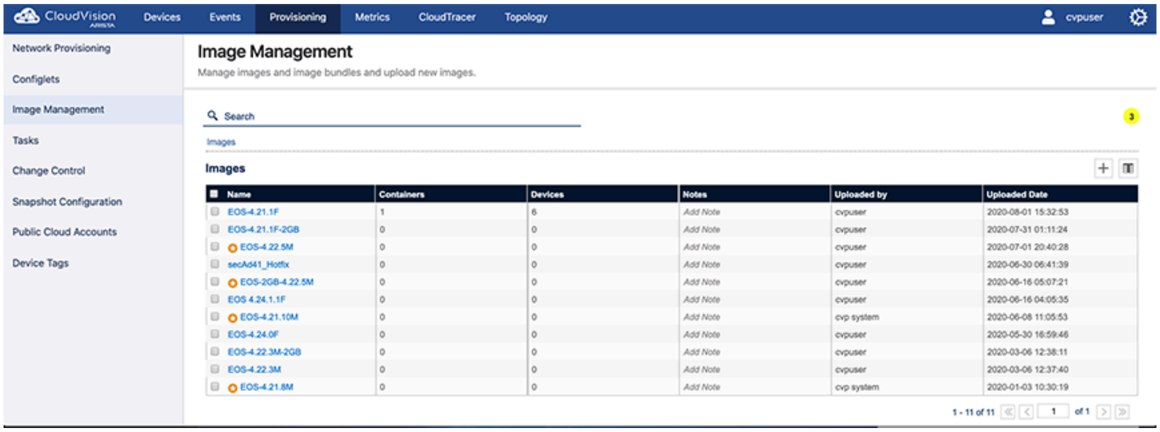


Image Management

Manage images and image bundles and upload new images.

Images

Name	Containers	Devices	Notes	Uploaded by	Uploaded Date
EOS-4.21.1F	1	6	*Add Note*	cvpuser	2020-08-01 15:32:53
EOS-4.21.1F-2GB	0	0	*Add Note*	cvpuser	2020-07-31 01:11:24
EOS-4.22.5M	0	0	*Add Note*	cvpuser	2020-07-01 20:40:28
secAd41_Hotfix	0	0	*Add Note*	cvpuser	2020-06-30 06:41:39
EOS-2GB-4.22.5M	0	0	*Add Note*	cvpuser	2020-06-16 05:07:21
EOS 4.24.1.1F	0	0	*Add Note*	cvpuser	2020-06-16 04:05:35
EOS-4.21.10M	0	0	*Add Note*	cvp system	2020-06-08 11:05:53
EOS-4.24.0F	0	0	*Add Note*	cvpuser	2020-05-30 16:59:46
EOS-4.22.3M-2GB	0	0	*Add Note*	cvpuser	2020-03-06 12:38:11
EOS-4.22.3M	0	0	*Add Note*	cvpuser	2020-03-06 12:37:40
EOS-4.21.8M	0	0	*Add Note*	cvp system	2020-01-03 10:30:19

1 - 11 of 11 « ‹ 1 of 1 › »

Related topics:

- Validating Images
- Upgrading Extensible Operating System (EOS) Images
- Creating Image Bundles
- The Bundle Information Page

12.2 Validating Images

CloudVision Portal (CVP) provides automatic EOS image validation. This automated validation process helps to ensure that all devices in your CVP environment have EOS images that are supported by CVP.

The automatic validation of EOS images takes place whenever you:

- Upload images to CVP or add images to images bundles.
- Add devices to your CVP environment.

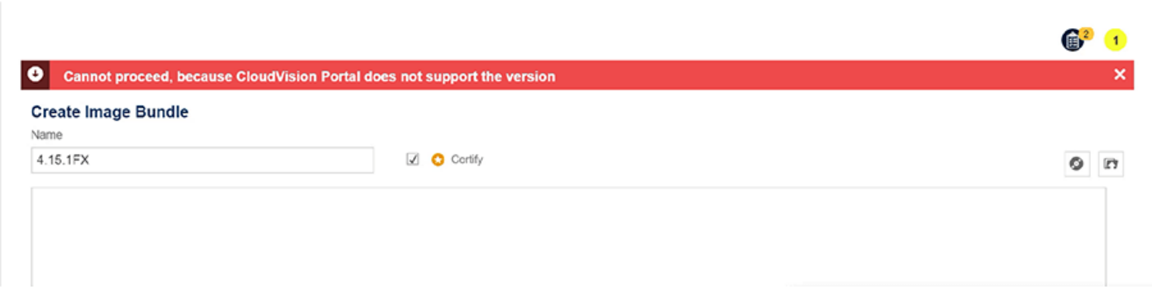
The automatic image validation ensures that images that are available to be included in image bundles and assigned to devices are supported by CVP.

Note: EOS images that are not supported cannot be added to an image bundle, or assigned to devices.

12.2.1 Alerts Indicating Unsupported EOS Image Versions

If you attempt to include an unsupported version of an EOS image when creating an image bundle, CVP alerts you with an error to let you know that the upload cannot be done, because the version of the EOS image you are trying to upload is not supported.

Figure 12-2: Alerts



Cannot proceed, because CloudVision Portal does not support the version

Create Image Bundle

Name

4.15.1FX

☑ Certify

If you attempt to add a device to CVP that has an unsupported EOS image, the Status column of the Inventory page indicates that an upgrade is required.

The Network Provisioning page also indicate that the device is running an unsupported image (this alert shows only when placing your cursor over the device icon).

Related topics:

- Upgrading Extensible Operating System (EOS) Images
- Creating Image Bundles
- The Bundle Information Page
- Image Management Page

12.3 Upgrading Extensible Operating System (EOS) Images

CloudVision Portal (CVP) provides the functionality to upgrade the EOS image on a device. Typically, you upgrade the image on a device to change the version of the image from an unsupported image version to a supported image version.

You upgrade device images by associating an EOS image with a device or a container (the association is referred to as an image association). Image associations follow the same container inheritance rules as configlet associations. This means that the image you select to be associated is automatically inherited (assigned) to all devices under the level in the hierarchy at which you associate the image.

Note: When performing an image push, CloudVision checks if the target EOS image is already present on flash. If the `.swi` file is available, CloudVision uses the same file instead of downloading a new image from the network. This reduces network costs and time incurred during image upgrades.

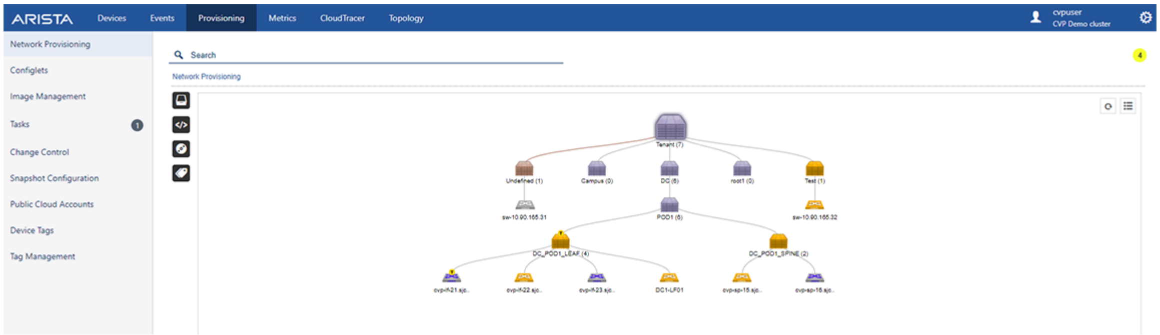
For more information, see:

- Example of Image Association
- Tip for Handling Multiple Image Association Tasks

12.3.1 Example of Image Association

This example shows the behavior of image associations in a multi-level network hierarchy. The hierarchy in this example contains a tenant container named Demo-Lab. The Demo-Lab container has five child containers named CVX, Host-TOR1, Leaf, Spine, and TOR2.

Figure 12-3: Same Task Scheduled for Every Device in CVX Container



Based on the rules for image association inheritance, the Demo-Lab container could have selected the *4.18.8M* device EOS image.

Figure 12-4: Example of image Association (Example 1)

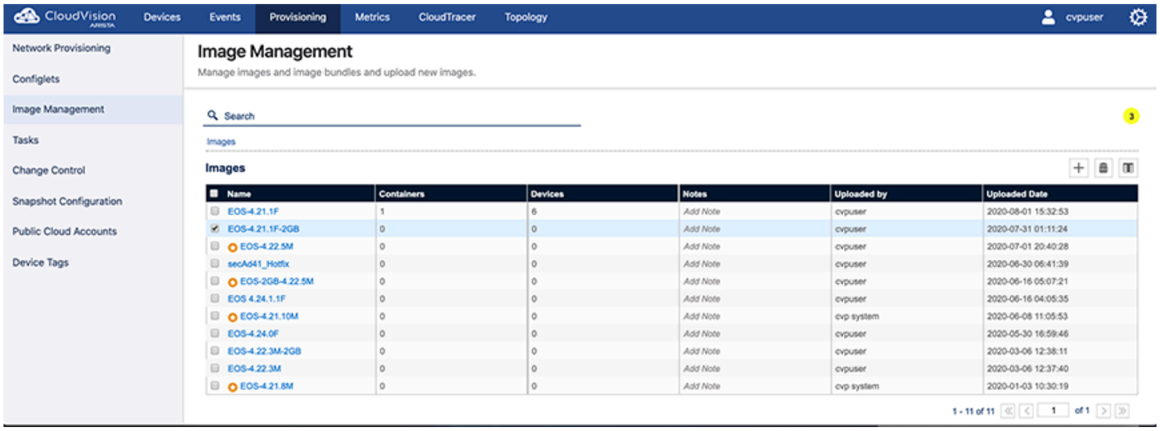


Image Management

Manage images and image bundles and upload new images.

Images

□	Name	Containers	Devices	Notes	Uploaded by	Uploaded Date
□	EOS-4.21.1F	1	6	Add Note	cvpuser	2020-08-01 15:32:53
☑	EOS-4.21.1F-2GB	0	0	Add Note	cvpuser	2020-07-31 01:11:24
□	○ EOS-4.22.5M	0	0	Add Note	cvpuser	2020-07-01 20:40:28
□	secAd41_Hotfix	0	0	Add Note	cvpuser	2020-06-30 06:41:39
□	○ EOS-2GB-4.22.5M	0	0	Add Note	cvpuser	2020-06-16 05:07:21
□	EOS 4.24.1.1F	0	0	Add Note	cvpuser	2020-06-16 04:05:35
□	○ EOS-4.21.10M	0	0	Add Note	cvp system	2020-06-08 11:05:53
□	EOS-4.24.0F	0	0	Add Note	cvpuser	2020-05-30 16:59:46
□	EOS-4.22.3M-2GB	0	0	Add Note	cvpuser	2020-03-06 12:38:11
□	EOS-4.22.3M	0	0	Add Note	cvpuser	2020-03-06 12:37:40
□	○ EOS-4.21.8M	0	0	Add Note	cvp system	2020-01-03 10:30:19

1 - 11 of 11 1 of 1

The CVX container could override that image selection (*4.18.8M* image) for its devices by selecting the *4.20.7M* image. As a result, all of the devices under CVX are assigned the *4.20.7M* image, and the devices under Host-TOR1, Leaf, Spine and TOR2 inherit the *4.18.8M* image from the Demo-Lab container.

Figure 12-5: Example of Image Association (Example 2)

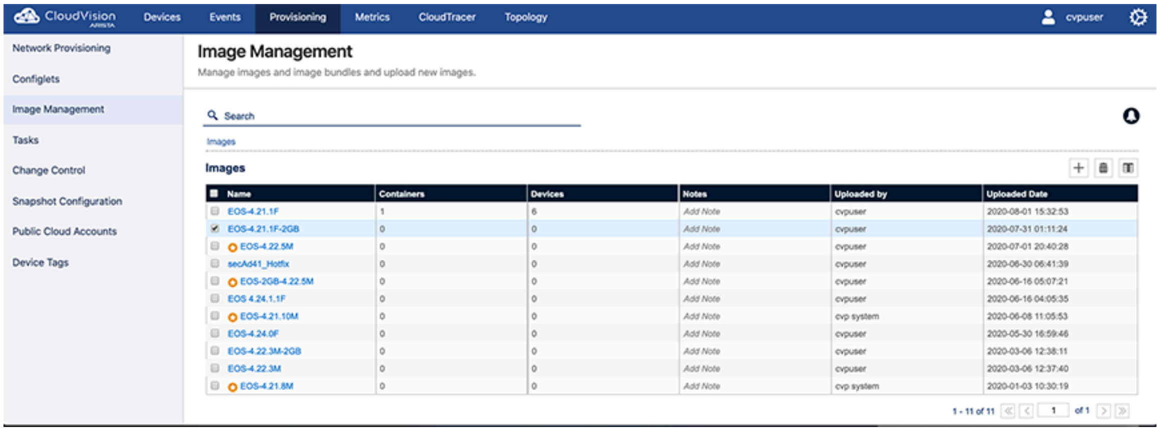


Image Management

Manage images and image bundles and upload new images.

Images

☐ Name	Containers	Devices	Notes	Uploaded by	Uploaded Date
☐ EOS-4.21.1F	1	6	Add Note	cvpuser	2020-08-01 15:32:53
☑ EOS-4.21.1F-2GB	0	0	Add Note	cvpuser	2020-07-31 01:11:24
☐ ○ EOS-4.22.5M	0	0	Add Note	cvpuser	2020-07-01 20:40:28
☐ secAd41_Hotfix	0	0	Add Note	cvpuser	2020-06-30 06:41:39
☐ ○ EOS-2GB-4.22.5M	0	0	Add Note	cvpuser	2020-06-16 05:07:21
☐ EOS 4.24.1.1F	0	0	Add Note	cvpuser	2020-06-16 04:05:35
☐ ○ EOS-4.21.10M	0	0	Add Note	cvp system	2020-06-08 11:05:53
☐ EOS-4.24.0F	0	0	Add Note	cvpuser	2020-05-30 16:59:46
☐ EOS-4.22.3M-2GB	0	0	Add Note	cvpuser	2020-03-06 12:38:11
☐ EOS-4.22.3M	0	0	Add Note	cvpuser	2020-03-06 12:37:40
☐ ○ EOS-4.21.8M	0	0	Add Note	cvp system	2020-01-03 10:30:19

1 - 11 of 11   1   of 1

If an image association is changed at any level, and the change is saved in the **Network Provisioning** page, the following occurs:

- The change impacts all devices under that level.
- A task is automatically created to upgrade the impacted devices.

For example, if the image selection was removed at the CVX level, the following would occur:

- All of the devices under the CVX level would inherit the Demo-Lab image.
- A task would be scheduled for every device in CVX to use the Demo-Lab image.

Related topics:

- Tip for Handling Multiple Image Association Tasks
- Creating Image Bundles
- The Bundle Information Page
- Image Management Page
- Validating Images

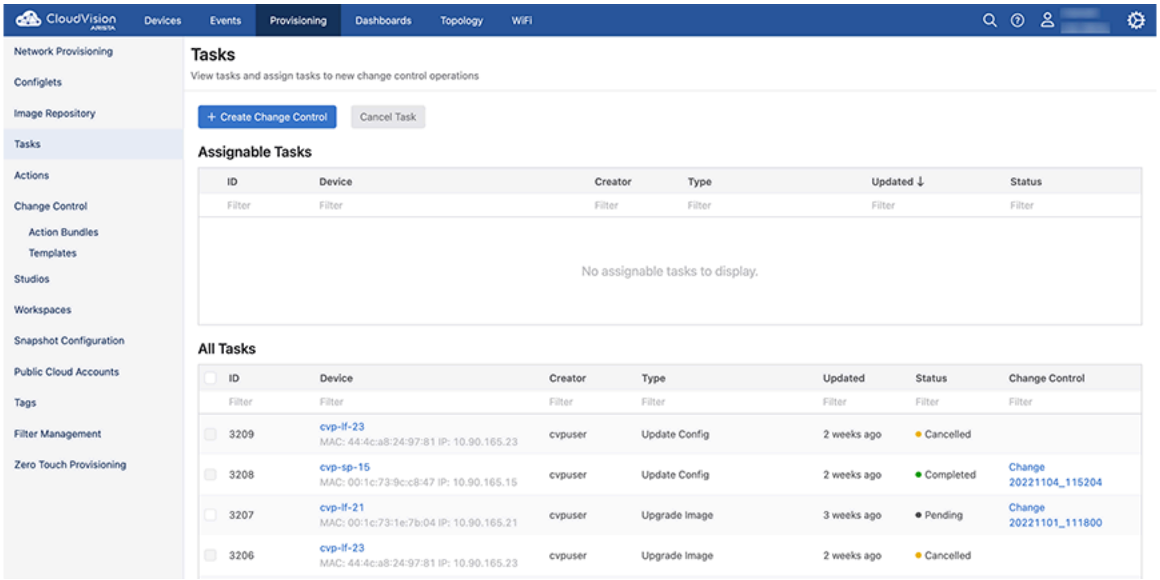
12.3.2 Tip for Handling Multiple Image Association Tasks

When several image association tasks are scheduled to be completed, use the following steps to execute the tasks. These steps help you to execute the tasks more efficiently.

1. Search for **Pending** in the Tasks page to find the tasks to be executed (status is “Pending”).
2. Select them all by clicking the checkbox next to the Task ID heading.

If the search results returns multiple pages of tasks, then click the checkbox at the top of each page to select the tasks so they can be executed.

Figure 12-6: Selecting Multiple Tasks to be Executed



Tasks

View tasks and assign tasks to new change control operations

Assignable Tasks

ID	Device	Creator	Type	Updated ↓	Status
Filter	Filter	Filter	Filter	Filter	Filter

No assignable tasks to display.

All Tasks

□	ID	Device	Creator	Type	Updated	Status	Change Control
	Filter	Filter	Filter	Filter	Filter	Filter	Filter
□	3209	cvp-lf-23 MAC: 44:4c:a8:24:97:81 IP: 10.90.165.23	cvpuser	Update Config	2 weeks ago	● Cancelled	
□	3208	cvp-sp-15 MAC: 00:1c:73:9c:c8:47 IP: 10.90.165.15	cvpuser	Update Config	2 weeks ago	● Completed	Change 20221104_115204
□	3207	cvp-lf-21 MAC: 00:1c:73:1e:7b:04 IP: 10.90.165.21	cvpuser	Upgrade Image	3 weeks ago	● Pending	Change 20221101_111800
□	3206	cvp-lf-23 MAC: 44:4c:a8:24:97:81 IP: 10.90.165.23	cvpuser	Upgrade Image	2 weeks ago	● Cancelled	

3. Click the **Play** icon to execute the selected tasks all at once.

Related topics:

- Creating Image Bundles
- The Bundle Information Page
- Image Management Page
- Validating Images
- Example of Image Association

12.4 Creating Image Bundles

Creating image bundles is a key image management task. You create image bundles so that you have supported image versions available to be assigned to devices in your CVP environment.

Note: An image bundle must have one `.swi` file. Extensions are optional (not required for image bundles), but you can add one or more extensions to an image bundle.

Pre-requisite: To ensure that you include valid (supported) EOS images in the bundles you create, make sure you validate the images you want to include in the bundle (see Validating Images).

Complete the following steps to create an image bundle:

1. Go to the **Image Management** page.
2. Click the "**+**" icon in the grid.

This loads the **Create Image Bundle** page.

Figure 12-7: Create Image Bundle page

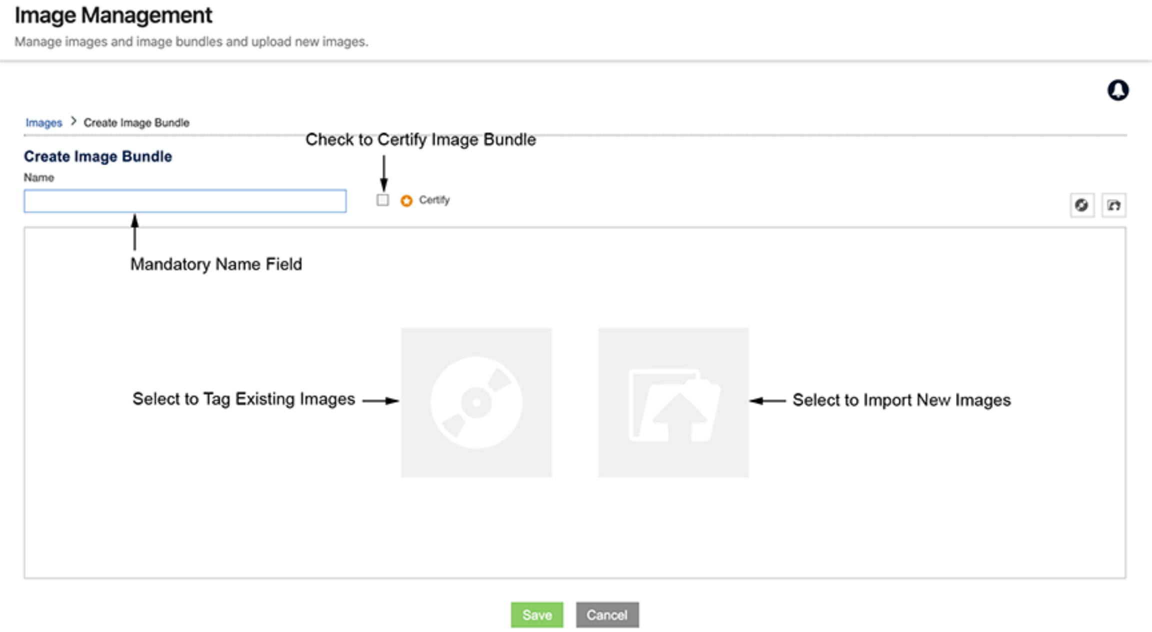


Image Management
Manage images and image bundles and upload new images.
Images > Create Image Bundle
Create Image Bundle
Name
Check to Certify Image Bundle
Certify
Mandatory Name Field
Select to Tag Existing Images
Select to Import New Images
Save
Cancel

For more information, see:

- Creating a Bundle by Tagging Existing Image Bundles
- Creating a Bundle by Uploading a New Image
- Adding EOS Extensions to Image Bundles

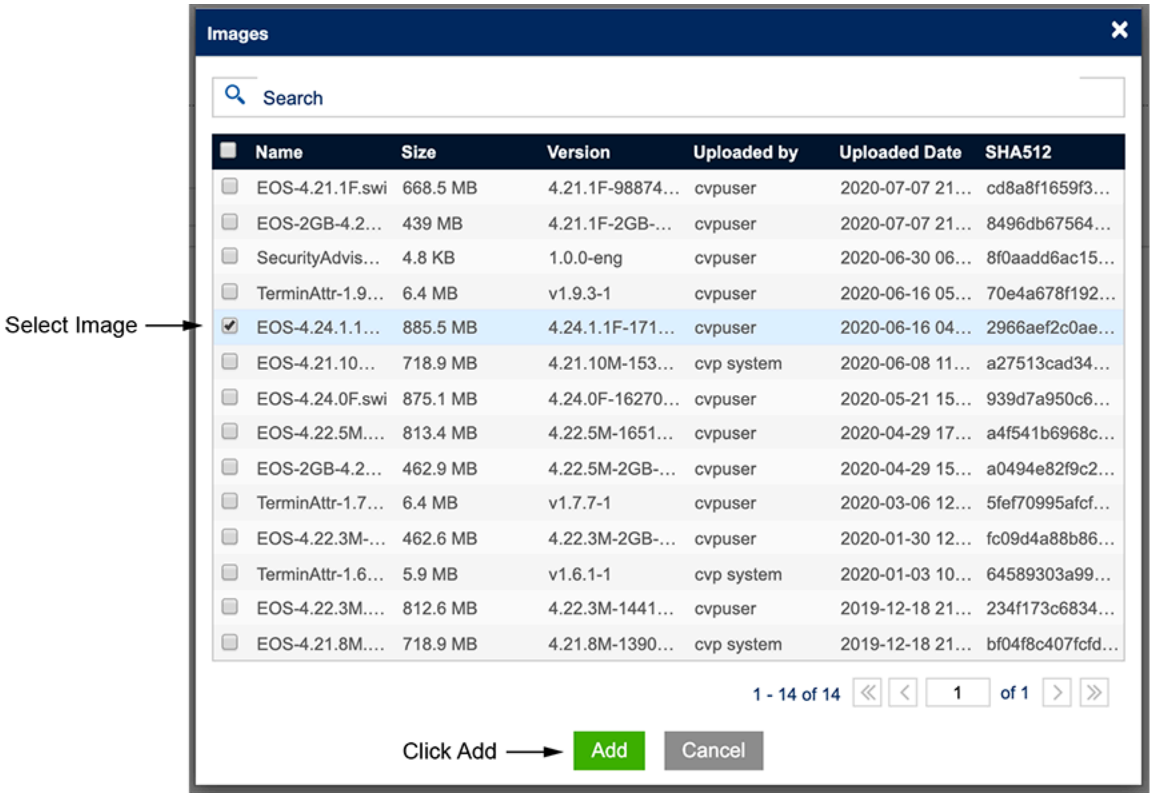
12.4.1 Creating a Bundle by Tagging Existing Image Bundles

CloudVision Portal (CVP) enables you to create a new image bundle by tagging existing image bundles. This prevents you from having to import the same image again to create another bundle.

1. Go to the **Image Management** page.
2. Click the “**+**” icon and then the Disk icon.

1. This opens the Images dialog, which lists all of the available images.

Figure 12-8: Images dialog



☐	Name	Size	Version	Uploaded by	Uploaded Date	SHA512
☐	EOS-4.21.1F.swi	668.5 MB	4.21.1F-98874...	cvpuser	2020-07-07 21...	cd8a8f1659f3...
☐	EOS-2GB-4.2...	439 MB	4.21.1F-2GB-...	cvpuser	2020-07-07 21...	8496db67564...
☐	SecurityAdvis...	4.8 KB	1.0.0-eng	cvpuser	2020-06-30 06...	8f0aadd6ac15...
☐	TerminAttr-1.9...	6.4 MB	v1.9.3-1	cvpuser	2020-06-16 05...	70e4a678f192...
☑	EOS-4.24.1.1...	885.5 MB	4.24.1.1F-171...	cvpuser	2020-06-16 04...	2966aef2c0ae...
☐	EOS-4.21.10...	718.9 MB	4.21.10M-153...	cvp system	2020-06-08 11...	a27513cad34...
☐	EOS-4.24.0F.swi	875.1 MB	4.24.0F-16270...	cvpuser	2020-05-21 15...	939d7a950c6...
☐	EOS-4.22.5M....	813.4 MB	4.22.5M-1651...	cvpuser	2020-04-29 17...	a4f541b6968c...
☐	EOS-2GB-4.2...	462.9 MB	4.22.5M-2GB-...	cvpuser	2020-04-29 15...	a0494e82f9c2...
☐	TerminAttr-1.7...	6.4 MB	v1.7.7-1	cvpuser	2020-03-06 12...	5fef70995afcf...
☐	EOS-4.22.3M-...	462.6 MB	4.22.3M-2GB-...	cvpuser	2020-01-30 12...	fc09d4a88b86...
☐	TerminAttr-1.6...	5.9 MB	v1.6.1-1	cvp system	2020-01-03 10...	64589303a99...
☐	EOS-4.22.3M....	812.6 MB	4.22.3M-1441...	cvpuser	2019-12-18 21...	234f173c6834...
☐	EOS-4.21.8M....	718.9 MB	4.21.8M-1390...	cvp system	2019-12-18 21...	bf04f8c407fcfd...

1 - 14 of 14 « ‹ 1 of 1 › »

3. Search for the desired image.
4. Select the image and click **Add** to add the image to the bundle.

   The image will be displayed in the grid of the **Create Image Bundle** page.

Figure 12-9: Added image shown in Create Image Bundle page

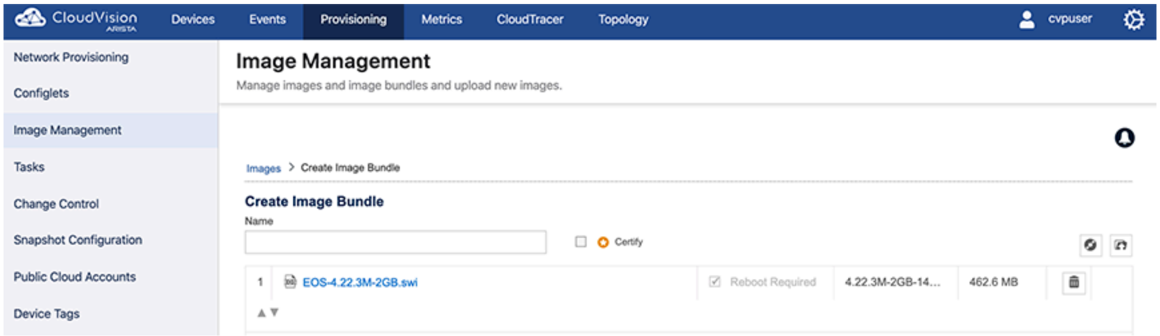


Image Management

Manage images and image bundles and upload new images.

Images > Create Image Bundle

Create Image Bundle

Name

☐ Certify

1	EOS-4.22.3M-2GB.swi	☑ Reboot Required	4.22.3M-2GB-14...	462.6 MB

5. Click **Save** to create the new image bundle.

Related topics:

- Creating a Bundle by Uploading a New Image
- Adding EOS Extensions to Image Bundles

12.4.2 Creating a Bundle by Uploading a New Image

CloudVision Portal (CVP) enables you to create new image bundles by uploading new images to CVP.

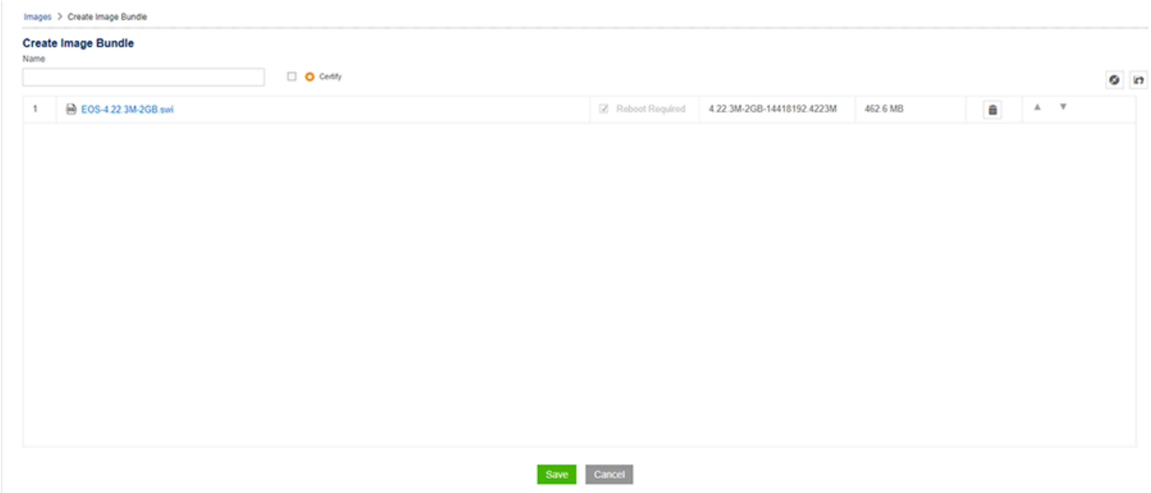
1. Go to the **Create Image Bundle** page.
2. Click the upload from local icon available next to disk icon.

This opens a dialog to search and upload .swi files from system.

3. Navigate to the desired .swi file and upload it to CVP.

   The upload bar on the page shows the progress of the upload.

   Figure 12-10: Uploading .swi files to CVP (upload in progress)



Images > Create Image Bundle

Create Image Bundle

Name

☐ ○ Certify

1	EOS-4.22.3M-2GB.swi	☑ Reboot Required	4.22.3M-2GB-14418192.4223M	462.6 MB		▲ ▼

4. Click **Save** to create the new image bundle.

12.4.3 Adding EOS Extensions to Image Bundles

CloudVision Portal (CVP) enables you to add EOS extensions to image bundles along with .swi images. Extensions are either .rpm files or .swix files. You upload .rpm or .swix files using the Images page. Extensions are optional for image bundles

Note: All selected extensions automatically checked to be installed and running on the device. The results are available for viewing under the **Compliance Overview** tab on **Devices** page.

Complete these steps to add EOS extensions to an image bundle:

1. Go to the **Create Image Bundle** page.
2. Click the upload from local icon.

   This opens a dialog to search and upload EOS extensions (.rpm or .swix files) from the system
3. Navigate to the desired .rpm or .swix files and upload them.

The upload bar on the page shows the progress of the upload. The extensions you uploaded are shown in the Create Image Bundle page

Figure 12-11: Create Image Bundle showing uploaded extensions

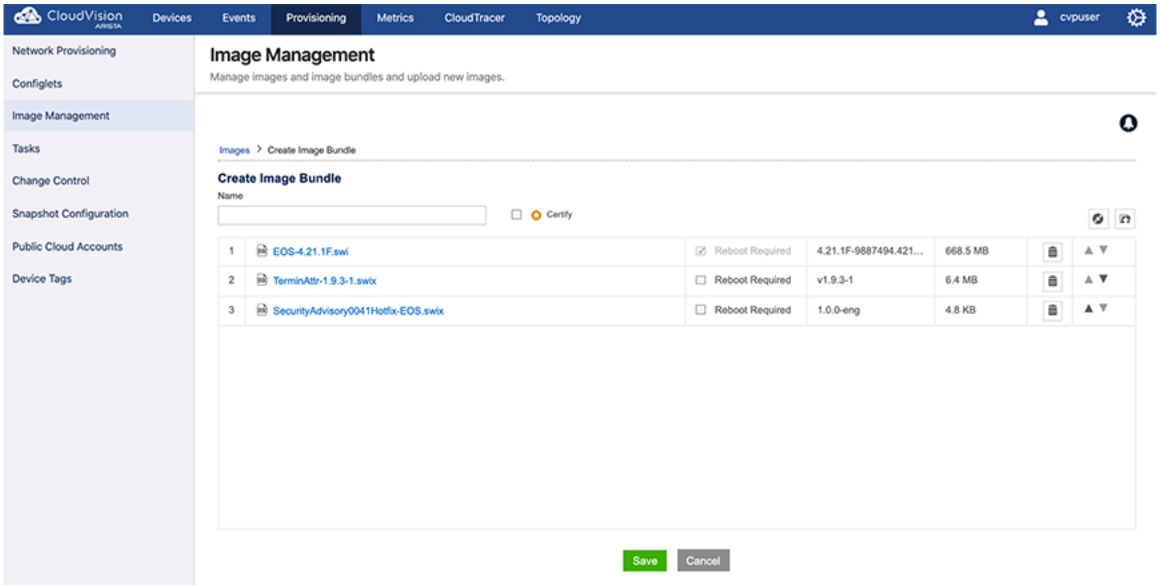


Image Management

Manage images and image bundles and upload new images.

Create Image Bundle

Name

□ Certify

1	EOS-4.21.1F.swi	☑ Reboot Required	4.21.1F-9887494.421...	668.5 MB
2	TerminAttr-1.9.3-1.swix	□ Reboot Required	v1.9.3-1	6.4 MB
3	SecurityAdvisory0041Hotfix-EOS.swix	□ Reboot Required	1.0.0-eng	4.8 KB

4. Select **Reboot Required** check-boxes for all extensions that require a reboot.
5. Click **Save**. The extensions are added to the image bundle.

   Once the image bundle is assigned to a device, a reboot task will be generated. The newly added extensions are installed on the device when the reboot task is executed. Any extensions that were previously installed but are not part of the current bundle are removed from the device.

12.5 The Bundle Information Page

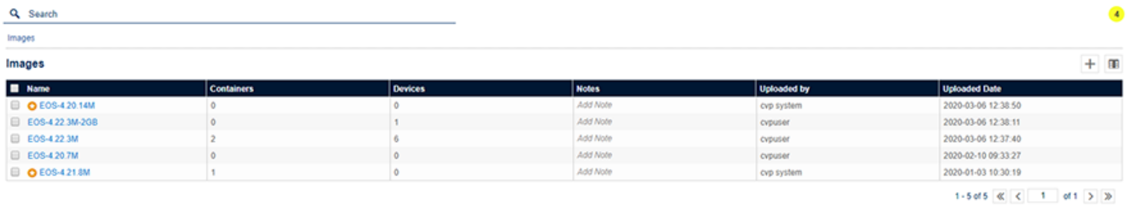
The Image Management page provides high-level information about an image bundle (for example, the number of containers to which an image bundle is associated, and the number of devices to which an image bundle is assigned).

To view more detailed information about image bundles, use the Bundle Information page, which you can open from the Image Management page.

Complete these steps to open the **Bundle Information** page.

1. Go to the **Image Management** page.
2. Click the name of image bundle for which you want to view information.

Figure 12-12: Opening the Bundle Information page



Images

Name	Containers	Devices	Notes	Uploaded by	Uploaded Date
EOS-4.20.14M	0	0	Add Note	cvp system	2020-03-06 12:38:50
EOS-4.22.3M-2GB	0	1	Add Note	cvpuser	2020-03-06 12:38:11
EOS-4.22.3M	2	6	Add Note	cvpuser	2020-03-06 12:37:40
EOS-4.20.7M	0	0	Add Note	cvpuser	2020-02-10 09:33:27
EOS-4.21.8M	1	0	Add Note	cvp system	2020-01-03 10:30:19

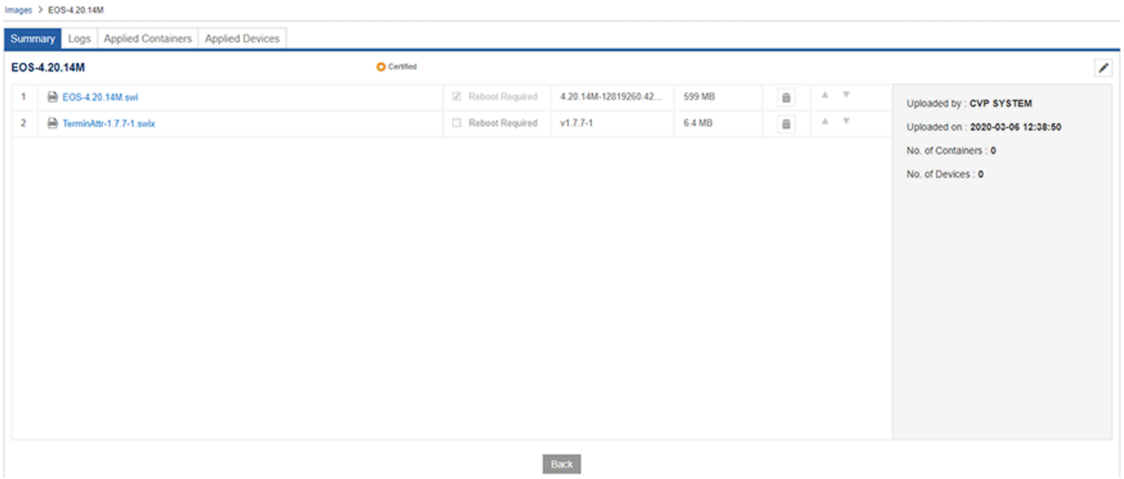
The **Bundle Information** page appears, showing information for the selected image bundle. Use the following tabs to view specific information about the selected image bundle.

- Summary Tab
- Logs Tab
- Applied Containers Tab
- Applied Devices Tab

12.5.1 Summary Tab

The Summary tab provides basic information about the Image Bundle. It also provides options to go back to the **Image Management** page, to open the dialog used to update image bundles, and to delete corresponding image bundle and its extensions.

Figure 12-13: Summary tab



EOS-4.20.14M

1	EOS-4.20.14M.swi	☑ Reboot Required	4.20.14M-12819260.42...	599 MB
2	TerminAttr-1.7.7-1.swix	□ Reboot Required	v1.7.7-1	6.4 MB

Uploaded by : **CVP SYSTEM**

Uploaded on : **2020-03-06 12:38:50**

No. of Containers : **0**

No. of Devices : **0**

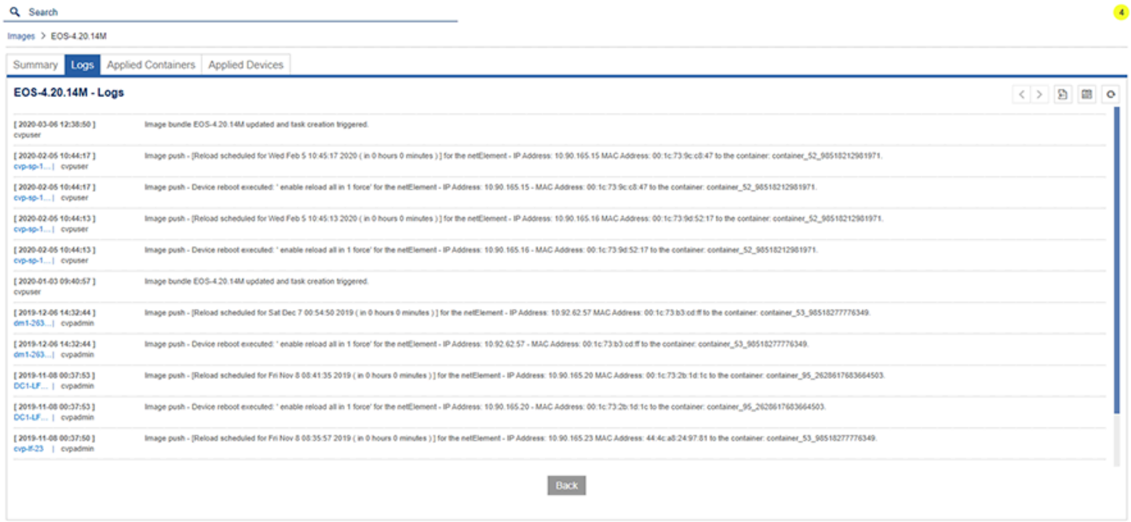
For details on the steps used to edit image bundles and delete image bundles, see:

- Updating Bundles
- Deleting Bundles

12.5.2 Logs Tab

The Logs tab provides complete information on the image assignment to devices and execution details. It also provides the option to go back to the **Image Management** page.

Figure 12-14: Logs tab



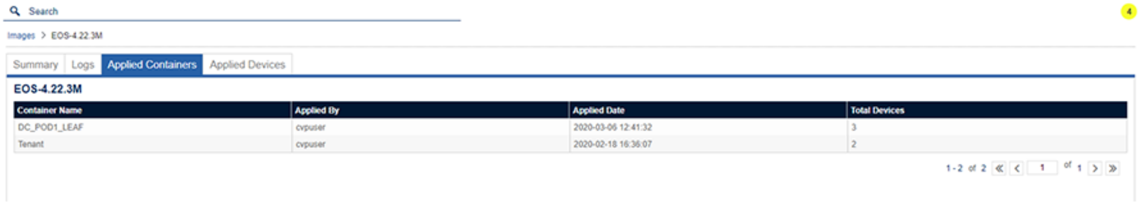
EOS-4.20.14M - Logs

```
[ 2020-03-06 12:38:50 ]      Image bundle EOS-4.20.14M updated and task creation triggered.
cvpuser
[ 2020-02-05 10:44:17 ]      Image push - [Reload scheduled for Wed Feb 5 10:45:17 2020 ( in 0 hours 0 minutes ) ] for the netElement - IP Address: 10.90.165.15 MAC Address: 00:1c:73:9c:c8:47 to the container: container_52_98518212981971.
cvp-sp-1... |  cvpuser
[ 2020-02-05 10:44:17 ]      Image push - Device reboot executed: ' enable reload all in 1 force' for the netElement - IP Address: 10.90.165.15 - MAC Address: 00:1c:73:9c:c8:47 to the container: container_52_98518212981971.
cvp-sp-1... |  cvpuser
[ 2020-02-05 10:44:13 ]      Image push - [Reload scheduled for Wed Feb 5 10:45:13 2020 ( in 0 hours 0 minutes ) ] for the netElement - IP Address: 10.90.165.16 MAC Address: 00:1c:73:9d:52:17 to the container: container_52_98518212981971.
cvp-sp-1... |  cvpuser
[ 2020-02-05 10:44:13 ]      Image push - Device reboot executed: ' enable reload all in 1 force' for the netElement - IP Address: 10.90.165.16 - MAC Address: 00:1c:73:9d:52:17 to the container: container_52_98518212981971.
cvp-sp-1... |  cvpuser
[ 2020-01-03 09:40:57 ]      Image bundle EOS-4.20.14M updated and task creation triggered.
cvpuser
[ 2019-12-06 14:32:44 ]      Image push - [Reload scheduled for Sat Dec 7 00:54:50 2019 ( in 0 hours 0 minutes ) ] for the netElement - IP Address: 10.92.62.57 MAC Address: 00:1c:73:b3:cd:ff to the container: container_53_98518277776349.
dm1-263... |  cvpadmin
[ 2019-12-06 14:32:44 ]      Image push - Device reboot executed: ' enable reload all in 1 force' for the netElement - IP Address: 10.92.62.57 - MAC Address: 00:1c:73:b3:cd:ff to the container: container_53_98518277776349.
dm1-263... |  cvpadmin
[ 2019-11-08 00:37:53 ]      Image push - [Reload scheduled for Fri Nov 8 08:41:35 2019 ( in 0 hours 0 minutes ) ] for the netElement - IP Address: 10.90.165.20 MAC Address: 00:1c:73:2b:1d:1c to the container: container_95_2628617683664503.
DC1-LF...  |  cvpadmin
[ 2019-11-08 00:37:53 ]      Image push - Device reboot executed: ' enable reload all in 1 force' for the netElement - IP Address: 10.90.165.20 - MAC Address: 00:1c:73:2b:1d:1c to the container: container_95_2628617683664503.
DC1-LF...  |  cvpadmin
[ 2019-11-08 00:37:50 ]      Image push - [Reload scheduled for Fri Nov 8 08:35:57 2019 ( in 0 hours 0 minutes ) ] for the netElement - IP Address: 10.90.165.23 MAC Address: 44:4c:a8:24:97:81 to the container: container_53_98518277776349.
cvp-lf-23  |  cvpadmin
```

12.5.3 Applied Containers Tab

The Applied Containers tab displays the details on the containers to which the bundle has been applied. It also displays the name of the user that applied the bundle and the date it was applied.

Figure 12-15: Applied Container tab



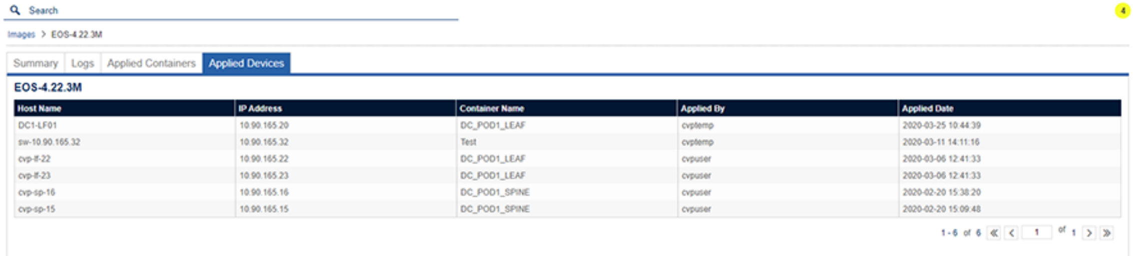
EOS-4.22.3M

Container Name	Applied By	Applied Date	Total Devices
DC_POD1_LEAF	cvpuser	2020-03-06 12:41:32	3
Tenant	cvpuser	2020-02-18 16:36:07	2

12.5.4 Applied Devices Tab

The **Applied Devices** tab displays the details on the devices to which the bundle is assigned, along with other information such as the parent container for the device, and the name of the user that applied the bundle and the date it was applied.

Figure 12-16: Applied Devices tab



EOS-4.22.3M

Host Name	IP Address	Container Name	Applied By	Applied Date
DC1-LF01	10.90.165.20	DC_POD1_LEAF	cvptemp	2020-03-25 10:44:39
sw-10.90.165.32	10.90.165.32	Test	cvptemp	2020-03-11 14:11:16
cvp-lf-22	10.90.165.22	DC_POD1_LEAF	cvpuser	2020-03-06 12:41:33
cvp-lf-23	10.90.165.23	DC_POD1_LEAF	cvpuser	2020-03-06 12:41:33
cvp-sp-16	10.90.165.16	DC_POD1_SPINE	cvpuser	2020-02-20 15:38:20
cvp-sp-15	10.90.165.15	DC_POD1_SPINE	cvpuser	2020-02-20 15:09:48

Related topics:

- Summary Tab
- Logs Tab
- Applied Containers Tab

12.5.5 Updating Bundles

Perform the following steps to update a bundle:

1. Go to the **Image Management** page.
2. Click the name of image bundle that you want to update.

The system displays the **Summary** tab.

Figure 12-17: Summary page showing bundle selected for edit

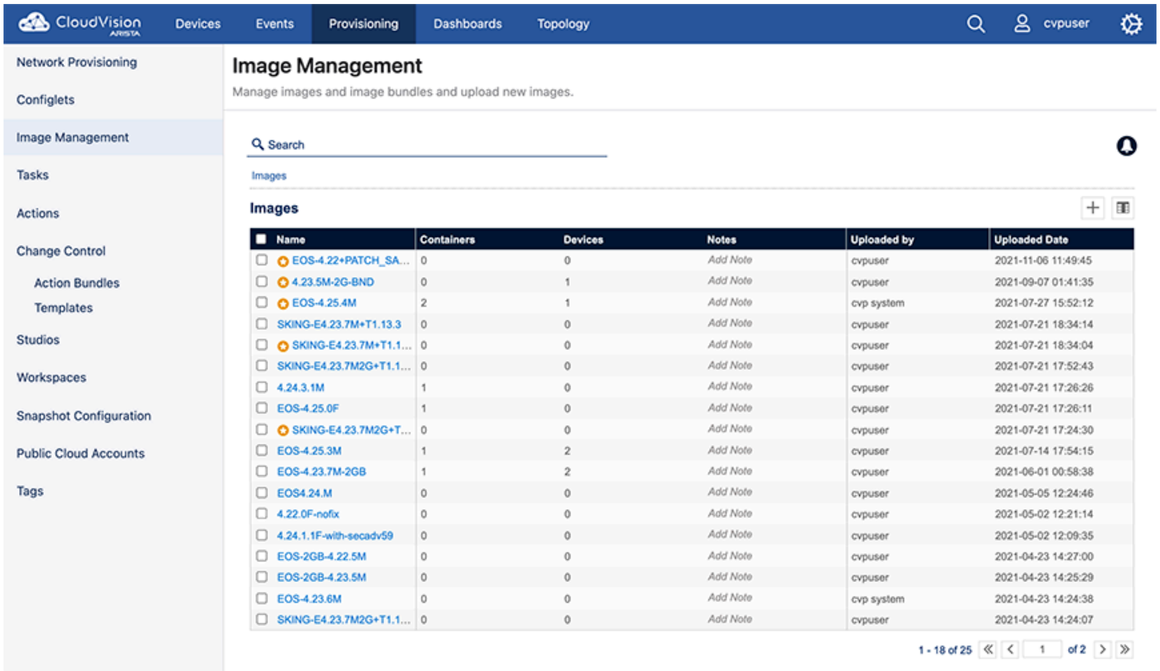


Image Management

Manage images and image bundles and upload new images.

Images

☐ Name	Containers	Devices	Notes	Uploaded by	Uploaded Date
☐ EOS-4.22+PATCH_SA...	0	0	*Add Note*	cvpuser	2021-11-06 11:49:45
☐ 4.23.5M-2G-BND	0	1	*Add Note*	cvpuser	2021-09-07 01:41:35
☐ EOS-4.25.4M	2	1	*Add Note*	cvp system	2021-07-27 15:52:12
☐ SKING-E4.23.7M+T1.13.3	0	0	*Add Note*	cvpuser	2021-07-21 18:34:14
☐ SKING-E4.23.7M+T1.1...	0	0	*Add Note*	cvpuser	2021-07-21 18:34:04
☐ SKING-E4.23.7M2G+T1.1...	0	0	*Add Note*	cvpuser	2021-07-21 17:52:43
☐ 4.24.3.1M	1	0	*Add Note*	cvpuser	2021-07-21 17:26:26
☐ EOS-4.25.0F	1	0	*Add Note*	cvpuser	2021-07-21 17:26:11
☐ SKING-E4.23.7M2G+T...	0	0	*Add Note*	cvpuser	2021-07-21 17:24:30
☐ EOS-4.25.3M	1	2	*Add Note*	cvpuser	2021-07-14 17:54:15
☐ EOS-4.23.7M-2GB	1	2	*Add Note*	cvpuser	2021-06-01 00:58:38
☐ EOS4.24.M	0	0	*Add Note*	cvpuser	2021-05-05 12:24:46
☐ 4.22.0F-nofix	0	0	*Add Note*	cvpuser	2021-05-02 12:21:14
☐ 4.24.1.1F-with-secadv59	0	0	*Add Note*	cvpuser	2021-05-02 12:09:35
☐ EOS-2GB-4.22.5M	0	0	*Add Note*	cvpuser	2021-04-23 14:27:00
☐ EOS-2GB-4.23.5M	0	0	*Add Note*	cvpuser	2021-04-23 14:25:29
☐ EOS-4.23.6M	0	0	*Add Note*	cvp system	2021-04-23 14:24:38
☐ SKING-E4.23.7M2G+T1.1...	0	0	*Add Note*	cvpuser	2021-04-23 14:24:07

1 - 18 of 25 « ‹ 1 of 2 › »

3. Click on the image name to edit.
4. Edit the bundle as needed.
5. Click **Save**.

Related topics:

- Deleting Bundles

12.5.6 Deleting Bundles

Only unused bundles can be deleted. If a bundle is assigned to a device or a container, it cannot be deleted from the inventory.

Perform the following steps to delete a bundle:

1. Go to the **Image Management** page.

2. Click the name of image bundle that you want to delete.

Figure 12-18: Deleting Bundles

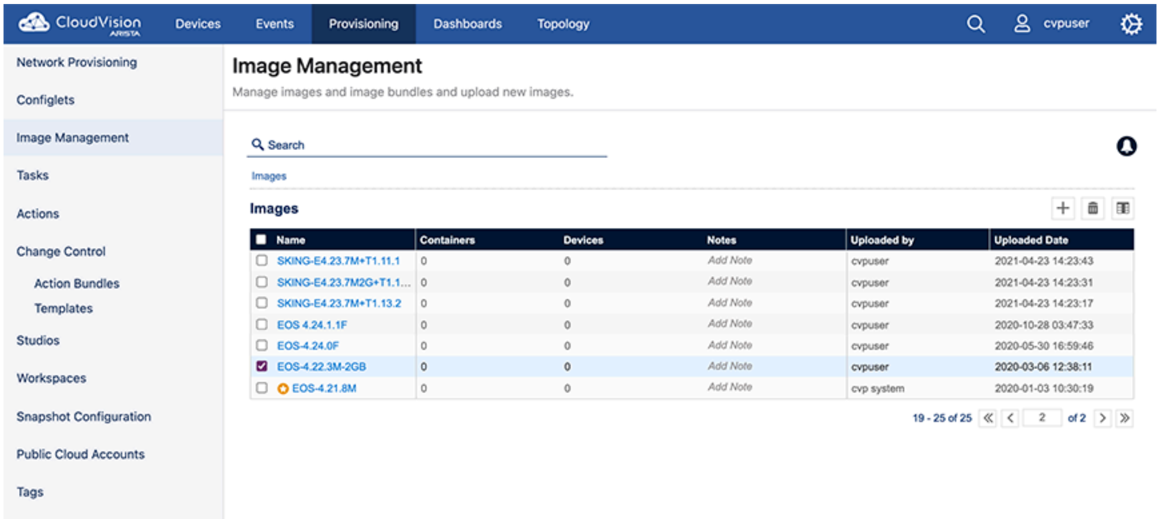


Image Management

Manage images and image bundles and upload new images.

Images

□ Name	Containers	Devices	Notes	Uploaded by	Uploaded Date
□ SKING-E4.23.7M+T1.11.1	0	0	Add Note	cvpuser	2021-04-23 14:23:43
□ SKING-E4.23.7M2G+T1.1...	0	0	Add Note	cvpuser	2021-04-23 14:23:31
□ SKING-E4.23.7M+T1.13.2	0	0	Add Note	cvpuser	2021-04-23 14:23:17
□ EOS 4.24.1.1F	0	0	Add Note	cvpuser	2020-10-28 03:47:33
□ EOS-4.24.0F	0	0	Add Note	cvpuser	2020-05-30 16:59:46
☑ EOS-4.22.3M-2GB	0	0	Add Note	cvpuser	2020-03-06 12:38:11
□ EOS-4.21.8M	0	0	Add Note	cvp system	2020-01-03 10:30:19

19 - 25 of 25 « ‹ 2 of 2 › »

3. Click the trash icon to delete the selected bundle from the inventory.

   The system prompts to confirm the deletion.
4. Click **Yes** to confirm deletion.
5. Click **Save**.

Note: The association can be removed only if a new bundle is assigned to device or container.

Note: When an image bundle is assigned to a container, no task will be spawned to the subordinate devices.

Related topics:

- Updating Bundles

Chapter 13

Partial Configuration Management

The partial configuration management feature specifies parts of configuration that should be managed by CVP. Each line in the configuration is classified in the following three categories:

- **Managed** - These configuration lines must be managed only by CVP.

  Note: Managed configuration lines are considered config compliant only when they synchronize with the designed and running configuration. In other words, updating managed configuration lines via non-CV sources will mark the device as non-compliant and cannot be reconciled by default. Only the user can reconcile these lines.
- **Unmanaged** - These configuration lines can't be managed by CVP.

  Note: Unmanaged configuration lines can be added to the running configuration via non-CVP sources without marking the device as non-compliant. These lines are ignored by CV during computation of configuration compliance and can never be reconciled.
- **Unspecified** - These configuration lines are by default managed and reconciled by CVP. They are not marked as managed or unmanaged by CVP.

Sections in this chapter include:

- Filters for Categorizing Sections in the Configuration
- Enabling Partial Configuration Management
- Filter Management
- Creating a New Filter
- Implications of Applied Filters
- Examples of Filter Management

13.1 Filters for Categorizing Sections in the Configuration

You can filter commands by using regular expressions. Filter highlights required configuration lines accordingly based on the following parameters:

- Filter Pattern
- Filter Type

Note: Level of a command represents the hierarchy of the configuration command.

13.1.1 Filter Pattern

A filter pattern is a list of section-aware configuration commands that can match the configuration on the device. It may contain the following wild-cards:

- The wild-card `*` matches anything (non-negative number of characters) in their commands. Commands are allowed to have multiple `*` in the same filter line as well.
- The wild-card `$` is a special command that is used to match an entire block of commands under the command matched till the previous level.

Note:

- CVP wild-cards are different from regular expression wild-cards. Filter pattern doesn't support regular expressions.
- A filter selects the whole block (all nested commands and sub-modes) from configuration which matches the last command string in the filter spec at that particular level.

Relative Order of Blocks in Filter Pattern

Filter Pattern	Matched Configuration
*ip *	ip routing no ip routing

transceiver*
$
	transceiver qsfp default-mode
	 4x10G
	   load-balance policies
	      load-balance sand
	 profile Orange
	         no fields mac
	         no fields mpls
	 fields symmetric-hash

transceiver *
load-balance policies
	load-balance policies
	      load-balance sand
	 profile Orange
	         no fields mac
	         no fields mpls
	 fields symmetric-hash

The order of the patterns at the same level is irrelevant. Hence the following filters are equivalent.

Note: `$` should be the last character in a configuration block. That is, adding commands after `$` inside the block triggers an error.

Filter 1	Filter 2	Filter 3

transceiver*
   load*
 	
Interface
 Management1
   ip *
   ipv6 *
	Interface
	 Management1
	   ip *
	   ipv6 *
	
	transceiver*
	   load*
		Interface
		 Management1
		   ipv6 *
		   ip *
		
		transceiver*
		   load*

13.1.2 Filter Type

A filter can be either managed or unmanaged.

13.1.2.1 Specific Filters

When multiple filters are applied for matching specified configuration lines, the filter with maximum levels specified is chosen for comparison.

Note: CVP highlights the managed lines in yellow and unmanaged lines in grey. In the example below, the bold text represents managed lines and the italic text represents unmanaged lines.

Filter 1 (Managed)	Filter 2 (Unmanaged)
transceiver* **$**	*transceiver** *load-balance**

Here, Filter 1 has only 1 level of command in the pattern whereas Filter 2 has 2 levels of command.

Note: $ is a special character and is not counted as a command. In other words, Filter 2 matches a more specific set of lines as shown below.

Configuration

```
transceiver qsfp default-mode 4x10G
   load-balance policies
      load-balance sand profile Orange
         no fields mac
```

Matched configuration for Filter 1

```
transceiver qsfp default-mode 4x10G
   load-balance policies
      load-balance sand profile Orange
         no fields mac
```

Matched configuration for Filter 2

```
load-balance policies
      load-balance sand profile Orange
         no fields mac
```

Thus, the combined result of the two filters would be:

```
transceiver qsfp default-mode 4x10G
   load-balance policies
      load-balance sand profile Orange
         no fields mac
```

13.1.2.2 Conflicting Filters

When two filters of different types match the same line and neither of them is more specific, they are said to be conflicting filters.

Note: CVP highlights the managed lines in yellow and unmanaged lines in grey. In the example below, the bold text represents managed lines and the italic text represents unmanaged lines.

Filter 1 (Managed)	Filter 2 (Unmanaged)	Configuration

transceiver*
load*
	*transceiver**
	*load-balance**
		`transceiver qsfp default-mode 4x10G`
		`load-balance policies`
		`load-balance sand profile Orange`
		`no fields mac`

These filters have conflicting patterns `load*` and `load-balance*`. CVP displays an error when conflicting filters are assigned to devices. If conflicting filters are assigned to a device, you must correct all filters for applying them correctly to the device.

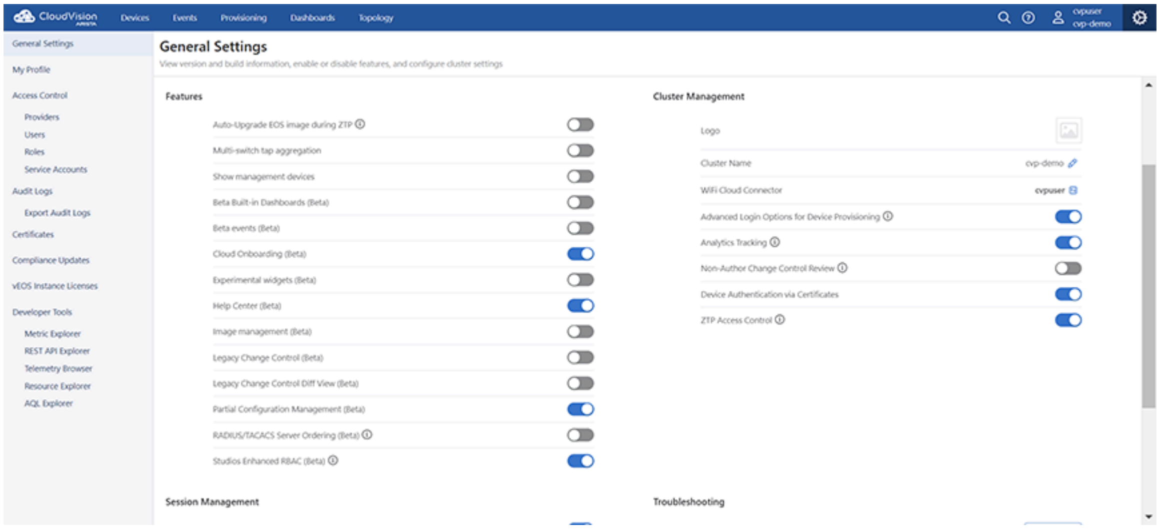
13.2 Enabling Partial Configuration Management

Perform the following steps if you do not find the **Filter Management** option under the **Provisioning** tab of the CVP screen:

1. Click the gear icon at the upper right corner of the screen.

   The browser displays the General Settings screen.

   Figure 13-1: Enabling Partial Configuration Management



General Settings

View version and build information, enable or disable features, and configure cluster settings

Features

Auto-Upgrade EOS image during ZTP	○
Multi-switch tap aggregation	○
Show management devices	○
Beta Built-in Dashboards (Beta)	○
Beta events (Beta)	○
Cloud Onboarding (Beta)	●
Experimental widgets (Beta)	○
Help Center (Beta)	●
Image management (Beta)	○
Legacy Change Control (Beta)	○
Legacy Change Control Diff View (Beta)	○
Partial Configuration Management (Beta)	●
RADIUS/TACACS Server Ordering (Beta)	○
Studios Enhanced RBAC (Beta)	●

Cluster Management

Logo	
Cluster Name	cvp-demo
WiFi Cloud Connector	cvpuser
Advanced Login Options for Device Provisioning	●
Analytics Tracking	●
Non-Author Change Control Review	○
Device Authentication via Certificates	●
ZTP Access Control	●

Session Management

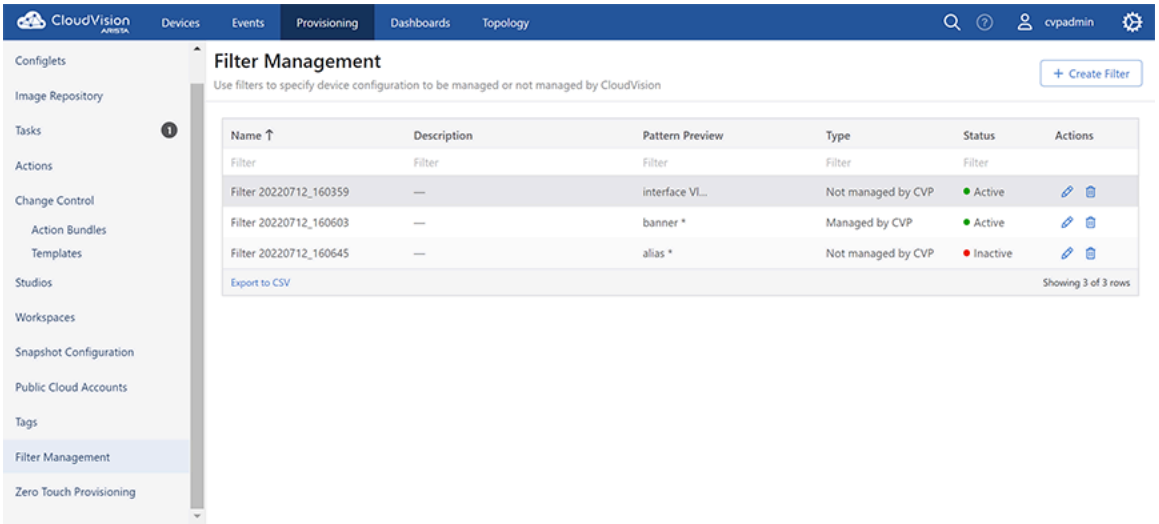
Troubleshooting

2. Under **Features**, enable **Partial Configuration Management (Beta)** using the toggle button.

13.3 Filter Management

The Filter Management screen lists all existing filters with all the fields associated with a filter. See the figure below.

Figure 13-2: Filter Management Screen



Filter Management

Use filters to specify device configuration to be managed or not managed by CloudVision

Name ↑	Description	Pattern Preview	Type	Status	Actions
Filter	Filter	Filter	Filter	Filter	
Filter 20220712_160359	—	interface Vl...	Not managed by CVP	● Active	
Filter 20220712_160603	—	banner *	Managed by CVP	● Active	
Filter 20220712_160645	—	alias *	Not managed by CVP	● Inactive	

Showing 3 of 3 rows

It provides options to perform the following tasks:

- Creating a filter
- Updating a filter
- Deleting a filter
- Enabling or disabling a filter
- Customizing the partial configuration management

To open the Filter Management screen, navigate to **Provisioning** > **Filter Management**. This screen provides brief information of current filters with the associated fields in a tabular format. See the following figure.

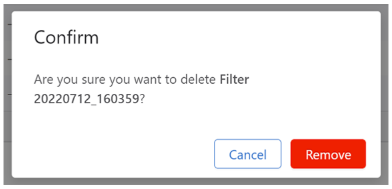
You can perform the following actions on this screen:

- On the upper right corner of the screen, click **+ Create Filter** to create a new filter. See Creating a New Filter.
- Under the **Pattern Preview** column, hover the cursor on the exclamatory mark to view the number of lines in the filter pattern.
- Under the **Status** column, green dots signify active filters and red dots signify inactive filters.
- Under the **Actions** column:
    - Click the edit icon to edit the corresponding filter.

      CVP opens the filter details screen for editing a filter. See Creating a New Filter.
    - Click the delete icon to delete the corresponding filter.

      Click **Confirm** when CVP opens the **Confirm** dialog box prompting to confirm the deletion.

Figure 13-3: Delete Filter Confirmation Dialog Box



Confirm

Are you sure you want to delete **Filter** 20220712_160359?

Note: Only inactive filters can be deleted.

- Click **Export to CSV** for downloading the table contents to your local drive.

13.4 Creating a New Filter

Perform the following tasks to create a new filter:

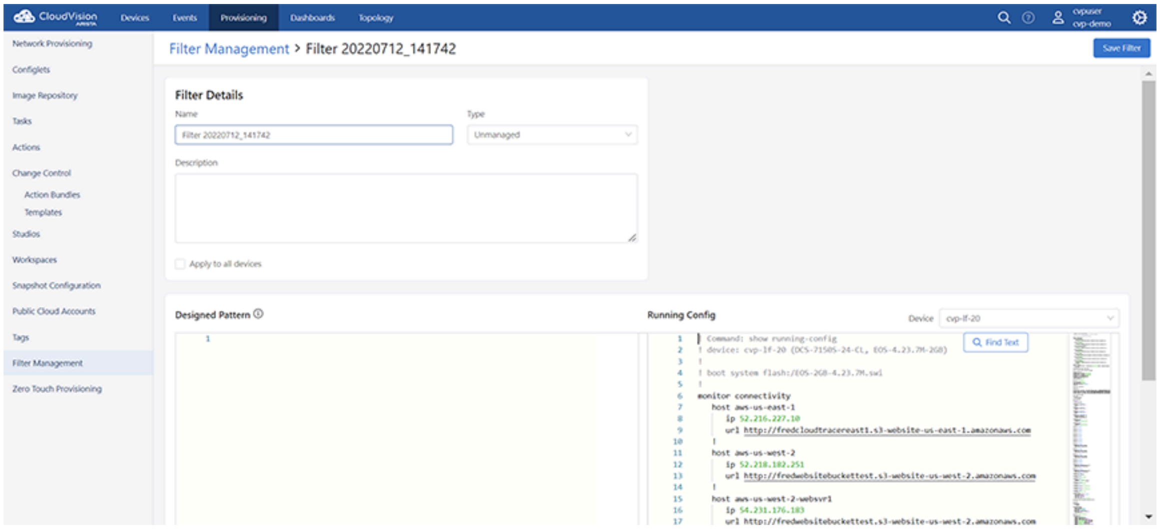
Note: If you are editing an existing filter, proceed to step 3.

1. Navigate to **Provisioning** > **Filter Management**.

   CVP opens the Filter Management screen.
2. Click **+ Create Filter**.

   CVP opens the screen for creating a new filter.

   Figure 13-4: Screen for Creating a New Filter



Filter Management > Filter 20220712_141742

Filter Details

Name: Filter 20220712_141742

Type: Unmanaged

Description

□ Apply to all devices

Designed Pattern

Running Config

Device: cvp-lf-20

```
! Command: show running-config
! device: cvp-lf-20 (DCS-7150S-24-CL, EOS-4.23.7M-2GB)
!
! boot system flash:/EOS-2GB-4.23.7M.swi
!
monitor connectivity
   host aws-us-east-1
      ip 52.216.227.10
      url http://fredcloudtracereast1.s3-website-us-east-1.amazonaws.com
   !
   host aws-us-west-2
      ip 52.218.182.251
      url http://fredwebsitebuckettest.s3-website-us-west-2.amazonaws.com
   !
   host aws-us-west-2-websvr1
      ip 54.231.176.183
      url http://fredwebsitebuckettest.s3-website-us-west-2.amazonaws.com
```

3. Provide the required filter details in corresponding fields:
   - **Filter Details** pane - Provides the following options to add filter details:
     - **Name** field - Type a unique filter name.

       Note: The filter name must not be blank.
     - **Type** dropdown menu - Select the filter type.
     - **Description** field - Provide brief information about the filter.
     - **Apply to all devices** checkbox - Select the checkbox to mark this filter as active else this filter is considered inactive.

       Note:
       - If the **Apply to all devices** checkbox is selected, the current filter (filter being added/edited) and all other active filters are validated against the running configuration of the selected device. This verifies if there are any conflicting filters.
       - If the **Apply to all devices** checkbox is not selected, only the current filter (filter being added/edited) is validated against the running configuration of the selected device.
   - **Designed Pattern** pane - Provide the tailored pattern for this filter.

Note: Applying the filter can change the managed configuration in designed configuration which results in non-compliance until it is pushed to the running configuration.

- **Running Config** pane - Displays the current configuration and provides the option to select the required device.

  Note:

  - Managed lines are highlighted in yellow and unmanaged lines are highlighted in grey color.
  - If an unmanaged configuration line being added matches with an assigned configlet of the selected device (including reconcile configlet) or if an added configuration line results in conflict with a configuration line in the existing configlets assigned to the device, the device will be marked out of compliance

  - **Device** dropdown menu - This drop down lists all available devices against which the filter can be validated.

4. Click **Save Filter**.

13.5 Implications of Applied Filters

The implications of applied filters in partial configuration management are:

- Configuration Compliance
- Provisioning
- Change Control Approval
- Task Execution
- Reconcile
- Studios and Workspaces

Configuration Compliance

Filter modification can change managed/unmanaged portions of designed and running configuration due to which configuration compliance status of some devices may get updated. In context of partial configuration management, the following logics determine the configuration compliance status of the device:

- Managed configuration lines and Unspecified configuration lines have the same compliance implications and they have to be in sync in the designed and running configuration for configuration compliance to be true. Which means changing such configuration lines outside CVP will mark the device out of compliance. Similarly modifying the designed configuration with addition/deletion of such configuration lines will result in out of compliance until they are pushed to the running configuration.
- Unmanaged configuration lines in the designed configuration will always result in configuration out of compliance. On the other hand, such configuration lines can be added to the running configuration outside CVP without causing the device to go out of compliance.
- Conflicting filters matching device’s designed or running configuration will mark the device out of compliance.

Provisioning

- Configlet management at device level -- Applied filters of `unmanaged` type can restrict CVP to modify corresponding unmanaged configuration lines. Configlets containing unmanaged configuration lines cannot be applied to a device. Validation of such proposed configuration will result in an error.
- Configlet management at container level -- Since this flow is not associated with a configuration validation process, it can result in making some unmanaged configuration lines part of the designed configuration. Hence, applying configlets containing unmanaged lines at container level will mark the underlying devices out of compliance. This can even create configuration push tasks, but they would fail later at the time of execution.

Change Control Approval

- Change controls with execute configuration task as one of their actions cannot be approved if the task diff contains unmanaged configuration lines in the designed configuration.
- Already approved change controls may get unapproved if filters associated with the underlying devices get changed.

Task Execution

Tasks with unmanaged configuration lines in the designed configuration will fail on execution. While viewing a task diff, inline errors will indicate the problematic lines and the relevant filters associated with the error.

Reconcile

- Reconcile at device level -- Unmanaged configuration lines from running configuration cannot be reconciled (tick boxes will not appear against those lines). Whereas managed lines from running configuration are not reconciled by default (tick boxes will be there, but not marked by default), but if the user wants, they can be reconciled explicitly by marking the tick boxes manually.
- Reconcile at container level -- Reconcile process at container level will never reconcile managed or unmanaged configuration lines from running configuration. Thus, it will only add unspecified lines from the running configuration to reconcile configlets. It can also delete existing managed lines from the reconciled configlet and thereby affect the configuration compliance status of the device. Hence it is recommended to have dedicated configlets for the managed configuration lines and not to keep them as part of the reconciled configlets.

Studios and Workspaces

- Workspace build will fail at the configuration validation step if the proposed configuration has unmanaged configuration lines or there are conflicting filters assigned to devices mapped to the workspace.
- Any change in filters mapped to affected devices in a workspace will not affect workspace submission. So any errors introduced by filter changes will only be seen in the Change Control created by workspace.
- Reverts in workspace will not change the state of filters.

13.6 Examples of Filter Management

Note: CVP highlights the managed lines in yellow and unmanaged lines in grey. In the example below, the bold text represents managed lines and the italic text represents unmanaged lines.

Config 1

```
router multicast
   ipv4
      routing
      route 232.1.1.1 192.168.0.1 iif Ethernet6 oif Ethernet20
   !
   vrf test
      ipv4
         routing
         route 238.1.1.1 2.2.2.2 iif Ethernet4 oif Ethernet41
         route 239.1.1.1 2.2.2.2 iif Ethernet4 oif Ethernet41
         route 239.3.3.3 3.3.3.3 iif Ethernet4 oif Ethernet5
         route 239.4.4.4 1.1.1.1 iif Ethernet42 oif Ethernet45
```

<table>
<tr><th>Filters</th><th>Result</th></tr>
<tr><td><pre>
router multicast
   $

router multicast
   vrf test
      ipv4
         route 239*
</pre></td><td><pre>
router multicast
   ipv4
      routing
      route 232.1.1.1
 192.168.0.1 iif Ethernet6 oif
 Ethernet20
   !
   vrf test
      ipv4
         routing
         route 238.1.1.1
 2.2.2.2 iif Ethernet4 oif
 Ethernet41
         route 239.1.1.1
 2.2.2.2 iif Ethernet4 oif
 Ethernet41
         route 239.3.3.3
 3.3.3.3 iif Ethernet4 oif
 Ethernet5
         route 239.4.4.4
 1.1.1.1 iif Ethernet42 oif
 Ethernet45
</pre></td></tr>
<tr><td><pre>
router multicast
   ipv4
      route*
   vrf test
      ipv4
         route 238*
router multicast
   vrf test
      ipv4
         route 239*
</pre></td><td><pre>
router multicast
   ipv4
      routing
      route 232.1.1.1
 192.168.0.1 iif Ethernet6 oif
 Ethernet20
   !
   vrf test
      ipv4
         routing
         route 238.1.1.1
 2.2.2.2 iif Ethernet4 oif
 Ethernet41
        route 239.1.1.1
 2.2.2.2 iif Ethernet4 oif
 Ethernet41
         route 239.3.3.3
 3.3.3.3 iif Ethernet4 oif
 Ethernet5
         route 239.4.4.4
 1.1.1.1 iif Ethernet42 oif
 Ethernet45
</pre></td></tr>
</table>

Config 2

```
transceiver qsfp default-mode 4x10G
   load-balance policies
      load-balance sand profile Orange
         no fields mac
      load-balance sand profile Blue
         no fields mac
```

Filters	Result
transceiver * load-balance policies load-balance sand profile * no fields mac	transceiver qsfp default-mode 4x10G load-balance policies load-balance sand profile Orange **no fields mac** load-balance sand profile Blue **no fields mac**
transceiver * load-balance policies load-balance sand profile Orange no fields mac	transceiver qsfp default-mode 4x10G load-balance policies load-balance sand profile Orange **no fields mac** load-balance sand profile Blue no fields mac

Chapter 14

Change Control

Task Management is an inventory of all the tasks generated in CloudVision. You can create a Change Control or cancel a task in task management.

Sections in this chapter include:

- Basic Options for Handling Tasks
- Using the Tasks Module
- Using the Change Control Module
- Non-Author Change Control Review
- Change Control Template

14.1 Basic Options for Handling Tasks

CloudVision provides two basic ways to handle tasks. You can handle tasks individually (task by task), or by groups of tasks.

To view and cancel tasks individually, use the Task Management module, which you can access by navigating to **Provisioning > Tasks** from the CloudVision Portal. For detailed information on the Tasks module, see Using the Tasks Module.

To execute grouped tasks (multiple tasks in the same group), use the Change Control module from either Tasks or Change Control screens. To access the Change Control screen, navigate to **Provisioning > Change Control** from the CloudVision Portal. For detailed information on the Change Control module, see Using the Change Control Module.

14.1.1 Creating Tasks

The following actions that affect the performance of devices are automatically generated as tasks:

- Assigning Configuration (assigning a configuration to a device or container)
- Adding Devices (adding a device from the undefined container to a defined container)
- Managing Devices (moving or removing devices from a container)

14.1.1.1 Assigning Configuration

1. Go to the Network Provisioning screen.
2. Select a device or container.
3. Assign configuration.
4. Save the topology to generate the task.

Note: Editing a configlet also generates a task.

14.1.1.2 Adding Devices

1. Go to the Network provisioning screen.
2. Select a container.
3. Add devices to the container.

4. Save the topology to generate the task.

   Note: If the hierarchy of the container has images or configlets, the created task will also include image push and configuration push tasks.

14.1.1.3 Managing Devices

1. Go to the Network provisioning screen.
2. Select a container.
3. Move or remove devices from the container.
4. Save the topology to generate the task.

14.2 Using the Tasks Module

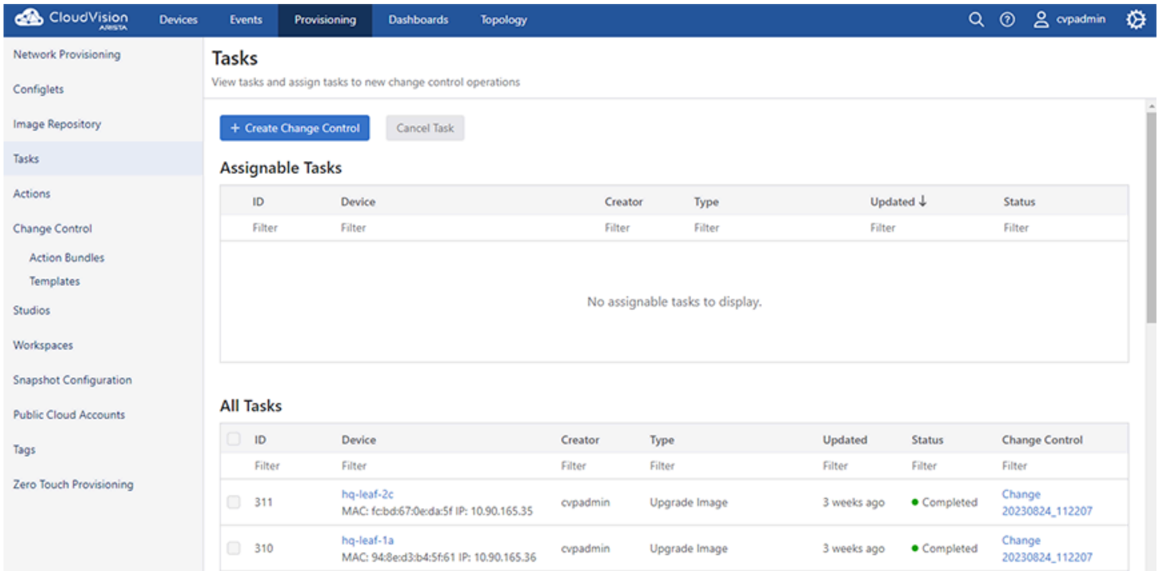
This module covers the following sections:

- Accessing the Tasks Summary Screen
- Creating Change Controls from the Tasks Summary Screen
- Creating Change Controls from the Change Controls Summary Screen
- Accessing the Tasks Details Screen
- Task Status

14.2.1 Accessing the Tasks Summary Screen

Use the **Tasks Summary** screen to create Change Controls, cancel tasks, view assignable and assigned tasks, navigate to the appropriate task details screen, and navigate to the device overview screen. See **Task Screen** below.

Figure 14-1: Tasks Screen



Tasks

View tasks and assign tasks to new change control operations

Assignable Tasks

ID	Device	Creator	Type	Updated ↓	Status
Filter	Filter	Filter	Filter	Filter	Filter

No assignable tasks to display.

All Tasks

□	ID	Device	Creator	Type	Updated	Status	Change Control
	Filter	Filter	Filter	Filter	Filter	Filter	Filter
□	311	hq-leaf-2c MAC: fc:bd:67:0e:da:5f IP: 10.90.165.35	cvpadmin	Upgrade Image	3 weeks ago	● Completed	Change 20230824_112207
□	310	hq-leaf-1a MAC: 94:8e:d3:b4:5f:61 IP: 10.90.165.36	cvpadmin	Upgrade Image	3 weeks ago	● Completed	Change 20230824_112207

To access the **Tasks Summary** screen, go to the **Provisioning** screen and click **Tasks** in the left menu.

The **Tasks Summary** screen consists of the following entities:

- **+ Create Change Control button** - Click this button to create a Change Control
- **Cancel Task(s) button** - Click this button to cancel selected assignable tasks
- **Assignable Tasks Table** - Lists assignable tasks with the following information:

  - **Task ID** - Displays the task ID.

    Click the **Task ID** go to the appropriate task details screen.
  - **Device** - Displays the device name on which this task is performed.

    Click the device name to open the appropriate **Device Overview** screen.
  - **Created By** - Displays who created the task.
  - **Type** - Displays the task type.
  - **Last Updated** - Displays when the task was last updated.
  - **Status** - Displays the task status.
- **Assigned Tasks Table** - Lists assigned tasks with the following information:
  - **Task ID -** Displays the task ID.

    Click the task ID go to the appropriate task details screen.
  - **Device -** Displays the device name on which this task is performed.

    Click the device name to open the appropriate **Device Overview** screen.
  - **Created By** - Displays who created the task.
  - **Type** - Displays the task type.
  - **Last Updated** - Displays when the task was last updated.
  - **Status -** Displays the task status.
  - **Change Control** - Displays the Change Control name.

    Click the Change Control name to go to the appropriate **Change Control Details** screen.

14.2.2 Creating Change Controls from the Tasks Summary Screen

The Change Control module selects and executes a group of tasks that you want to process simultaneously. While creating a Change Control, you add tasks with pending or failed status to the Change Control.

Complete the following steps to create a Change Control from the tasks summary screen:

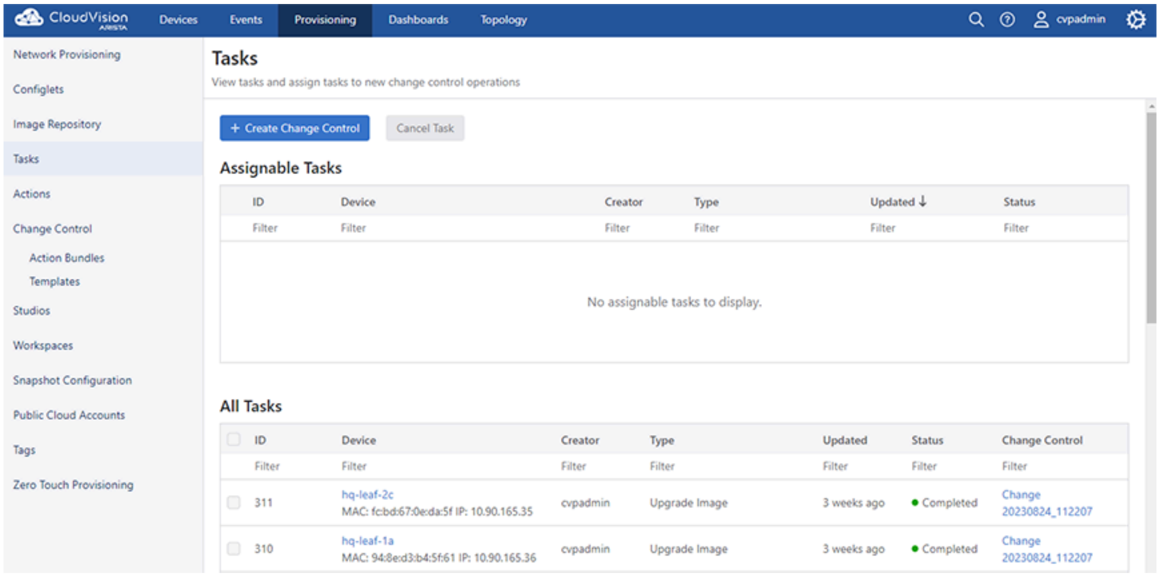
1. On the CloudVision Portal, click **Provisioning > Tasks.**

   The system displays the tasks summary screen.
2. Under the Assignable Tasks table, select tasks you want to include in the Change Control by selecting appropriate checkboxes.

   Note: If you do not select any tasks, the system creates a Change Control without tasks.

3. Click **+ Create Change Control** with *n tasks* where n is the count of selected tasks.

Figure 14-2: Create Change Control Button



Tasks

View tasks and assign tasks to new change control operations

Assignable Tasks

ID	Device	Creator	Type	Updated ↓	Status
Filter	Filter	Filter	Filter	Filter	Filter

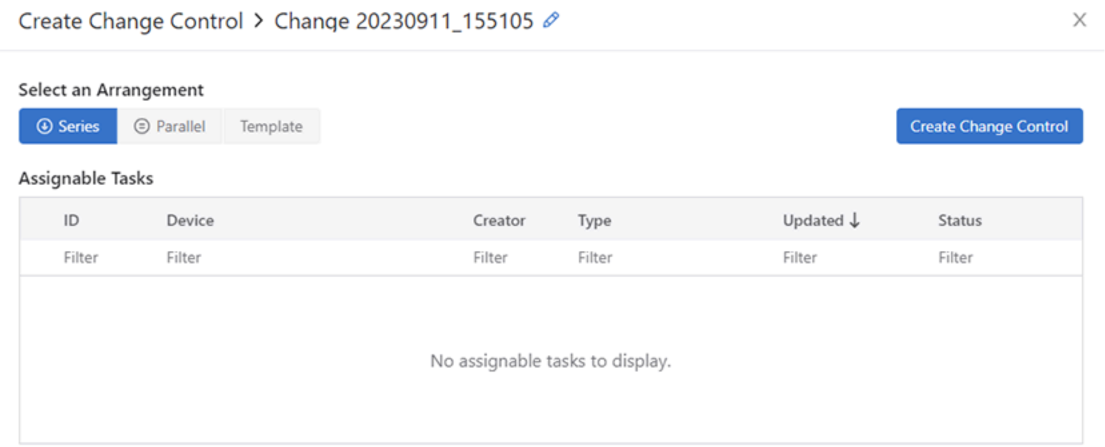
No assignable tasks to display.

All Tasks

□	ID	Device	Creator	Type	Updated	Status	Change Control
	Filter	Filter	Filter	Filter	Filter	Filter	Filter
□	311	hq-leaf-2c MAC: fc:bd:67:0e:da:5f IP: 10.90.165.35	cvpadmin	Upgrade Image	3 weeks ago	● Completed	Change 20230824_112207
□	310	hq-leaf-1a MAC: 94:8e:d3:b4:5f:61 IP: 10.90.165.36	cvpadmin	Upgrade Image	3 weeks ago	● Completed	Change 20230824_112207

The system displays the appropriate Change Control details screen.

Figure 14-3: Create a Change Control



Select an Arrangement

Assignable Tasks

ID	Device	Creator	Type	Updated ↓	Status
Filter	Filter	Filter	Filter	Filter	Filter

No assignable tasks to display.

14.2.3 Creating Change Controls from the Change Controls Summary Screen

The first step involved in using the **Change Control** module to manage tasks is to create a Change Control. While creating a Change Control, you add tasks with pending or failed status to the Change Control. By default, all tasks in the same Change Control are added in parallel. If you want to change the execution order, you can drag and drop the action cards on the **Change Control Details** screen. You can execute grouped tasks after a Change Control is created, reviewed, and approved.

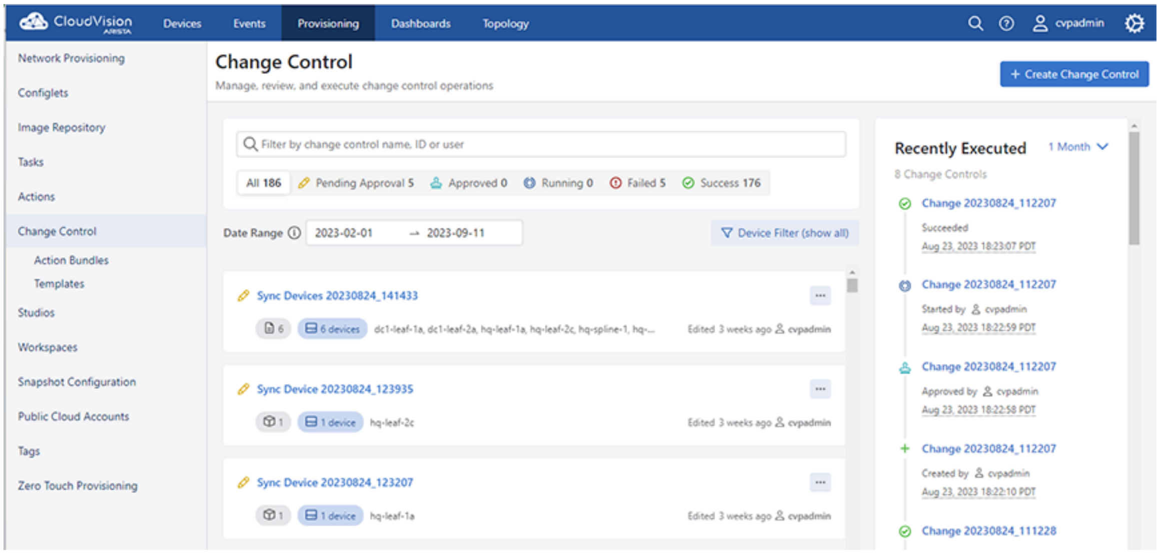
Note: If you do not add any tasks, the system creates a Change Control without tasks.

Complete the following steps to create a Change Control from the **Change Control Summary** screen:

1. On the CloudVision Portal, click **Provisioning > Change Control**.

The system displays the **Change Control Summary** screen.

Figure 14-4: Change Control Summary Screen



Change Control

Manage, review, and execute change control operations

Date Range 2023-02-01 → 2023-09-11

Sync Devices 20230824_141433
6 | 6 devices | dc1-leaf-1a, dc1-leaf-2a, hq-leaf-1a, hq-leaf-2c, hq-spline-1, hq-... | Edited 3 weeks ago cvpadmin

Sync Device 20230824_123935
1 | 1 device | hq-leaf-2c | Edited 3 weeks ago cvpadmin

Sync Device 20230824_123207
1 | 1 device | hq-leaf-1a | Edited 3 weeks ago cvpadmin

8 Change Controls

Change 20230824_112207
Succeeded
Aug 23, 2023 18:23:07 PDT

Change 20230824_112207
Started by cvpadmin
Aug 23, 2023 18:22:59 PDT

Change 20230824_112207
Approved by cvpadmin
Aug 23, 2023 18:22:58 PDT

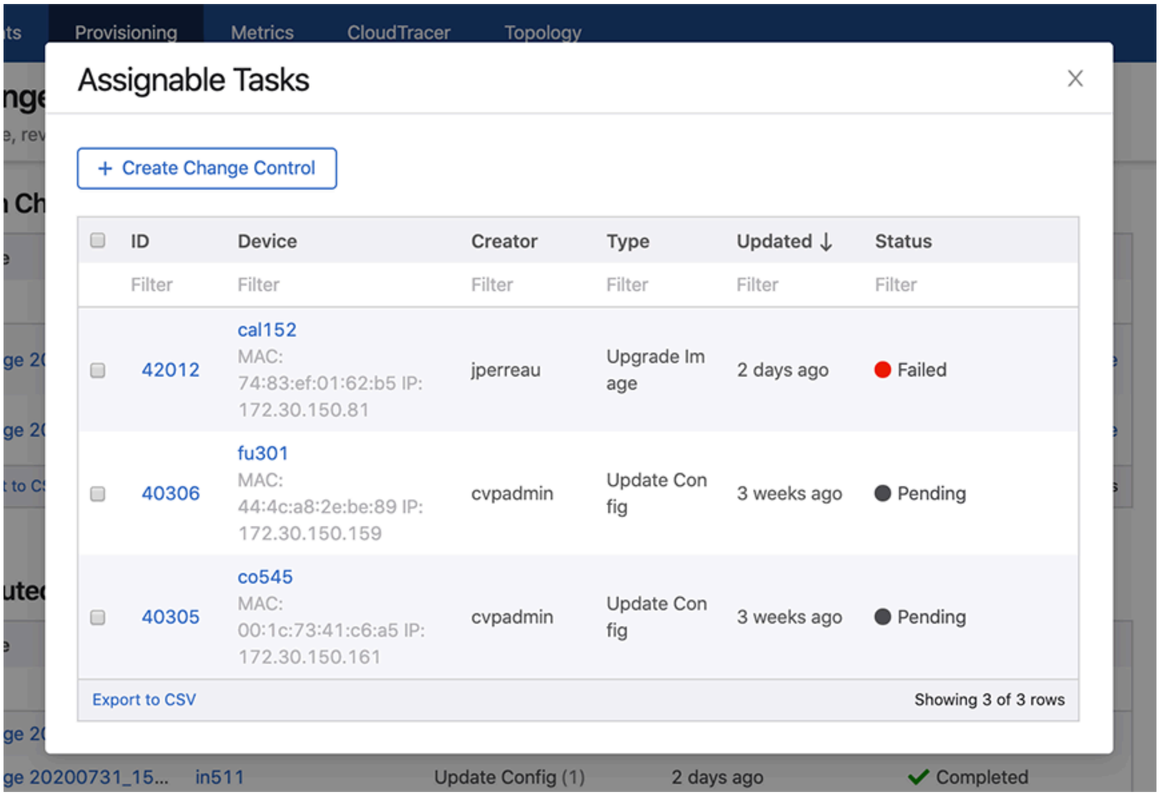
Change 20230824_112207
Created by cvpadmin
Aug 23, 2023 18:22:10 PDT

Change 20230824_111228

2. Click **+ Create Change Control** button at the upper right corner.

The system displays the **Assignable Tasks** dialog box.

Figure 14-5: Assignable Tasks Dialog Box with No Tasks Selected



□	ID	Device	Creator	Type	Updated ↓	Status
	Filter	Filter	Filter	Filter	Filter	Filter
□	42012	cal152 MAC: 74:83:ef:01:62:b5 IP: 172.30.150.81	jperreau	Upgrade Image	2 days ago	● Failed
□	40306	fu301 MAC: 44:4c:a8:2e:be:89 IP: 172.30.150.159	cvpadmin	Update Config	3 weeks ago	● Pending
□	40305	co545 MAC: 00:1c:73:41:c6:a5 IP: 172.30.150.161	cvpadmin	Update Config	3 weeks ago	● Pending

Showing 3 of 3 rows

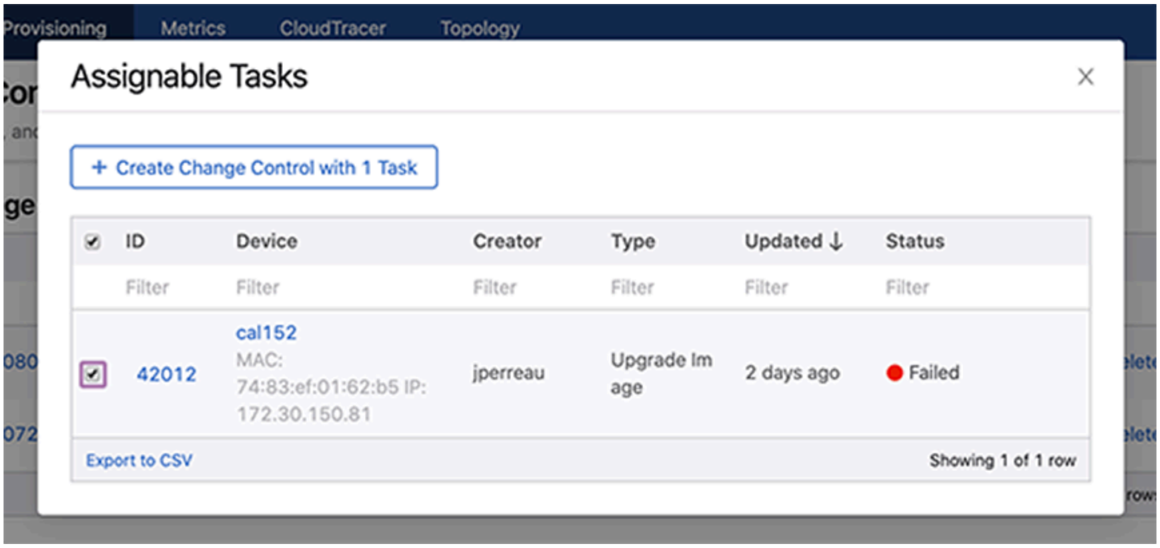
ge 20200731_15... in511 Update Config (1) 2 days ago ✓ Completed

3. Select tasks you want to include in the Change Control by selecting appropriate checkboxes.

Note: If you do not select any tasks, the system creates a Change Control without tasks.

4. Click **+ Create Change Control** with n tasks where n is the count of selected tasks.

Figure 14-6: Assignable Tasks Dialog Box with Tasks Selected



Assignable Tasks

+ Create Change Control with 1 Task

☑	ID	Device	Creator	Type	Updated ↓	Status
	Filter	Filter	Filter	Filter	Filter	Filter
☑	42012	cal152 MAC: 74:83:ef:01:62:b5 IP: 172.30.150.81	jperreau	Upgrade Image	2 days ago	● Failed

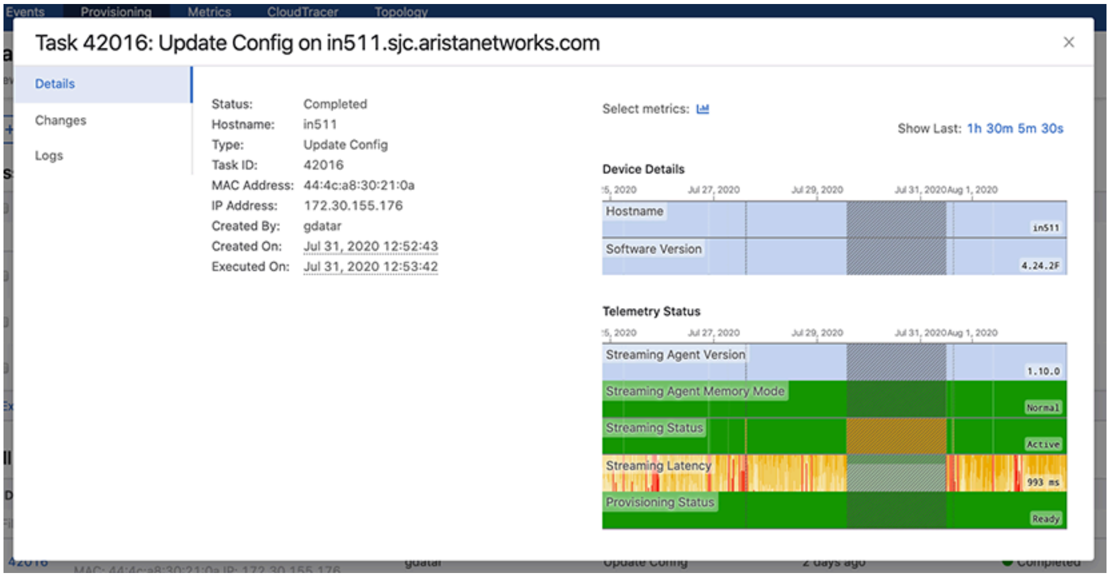
Export to CSV — Showing 1 of 1 row

The system displays the appropriate **Change Control Details** screen.

14.2.4 Accessing the Tasks Details Screen

The **Tasks details** screen provides detailed information for any given task. To access the Tasks details screen, click the task ID under the **Task ID** column in the **Tasks summary** screen.

Figure 14-7: Task Details Screen



Task 42016: Update Config on in511.sjc.aristanetworks.com

Status:	Completed
Hostname:	in511
Type:	Update Config
Task ID:	42016
MAC Address:	44:4c:a8:30:21:0a
IP Address:	172.30.155.176
Created By:	gdatar
Created On:	Jul 31, 2020 12:52:43
Executed On:	Jul 31, 2020 12:53:42

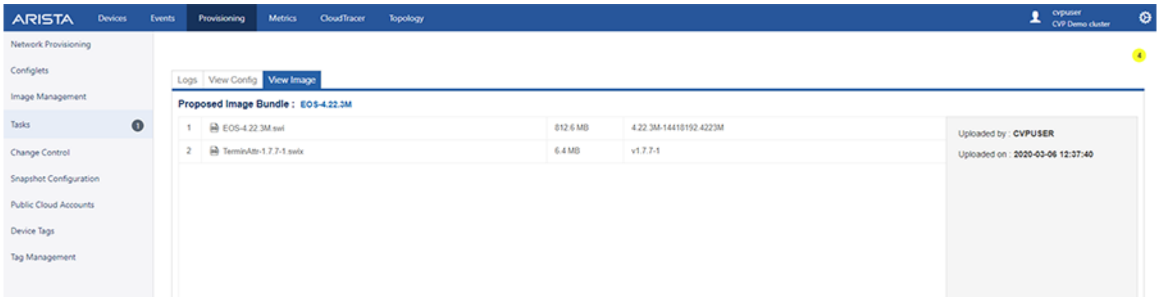
The **Tasks Details** screen provides the specified information in following tabs:

- **Pending tasks** icon - Displays the count of pending tasks
- **Notifications** - Displays the count of unread notifications.
- **Logs** tab - Displays logs of the appropriate task.

Note: This tab is displayed only for completed tasks.

- **View Image** tab - Provides detailed information on image changes.

  Figure 14-8: View Image Tab



Proposed Image Bundle : EOS-4.22.3M

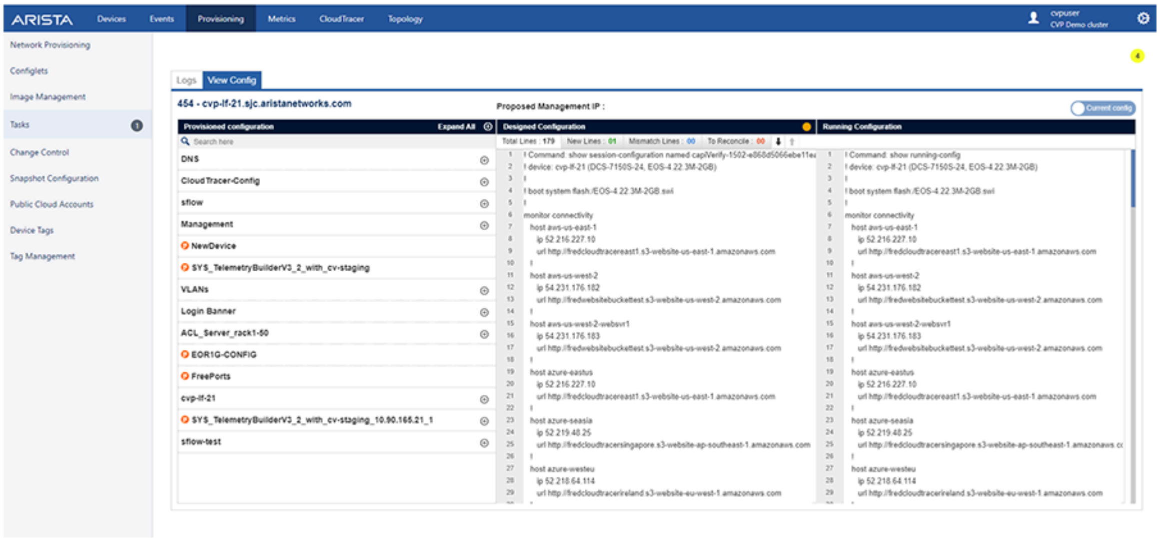
1	EOS-4.22.3M.swi	812.6 MB	4.22.3M-14418192.4223M
2	TerminAttr-1.7.7-1.swix	6.4 MB	v1.7.7-1

Uploaded by : **CVPUSER**

Uploaded on : **2020-03-06 12:37:40**

- **View Config** tab - Displays provisioned, designed, and running configuration changes.

  Figure 14-9: View Config Tab



454 - cvp-lf-21.sjc.aristanetworks.com

Proposed Management IP :

Provisioned configuration

- DNS
- CloudTracer-Config
- sflow
- Management
- NewDevice
- SYS_TelemetryBuilderV3_2_with_cv-staging
- VLANs
- Login Banner
- ACL_Server_rack1-50
- EOR1G-CONFIG
- FreePorts
- cvp-lf-21
- SYS_TelemetryBuilderV3_2_with_cv-staging_10.90.165.21_1
- sflow-test

Designed Configuration

Total Lines : 179 New Lines : 01 Mismatch Lines : 00 To Reconcile : 00

```
! Command: show session-configuration named capiVerify-1502-e868d5066ebe11e
! device: cvp-lf-21 (DCS-7150S-24, EOS-4.22.3M-2GB)
!
! boot system flash:/EOS-4.22.3M-2GB.swi
!
monitor connectivity
  host aws-us-east-1
    ip 52.216.227.10
    url http://fredcloudtracereast1.s3-website-us-east-1.amazonaws.com
  !
  host aws-us-west-2
    ip 54.231.176.182
    url http://fredwebsitebuckettest.s3-website-us-west-2.amazonaws.com
  !
  host aws-us-west-2-websvr1
    ip 54.231.176.183
    url http://fredwebsitebuckettest.s3-website-us-west-2.amazonaws.com
  !
  host azure-eastus
    ip 52.216.227.10
    url http://fredcloudtracereast1.s3-website-us-east-1.amazonaws.com
  !
  host azure-seasia
    ip 52.219.48.25
    url http://fredcloudtracersingapore.s3-website-ap-southeast-1.amazonaws.com
  !
  host azure-westeu
    ip 52.218.64.114
    url http://fredcloudtracerireland.s3-website-eu-west-1.amazonaws.com
```

Running Configuration

```
! Command: show running-config
! device: cvp-lf-21 (DCS-7150S-24, EOS-4.22.3M-2GB)
!
! boot system flash:/EOS-4.22.3M-2GB.swi
!
monitor connectivity
  host aws-us-east-1
    ip 52.216.227.10
    url http://fredcloudtracereast1.s3-website-us-east-1.amazonaws.com
  !
  host aws-us-west-2
    ip 54.231.176.182
    url http://fredwebsitebuckettest.s3-website-us-west-2.amazonaws.com
  !
  host aws-us-west-2-websvr1
    ip 54.231.176.183
    url http://fredwebsitebuckettest.s3-website-us-west-2.amazonaws.com
  !
  host azure-eastus
    ip 52.216.227.10
    url http://fredcloudtracereast1.s3-website-us-east-1.amazonaws.com
  !
  host azure-seasia
    ip 52.219.48.25
    url http://fredcloudtracersingapore.s3-website-ap-southeast-1.amazonaws.cc
  !
  host azure-westeu
    ip 52.218.64.114
    url http://fredcloudtracerireland.s3-website-eu-west-1.amazonaws.com
```

14.2.5 Task Status

All CloudVision Portal (CVP) tasks are automatically assigned a specific status by the system. The system automatically updates tasks status to indicate the current status of a task.

The task statuses are:

- Pending
- In-Progress
- Completed
- Failed
- Canceled

14.2.5.1 Pending

Any new task is generated with a 'Pending' status. This means that the task has been generated but not executed. You can execute a pending task at any time. Once the task is successfully executed (completed without failure), the status of the task changes to Completed.

14.2.5.2 In-Progress

A task being executed moves to “In-progress” state.

- Config assign, pushes the configuration on the device.
- Image assign, copies the image from CloudVision to the device.
- In-Progress tasks can be canceled.

Various statuses during the Change Control execution are:

- Execution In Progress
- Device Reboot In Progress
- Task Update In Progress
- Configlet Push In Progress
- Image Push In Progress
- Rollback Config Push In Progress
- Rollback Image Push In Progress
- Cancel In Progress
- ZTR Replacement In Progress

14.2.5.3 Completed

A task that has been completed. Upon completion, the status changes to Completed. Tasks with Completed status can't be executed or canceled.

14.2.5.4 Failed

A task moves to failed state due to multiple reasons such as:

- Device not reachable
- Wrong configuration
- Application problem

14.2.5.5 Canceled

A task that is removed from the queue of pending tasks. Tasks with the status of Completed or tasks that have already been canceled, cannot be canceled. Tasks with any status other than Canceled or Completed can be selected and canceled.

14.3 Using the Change Control Module

The **Change Control** module selects and executes a group of tasks that you want to process simultaneously. Selecting tasks and creating Change Controls function similarly in **Change Control** and **Task Management** modules.

Change Controls provides the following benefits:

- Sequencing tasks
- Adding unlimited snapshots to every device impacted by the Change Control execution
- Adding custom actions
- Pushing images via Multi-Chassis Link Aggregation (MLAG) In-Service Software Upgrade (ISSU) or Border Gateway Protocol (BGP) maintenance mode
- Reviewing the entire set of changes to approve Change Controls

Note: Snapshots display the state of impacted devices before and after the execution.

For more information about Change Controls, see:

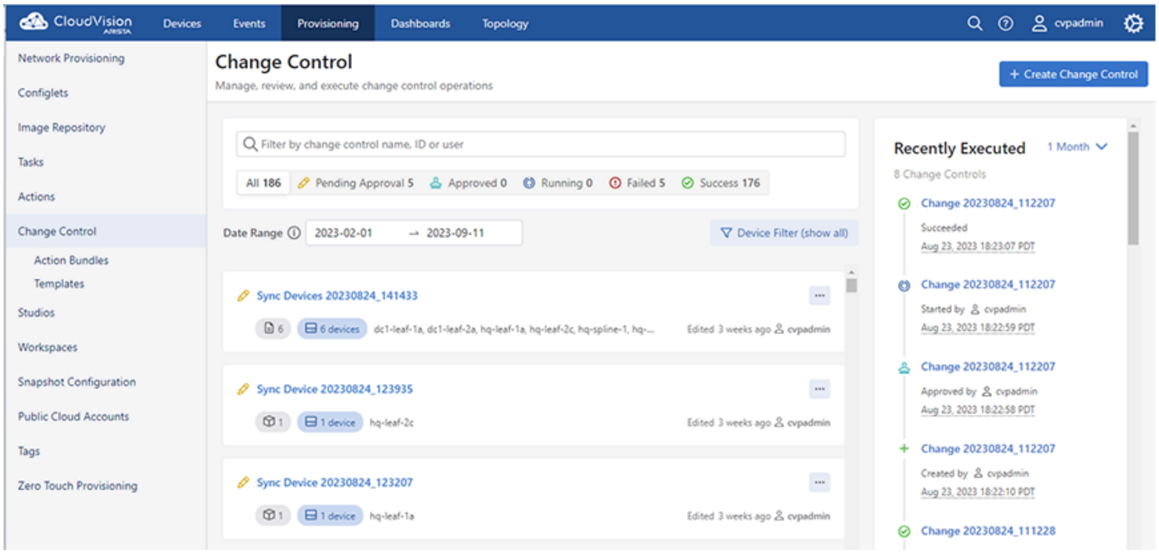
- Accessing the Change Control Summary Screen
- Accessing the Open Change Control Details Screen
- Creating Change Controls from the Change Controls Summary Screen

- Accessing the Open Change Control Details Screen

14.3.1 Accessing the Change Control Summary Screen

The Change Control summary screen is used to manage Change Controls.

Figure 14-10: Change Control Summary Screen



Change Control

Manage, review, and execute change control operations

All 186 | Pending Approval 5 | Approved 0 | Running 0 | Failed 5 | Success 176

Date Range 2023-02-01 → 2023-09-11

Sync Devices 20230824_141433
6 | 6 devices | dc1-leaf-1a, dc1-leaf-2a, hq-leaf-1a, hq-leaf-2c, hq-spline-1, hq-... | Edited 3 weeks ago cvpadmin

Sync Device 20230824_123935
1 | 1 device | hq-leaf-2c | Edited 3 weeks ago cvpadmin

Sync Device 20230824_123207
1 | 1 device | hq-leaf-1a | Edited 3 weeks ago cvpadmin

Recently Executed
8 Change Controls

Change 20230824_112207
Succeeded
Aug 23, 2023 18:23:07 PDT

Change 20230824_112207
Started by cvpadmin
Aug 23, 2023 18:22:59 PDT

Change 20230824_112207
Approved by cvpadmin
Aug 23, 2023 18:22:58 PDT

Change 20230824_112207
Created by cvpadmin
Aug 23, 2023 18:22:10 PDT

Change 20230824_111228

To access the Change Control screen, go to the Provisioning screen, and click Change Control in the left menu.

The Change Control screen consists of the following entities:

- **Open Change Controls** and **Executed Change Controls** tables - Lists corresponding Change Controls with the following information:
  - **Name** - Displays the Change Control name

    Click the Change Control name to go to the appropriate Change Control details screen.
  - **Devices** - Displays devices used in the Change Control

    Click the device name to go to the appropriate Device Overview screen.
  - **Action** - Displays types of actions to be executed by the Change Control
  - **Last Updated** - Displays when the Change Control was last updated
  - **Status** - Displays the Change Control status

    Note:

    - Under the **Status** column of the **Open Change Controls** table, a pending Change Controls is represented with a doc-edit icon and an approved Change Controls is represented with a user-check icon.
    - Under the **Status** column of the **Open Change Controls** table, a failed Change Control is represented with a cross mark and a completed Change Control is represented with a tick mark.
    - Hover the cursor on the status icon in **Open Change Controls** table to view how long ago the current approval status was updated. When you hover the cursor on the status icon in **Executed Change Controls** table, it also displays the approver's name.
- In the **Open Change Controls** table, click **Delete** to delete the appropriate Change Control.

  Note: After you delete an open Change Control, the system returns any tasks used by the deleted Change Control to the assignable tasks pool for reallocation.
- **Recent Activity** pane - Lists most recent activities like updated, executed, and deleted Change Controls.

Note: Click on the Change Control name to go to the appropriate Change Control details screen.

- **+ Create Change Control -** Click this button to create a Change Control
- **Export to CSV -** Exports the summary data to a CSV file.

14.3.2 Accessing the Open Change Control Details Screen

The open Change Control details screen performs the following functions:

- Displays Change Control information
- Adds actions to Change Control
- Adds, edits, and deletes child stages
- Reviews and approves Change Control

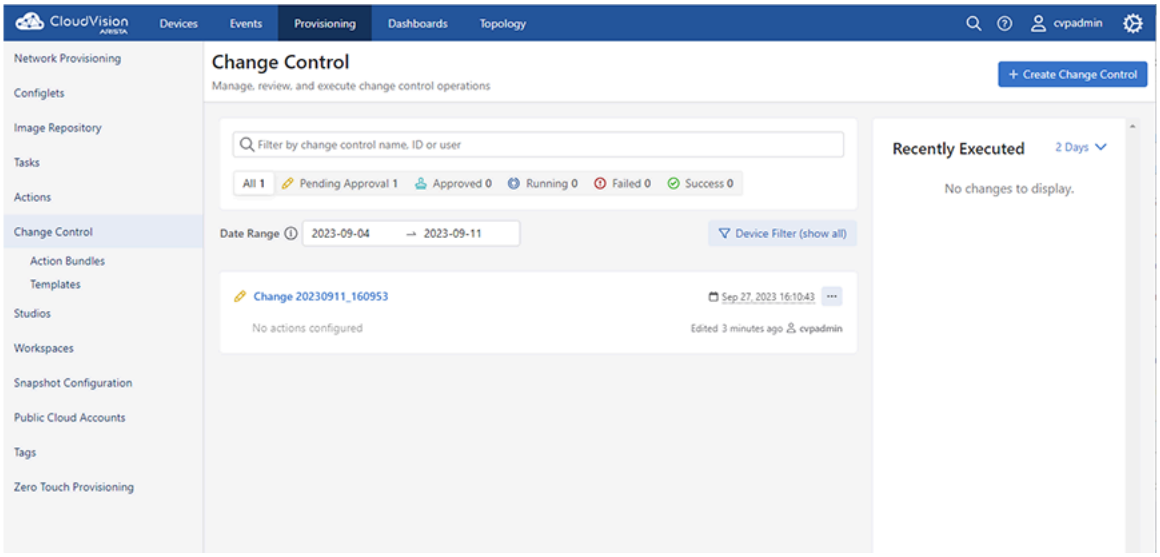
Perform the following steps to access the Change Control details screen:

1. On the CloudVision Portal, click **Provisioning** > **Change Control**.

   The system displays the Change Control summary screen.
2. Under the **Open Change Controls** table, click one of the listed Change Controls.

   The system displays the Change Control details screen.

Figure 14-11: Change Control Details Screen



Change Control

Manage, review, and execute change control operations

Date Range 2023-09-04 → 2023-09-11

Change 20230911_160953 — Sep 27, 2023 16:10:43

No actions configured — Edited 3 minutes ago cvpadmin

No changes to display.

The Change Control details screen consists of the following panels:

- Header Panel
- Main Panel
- Edit Panel

Header Panel

This primary panel provides the following basic information on the Change Control:

- Edit icon to update the Change Control name
- Change Control information -
  - The open Change Control details screen displays the status, scheduled date, last editor, count of affected devices, and Universally Unique Identifier (UUID).

Note:

- Click the **Scheduled for** field and select the date to run the Change Control.
- Hover the mouse cursor over the clock icon to view the last time of action.
- Hover the cursor on the count of affected devices to view their list. Clicking on an affected device opens the corresponding Device Overview screen.
- Clicking the copy icon next to the UUID copies the UUID to the clipboard.

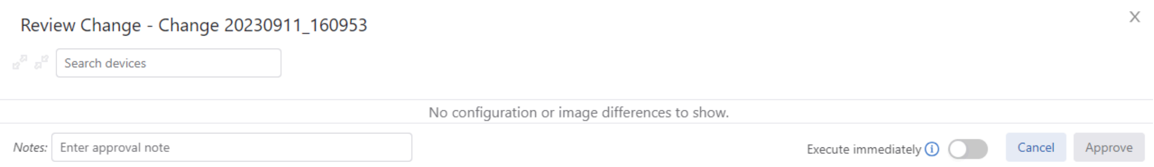
- The executed Change Control details screen displays the status, approver, time of start, last editor, and count of affected devices.

  Note:

  - Click **Review** next to the status for details on review and approve process.

- **Review and Approve** - Click **Review and Approve** in open Change Controls for assessing Change Control updates. These updates include configuration differences, and image bundle changes when appropriate.

  Figure 14-12: Review and Approve Pop-Up Window

  Review Change - Change 20230911_160953

  Search devices

  No configuration or image differences to show.

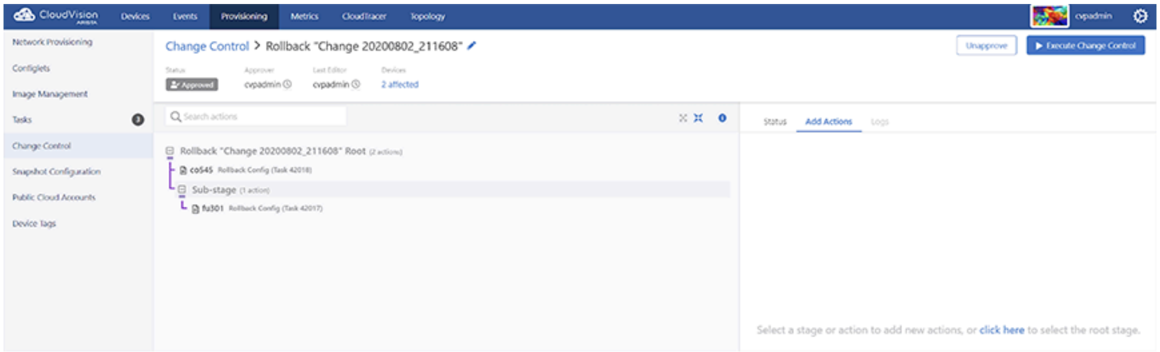
  Notes: Enter approval note

  Click **Approve** to accept Change Control updates.

  Note: (Optional) Approver can leave comments in the ***Notes:*** field.

- On the approved Change Control details screen, click **Unapprove** to revert the approval status and **Execute Change Control** to run approved Change Controls.

  Figure 14-13: Approved Change Control

  Change Control > Rollback "Change 20200802_211608"

  Status: Approved | Approver: cvpadmin | Last Editor: cvpadmin | Devices: 2 affected

  Rollback "Change 20200802_211608" Root (2 actions)
  co545 Rollback Config (Task 42018)
  Sub-stage (1 action)
  fu301 Rollback Config (Task 42017)

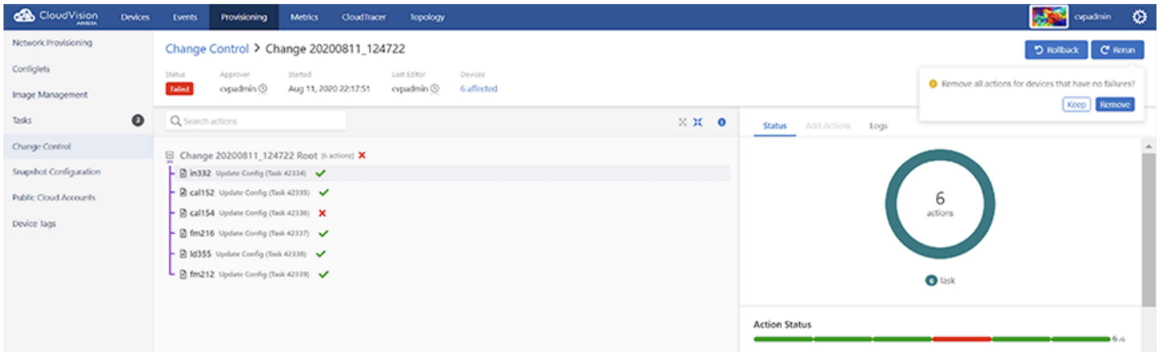
  Select a stage or action to add new actions, or click here to select the root stage.

  Note: CVP executes Change Controls in the following ways:

  - Runs approved Change Controls immediately if sufficient privileges are set for the **Change Control Management** permission.
  - Stops the change automatically if an action fails.
  - Runs actions in progress until complete.

- On the failed Change Control details screen, click **Rerun** to repeat the execution of a completed but failed Change Control. This creates a new Change Control that must be approved again.

Figure 14-14: Rerun Change Control



Change Control > Change 20200811_124722

Status	Approver	Started	Last Editor	Devices
Failed	cvpadmin	Aug 11, 2020 22:17:51	cvpadmin	6 affected

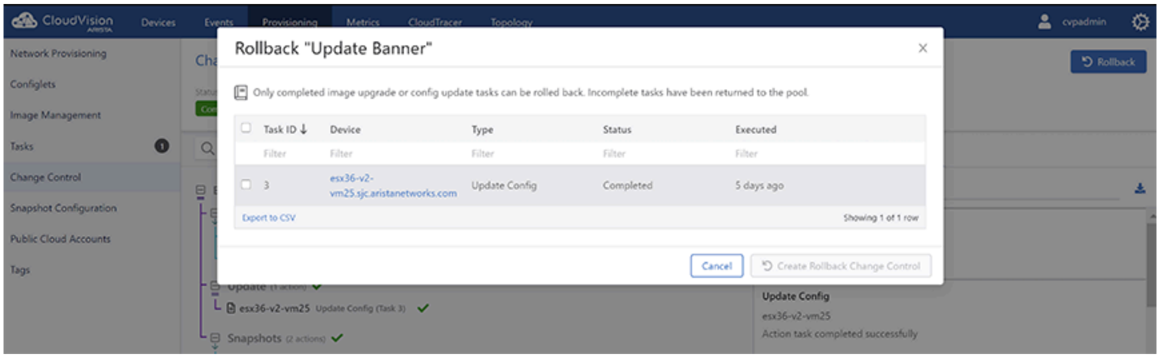
Remove all actions for devices that have no failures? Keep Remove

Change 20200811_124722 Root (6 actions) ✗
- in332 Update Config (Task 42334) ✓
- cal152 Update Config (Task 42335) ✓
- cal154 Update Config (Task 42336) ✗
- fm216 Update Config (Task 42337) ✓
- ld355 Update Config (Task 42338) ✓
- fm212 Update Config (Task 42339) ✓

Note: Click **Remove** when CVP prompts you with **Remove all actions for devices that have no failures?** for skipping the rerun of completed actions.

- Click **Rollback** in executed Change Controls to open the Rollback *Change Control* pop-up window. To create a rollback after evaluating the executed Change Control, select tasks to rollback from the table and click **Create Rollback Change Control**.

Figure 14-15: Rollback Pop-Up Window



Rollback "Update Banner"

Only completed image upgrade or config update tasks can be rolled back. Incomplete tasks have been returned to the pool.

□	Task ID ↓	Device	Type	Status	Executed
	Filter	Filter	Filter	Filter	Filter
□	3	esx36-v2-vm25.sjc.aristanetworks.com	Update Config	Completed	5 days ago

Export to CSV — Showing 1 of 1 row

Update (1 action) ✓
- esx36-v2-vm25 Update Config (Task 3) ✓

Snapshots (2 actions) ✓

Update Config
esx36-v2-vm25
Action task completed successfully

Note: CVP rolls back only completed configuration updates and image upgrade tasks.

Main Panel

This main panel consists of the following entities:

- Search bar - Enter a string to perform a search in the Change Control tree.
- Expand icon - Click to expand all stages.
- Collapse icon - Click to collapse all stages.
- Information icon - Click to get help on Change Control.
- Change Control tree - Change Controls are composed of actions and stages. Action types include tasks, CLI snapshots, health checks, custom scripts, enter BGP maintenance mode, and exit BGP maintenance mode, and other custom actions.

Note: Different icons represent various task types like adding a new device, updating configuration on a device, and updating software image bundle on a device. Actions are represented with a bolt symbol.

Actions are grouped and nested within stages via drag and drop.

Note:

- Tasks being executed in parallel do not block subsequent actions in that branch.
- In a series execution, the Change Control execution starts from the first item and works its way from top to bottom. The next action starts only when the previous action completed successfully.
- You can toggle the option by clicking the stage type dropdown menu in the edit panel.

Edit Panel

This panel edits stages and actions.

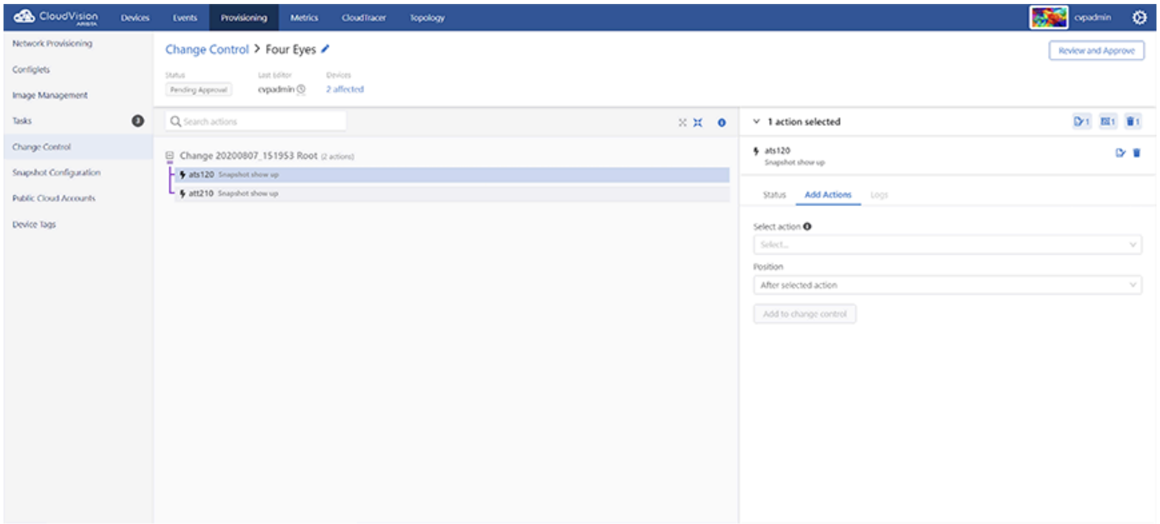
- Edit a stage - Click the required stage in the main panel. The edit panel provides the following options:
  - Show details icon - Click to view associated configuration differences, image bundle changes, and action details.
  - Remove icon - Click to delete the stage.

    > **Note:** Select multiple tasks to view details and delete multiple tasks simultaneously. Use **command**-click or **Ctrl**-click to select multiple items. To select a range of items, click the first item and then **Shift**-click the last item.
  - Group icon - Select multiple tasks to group them into sub-stages.
  - Edit icon - Click to edit the stage name.
  - Change Control stage type dropdown menu - Click to select the Change Control stage type.

    > **Note:** By default, all tasks and actions execute in series.
  - Plus icon - Click to add a child stage.
  - Status - Displays telemetry of each device in the stage.

    > **Note:**
    >
    > - Hover the cursor on ***n* metric group** to view selected devices.
    >
    >   > **Note:** *n* represents the count of selected metric groups.
    > - Hover the cursor on ***n* device(s)** to view selected metric groups.
    >
    >   > **Note:** *n* represents the count of selected devices.
  - Add actions - Adds actions to open Change Control. Select the required action and placement from corresponding dropdown menus; and click **Add to change control** to update selected changes.

Figure 14-16: Add Actions to Change Control



Status: Pending Approval
Last Editor: cvpadmin
Devices: 2 affected

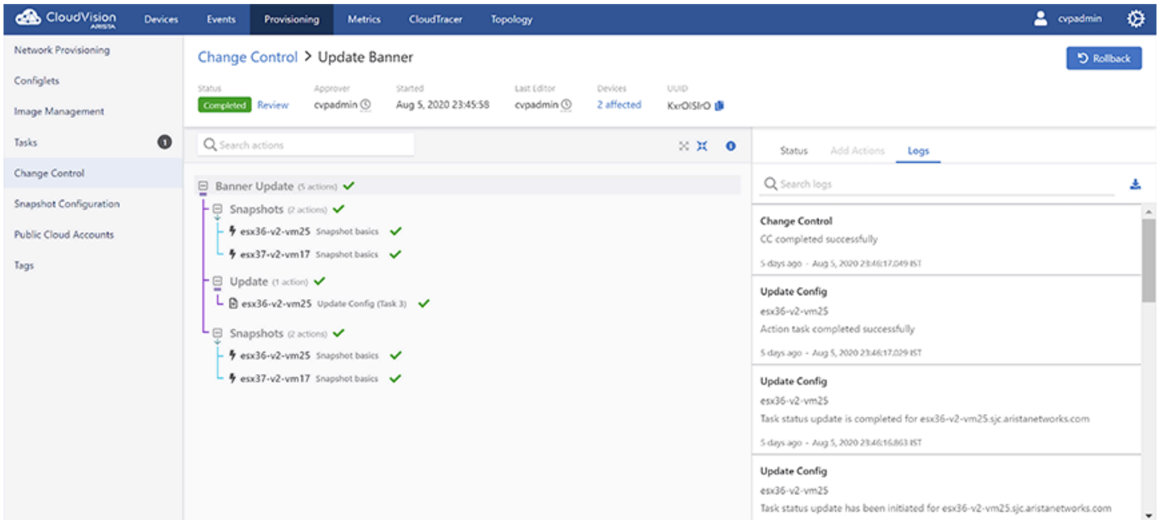
Change 20200807_151953 Root (2 actions)
ats120 Snapshot show up
att210 Snapshot show up

ats120
Snapshot show up

Position: After selected action

- **Logs** - Displays logs of each update in the executed Change Control process.

Figure 14-17: Change Control Logs



Change Control > Update Banner

Status: Completed Review
Approver: cvpadmin
Started: Aug 5, 2020 23:45:58
Last Editor: cvpadmin
Devices: 2 affected
UUID: KxrOlSlrO

Banner Update (5 actions) ✓
- Snapshots (2 actions) ✓
  - esx36-v2-vm25 Snapshot basics ✓
  - esx37-v2-vm17 Snapshot basics ✓
- Update (1 action) ✓
  - esx36-v2-vm25 Update Config (Task 3) ✓
- Snapshots (2 actions) ✓
  - esx36-v2-vm25 Snapshot basics ✓
  - esx37-v2-vm17 Snapshot basics ✓

```
Change Control
CC completed successfully
5 days ago - Aug 5, 2020 23:46:17.049 IST

Update Config
esx36-v2-vm25
Action task completed successfully
5 days ago - Aug 5, 2020 23:46:17.029 IST

Update Config
esx36-v2-vm25
Task status update is completed for esx36-v2-vm25.sjc.aristanetworks.com
5 days ago - Aug 5, 2020 23:46:16.863 IST

Update Config
esx36-v2-vm25
Task status update has been initiated for esx36-v2-vm25.sjc.aristanetworks.com
```

Note:

- Use the search logs bar for filtering logs based on a string.
- Click the download icon to download logs to your local drive.

14.3.3 Creating Change Controls from the Change Controls Summary Screen

The first step involved in using the **Change Control** module to manage tasks is to create a Change Control. While creating a Change Control, you add tasks with pending or failed status to the Change Control. By default, all tasks in the same Change Control are added in parallel. If you want to change the execution order, you can drag and drop the action cards on the **Change Control Details** screen. You can execute grouped tasks after a Change Control is created, reviewed, and approved.

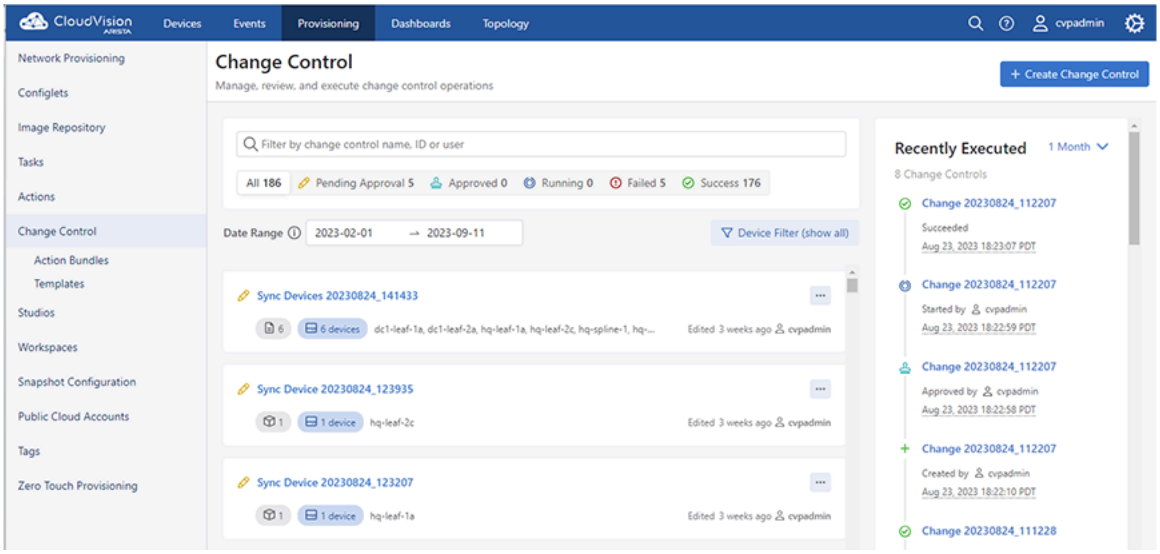
Note: If you do not add any tasks, the system creates a Change Control without tasks.

Complete the following steps to create a Change Control from the **Change Control Summary** screen:

1. On the CloudVision Portal, click **Provisioning > Change Control**.

The system displays the **Change Control Summary** screen.

Figure 14-18: Change Control Summary Screen



Change Control

Manage, review, and execute change control operations

Date Range 2023-02-01 → 2023-09-11

Sync Devices 20230824_141433

6 | 6 devices | dc1-leaf-1a, dc1-leaf-2a, hq-leaf-1a, hq-leaf-2c, hq-spline-1, hq-... | Edited 3 weeks ago cvpadmin

Sync Device 20230824_123935

1 | 1 device | hq-leaf-2c | Edited 3 weeks ago cvpadmin

Sync Device 20230824_123207

1 | 1 device | hq-leaf-1a | Edited 3 weeks ago cvpadmin

Recently Executed

8 Change Controls

Change 20230824_112207
Succeeded
Aug 23, 2023 18:23:07 PDT

Change 20230824_112207
Started by cvpadmin
Aug 23, 2023 18:22:59 PDT

Change 20230824_112207
Approved by cvpadmin
Aug 23, 2023 18:22:58 PDT

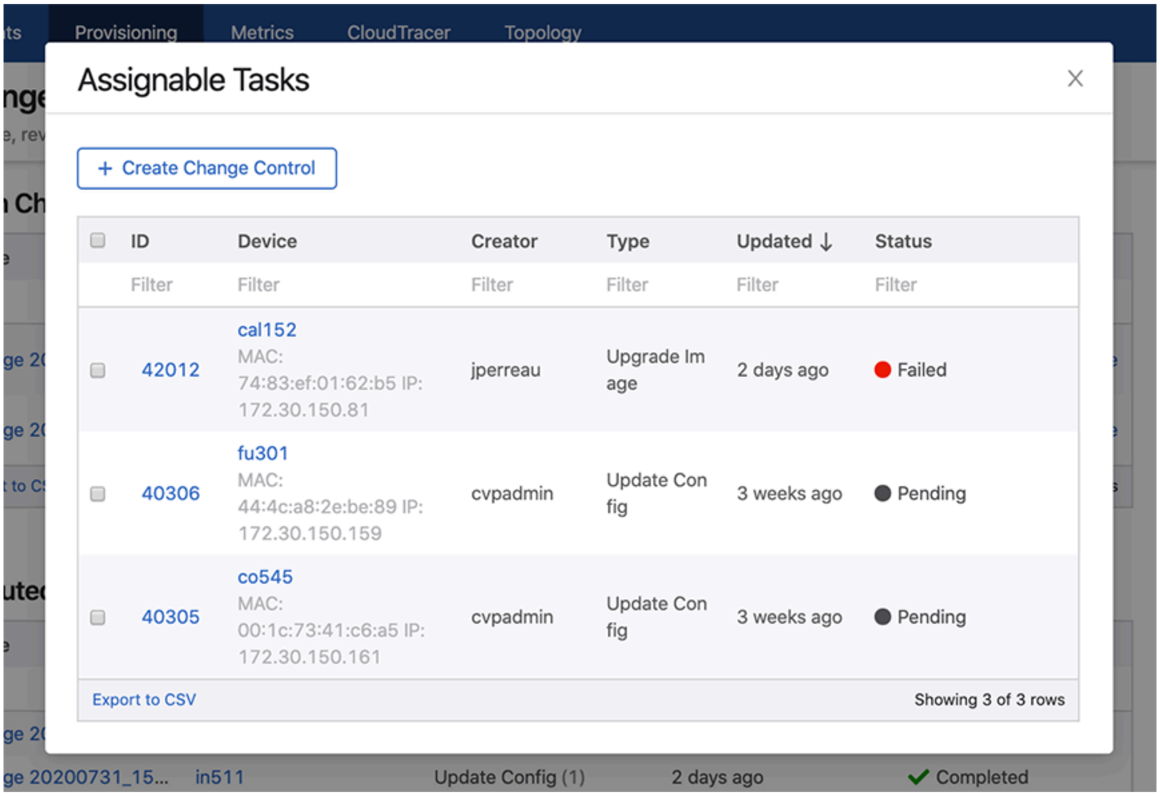
Change 20230824_112207
Created by cvpadmin
Aug 23, 2023 18:22:10 PDT

Change 20230824_111228

2. Click **+ Create Change Control** button at the upper right corner.

   The system displays the **Assignable Tasks** dialog box.

   Figure 14-19: Assignable Tasks Dialog Box with No Tasks Selected



Assignable Tasks

☐	ID	Device	Creator	Type	Updated ↓	Status
	Filter	Filter	Filter	Filter	Filter	Filter
☐	42012	cal152 MAC: 74:83:ef:01:62:b5 IP: 172.30.150.81	jperreau	Upgrade Image	2 days ago	● Failed
☐	40306	fu301 MAC: 44:4c:a8:2e:be:89 IP: 172.30.150.159	cvpadmin	Update Config	3 weeks ago	● Pending
☐	40305	co545 MAC: 00:1c:73:41:c6:a5 IP: 172.30.150.161	cvpadmin	Update Config	3 weeks ago	● Pending

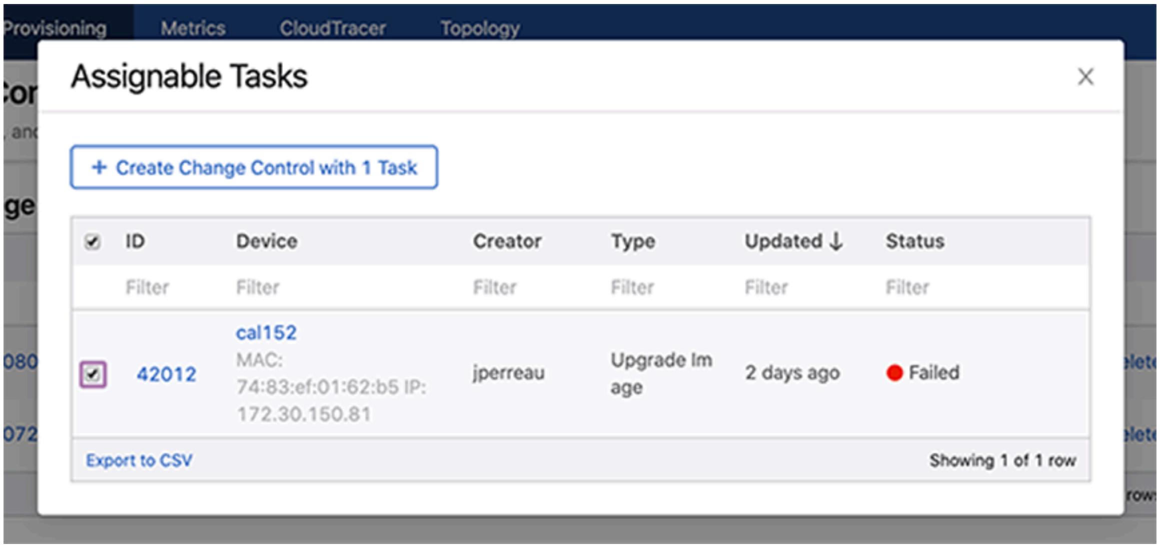
Showing 3 of 3 rows

3. Select tasks you want to include in the Change Control by selecting appropriate checkboxes.

   Note: If you do not select any tasks, the system creates a Change Control without tasks.

4. Click **+ Create Change Control** with n tasks where n is the count of selected tasks.

Figure 14-20: Assignable Tasks Dialog Box with Tasks Selected



Assignable Tasks

☑	ID	Device	Creator	Type	Updated ↓	Status
	Filter	Filter	Filter	Filter	Filter	Filter
☑	42012	cal152 MAC: 74:83:ef:01:62:b5 IP: 172.30.150.81	jperreau	Upgrade Image	2 days ago	● Failed

Showing 1 of 1 row

The system displays the appropriate **Change Control Details** screen.

14.3.4 Accessing the Open Change Control Details Screen

The open Change Control details screen performs the following functions:

- Displays Change Control information
- Adds actions to Change Control
- Adds, edits, and deletes child stages
- Reviews and approves Change Control

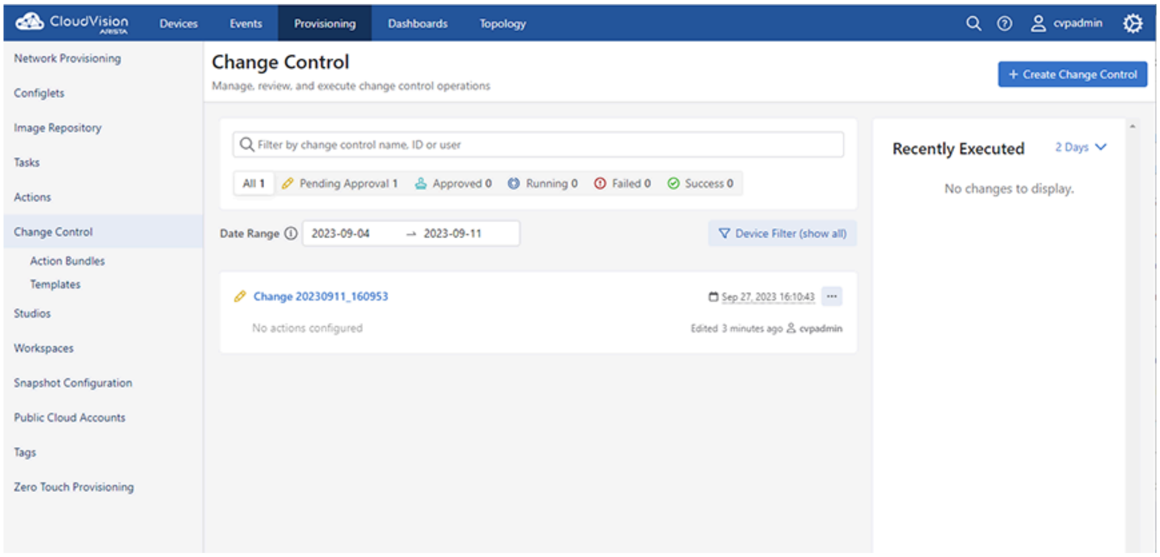
Perform the following steps to access the Change Control details screen:

1. On the CloudVision Portal, click **Provisioning** > **Change Control**.

   The system displays the Change Control summary screen.
2. Under the **Open Change Controls** table, click one of the listed Change Controls.

The system displays the Change Control details screen.

Figure 14-21: Change Control Details Screen



Date Range 2023-09-04 → 2023-09-11

Change 20230911_160953 — Sep 27, 2023 16:10:43

No actions configured — Edited 3 minutes ago cvpadmin

The Change Control details screen consists of the following panels:

- Header Panel
- Main Panel
- Edit Panel

Header Panel

This primary panel provides the following basic information on the Change Control:

- Edit icon to update the Change Control name
- Change Control information -
  - The open Change Control details screen displays the status, scheduled date, last editor, count of affected devices, and Universally Unique Identifier (UUID).

    Note:

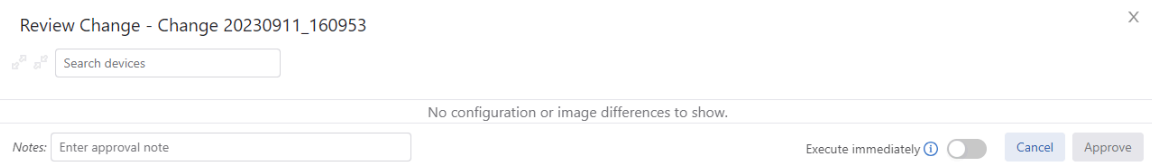
    - Click the **Scheduled for** field and select the date to run the Change Control.
    - Hover the mouse cursor over the clock icon to view the last time of action.
    - Hover the cursor on the count of affected devices to view their list. Clicking on an affected device opens the corresponding Device Overview screen.
    - Clicking the copy icon next to the UUID copies the UUID to the clipboard.
  - The executed Change Control details screen displays the status, approver, time of start, last editor, and count of affected devices.

    Note:

    - Click **Review** next to the status for details on review and approve process.

- **Review and Approve** - Click **Review and Approve** in open Change Controls for assessing Change Control updates. These updates include configuration differences, and image bundle changes when appropriate.

  Figure 14-22: Review and Approve Pop-Up Window

  Review Change - Change 20230911_160953

  Search devices

  No configuration or image differences to show.

  Notes: Enter approval note

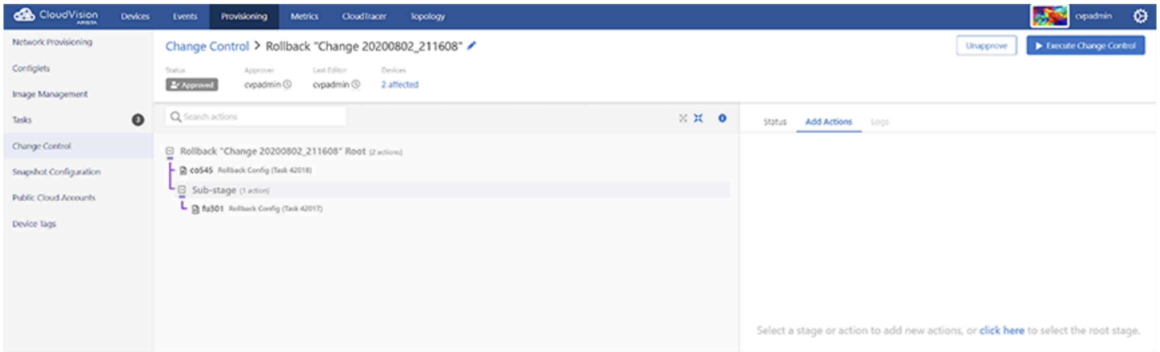
  Execute immediately

  Click **Approve** to accept Change Control updates.

  > **Note:** (Optional) Approver can leave comments in the ***Notes:*** field.

- On the approved Change Control details screen, click **Unapprove** to revert the approval status and **Execute Change Control** to run approved Change Controls.

  Figure 14-23: Approved Change Control

  Change Control > Rollback "Change 20200802_211608"

  Status: Approved | Approver: cvpadmin | Last Editor: cvpadmin | Devices: 2 affected

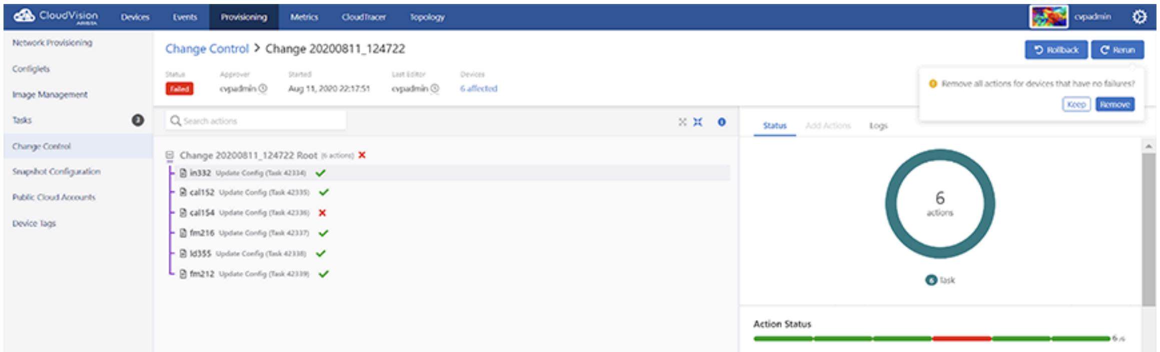
  Rollback "Change 20200802_211608" Root (2 actions)
  - co545 Rollback Config (Task 42018)
  - Sub-stage (1 action)
    - fu301 Rollback Config (Task 42017)

  Select a stage or action to add new actions, or click here to select the root stage.

  > **Note:** CVP executes Change Controls in the following ways:
  >
  > - Runs approved Change Controls immediately if sufficient privileges are set for the **Change Control Management** permission.
  > - Stops the change automatically if an action fails.
  > - Runs actions in progress until complete.

- On the failed Change Control details screen, click **Rerun** to repeat the execution of a completed but failed Change Control. This creates a new Change Control that must be approved again.

  Figure 14-24: Rerun Change Control

  Change Control > Change 20200811_124722

  Status: Failed | Approver: cvpadmin | Started: Aug 11, 2020 22:17:51 | Last Editor: cvpadmin | Devices: 6 affected

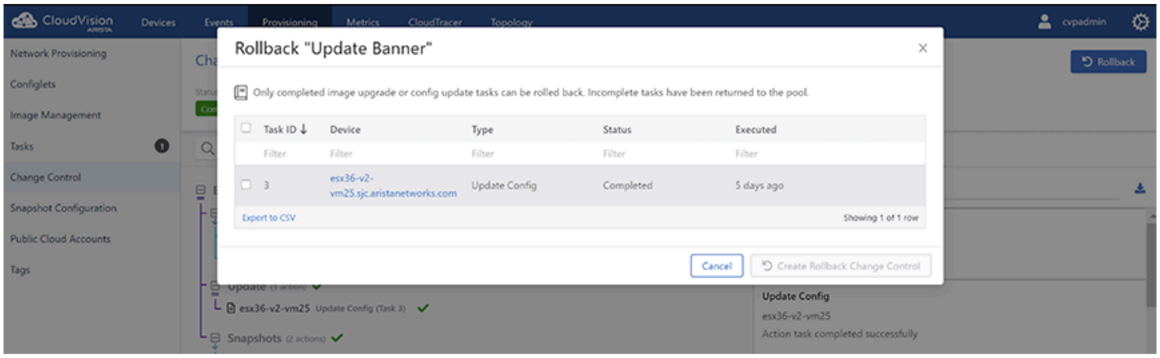
  Change 20200811_124722 Root (6 actions) ✗
  - in332 Update Config (Task 42334) ✓
  - cal152 Update Config (Task 42335) ✓
  - cal154 Update Config (Task 42336) ✗
  - fm216 Update Config (Task 42337) ✓
  - ld355 Update Config (Task 42338) ✓
  - fm212 Update Config (Task 42339) ✓

  Remove all actions for devices that have no failures?

  > **Note:** Click **Remove** when CVP prompts you with **Remove all actions for devices that have no failures?** for skipping the rerun of completed actions.

- Click **Rollback** in executed Change Controls to open the Rollback *Change Control* pop-up window. To create a rollback after evaluating the executed Change Control, select tasks to rollback from the table and click **Create Rollback Change Control**.

Figure 14-25: Rollback Pop-Up Window



Rollback "Update Banner"

Only completed image upgrade or config update tasks can be rolled back. Incomplete tasks have been returned to the pool.

□	Task ID	Device	Type	Status	Executed
	Filter	Filter	Filter	Filter	Filter
□	3	esx36-v2-vm25.sjc.aristanetworks.com	Update Config	Completed	5 days ago

Export to CSV

Showing 1 of 1 row

Cancel

Create Rollback Change Control

Update Config

esx36-v2-vm25

Action task completed successfully

Note: CVP rolls back only completed configuration updates and image upgrade tasks.

Main Panel

This main panel consists of the following entities:

- Search bar - Enter a string to perform a search in the Change Control tree.
- Expand icon - Click to expand all stages.
- Collapse icon - Click to collapse all stages.
- Information icon - Click to get help on Change Control.
- Change Control tree - Change Controls are composed of actions and stages. Action types include tasks, CLI snapshots, health checks, custom scripts, enter BGP maintenance mode, and exit BGP maintenance mode, and other custom actions.

  Note: Different icons represent various task types like adding a new device, updating configuration on a device, and updating software image bundle on a device. Actions are represented with a bolt symbol.

  Actions are grouped and nested within stages via drag and drop.

  Note:

  - Tasks being executed in parallel do not block subsequent actions in that branch.
  - In a series execution, the Change Control execution starts from the first item and works its way from top to bottom. The next action starts only when the previous action completed successfully.
  - You can toggle the option by clicking the stage type dropdown menu in the edit panel.

Edit Panel

This panel edits stages and actions.

- Edit a stage - Click the required stage in the main panel. The edit panel provides the following options:
  - Show details icon - Click to view associated configuration differences, image bundle changes, and action details.
  - Remove icon - Click to delete the stage.

    Note: Select multiple tasks to view details and delete multiple tasks simultaneously. Use **command**-click or **Ctrl**-click to select multiple items. To select a range of items, click the first item and then **Shift**-click the last item.
  - Group icon - Select multiple tasks to group them into sub-stages.

- Edit icon - Click to edit the stage name.
- Change Control stage type dropdown menu - Click to select the Change Control stage type.

  Note: By default, all tasks and actions execute in series.

- Plus icon - Click to add a child stage.
- Status - Displays telemetry of each device in the stage.

  Note:

  - Hover the cursor on ***n* metric group** to view selected devices.

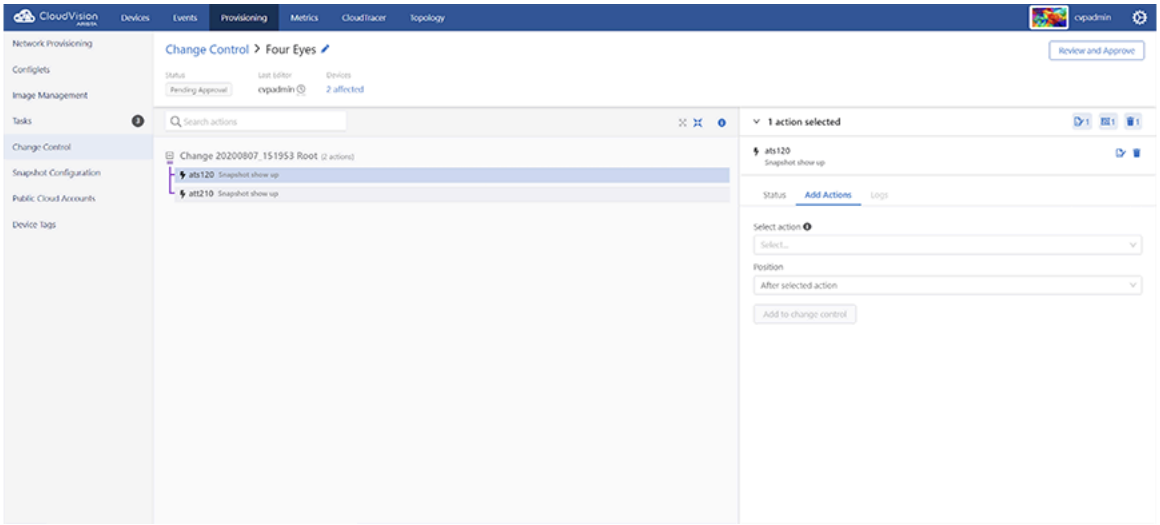
    Note: *n* represents the count of selected metric groups.

  - Hover the cursor on ***n* device(s)** to view selected metric groups.

    Note: *n* represents the count of selected devices.

- Add actions - Adds actions to open Change Control. Select the required action and placement from corresponding dropdown menus; and click **Add to change control** to update selected changes.

  Figure 14-26: Add Actions to Change Control



Change Control > Four Eyes

Status: Pending Approval
Last Editor: cvpadmin
Devices: 2 affected

Change 20200807_151953 Root (2 actions)
- ats120 Snapshot show up
- att210 Snapshot show up

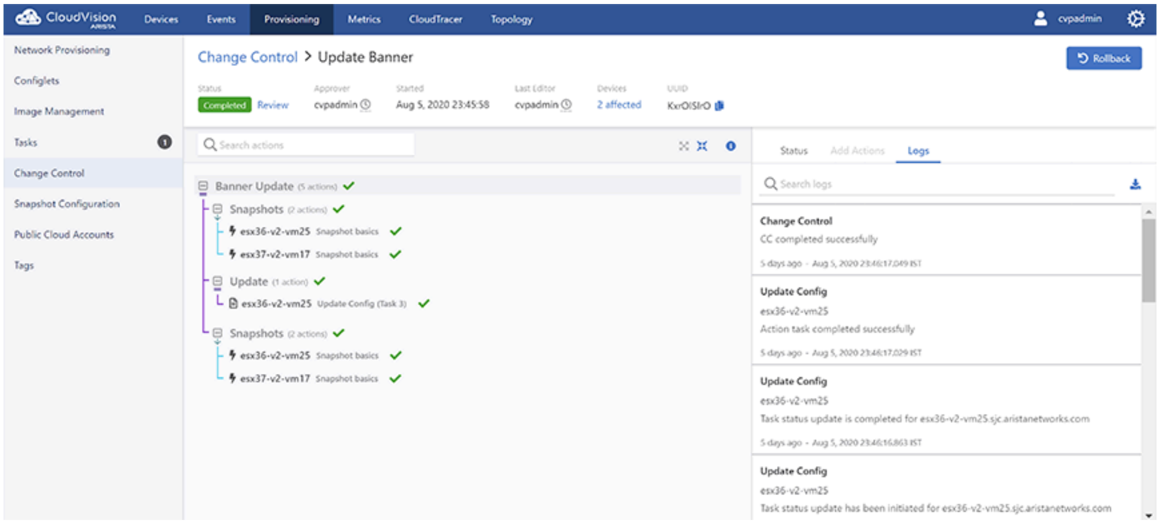
1 action selected

ats120
Snapshot show up

Select action: Select...
Position: After selected action

- **Logs** - Displays logs of each update in the executed Change Control process.

Figure 14-27: Change Control Logs



Change Control > Update Banner

Status: Completed Review
Approver: cvpadmin
Started: Aug 5, 2020 23:45:58
Last Editor: cvpadmin
Devices: 2 affected
UUID: KxrOISlrO

Banner Update (5 actions) ✓
Snapshots (2 actions) ✓
esx36-v2-vm25 Snapshot basics ✓
esx37-v2-vm17 Snapshot basics ✓
Update (1 action) ✓
esx36-v2-vm25 Update Config (Task 3) ✓
Snapshots (2 actions) ✓
esx36-v2-vm25 Snapshot basics ✓
esx37-v2-vm17 Snapshot basics ✓

Change Control
CC completed successfully
5 days ago - Aug 5, 2020 23:46:17.049 IST

Update Config
esx36-v2-vm25
Action task completed successfully
5 days ago - Aug 5, 2020 23:46:17.029 IST

Update Config
esx36-v2-vm25
Task status update is completed for esx36-v2-vm25.sjc.aristanetworks.com
5 days ago - Aug 5, 2020 23:46:16.863 IST

Update Config
esx36-v2-vm25
Task status update has been initiated for esx36-v2-vm25.sjc.aristanetworks.com

Note:

- Use the search logs bar for filtering logs based on a string.
- Click the download icon to download logs to your local drive.

14.3.4.1 Change Control Drop-Down Menu

Click the Change Control drop-down menu to select another Change Control.

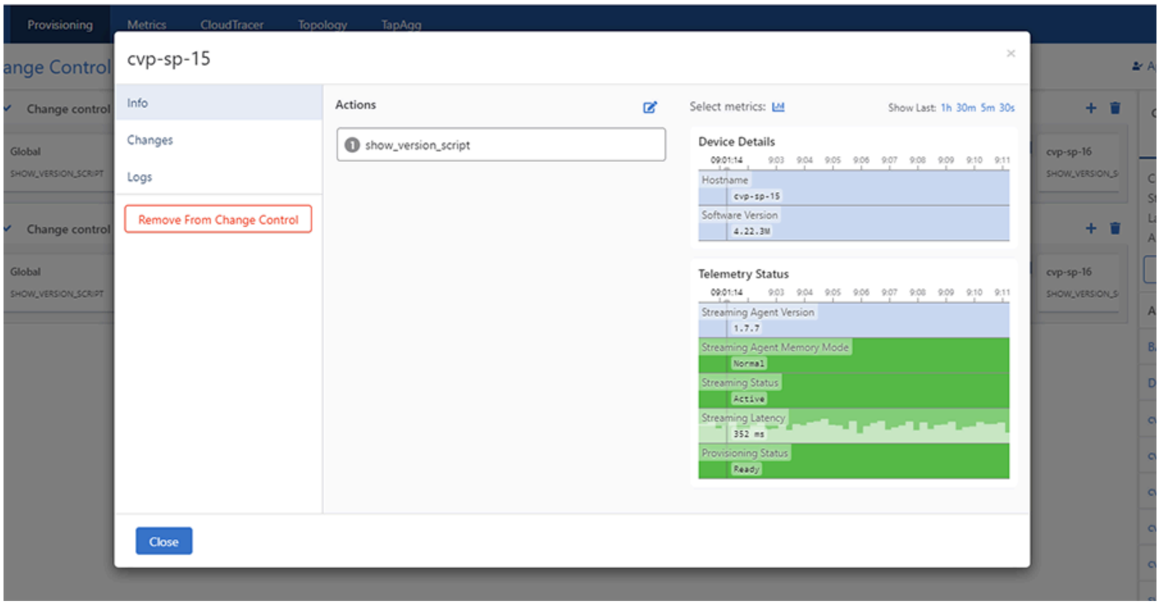
14.3.4.2 Change Control Stages

These panes consists of the following entities:

- Change Control stage name - Click either the Change Control name or the corresponding edit icon to update the name.
- Add a stage icon - Click the plus icon at the upper right corner of the stage to add a stage.
- Delete a stage icon - Click the appropriate trash icon at the upper right corner of the stage to delete the corresponding stage.
- Edit actions icon - Click the thunder icon within a card to edit or view the appropriate leaf.

- For open Change Controls, the system displays the actions window to edit the appropriate leaf.

Figure 14-28: Info Tab in Edit Actions



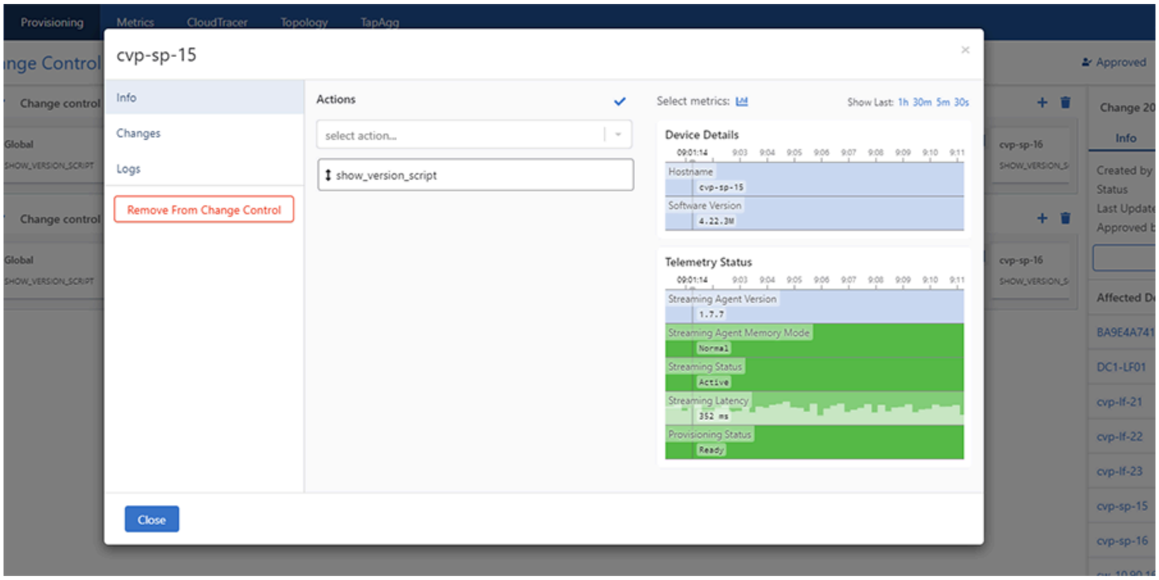
Note: For completed Change Controls, the system displays the actions window to view the appropriate leaf.

This window consists of the following entities:

- **Info** tab **-** This tab lists the actions to be run, edits actions, and displays action details.

  Click the edit icon to reorder and edit actions.

  Figure 14-29: Reorder and Edit Actions Screen

  - Click the select action drop-down menu and select the required action.

    Note: The system displays selected actions beneath the select action drop-down menu.

  - Click **Clear** at the end of a field to delete the appropriate action.

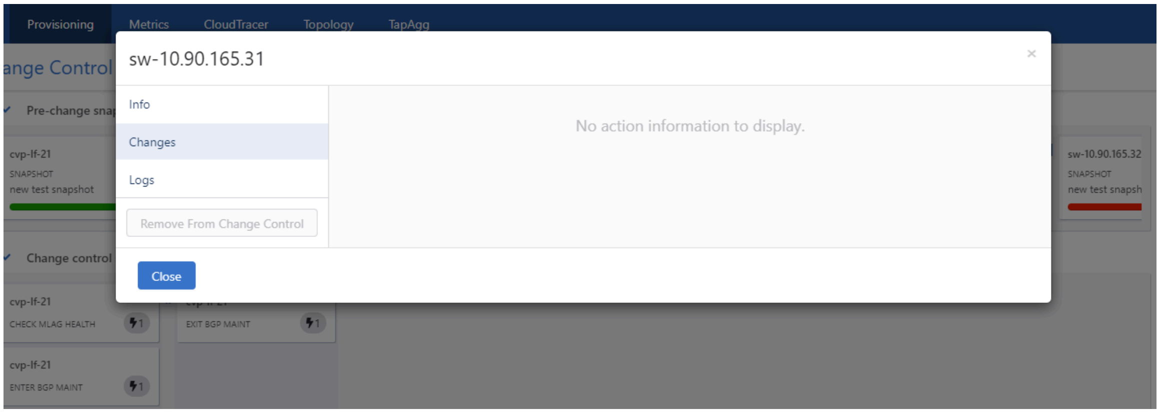
> **Note:** This option is available only for a card with multiple actions. The main action in a card is not available to clear.

- Click the check-mark to save changes.

> **Note:** Here, actions comprise of provisioning, Border Gateway Protocol (BGP) maintenance, health checks, and snapshots.

- **Configuration Changes** tab - For tasks, this tab displays any configuration or image differences that will be applied as part of the task.

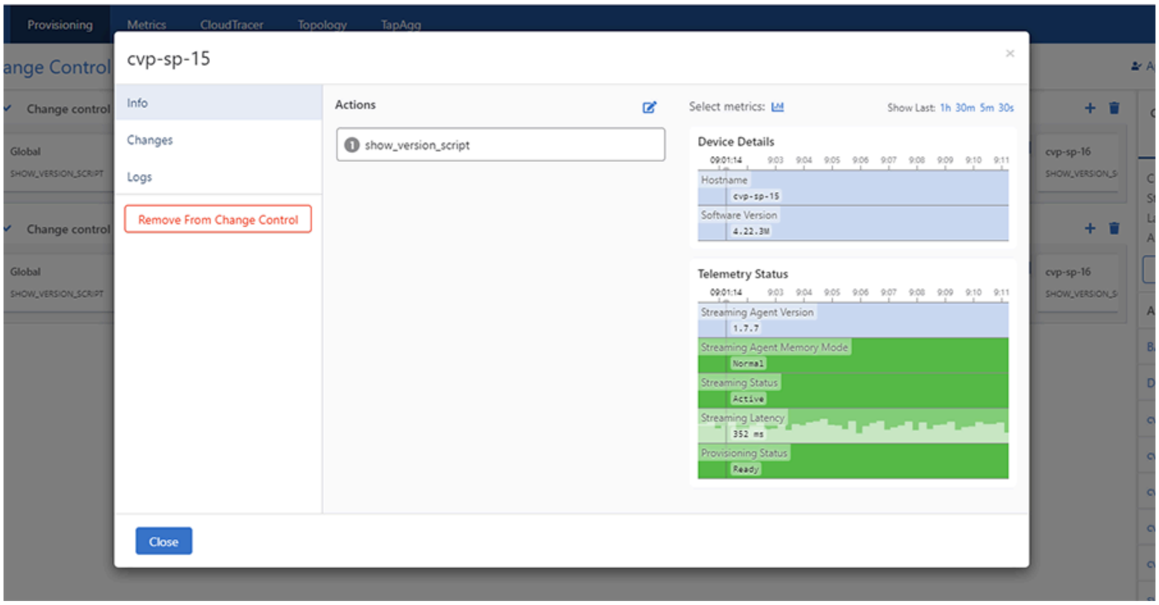
  Figure 14-30: Configuration Changes Tab in Edit Actions



No action information to display.

- **Logs** tab - This tab displays log information of completed Change Controls.

  Figure 14-31: Logs Tab in Edit Actions



Hostname: cvp-sp-15
Software Version: 4.22.3M
Streaming Agent Version: 1.7.7
Streaming Agent Memory Mode: Normal
Streaming Status: Active
Streaming Latency: 352 ms
Provisioning Status: Ready

- **Remove from Change Control** button - Click Remove from Change Control to remove this task from the stage.

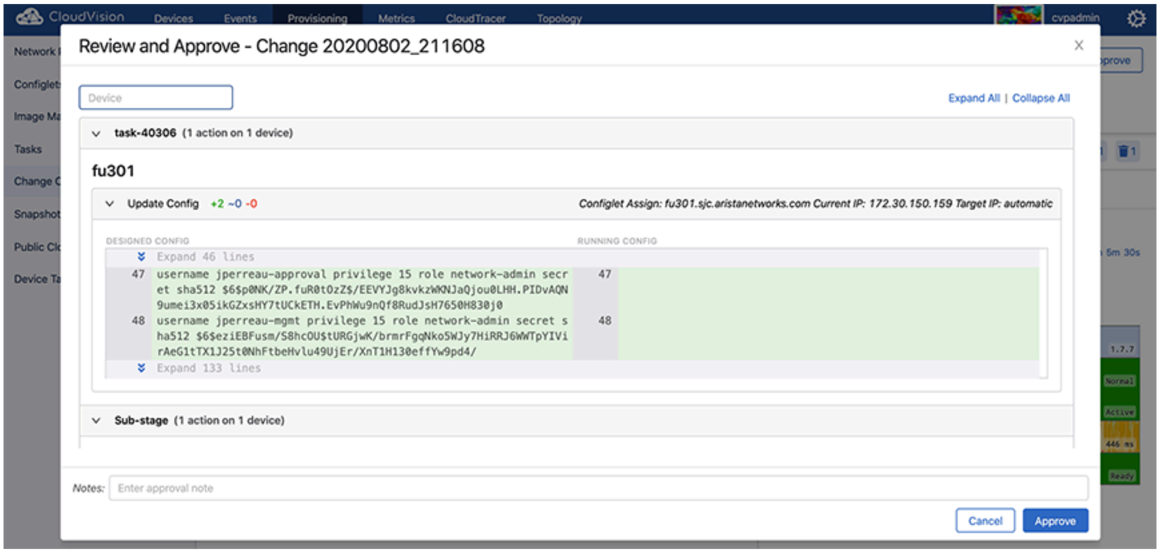
  > **Note:** Click **Remove** on the **Confirm** pop-up dialog box to confirm the deletion.

  - **Done** button - Click **Done** to save changes.
- Trashbin icon - Click the trashbin icon at the upper right corner of the pane to delete the stage.

14.3.4.3 Review and Approve

Click the **Review** and **Approve** button at the upper right corner of the Change Control screen to review and approve the Change Control. This button displays the **Review and Approve** dialog box for the selected Change Control.

Figure 14-32: Review and Approve Dialog Box



Review and Approve - Change 20200802_211608

task-40306 (1 action on 1 device)

fu301

Update Config +2 ~0 -0   *Configlet Assign: fu301.sjc.aristanetworks.com Current IP: 172.30.150.159 Target IP: automatic*

```
DESIGNED CONFIG                                                  RUNNING CONFIG
     Expand 46 lines
 47  username jperreau-approval privilege 15 role network-admin secr   47
     et sha512 $6$p0NK/ZP.fuR0tOzZ$/EEVYJg8kvkzWKNJaQjou0LHH.PIDvAQN
     9umei3x05ikGZxsHY7tUCkETH.EvPhWu9nQf8RudJsH7650H830j0
 48  username jperreau-mgmt privilege 15 role network-admin secret s   48
     ha512 $6$eziEBFusm/S8hcOU$tURGjwK/brmrFgqNko5WJy7HiRRJ6WWTpYIVi
     rAeG1tTX1J25t0NhFtbeHvlu49UjEr/XnT1H130effYw9pd4/
     Expand 133 lines
```

Sub-stage (1 action on 1 device)

Notes: Enter approval note

This window consists of a device search field and a list of changes by Change Control stages.

Type the device name in the search field and if available, the system displays the list of changes for the specified device.

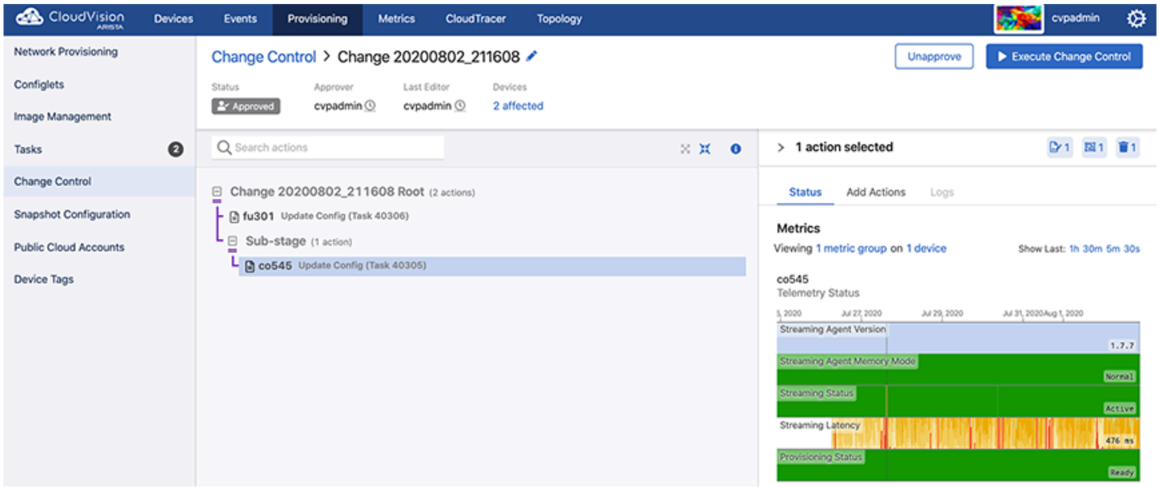
The expanded Change Control stage list displays details of the actions to be executed in each stage, grouped by a device.

If you are happy with configuration changes, click the **Approve** button at the lower right corner of the dialog box to approve the Change Control.

14.3.4.4 Execute Change Control

After approval, the **Review and Approve** button is replaced with the Execute Change Control button.

Figure 14-33: Execute Change Control Button



Change Control > Change 20200802_211608

Status: Approved | Approver: cvpadmin | Last Editor: cvpadmin | Devices: 2 affected

Change 20200802_211608 Root (2 actions)
- fu301 Update Config (Task 40306)
- Sub-stage (1 action)
  - co545 Update Config (Task 40305)

1 action selected

Metrics

Viewing 1 metric group on 1 device   Show Last: 1h 30m 5m 30s

co545
Telemetry Status

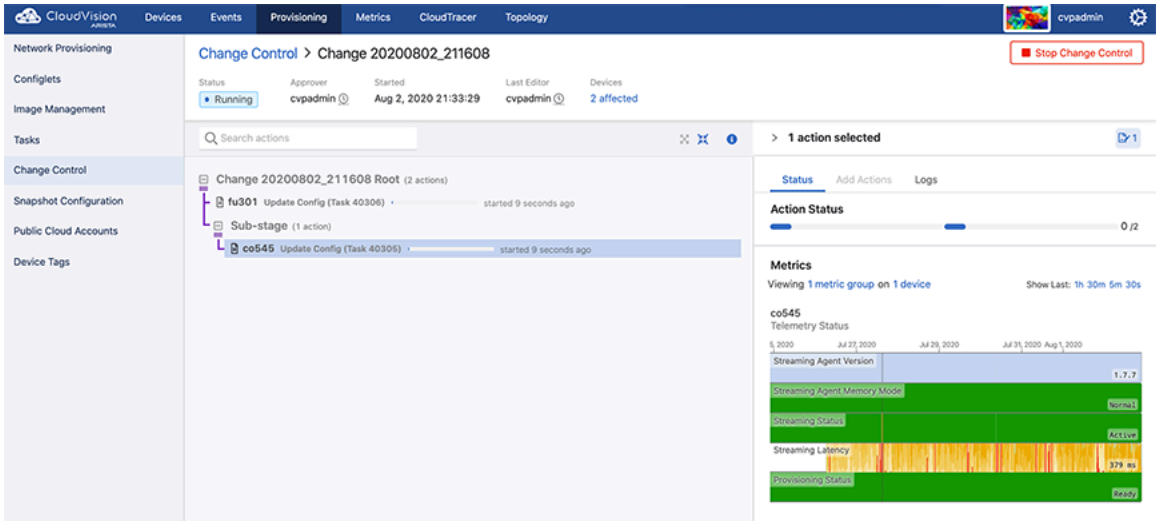
Click the **Execute Change Control** button to execute the Change Control.

Note: A Change Control is executed until all actions are either completed or there is a failure in one or more of the actions.

14.3.4.5 Stop Change Control

While the system is executing changes specified in Change Control, it replaces the **Execute Change Control** button with the **Stop Change Control** button.

Figure 14-34: Stop Change Control Button

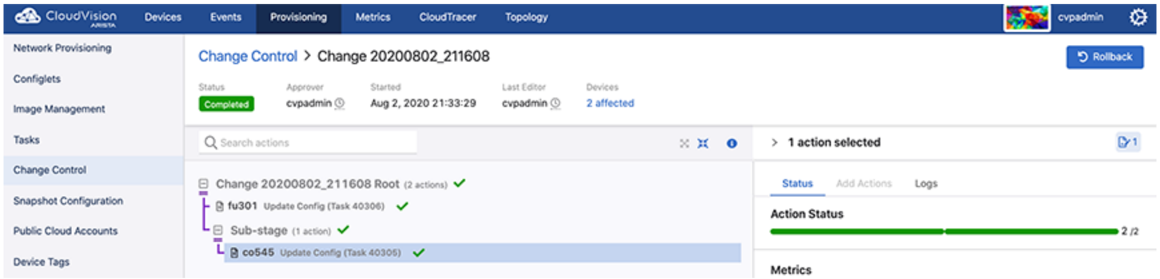


Click the **Stop Change Control** button to stop the execution of Change Control.

Note: Clicking the **Stop Change Control** button returns failed and incomplete tasks to the assignable tasks pool for reallocation.

If a Change Control has revertible actions, the system replaces the Stop Change Control button with the **Rollback Change** button after the execution of all actions.

Figure 14-35: Rollback Change Button



Click the **Rollback Change** button to rollback the execution of Change Control.

14.4 Non-Author Change Control Review

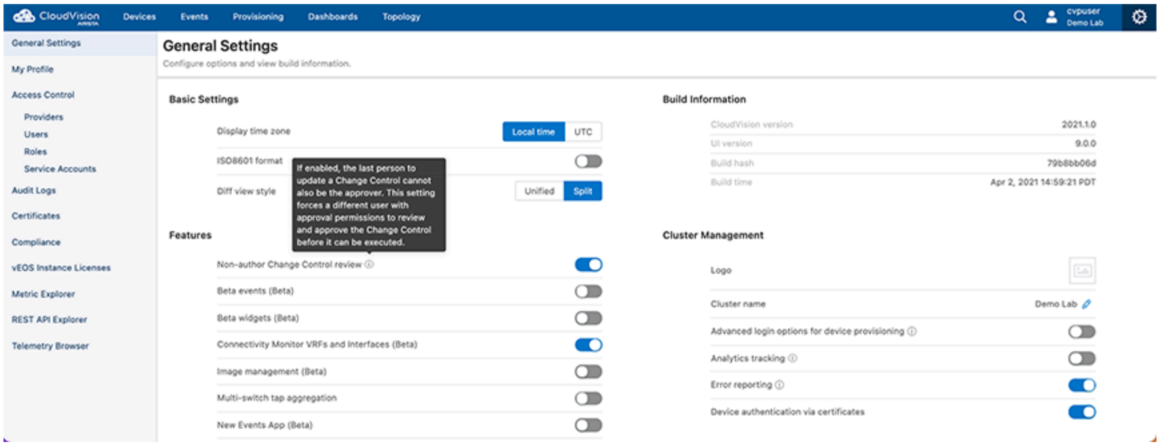
The non-author change control review feature enforces change control reviews by someone other than the author. This ensures that two separate people have reviewed a change before it is approved and can be rolled out onto the network.

Enabling Non-Author Change Control Review

Note: This feature can only be enabled from the **Cluster Management** role.

From the **General Settings** menu, select the **Non-author Change Control review** toggle to enable the feature.

Figure 14-36: Enabling Non-Author Change Control Review



General Settings

Configure options and view build information.

Basic Settings

- Display time zone: Local time (selected) / UTC
- ISO8601 format: off
- Diff view style: Unified / Split (selected)

If enabled, the last person to update a Change Control cannot also be the approver. This setting forces a different user with approval permissions to review and approve the Change Control before it can be executed.

Features

- Non-author Change Control review ⓘ: on
- Beta events (Beta): off
- Beta widgets (Beta): off
- Connectivity Monitor VRFs and Interfaces (Beta): on
- Image management (Beta): off
- Multi-switch tap aggregation: off
- New Events App (Beta): off

Build Information

CloudVision version	2021.1.0
UI version	9.0.0
Build hash	79b8bb06d
Build time	Apr 2, 2021 14:59:21 PDT

Cluster Management

- Logo
- Cluster name: Demo Lab
- Advanced login options for device provisioning ⓘ: off
- Analytics tracking ⓘ: off
- Error reporting ⓘ: on
- Device authentication via certificates: on

Pending and approved changes are displayed in the Change Control screen located in the Provisioning tab.

When the feature is enabled, the user making the change (author) will not be allowed to modify the approval status (approve/disapprove) of their own changes.

14.5 Change Control Template

Change Control Template allows you to build and structure common change control operations, and to repeat them without having to rebuild or re-specify the actions and sequences. The template is easily modified which enables you to execute evolving change control operations quickly and efficiently.

To configure a Change Control Template, use the Action Bundle and Stage Rule tools. Each Stage Rule depends on an Action Bundle for its content, so at least one Action Bundle must be created before you can start using Change Control Templates.

Stage Rules

A Template is defined by a list of Stage Rules. Stage Rules can be executed in Series or Parallel at the root of the change control. Each Stage Rule is linked to one Action Bundle, which supplies the content for that stage.

Action Bundles

An Action Bundle is a specific sequence of actions that contain up to one task action and a limitless number of non-task actions. Action Bundles are reusable across multiple Templates and allow you to construct a specific sequence of actions without defining the tasks or devices that they will be applied to.

Workflow

Creating and implementing a change control event with a Template, requires five basic steps:

1. Create or select one or more Action Bundles.
2. Assign each Action Bundle to a Stage Rule.
3. Configure the Stage Rules of the Template.
4. Save the Template.

5. Apply the Template in Change Control.

Once the Template has been saved, it will be available to apply repeatedly. For future change control operations with the same actions and sequence, you will only need to follow Step 5.

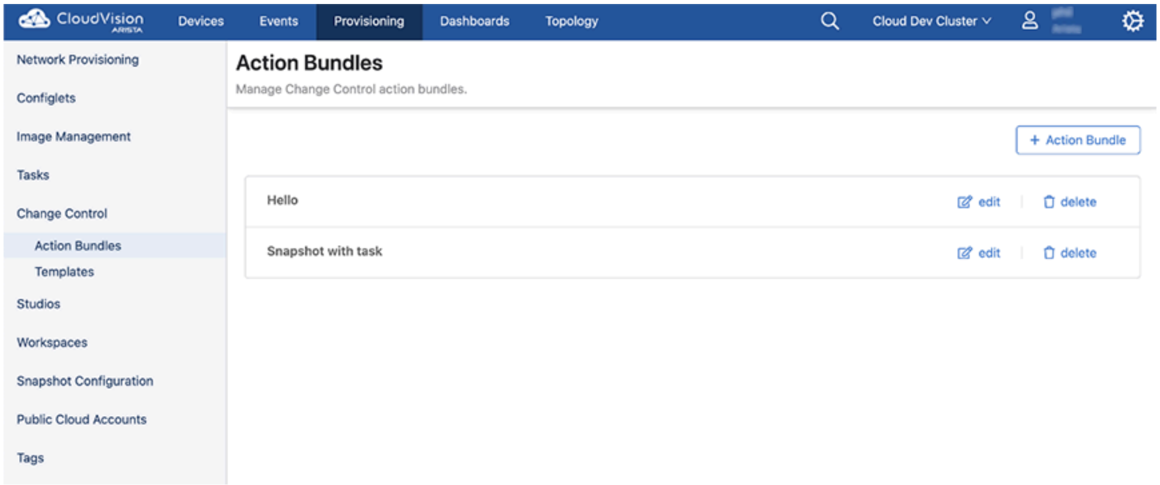
14.5.1 Action Bundles

Action Bundles are a determined sequence of actions that can include up to one task action and an unlimited number of non-task actions. The Action Bundles are assigned them to the Stage Rules of a Template, which means that you will want to create, edit, and delete Action Bundles.

14.5.1.1 Accessing Action Bundles

You can manage Action Bundles by selecting **Provisioning** in the navigation bar and then selecting **Action Bundles**.

Figure 14-37: Action Bundles



Action Bundles

Manage Change Control action bundles.

Hello

Snapshot with task

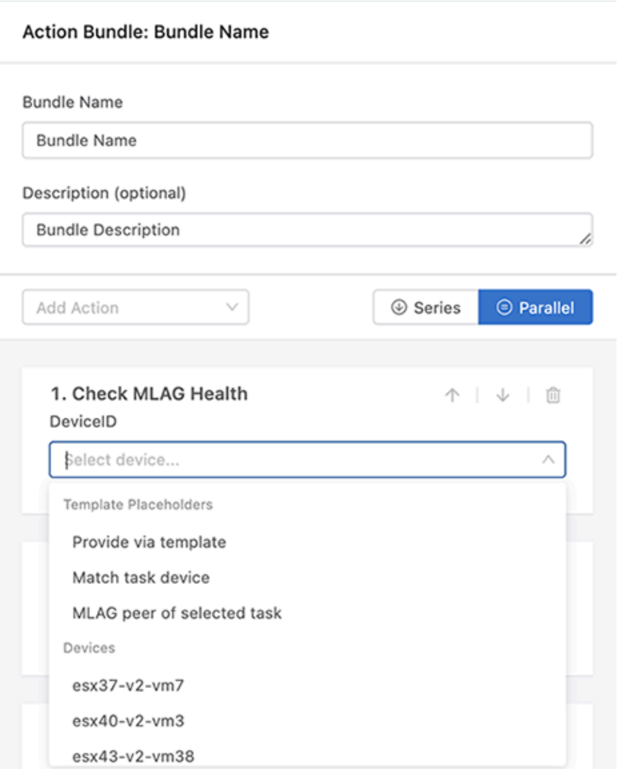
14.5.1.2 Creating a New Action Bundle

When creating a new Action Bundle, one task action and unlimited non-task actions can be added.

1. Click **+ Action Bundle**
2. In the side panel that opens, enter a bundle name and an optional description and then click the **Add Action** menu.

3. Select an action from the available list.

Figure 14-38: Select an Action



Action Bundle: Bundle Name

Bundle Name: Bundle Name

Description (optional): Bundle Description

Note: Every action except for Execute Task is a non-task action. You can only add one task action for each Action Bundle.

4. Depending on the action type selected, you may have some additional options for what devices you can assign the action to.

   Note: The task action will always have its device assigned in the Stage Rule of the Template that the Action Bundle is applied to. For more information on these options, see Device Placeholders and Static Arguments.

5. Select the actions of this Action Bundle to be executed in series or parallel.
6. Review the list of actions, and click **Save**. The Action Bundle will now be available to be assigned in the Stages Rules of Templates.

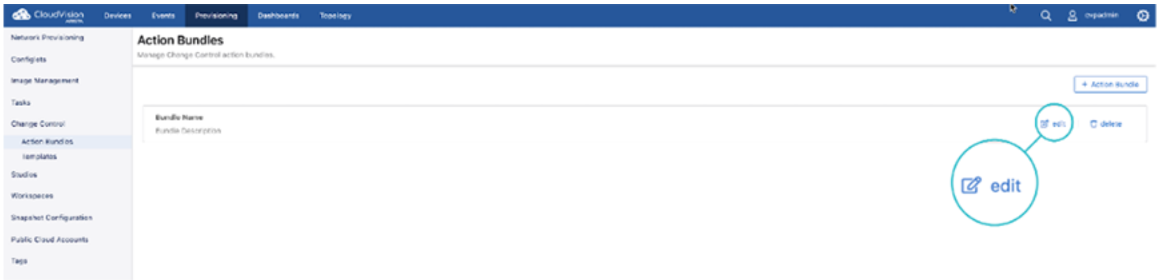
14.5.1.3 Editing an Action Bundle

To edit an Action Bundle.

Note: Upon saving the edits, any template that the Action Bundle is a component of will be updated.

1. Click **Edit** on the Action Bundle to be modified.

Figure 14-39: Editing an Action Bundle



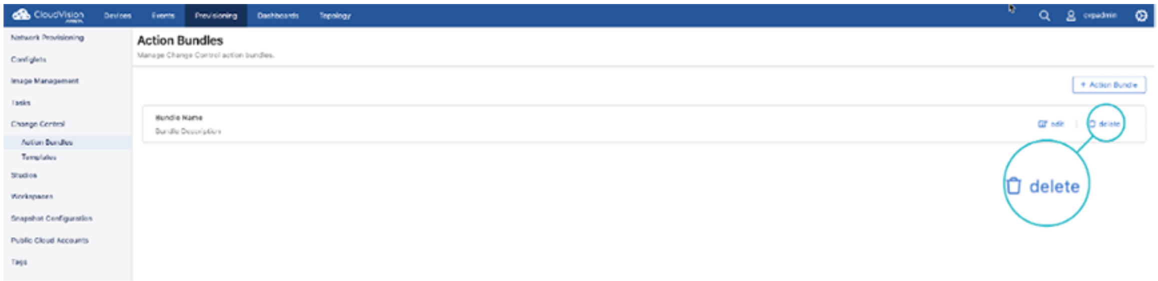
2. From the side panel, add new actions, modify the order of existing actions, or delete existing actions.
3. Click **Save** to update the Action Bundle.

14.5.1.4 Deleting an Action Bundle

Note: The following procedure does not remove the Action Bundle from any assigned Template.

1. Select **Delete**.

Figure 14-40: Deleting an Action Bundle



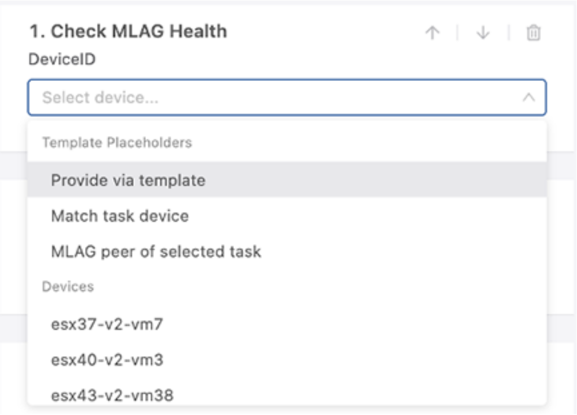
2. A modal that will ask you to cancel or remove. Click **Remove**.

14.5.1.5 Device Placeholders and Static Arguments

When creating or editing the actions of an Action Bundle, you can assign device placeholders instead of specific devices to the action. These placeholders are then defined when the Action Bundle is added to the Stage Rule of a Template. This gives you the flexibility to assign the same Action Bundle to multiple Templates.

The following is a complete list of device placeholders, along with a sample list of devices you can statically apply the action to:

Figure 14-41: Device Placeholders

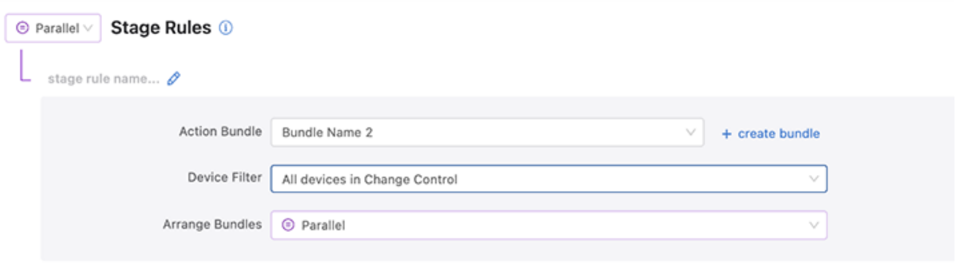


The placeholders available to you vary based upon the combination of action types that you have already selected. Consequently, additional placeholders may become available for an action after you have added more actions to the Action Bundle. Specifically, ‘Match task device’ and ‘MLAG peer of selected task’ only appear when the Action Bundle contains a task.

Provide via Template

When this action is assigned as a placeholder, you will configure it when building the Template. You can use the Device Filter field in the Stage Rule that the Action Bundle is applied to.

Figure 14-42: Provide via Template



Action Bundle: Bundle Name 2

Device Filter: All devices in Change Control

Arrange Bundles: Parallel

Select one of the following options:

- **All Devices in Change Control**: This option matches all devices associated with the change control (defined by which tasks are linked to the change control)
- **Regular Expression**: This option allows you to select certain devices from Change Control by defining a regular expression to evaluate against the device hostname

Match Task Device

An Action Bundle can contain a maximum of one task action. The device of the task is assigned in the Template using the Device Filter field.

When configuring the Action Bundle, a non-task action with the placeholder Match Task Device can be assigned. This means that the device associated with the task will be applied to the non-task action.

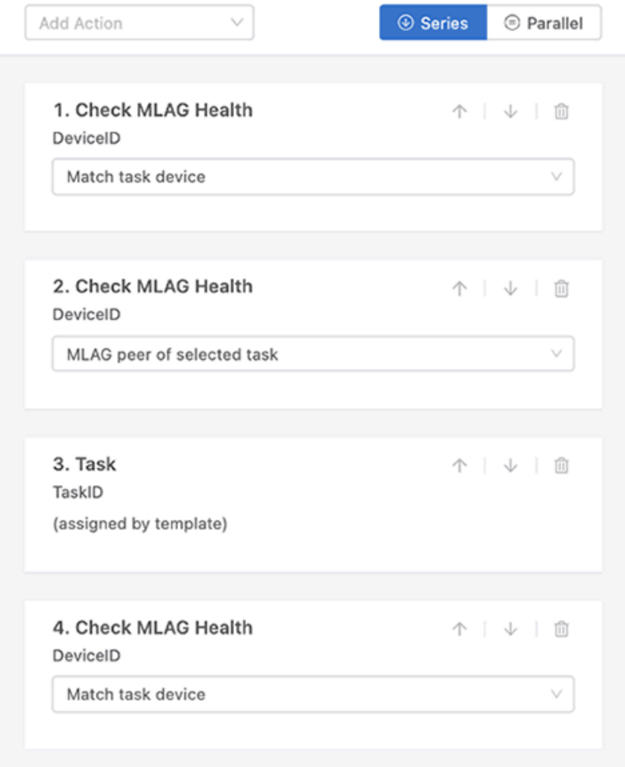
MLAG Peer of Selected Task

This placeholder enables you to sequence MLAG upgrades. You can run non-task actions on the MLAG peer of the device that the task in the Action Bundle is assigned to.

By using this placeholder, the MLAG Health Check can be run against the MLAG peer before running the task.

The following figure is an example of how actions can be arranged so that the MLAG health of both the task device and the task device's MLAG peer are checked before running the task. The last action checks the MLAG health of the task device after the task has been performed.

Figure 14-43: MLAG Peer of Selected Task



1. Check MLAG Health
DeviceID
Match task device

2. Check MLAG Health
DeviceID
MLAG peer of selected task

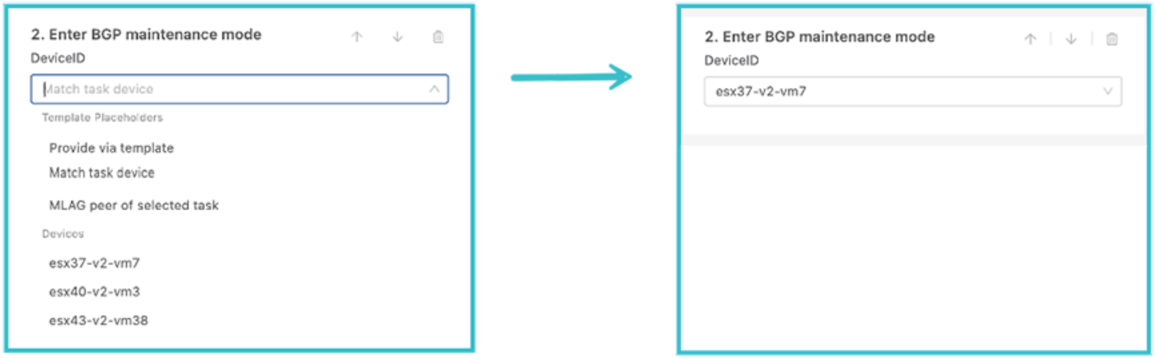
3. Task
TaskID
(assigned by template)

4. Check MLAG Health
DeviceID
Match task device

Static Action Arguments

Static arguments can be applied in an Action Bundle by assigning certain non-task actions with a specific device. This enables you to always have a particular action run against a specific device when the Action Bundle is applied to a Stage Rule in a template.

Figure 14-44: Static Action Arguments



2. Enter BGP maintenance mode
DeviceID
Match task device
Template Placeholders
Provide via template
Match task device
MLAG peer of selected task
Devices
esx37-v2-vm7
esx40-v2-vm3
esx43-v2-vm38

2. Enter BGP maintenance mode
DeviceID
esx37-v2-vm7

14.5.2 Templates

Action Bundles will be assigned to a Template. With the Template you will bundle and sequence specific actions and group those action bundles into stages to define the upgrade sequence.

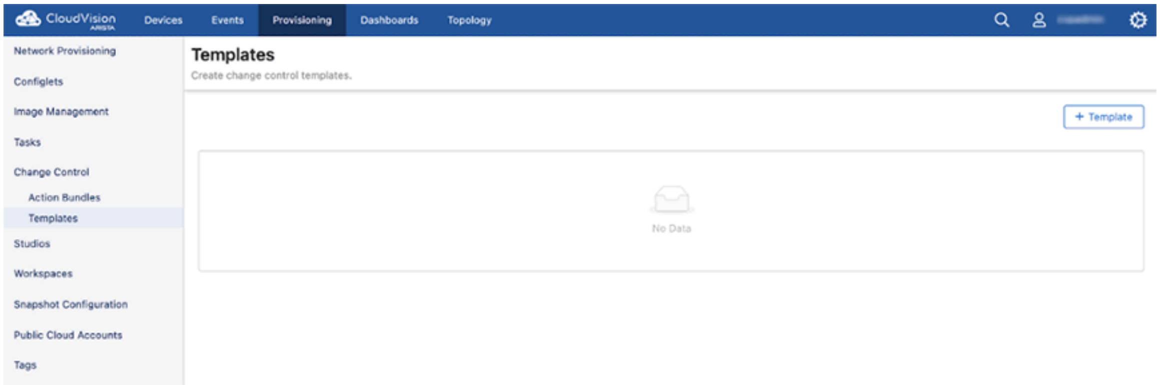
Note: Applying a Template to a change control is a single operation. The Template is not permanently linked to the change control; therefore, making changes to a Template after it has been applied to a change control will have no effect on the existing change control.

- A Template can be applied multiple times. Each time the existing structure will be completely overwritten, and only the tasks will remain as the sole input to the Template.
- This feature cannot be used to craft arbitrarily complex change controls, and advanced users may want to leverage the Change Control API to construct custom layouts.

Accessing Templates

Select **Provisioning** and select **Templates**. The following screen will be displayed.

Figure 14-45: Accessing Templates

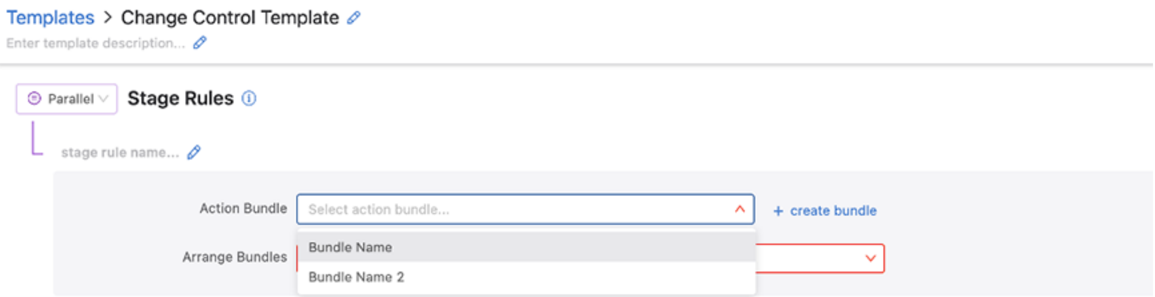


14.5.2.1 Create a New Template

When creating a new Template, an unlimited number of Stages Rules can be added using at least one Action Bundle.

1. Select **+ Template** from the Templates screen.
2. Each Stage Rule is associated with a single Action Bundle. Select an Action Bundle from the menu or create a new one.

Figure 14-46: Create a New Template

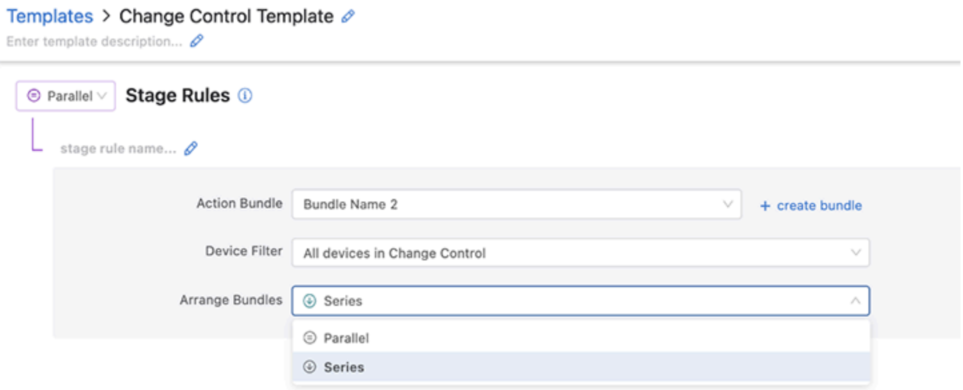


3. Once you have assigned an Action Bundle, complete any additional fields associated with the specific Action Bundle.

Note: If the Action Bundle contains device placeholders, a Device Filter will appear. This is used to define which devices will be applied to this Action Bundle.

4. A sub-stage will be created for every populated Action Bundle. Arrange the sub-stages in Series or Parallel.

Figure 14-47: Stage Rule



Templates > Change Control Template

Enter template description...

Parallel | Stage Rules

stage rule name...

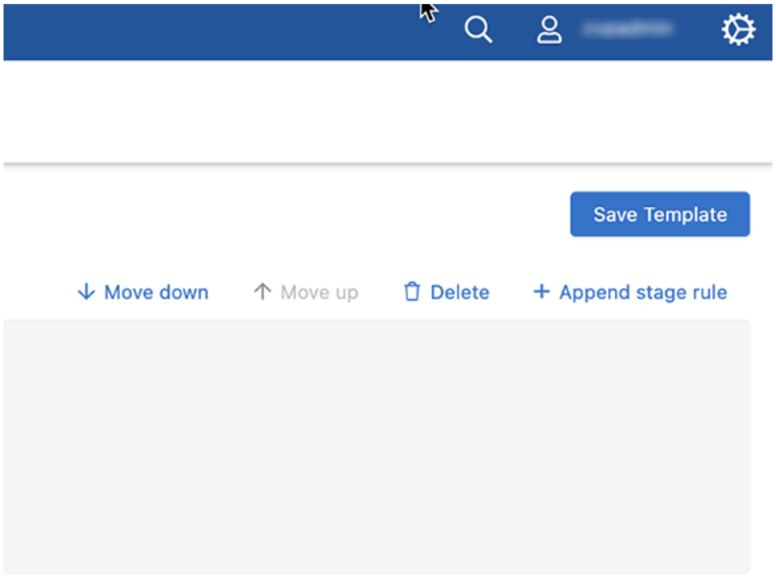
Action Bundle: Bundle Name 2

Device Filter: All devices in Change Control

Arrange Bundles: Series

5. You can repeat Steps 2-4 to create a Stage Rule for each Action Bundle to be added to the Template, and then arrange the order of the Stage Rules.

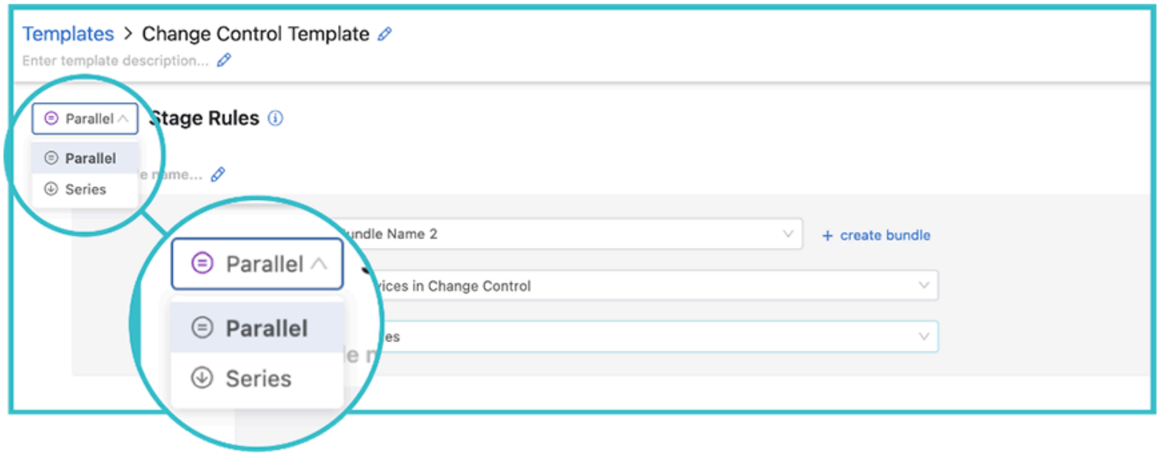
Figure 14-48: Order Stage Rules



Note: The same Action Bundle can be applied to multiple stages, each with a unique Device Filter.

6. Set the Stage Rules to execute in Series or Parallel.

Figure 14-49: Set Stage Rule



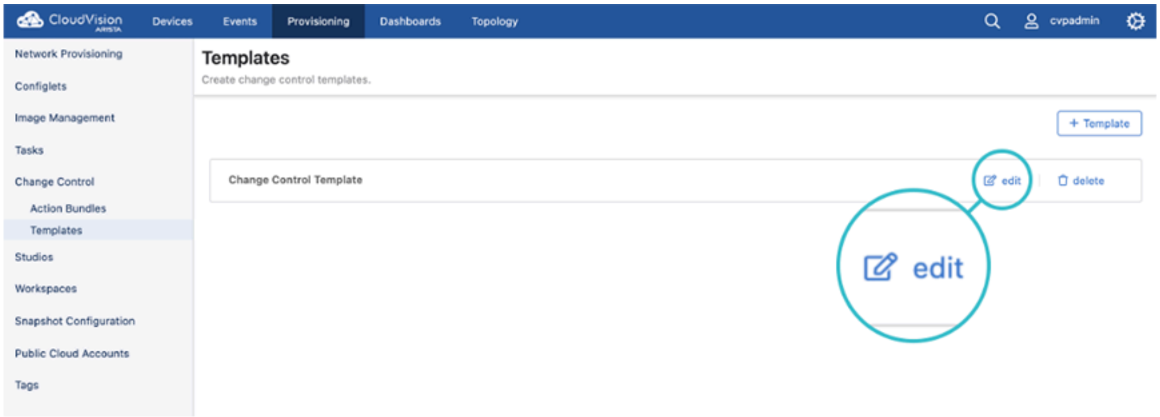
7. When done, select **Save Template**.

14.5.2.2 Edit a Template

Note: Any changes made to a Template will not be updated for any change control operations it has been applied to. The Template will need to be reapplied.

1. Click **Edit** on the Template to modify. The Template screen will display its current Stage Rules and details, how they are ordered, and the manner in which they will be executed.

Figure 14-50: Edit a Template

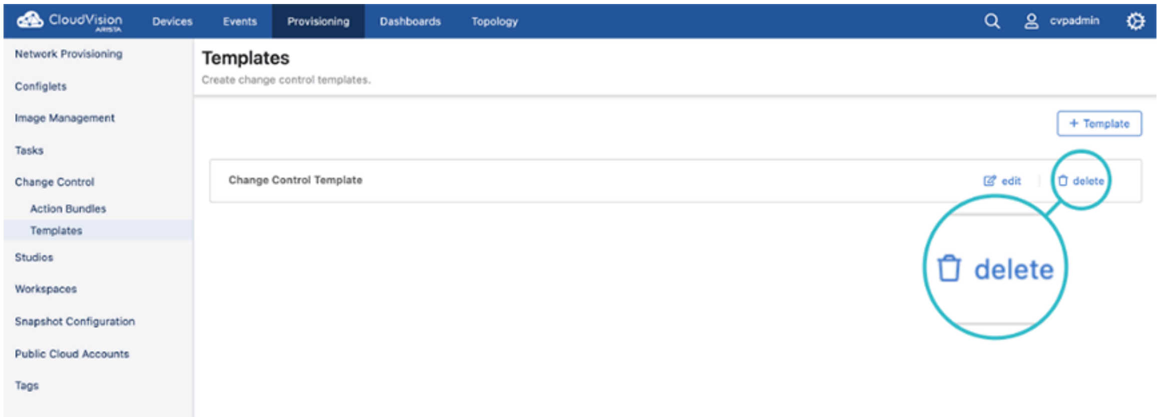


2. Edit any of the details by amending the fields, using the up and down arrows, or deleting Stage Rules.
3. Click **Save** Template when done.

14.5.2.3 Delete a Template

1. Click **Delete** on the Template you wish to remove.

Figure 14-51: Delete a Template



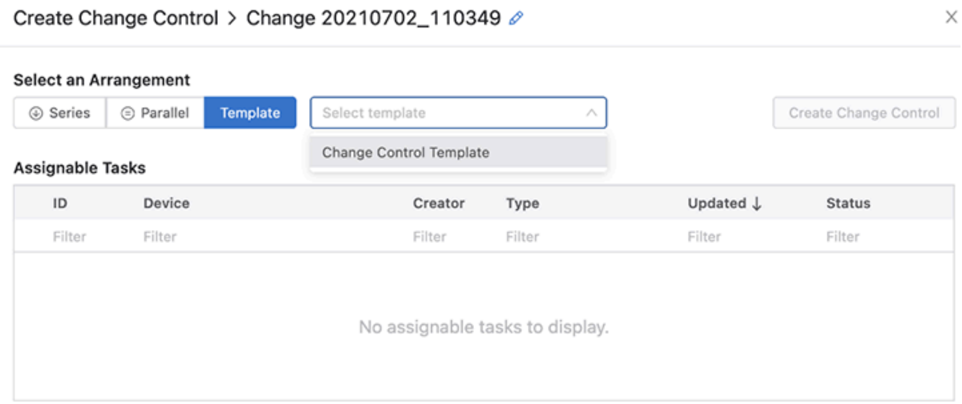
Note: Deleting a template will not affect change controls that were previously generated using that template.

14.5.2.4 Creating a New Change Control with a Template

Follow these instructions to create a change control and apply a Template at the same time.

1. Select **Tasks** or **Change Control** under the Provisioning tab, and click **Create Change Control**.
2. In the screen that is displayed, enter a name for the change control and select the tasks that should be included in the change control.
3. To build the change control with a Template, click **Template**.

Figure 14-52: Creating a New Change Control with a Template


Create Change Control > Change 20210702_110349

ID	Device	Creator	Type	Updated ↓	Status
Filter	Filter	Filter	Filter	Filter	Filter

No assignable tasks to display.

4. From the menu, select a Template and select **Create Change Control**.
5. The Change Control screen will be displayed. Revise to the change control format, review and approve the proposed changes as needed. When done execute the network changes.

14.5.2.5 Applying a Template to an Existing Change Control

If a change control has been created but not approved or executed, you can apply a Template to it.

1. Select **Change Control**, and select the desired change control from the Open Change Control list.
2. The Change Control edit screen of the selected change control is displayed. Click **Select a Template** to open up a menu of your Templates.
3. Select the Template that you want to apply to the change control and click **Apply Template**.The Template configuration will be added to the change control for review and approval.

Note: Applying a Template to a change control operation is a single operation. Any changes made to the Template will not be automatically applied to the change control.

14.6 Creating and Managing Custom Actions

The **Actions** menu in the CloudVision portal enables you to create and manage frequently used actions in the **Action Bundles** and **Change Control** operations menu.

Apart from the existing set of actions, a new suite of actions is added to perform additional change control operations on your desired devices. In the **Actions** menu, you can view the arguments of built-in actions and create and manage custom actions, which you can apply in a **change control** operation. Creating your own custom actions enable you to execute actions specific to your network, which you or another CloudVision user has defined. Additionally, provisioning devices using a change control operation enables you to have granular control over the actions during the change control operation.

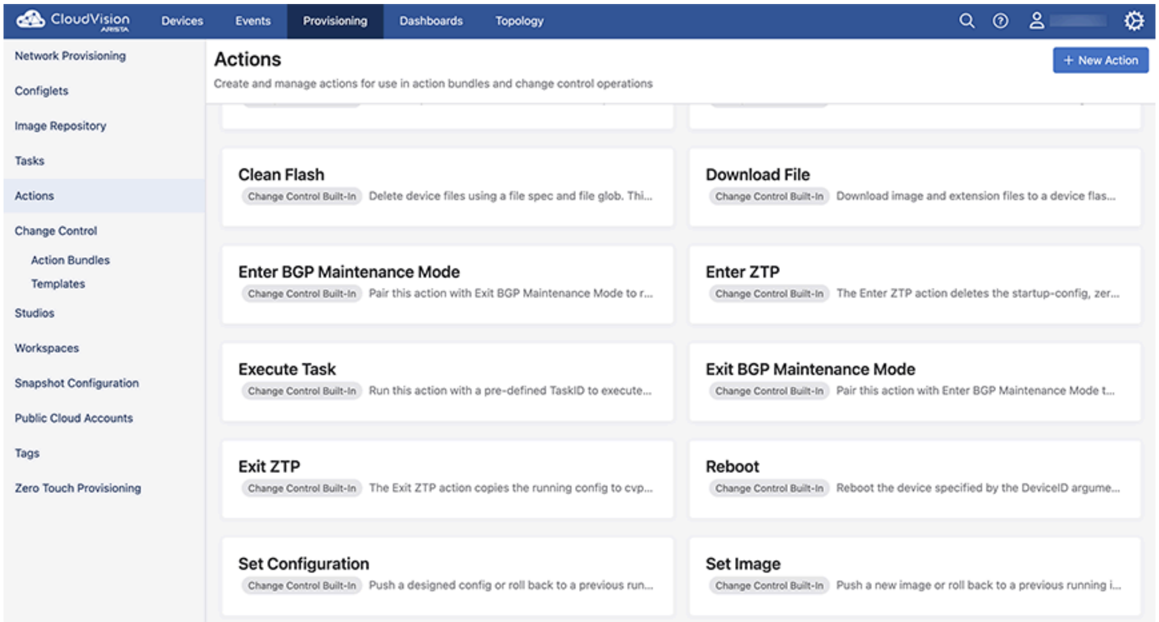
Starting with the 2023.2.0 release, the following new actions are available in the Actions menu.

Table 16: New Actions in Release 2023.2.0

Actions	Description
Clean Flash	Creates space on a device by deleting files in the flash directory.
Download File	Download files from CloudVision to a device.
Enter ZTP	Puts the device in zero touch provisioning mode.
Exit ZTP	Removes the device from zero touch provisioning mode.
Reboot	Reboots the device.
Set Configuration	Applies the configuration on the device.
Set Image	Installs an image on the device.

See image below for the newly added actions.

Figure 14-53: New Actions in Release 2023.2.0



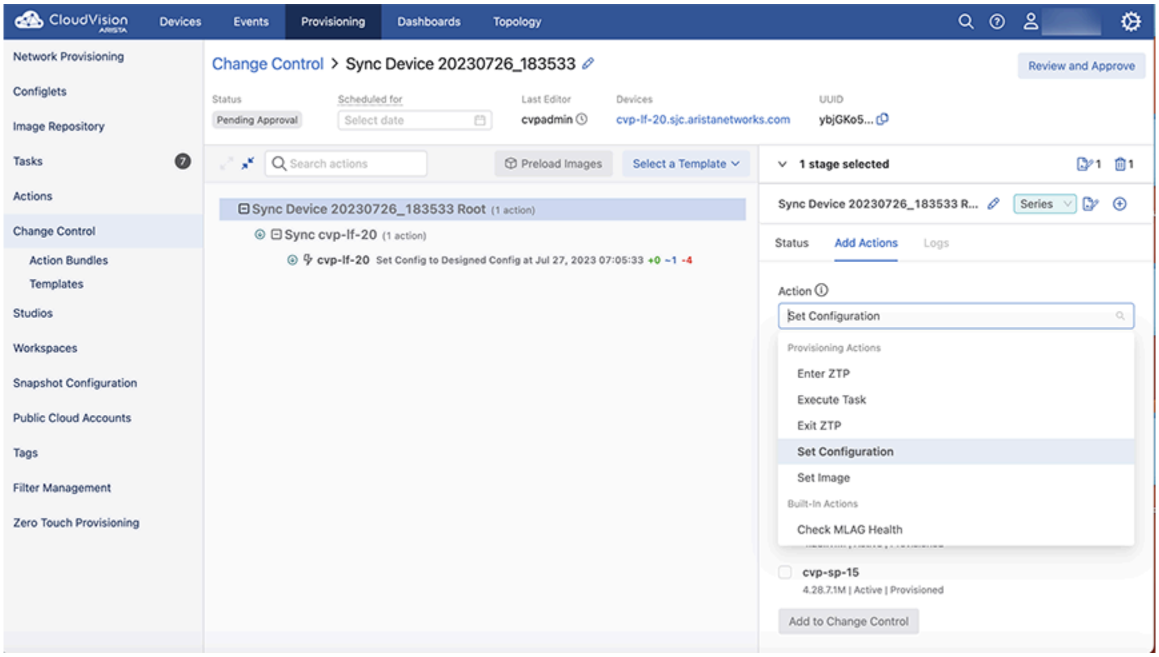
Actions

Create and manage actions for use in action bundles and change control operations

Clean Flash Change Control Built-In Delete device files using a file spec and file glob. Thi...	**Download File** Change Control Built-In Download image and extension files to a device flas...
Enter BGP Maintenance Mode Change Control Built-In Pair this action with Exit BGP Maintenance Mode to r...	**Enter ZTP** Change Control Built-In The Enter ZTP action deletes the startup-config, zer...
Execute Task Change Control Built-In Run this action with a pre-defined TaskID to execute...	**Exit BGP Maintenance Mode** Change Control Built-In Pair this action with Enter BGP Maintenance Mode t...
Exit ZTP Change Control Built-In The Exit ZTP action copies the running config to cvp...	**Reboot** Change Control Built-In Reboot the device specified by the DeviceID argume...
Set Configuration Change Control Built-In Push a designed config or roll back to a previous run...	**Set Image** Change Control Built-In Push a new image or roll back to a previous running i...

You can use the above actions through the **Change Control** menu for configuring change control operations as shown in the image below. The new provisioning actions are available under Provisioning Actions or Built-In Actions and function like any pre-existing built-in action.

Figure 14-54: Change Control Actions



Change Control > Sync Device 20230726_183533

Status: Pending Approval | Scheduled for: Select date | Last Editor: cvpadmin | Devices: cvp-lf-20.sjc.aristanetworks.com | UUID: ybjGKo5...

Sync Device 20230726_183533 Root (1 action)

Sync cvp-lf-20 (1 action)

cvp-lf-20 Set Config to Designed Config at Jul 27, 2023 07:05:33 +0 ~1 -4

1 stage selected

Sync Device 20230726_183533 R...

Action: Set Configuration

Provisioning Actions
- Enter ZTP
- Execute Task
- Exit ZTP
- Set Configuration
- Set Image

Built-In Actions
- Check MLAG Health

cvp-sp-15
4.28.7.1M | Active | Provisioned

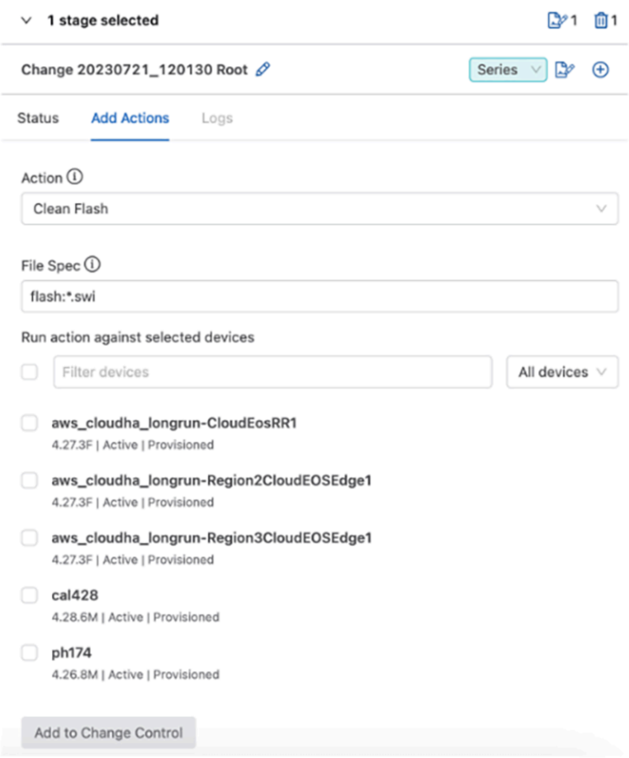
When you select an action, you must also choose the devices to run the action against. See below sections for details on each action.

Clean Flash Action

The **Clean Flash** action deletes the files from flash memory on a device. You must define the file specifications and the devices that the action should run against. From the Change Control Actions page,

1. Select **Clean Flash** as in the image below:

   Figure 14-55: Change Control - Clean Flash



Action

Clean Flash

File Spec

flash:*.swi

Run action against selected devices

☐ aws_cloudha_longrun-CloudEosRR1
4.27.3F | Active | Provisioned

☐ aws_cloudha_longrun-Region2CloudEOSEdge1
4.27.3F | Active | Provisioned

☐ aws_cloudha_longrun-Region3CloudEOSEdge1
4.27.3F | Active | Provisioned

☐ cal428
4.28.6M | Active | Provisioned

☐ ph174
4.26.8M | Active | Provisioned

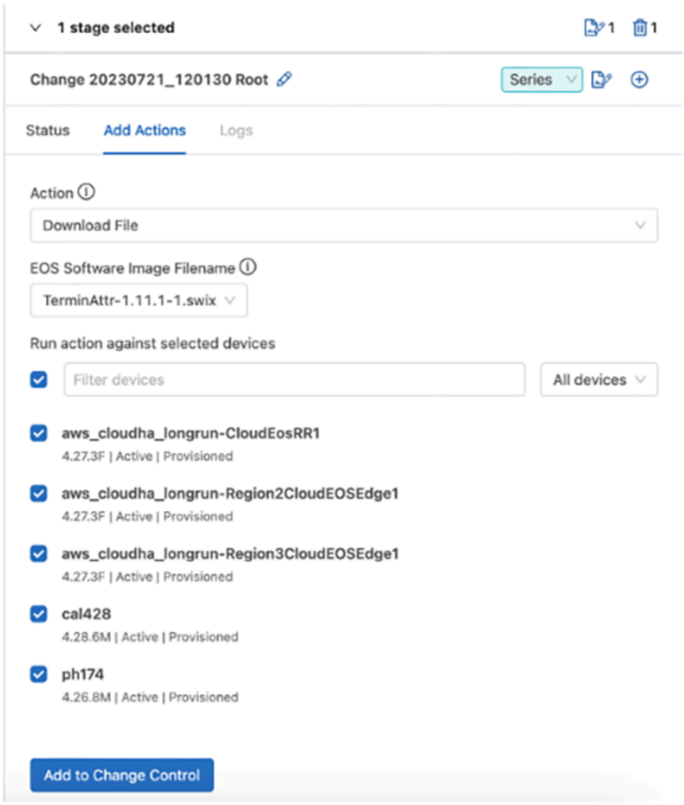
2. Enter a **File Spec**. By default, **flash:*swi** is populated.
3. Select one or more devices to run the action against.
4. Click **Add to Change Control**.

Download File Action

Using the **Download File** action, you can download images and extensions from the *Image Repository* onto a device. This enables you to preload files on a device before updating the image or extension and helps in saving time while executing a change control for updating the device.

1. From the **Change Control** page, select the **Download File** against a device, it downloads the selected file to the flash directory of the device. See image below:

   Figure 14-56: Download File Action



Change 20230721_120130 Root

Action: Download File

EOS Software Image Filename: TerminAttr-1.11.1-1.swix

Run action against selected devices

☑ aws_cloudha_longrun-CloudEosRR1
4.27.3F | Active | Provisioned

☑ aws_cloudha_longrun-Region2CloudEOSEdge1
4.27.3F | Active | Provisioned

☑ aws_cloudha_longrun-Region3CloudEOSEdge1
4.27.3F | Active | Provisioned

☑ cal428
4.28.6M | Active | Provisioned

☑ ph174
4.26.8M | Active | Provisioned

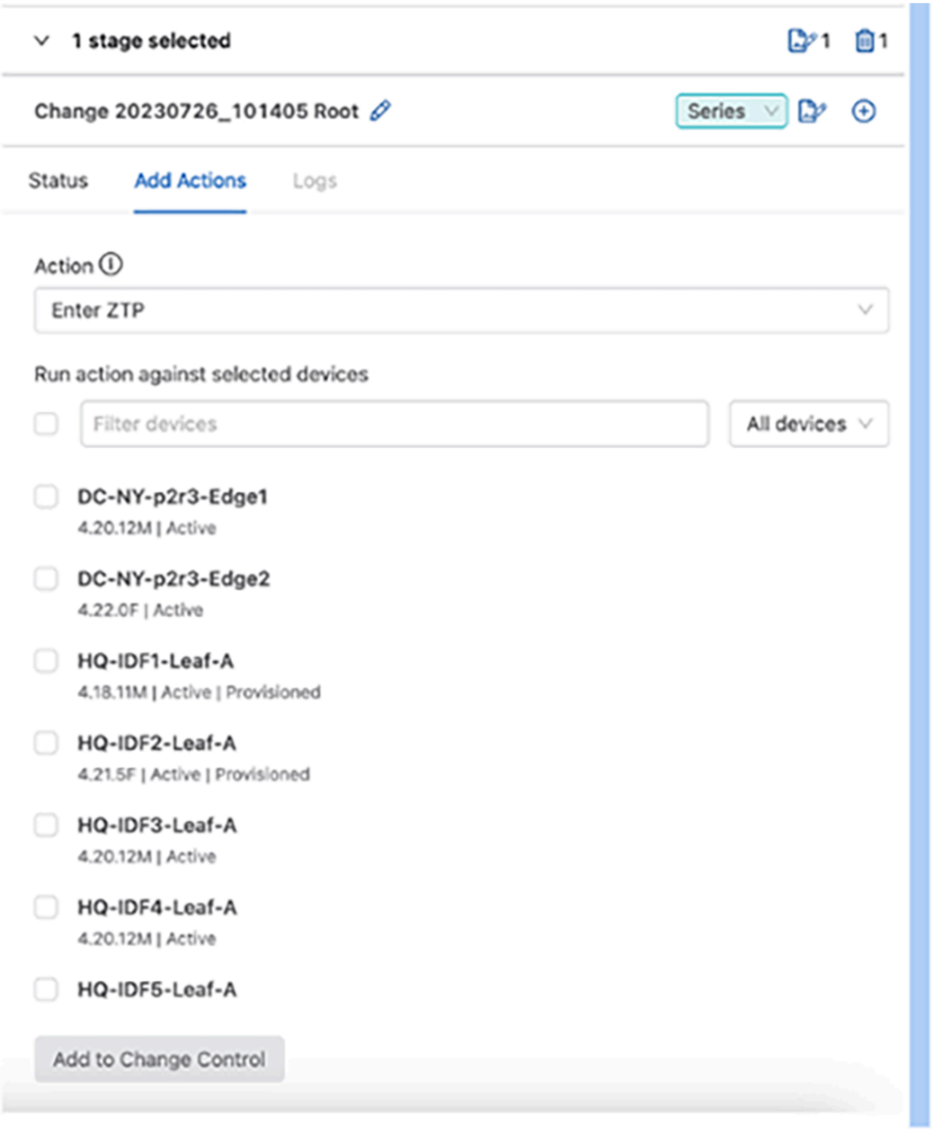
2. Select an image or extension from the **EOS Software Image Filename** drop-down menu. All files added to the *Image Repository* are available from the drop-down menu. If your desired software file is not available in this list, add it to the *Image Repository* and try again.
3. Select the devices to run the action against from the **Run action against selected devices** field.
4. Click **Add to Change Control**. The selected file gets downloaded onto the device.

Enter ZTP Action

Choosing this action puts a device in Zero Touch Provisioning (ZTP) mode.

1. From the **Change Control** page, select the **Enter ZTP** action. See image below:

   Figure 14-57: Enter ZTP Action



Change 20230726_101405 Root

Action: Enter ZTP

Run action against selected devices

□ DC-NY-p2r3-Edge1
4.20.12M | Active

□ DC-NY-p2r3-Edge2
4.22.0F | Active

□ HQ-IDF1-Leaf-A
4.18.11M | Active | Provisioned

□ HQ-IDF2-Leaf-A
4.21.5F | Active | Provisioned

□ HQ-IDF3-Leaf-A
4.20.12M | Active

□ HQ-IDF4-Leaf-A
4.20.12M | Active

□ HQ-IDF5-Leaf-A

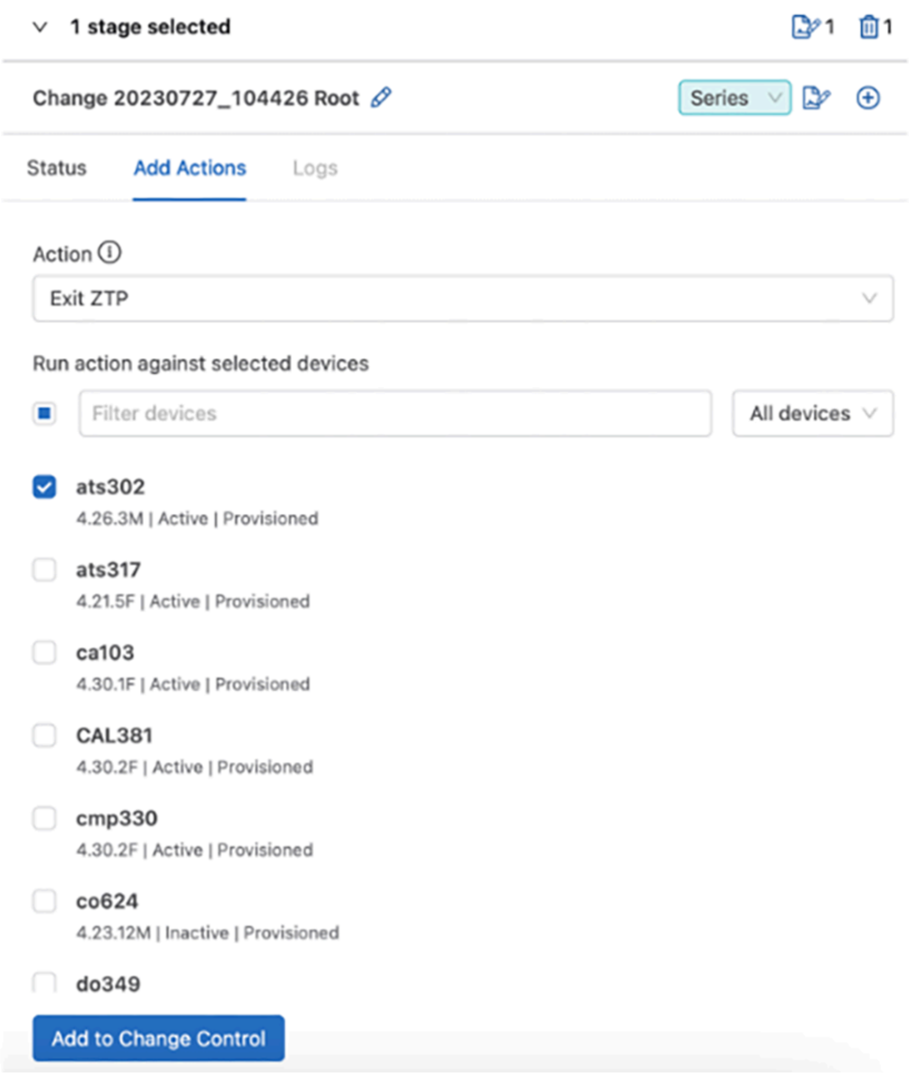
2. Select the devices to run the action against from the **Run action against selected devices** field.
3. Click **Add to Change Control**. The selected devices are now in ZTP mode.

Exit ZTP Action

The **Exit ZTP** action gets the device out of ZTP mode.

1. From the **Change Control** page, select the **Exit ZTP** action. See image below:

   Figure 14-58: Exit ZTP Action

   Action: Exit ZTP

   Run action against selected devices

   Filter devices | All devices

   ☑ ats302
   4.26.3M | Active | Provisioned

   □ ats317
   4.21.5F | Active | Provisioned

   □ ca103
   4.30.1F | Active | Provisioned

   □ CAL381
   4.30.2F | Active | Provisioned

   □ cmp330
   4.30.2F | Active | Provisioned

   □ co624
   4.23.12M | Inactive | Provisioned

   □ do349

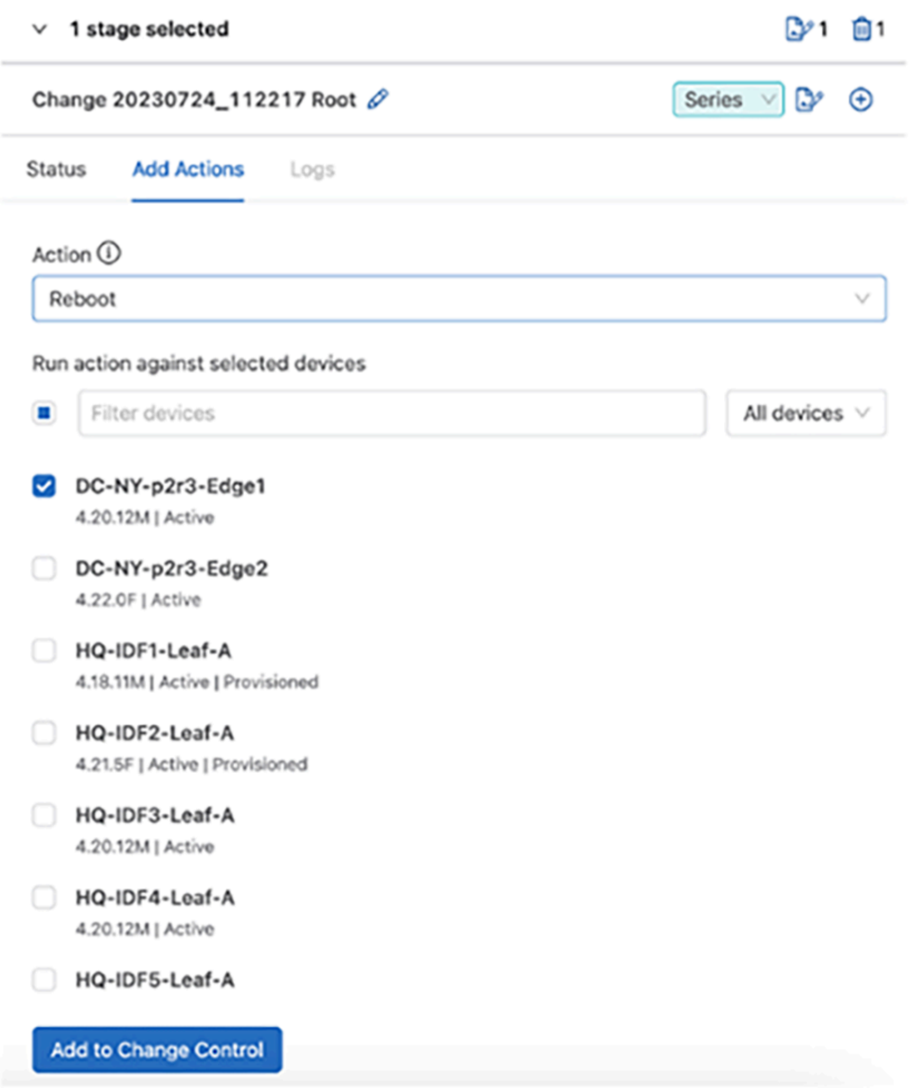
2. Select the devices to run the action against from the **Run action against selected devices** field.
3. Click **Add to Change Control**. The selected devices now exit the ZTP mode.

Reboot Action

You can reboot a device by using the **Reboot** action. As a result, the selected devices stop forwarding traffic until the devices are completely restarted.

1. From the **Change Control** page, select the **Reboot** action. See image below:

Figure 14-59: Reboot Action



1 stage selected 1 1

Change 20230724_112217 Root

Action: Reboot

Run action against selected devices

☑ DC-NY-p2r3-Edge1
4.20.12M | Active

☐ DC-NY-p2r3-Edge2
4.22.0F | Active

☐ HQ-IDF1-Leaf-A
4.18.11M | Active | Provisioned

☐ HQ-IDF2-Leaf-A
4.21.5F | Active | Provisioned

☐ HQ-IDF3-Leaf-A
4.20.12M | Active

☐ HQ-IDF4-Leaf-A
4.20.12M | Active

☐ HQ-IDF5-Leaf-A

2. Select the devices to run the action against from the **Run action against selected devices** field.
3. Click **Add to Change Control**. The selected devices are rebooted.

Set Configuration Action

The **Set Configuration** action applies the designed configuration to a device. This action reduces the time required and enhances the device configuration process significantly. This action computes a delta configuration between the designed configuration and the running configuration on the selected device. The delta configuration captures the sequence of commands that should be applied to the running configuration of the selected device so as to transform the configuration into the designed configuration. This configuration push is an atomic transactional process, where only the delta commands are parsed and evaluated by AAA, thereby saving significant time in completing the configuration process (that is, without having to process the entire designed configuration on the selected device).

The **Set Configuration** action is efficient in comparison to the **Update Config** task when:

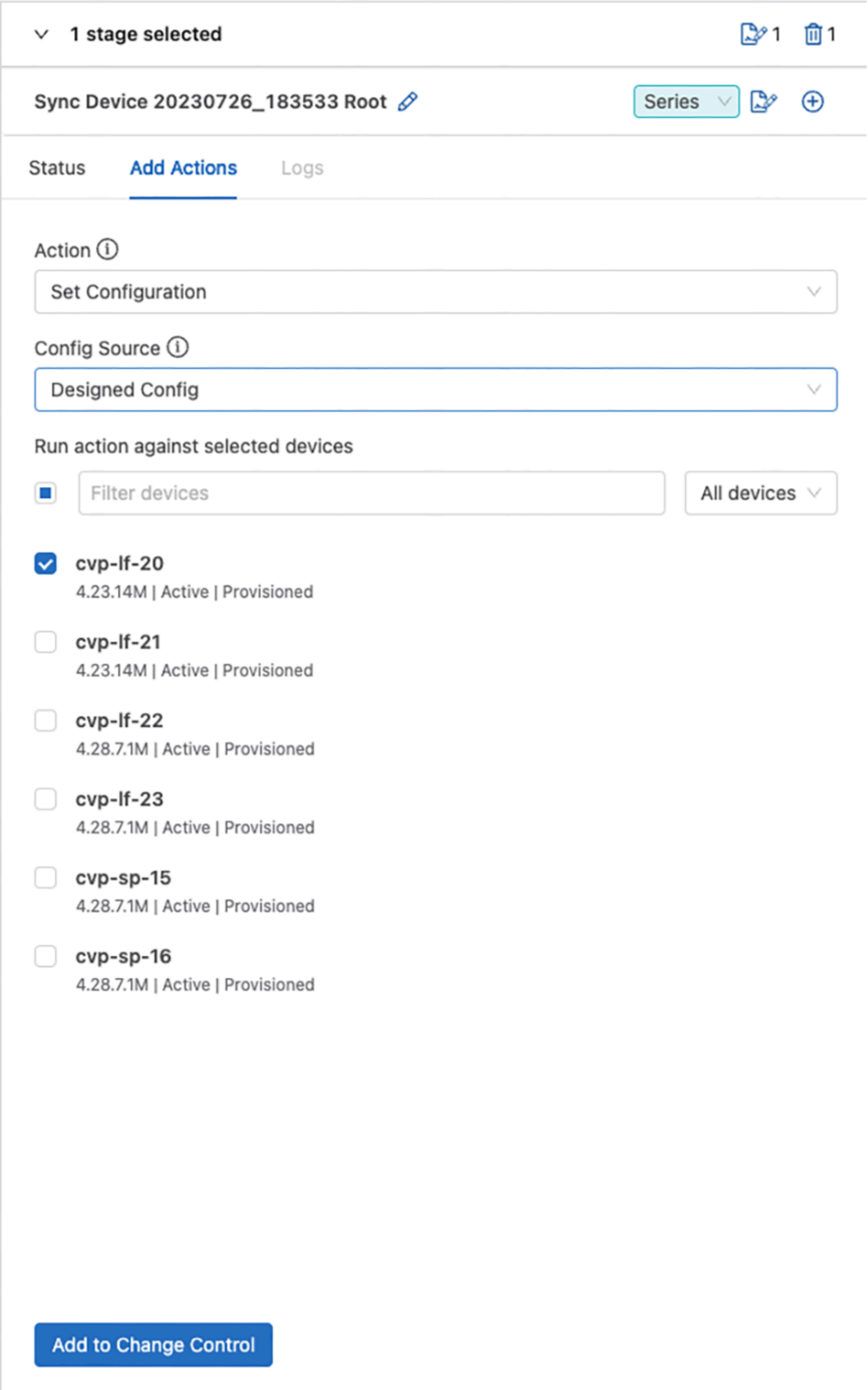
- Per-command authorization and accounting are enabled on the device.
- The designed configuration is large.

- The difference between the designed configuration and the running configuration is smaller than the designed configuration (that is, the delta is relatively small).

Note: If the delta configuration does not match with the designed configuration, then a complete push of the designed configuration is automatically done by the **Set Config** action.

1. From the **Change Control** page, select the **Set Configuration** action. See image below:

Figure 14-60: Set Configuration Action



1 stage selected

Sync Device 20230726_183533 Root

Series

Status | Add Actions | Logs

Action: Set Configuration

Config Source: Designed Config

Run action against selected devices

Filter devices | All devices

☑ cvp-lf-20
4.23.14M | Active | Provisioned

☐ cvp-lf-21
4.23.14M | Active | Provisioned

☐ cvp-lf-22
4.28.7.1M | Active | Provisioned

☐ cvp-lf-23
4.28.7.1M | Active | Provisioned

☐ cvp-sp-15
4.28.7.1M | Active | Provisioned

☐ cvp-sp-16
4.28.7.1M | Active | Provisioned

2. From the **Config Source** drop-down menu, select the type of configuration that you want to apply from:

- **Designed Configuration**: Pushes the designed configuration from CloudVision onto the selected device.

- **Running Configuration**: Rolls back the configuration to a previous running configuration based on the provided timestamp.

3. Select the devices to run the action against from the **Run action against selected devices** field.
4. Click **Add to Change Control**. The selected devices are updated with the new configuration.

Guidelines to Troubleshoot for Set Configuration Action

If the **Set Configuration** action takes more than a reasonable time to execute on a device, then explore the following possibilities and take action accordingly:

- **How big is the delta configuration in comparison to the designed configuration?**

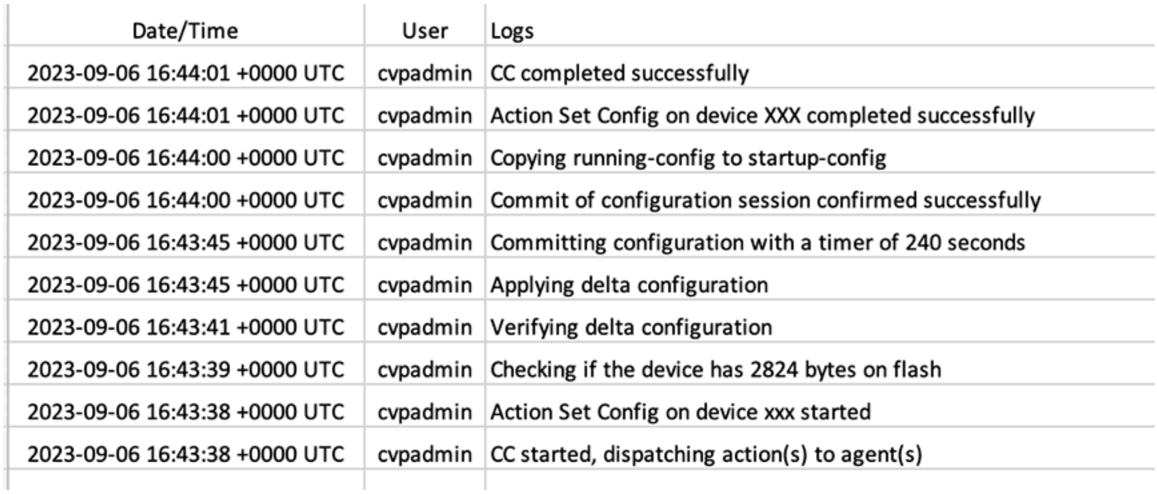
  If the delta configuration is almost as same as the designed configuration, then, there might not be any significant improvement in configuration push time. This is because when the designed configuration is being pushed on a switch for the first time, all the lines in the designed configuration are also added to the switch.
- **Is command authorization and accounting enabled on the switch?**

  When AAA is enabled on the switch, each line in the delta configuration is parsed through AAA. In this case, the performance of the AAA server should be checked to see if that is taking a significant amount of time.
- **Was delta configuration successful?**

  If the delta configuration is unsuccessful, then the entire designed configuration gets pushed, resulting in longer than expected configuration push times. Check the Change Control logs to see if the delta configuration push failed and the reason for the failure.

You can view the action logs in Change Control. These logs display any exceptions, errors, or warnings when executing the various actions. Below is an example of a successful log file:

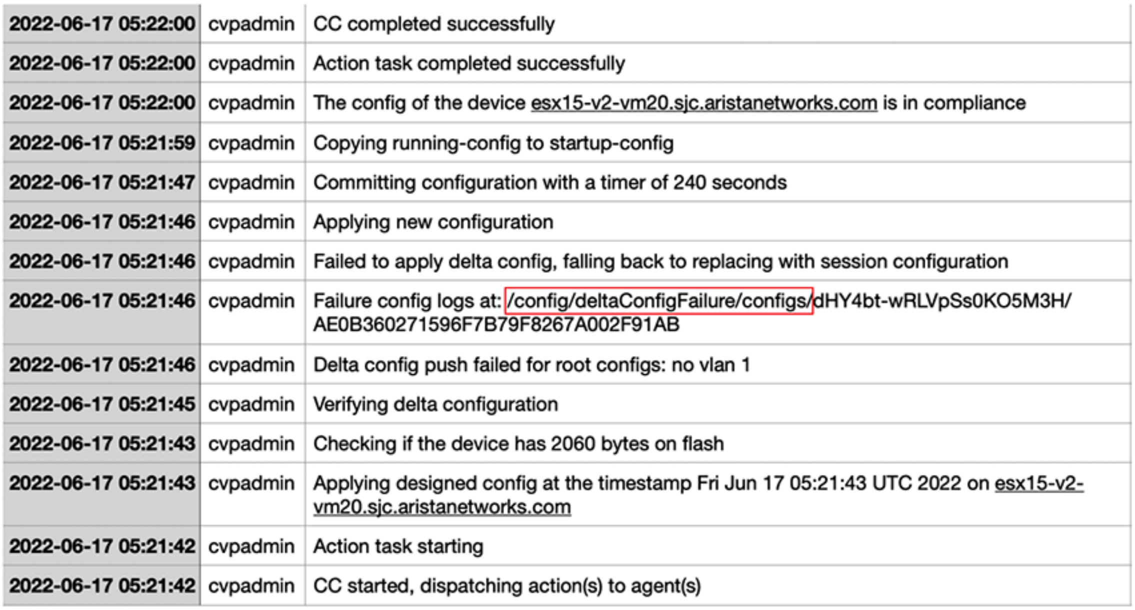
Figure 14-61: Change Control Success Log Sample



Date/Time	User	Logs
2023-09-06 16:44:01 +0000 UTC	cvpadmin	CC completed successfully
2023-09-06 16:44:01 +0000 UTC	cvpadmin	Action Set Config on device XXX completed successfully
2023-09-06 16:44:00 +0000 UTC	cvpadmin	Copying running-config to startup-config
2023-09-06 16:44:00 +0000 UTC	cvpadmin	Commit of configuration session confirmed successfully
2023-09-06 16:43:45 +0000 UTC	cvpadmin	Committing configuration with a timer of 240 seconds
2023-09-06 16:43:45 +0000 UTC	cvpadmin	Applying delta configuration
2023-09-06 16:43:41 +0000 UTC	cvpadmin	Verifying delta configuration
2023-09-06 16:43:39 +0000 UTC	cvpadmin	Checking if the device has 2824 bytes on flash
2023-09-06 16:43:38 +0000 UTC	cvpadmin	Action Set Config on device xxx started
2023-09-06 16:43:38 +0000 UTC	cvpadmin	CC started, dispatching action(s) to agent(s)

Below is an example of a Change Control log file where the action failed:

Figure 14-62: Change Control Log - Failure



2022-06-17 05:22:00	cvpadmin	CC completed successfully
2022-06-17 05:22:00	cvpadmin	Action task completed successfully
2022-06-17 05:22:00	cvpadmin	The config of the device esx15-v2-vm20.sjc.aristanetworks.com is in compliance
2022-06-17 05:21:59	cvpadmin	Copying running-config to startup-config
2022-06-17 05:21:47	cvpadmin	Committing configuration with a timer of 240 seconds
2022-06-17 05:21:46	cvpadmin	Applying new configuration
2022-06-17 05:21:46	cvpadmin	Failed to apply delta config, falling back to replacing with session configuration
2022-06-17 05:21:46	cvpadmin	Failure config logs at: /config/deltaConfigFailure/configs/dHY4bt-wRLVpSs0KO5M3H/AE0B360271596F7B79F8267A002F91AB
2022-06-17 05:21:46	cvpadmin	Delta config push failed for root configs: no vlan 1
2022-06-17 05:21:45	cvpadmin	Verifying delta configuration
2022-06-17 05:21:43	cvpadmin	Checking if the device has 2060 bytes on flash
2022-06-17 05:21:43	cvpadmin	Applying designed config at the timestamp Fri Jun 17 05:21:43 UTC 2022 on esx15-v2-vm20.sjc.aristanetworks.com
2022-06-17 05:21:42	cvpadmin	Action task starting
2022-06-17 05:21:42	cvpadmin	CC started, dispatching action(s) to agent(s)

Note: Based on the error messages in the log files, you can debug the issue by using the Telemetry Browser in CloudVision.

The log file contains the path `/config/deltaConfigFailure/configs/<ccID>/<deviceID>`, where you can find the failure details. In the log files, you can find three types of messages as below:

- **Exceptions**: In these types of messages, you can view both the expected configuration (designed config) and the actual config during verification in the form: **"EXPECTED:...GOT:..."**. This message helps you to determine which configuration lines did not run as expected. See below section for details on Exceptions.
- **Errors**: If you see an error for a particular command, it means that this command was not added or deleted resulting in the failure of the delta configuration push.
- **Warnings**: A warning for a particular command on a specific device helps you to debug why the actual configuration after applying the delta configuration is different from the expected configuration. Note that some warnings may be unrelated to the failure.

What are Exceptions?

An exception occurs when the **Set Configuration** action fails to remove some running configuration from the selected device. This occurs for certain types of EOS commands, where the action may run, but the delta configuration that is pushed by the **Set Configuration** action fails and CloudVision subsequently pushes the entire designed configuration onto the device. You must configure the *Exceptions* separately to resolve the issue.

For example, an exception can occur for a command, `switchport port-security violation protect`. Without any additional configuration from the user, the **Set Configuration** action removes the command by using the `default switchport port-security violation protect` command. As this is an invalid command the configuration does not get removed. As a result, the **Set Configuration** action fails and pushes the complete designed configuration on the device.

How to View the Exceptions

To view the exceptions occurring due to the **Set Configuration** action, go to **Settings** > **Telemetry Browser** and select **cvp** under **Application Datasets**. See image below:

Navigate to path /`config/deltaConfigExceptions/`

As of the 2023.2.0 release, you may see one exception related to command parameters, that is, the parameters are dropped by prepending *default*. For example, to delete the command: `switchport port-security violation protect`, the command should be `default switchport port-security`.

How to add custom exceptions

You can add custom exceptions for the **Set Configuration** action in CloudVision by using the REST API commands. To add an exception to the path `config/deltaConfigExceptions/paramCommands`, type:

```
/cvpi/tools/apish publish --dataset-name cvp --path  /config/deltaConfigExcepti
ons/paramCommands/delete --update '{"key": "<Command-Prefix>", "value":
 "<Delete-Command>"}'
```

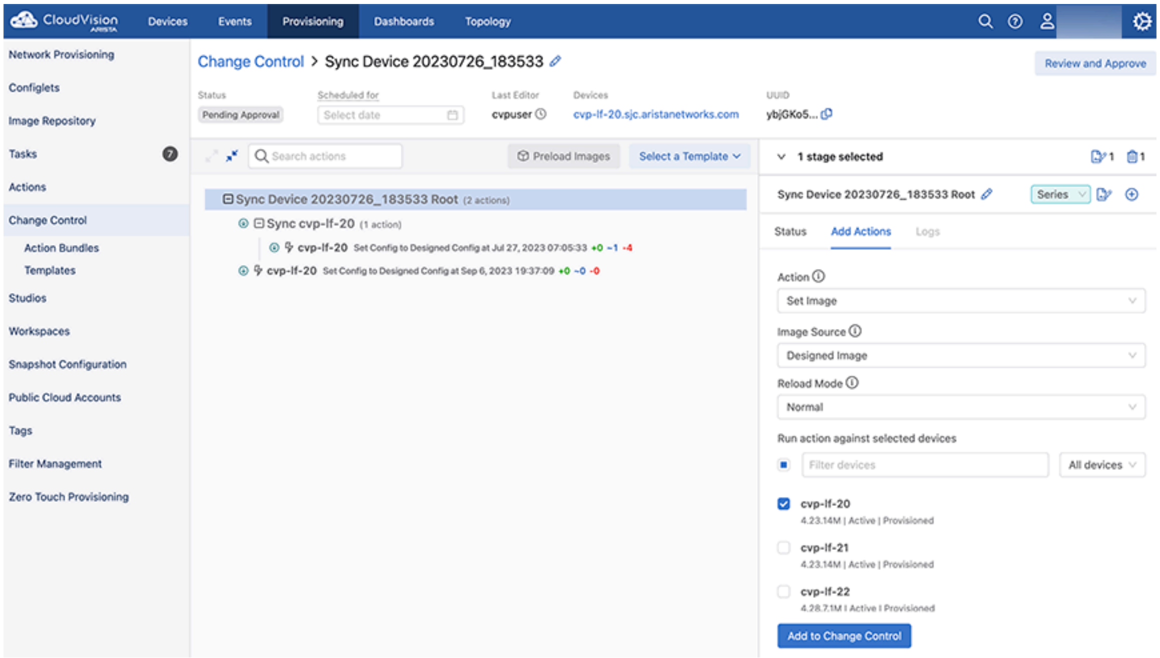
Set Image Action

The **Set Image** action enables you to update a device with a selected image. You can select the images available in the *Image Repository* only. You can also select the device reload mode that includes the Smart System Upgrade (SSU) options.

When using this action, you can also use the **Preload Image** feature that creates a separate change control operation. That operation downloads the image files onto selected devices and enables the **Set Image** action to run faster by skipping the download image step. See image below:

1. From the **Change Control** page, select the **Set Image** action. See image below:

   Figure 14-63: Set Image Action Page1



Change Control > Sync Device 20230726_183533

Status: Pending Approval
Scheduled for: Select date
Last Editor: cvpuser
Devices: cvp-lf-20.sjc.aristanetworks.com
UUID: ybjGKo5...

Sync Device 20230726_183533 Root (2 actions)
Sync cvp-lf-20 (1 action)
cvp-lf-20 Set Config to Designed Config at Jul 27, 2023 07:05:33 +0 ~1 -4
cvp-lf-20 Set Config to Designed Config at Sep 6, 2023 19:37:09 +0 ~0 -0

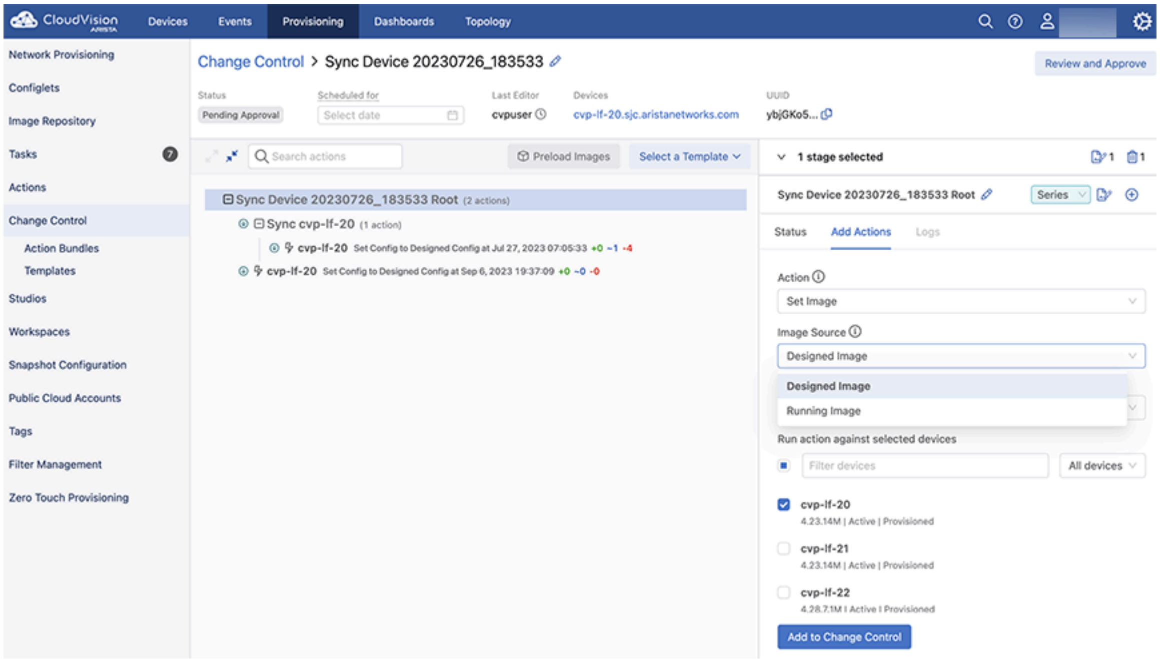
1 stage selected 1 1
Sync Device 20230726_183533 Root Series

Action: Set Image
Image Source: Designed Image
Reload Mode: Normal
Run action against selected devices
Filter devices — All devices
☑ cvp-lf-20 4.23.14M | Active | Provisioned
□ cvp-lf-21 4.23.14M | Active | Provisioned
□ cvp-lf-22 4.28.7.1M | Active | Provisioned

2. Select an **Image Source** (see image below):
   - **Designed Image**: To install the designed image from CloudVision on the selected device (s).

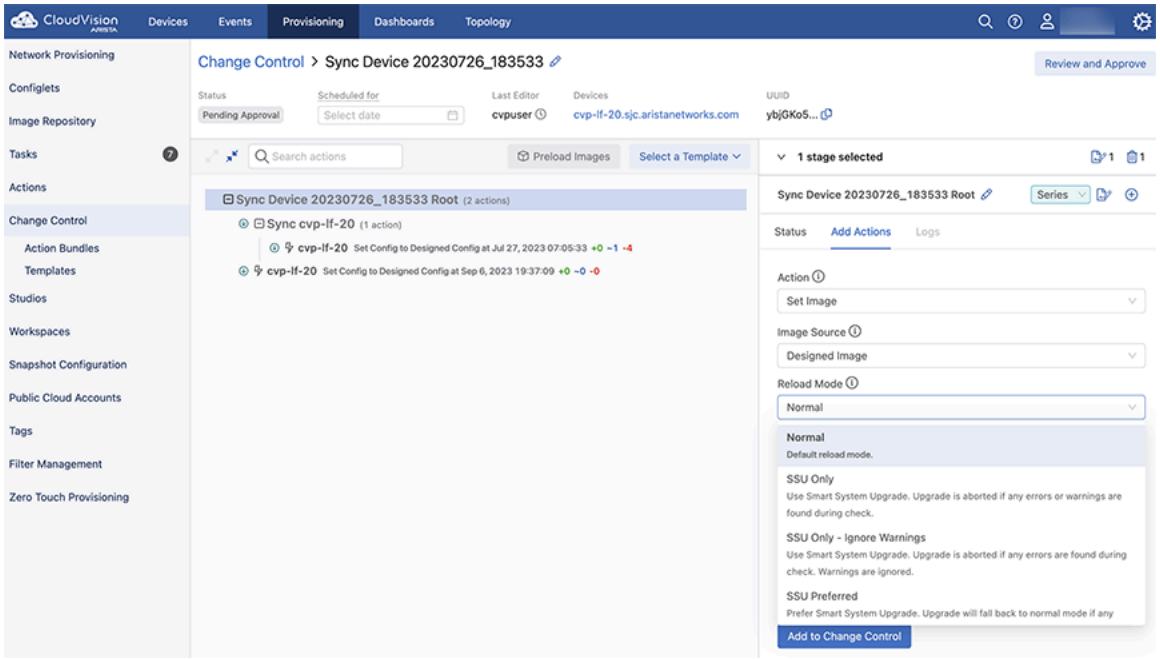
- **Running Image**: To roll back to a previous running image on the device by using the selected time from timepicker.

Figure 14-64: Set Image Action - Image Source Options



3. Select a **Reload Mode** (see image below):

Figure 14-65: Set Image Action - Select Reload Mode


CloudVision
Devices
Events
Provisioning
Dashboards
Topology
Network Provisioning
Configlets
Image Repository
Tasks
Actions
Change Control
Action Bundles
Templates
Studios
Workspaces
Snapshot Configuration
Public Cloud Accounts
Tags
Filter Management
Zero Touch Provisioning
Change Control > Sync Device 20230726_183533
Review and Approve
Status
Pending Approval
Scheduled for
Select date
Last Editor
cvpuser
Devices
cvp-lf-20.sjc.aristanetworks.com
UUID
ybjGKo5...
Search actions
Preload Images
Select a Template
Sync Device 20230726_183533 Root (2 actions)
Sync cvp-lf-20 (1 action)
cvp-lf-20 Set Config to Designed Config at Jul 27, 2023 07:05:33 +0 -1 -4
cvp-lf-20 Set Config to Designed Config at Sep 6, 2023 19:37:09 +0 -0 -0
1 stage selected
Sync Device 20230726_183533 Root
Series
Status
Add Actions
Logs
Action
Set Image
Image Source
Designed Image
Reload Mode
Normal
Normal
Default reload mode.
SSU Only
Use Smart System Upgrade. Upgrade is aborted if any errors or warnings are found during check.
SSU Only - Ignore Warnings
Use Smart System Upgrade. Upgrade is aborted if any errors are found during check. Warnings are ignored.
SSU Preferred
Prefer Smart System Upgrade. Upgrade will fall back to normal mode if any
Add to Change Control

Smart System Upgrade (SSU) minimizes traffic loss during image upgrades. SSU leverages protocols capable of graceful restart and minimizes traffic loss during upgrades. Select one of the **Reload Mode** options from the drop-down menu:

- **Normal**: This option does not use SSU. The device reboots and traffic forwarding stops until the device is restarted.

- **SSU Only**: This option enables CloudVision to first check for any warnings or errors by using the `show reload fast-boot` command. If there are any errors or warnings, the upgrade attempt fails and the errors and warnings are reported back to the user. If there are no errors or warnings, then `reload fast-boot now` command is executed, and the device attempts an SSU.
- **SSU Only Ignore Warnings**: When you select this option, CloudVision first checks for any errors by using `show reload fast-boot` command. If there are any errors, the upgrade attempt fails and the errors are reported back to the user. If there are only warnings, the SSU upgrade proceeds and CloudVision issues a `reload fast-boot now` command and an SSU is attempted.
- **SSU Preferred**: When you select this option, CloudVision first checks for any warnings or errors using the `show reload fast-boot` command. If there are any errors or warnings, then CloudVision aborts the SSU and falls back to **Normal** reload mode.
- **SSU Preferred Ignore Warnings**: When you select this option, CloudVision first checks for any errors or warnings using the `show reload fast-boot` command. If there are only warnings, then SSU is attempted. If there are any errors, **Normal** reload is attempted.

4. Select the devices to run the action against from the **Run action against selected devices** field.
5. Click **Add to Change Control**. The selected devices are updated with the new image.

Chapter 15

Authentication & Authorization (CVP)

Authentication determines if the provided user credentials (username/password) are correct. If authentication succeeds, the user is logged in.

Authorization determines what operations the user can perform after login. Authorization can be for no access, read access, or read and write access.

In the Access Control page, the type of Authentication and Authorization can be defined. AAA servers are defined in this page.

This module guides account management administrators to manage AAA servers, user accounts, and user roles. It provides the functionality required to manage all aspects of user accounts.

Note: Only account management administrators have the permissions to manage accounts.

Sections in this chapter include:

- Access Requirements for Image Bundle Upgrades
- Managing AAA Servers
- About Users and Roles
- Managing User Accounts
- Managing User Roles
- Service Accounts
- Viewing Activity Logs
- Advanced Login Options
- Access to the Access Control Page

15.1 Access Requirements for Image Bundle Upgrades

If AAA is configured (enabled) on the switch, you must have certain access rights before you can perform image bundle upgrades on the switch.

The specific access rights required to perform image bundle upgrades when AAA is configured are:

- Config session
- Bash

The access rights to execute bash commands is required because the following bash command must be executed to upgrade image bundles:

```
bash timeout 10 sudo rm -f /mnt/flash/boot-extensions && echo -e '' > /mnt/
flash/boot-extensions
```

Note: If AAA is enabled and you attempt to perform image bundle upgrades without having these required access rights, the upgrade will fail and the following error occurs:

```
Jul 11 11:36:45 cd342 Aaa: %AAA-4-CMD_AUTHZ_FAILED: User cvpadmin failed
 authorization to execute command 'bash timeout 10 sudo rm -f
/mnt/flash/boot-extensions && echo -e '' > /mnt/flash/boot-extensions
```

15.2 Managing AAA Servers

The system uses the following functionalities to manage AAA servers:

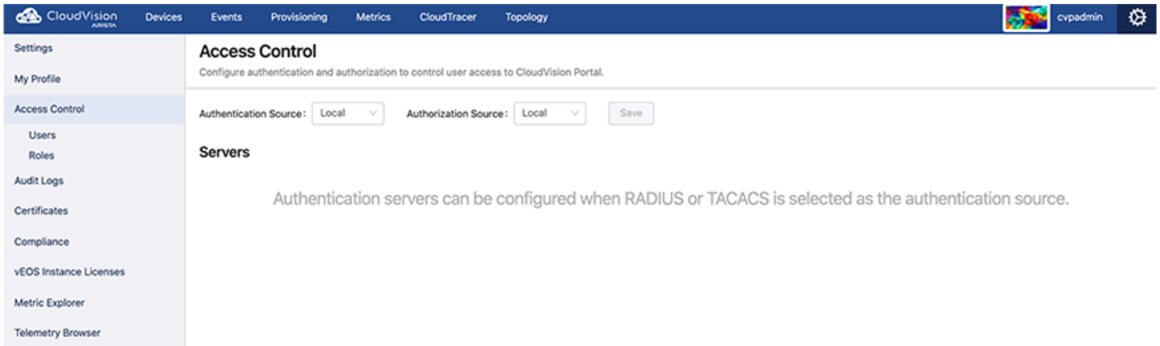
- Adding AAA Servers
- Modifying AAA Servers
- Removing AAA Servers

15.2.1 Adding AAA Servers

1. Navigate to the **Access Control** Page.
2. Click the Authentication source drop-down menu and select either RADIUS or TACACS.

   The Access Control page lists all current servers. See Access to the Access Control Page.
3. Click **+ New Server** at the upper right corner of the **Servers** section.

   Figure 15-1: + New Server in Access Control Page



Configure authentication and authorization to control user access to CloudVision Portal.

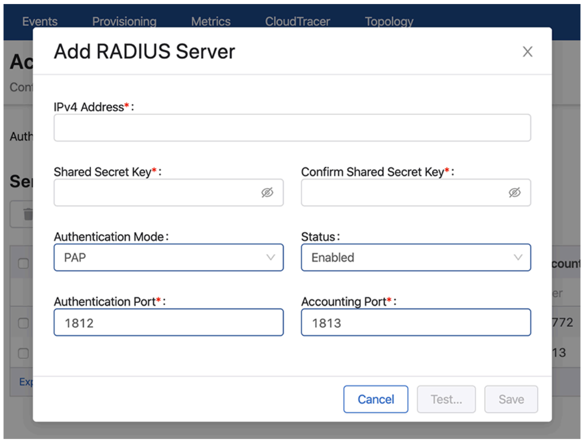
Authentication Source: Local

Authorization Source: Local

Authentication servers can be configured when RADIUS or TACACS is selected as the authentication source.

   The system pops-up the New Server window.

   Figure 15-2: New Server Pop-Up Window



IPv4 Address*:

Shared Secret Key*:

Confirm Shared Secret Key*:

Authentication Mode: PAP

Status: Enabled

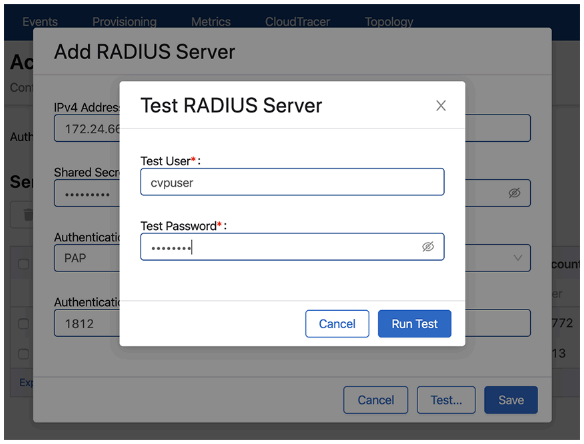
Authentication Port*: 1812

Accounting Port*: 1813

4. Provide the required Information in corresponding fields.
5. If required, click **Test** for testing the new configuration. Else, skip to step 8.

6. Enter your credentials when the **Test Server** pop-up prompts for it.

Figure 15-3: Test Server Pop-Up Window



Add RADIUS Server

IPv4 Address: 172.24.66

Shared Secret: •••••••••

Authentication: PAP

Authentication: 1812

Test RADIUS Server

Test User*: cvpuser

Test Password*: ••••••••

7. Click **Run Test**.

The system displays test results. If required, modify the configuration based on the test result.

8. Click **Save**.

The server is added to the list of servers in the AAA grid.

Related topics:

- Access to the Access Control Page
- Modifying AAA Servers
- Removing AAA Servers

15.2.2 Modifying AAA Servers

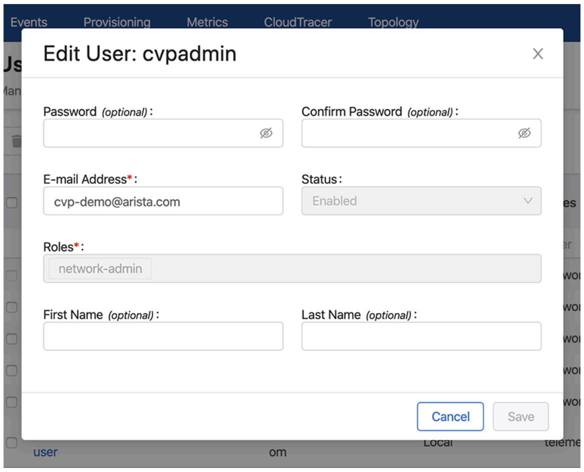
1. Navigate to the **Access Control** Page.
2. Select desired modes from **Authentication source** and **Authorization source** drop-down menus

   The system lists all registered servers of the selected AAA server type. See Access to the Access Control Page.

3. Click the edit icon available next to IP address of the corresponding server.

   The system pops-up the Edit Server window.

Figure 15-4: Edit Server Pop-Up Window



Edit User: cvpadmin

Password (optional):

Confirm Password (optional):

E-mail Address*: cvp-demo@arista.com

Status: Enabled

Roles*: network-admin

First Name (optional):

Last Name (optional):

4. Modify the required information.
5. If required, click **Test** to verify latest changes.
6. Click **Save**.

Note: To apply external authentication, there should be at least one enabled server listed in the page.

15.2.2.1 Adding Vendor Specific Codes to AAA Servers

You can add vendor specific codes to AAA servers for the following:

- RADIUS
- TACACS+
- CISCO ACS

15.2.2.1.1 RADIUS

Arista Vendor Specific Code: add it to the RADIUS dictionary.

```
VENDOR Arista 30065
BEGIN-VENDOR Arista
ATTRIBUTE Arista-AVPair 1 string
END-VENDOR Arista
```

To specify role for a user

```
"bob"     Cleartext-Password := "Pa$sW04d"
                Arista-AVPair = "shell:cvp-roles=network-admin",
                Service-Type = NAS-Prompt-User
```

15.2.2.1.2 TACACS+

For TACACS+ there is no vendor specific code, just different strings.

Note: CloudVision support for TACACS+ servers can be affected with the setting of the “service” parameter. Some TACACS servers may require "service = shell" instead of "service = exec" in the TACACS+ configuration (*tacacs.conf*).

This example configures user “bob” in the admin group and specifies certain attributes. It specifies a "cvp-roles" attribute for the CloudVision role name (it can also be a list of roles).

```
A. tacacs.conf
group = admingroup {
   default service = deny
   service = exec {
      default attribute = permit
      priv-lvl = 15
      cvp-roles = network-admin
   }
 enable = nopassword

}
user = bob {
   login = cleartext "secret"
 member = admingroup
}
B. CVP AAA settings
C. Switch AAA configlet
```

15.2.2.1.3 CISCO ACS

To ensure that authentication and authorization work properly, complete the following procedures.

- Creating Identity Groups and Users
- Creating a Shell Profile using ACS
- Creating and Mofiying Access Policy

15.2.2.1.3.1Creating Identity Groups and Users

1. Select **Users and Identity Stores**, and then select **Identity Groups**.
2. Make sure a group named <*user-group*> exists. If this group does not exist, add it.
3. Add new users under the group named <*user-group*>.

15.2.2.1.3.2Creating a Shell Profile using ACS

1. Go to the **Policy Elements** page.
2. Select **Device Administration > Shell Profiles**.
3. Click the **Create** button to create a new shell profile.
4. Select the **Custom Attributes** tab, and then add a new mandatory attribute named “cvp-roles”.
5. Specify one or more of the following values to the new “cvp-roles” attribute:
   - network-admin
   - network-operator

   Note: If you have created custom role(s) under CVP Account Management, you can use them.
6. Check to make sure that under the “Common Tasks Attributes” table, “Assigned Privilege Level” and “Max Privilege Level” are added by default with and the specified value is **15**. Also, verify that requirement is set “Mandatory.”

15.2.2.1.3.3Creating and Modifying Access Policy

1. Go to the Access Policies section and select the **Default Device Admin** policy.
2. Make sure that “Allow PAP/ASCII” option in the Authorization section is enabled (selected).
3. In the Authorization section, create a new rule named “Rule-1”.
4. Make sure that the status of the new rule (“Rule-1”) is Enabled, and set the identity group as “<*user-group*>”.
5. Select the shell profile that outlines the cvp-roles for all users under the group named <*user-group*>.

   Note: Alternatively, you can set add shell profile in the “default rule” section.
6. Make sure that “Service Selection Rules” (under the “Access Policies” section), is using the policy named “Default Device Admin”. The policy should be listed in the “Results” column of “Service Selection Policy” table, and the “status” column should be green, indicating that the policy is enabled.

   The shell profile should be automatically applied to all users under the ground named <*user-group*>.

15.2.2.1.4 Supported TACACS Types

CloudVision Portal (CVP) supports different types of TACACS. Table **Supported TACACS Types** lists the supported types of TACACS, including the following information for each TACACS type:

- Supported version
- Service shell (whether it is supported for each type)
- Service exec (only the following attributes are supported):
  - acl

- default
- double-quote-values
- message
- optional
- protocol
- return
- script
- set

Table 17: Supported TACACS Types

TACACS Type	Supported Version	Service Shell	Service Exec
tac_plus (Shruberry)	F4.0.4.26	Not Applicable	Supported
tac_plus (Probono)	201706241310 201503290942/DES	Supported	Supported
CISCO ACS	4.4.0.46 5.3.0.40	Supported	Not Applicable

Related topics:

- Access to the Access Control Page
- Adding AAA Servers
- Removing AAA Servers

15.2.3 Removing AAA Servers

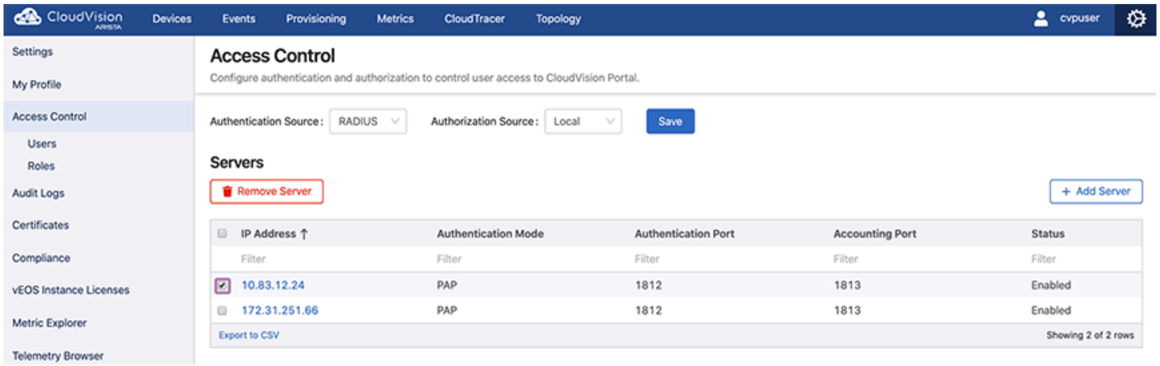
Complete these steps to remove AAA servers:

1. Navigate to the **Access Control** page.
2. Select required options from **Authentication source** and **Authorization source** drop-down menus.

   The systems lists all current servers.
3. Select required servers for removal.
4. Click **Remove Server(s)** at the upper right corner of the **Servers** section.

   The systems lists all current servers.

   Figure 15-5: Remove AAA Servers

   Access Control

   Configure authentication and authorization to control user access to CloudVision Portal.

   Authentication Source : RADIUS

   Authorization Source : Local

   Servers

□	IP Address ↑	Authentication Mode	Authentication Port	Accounting Port	Status
	Filter	Filter	Filter	Filter	Filter
☑	10.83.12.24	PAP	1812	1813	Enabled
□	172.31.251.66	PAP	1812	1813	Enabled

   Showing 2 of 2 rows
5. Click **Delete**.

   The system deletes selected AAA servers.

Related Topics:

- Access to the Access Control Page
- Adding AAA Servers
- Modifying AAA Servers

15.3 About Users and Roles

Account management is based on users and roles. In the CloudVision Portal, users and roles have specific meaning.

Users	A user is a person who uses the CVP application and is authenticated by the system through the use of account credentials (username and password). which is maintained by CVP or external enterprise servers. Only the users with account management module credentials (Account management administrator) can create and manage users. The account management administrator specifies the authentication credentials, name and contact information, status, and CVP permissions when creating user accounts for new users. Account management administrators control which CVP modules users are authorized to use by assigning roles to users (the role assignments can be changed as needed at any time). **Note:** Activity of CVP users is logged and can be viewed in the Audit Logs page.
Roles	A role is a set of read and write module permissions that defines user authorization to modules in CloudVision Portal. The account management administrator specifies the read and write permissions of each module when they create roles. Only account management administrators can create and manage roles. Roles enable account management administrators to efficiently manage user permissions by assigning roles to users, and by changing the role assigned to users. CloudVision Portal provides two default roles, one for the system administrator (network-admin) and one for a basic operator (network-operator).

15.3.1 Default Roles

CloudVision Portal provides two default roles. These default roles can be assigned to users as needed.

network-admin	A user with the default “network-admin” role has read and write permissions for all CVP modules. In addition, this role has both device-level write permissions and database-level write permissions.
network-operator	A user with the default “network-operator” role has only read permissions for all CVP modules. Users with this role cannot make changes to the CVP database.

Note: The read and write permissions cannot be changed for the default roles. But, custom roles can be created where read and write permissions can be modified.

For more information, see Managing User Accounts.

15.4 Managing User Accounts

The system uses the following functionalities to manage user accounts:

- Adding New User Accounts
- Modifying User Accounts
- Removing User Accounts

15.4.1 Adding New User Accounts

When you create a new user account, you specify the login information (authentication credentials) of a person that needs to use one or more CVP modules. Personal information for the new user account is optional and can be specified when you create the new user or at a later time.

By default, new user accounts are enabled. The new user is able to use the CVP modules they are permitted to use, based on the role assigned to them. If you do not want the new user to use CVP at this time, select the Disable option (a Status option). You can enable the user account at a later time.

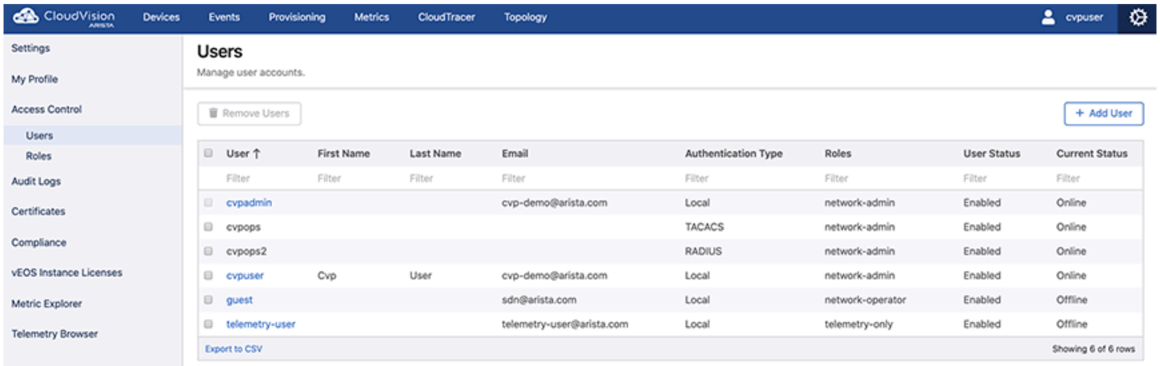
Note: As an alternative to creating user accounts in CVP, you can point CVP to an external AAA server that automatically creates users and maps them to roles during first login.

Complete these steps to create a new user:

1. Navigate to the **Access Control** page.
2. Under **Access Control** in the left menu, click **Users**.

   The Users page lists all current users.

   Figure 15-6: Users Page



Users

Manage user accounts.

□	User ↑	First Name	Last Name	Email	Authentication Type	Roles	User Status	Current Status
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
□	cvpadmin			cvp-demo@arista.com	Local	network-admin	Enabled	Online
□	cvpops				TACACS	network-admin	Enabled	Online
□	cvpops2				RADIUS	network-admin	Enabled	Online
□	cvpuser	Cvp	User	cvp-demo@arista.com	Local	network-admin	Enabled	Online
□	guest			sdn@arista.com	Local	network-operator	Enabled	Offline
□	telemetry-user			telemetry-user@arista.com	Local	telemetry-only	Enabled	Offline

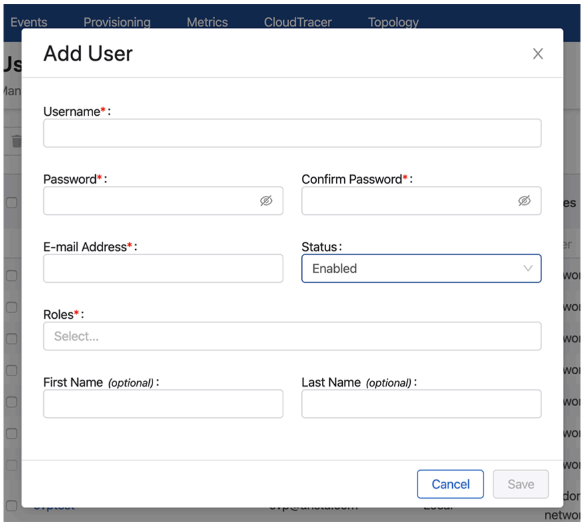
Showing 6 of 6 rows

3. Click **+ New User** at the upper right corner of the Users page.

The system pops-up the **New User** window.

Note: The **New User** pop-up window creates users only with the ‘Local’ authentication type.

Figure 15-7: New User Pop-Up Window



Username*:

Password*:

Confirm Password*:

E-mail Address*:

Status: Enabled

Roles*: Select...

First Name *(optional)*:

Last Name *(optional)*:

4. Provide the required information in corresponding fields.
5. Click **Save**.

The new user account is created.

Note: If the specified role is unavailable in the local CVP, then the network-operator role is automatically assigned to either the RADIUS or TACACS user. Unless you set the account status to disabled, the new user is active using CVP modules based on the role assigned to the user. If user roles conflict when multiple roles are assigned to a user account, the user role with higher privileges is applied to the user account.

Related topics:

- Modifying User Accounts
- Removing User Accounts
- Viewing Activity Logs

15.4.2 Modifying User Accounts

Modifying user accounts enables you to change the following aspects of existing user accounts:

- Login information (password)
- Contact information (email address)
- Status (enabled or disabled)
- Role(s) (the CVP role(s) assigned to the user)
- Personal information (first and last names)

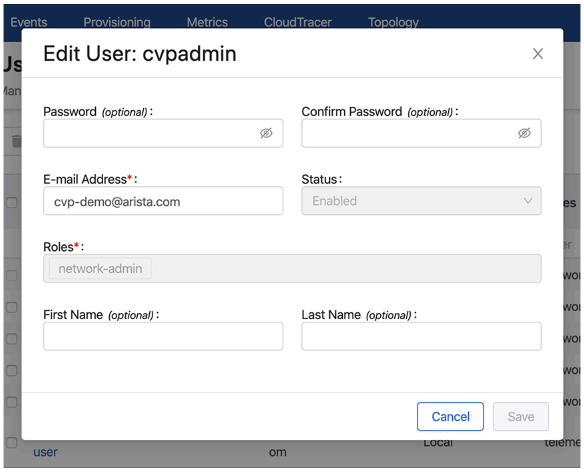
Note: Once changes are saved, they are implemented immediately.

Complete these steps to modify a user account.

1. Navigate to the Access Control page.
2. Under **Access Control**, click **Users**.
3. In the **Users** page, click the edit icon available next to the corresponding user name.

The system pops-up the **Edit User** window displaying all information related to the corresponding user.

Figure 15-8: Edit User Pop-Up Window



Edit User: cvpadmin

Password *(optional)* :

Confirm Password *(optional)* :

E-mail Address* : cvp-demo@arista.com

Status : Enabled

Roles* : network-admin

First Name *(optional)* :

Last Name *(optional)* :

4. Modify the required information.
5. Click **Save**.

Related Topics:

- Adding New User Accounts
- Removing User Accounts
- Viewing Activity Logs

15.4.3 Removing User Accounts

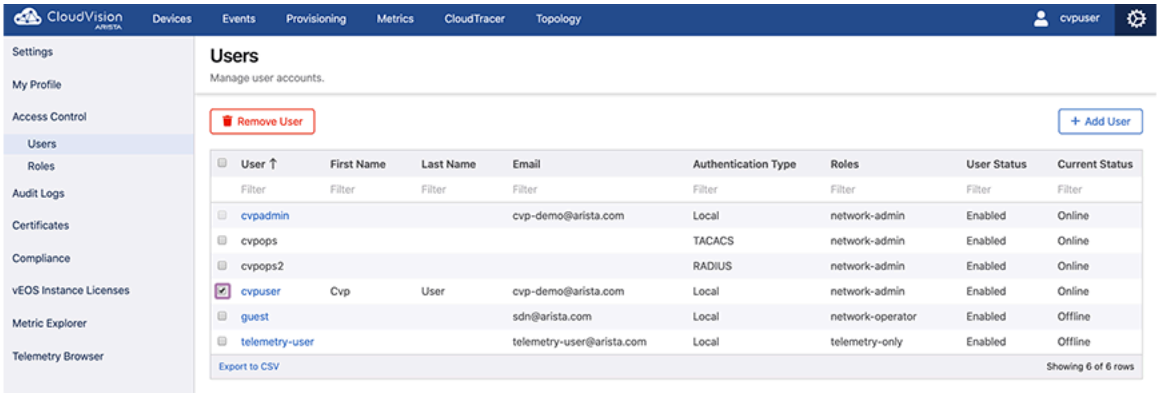
Complete these steps to remove a user account:

1. Navigate to the **Access Control** page.
2. Under **Access Control** in the left, click **Users**.

   The **Users** page appears displays all current user accounts.
3. Select the users for removal.
4. Click **Remove User/Remove Users** at the upper right corner of the Users page.

   The system prompts to confirm deletion.

Figure 15-9: Remove User Account



Users

Manage user accounts.

	User ↑	First Name	Last Name	Email	Authentication Type	Roles	User Status	Current Status
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
□	cvpadmin			cvp-demo@arista.com	Local	network-admin	Enabled	Online
□	cvpops				TACACS	network-admin	Enabled	Online
□	cvpops2				RADIUS	network-admin	Enabled	Online
☑	cvpuser	Cvp	User	cvp-demo@arista.com	Local	network-admin	Enabled	Online
□	guest			sdn@arista.com	Local	network-operator	Enabled	Offline
□	telemetry-user			telemetry-user@arista.com	Local	telemetry-only	Enabled	Offline

5. Click **Delete.**

   The system deletes selected user accounts.

Related Topics:

- Adding New User Accounts
- Modifying User Accounts
- Viewing Activity Logs

15.5 Managing User Roles

The system uses the following functionalities to manage user roles:

- Adding New User Roles
- Modifying User Roles
- Removing User Roles

15.5.1 Adding New User Roles

CloudVision Portal enables you to create new roles as needed to ensure that you are able to efficiently manage CVP user permissions. When you create a new role, you specify the read and write permissions for each CVP module.

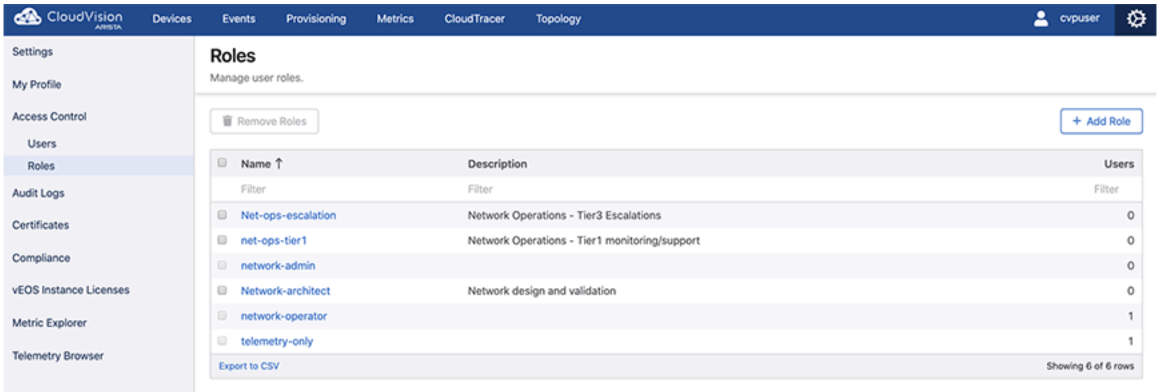
Once a role has been created, it is automatically added to the list of Available roles, and you can assign it to users that should have the permissions defined in the role. When you assign the role to a user, they inherit the read and write permissions defined in the role.

Complete the following steps to create new roles:

1. Navigate to the **Access Control** page.
2. Under **Access Control** in the left menu, click **Roles**.

   The Roles page lists all current roles.

   Figure 15-10: Roles Page



Roles

Manage user roles.

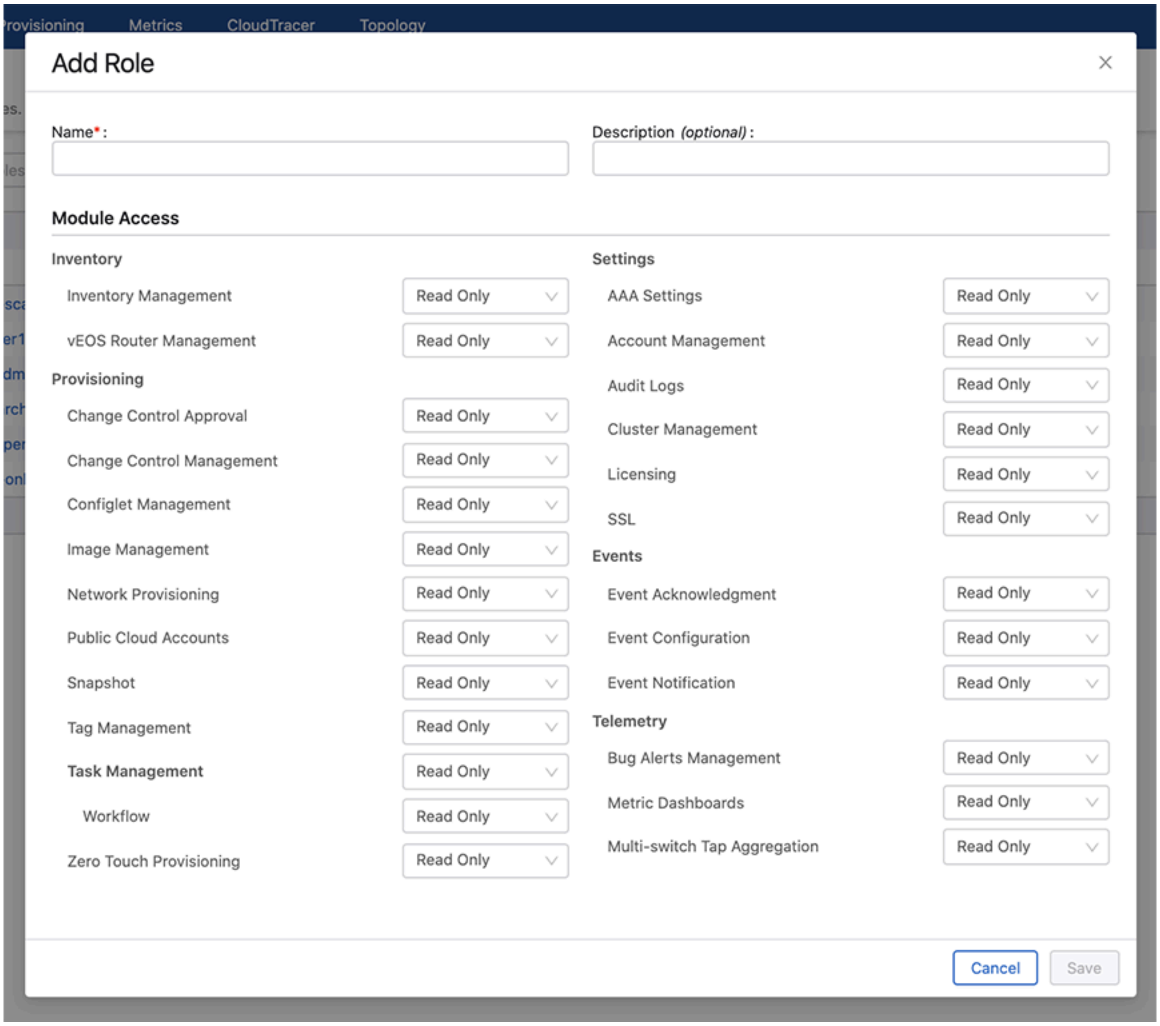
□	Name ↑	Description	Users
	Filter	Filter	Filter
□	Net-ops-escalation	Network Operations - Tier3 Escalations	0
□	net-ops-tier1	Network Operations - Tier1 monitoring/support	0
□	network-admin		0
□	Network-architect	Network design and validation	0
□	network-operator		1
□	telemetry-only		1

Showing 6 of 6 rows

3. Click **+ New Role** at the upper right corner of the Roles page.

The system pops-up the New Role window.

Figure 15-11: New Role Pop-Up Window



Add Role

Name*:

Description *(optional)*:

Module Access

Inventory	
Inventory Management	Read Only
vEOS Router Management	Read Only
Provisioning	
Change Control Approval	Read Only
Change Control Management	Read Only
Configlet Management	Read Only
Image Management	Read Only
Network Provisioning	Read Only
Public Cloud Accounts	Read Only
Snapshot	Read Only
Tag Management	Read Only
Task Management	Read Only
Workflow	Read Only
Zero Touch Provisioning	Read Only

Settings	
AAA Settings	Read Only
Account Management	Read Only
Audit Logs	Read Only
Cluster Management	Read Only
Licensing	Read Only
SSL	Read Only
Events	
Event Acknowledgment	Read Only
Event Configuration	Read Only
Event Notification	Read Only
Telemetry	
Bug Alerts Management	Read Only
Metric Dashboards	Read Only
Multi-switch Tap Aggregation	Read Only

4. Provide the required information in corresponding fields.
5. Click **Save**.

The new role is saved to the CVP database and is available to be assigned to users.

Note: The roles created can be assigned to locally created users or by the external AAA server to its known users.

Related topics:

- Adding New User Roles
- Modifying User Roles
- Viewing Activity Logs

15.5.2 Modifying User Roles

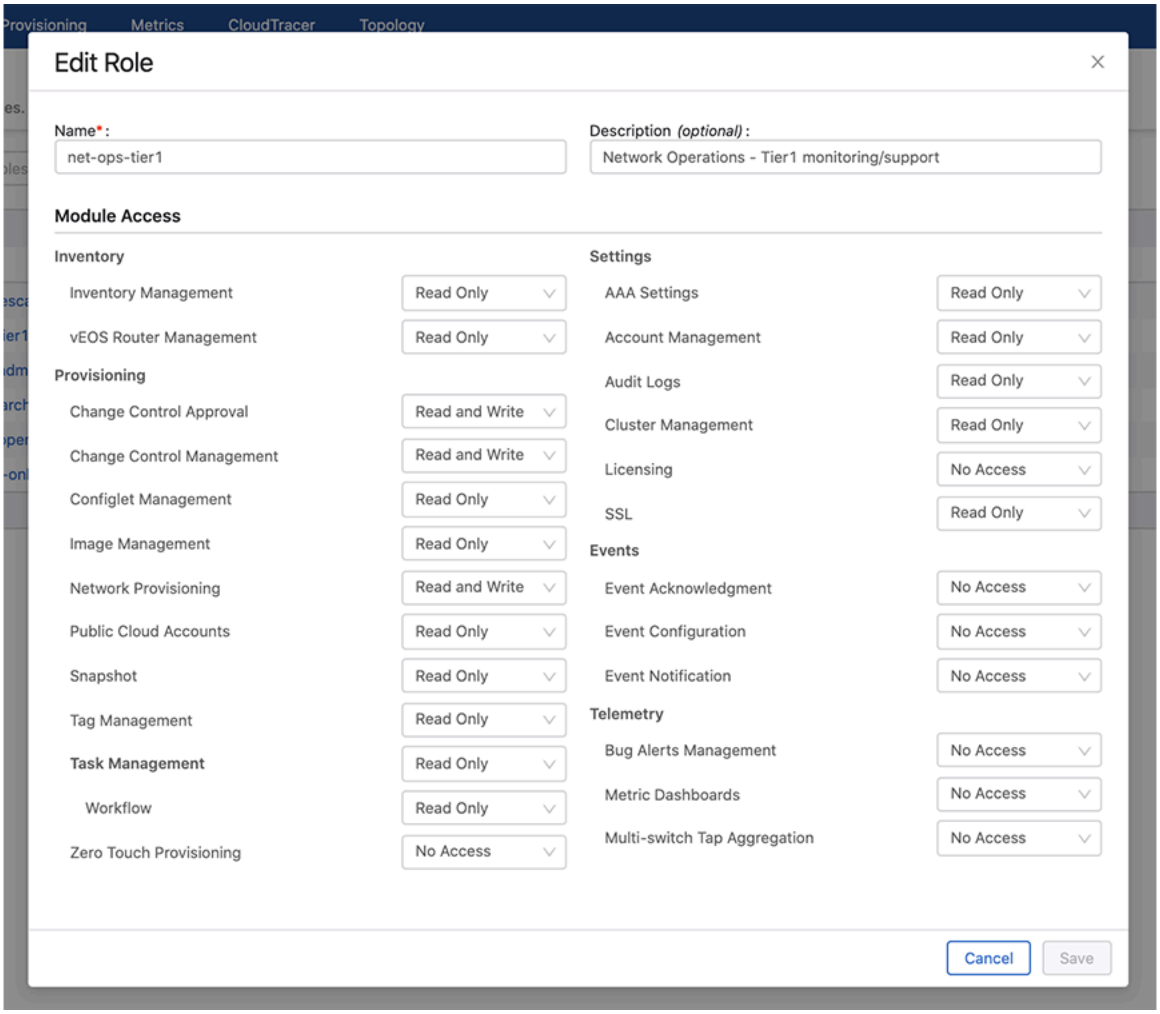
CloudVision Portal provides the functionality required to change the permissions of an existing role. This enables you to efficiently change the permissions of all users that are assigned the role. After you modify the role, all users assigned the role inherit the read and write permissions defined in the new version of the role.

Complete the following steps to modify an existing role:

1. Navigate to the **Access Control** page.
2. Under in the left menu, click **Roles**.
3. In the **Roles** page, click the edit icon available next to the corresponding role name.

   The system pops-up the **Edit Role** window displaying all information related to the corresponding role.

Figure 15-12: Edit Role Pop-Up Window



Edit Role

Name*: net-ops-tier1

Description *(optional)*: Network Operations - Tier1 monitoring/support

Module Access

Inventory	
Inventory Management	Read Only
vEOS Router Management	Read Only
Provisioning	
Change Control Approval	Read and Write
Change Control Management	Read and Write
Configlet Management	Read Only
Image Management	Read Only
Network Provisioning	Read and Write
Public Cloud Accounts	Read Only
Snapshot	Read Only
Tag Management	Read Only
Task Management	Read Only
Workflow	Read Only
Zero Touch Provisioning	No Access

Settings	
AAA Settings	Read Only
Account Management	Read Only
Audit Logs	Read Only
Cluster Management	Read Only
Licensing	No Access
SSL	Read Only
Events	
Event Acknowledgment	No Access
Event Configuration	No Access
Event Notification	No Access
Telemetry	
Bug Alerts Management	No Access
Metric Dashboards	No Access
Multi-switch Tap Aggregation	No Access

4. Modify the required Information.
5. Click **Save**.

   The new version of the role is saved to the CVP database.

   Note: All users assigned the role inherit the read and write permissions defined in the new version of the role.

Related topics:

- Adding New User Roles
- Removing User Roles
- Viewing Activity Logs

15.5.3 Removing User Roles

Complete these steps to remove a user role:

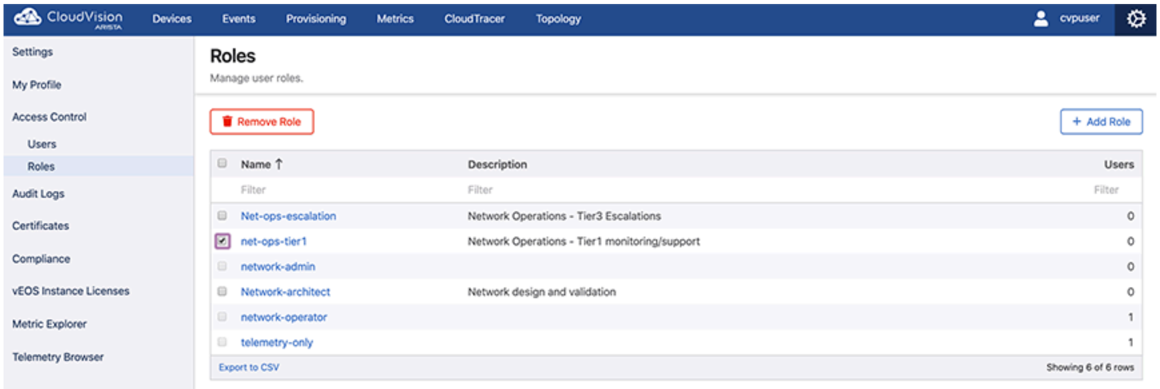
1. Navigate to the **Access Control** page.

2. Under **Access Control** in the left menu, click **Roles**.

   The Roles page lists all current user roles.
3. Select the required user roles for removal.
4. Click **Remove Role/Remove Roles** at the upper right corner of the **Roles** page.

   The system prompts to confirm removal.

   Figure 15-13: Remove User Role



Roles

Manage user roles.

□	Name ↑	Description	Users
	Filter	Filter	Filter
□	Net-ops-escalation	Network Operations - Tier3 Escalations	0
☑	net-ops-tier1	Network Operations - Tier1 monitoring/support	0
□	network-admin		0
□	Network-architect	Network design and validation	0
□	network-operator		1
□	telemetry-only		1

Showing 6 of 6 rows

5. Click **Delete**.

   The system deletes selected user roles.

   Note: A role assigned to user(s) cannot be deleted.

Related topics:

- Adding New User Roles
- Modifying User Roles
- Viewing Activity Logs

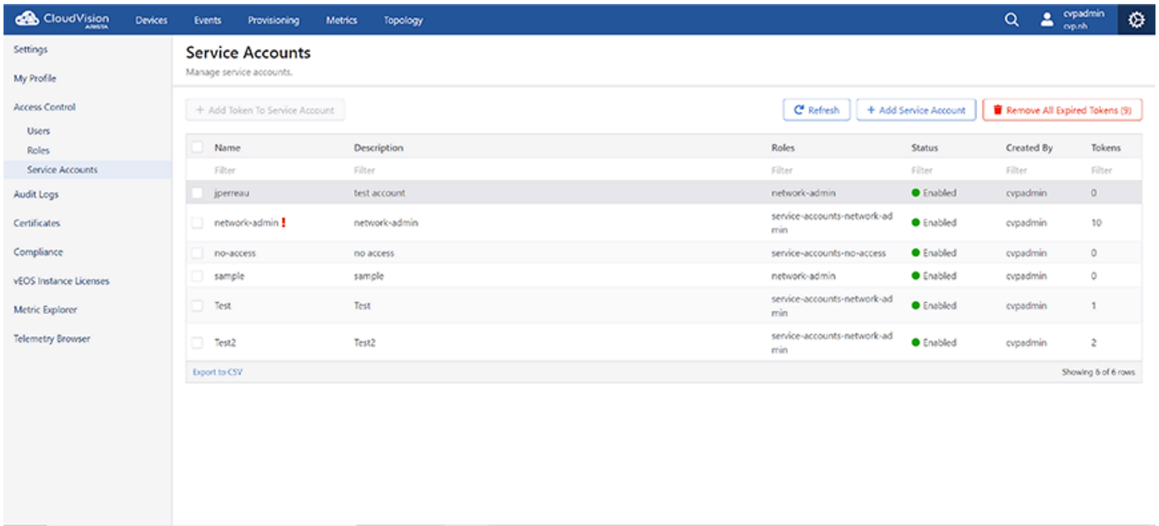
15.6 Service Accounts

The service accounts in CloudVision access APIs in a controlled manner. You must create authentication tokens for service accounts to validate APIs.

To access the Service Accounts screen, navigate to the Settings screen (Click the gear icon at the upper right corner of the screen) > **Access Control** > **Service Accounts**.

The Service Accounts screen provides brief information of all service accounts in a tabular format. See the figure below.

Figure 15-14: Service Accounts Screen



Service Accounts

Manage service accounts.

Name	Description	Roles	Status	Created By	Tokens
jperreau	test account	network-admin	● Enabled	cvpadmin	0
network-admin !	network-admin	service-accounts-network-admin	● Enabled	cvpadmin	10
no-access	no access	service-accounts-no-access	● Enabled	cvpadmin	0
sample	sample	network-admin	● Enabled	cvpadmin	0
Test	Test	service-accounts-network-admin	● Enabled	cvpadmin	1
Test2	Test2	service-accounts-network-admin	● Enabled	cvpadmin	2

Showing 6 of 6 rows

Note: The red exclamation mark on service accounts indicates expired tokens. Hovering the cursor on the red exclamation mark displays the count of expired tokens.

You can perform the following tasks from this screen:

- Adding Service Accounts
- Editing Service Accounts
- Adding Tokens to Service Accounts
- Deleting Service Account Tokens

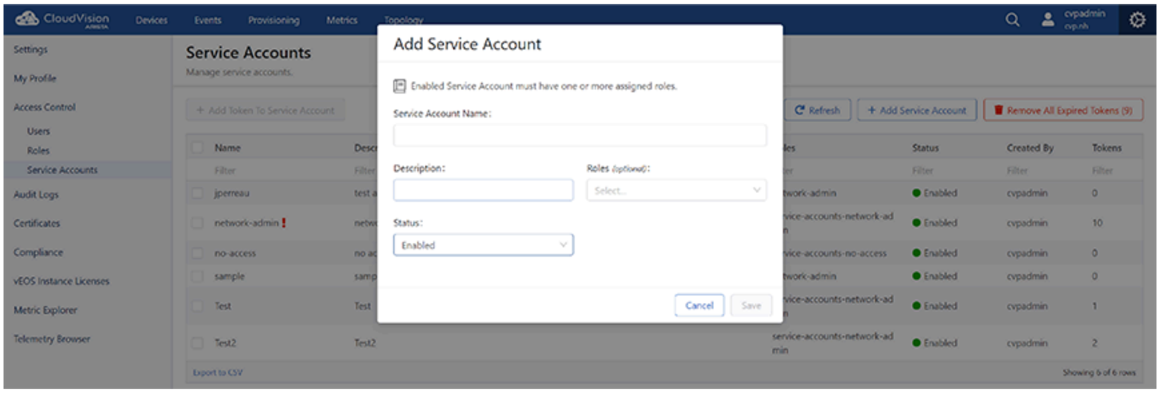
15.6.1 Adding Service Accounts

Perform the following steps to add a service account:

1. On the Service Accounts screen, click **+ Add Service Account**.

   The system displays the Add Service Account screen.

   Figure 15-15: Add Service Account Screen



Add Service Account

Enabled Service Account must have one or more assigned roles.

Service Account Name:

Description:

Roles (optional): Select...

Status: Enabled

2. Type the service account name and description in respective fields.
3. Select preferred roles (optional) and status from respective dropdown menus.

   Note:

- Enabled service accounts must have one or more roles assigned to it.
- Disabled service accounts may not have any roles assigned to it.

4. Click **Save**.

Note: If the Service Accounts screen does not display the new service account, Click **Refresh**.

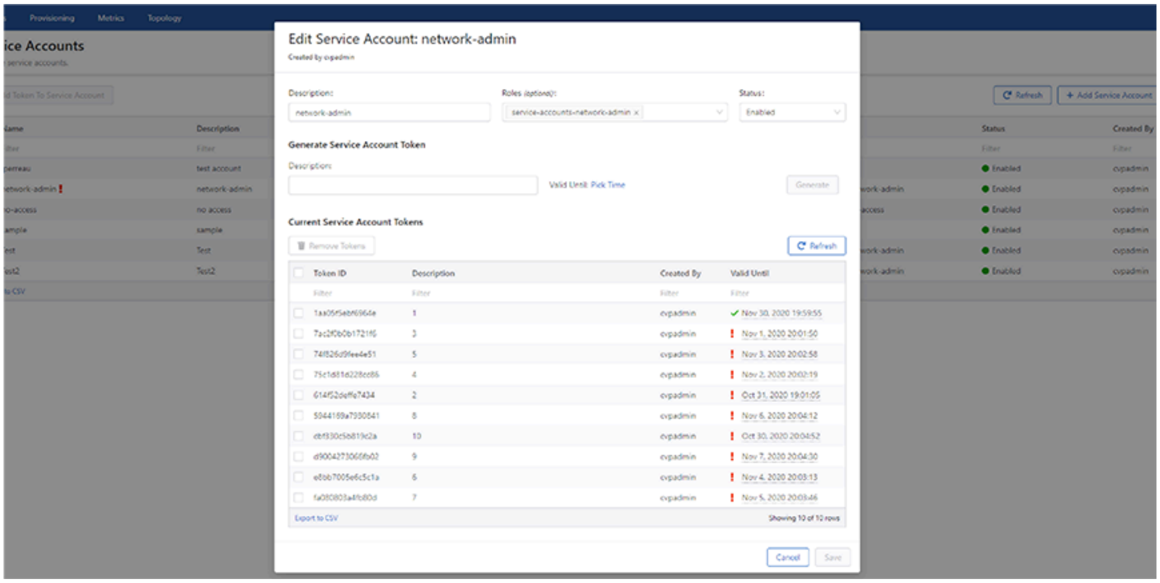
15.6.2 Editing Service Accounts

Perform the following steps to edit a service account:

1. On the Service Accounts screen, click the required service account listed in the table.

   CVP opens the **Edit Service Account:** *service_name* screen.

   Figure 15-16: Edit Service Account Screen



Edit Service Account: network-admin

Created by cvpadmin

Description: network-admin

Roles *(optional)*: service-accounts-network-admin ×

Status: Enabled

Generate Service Account Token

Description:

Valid Until: Pick Time

Generate

Current Service Account Tokens

Remove Tokens

Refresh

□	Token ID	Description	Created By	Valid Until
	Filter	Filter	Filter	Filter
□	1aa05f5ebf6964e	1	cvpadmin	✓ Nov 30, 2020 19:59:55
□	7ac2f0b0b17216	3	cvpadmin	! Nov 1, 2020 20:01:50
□	74f826d9fee4e51	5	cvpadmin	! Nov 3, 2020 20:02:58
□	75c1d81d228ec86	4	cvpadmin	! Nov 2, 2020 20:02:19
□	614f52deffe7434	2	cvpadmin	! Oct 31, 2020 19:01:05
□	5044169a7980841	8	cvpadmin	! Nov 6, 2020 20:04:12
□	dbf830c5b819c2a	10	cvpadmin	! Oct 30, 2020 20:04:52
□	d9004273066fb02	9	cvpadmin	! Nov 7, 2020 20:04:30
□	e8bb7005e6c5c1a	6	cvpadmin	! Nov 4, 2020 20:03:13
□	fa080803a4fc80d	7	cvpadmin	! Nov 5, 2020 20:03:46

Export to CSV

Showing 10 of 10 rows

Cancel Save

Note: Alternatively, select the checkbox of required service account and click **+ Add Token to Service Account**.

2. Update required changes in the **Description** field, **Roles** dropdown and **Status** dropdown.

   Note:

   - Enabled service accounts must have one or more roles assigned to it.
   - Disabled service accounts may not have any roles assigned to it.

3. Click **Save**.

15.6.3 Adding Tokens to Service Accounts

Perform the following steps to create a token for service accounts:

1. On the Service Accounts screen, click the required service account listed in the table.

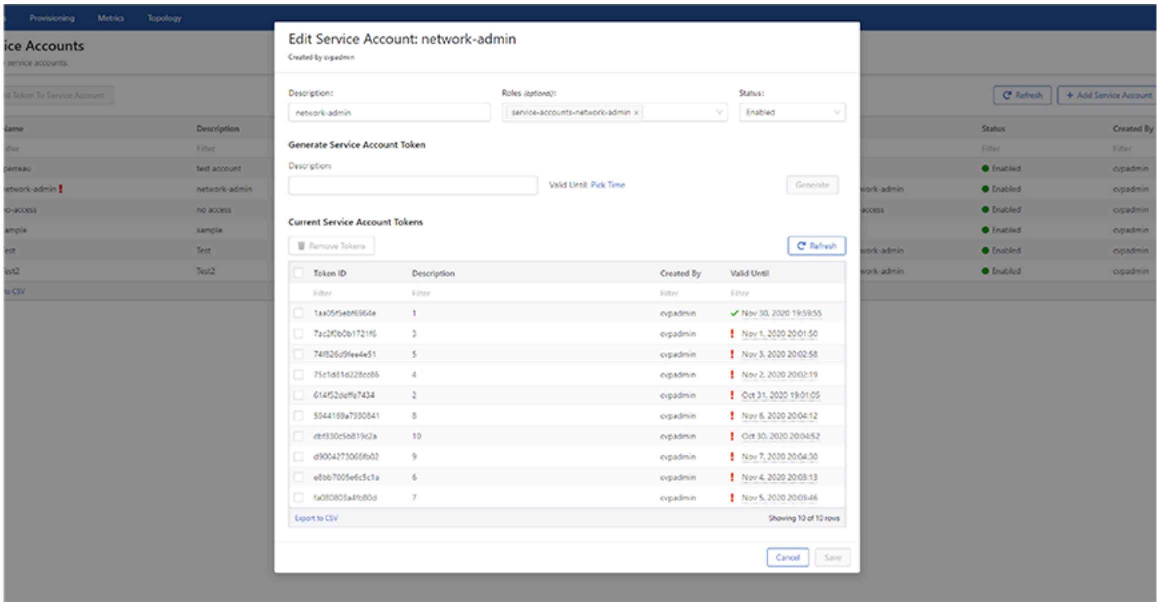
   CVP opens the **Edit Service Account:** *service_name* screen.

   Note: Alternatively, select the checkbox of required service account and click **+ Add Token to Service Account**.

2. Under **Generate Service Account Token**, type brief summary in the **Description** field.

See the figure below.

Figure 15-17: Generate Service Account Token



Edit Service Account: network-admin

Created by cvpadmin

Description: network-admin

Roles *(optional)*: service-accounts-network-admin ×

Status: Enabled

Generate Service Account Token

Description:

Valid Until: Pick Time

Generate

Current Service Account Tokens

Remove Tokens

Refresh

□	Token ID	Description	Created By	Valid Until
	Filter	Filter	Filter	Filter
□	1aa05f5ebf6964e	1	cvpadmin	✓ Nov 30, 2020 19:59:55
□	7ac2f0b0b1721f6	3	cvpadmin	! Nov 1, 2020 20:01:50
□	74f826d9fee4e51	5	cvpadmin	! Nov 3, 2020 20:02:58
□	75c1d81d228ec86	4	cvpadmin	! Nov 2, 2020 20:02:19
□	614f52deffe7434	2	cvpadmin	! Oct 31, 2020 19:01:05
□	5944169a7930841	8	cvpadmin	! Nov 6, 2020 20:04:12
□	cbf330c5b819c2a	10	cvpadmin	! Oct 30, 2020 20:04:52
□	d9004273066fb02	9	cvpadmin	! Nov 7, 2020 20:04:30
□	e8bb7005e6c5c1a	6	cvpadmin	! Nov 4, 2020 20:03:13
□	fa0f0803a4fb80d	7	cvpadmin	! Nov 5, 2020 20:03:46

Export to CSV

Showing 10 of 10 rows

Cancel

Save

3. Click **Pick Time** and select the expiry date.

   Note: The maximum duration for validity is one year.

4. Click **Generate**.

   Note: If the table under **Current Service Account Tokens** does not display the new token, click **Refresh**. The new token gets access to APIs based on roles selected for the service account.

15.6.4 Deleting Service Account Tokens

Perform the following steps to delete a service account:

1. On the Service Accounts screen, click the required service account listed in the table.

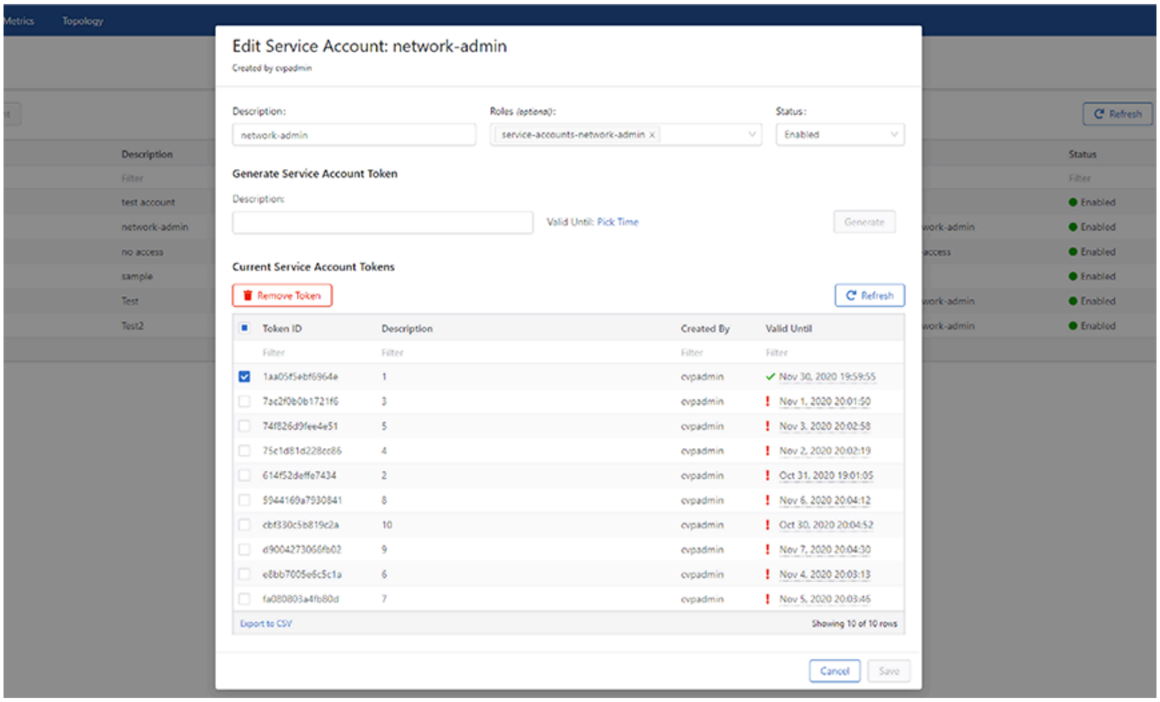
   CVP opens the **Edit Service Account:** *service_name* screen. Tokens associated to this service accounts are listed in the table under **Current Service Account Tokens**.

   Note: Alternatively, select the checkbox of the required service account and click **+ Add Token to Service Account**.

2. Select token(s) to be deleted.
3. Click **Remove Token(s)**.

See the figure below.

Figure 15-18: Delete Service Account Tokens



Edit Service Account: network-admin

Created by cvpadmin

Description: network-admin

Roles *(optional)*: service-accounts-network-admin ×

Status: Enabled

Generate Service Account Token

Description:

Valid Until: Pick Time

Current Service Account Tokens

	Token ID	Description	Created By	Valid Until
☑	1aa05f5ebf6964e	1	cvpadmin	✓ Nov 30, 2020 19:59:55
□	7ac2f0b0b1721f6	3	cvpadmin	! Nov 1, 2020 20:01:50
□	74f826d9fee4e51	5	cvpadmin	! Nov 3, 2020 20:02:58
□	75c1d81d228cc86	4	cvpadmin	! Nov 2, 2020 20:02:19
□	614f52deffe7434	2	cvpadmin	! Oct 31, 2020 19:01:05
□	5944169a7930841	8	cvpadmin	! Nov 6, 2020 20:04:12
□	cbf330c5b819c2a	10	cvpadmin	! Oct 30, 2020 20:04:52
□	d9004273066fb02	9	cvpadmin	! Nov 7, 2020 20:04:30
□	e8bb7005e6c5c1a	6	cvpadmin	! Nov 4, 2020 20:03:13
□	fa080803a4fb80d	7	cvpadmin	! Nov 5, 2020 20:03:46

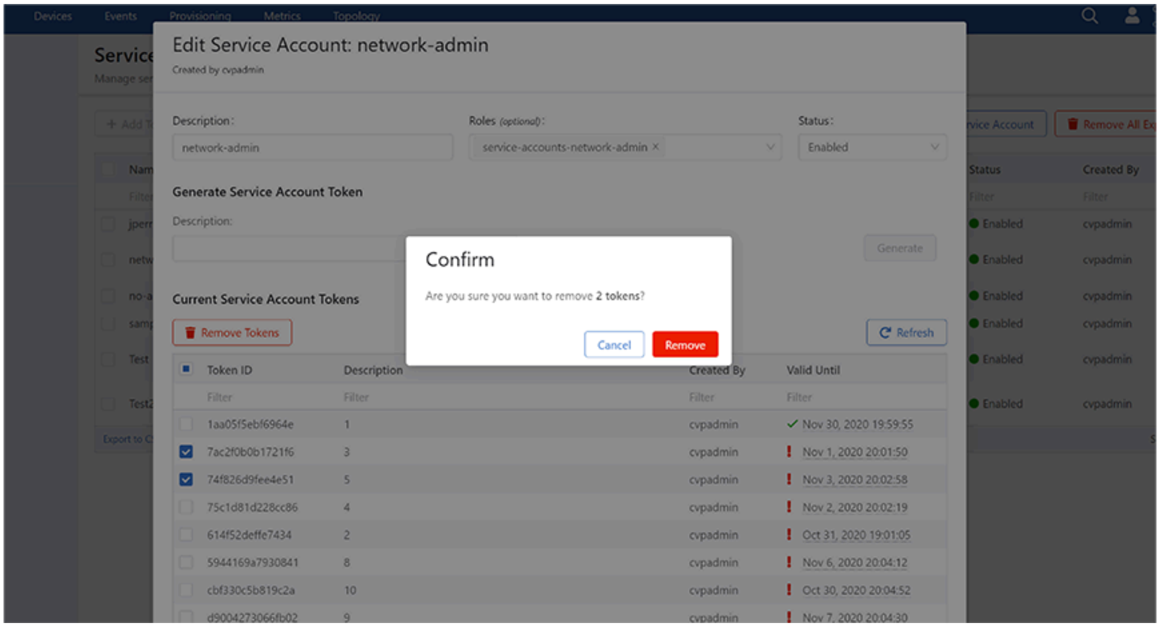
Export to CSV Showing 10 of 10 rows

CVP prompts to confirm the initiated task.

4. Click **Remove** on the confirmation box.

See the figure below.

Figure 15-19: CVP Confirmation to Delete Tokens



Edit Service Account: network-admin

Created by cvpadmin

Description: network-admin

Roles *(optional)*: service-accounts-network-admin ×

Status: Enabled

Confirm

Are you sure you want to remove 2 tokens?

	Token ID	Description	Created By	Valid Until
□	1aa05f5ebf6964e	1	cvpadmin	✓ Nov 30, 2020 19:59:55
☑	7ac2f0b0b1721f6	3	cvpadmin	! Nov 1, 2020 20:01:50
☑	74f826d9fee4e51	5	cvpadmin	! Nov 3, 2020 20:02:58
□	75c1d81d228cc86	4	cvpadmin	! Nov 2, 2020 20:02:19
□	614f52deffe7434	2	cvpadmin	! Oct 31, 2020 19:01:05
□	5944169a7930841	8	cvpadmin	! Nov 6, 2020 20:04:12
□	cbf330c5b819c2a	10	cvpadmin	! Oct 30, 2020 20:04:52
□	d9004273066fb02	9	cvpadmin	! Nov 7, 2020 20:04:30

5. Click **Save**.

Note:

- If the table continues to display deleted token(s), click **Refresh**.

- To simultaneously delete all expired tokens across all service accounts, click **Remove all Expired tokens (*n*)** on the Service Accounts screen where *n* stands for the number of expired tokens.

15.7 Viewing Activity Logs

The **Audit Logs** page displays activity logs of user accounts and user roles.

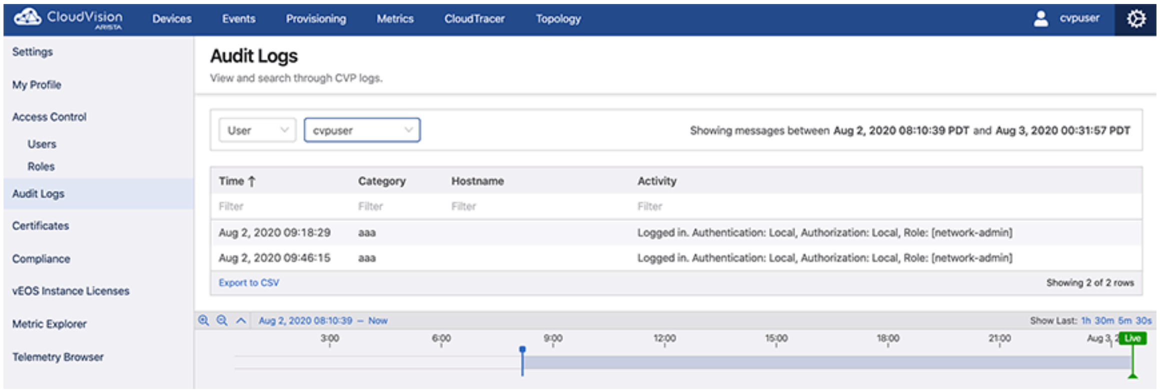
Complete these steps to view activity logs:

1. Click the gear icon at the upper right corner of the CVP page.
2. Click **Audit Logs** on the left menu.

   The system displays the Audit Logs page.
3. Select desired options from **View** logs for drop-down menus.

   The system displays corresponding logs.

   Figure 15-20: Audit Logs Page



Audit Logs

View and search through CVP logs.

Showing messages between **Aug 2, 2020 08:10:39 PDT** and **Aug 3, 2020 00:31:57 PDT**

Time ↑	Category	Hostname	Activity
Filter	Filter	Filter	Filter
Aug 2, 2020 09:18:29	aaa		Logged in. Authentication: Local, Authorization: Local, Role: [network-admin]
Aug 2, 2020 09:46:15	aaa		Logged in. Authentication: Local, Authorization: Local, Role: [network-admin]

Showing 2 of 2 rows

15.8 Advanced Login Options

Multi-Factor Authentication (MFA) and One-Time Passwords authenticate all CVP managed devices when you authenticate with CVP. CVP runs CLIs on managed devices by sending eAPI requests over the gRPC connection established by TerminAttr.

Note:

- Under **Cluster Management** on the settings screen, enable **Advanced login options for device provisioning** to use MFA and one-time passwords.
- CVP needs TACACS to perform command authorization and accounting as per EOS configuration.
- Use the new Device class to make eAPI requests for using this mechanism in Configlet Builder python scripts.

Pre-requisities to install this feature are:

- Devices must run CVP 2018.2.3 or later releases
- Managed devices must have TerminAttr version 1.5.0 or later versions

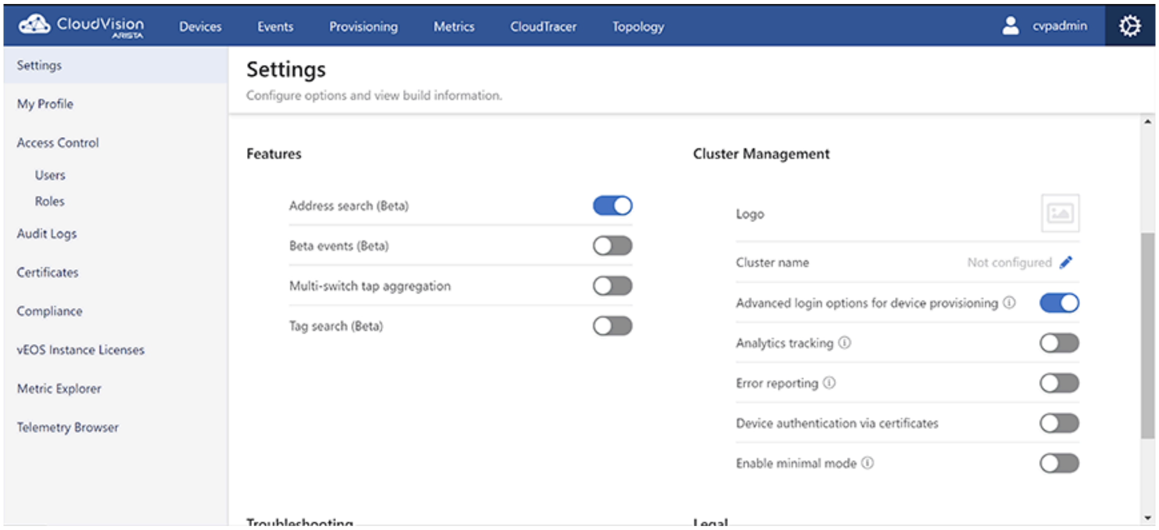
  Note: TerminAttr is included with EOS, but may be a version earlier than v1.5.0. Newer versions are available as an extension (swix)

  Refer to CVP and TerminAttr release notes available at https://www.arista.com/en/support/software-download for detailed information on compatible TerminAttr versions with CVP and EOS.

- Ensure that the eAPI unix domain socket is enabled with `management api http-commands` and `protocol unix-socket` configurations in devices running EOS releases prior to 4.20

To enable MFA and One-Time Passwords authentication, enable **Advanced login options for device provisioning** using the toggle button under **Cluster Management** on the Settings page. See the figure below.

Figure 15-21: Advanced Login Options for Device Provisioning Toggle Button



Settings

Configure options and view build information.

Features

Address search (Beta)	☑
Beta events (Beta)	☐
Multi-switch tap aggregation	☐
Tag search (Beta)	☐

Cluster Management

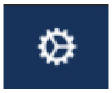
Logo	
Cluster name	Not configured
Advanced login options for device provisioning ⓘ	☑
Analytics tracking ⓘ	☐
Error reporting ⓘ	☐
Device authentication via certificates	☐
Enable minimal mode ⓘ	☐

15.9 Access to the Access Control Page

To gain access to the Access Control Page, complete the following:

1. Click the gear icon on the home page.

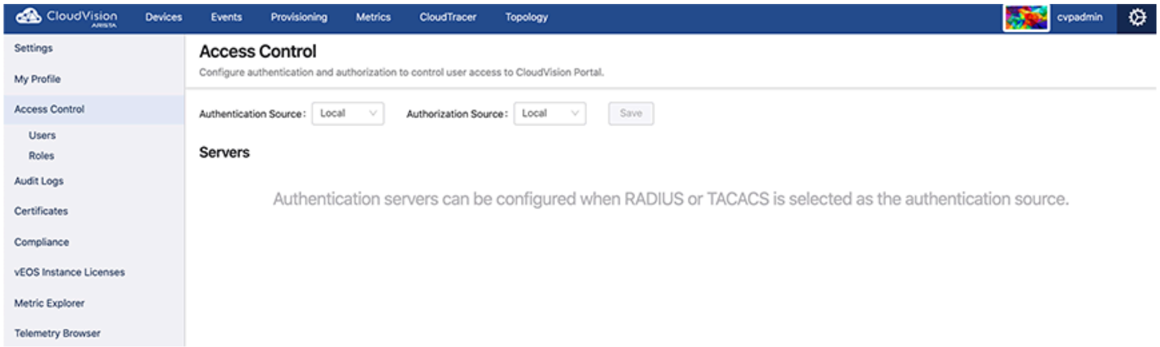
   Figure 15-22: Gear Icon

2. Click **Access Control** in the left menu.

   The system displays the Initial Access Control screen.

   Figure 15-23: Initial Access Control Page

   Access Control

   Configure authentication and authorization to control user access to CloudVision Portal.

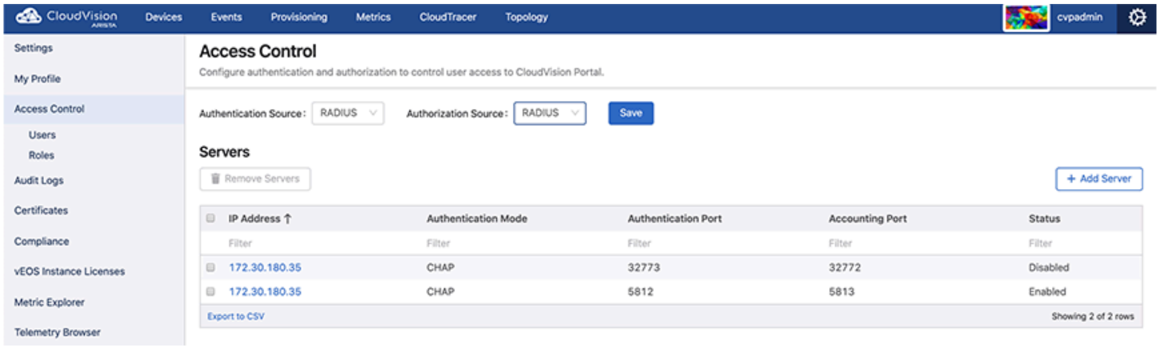
   Authentication Source : Local   Authorization Source : Local

   Servers

   Authentication servers can be configured when RADIUS or TACACS is selected as the authentication source.

The system displays the **Servers** section when either RADIUS or TACACS is selected as Authentication source.

Figure 15-24: AAA Access Control Page



Access Control

Configure authentication and authorization to control user access to CloudVision Portal.

Authentication Source: RADIUS
Authorization Source: RADIUS

Servers

IP Address	Authentication Mode	Authentication Port	Accounting Port	Status
172.30.180.35	CHAP	32773	32772	Disabled
172.30.180.35	CHAP	5812	5813	Enabled

Showing 2 of 2 rows

- If the authentication is local, the authorization must be done locally.
- If the authentication is done externally, the authorization can be done locally or externally.

Table 18: Server Authentication and Authorization

Authentication	Authorization
Local	Local
RADIUS	Local RADIUS
TACACS	Local TACACS

Note: External servers supported by CloudVision are RADIUS and TACACS.

Related topics:

- Managing AAA Servers
- Managing User Accounts
- Managing User Roles
- Access Requirements for Image Bundle Upgrades

Chapter 16

CloudVision Topology

The CloudVision Topology screen provides an explicit visual representation of the connectivity of your network, allowing you to understand your network's structure and performance more easily. It provides the following benefits:

- Easily understand parts of your network by collapsing or filtering out irrelevant parts
- Explore the historical state and performance of your network or watch it update live
- Support for both datacenter and campus style network connectivity

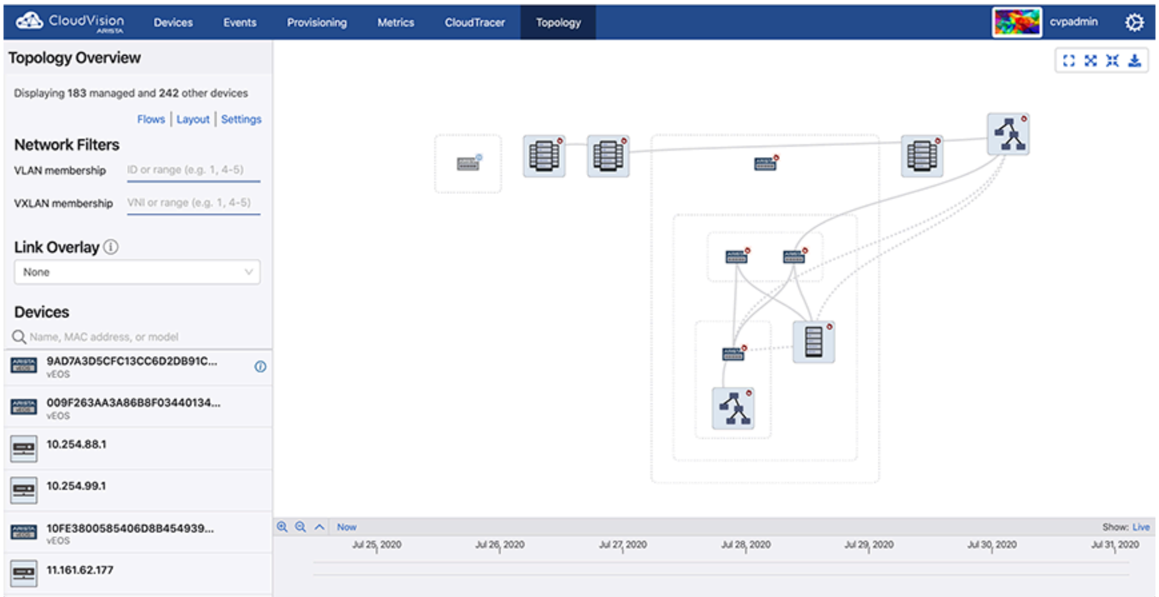
CloudVision topology provides Virtual Extensible LAN (VXLAN), Internet Protocol Security (IPsec), Distributed Path Selection (DPS), and Link Layer Discovery Protocol (LLDP) network links between endpoints.

Note:

- Information and Statistics for each member link is accessed from the side panel. See Topology Overview.
- If this screen does not display any devices, refer to the CVP release notes at https://www.arista.com/en/support/software-download for compatibility issues.

To view the Topology screen, click the **Topology** tab on the CloudVision Portal.

Figure 16-1: Topology Screen



Displaying 183 managed and 242 other devices

VLAN membership: ID or range (e.g. 1, 4-5)

VXLAN membership: VNI or range (e.g. 1, 4-5)

Link Overlay: None

Name, MAC address, or model

9AD7A3D5CFC13CC6D2DB91C... vEOS

009F263AA3A86B8F03440134... vEOS

10.254.88.1

10.254.99.1

10FE3800585406D8B454939... vEOS

11.161.62.177

This screen is divided into main and side panels. The main panel displays the main topology visualization. Devices are drawn with paths to connect them if they share at least one network connection. They are grouped into containers that can be expanded or collapsed to control which portions of the network are displayed in detail. See Main Panel of the Topology Screen .

The side panel provides the following panes to perform the specified functionalities:

- To customize the network view:
  - Topology Overview
  - Topology Layout Pane

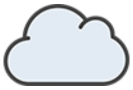
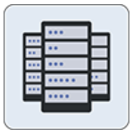
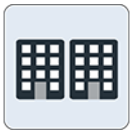
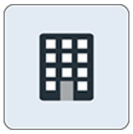
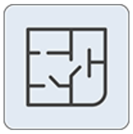
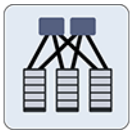
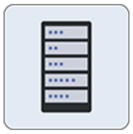
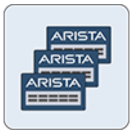
    - Topology Options Pane
- To view the component information:
    - Container Details Pane
    - Device Details Pane
    - Link Details Panel
    - Flow Visibility

16.1 Main Panel of the Topology Screen

The main panel displays the network topology where devices are grouped into containers according to their connectivity or assigned role in the network.

The icons in the following table represents specified containers:

Table 19: Icons Used in Network Topology

Cloud 	Datacenter 	Campus 
Building 	Floor 	Pod 
Rack 	Spine 	

The icons in the following table represents specified devices:

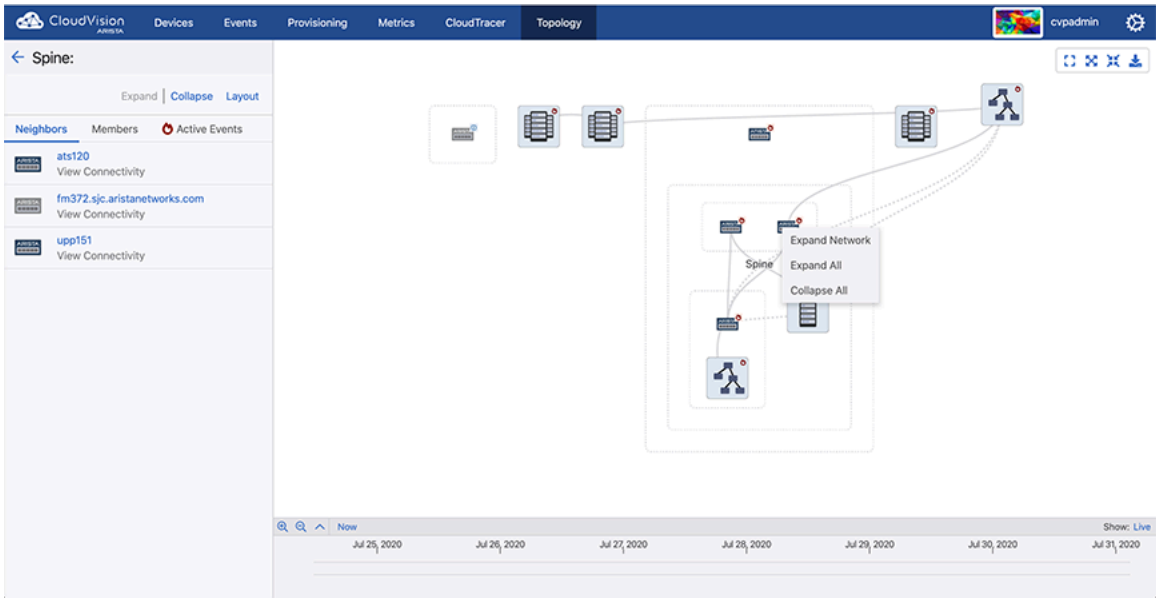
Table 20: Device Icons

Switch	Wireless Access Point	Management Device Badge
ARISTA	ARISTA **Note:** Blue WAP represents managed devices. Gray WAP represents unmanaged devices.	☸ **Note:** This badge next to a device icon represents a management device.
Computer	**Third Party Device**	**Telephone**
💻	🖴	☎

This panel provides the following options for a detailed view:

- Zoom to fit icon - Click to fit the topology on the screen.
- Expand containers icon - Click to expand all containers in the topology.
- Collapse containers icon - Click to collapse all containers in the topology.
- Alternatively, right-click on the main panel to get **Expand Network**, **Expand All**, and **Collapse All** options.

Figure 16-2: Right-Click on a Device

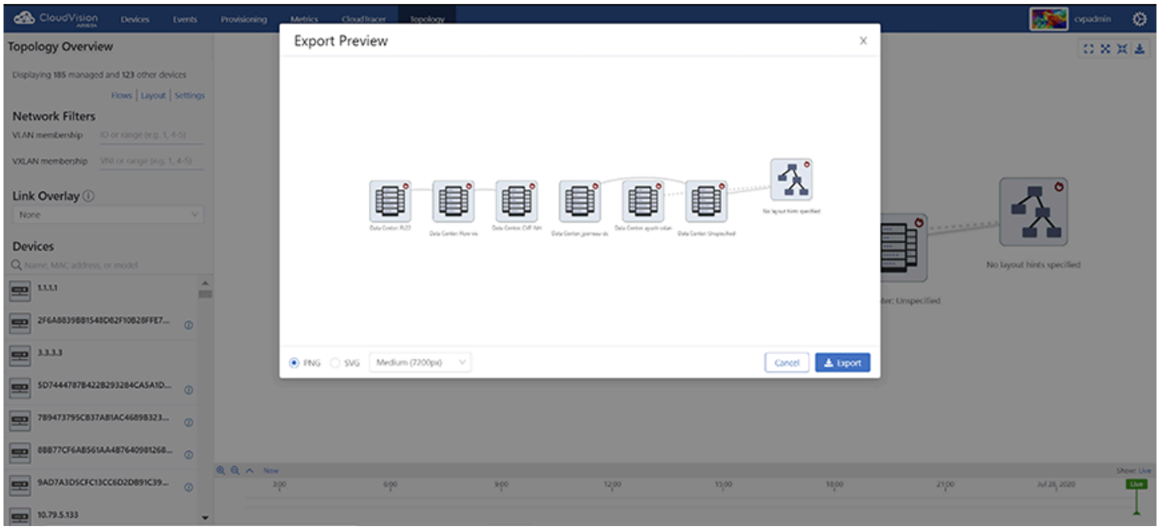


Note: Right-click on a cluster to get cluster specific context menu options.

- Download icon - Click to open the Export Preview pop-up window. Click **Export** for downloading the current topology image to your local drive in either PNG or SVG formats with selected image resolution.

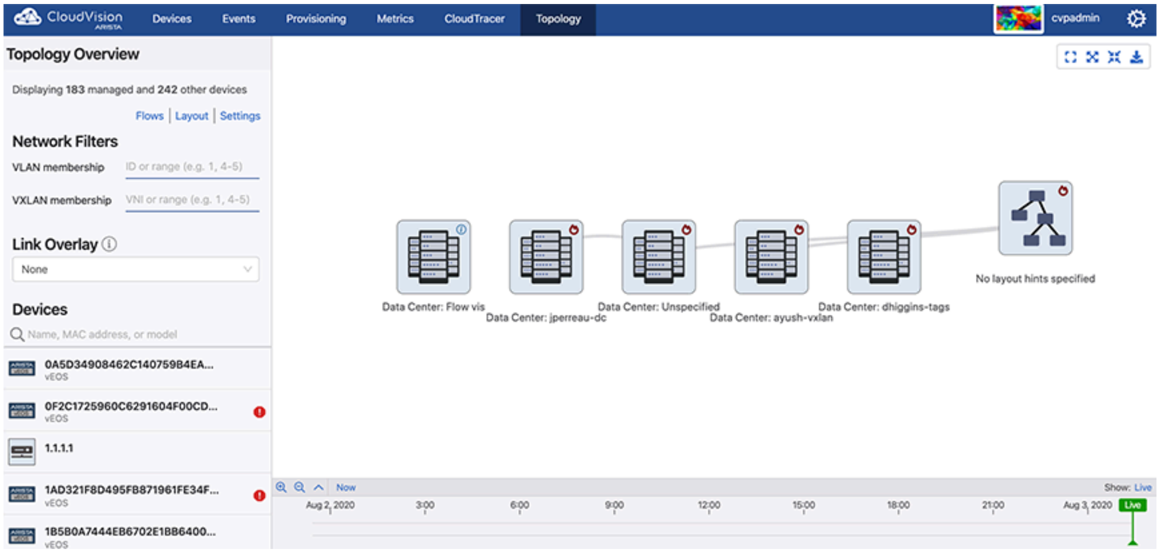
Note: We recommend to select higher resolutions for readable device labels in bigger topologies.

Figure 16-3: Export Preview Pop-Up Window



- Double-click on a container to expand it.
- To collapse a container, hover the cursor on a dotted rectangular box and click on the displayed hyphen symbol.

Figure 16-4: Collapse a Container



- Click container component(s) to view corresponding information on the left panel.
- Selected components are highlighted with dashed frame.

Note: Press and hold the shift key while selecting multiple devices. Press and hold the shift key while dragging to select a region.

- Hover the cursor on a topology component to view the count of corresponding events.

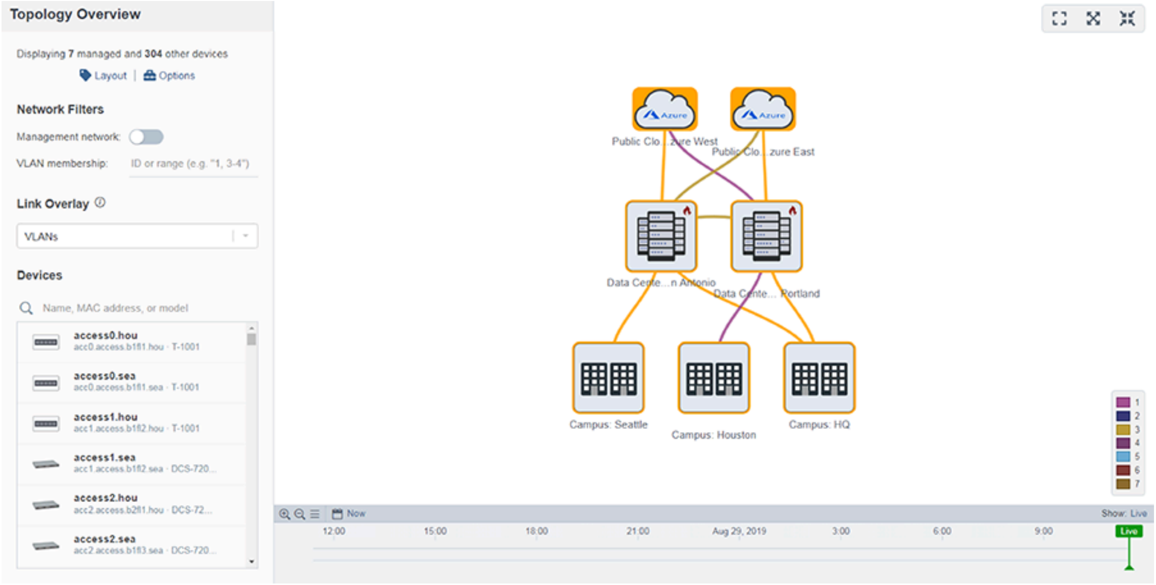
Note: You must enable the option to view events.

16.2 Topology Overview

The Topology Overview pane provides the following options:

- **Layout** - Click to view the **Topology Layout** pane. See Topology Layout Pane.
- **Options** - Click to view the **Topology Options** pane. See Topology Options Pane.
- **Network Filters** - Provides the following options to filter networks:
  - **Tags** - To view desired tags by name and value. The main Topology view will be updated and only devices with the chosen tags will be displayed.
  - **Management network** - Display or hide management networks using the toggle button.
  - **VLAN membership** - To view desired VLAN(s), type either a VLAN ID or a range of VLANs.

Figure 16-5: VLANs in Topology



Topology Overview

Displaying **7** managed and **304** other devices

Layout | Options

Network Filters

Management network: ○

VLAN membership: ID or range (e.g. "1, 3-4")

Link Overlay ⓘ

VLANs

Devices

Name, MAC address, or model

access0.hou
acc0.access.b1f1.hou · T-1001

access0.sea
acc0.access.b1f1.sea · T-1001

access1.hou
acc1.access.b1f2.hou · T-1001

access1.sea
acc1.access.b1f2.sea · DCS-720...

access2.hou
acc2.access.b2f1.hou · DCS-72...

access2.sea
acc2.access.b1f3.sea · DCS-720...

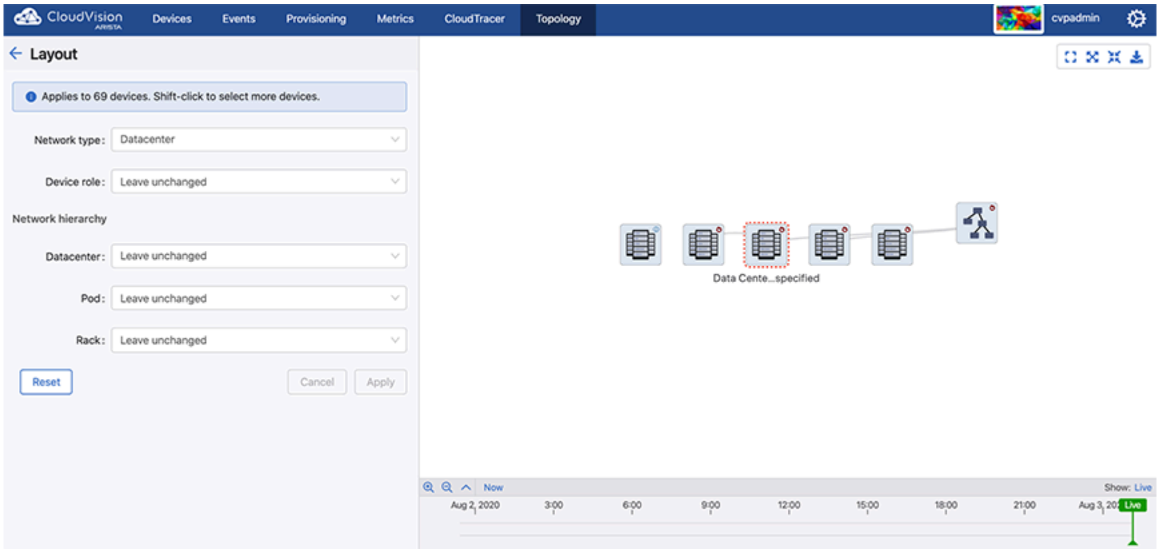
Note: The right panel displays selected VLAN(s) distinguished with various colors.

- **Link Overlay** drop-down menu - Select an overlay to color each link based on selected metric type. Options include:
  - Active Events
  - Bandwidth Utilization
  - Discard Rate
  - Error Rate
  - Traffic Throughput
  - VLANs
  - None
- Devices
  - Search field - Type the device name, MAC address, or model to perform a quick search.
  - List of devices - Click on a device to view the detailed information of corresponding device. See Device Details Pane.

16.3 Topology Layout Pane

On the Topology Overview pane, click **Layout** and select a container component from the topology on the right panel to edit layout hints of multiple device(s) in the **Topology Layout** pane.

Figure 16-6: Topology Layout Pane



Applies to 69 devices. Shift-click to select more devices.

Network type: Datacenter

Device role: Leave unchanged

Network hierarchy

Datacenter: Leave unchanged

Pod: Leave unchanged

Rack: Leave unchanged

Topology automatically tries to guess a layout with specified containers and roles for your devices based on their connectivity and advertised LLDP capabilities. However, you might sometimes find that the automatic categorization is incorrect, or you simply want a custom layout different from what was originally envisioned. The **Layout** pane lets you override the automatic categorizations and control the layout more directly.

The layout works on the basis of hints that describe the role of a device, whether it exists within a datacenter or campus network, and where it should go in that network. Devices with similar roles and positions in the hierarchy are grouped together. Parallel hierarchies like network pods or racks are created if different names are used.

Examples

- A device named *athens* is a datacenter leaf switch, but it has no rack server connections yet and is miscategorized as an edge switch. You can click on athens and then select **Node type** as **leaf** to force it to take on a leaf role. It moves into the leaf position inside its datacenter hierarchy.
- To partition your network into New York and San Francisco datacenters, multi-select the devices or containers that must go in the New York datacenter, type **New York** in the **Datacenter** field, and confirm it. Repeat the same process for San Francisco. Now, your network is divided between these two datacenters, and you can expand or collapse New York and San Francisco datacenters independently to view only one datacenter at a time.

This pane provides the following selections:

- **Network type** drop-down menu - Select the network type that most closely matches your network arrangement. It provides the following options:
  - **Campus** - Devices are manually arranged in containers for different buildings and floors. It provides the following options:
    - **Node type** drop-down menu - Select the preferred device type or roles.

        - **Building** drop-down menu - Select the building name that the selected device preferred to be placed into.
        - **Floor** drop-down menu - Select the preferred floor number in the selected building.
        - **Devices** drop-down menu (Optional) - Set a name to be used to group devices in the selected floor.
    - **Datacenter** - Aspine-and-leaf type layout is used and devices are arranged into pods and racks. It provides the following options:
        - **Node Type** drop-down menu - Select the preferred device type or roles.
        - **Pod** drop-down menu - Select the pod name that the selected device preferred to be placed into.

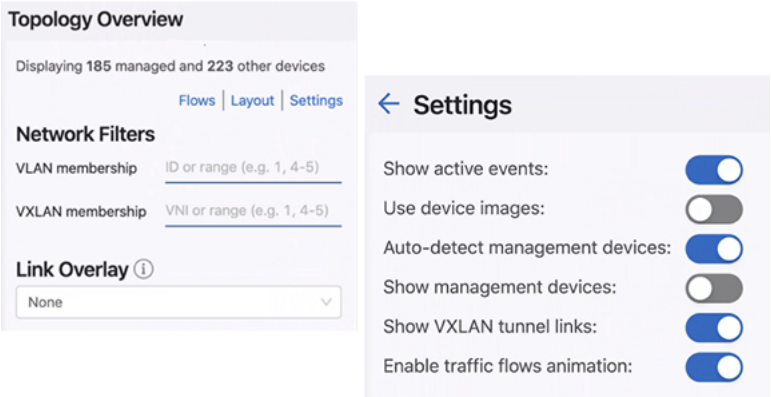
          Note: Devices in different pods of the same datacenter appear in different pod containers that can be expanded and collapsed independently.
        - **Rack** drop-down menu - Select the name of a rack similar to pod.
- **Show Advanced** - Click to view the **Skip Auto-Generated Classifications** drop-down menu.

  Note: Click **Hide Advanced** to hide the **Skip Auto-Generated Classifications** drop-down menu. If the **Skip Auto-Generated Classifications** option is enabled, CVP does not automatically identifies the device(s). Only manually-provided layout hints affect the layout of the selected device(s).
- **Set all to Auto** - Use the automatic layout classification exclusively; all manually-specified layout hints are removed from selected devices.
- **Save** button - Click to save latest changes.

16.4 Topology Options Pane

On the **Topology Overview** pane, click **Options** to edit display settings of topology.

Figure 16-7: Topology Options Screen



Topology Overview

Displaying 185 managed and 223 other devices

Network Filters

VLAN membership: ID or range (e.g. 1, 4-5)

VXLAN membership: VNI or range (e.g. 1, 4-5)

Link Overlay ⓘ

None

← Settings

Show active events: ●

Use device images: ○

Auto-detect management devices: ●

Show management devices: ○

Show VXLAN tunnel links: ●

Enable traffic flows animation: ●

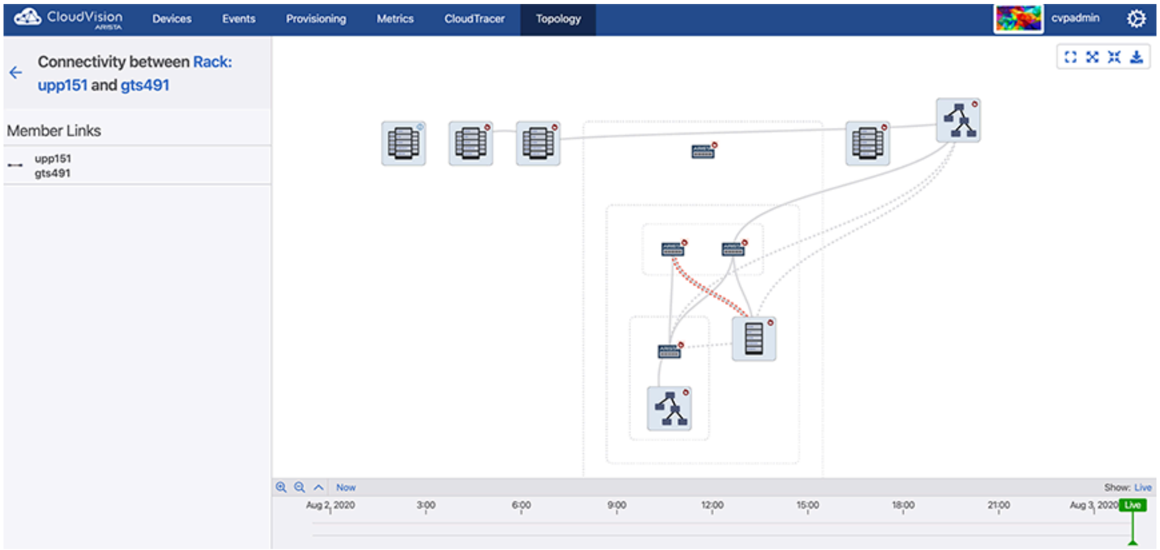
This pane provides the following selections:

- **Show active events:** toggle button - If this option is enabled, active events are shown as badges on devices. These are the same events that are displayed on the Events page. If the same device has multiple events, the badge type of the highest severity event is displayed. Containers also show badges if they contain any devices with active events. This allows you to quickly find active events anywhere in a large network.

  Note: This option is enabled by default.

- **Use device images:** toggle button - Enable this option to view photorealistic device images for identified devices. If this option is disabled, icons are used instead. See Figure 461: Network Hierarchy Tree with Images.

Figure 16-8: Network Hierarchy Tree with Images

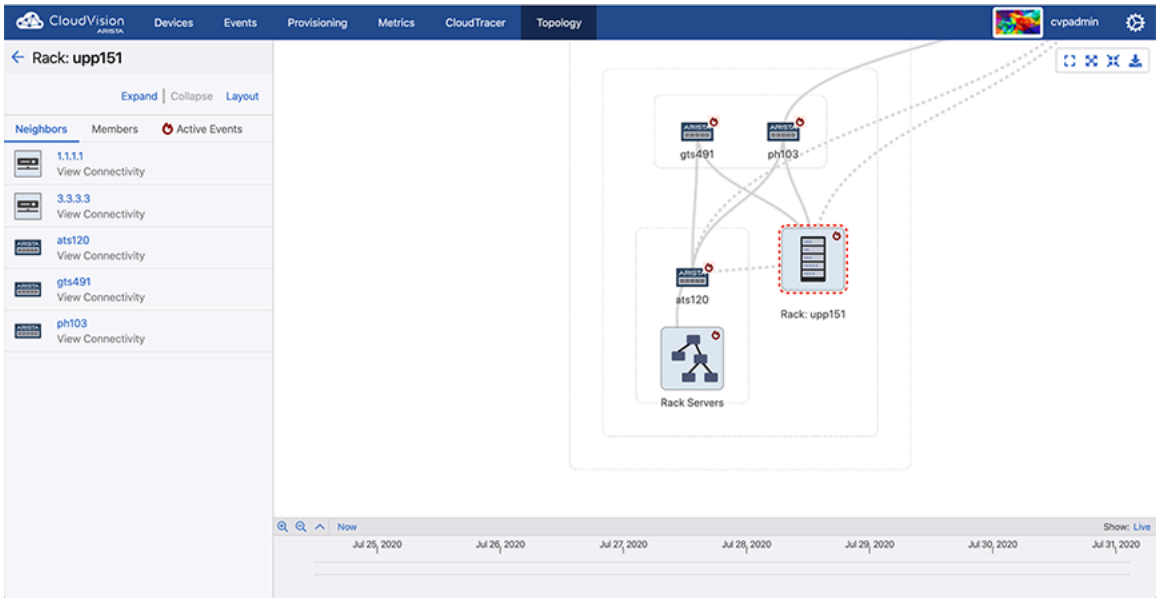


- **Auto-detect management devices: -** If this option is disabled, CVP will not attempt to automatically identify management devices. Devices are considered management devices if they are known to have a relatively high number of connections over a management interface.
- **Auto tagger hints** pane - Influences the way devices are arranged. If a device's hostname matches the provided text string or regular expression, it will automatically be tagged with the given role. Options include:
  - **Spine Hint**: - Type a text string that is used to identify matching spine devices.
  - **Leaf Hint**: - Type a text string that is used to identify matching leaf devices.
- **Save** button - Click to save latest changes.

16.5 Container Details Pane

To view more information about a device or the devices in a container, click the corresponding device or container on the right panel.

Figure 16-9: Container Pane



This screen provides the following functionalities:

- **Expand** - Expands the selected container.
- **Collapse** - Collapses the selected container.
- **Layout** - Edits layout hints of the selected container. See Topology Layout Pane.
- **Neighbors** - Displays the list of connected devices from neighboring container.

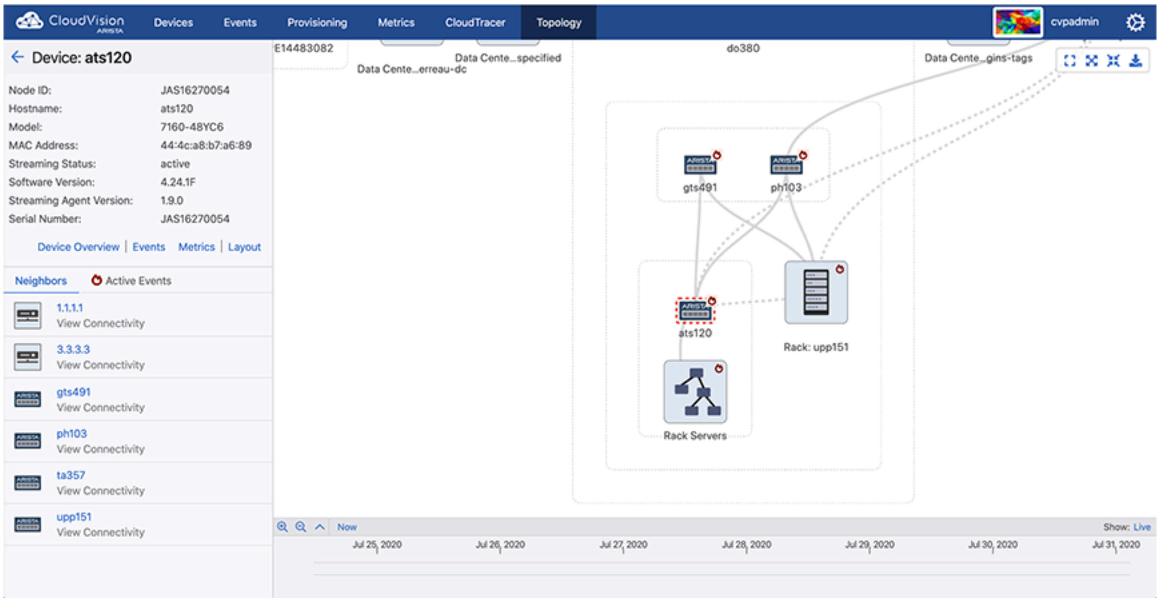
  Note: Click on any neighboring device name to view the corresponding device pane. See Device Details Pane.
- **Members** - Displays the list of container members. Each entry provides the following options:
  - **Device name** - Click to view the corresponding device pane. See Device Details Pane.
  - **View Connectivity** - Click to view the connectivity between selected device and neighboring device. See Link Details Panel.
- **Active Events** (Optional) - Displays events of the selected container. Click on an event link to view the corresponding event details screen.

  Note: This option is available only when the **Show active events** option is enabled in the Topology Options pane. See Topology Options Pane.

16.6 Device Details Pane

To get a device pane, click on a device (switch, wireless access point, server, or telephone) in the right panel.

Figure 16-10: Device Details Pane



Device: ats120

Node ID:	JAS16270054
Hostname:	ats120
Model:	7160-48YC6
MAC Address:	44:4c:a8:b7:a6:89
Streaming Status:	active
Software Version:	4.24.1F
Streaming Agent Version:	1.9.0
Serial Number:	JAS16270054

Device Overview | Events Metrics | Layout

Neighbors | Active Events

- 1.1.1.1 View Connectivity
- 3.3.3.3 View Connectivity
- gts491 View Connectivity
- ph103 View Connectivity
- ta357 View Connectivity
- upp151 View Connectivity

This screen provides the following functionalities:

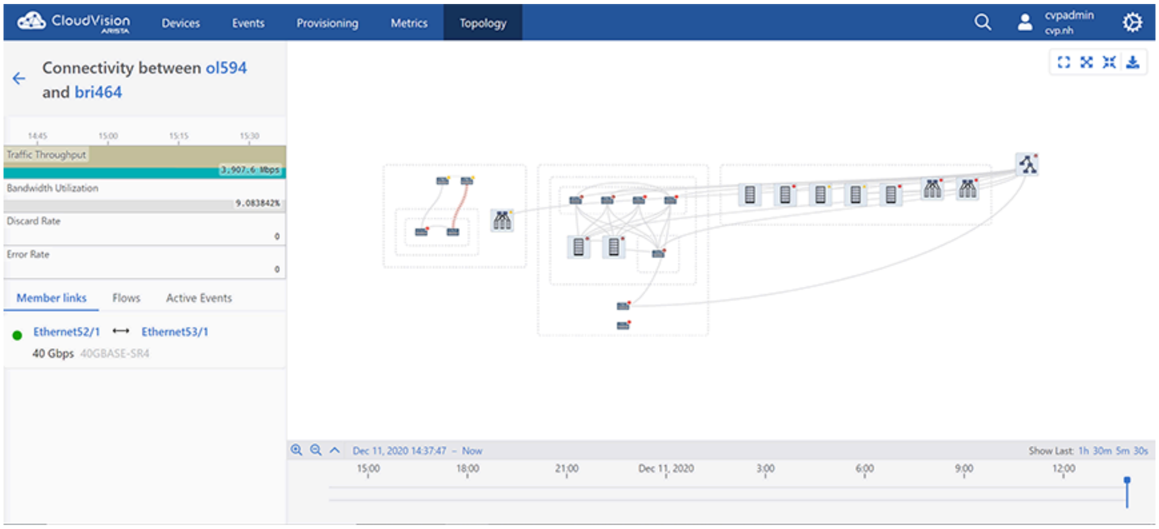
- Additional information on the device.
- **Device Overview** - Click to view the Interface Overview screen. Device Overview
- **Events** - Click to view the Events summary screen. See Events Summary Screen.
- **Layout** - Click to edit layout hints of the selected device. See Topology Layout Pane.
- **Neighbors** - Displays the neighbors list of selected device. Each entry provides the following options:
  - ***Device name*** - Click to view the corresponding device pane.
  - **View Connectivity** - Click to view the connectivity between selected device and neighboring device. See Link Details Panel.
- **Active Events** (Optional) **-** Displays events of the selected device. Click on an event link to view the corresponding **Event Details** screen.

Note: This option is available only when the **Show active events** option is enabled in the **Topology Options** pane. See Topology Options Pane.

16.7 Link Details Panel

To view the links panel, click on a connectivity link between two components on the right panel.

Figure 16-11: Links Panel



Connectivity between ol594 and bri464

Traffic Throughput 3,907.6 Mbps

Bandwidth Utilization 9.083842%

Discard Rate 0

Error Rate 0

Ethernet52/1 ⟷ Ethernet53/1

40 Gbps 40GBASE-SR4

Links represent connections between devices or clusters of devices. If two devices or clusters have at least one network connection, a link is drawn to connect them. If they have many network connections, they still have a single link in the topology view and information provided for the link is aggregated over those connections. Expanding and collapsing containers expand and collapse links; you may sometimes want to expand containers to see links in greater detail.

This screen provides the following information of the selected connectivity link:

- Click on a device name to view the corresponding device panel.
- Metrics - Displays statistics of traffic throughput, bandwidth utilization, discard rate, and error rate.

  Note: Hover the cursor on the metrics to view metrics at the corresponding time.

- **Member Links** - Displays the list of connected ports.

  Note: Click on any connected port link to view the corresponding **Interface Overview** screen.

- **Flows** - Displays traffic flows active on the selected connectivity link.

  Note: Clicking on a listed traffic flow link provides information on connected devices.

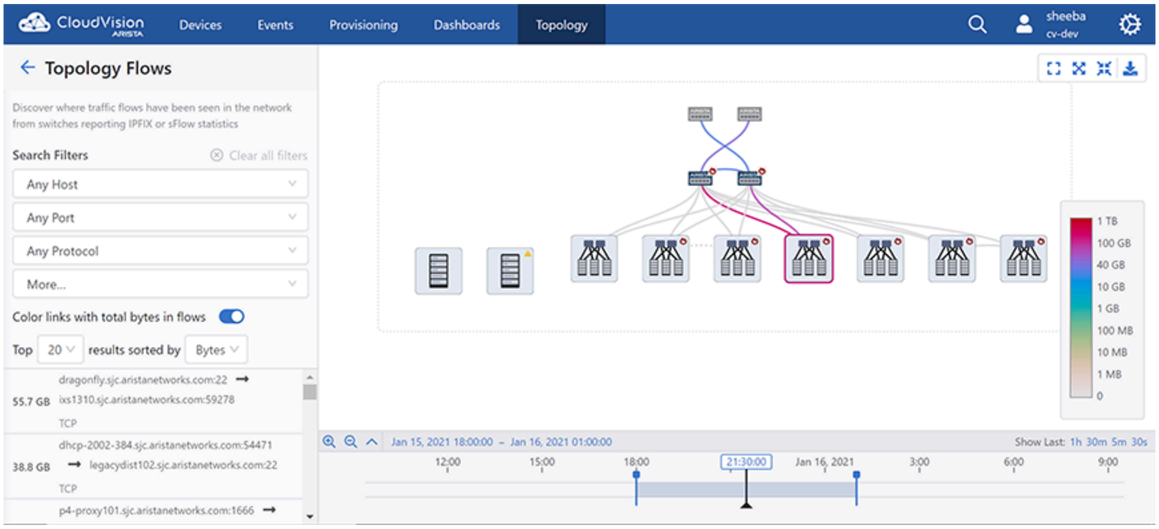
- **Events** - Displays events of the selected connectivity link. Click on an event link to view the corresponding **Event Details** screen.

  Note: This option is available only when the **Show active events** option is enabled in the **Topology Options** panel. See Topology Options Pane.

16.8 Flow Visibility

On the Topology Overview pane, click **Flows** to open the **Topology Flows** panel. This screen displays traffic flows detected by EOS devices on the network.

Figure 16-12: Topology Flow Search



Topology Flows

Discover where traffic flows have been seen in the network from switches reporting IPFIX or sFlow statistics

Search Filters ⓧ Clear all filters

Any Host

Any Port

Any Protocol

More...

Color links with total bytes in flows

Top 20 results sorted by Bytes

55.7 GB dragonfly.sjc.aristanetworks.com:22 → ixs1310.sjc.aristanetworks.com:59278 TCP

38.8 GB dhcp-2002-384.sjc.aristanetworks.com:54471 → legacydist102.sjc.aristanetworks.com:22 TCP

p4-proxy101.sjc.aristanetworks.com:1666 →

Note:

- CVP displays traffic flows only when SFLOW or IPFIX are configured on EOS devices.
- For complete flow visibility, flow collectors are required on all devices along the traffic flow path.

The **Topology Flows** panel provides search filters.

Search for traffic flows the following filters:

- Data source (Flow Tracking (sFlow or IPFIX) or Inband telemetry
- IP address
- Host
- Port
- Protocol
- VRF
- Latency
- Locality

Use the **Color links with total bytes in flows** toggle button to view aggregated bytes or packets of a traffic flow on a single link.

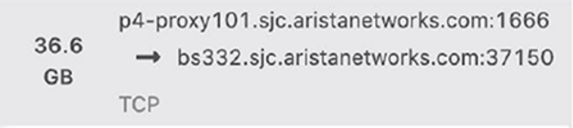
Note:

- The color of the link depends on the corresponding flow metric as displayed on the color chart.
- Hover the cursor on a topology flow to view the flow metric of the corresponding link.

You can limit the count of displayed flows via the options available in the **Top** menu. Traffic flows sorted by the selected metric (**Bytes**, **Packets**, **Mean Latency**, **Max Latency**, and **Min Latency** from the **results sorted by** menu are displayed on the top of the list.

The listed traffic flows in the side panel displays the five-tuple information. The arrow indicates the direction of traffic flow.

Figure 16-13: Topology Host showing Flows



36.6 GB

p4-proxy101.sjc.aristanetworks.com:1666

→ bs332.sjc.aristanetworks.com:37150

TCP

In this example, TCP protocol is used in the traffic flowing from p4-proxy101.sjc.aristanetworks.com via 1666 port to bs332.sjc.aristanetworks.com via 37150 port. 36.6GB of data is flown over the given time window.

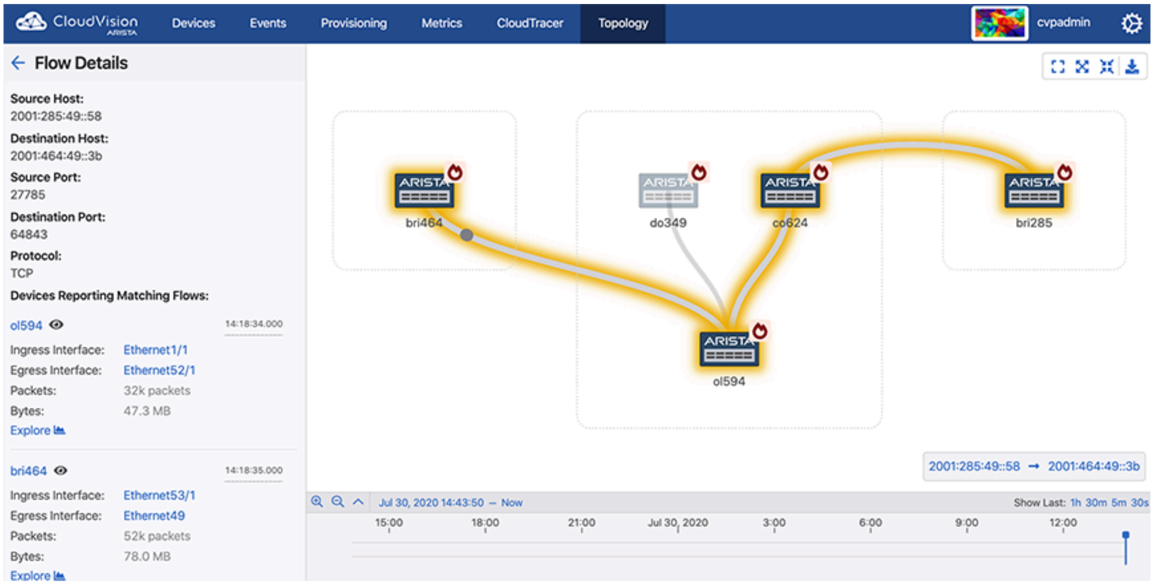
Flows are displayed based on the timeline selected at the bottom of the Window. To search previous flows, select an earlier time by either using the timeline's time selector, or by dragging the displayed time window to a different position.

Note: Live view updates the data every 60 seconds.

Flow Highlight

Clicking on a listed traffic flow result highlights the nodes and edges in the graph where the flow has been seen. Animated dots indicate the direction of the traffic flow.

Figure 16-14: Highlighted Traffic Flow



Flow Details

Source Host:
2001:285:49::58

Destination Host:
2001:464:49::3b

Source Port:
27785

Destination Port:
64843

Protocol:
TCP

Devices Reporting Matching Flows:

ol594 — 14:18:34.000

Ingress Interface:	Ethernet1/1
Egress Interface:	Ethernet52/1
Packets:	32k packets
Bytes:	47.3 MB

Explore

bri464 — 14:18:35.000

Ingress Interface:	Ethernet53/1
Egress Interface:	Ethernet49
Packets:	52k packets
Bytes:	78.0 MB

Explore

Note:

- In environments that capture flow data through sFlow, devices may not capture short-lived or small flows, especially if the selected time window is small.
- This highlight does not guarantee to capture the exact path; it just displays all the devices and links where that flow was seen in the given time window.

The **Devices Reporting Matching Flows** section displays the five-tuple information and lists devices that reported the flow. Each device entry includes the ingress and egress port-channels, ingress and egress interface, packets, bytes and the timestamp when this flow was seen given the time window.

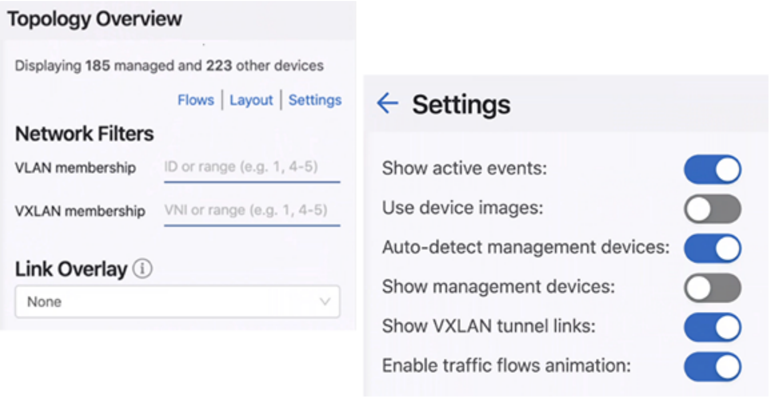
Click on the following entities to view the corresponding specified information:

- Eye icon to magnify the device on the main panel
- *Device hostname* to view the Device Overview page
- *Interface* to view the Interface Overview page
- **Explore** button to view this flow on the Traffic Flows section

Flow Animation

To view traffic flow animation, click **Settings** on the **Topology Overview** panel and enable it using the **Enable traffic flows animation** toggle button.

Figure 16-15: Enabling Traffic Flow Animation in Settings



Topology Overview

Displaying 185 managed and 223 other devices

Flows | Layout | Settings

Network Filters

VLAN membership: ID or range (e.g. 1, 4-5)

VXLAN membership: VNI or range (e.g. 1, 4-5)

Link Overlay ⓘ

None

← Settings

Show active events: ●

Use device images: ○

Auto-detect management devices: ●

Show management devices: ○

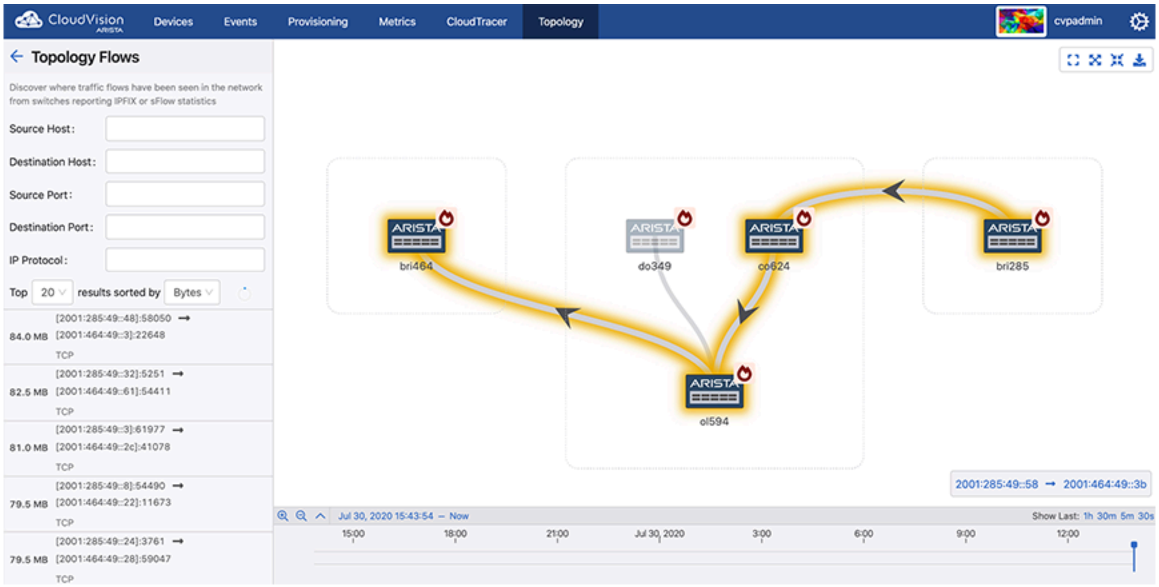
Show VXLAN tunnel links: ●

Enable traffic flows animation: ●

Note: Few browsers consume high amounts of CPU to render traffic flow animations.

If traffic flow animation is disabled, animated dots are replaced with static arrows indicating the direction of flow.

Figure 16-16: Topology with Disabled Traffic Flow Animation



← Topology Flows

Discover where traffic flows have been seen in the network from switches reporting IPFIX or sFlow statistics

Source Host:

Destination Host:

Source Port:

Destination Port:

IP Protocol:

Top 20 results sorted by Bytes

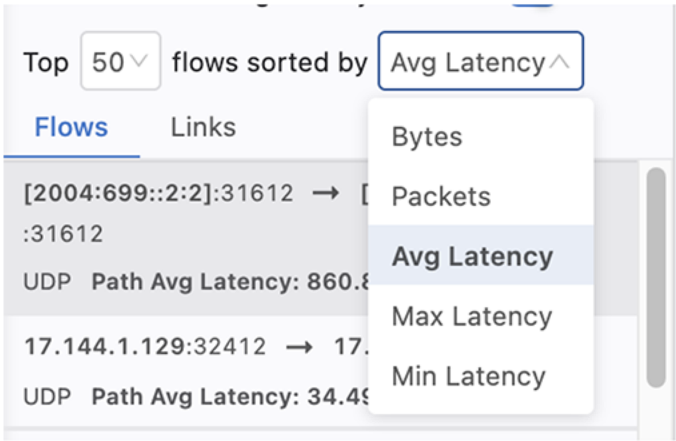
```
         [2001:285:49::48]:58050 →
84.0 MB  [2001:464:49::3]:22648
         TCP
         [2001:285:49::32]:5251 →
82.5 MB  [2001:464:49::61]:54411
         TCP
         [2001:285:49::3]:61977 →
81.0 MB  [2001:464:49::2c]:41078
         TCP
         [2001:285:49::8]:54490 →
79.5 MB  [2001:464:49::22]:11673
         TCP
         [2001:285:49::24]:3761 →
79.5 MB  [2001:464:49::28]:59047
         TCP
```

2001:285:49::58 → 2001:464:49::3b

Links Panel

The Links panel is accessible via clicking the **Links** tab and displays the topology connections where the top traffic flows have been seen.

Figure 16-17: Links Panel



Top 50 flows sorted by Avg Latency

[2004:699::2:2]:31612 → [
:31612
UDP Path Avg Latency: 860.8
17.144.1.129:32412 → 17.
UDP Path Avg Latency: 34.49

Chapter 17

CloudVision Studios

CloudVision Studios is a powerful tool for managing the configuration of network features. The intuitive interface is fully customizable, meaning that you can create and edit your own network features for configuration. This gives you complete control over the configuration of your network.

Sections in the chapter include:

- Getting Started with Studios
- Accessing Studios
- Workflow Overview
- Studio Elements and Functions
- Built-In Studios
- MSS-G with Dynamic Configuration from Forescout
- ISE/MSS-G Integration

Requirements

To use Studios, the following requirements must be installed:

- CloudVision minimum version: 2021.2.0

Features

The following features are available:

- Out-of-the-box support for common workflow configurations
- Unified Day-1 and Day-2 workflows
- Customizable Studios for bespoke workflow configuration
- In-depth and accessible change control
- Simultaneous configuration and management of separate network features
- First-class gRPC + REST APIs that easily integrate third-party resources

Known Limitations

The following is a list of known limitations in the beta-version of CloudVision Studios:

- Configuration-reconciliation: this is handled by the Network Provisioning UI
- CloudVision Studios cannot be applied to devices in an undefined container
- Studios rollback: once a Workspace and its configuration have been submitted, a user will need to undo those changes by creating and submitting a new Workspace
- Studio input actions: scripts that automatically complete Studio inputs on a user's behalf (e.g. integrating with an IPAM) are not yet supported
- Per-Studio or per-device RBAC: Phase 1 will include per-user roles and permission management that let users read and write Studio data, but do not limit user roles to specific Studios
- Users should only have one Workspace open at a time. If users have two open Workspaces that contain conflicts with one another and submit one of those Workspaces, the other may not be able to build correctly. Consequently, that second Workspace may need to be abandoned or reconfigured
- Workspaces should not be created on CloudVision clusters that manage more than 100 devices

17.1 Getting Started with Studios

Before using Studios, it is important to understand the two main elements: the Studios and Workspaces. You will use the two of these together to make changes to the mainline configuration of your network.

Studio

A Studio is an input template for a particular aspect or feature of a network. It defines the attributes of any devices belonging to that feature. All your Studios are visible on the Studios home screen.

When you visit Studios for the first time, you will see that there are already several built-in Studios. These cover some common network features, and each is explained separately in the section Built-In Studios. You can create your own custom-built Studios so that you can determine a new network feature for configuration.

Workspace

A Workspace is what you use to create, configure, or edit a Studio’s inputs, and to tag the devices that a Studio affects. It can be used to configure one or more Studios, which means that you can implement configuration changes across multiple network features at the same time.

There are three states a Workspace can have:

- **Submitted**: A Workspace that has configured one or more Studios and been submitted for approval in Change Control
- **Open**: A Workspace that has been created but not yet submitted
- **Abandoned**: A Workspace that has been discarded before submission

Note: Give any Workspace or Studio you create a relevant name and description, describing how it relates to the configuration of your network.

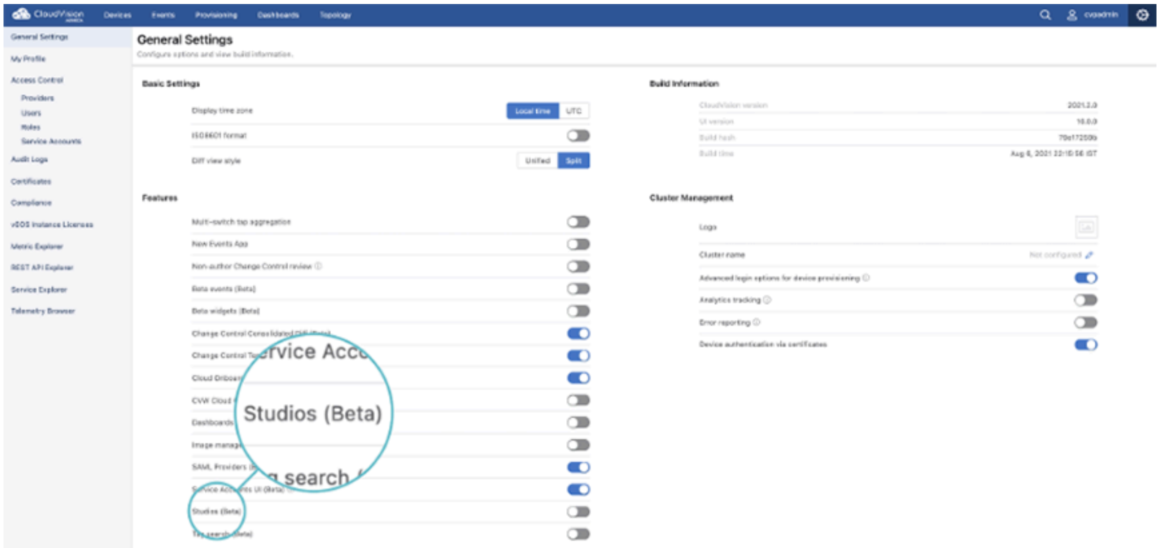
17.2 Accessing Studios

Studios is currently in beta-version and needs to be enabled in the CloudVision settings before it can be used.

To enable Studios

1. Select the **Settings** icon in the top-right of CloudVision and browse the list of features for **Studios (Beta)**. Switch the toggle to the **ON** position.

Figure 17-1: Enabling Studios



General Settings

Configure options and view build information.

Basic Settings

Display time zone: Local time | UTC

ISO8601 format ○

Diff view style: Unified | Split

Features

Multi-switch tap aggregation ○

New Events App ○

Non-author Change Control review ⓘ ○

Beta events (Beta) ○

Beta widgets (Beta) ○

Change Control Consolidated Diff (Beta) ●

Change Control T ●

Cloud Onboar ●

CVW Cloud ○

Dashboards ○

Image manage ○

SAML Providers ●

Service Accounts UI (Beta) ⓘ ●

Studios (Beta) ○

Tag search (Beta) ○

Build Information

CloudVision version	2021.2.0
UI version	18.0.0
Build hash	70e17250b
Build time	Aug 6, 2021 22:10:56 IST

Cluster Management

Logo

Cluster name: Not configured

Advanced login options for device provisioning ⓘ ●

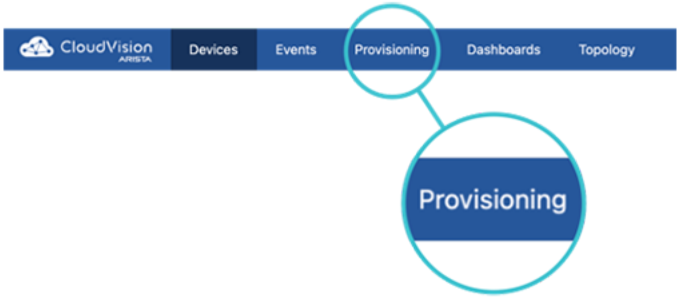
Analytics tracking ⓘ ○

Error reporting ⓘ ○

Device authentication via certificates ●

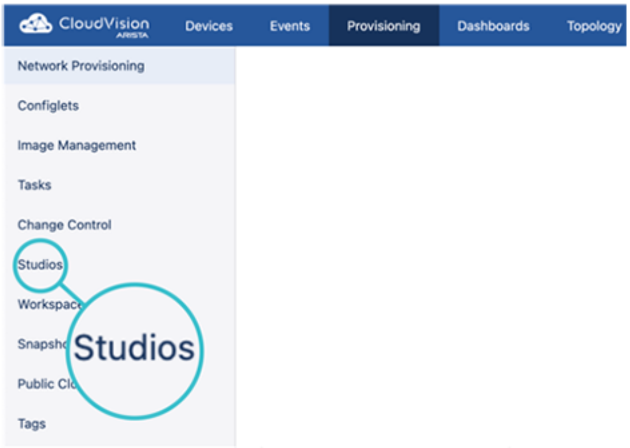
2. Once you have enabled Studios, click on the **Provisioning** tab.

Figure 17-2: Provisioning Tab



3. Select **Studios** on the sidebar.

Figure 17-3: Selecting Studios from the sidebar



4.

The Studios home screen is displayed. This is where you will initiate all your configurations. You can view your Workspaces and see their statuses by selecting on **Workspaces** under **Studios**.

17.2.1 Per-Studio Role Based Access Control

Per-Studio Role Based Access Control (RBAC) provides CloudVision users with granular control over access permissions for individual studios. A relevant user can grant differing permissions to other users for both management and input configuration of individual studios. Management includes the studio creation and deletion, its template, and its schema; input configuration includes the assignment of tags and the configuration of a studio's inputs.

A user's permissions are controlled and assigned through the use of roles in Access Control. Each role is configured with separate No Access, Read Only, or Read and Write access for the Management and Input Configuration permissions of a studio.

By default there are no per-studio permissions for CloudVision built-in roles.

Role Permissions

On a per-studio basis, the permissions have the following effect:

Table 21: Role Permissions

Permission	Management	Input Configuration
No Access	The user will not be able to access the studio's schema and template or be able to delete the studio	The user will not be able to see the studio in Studios
Read Only	The user will only be able view a studios schema and template, and will not be able to delete the studio	A user can only view the input configuration and device assignment of the studio
Read and Write	The user can edit the schema and template of a studio and can delete the studio	A user can configure the device assignment and inputs of the studio

Users may encounter on-screen errors when configuring roles if the permissions set for Management and Input Configuration do not result in a valid combination. A summary of the valid combinations is available here:

Table 22: Valid Role Based Combinations

Management	Input Configuration
No Access	No Access
Read Only	• No Access • Read Only • Read and Write
Read and Write	Read and Write

Related Topics:

- Enabling and Accessing Per-Studio Permissions
- Configuring Permissions for Studios Role Based Access Control
- Updating Workspace Permissions

17.2.1.1 Enabling and Accessing Per-Studio Permissions

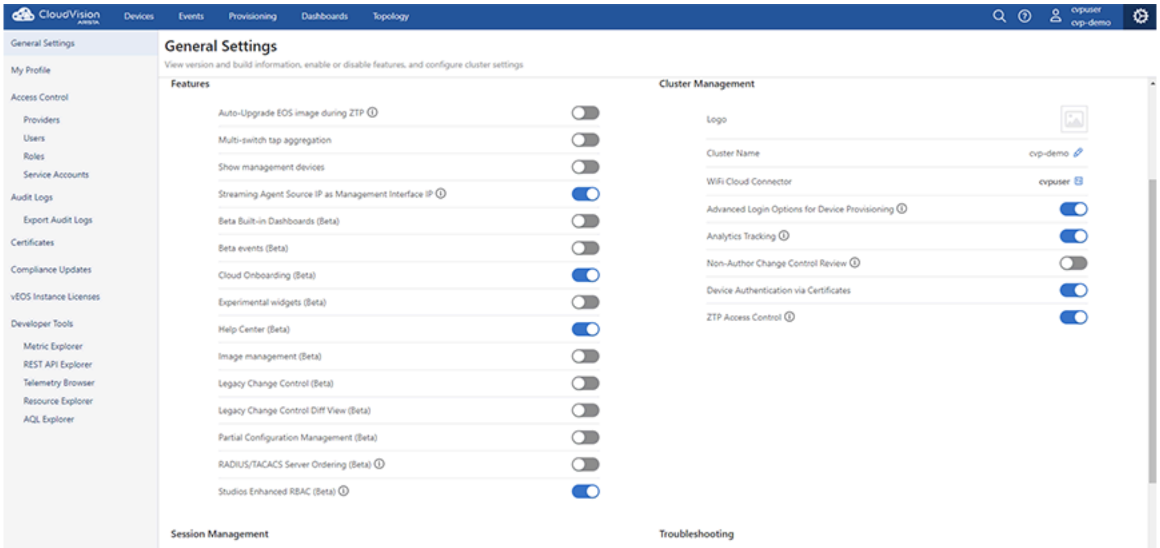
The Studio Role Based Access Control must be enabled before it can be accessed.

Enabling Per-Studio Permissions

Per-Studio Role Based Access Control must be enabled in the Features section of General Settings.

1. Select the Setting icon to open the General Settings page.
2. Select the toggle for **Studios Enhanced RBAC (Beta)**.

Figure 17-4: General Settings



General Settings

View version and build information, enable or disable features, and configure cluster settings

Features

Auto-Upgrade EOS image during ZTP ⓘ	○
Multi-switch tap aggregation	○
Show management devices	○
Streaming Agent Source IP as Management Interface IP ⓘ	●
Beta Built-in Dashboards (Beta)	○
Beta events (Beta)	○
Cloud Onboarding (Beta)	●
Experimental widgets (Beta)	○
Help Center (Beta)	●
Image management (Beta)	○
Legacy Change Control (Beta)	○
Legacy Change Control Diff View (Beta)	○
Partial Configuration Management (Beta)	○
RADIUS/TACACS Server Ordering (Beta) ⓘ	○
Studios Enhanced RBAC (Beta) ⓘ	●

Cluster Management

Logo	
Cluster Name	cvp-demo
WiFi Cloud Connector	cvpuser
Advanced Login Options for Device Provisioning ⓘ	●
Analytics Tracking ⓘ	●
Non-Author Change Control Review ⓘ	○
Device Authentication via Certificates	●
ZTP Access Control ⓘ	●

Session Management

Troubleshooting

Figure 17-5: Studios Role Based Access Control (RBAC) Toggle

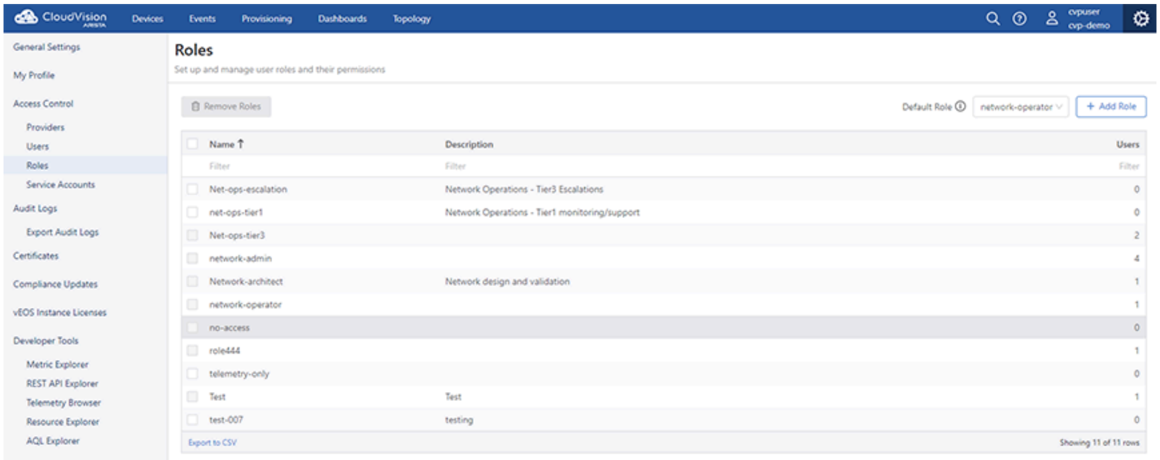
Studios Enhanced RBAC (Beta) ⓘ ●

Accessing Per-Studio Permissions

Once Studios Role Based Access Control (RBAC) is enabled, any existing roles can be edited with per-studio permissions or new roles can be created with those permissions and assigned to users.

The permissions can be accessed through Roles in Access Control when editing or creating a role. Scroll down to Studios, which can be expanded to show the Per-Studio Permissions.

Figure 17-6: Roles Screen



Roles

Set up and manage user roles and their permissions

Default Role: network-operator

Name ↑	Description	Users
Net-ops-escalation	Network Operations - Tier3 Escalations	0
net-ops-tier1	Network Operations - Tier1 monitoring/support	0
Net-ops-tier3		2
network-admin		4
Network-architect	Network design and validation	1
network-operator		1
no-access		0
role444		1
telemetry-only		0
Test	Test	1
test-007	testing	0

Showing 11 of 11 rows

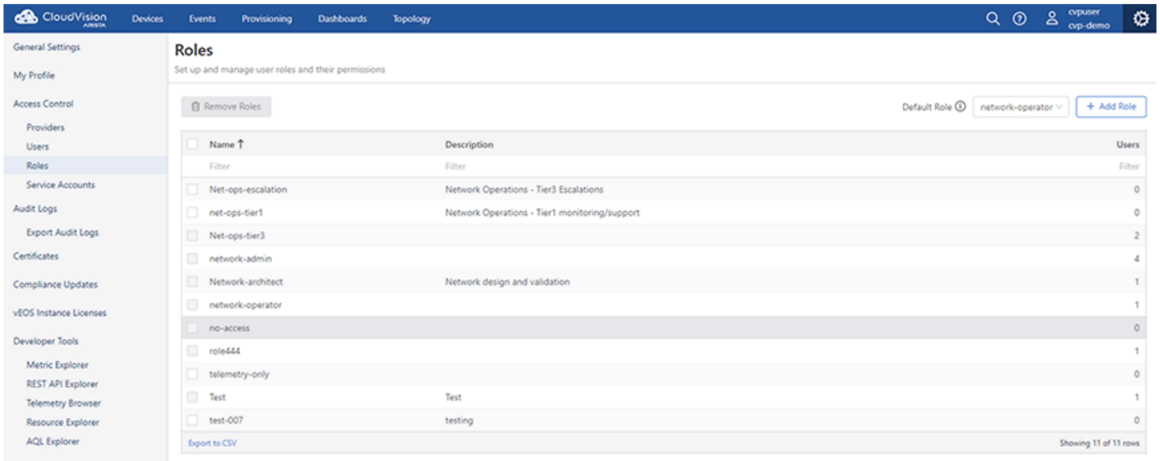
Each studio available in Studios can be added and permissions assigned to the role for that studio. Any studio that is not added to the list will have the global permissions defined above.

17.2.1.2 Configuring Permissions for Studios Role Based Access Control

Create a new role or edit an existing role, which will bring up the permissions modal. Scroll down to Studios and expand it. You will then begin the process by configuring the default (global) permissions. After the default permissions are set, you will configure the per-studio permissions.

1. Select a role from the list or select **Add Role**.

   Figure 17-7: Roles List



Roles

Set up and manage user roles and their permissions

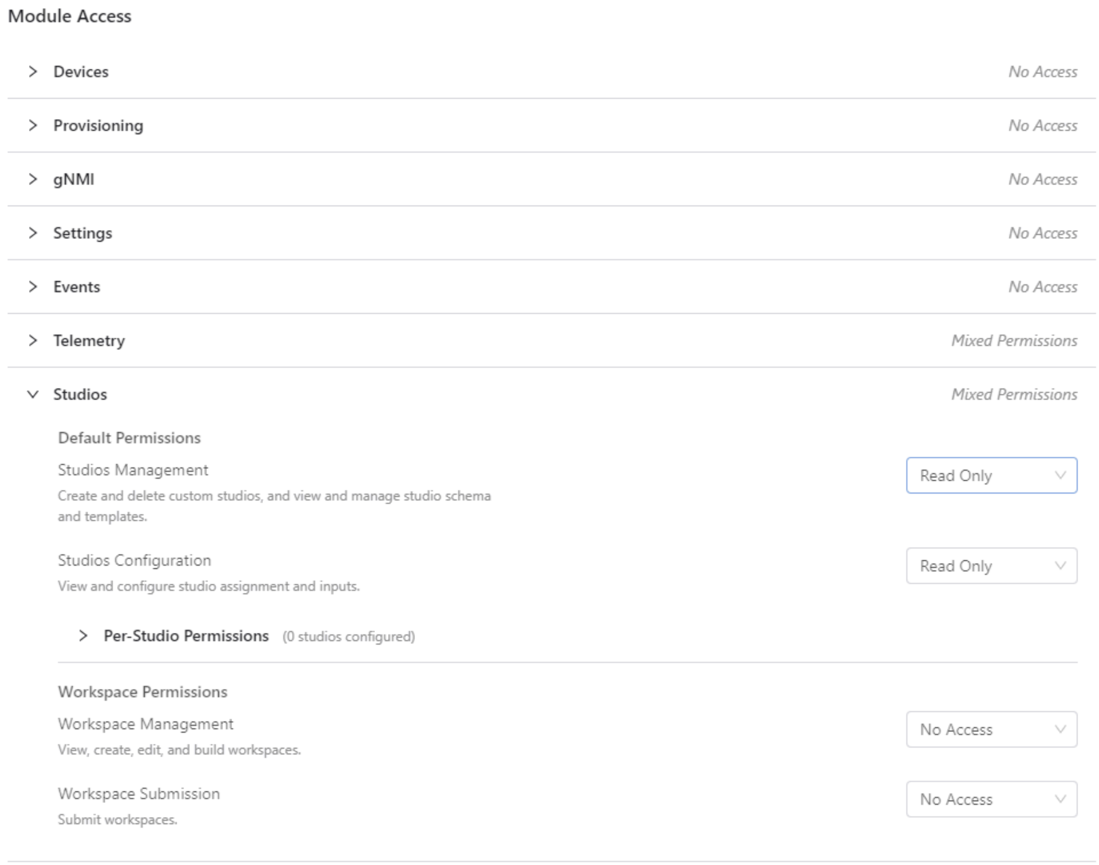
Default Role: network-operator

Name ↑	Description	Users
Net-ops-escalation	Network Operations - Tier3 Escalations	0
net-ops-tier1	Network Operations - Tier1 monitoring/support	0
Net-ops-tier3		2
network-admin		4
Network-architect	Network design and validation	1
network-operator		1
no-access		0
role444		1
telemetry-only		0
Test	Test	1
test-007	testing	0

Showing 11 of 11 rows

2. From Module Access menu, open Studios.

Figure 17-8: Module Access Menu



Module Access

- > Devices — No Access
- > Provisioning — No Access
- > gNMI — No Access
- > Settings — No Access
- > Events — No Access
- > Telemetry — Mixed Permissions
- ∨ Studios — Mixed Permissions

Default Permissions

Studios Management — Read Only
Create and delete custom studios, and view and manage studio schema and templates.

Studios Configuration — Read Only
View and configure studio assignment and inputs.

> Per-Studio Permissions (0 studios configured)

Workspace Permissions

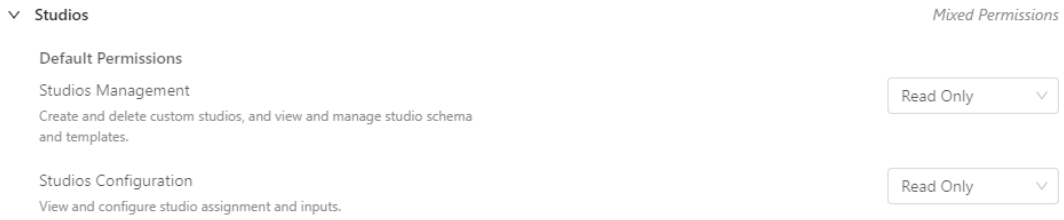
Workspace Management — No Access
View, create, edit, and build workspaces.

Workspace Submission — No Access
Submit workspaces.

3. Configure the default settings for Studios, which apply to all studios.

Note: The default permissions will be overridden by any per-studio permissions you assign for a selected studio.

Figure 17-9: Studios Default Permissions



∨ Studios — Mixed Permissions

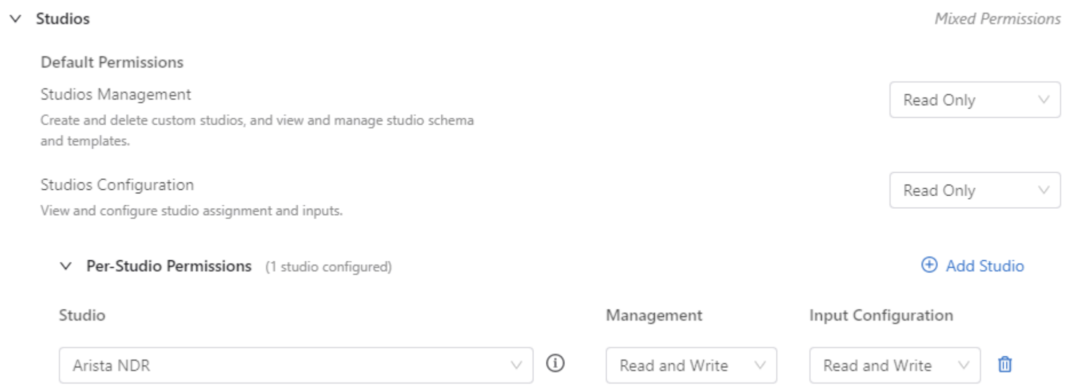
Default Permissions

Studios Management — Read Only
Create and delete custom studios, and view and manage studio schema and templates.

Studios Configuration — Read Only
View and configure studio assignment and inputs.

4. Open the Per-Studio Permissions section of the menu.

Figure 17-10: Per-Studio Permissions



Studios

Mixed Permissions

Default Permissions

Studios Management: Read Only

Create and delete custom studios, and view and manage studio schema and templates.

Studios Configuration: Read Only

View and configure studio assignment and inputs.

Per-Studio Permissions (1 studio configured)

Add Studio

Studio	Management	Input Configuration
Arista NDR	Read and Write	Read and Write

5. Select a Studio from the list or select **Add Studio**,
6. Set the Management and Input Configuration for the Studio.

Note: The permissions are set by default to the default permissions for Studios. Changing the permissions will override the default permissions for the selected Studio.

7. You can add more Studios and configure the per-studio permissions for each. When you are finished select **Save**.

17.2.1.3 Updating Workspace Permissions

The permissions for Workspaces are impacted by any per-studio permissions.

A user with Read and Write permissions for any studios will not be able to create or manage workspaces if they do not have Read and Write permissions for Workspace Management. This means another user with the relevant permissions will need to create and build workspaces. Similarly, a user must have Read and Write access to Workspace Submission in order to submit a workspace. If a user has Read and Write access for a studio, they will be unable to submit any workspaces they use to configure the studio.

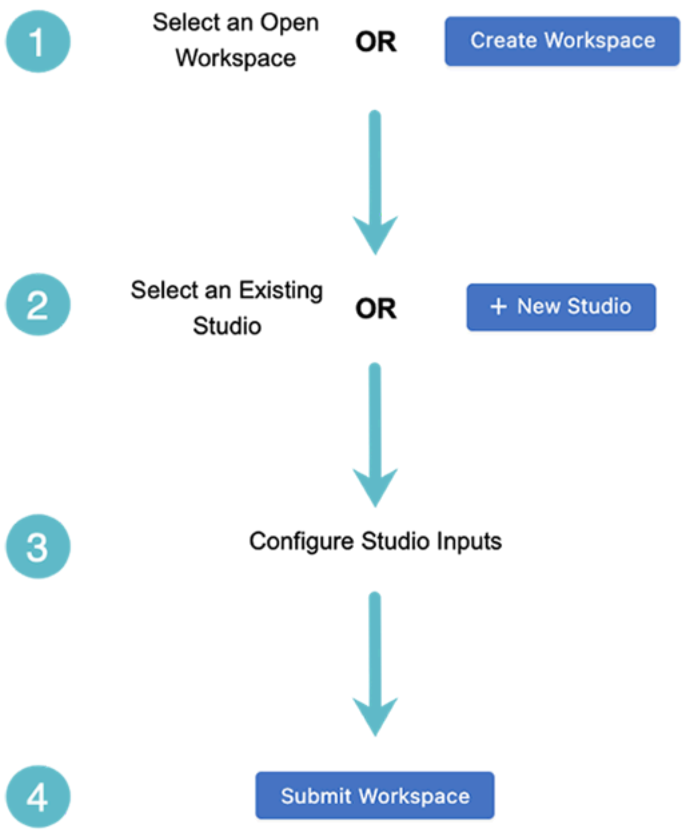
An error will be displayed when the user’s per-studio permissions conflict with their Workspace Submission permission.

17.3 Workflow Overview

Whenever you use Studios, you will begin by either creating a new Workspace or selecting an open Workspace. You will use a Workspace to implement any changes you want to make to one or more Studios. Once you have configured the changes, you will submit the Workspace. It will then be available in Change Control for the relevant user to approve or reject.

If you aree using Studios for the first time, create a Workspace and then select the Inventory and Topology Studio to commission devices for use in Studios.

Figure 17-11: Studios Workflow



Note: Once a Workspace has been submitted, it cannot be used again. If you wish to make further changes to a Studio, you'll need to create a new Workspace or select an open Workspace.

17.3.1 Commissioning Devices for Use in Studios

To configure any devices in Studios and Workspaces, you will first need to commission them for use in Studios. This is the purpose of the Inventory and Topology Studio.

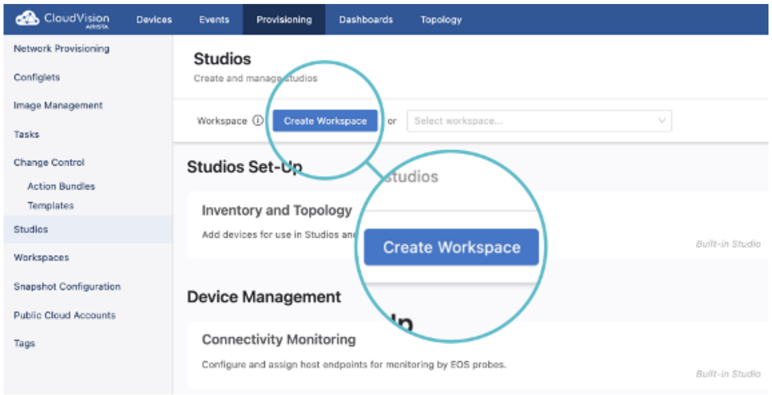
To commission devices, you will first create a Workspace and then select the Inventory and Topology Studio. There you will add devices and configure their interface connections. These devices can then be assigned to another Studio using tags.

Note: You will not be able to assign devices to any Studios until you have commissioned devices using the Inventory and Topology Studio.

17.3.2 Creating a Workspace

1. Click **Create Workspace**, which will bring up the Create New Workspace modal.

Figure 17-12: Create a Workspace



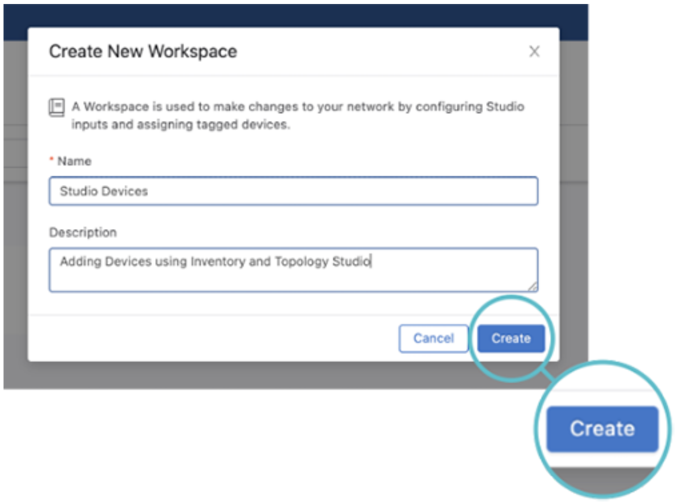
Create and manage studios

Add devices for use in Studios an

Configure and assign host endpoints for monitoring by EOS probes.

2. Give your new Workspace a name and a description, and then click **Create**.

Figure 17-13: Name and Describe the Workspace



A Workspace is used to make changes to your network by configuring Studio inputs and assigning tagged devices.

* Name: Studio Devices

Description: Adding Devices using Inventory and Topology Studio

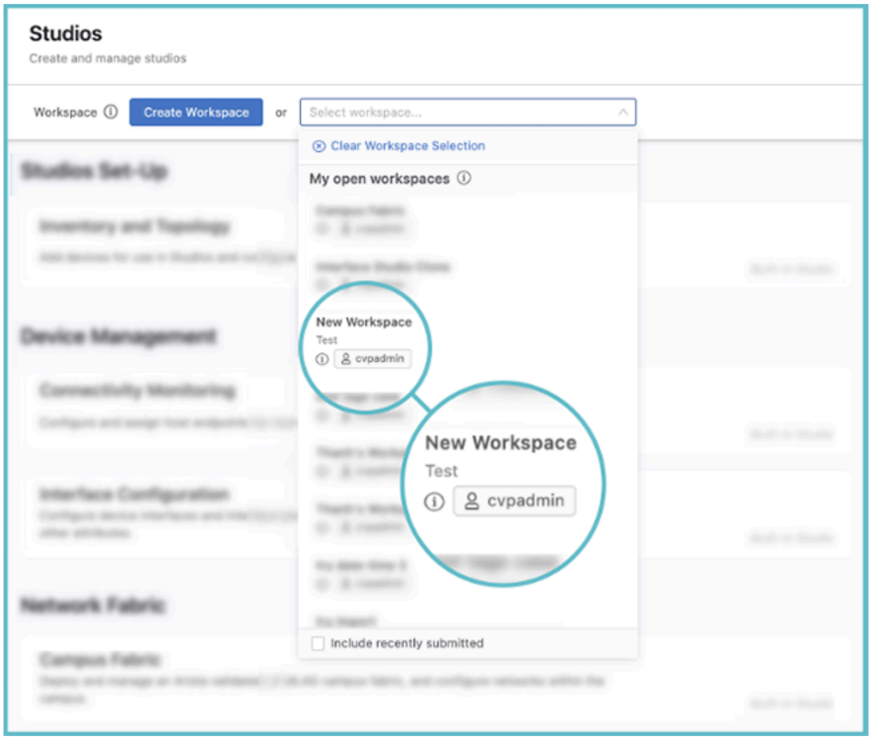
The Workplace you have created can now be used to manage the configuration of one or more Studios. It will be available for use in the Workspace dropdown menu.

17.3.3 Configuring an Existing Studio

To begin the process of configuring a Studio, you will need to either create a Workspace or already have an open Workspace available for use.

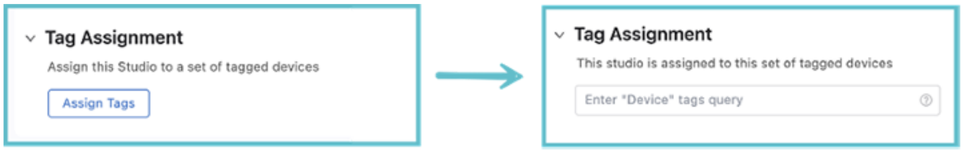
1. Create a Workspace or click the Workspace dropdown menu and select the open Workspace that you want to configure the Studio inputs with.

   Figure 17-14: Selecting a Workspace

2. Click on the existing Studio that you want to edit.
3. Manage the devices the Studio is assigned to by clicking **Tag Assignment** and selecting **Assign Tags**.

   Figure 17-15: Tag Assignment

   
   Tag Assignment
Assign this Studio to a set of tagged devices
Assign Tags
Tag Assignment
This studio is assigned to this set of tagged devices
Enter "Device" tags query

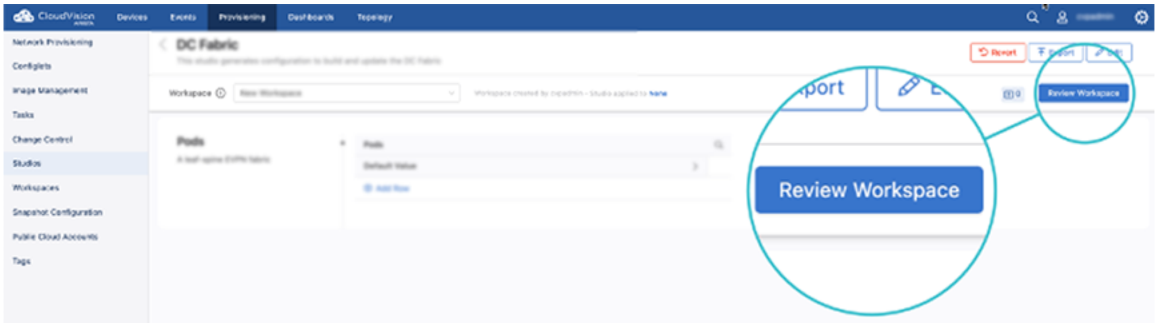
   For more information on how to use Tags, see Tags.

   Note: If the devices you wish to use for the Studio are not available for selection, you will need to commission them for Studios with the Inventory and Topology Studio.
4. Navigate through the Studio interface and configure your new input values.

   If you want to add or remove the input variables themselves, see Editing a Studio’s Schema.

5. Once all the changes have been made, you can click **Review Workspace**.

Figure 17-16: Review Workspace



You will now be brought to the Build Screen that forms part of the Workspace submission process.

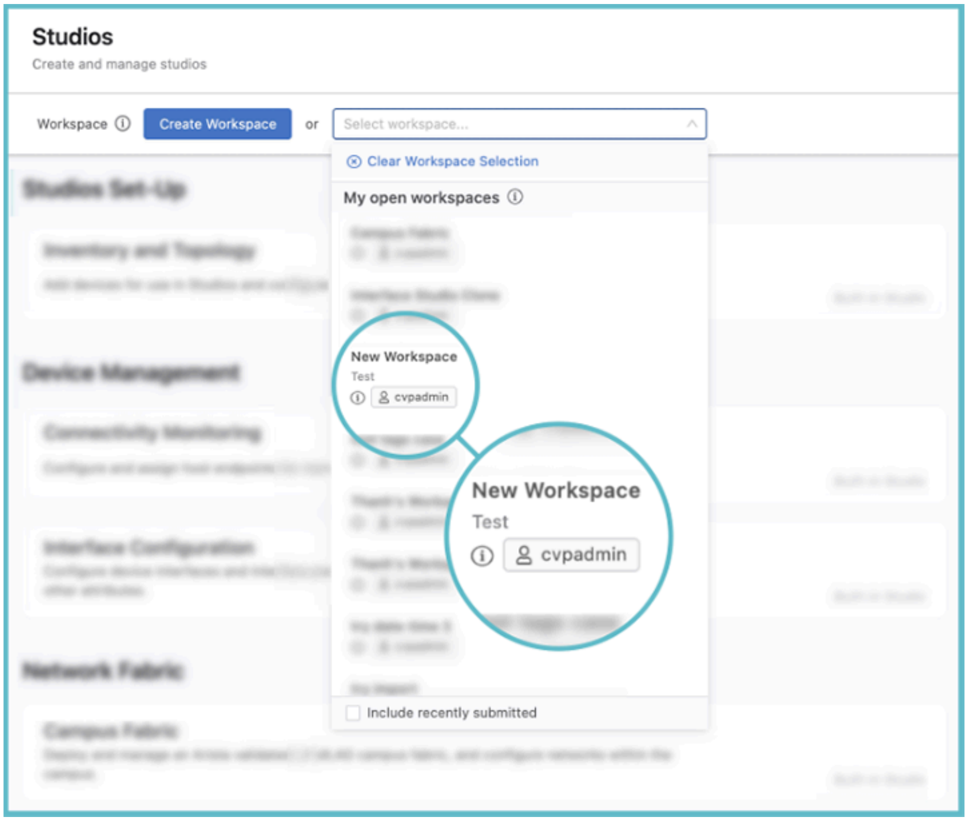
Note: If you want to make changes to multiple Studios with the same Workspace, do not click **Review Workspace** at Step 4. Return to the Studios home screen and repeat Steps 1-3, selecting the same Workspace for each Studio you want to configure.

17.3.4 Creating a New Studio

A new Studio will add a custom network feature to your Studio Suite, which you can then configure by defining its inputs. When creating a new Studio, you select these inputs and build its interface with the use of Schema.

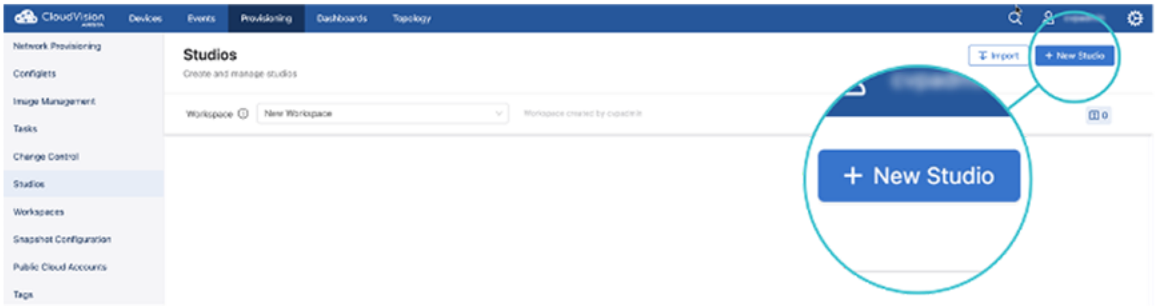
1. Click the **Workspace** menu and select the Workspace you want to use to create the new Studio.

Figure 17-17: Select Workspace



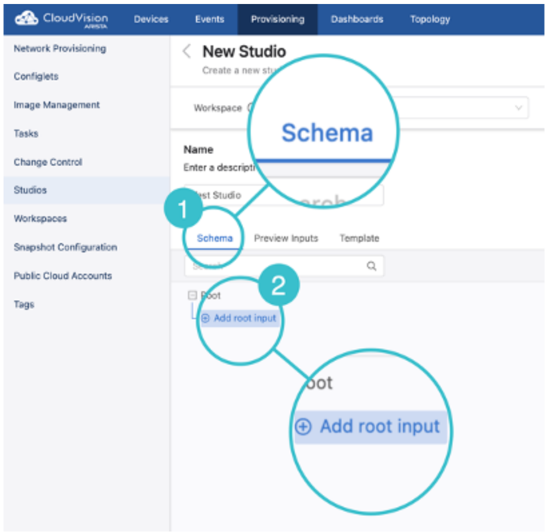
2. Click the **New Studio** button in the header.

Figure 17-18: Create New Studio



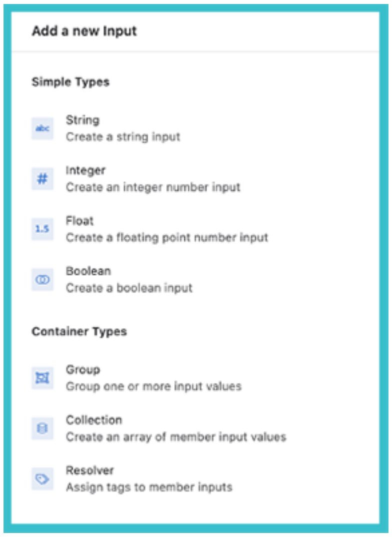
3. The Edit screen is displayed. You must enter a name and description for the new Studio.
4. After providing the Studio a name and description, you can configure the data that the Studio will collect as inputs. First click **Schema** then click **Add Root Input**.

Figure 17-19: Add Root Input



5. Select one of the inputs to configure a variable of the Studio from the section labelled Add New Input. For an explanation of schema inputs, see Input Types.

Figure 17-20: Add New Input



Add a new Input

Simple Types

- String — Create a string input
- Integer — Create an integer number input
- Float — Create a floating point number input
- Boolean — Create a boolean input

Container Types

- Group — Group one or more input values
- Collection — Create an array of member input values
- Resolver — Assign tags to member inputs

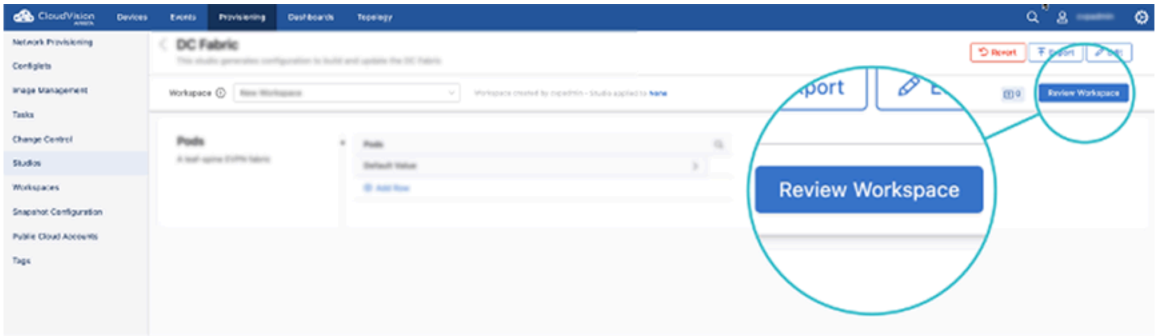
Note: You can configure the Schema input as a CLI configuration by using the Template function once you have created the new input with Schema.

6. Once all the changes have been made, click **Review Workspace** to begin the build process. Once that is completed, the Studio will appear in your Studio Suite.

17.3.5 Submitting a Workspace

1. Click the **Review Workspace** button in the header.

Figure 17-21: Review Workspace

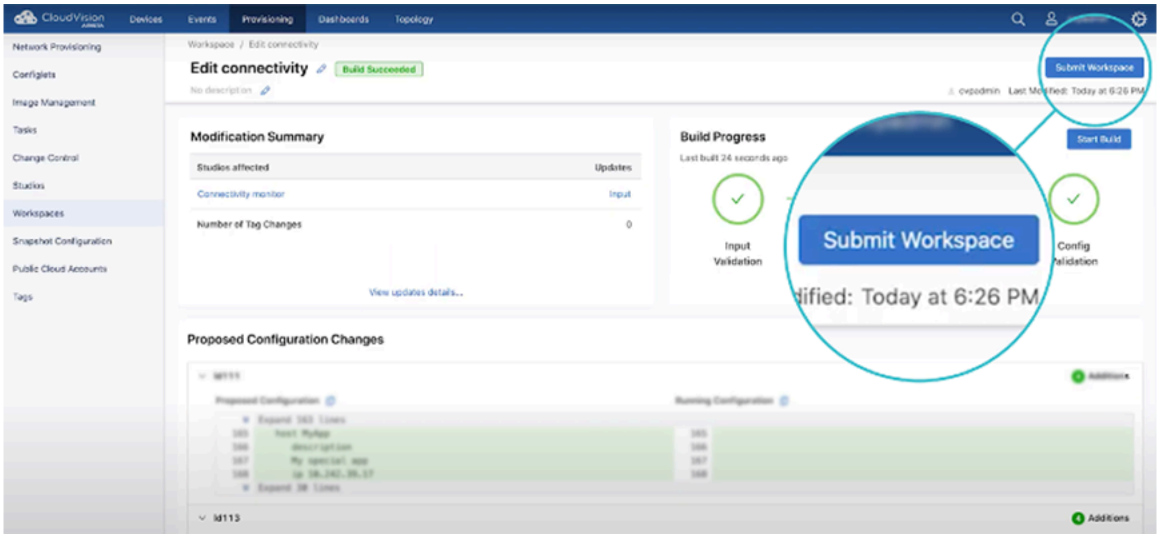


2. The Workspace will be automatically built for submission, which includes input validation, compiling the configuration, and the validation of the configuration. On the Build screen, you will be able to review the proposed configuration changes.

Note: The Workspace is automatically built only for the first time that you click **Review Workspace**. Any subsequent changes made after that will require that you re-build the Workspace by clicking **Build**.

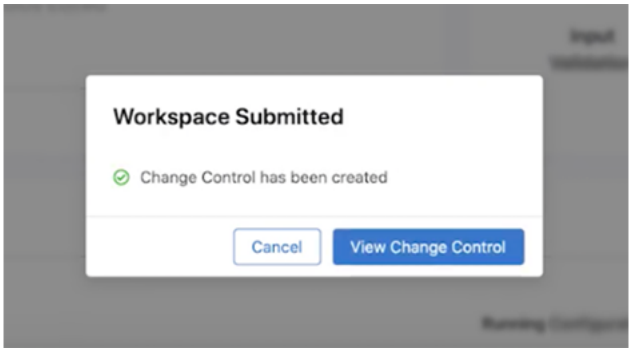
3. Once satisfied, you can click **Submit Workspace**.

   Figure 17-22: Submit Workspace



4. You will be presented with a modal that will bring you to Change Control.

   Figure 17-23: Workspace Submitted



Workspace Submitted

Change Control has been created

The relevant user will then be able to approve the Workspace, and its configuration will then become part of the mainline configuration of your network.

17.4 Studio Elements and Functions

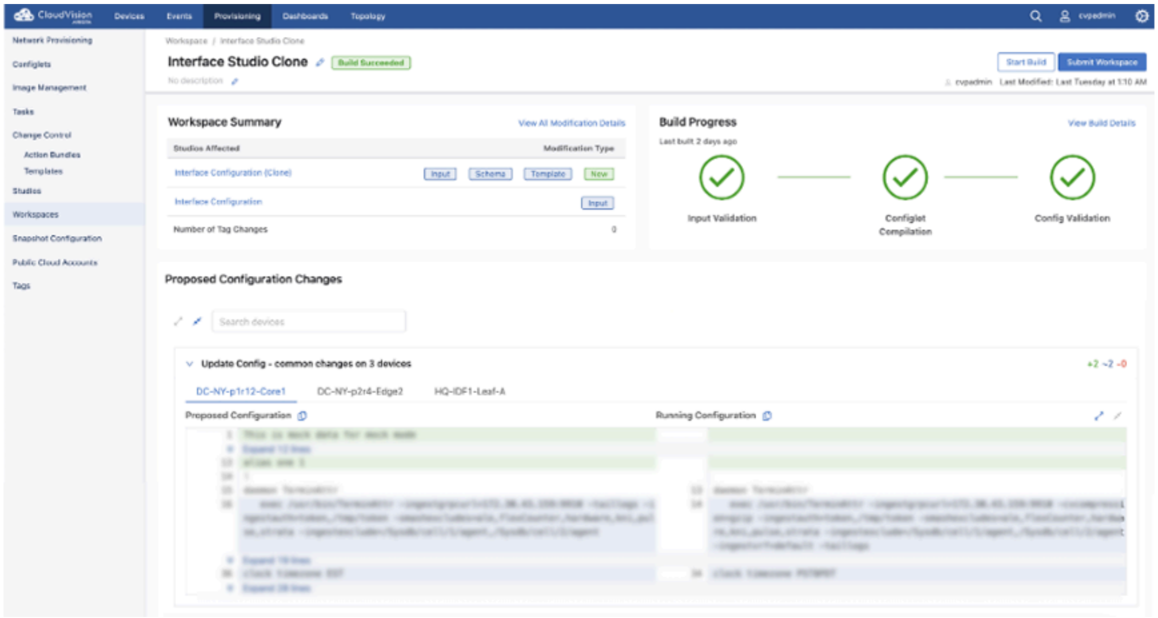
To make the most of Studios, you will need to know a little more about the tools you have control over. This section explains the full use of the different components that make up the Studios interface, which all either form a part of or enhance the workflows.

17.4.1 Reviewing a Workspace

The Workspace build screen appears after you have clicked **Review Workspace**. It provides you with important information on the Workspace's configuration before submitting to Change Control for approval.

There are several elements in the screen.

Figure 17-24: Reviewing a Workspace



Interface Studio Clone Build Succeeded

No description

cvpadmin Last Modified: Last Tuesday at 1:10 AM

Workspace Summary

Studios Affected	Modification Type
Interface Configuration (Clone)	Input Schema Template New
Interface Configuration	Input
Number of Tag Changes	0

Build Progress

Last built 2 days ago

Proposed Configuration Changes

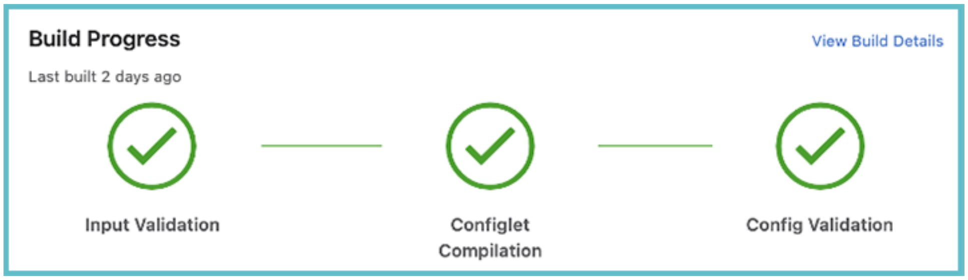
Update Config - common changes on 3 devices

17.4.1.1 Build Progress

The most important element for indicating if there are any problems with the Workspace configuration is the Build Progress section. It shows you if the Workspace configuration contains any conflicts and if device configlets have been compiled correctly. It is composed of three components:

- **Input Validation:** Checks whether the values of the inputs follow the schema rules.
- **Configlet Compilation:** Identifies any coding errors.
- **Config Validation:** Determines whether the affected devices can support the proposed configuration.

Figure 17-25: Build Progress



Build Progress

Last built 2 days ago

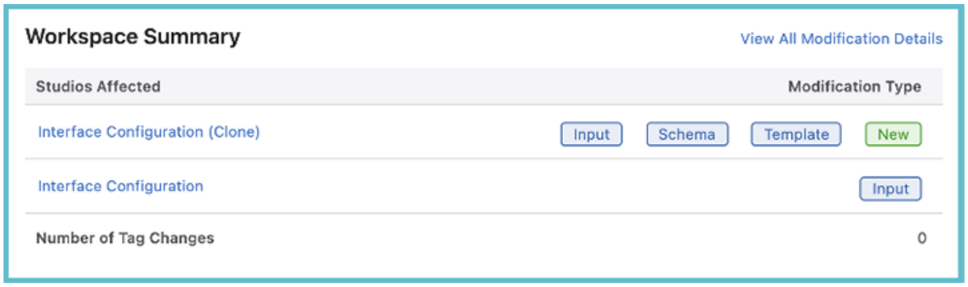
By clicking **View Build Details**, you can see each of these components for the individual devices that the configuration affects.

This shows you the build progress for each device, and it helps you identify the devices the build progress has failed on.

17.4.1.2 Workspace Summary

The Workspace Summary table provides a brief overview of the type of modifications that a Workspace will make.

Figure 17-26: Workspace Summary



Workspace Summary

View All Modification Details

Studios Affected	Modification Type
Interface Configuration (Clone)	Input Schema Template New
Interface Configuration	Input
Number of Tag Changes	0

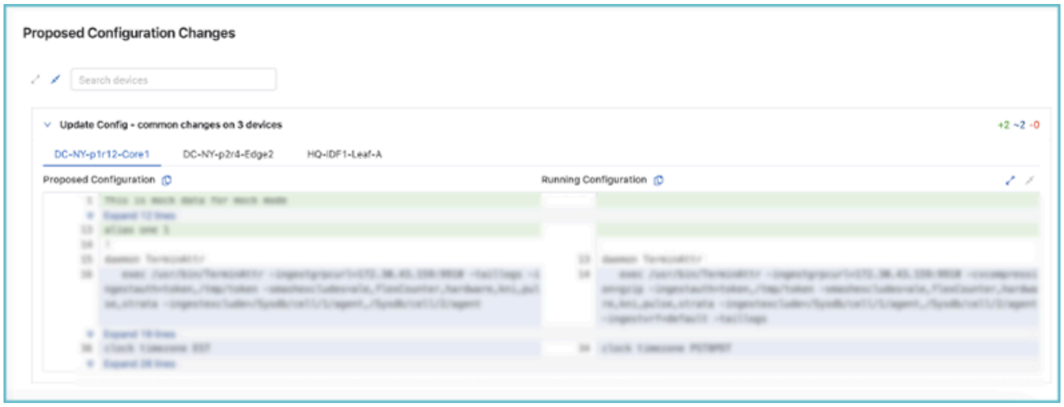
On the left-hand side, you can see each of the Studios that the configuration affects. On the right is displayed the type of change that has been made with the Workspace. By clicking on the type of configuration change, you will be brought to the screen in which that change was implemented.

Click **View All Modification Details,** to view all the configuration changes displayed together in the manner of Schema inputs.

17.4.1.3 Proposed Configuration Changes

Review the Proposed Configuration Changes to compare the Workspace configuration changes with what currently exists in the network.

Figure 17-27: Proposed Configuration Changes



Proposed Configuration Changes

Search devices

Update Config - common changes on 3 devices +2 ~2 -0

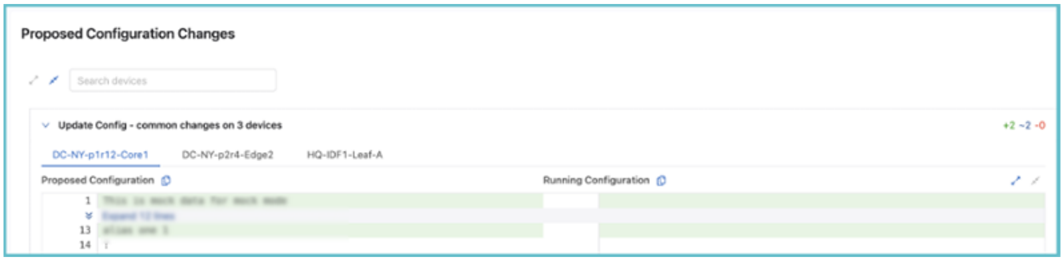
DC-NY-p1r12-Core1 DC-NY-p2r4-Edge2 HQ-IDF1-Leaf-A

Proposed Configuration

Running Configuration

This is shown for each individual device, and clicking on the device name will show you its proposed configuration.

Figure 17-28: Proposed Configuration - Compare



Proposed Configuration Changes

Search devices

Update Config - common changes on 3 devices +2 ~2 -0

DC-NY-p1r12-Core1 DC-NY-p2r4-Edge2 HQ-IDF1-Leaf-A

Proposed Configuration

Running Configuration

On the left are your proposed changes and on the right is the existing configuration. It is color-coded for easy reference:

- Green = additions
- Blue = modifications
- Red = deletion

17.4.2 Tags

A tag is a value-label pair that you apply to a device or an interface. User Tags allows you to group devices or interfaces that share a common characteristic under a tag. By way of example, you could have:

Role: Spine or **DC**: New York

With Studios, you can then use these User Tags to create a separate configuration for different groups of devices. For instance, if you wish to separately configure the spines and leafs of a data center fabric, you can do so by tagging the relevant devices as spines or leafs.

Note: User Tags are not just for Studios, they have already been implemented for use with Event Customization, Event Notification, and Dashboard Configuration.

17.4.2.1 User Tags and System Tags

Only User Tags are supported in Studios, which are tags created and defined by a user of CloudVision through the following process.

System Tags are created by CloudVision and based upon characteristics or attributes of devices. These tags cannot be created or edited by you or any other CloudVision user. System tags are not static and could affect the stability of any Workspace configurations you create. For this reason, only User Tags are available in Studios.

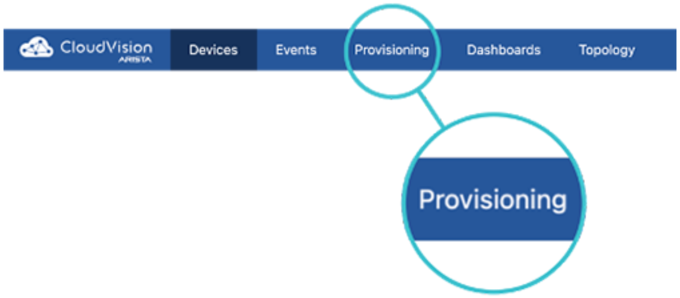
Any changes made to User Tags can impact the configuration of devices. For this reason, User Tags can only be deployed inside a Workspace. When you build the Workspace and review its changes, you will then see any impact the tags have on the Workspace proposed configuration and can rectify it accordingly.

17.4.2.2 Creating Tags

To tag devices with User Tags, you will need to leave the Studios environment:

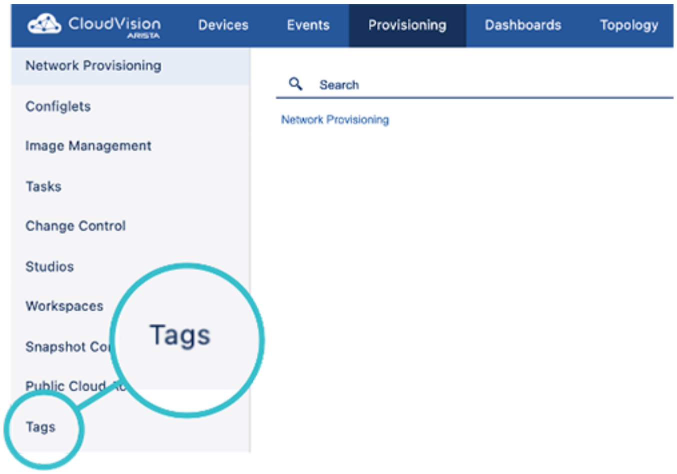
1. Click on the **Provisioning** tab, if necessary.

Figure 17-29: Provisioning Tab



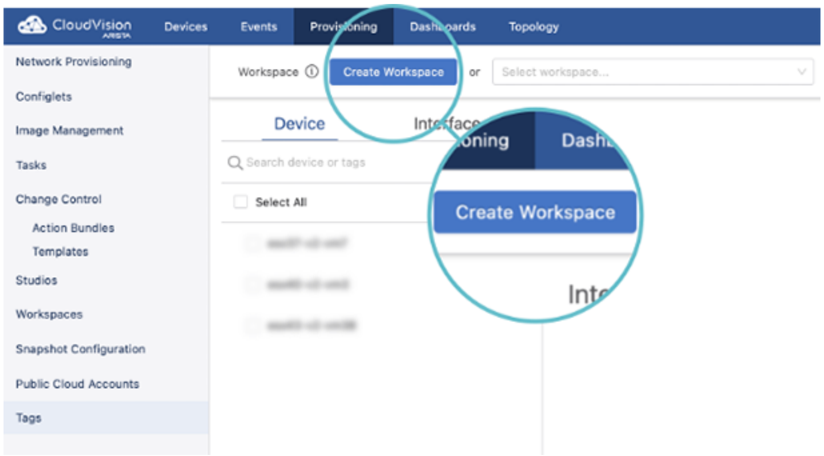
2. Click on **Tags**.

Figure 17-30: Tags



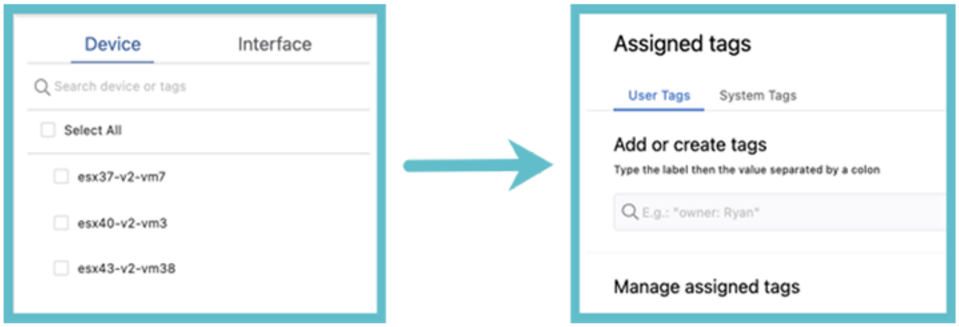
3. Click **Create Workspace** or select an open Workspace from the dropdown menu.

Figure 17-31: Create Workspace



4. Select one or more devices or interfaces, and then enter a value under **Add or Create Tags**.

Figure 17-32: Add or Create Tags



5. Click **Create and Assign** to give the tag to the selected device or devices.

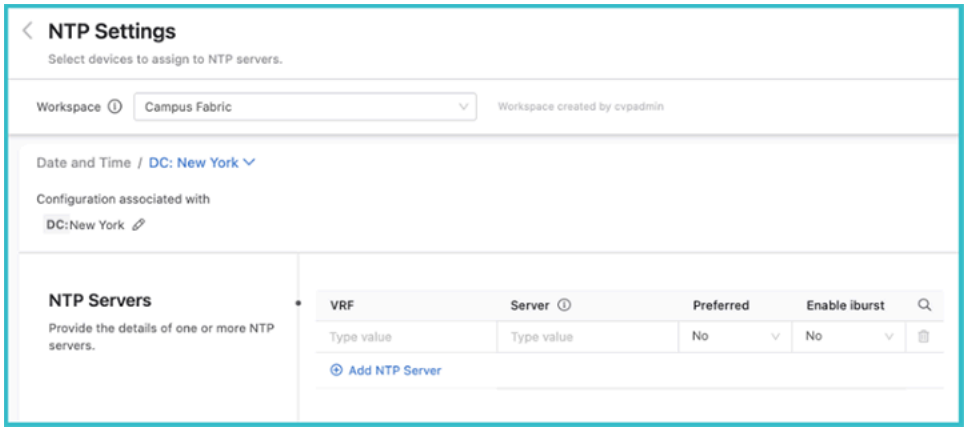
17.4.2.3 Applying Tags in Studios

You will use User Tags in two places in Studios: as the field data for a resolver input, and when assigning a Studio to devices.

Resolver Input

Resolver Input is a Container Type that allows you to apply the input variables associated with it to a selection of devices. The following is an example of a resolver input, which, in this case, allows you to select tagged devices that you will assign to an NTP server.

Figure 17-33: Resolver Input



NTP Settings

Select devices to assign to NTP servers.

Workspace: Campus Fabric

Workspace created by cvpadmin

Date and Time / DC: New York

Configuration associated with DC:New York

NTP Servers

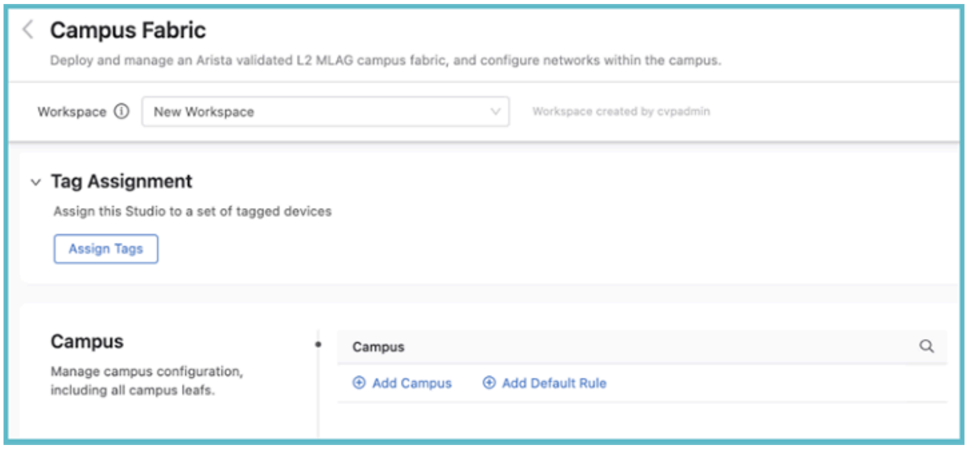
Provide the details of one or more NTP servers.

VRF	Server	Preferred	Enable iburst
Type value	Type value	No	No

Studio Tag Assignment

Within each Studio, with the exception of Inventory and Topology, there is a Tag Assignment option.

Figure 17-34: Tag Assignment



Campus Fabric

Deploy and manage an Arista validated L2 MLAG campus fabric, and configure networks within the campus.

Workspace: New Workspace

Workspace created by cvpadmin

Tag Assignment

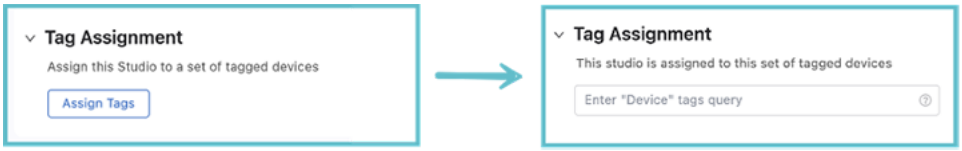
Assign this Studio to a set of tagged devices

Campus

Manage campus configuration, including all campus leafs.

You will use Tag Assignment to specify the devices that any given Studio configuration affects. All of the tagged devices you select must already have been commissioned for use in Studios with the Inventory and Topology Studio. In order to assign devices, click **Assign Tags** and then enter a device tag query.

Figure 17-35: Tag Assignment



Tag Assignment

Assign this Studio to a set of tagged devices

Tag Assignment

This studio is assigned to this set of tagged devices

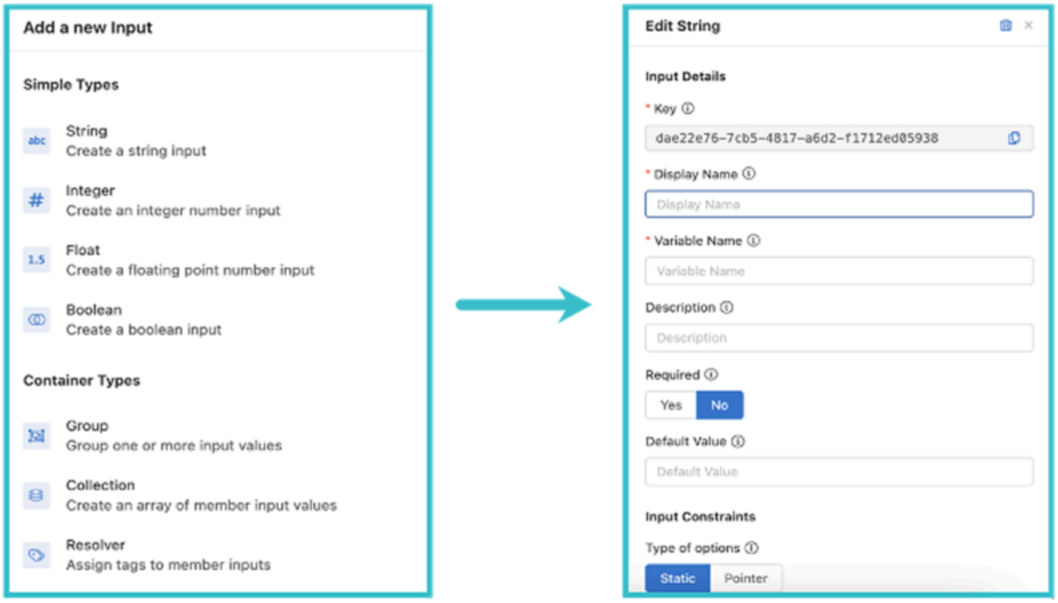
You can edit these tagged devices at any point with a Workspace by clicking the pencil icon to the right of the last tag.

You can use tags to apply an entire Studio to a selected group of devices. For example, you may want the configuration of a Studio to relate only to devices in a particular data center. All devices in that data center can be tagged under a label, and you can assign that Studio to that tag label.

17.4.3 Schema

Schema are the input variables of a Studio and are used to collect data from a CloudVision User. They are defined when either Creating a New Studio or editing an existing Studio. You do this by selecting an input type in the Studio Edit screen and then completing a form.

Figure 17-36: Schema



Key: dae22e76-7cb5-4817-a6d2-f1712ed05938

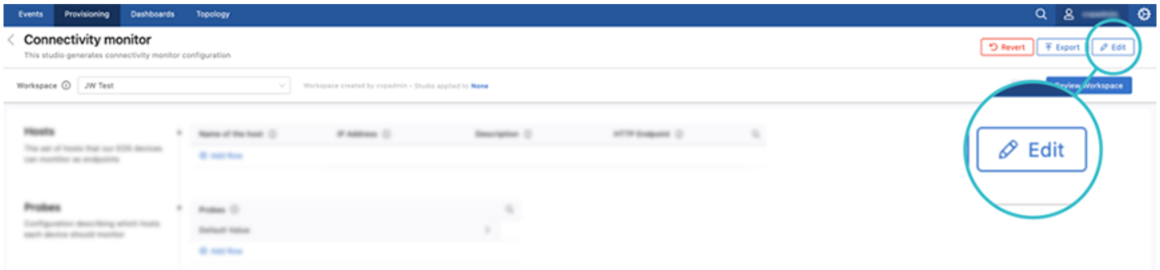
17.4.3.1 Editing a Studio Schema

Only custom Studios can be edited.

Note: Built-in Studio schemas cannot be edited.

To edit a custom Studio Schema, create a new Workspace or select an open Workspace and then click the **Edit** button within a Studio.

Figure 17-37: Editing a Studio Schema



At the Studio Edit screen, you can select Schema and the process will be the same as creating a new Studio.

Note: While you cannot edit built-in Studios, you can export and then import the Studio as a clone that you can edit.

17.4.3.2 Input Types

Schema inputs can be broadly classified into two categories:Base Types and Container Types.

Base Types are inputs that hold a real value and have a defined format. In general, these inputs can be validated to ensure that their value matches the defined format. You can also add constraints that restrict the values that can be entered in their fields.

Container Types are inputs that group one or more Base Types into a unit. They can be used to assign a set of inputs to a specific group of devices, allow a Studio to provide multiple values for a given input, or to group multiple Base Types and make them into an input unit.

Each input type is further divided into different data types:

Base Types consist of:

- String
- Integer
- Float
- Boolean

Container Types consist of:

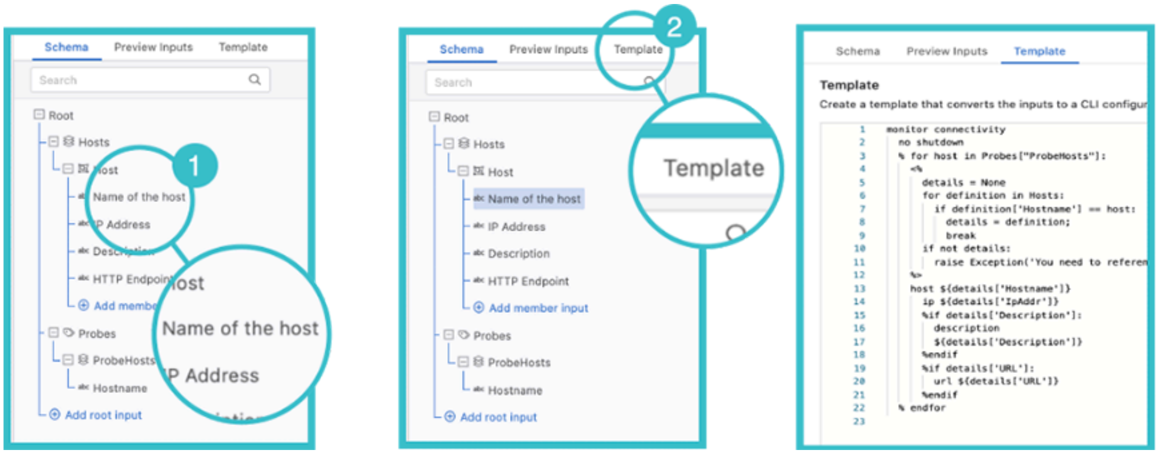
- Resolver
- Collection
- Group

You can find a full description of each data type in Appendix 2: Schema Input Types.

17.4.4 Template

Once you have defined an the variables for an input under Schema, you can use Template to convert the input into a CLI configuration. You can click on the input you want to configure, and then click **Template**.

Figure 17-38: Template



Template

Create a template that converts the inputs to a CLI configur

```
monitor connectivity
  no shutdown
  % for host in Probes["ProbeHosts"]:
    <%
      details = None
      for definition in Hosts:
        if definition['Hostname'] == host:
          details = definition;
          break
      if not details:
        raise Exception('You need to referen
    %>
    host ${details['Hostname']}
      ip ${details['IpAddr']}
      %if details['Description']:
        description
        ${details['Description']}
      %endif
      %if details['URL']:
        url ${details['URL']}
      %endif
  % endfor

```

17.4.4.1 Mark-Up Language

You have a choice of two languages when writing a Template, Mako or Jinja2. The default setting is Mako, but you can select Jinja2 or change back to Mako by using the below toggle:

Both Mako and Jinja2 have a lightweight syntax that allows you to leverage the underlying Python of Studios to create an effective Template.

You can find a primer on Mako syntax here and for Jinja2 here. There is also a short guide for using Mako for Template in Appendix 1: Mako Syntax.

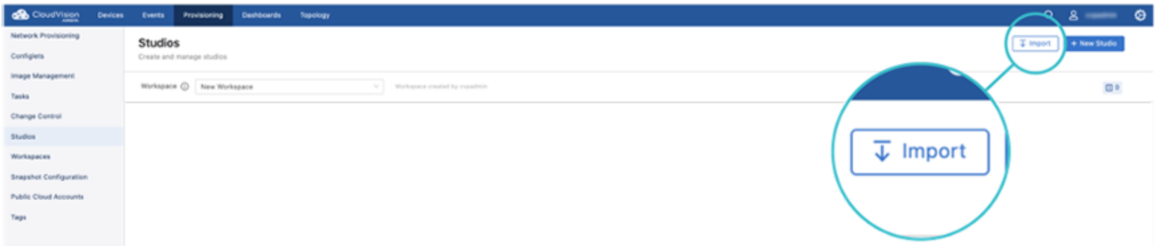
17.4.5 Importing and Exporting Studios

Studios are saved and distributed as .yaml files. The file contains the entire schema definition, template, and input values. You can easily import and export Studios using CloudVision.

Importing

1. Click **Create Workspace** or select an open Workspace from the dropdown menu.
2. Click **Import**.

Figure 17-39: Import



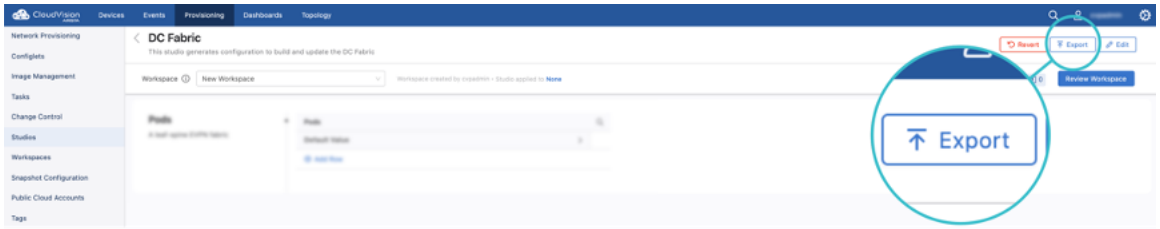
3. On the Import Studio modal, select the Studio file and then click **Import**.

The imported Studio will now be part of your Studio Suite.

Exporting

1. From your Studio Suite, select the Studio you wish to export.
2. Within the Studio screen, click **Export**.

Figure 17-40: Export



3. A pop-up box will appear, which will ask you the details for downloading the file. Enter the details and click **Download** or **Save**.

17.5 Built-In Studios

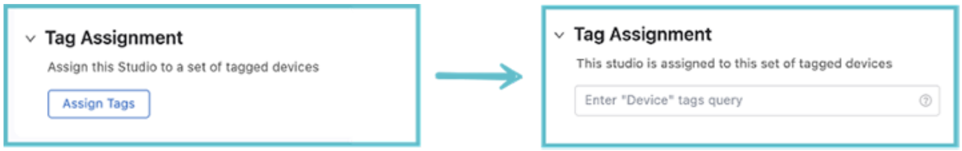
There are currently seven built-in Studios in the beta-version, which each relate to a network feature. You can create your own custom-built Studios by following the Creating a New Studio instructions.

Any devices you wish to include in a Workspace configuration must already have been commissioned by using the Inventory and Topology Studio. Consequently, this is the first Studio that you should use and which enables the use of all other Studios.

When using any Studio, except for Inventory and Topology, it is important to remember that you need to assign User Tags to the Studio. These tags relate to devices commissioned with the Inventory and Topology Studio. Only devices tagged to a Studio will be affected by any proposed configuration.

When you open up any Studio, other than Inventory and Topology, you will see the tag assignment option. Click **Assign Tags** and enter the User Tags for the devices you want the Studio to affect.

Figure 17-41: Tag Assignment



Tag Assignment

Assign this Studio to a set of tagged devices

Tag Assignment

This studio is assigned to this set of tagged devices

Enter "Device" tags query

17.5.1 Inventory and Topology

This will be the first Studio that you'll use, because it is responsible for making devices and their interfaces available for configuration in Studios. It serves as a control point for separating or combining your wider network topology with the topology that Studios configures.

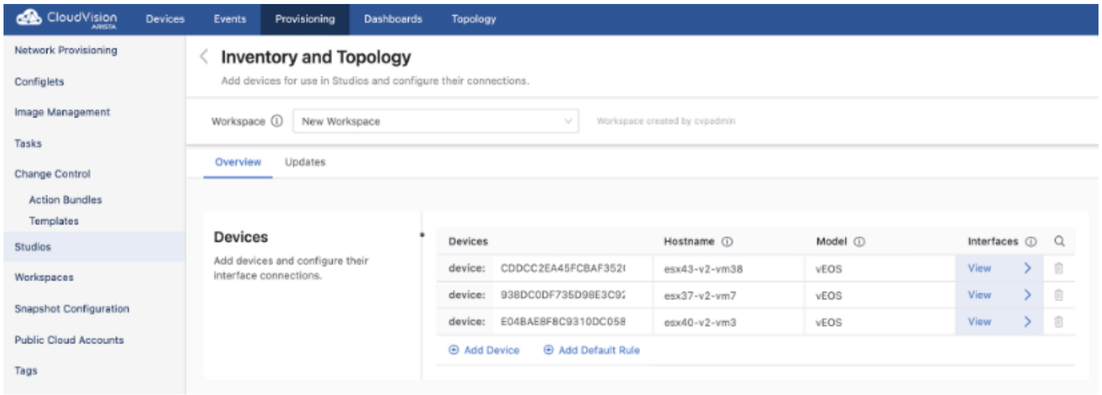
With the Inventory and Topology Studio, you can accept devices and interface changes in your wider network topology and incorporate those devices and changes into Studios configuration. You can also use it to manually add devices and configure their interfaces for use in Studios.

Note: The Updates tab is the easiest way to commission devices for Studios, and is what you should use most often. The Updates tab receives and displays device and interface changes in your wider network, which you can quickly accept or ignore for use in Studios.

17.5.1.1 Adding a Device and Configuring its Interfaces

When you click on **Inventory and Topology**, the Inventory and Topology page is displayed.

Figure 17-42: Inventory and Topology



Inventory and Topology

Add devices for use in Studios and configure their connections.

Workspace: New Workspace

Workspace created by cvpadmin

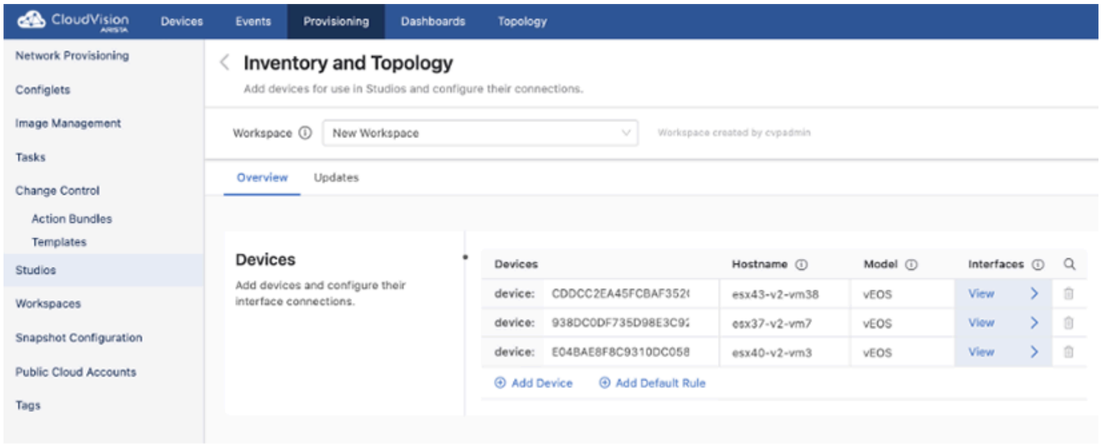
Devices

Add devices and configure their interface connections.

Devices		Hostname	Model	Interfaces
device:	CDDCC2EA45FCBAF352(	esx43-v2-vm38	vEOS	View
device:	938DC0DF735D98E3C9:	esx37-v2-vm7	vEOS	View
device:	E04BAE8F8C9310DC058	esx40-v2-vm3	vEOS	View

From the Inventory and Topology page you can add devices and then configure their interfaces. Any device added here will be made available for use in other Studios. Once the information for each device has been entered, click **View**. This will display the Devices page, which shows the interfaces on a selected device. From this page you can add device interfaces and configure their connections to other device interfaces

Figure 17-43: Inventory and Topology - Device Interfaces



Inventory and Topology

Add devices for use in Studios and configure their connections.

Workspace: New Workspace — Workspace created by cvpadmin

Devices

Add devices and configure their interface connections.

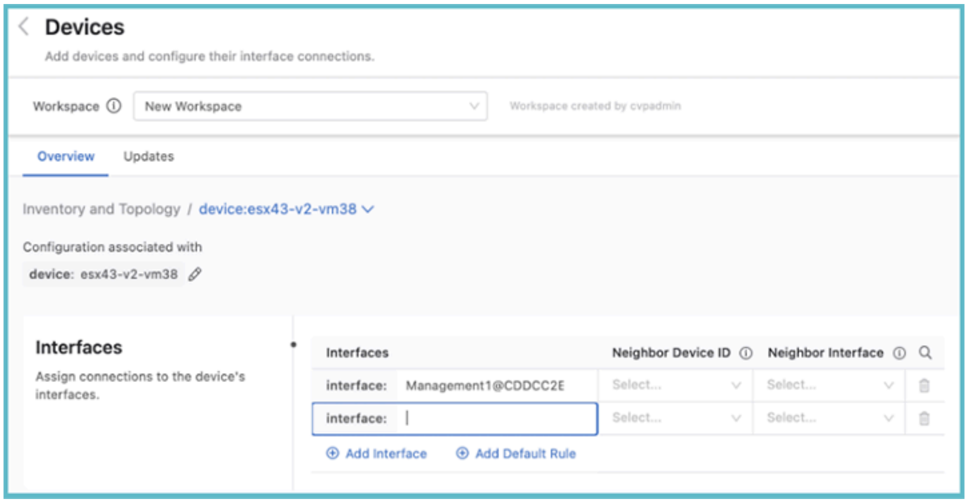
Devices		Hostname	Model	Interfaces
device:	CDDCC2EA45FCBAF352(	esx43-v2-vm38	vEOS	View
device:	938DC0DF735D98E3C9;	esx37-v2-vm7	vEOS	View
device:	E04BAE8F8C9310DC058	esx40-v2-vm3	vEOS	View

Note: All connections are bidirectional. It is not possible to create unidirectional connections.

17.5.1.2 Managing Updates to the Network Topology

Select the **Updates** tab, to view new devices and amendments to device connections in your network. You can quickly add any device or interface changes in your network by using Updates.

Figure 17-44: Devices - Updates Tab



Devices

Add devices and configure their interface connections.

Workspace: New Workspace — Workspace created by cvpadmin

Inventory and Topology / device:esx43-v2-vm38

Configuration associated with

device: esx43-v2-vm38

Interfaces

Assign connections to the device's interfaces.

Interfaces		Neighbor Device ID	Neighbor Interface
interface:	Management1@CDDCC2E	Select...	Select...
interface:		Select...	Select...

All updates and their type will be listed here, and you can choose to accept these updates or ignore them. Accepting adds devices and their interfaces for use in Studios and updates any configuration in Studios the device relates to. Ignoring the updates will omit them from being configured in any Studio.

Note: In the beta-version, clicking **Ignore for Now** will result in updates remaining in the Review Updates list.

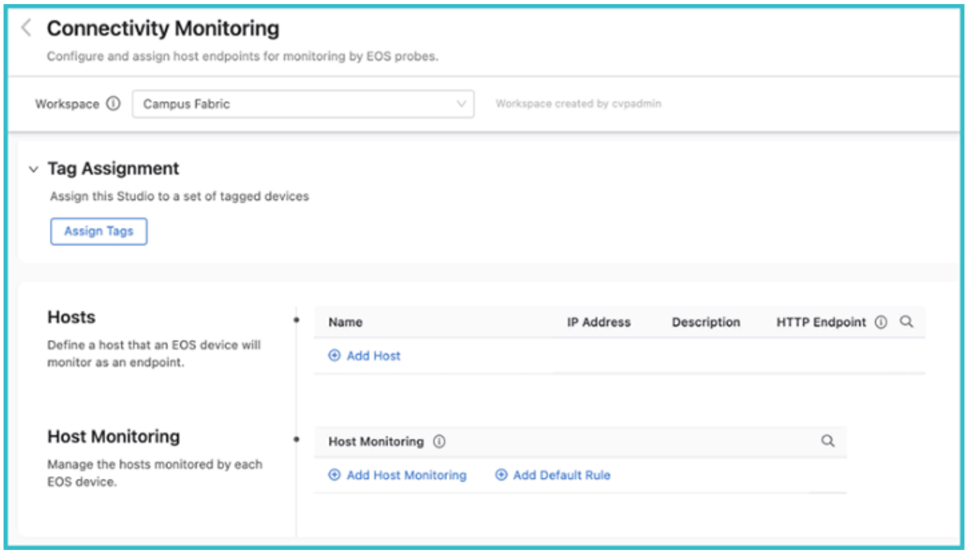
17.5.2 Connectivity Monitor

The Connectivity Monitor Studio configures an EOS feature to send probes to a remote host. EOS will then report latency, jitter, round-trip times, and HTTP connectivity to those remote hosts. The corresponding telemetry for the monitored hosts can be found under Devices and Dashboards.

With Connectivity Monitor, you can set up or update the hosts and set which hosts should be monitored.

Select the Connectivity Monitor Studio to display the following screen.

Figure 17-45: Connectivity Monitor



Connectivity Monitoring

Configure and assign host endpoints for monitoring by EOS probes.

Workspace: Campus Fabric

Workspace created by cvpadmin

Tag Assignment

Assign this Studio to a set of tagged devices

Hosts

Define a host that an EOS device will monitor as an endpoint.

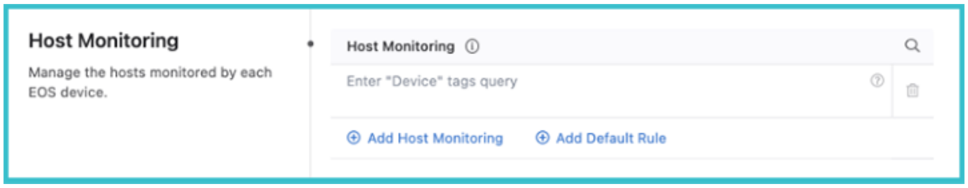
Host Monitoring

Manage the hosts monitored by each EOS device.

From the Connectivity Monitor screen, the hosts that the probes will monitor can be defined. Enter a name for the device followed by the IP address and a description for the host. Enter an optional HTTP URL, which will configure the EOS to measure the HTTP response time for that URL.

Groups of devices can be defined for monitoring by an EOS probe using Host Monitoring. Use device tags to define the host groups.

Figure 17-46: Host Monitoring

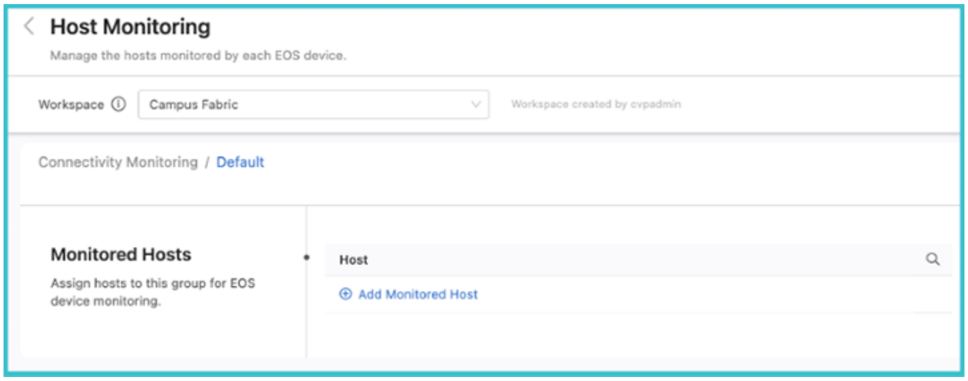


Host Monitoring

Manage the hosts monitored by each EOS device.

After one or more device tags have been defined, click on the arrow to the right. This will allow you to add hosts to the tagged group for monitoring. These hosts must already have been defined in the previous Hosts section.

Figure 17-47: Host Monitoring - Monitored Hosts



Host Monitoring

Manage the hosts monitored by each EOS device.

Workspace: Campus Fabric

Workspace created by cvpadmin

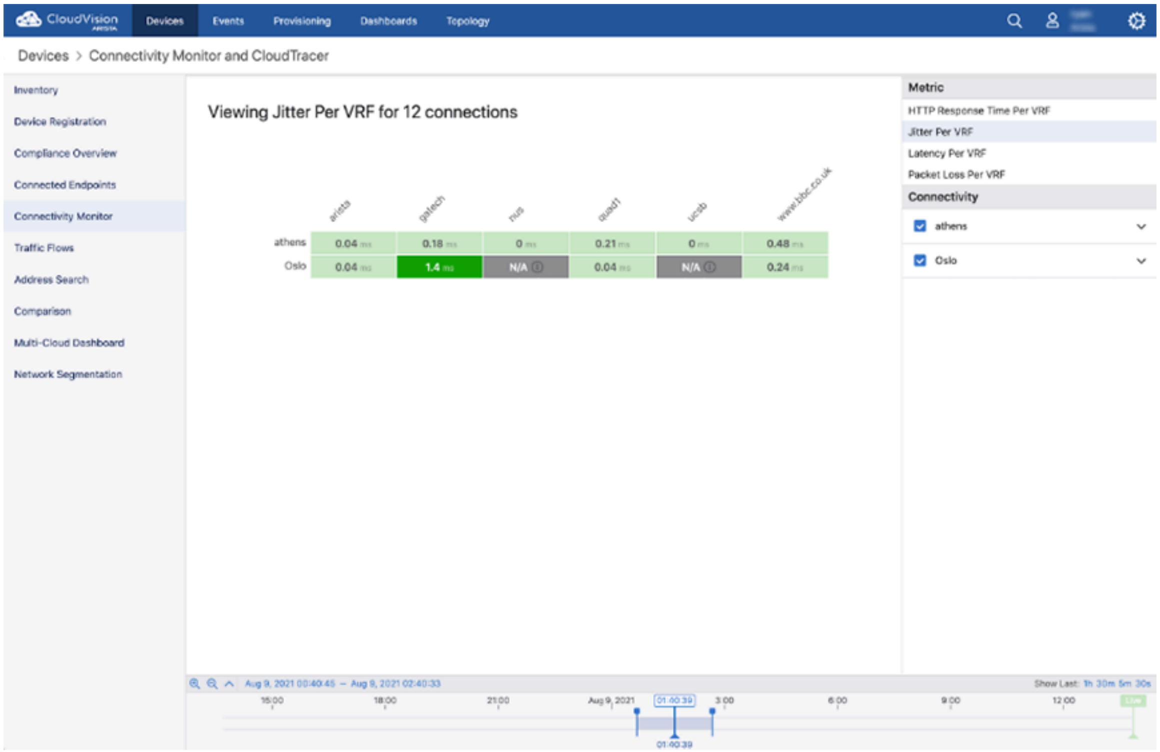
Connectivity Monitoring / Default

Monitored Hosts

Assign hosts to this group for EOS device monitoring.

After the Studio has been configured, review the Workspace and submit to Change Control. Once it has been approved, the results of the configured monitoring can be viewed by selecting the Connectivity Monitor under Devices.

Figure 17-48: Devices - Connectivity Monitor



Viewing Jitter Per VRF for 12 connections

	arista	gatech	nus	quad1	ucsb	www.bbc.co.uk
athens	0.04 ms	0.18 ms	0 ms	0.21 ms	0 ms	0.48 ms
Oslo	0.04 ms	1.4 ms	N/A ⓘ	0.04 ms	N/A ⓘ	0.24 ms

17.5.3 Date and Time

The Date and Time Studio is used to set the device time zones and to assign devices to NTP servers.

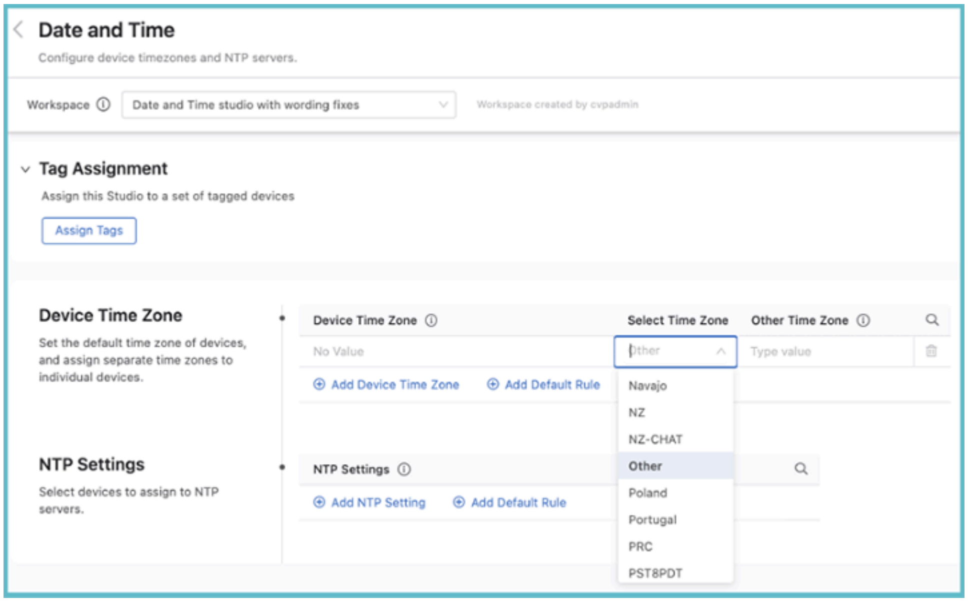
17.5.3.1 Setting a Device Time Zone

You can assign time zones to a set of tagged devices, and set a default time zone that is applied to all assigned devices not specified with a device tag query.

To set a time zone, click **Add Device Time Zone** or **Add Default Rule**. If relevant, enter a device tag, and then select a time zone from the drop down menu.

Time zones are ordered alphabetically. If the desired time zone is not in the list, select **Other** and enter a name for that time zone in the Other Time Zone field.

Figure 17-49: Setting a Device Time Zone



Date and Time

Configure device timezones and NTP servers.

Workspace: Date and Time studio with wording fixes

Workspace created by cvpadmin

Tag Assignment

Assign this Studio to a set of tagged devices

Device Time Zone

Set the default time zone of devices, and assign separate time zones to individual devices.

Device Time Zone	Select Time Zone	Other Time Zone
No Value	Other	Type value

NTP Settings

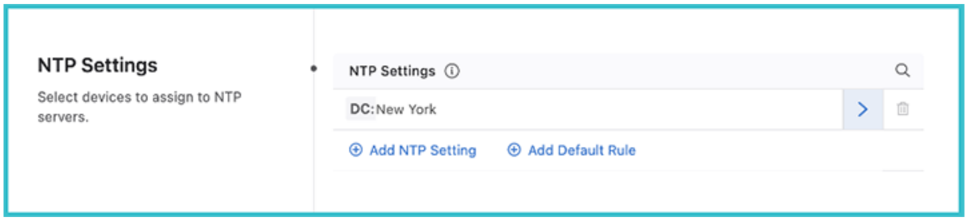
Select devices to assign to NTP servers.

Once you have assigned time zones to devices and optionally set the default time zone, review and submit the Workspace. Once it is approved and executed in Change Control, the new settings will come into effect on your network.

17.5.3.2 Configuring the NTP Settings

You can assign devices to an NTP server using device tags. Click **Add NTP Setting** and then enter a device tag to select devices with that tag. When done, click the arrow on the right.

Figure 17-50: Configuring the NTP Settings



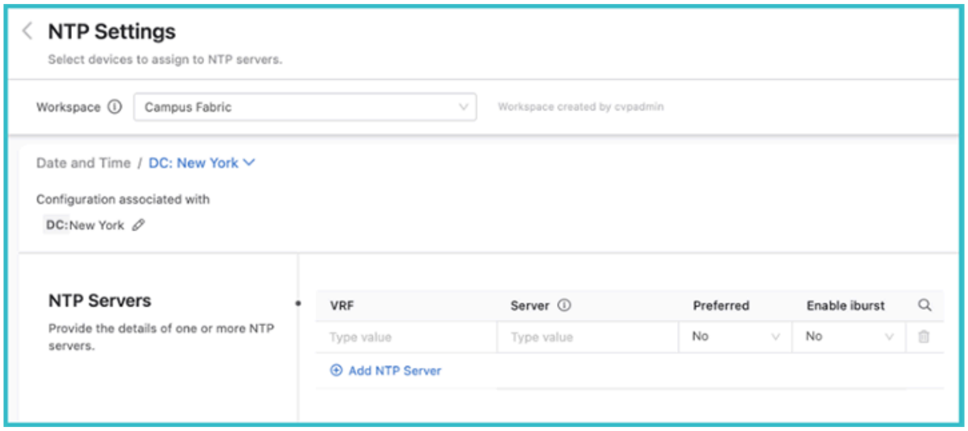
NTP Settings

Select devices to assign to NTP servers.

NTP Settings
DC:New York

Add NTP servers for these tagged devices by clicking **Add NTP Server**. Multiple servers can be added for the selected device tag, but only one server should be set as preferred. You can also enable iburst, which will send eight packets to the NTP server on start-up instead of a single packet. This will allow for faster synchronization.

Figure 17-51: Configuring Additional NTP Settings



NTP Settings

Select devices to assign to NTP servers.

Workspace: Campus Fabric — Workspace created by cvpadmin

Date and Time / DC: New York

Configuration associated with DC:New York

NTP Servers

Provide the details of one or more NTP servers.

VRF	Server	Preferred	Enable iburst
Type value	Type value	No	No

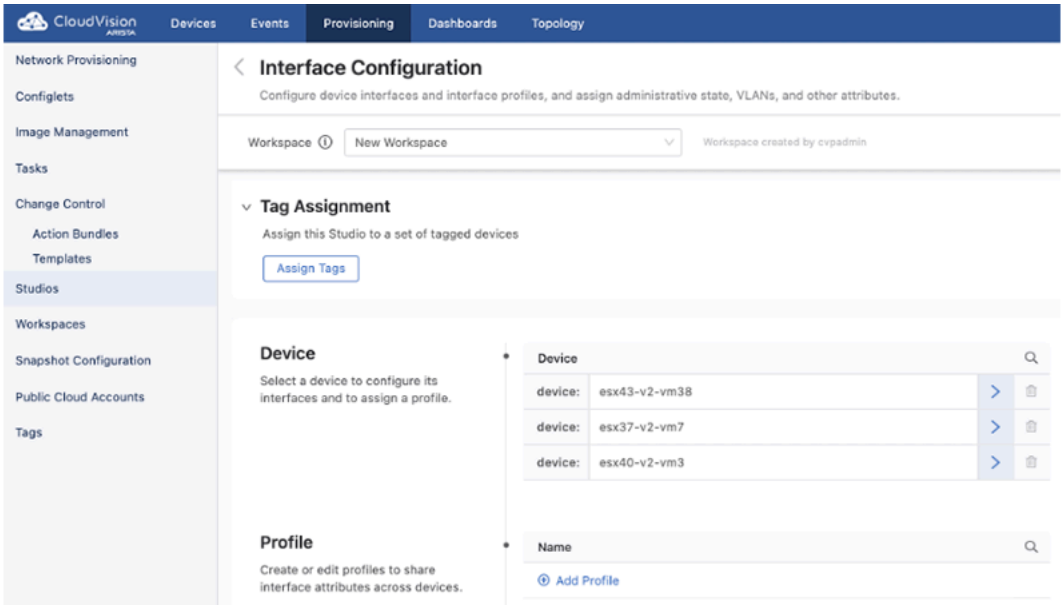
When you have assigned NTP servers to all the device tags, review and submit the Workspace. Once it is approved and executed in Change Control, the NTP settings will come into effect on your network.

17.5.4 Interface Configuration

The Interface Configuration Studio is used to provision interfaces that have been defined elsewhere. With it, you can configure interface speed, switchport mode, access VLAN or tagged VLANs, and enable or disable the interface. You can set up profiles with configurations for these attributes, which can then be applied to multiple interfaces. The use of profiles means that you do not need to separately configure repeating attributes for each device.

Select **Interface Configuration** to display the following screen.

Figure 17-52: Interface Configuration



Interface Configuration

Configure device interfaces and interface profiles, and assign administrative state, VLANs, and other attributes.

Workspace: New Workspace — Workspace created by cvpadmin

Tag Assignment

Assign this Studio to a set of tagged devices

Device

Select a device to configure its interfaces and to assign a profile.

Device	
device:	esx43-v2-vm38
device:	esx37-v2-vm7
device:	esx40-v2-vm3

Profile

Create or edit profiles to share interface attributes across devices.

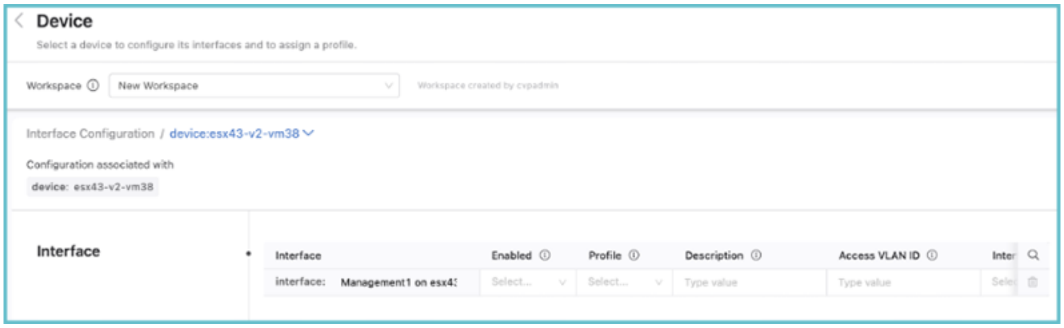
Name

You can either configure an interface belonging to an individual device, or you can configure an interface profile.

17.5.4.1 Configure a Device

All devices that have been commissioned for Studios using Inventory and Topology Studio will be listed under Device. Select the device to configure one or more interfaces for by clicking the arrow on the right.

Figure 17-53: Configure a device



Device

Select a device to configure its interfaces and to assign a profile.

Workspace: New Workspace

Workspace created by cvpadmin

Interface Configuration / device:esx43-v2-vm38

Configuration associated with

device: esx43-v2-vm38

Interface

Interface	Enabled	Profile	Description	Access VLAN ID	Inter
interface: Management1 on esx43	Select...	Select...	Type value	Type value	Sele

The list of interfaces that can be configured on this device and the available options are displayed. Scroll to the right to see all of the available options.

There is also a profile option, which can be used to assign a profile to the device. If you assign a profile, you do not need to enter a value for any other inputs; any values that you do enter for other inputs will override the values of the profile.

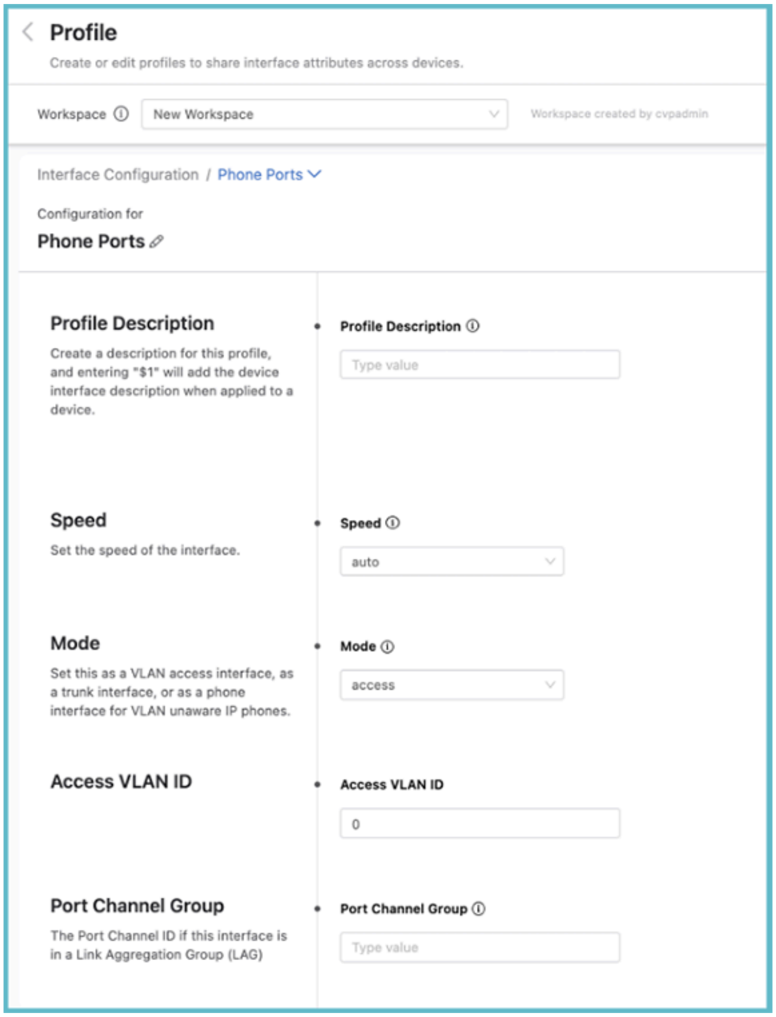
Note: If a device you want to configure is not available for selection, add it using the Inventory and Topology Studio.

17.5.4.2 Configuring a Profile

Profiles are used to avoid having to configure each device interface separately. You can create profiles with different characteristics and then assign a single profile to a device interface, which will apply the configuration associated with that profile to the interface of the device.

On the homescreen of Interface Configuration, click **Add Profile**. Enter a profile name and click the arrow on the right. The following screen is displayed.

Figure 17-54: Configuring a Profile



Profile

Create or edit profiles to share interface attributes across devices.

Workspace: New Workspace

Workspace created by cvpadmin

Interface Configuration / Phone Ports

Configuration for

Phone Ports

Profile Description

Create a description for this profile, and entering "$1" will add the device interface description when applied to a device.

Profile Description: Type value

Speed

Set the speed of the interface.

Speed: auto

Mode

Set this as a VLAN access interface, as a trunk interface, or as a phone interface for VLAN unaware IP phones.

Mode: access

Access VLAN ID

Access VLAN ID: 0

Port Channel Group

The Port Channel ID if this interface is in a Link Aggregation Group (LAG)

Port Channel Group: Type value

From the Profile screen, the speed, the switchport mode, the VLAN access, or tagged VLANs can be set. The mode selected for the interface may present you with more input options. When entering a description for the profile, enter “$1” which will pull the individual interface’s description into the description when applied to a device. For instance, you could give the profile description “Floor 3 phone ports: $1”; when you apply this profile to a device interface with the description “Office 1”, the full description of the interface will then be read elsewhere as: “Floor 3 Phone Ports: Office 1”.

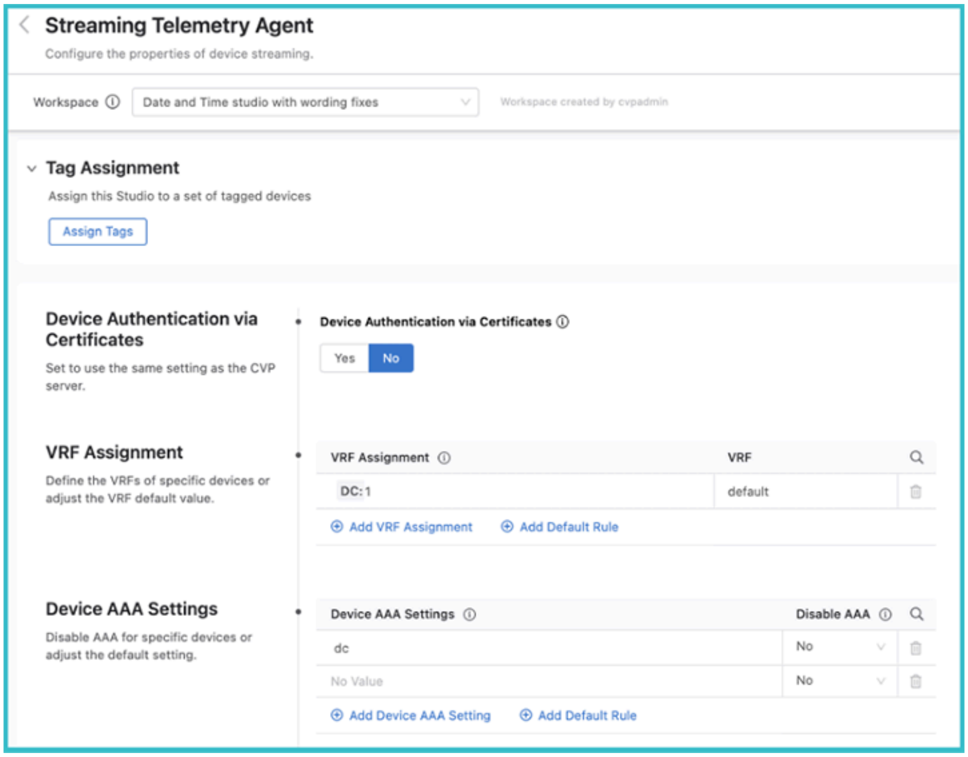
When the profile has been configured, apply it to device interfaces by selecting a device to configure. The profile can be applied to multiple interfaces across multiple devices. If you enter any individual interface parameters with a profile selected, the individual parameters will override those of the profile.

17.5.5 Streaming Telemetry Agent

The Streaming Telemetry Agent Studio enables you to define the streaming telemetry agent (TerminAttr) configuration for EOS devices streaming to CloudVision. The streaming telemetry agent is integral to the communication of state between network devices and CloudVision.

When you open the Studio, the following screen will be displayed.

Figure 17-55: Streaming Telemetry Agent



Streaming Telemetry Agent

Configure the properties of device streaming.

Workspace: Date and Time studio with wording fixes

Workspace created by cvpadmin

Tag Assignment

Assign this Studio to a set of tagged devices

Device Authentication via Certificates

Set to use the same setting as the CVP server.

Device Authentication via Certificates: Yes [✓ No]

VRF Assignment

Define the VRFs of specific devices or adjust the VRF default value.

VRF Assignment	VRF
DC:1	default

Device AAA Settings

Disable AAA for specific devices or adjust the default setting.

Device AAA Settings	Disable AAA
dc	No
No Value	No

17.5.5.1 Authentication

The first input determines how device streaming should be authenticated. There are two ways for the CVP server to authenticate the device sending the telemetry information:

- Certificate
- Ingest key

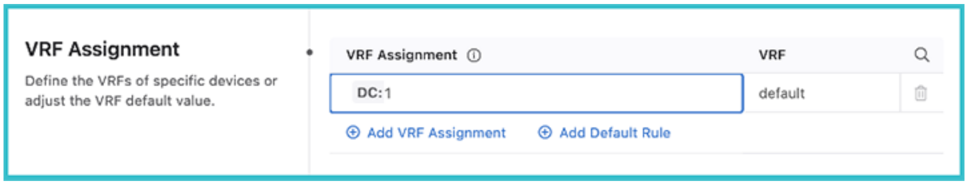
If you select **No**, the ingest key will be used, which is a shared cleartext key. This key is defined as part of the CloudVision set up process.

By selecting **Yes**, certificates are used for streaming authentication. CloudVision generates a JSON Web Token (JWT) that is then saved to a temporary location (e.g. /tmp/token). This token is used by TerminAttr for the initial secure authentication, and once authentication is successful, TerminAttr generates a certificate signing request (CSR) and sends it to the CloudVision server, which then signs the CSR with its own CA certificate and provides the generated client certificate to TerminAttr and stores it in the certificate partition on EOS. After this, TerminAttr will switch to using the client certificate and key, and renames the token by appending .backup to the filename and will not use it anymore.

17.5.5.2 VRF Assignment

Once you have selected the mode for authenticating the data, the VRF assignment can be selected. Here you will select devices with a tag query and then assign them to a VRF.

Figure 17-56: VRF Assignment



VRF Assignment

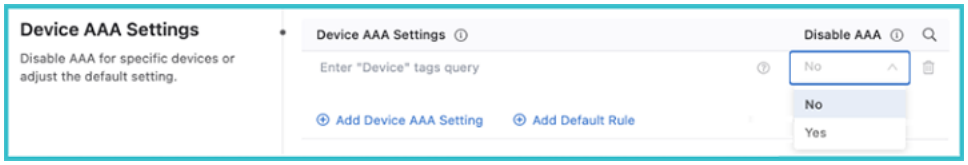
Define the VRFs of specific devices or adjust the VRF default value.

VRF Assignment	VRF
DC:1	default

17.5.5.3 Device AAA Settings

You can select devices using a tag query and disable elements of AAA for them.

Figure 17-57: Device AAA Settings



Device AAA Settings

Disable AAA for specific devices or adjust the default setting.

Device AAA Settings	Disable AAA
Enter "Device" tags query	No

When disabling AAA, you are disabling authorization and accounting for eAPI commands sent by CloudVision to TerminAttr only when the Advanced Login setting is used. This does not affect AAA for other transports, such as SSH or eAPI over HTTPS.

The Advanced Login setting has been the default login method since version 2021.2.0. It can use multi-factor authentication and one-time passcodes to authenticate all CloudVision managed devices when you authenticate with CloudVision. When you select **Yes**, all eAPI requests are sent over the gRPC session established by TerminAttr instead of eAPI over HTTPS.

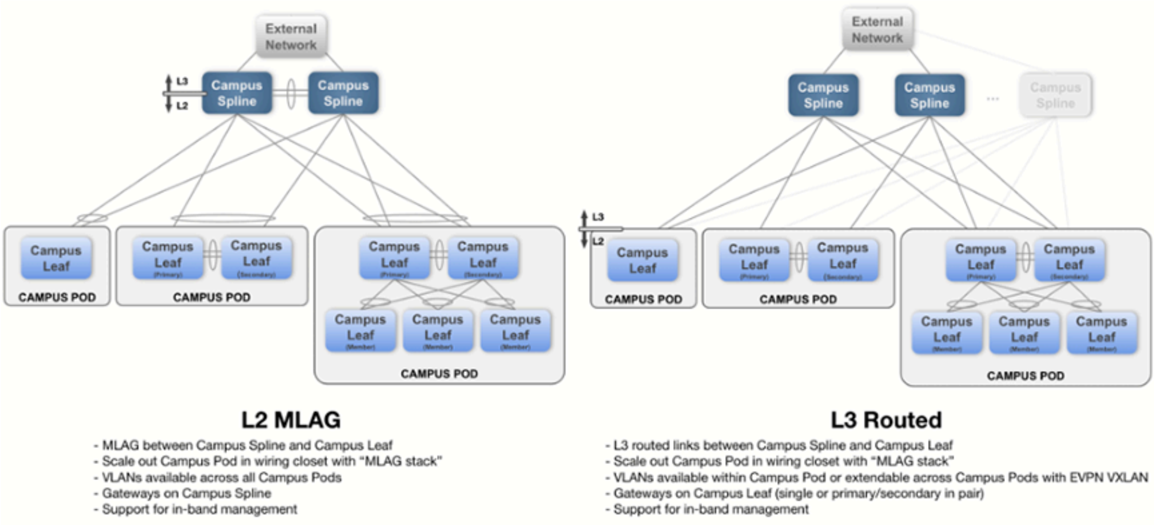
Disabling AAA is required in situations when the Advanced login setting is enabled and users are authenticated with certain RADIUS servers, where the server does not support authorization requests that do not have a preceding authentication request.

17.5.6 Campus Fabric

The Campus Fabric Studio provides a single point of control over the configuration of a campus network. The Studio is designed to allow the user to deploy and manage campus devices within the network using design patterns consistent with Arista best practices.

The Studio supports two common campus fabric designs. These designs are illustrated below, with support in beta-version for the L2 MLAG fabric.

Figure 17-58: Campus Fabric



L2 MLAG

- MLAG between Campus Spline and Campus Leaf
- Scale out Campus Pod in wiring closet with "MLAG stack"
- VLANs available across all Campus Pods
- Gateways on Campus Spline
- Support for in-band management

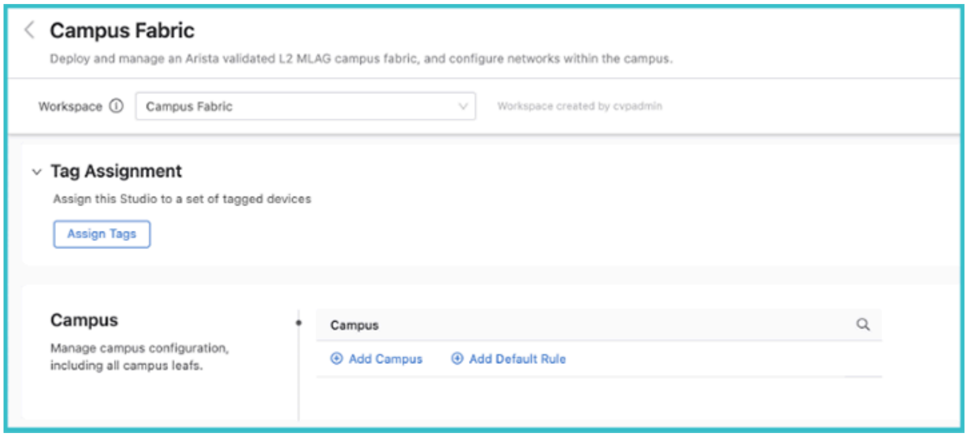
L3 Routed

- L3 routed links between Campus Spline and Campus Leaf
- Scale out Campus Pod in wiring closet with "MLAG stack"
- VLANs available within Campus Pod or extendable across Campus Pods with EVPN VXLAN
- Gateways on Campus Leaf (single or primary/secondary in pair)
- Support for in-band management

17.5.6.1 Deploying and Configuring a Campus

Select **Campus Fabric** to display the Campus Fabric screen.

Figure 17-59: Campus Fabric



Campus Fabric

Deploy and manage an Arista validated L2 MLAG campus fabric, and configure networks within the campus.

Workspace: Campus Fabric — Workspace created by cvpadmin

Tag Assignment

Assign this Studio to a set of tagged devices

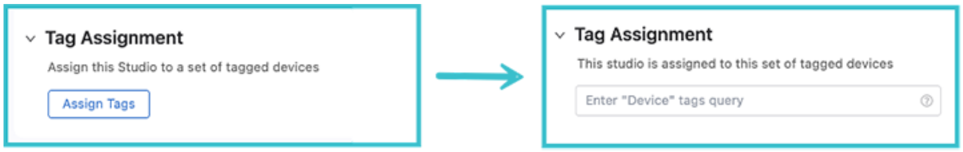
Campus

Manage campus configuration, including all campus leafs.

To create a new campus, click **Add Campus** and enter a name for the campus network. When done, click the arrow on the right.

The main configuration screen for the campus will be displayed.

Figure 17-60: Tag Assignment



Tag Assignment

Assign this Studio to a set of tagged devices

Tag Assignment

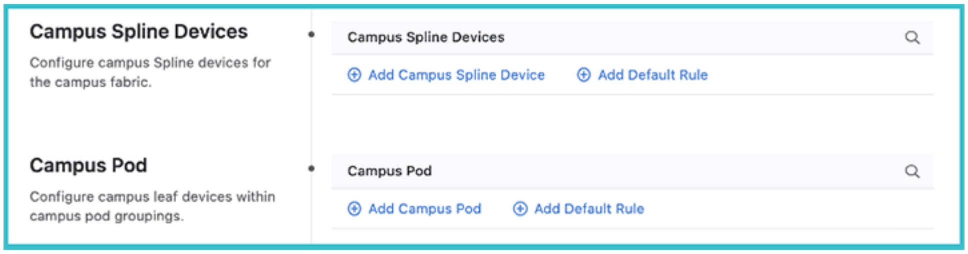
This studio is assigned to this set of tagged devices

To assign devices that belong to this campus, cick the dropdown arrow beside Tag Assignment and click **Assign Tags**. You can now add devices with a tag query to this campus network. If a desired device is not present, add it using the Inventory and Topology Studio or, if the tag is not present, create a new User Tag.

Next, configure the parameters and aspects of the L2 MLAG fabric. These parameters are used throughout the campus network when an MLAG pair exists. Configure the VLANs that will be defined for the campus network. A special management network may be defined when in-band management of the switches is required. The SVI virtual address is used as the anycast gateway across the campus Spline switches, as well as an IP helper address for DHCP relay functionality.

Central to the configuration of a campus network is assigning the roles to the selected devices in its fabric. They can be either campus Spline devices or leaf devices within a pod.

Figure 17-61: Assigning Roles



Campus Spline Devices

Configure campus Spline devices for the campus fabric.

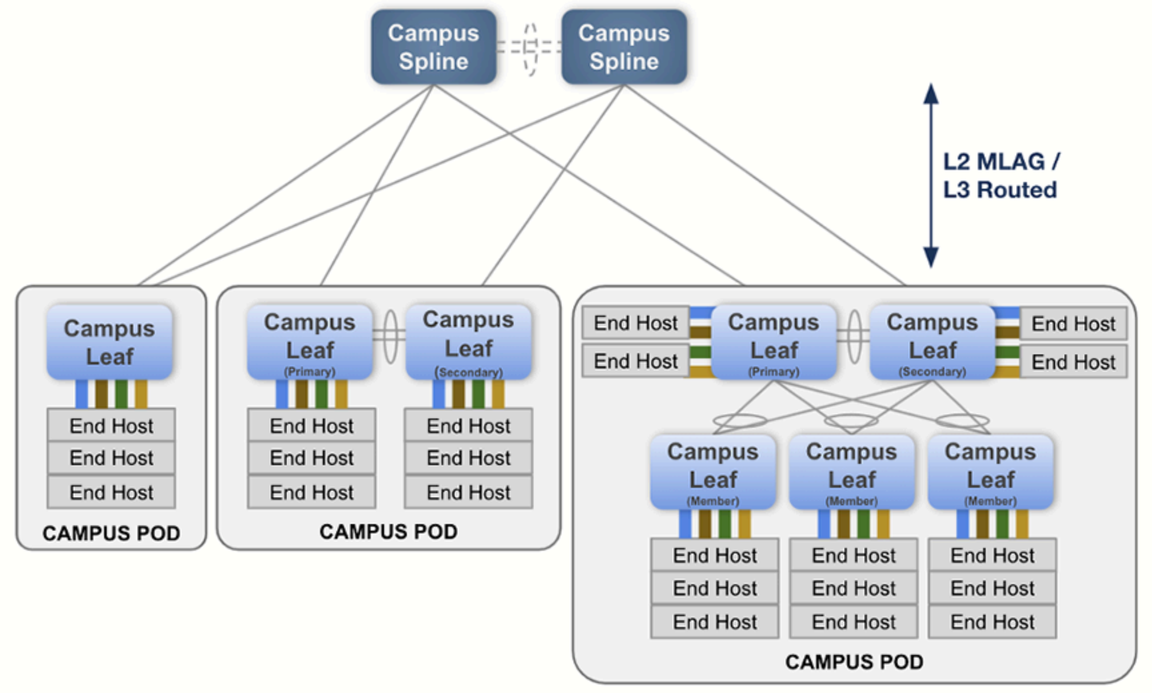
Campus Pod

Configure campus leaf devices within campus pod groupings.

A campus Spline device may be used for both connecting downstream campus leaf switches, as well as connecting hosts. The campus Spline device will often have links toward networks external to the campus fabric.

A pod is a collection of leaf devices that connect to a campus Spline pair of switches. Each pod consists of one or more switches and may be used to form an MLAG stack. Some examples of campus pods are shown below:

Figure 17-62: Examples of Campus Pods



The selection of devices available to assign either as campus Splines or as members of a pod are those that you defined earlier on this screen as belonging to the campus.

The connections between devices are configured in the Inventory and Topology Studio. If the devices are already wired-up in your network, they will be shown there. If not, the intended connections can be specified in that Studio, and configuration for those interfaces will be generated.

To build a campus network, you'll need the following connections:

- Between campus Splines: all interfaces connecting to the two Splines will be configured as an MLAG peer-link port channel.
- Between Splines and campus pod primary and secondary: these connections are referred to as "uplinks" and "downlinks". They should be arranged according to the L2 MLAG design shown above. Configure these connections as multi-chassis link aggregation (MLAG) port channels.
- Between the campus pod primary and secondary: all interfaces of the two leaf switches will be configured as an MLAG peer link port channel.
- Between pod primary and secondary and pod members: the connections between these devices are configured as multi-chassis link aggregation (MLAG) port channels

Once the configurations of your campus fabric have been set, submit the Workspace and your campus network will be available for review and approval in Change Control.

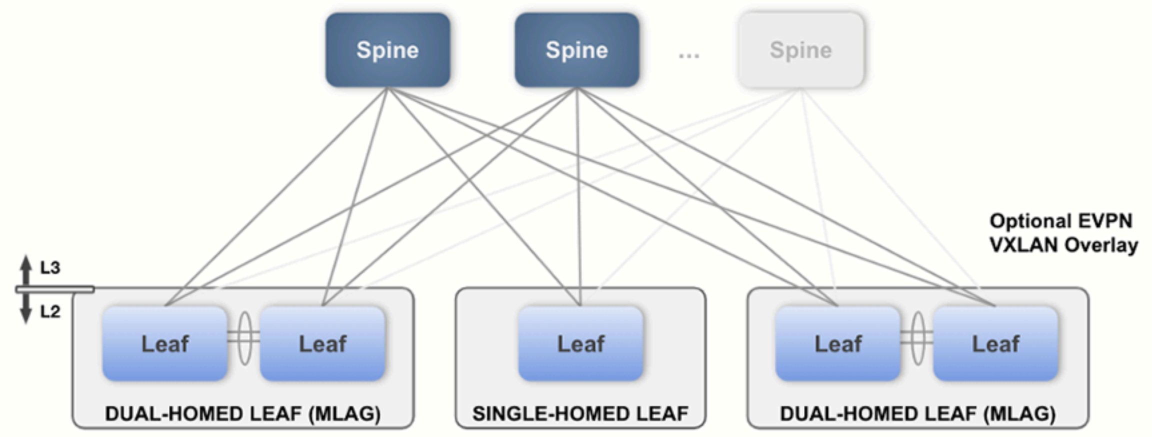
17.5.7 Layer 3 Leaf-Spine

You'll use this Studio along with EVPN Services to build a layer 3 leaf-spine network. The L3 Leaf-Spine Studio configures Day 1 deployment of the network, and EVPN Services configures Day 2 operations.

Note: In its beta-version, the Studio only supports BGP EVPN-VXLAN fabrics. It does not currently support the configuration of super-spines, multiple parallel transit connections between the same leaf and spine switches, detect/set speed on interfaces, and doesn't support recirc channels on platforms that require them for VXLAN routing.

The Studio has been designed to support the following Arista validated L3 leaf-spine design:

Figure 17-63: Layer 3 Leaf-Spine



Note: In order to build this design, you'll first need to use the Inventory and Topology Studio to either accept the LLDP derived topology connections or manually add devices and interface connections.

17.5.7.1 Layer 3 Leaf-Spine - Required Tags

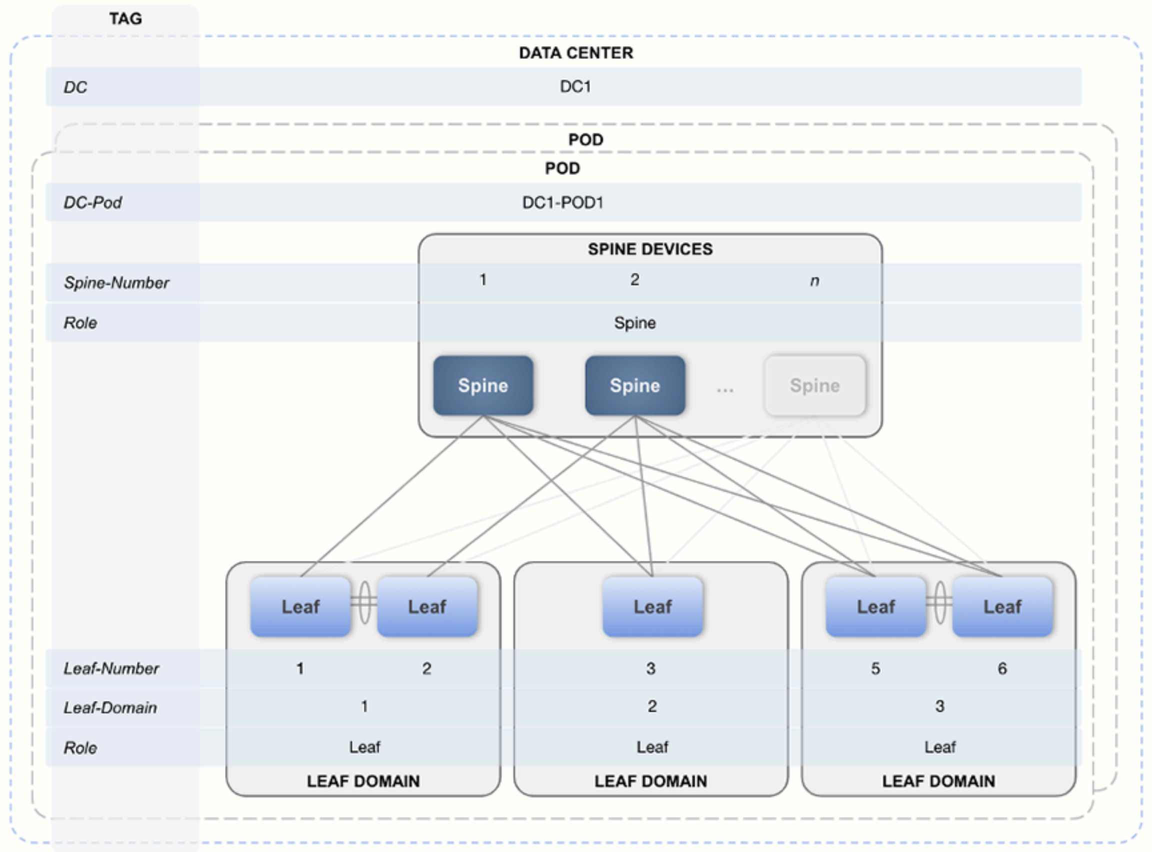
The following device tags must be in place before configuring the inputs in this Studio. You can create these tags within the same Workspace by accessing Tags.

Table 23: Leaf-Spine Required Tags

Tag	Example	Description
DC	DC: DC1	DC defines the data center that is being configured.
DC-Pod	DC-Pod: DC1	Data center pod name.
Role	Role: Leaf Role: Spine	Device Role. Can either be a leaf or spine.
Spine-Number	Spine-Number: 1	The number for a spine device. Each spine must have a unique number.
Leaf-Domain	Leaf-Domain: 1	Specifies the leafs within a common AS, which is usually an MLAG pair of leafs. The value must be an integer.
Leaf-Number	Leaf-Number: 1	The number for a leaf device. Each leaf must have a unique number. Leaf pairs are assumed to be numbered consecutively starting with an odd number (e.g. the device tagged Leaf-Number:9 and the device tagged Leaf-Number:10 are two devices in an MLAG pair of leafs). If a leaf is not part of an MLAG pair, just use one number of the odd-even pair and do not use the other number for another leaf (e.g. the device tagged Leaf-Number:1 will be configured as a standalone leaf if no other device is tagged Leaf-Number:2).

The tag placement is illustrated in the following diagram:

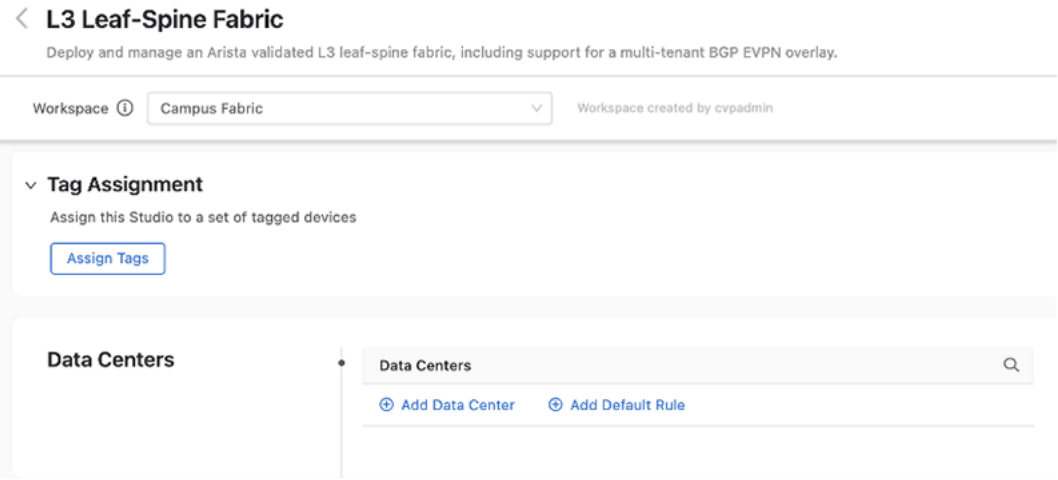
Figure 17-64: Layer 3 Leaf-Spine - Required Tags



17.5.7.2 Configuring the Fabric

Once tags are in place, you can create a data center in the Studio using the Data Center (DC) tag.

Figure 17-65: Configuring the Fabric



L3 Leaf-Spine Fabric

Deploy and manage an Arista validated L3 leaf-spine fabric, including support for a multi-tenant BGP EVPN overlay.

Workspace: Campus Fabric

Workspace created by cvpadmin

Tag Assignment

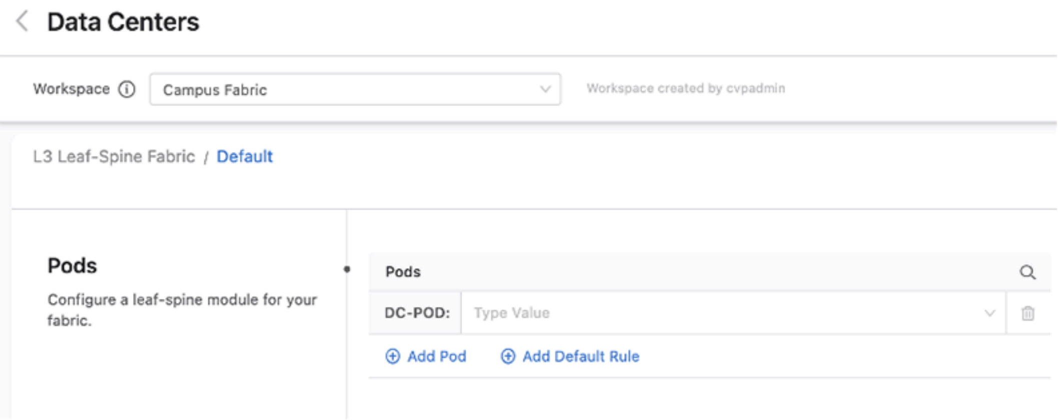
Assign this Studio to a set of tagged devices

Data Centers

Data Centers

After a data center is in place, then create and configure its pods. Each pod is a leaf-spine module inside the data center fabric. Use the DC-Pod tag to assign devices to a pod.

Figure 17-66: Configuring the Fabric - Pods



Data Centers

Workspace: Campus Fabric

Workspace created by cvpadmin

L3 Leaf-Spine Fabric / Default

Pods

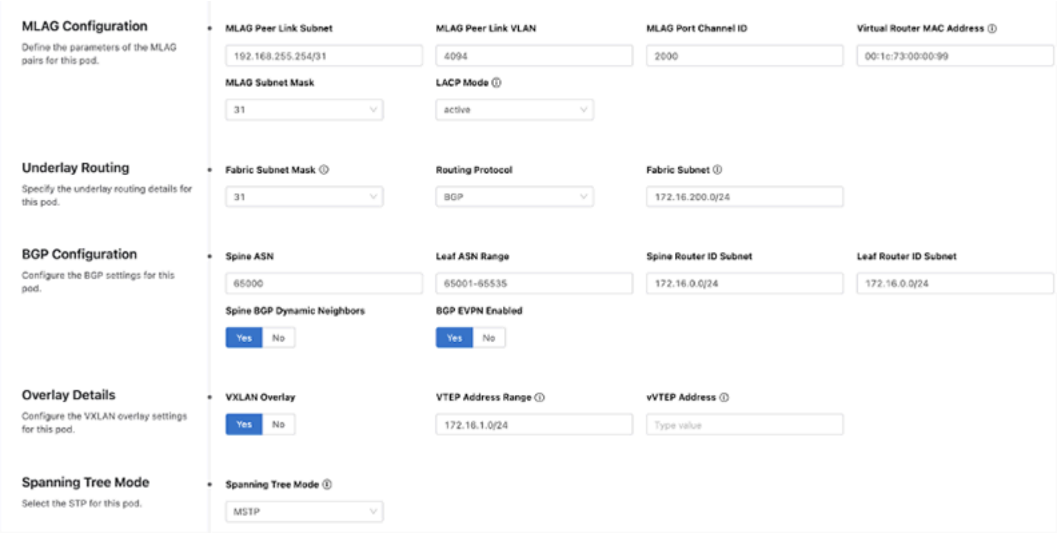
Configure a leaf-spine module for your fabric.

Pods

DC-POD: Type Value

Next, you will be presented with pre-filled values for the fabric of this pod, along with sections that allow you to add leaf and spine devices. Change the fabric configuration for the pod as needed.

Figure 17-67: Configuring the Fabric - Pod Configuration



MLAG Configuration

Define the parameters of the MLAG pairs for this pod.

- MLAG Peer Link Subnet: 192.168.255.254/31
- MLAG Peer Link VLAN: 4094
- MLAG Port Channel ID: 2000
- Virtual Router MAC Address: 00:1c:73:00:00:99
- MLAG Subnet Mask: 31
- LACP Mode: active

Underlay Routing

Specify the underlay routing details for this pod.

- Fabric Subnet Mask: 31
- Routing Protocol: BGP
- Fabric Subnet: 172.16.200.0/24

BGP Configuration

Configure the BGP settings for this pod.

- Spine ASN: 65000
- Leaf ASN Range: 65001-65535
- Spine Router ID Subnet: 172.16.0.0/24
- Leaf Router ID Subnet: 172.16.0.0/24
- Spine BGP Dynamic Neighbors: [✓ Yes] No
- BGP EVPN Enabled: [✓ Yes] No

Overlay Details

Configure the VXLAN overlay settings for this pod.

- VXLAN Overlay: [✓ Yes] No
- VTEP Address Range: 172.16.1.0/24
- vVTEP Address: Type value

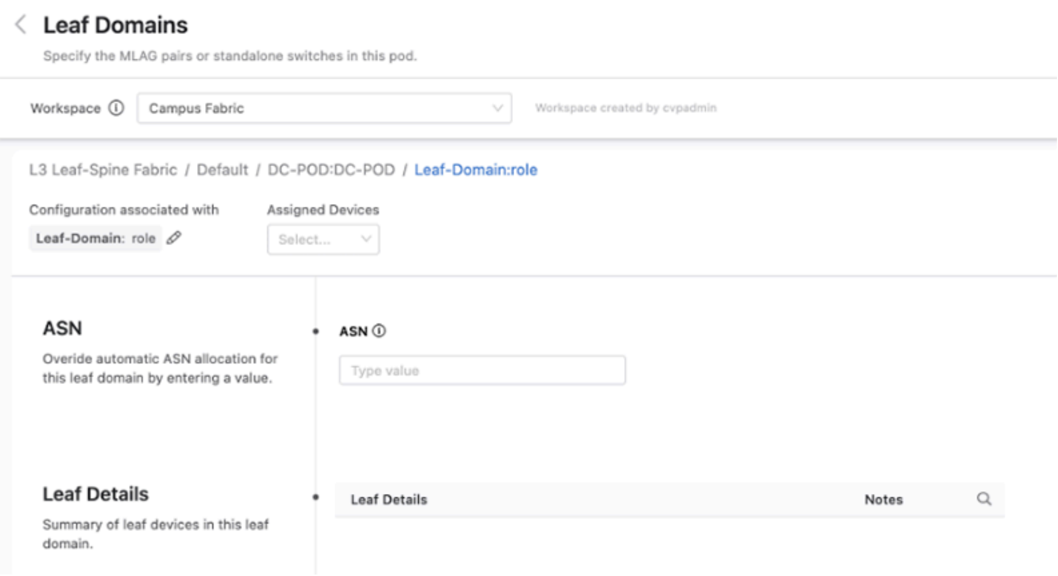
Spanning Tree Mode

Select the STP for this pod.

- Spanning Tree Mode: MSTP

You can add spine and leaf devices by using the Role tag. When adding a leaf device, you can further specify an ASN that will override the ASN number set at the pod level. You'll also be able to see on this screen a summary of all the devices in this domain.

Figure 17-68: Configuring the Fabric - Summary



Leaf Domains

Specify the MLAG pairs or standalone switches in this pod.

Workspace: Campus Fabric — Workspace created by cvpadmin

L3 Leaf-Spine Fabric / Default / DC-POD:DC-POD / Leaf-Domain:role

Configuration associated with: Leaf-Domain: role

Assigned Devices: Select...

ASN

Overide automatic ASN allocation for this leaf domain by entering a value.

ASN: Type value

Leaf Details

Summary of leaf devices in this leaf domain.

Leaf Details	Notes

Once you have configured all the data centers, pods, and their devices, review and submit the Workspace. A change control containing the configuration updates associated with the changes from the Workspace will be created. Review, approve, and execute the change control for the fabric configuration defined in the Workspace to take effect in the network.

Note: You can then stretch VLANs and VRFs across the newly deployed pods by using the EVPN Services Studio.

17.5.8 EVPN Services

The EVPN Services Studio allows you to deploy L2 and L3 network services. These services are applied to tenants that you create. Each tenant shares a common Virtual Network Identifier (VNI) range for MAC-VRF assignment.

Note: EVPN Services Studio is designed to implement Day 2 operations on top of the Day 1 fabric created with the Layer 3 Leaf-Spine Studio.

17.5.8.1 EVPN Services - Required Tags

The following tags are required for this Studio. They will already be in place if you have deployed an L3 leaf-spine fabric with the Layer 3 Leaf-Spine Fabric Studio.

Table 24: Required Tags

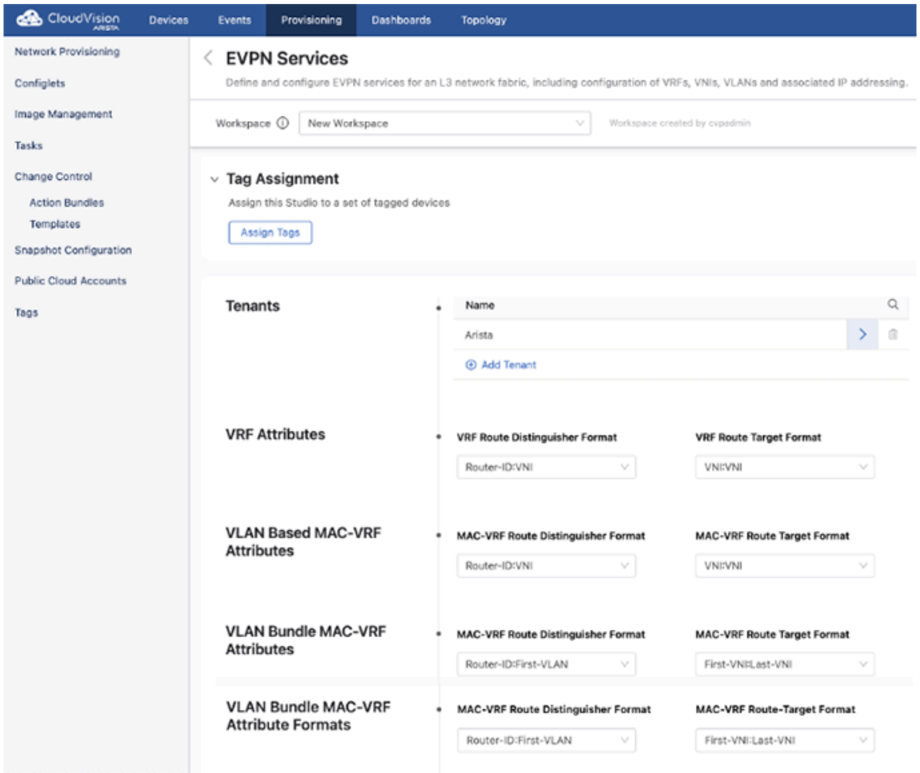
Tag	Example	Description
router_bgp.as	router_bgp.as:65050	Defines the BGP ASN that the switch will use when configuring overlay VRFs, VLANs, and VLAN aware bundles.
router_bgp.router_id	router_bgp.router_id:172.16.0.1	Defines the BGP Router ID used on the switch and makes up part of the route-distinguisher and route-target fields.
mlag_configuration.peer_link	mlag_configuration.peer_link:Port-Channel2000	Specifies the MLAG peer link used on a switch that has an MLAG peer. **Note:** This tag is only necessary for MLAG peer relevant configuration.
Leaf-Domain	Leaf-Domain:1	Specifies the leafs within a common AS, which are usually an MLAG pair of Leafs. The value must be an integer. **Note:** This tag is only necessary for MLAG peer relevant configuration.
Leaf-Number	Leaf-Number:1	For a leaf device, its number. Each leaf must have a unique number. Leaf pairs are assumed to be numbered consecutively starting with an odd number (e.g. the device tagged Leaf-Number:9 and the device tagged Leaf-Number:10 are two devices in an MLAG pair of leafs). If a leaf is not part of an MLAG pair, just use one number of the odd-even pair and don't use the other number for another leaf (e.g. the device tagged Leaf-Number:1 will be configured as a standalone leaf if no other device is tagged Leaf-Number:2). **Note:** This tag is only necessary for MLAG peer relevant configuration.

Note: If you do not want to use the L3 Leaf-Spine Fabric Studio, then you will need to create these tags before configuring the EVPN Services Studio.

17.5.8.2 Configuring EVPN Services

When you open EVPN Services, the following screen will be displayed. From this screen, tenants are created and the default VRF and MAC-VRF attributes for all tenants are created.

Figure 17-69: Configuring EVPN Services



EVPN Services

Define and configure EVPN services for an L3 network fabric, including configuration of VRFs, VNIs, VLANs and associated IP addressing.

Workspace: New Workspace

Workspace created by cvpadmin

Tag Assignment

Assign this Studio to a set of tagged devices

Tenants

Name
Arista

VRF Attributes
- VRF Route Distinguisher Format: Router-ID:VNI
- VRF Route Target Format: VNI:VNI

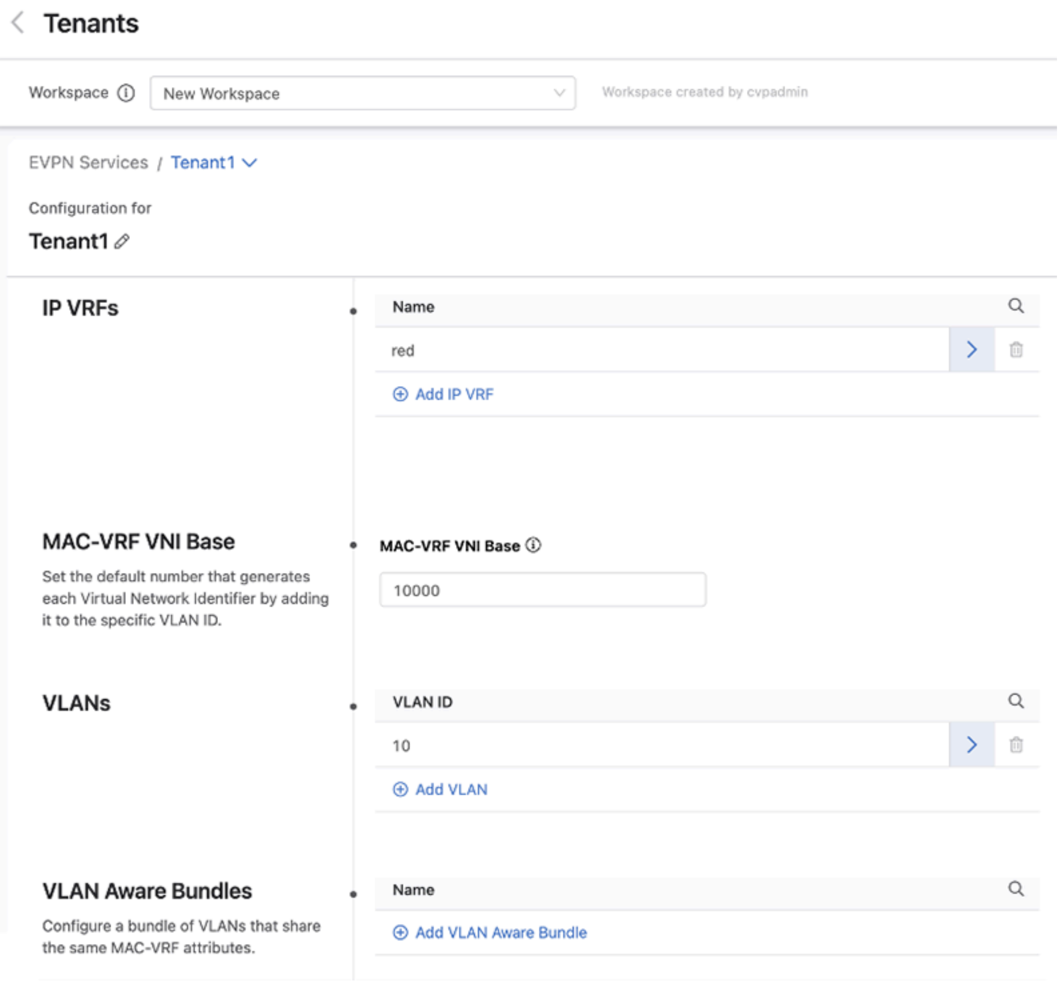
VLAN Based MAC-VRF Attributes
- MAC-VRF Route Distinguisher Format: Router-ID:VNI
- MAC-VRF Route Target Format: VNI:VNI

VLAN Bundle MAC-VRF Attributes
- MAC-VRF Route Distinguisher Format: Router-ID:First-VLAN
- MAC-VRF Route Target Format: First-VNI:Last-VNI

VLAN Bundle MAC-VRF Attribute Formats
- MAC-VRF Route Distinguisher Format: Router-ID:First-VLAN
- MAC-VRF Route-Target Format: First-VNI:Last-VNI

When creating a tenant or selecting an existing tenant to configure, you can create VRFs and VLANs for use within this tenant. You will also determine the base number used to generate VNIs.

Figure 17-70: Configuring EVPN Tenants



Tenants

Workspace ⓘ New Workspace

Workspace created by cvpadmin

EVPN Services / Tenant1

Configuration for

Tenant1

IP VRFs

Name
red

⊕ Add IP VRF

MAC-VRF VNI Base

Set the default number that generates each Virtual Network Identifier by adding it to the specific VLAN ID.

MAC-VRF VNI Base ⓘ: 10000

VLANs

VLAN ID
10

⊕ Add VLAN

VLAN Aware Bundles

Configure a bundle of VLANs that share the same MAC-VRF attributes.

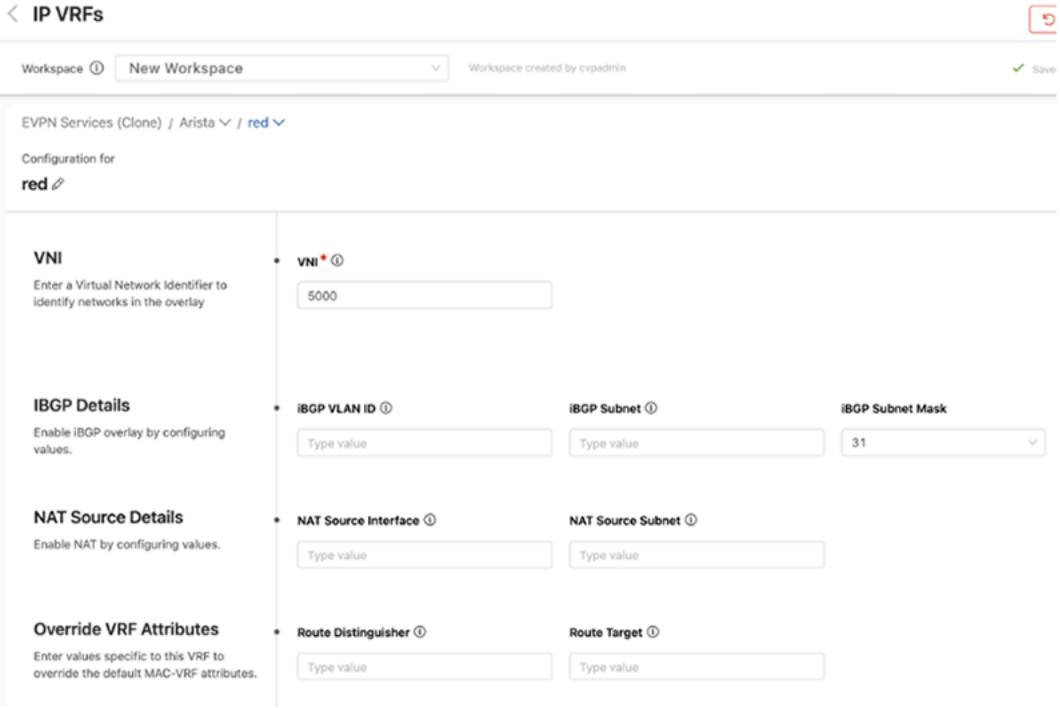
Name

⊕ Add VLAN Aware Bundle

17.5.8.3 VRFs

When configuring a VRF, always specify a VNI. The remaining fields are all optional and their use depends upon how you are configuring your network.

Figure 17-71: VRFs



IP VRFs

Workspace: New Workspace — Workspace created by cvpadmin — ✓ Save

EVPN Services (Clone) / Arista / red

Configuration for

red

VNI

Enter a Virtual Network Identifier to identify networks in the overlay

VNI*: 5000

IBGP Details

Enable iBGP overlay by configuring values.

iBGP VLAN ID: Type value

iBGP Subnet: Type value

iBGP Subnet Mask: 31

NAT Source Details

Enable NAT by configuring values.

NAT Source Interface: Type value

NAT Source Subnet: Type value

Override VRF Attributes

Enter values specific to this VRF to override the default MAC-VRF attributes.

Route Distinguisher: Type value

Route Target: Type value

The iBGP Detail fields are necessary when a VTEP is composed of a pair of leaf switches that have a host (or hosts) connected to only one switch in an MLAG pair. If incoming traffic arrives at the leaf switch in the pair that the host is not connected to, the leaf switch will drop that packet. By configuring a VLAN and SVI to establish an IBGP peering on for this VRF, both switches in an MLAG pair are aware of all host connections including those connected to only one switch.

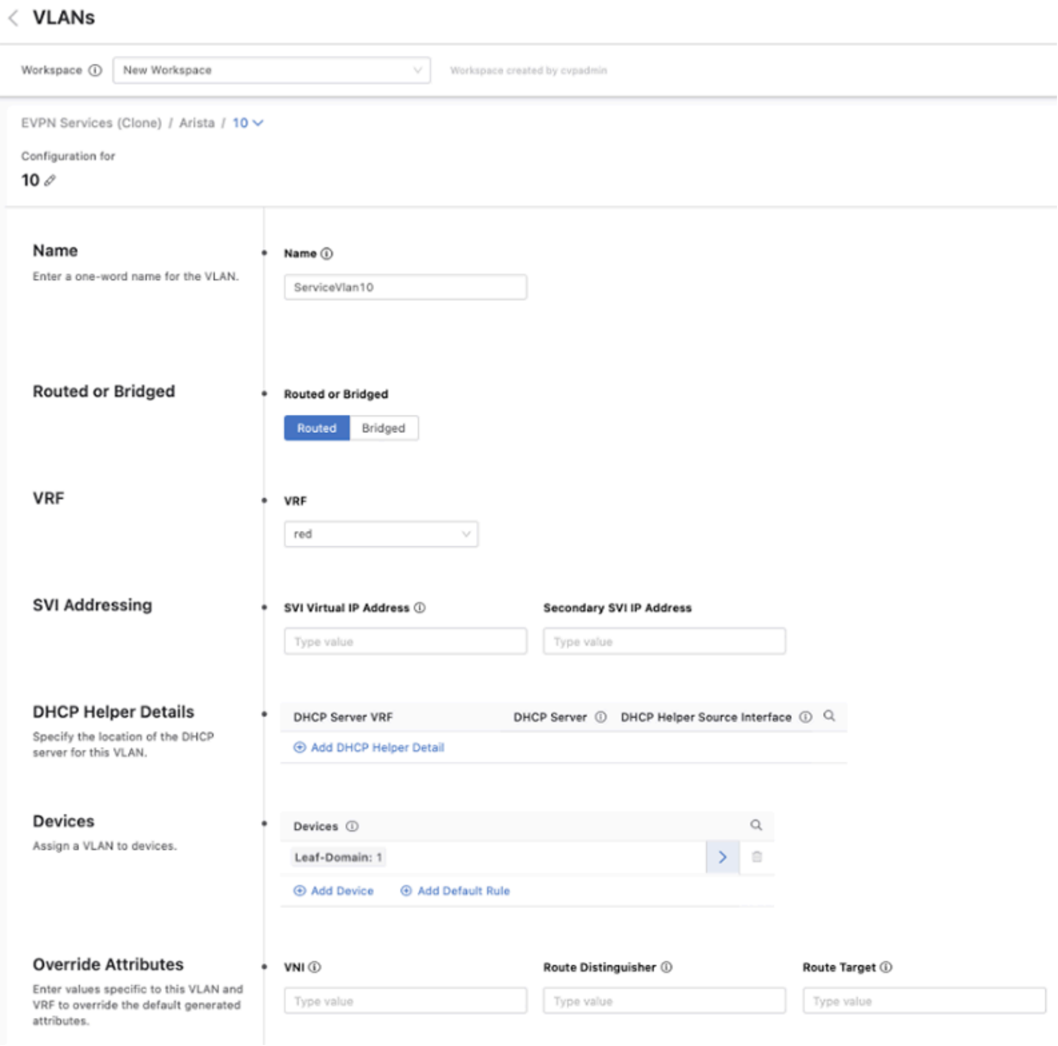
NAT Source Details are used to configure a virtual source NAT address for the VRF. It is used mainly for troubleshooting, because all VTEPs share the same IP address and MAC address for each SVI. This means that pings to workloads behind remote VTEPs or local workloads (e.g. MLAG VTEPs) may not be successful because the reply cannot be returned. When the destination host responds to either an ARP request or ICMP echo request, the reply is processed by the first VTEP it arrives at, which is because all VTEPs have the same IP and MAC address. In order for each VTEP to successfully ping a workload, configuring a NAT source address enables a dedicated loopback interface that can be used as the source address for pings within a VRF.

The Override VRF Attributes section allows you to override the default VRF attributes associated with this VRF.

17.5.8.4 VLANs

A name must be provided for each VLAN that is created. Then select whether it is applied to a routed or bridged setting.

Figure 17-72: VLANs



VLANs

Workspace ⓘ New Workspace

Workspace created by cvpadmin

EVPN Services (Clone) / Arista / 10

Configuration for

10

Name

Enter a one-word name for the VLAN.

Name ⓘ: ServiceVlan10

Routed or Bridged

Routed or Bridged: [✓ Routed] Bridged

VRF

VRF: red

SVI Addressing

SVI Virtual IP Address ⓘ: Type value

Secondary SVI IP Address: Type value

DHCP Helper Details

Specify the location of the DHCP server for this VLAN.

DHCP Server VRF	DHCP Server ⓘ	DHCP Helper Source Interface ⓘ

⊕ Add DHCP Helper Detail

Devices

Assign a VLAN to devices.

Devices ⓘ
Leaf-Domain: 1

⊕ Add Device ⊕ Add Default Rule

Override Attributes

Enter values specific to this VLAN and VRF to override the default generated attributes.

VNI ⓘ: Type value

Route Distinguisher ⓘ: Type value

Route Target ⓘ: Type value

By default, the toggle is set to routed. You can also provide details of a DHCP server and provide a default gateway by entering a Switched Virtual Interface (SVI) virtual IP address, which are options only available with a routed VLAN.

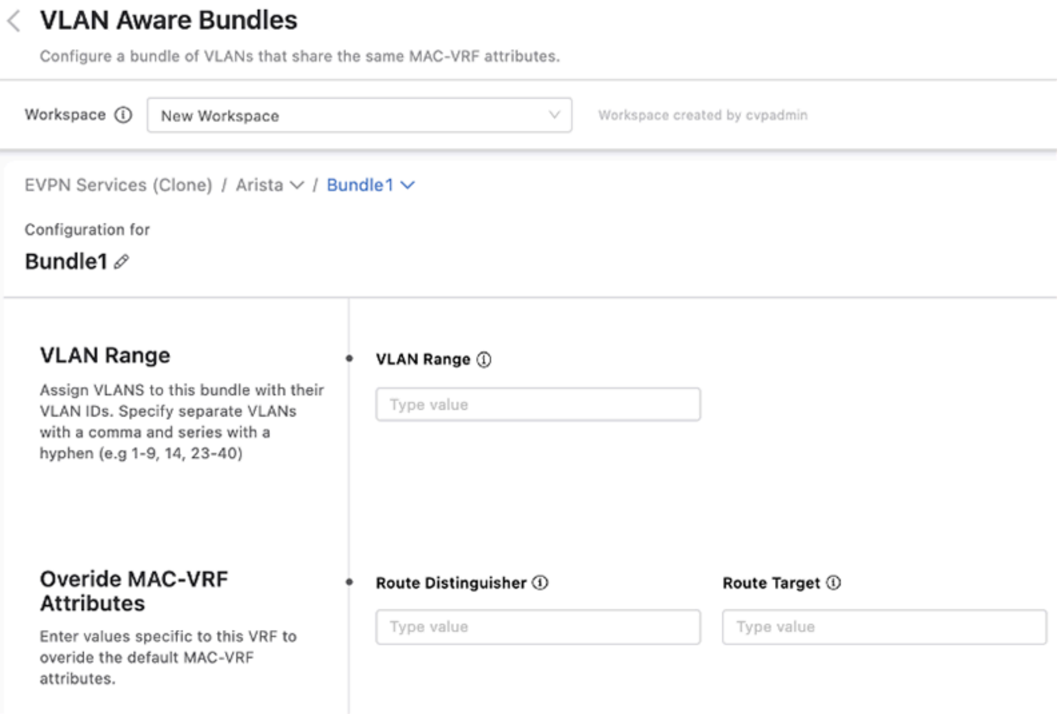
The last two options, Devices and Override Attributes, are shared with a bridged VLAN, where devices can be assigned to this VLAN and override the default values generated for configuration elements associated with this VLAN.

Note: When assigning devices to a VLAN, make sure to toggle the value for the Apply column to **Yes** to configure that VLAN.

17.5.8.5 VLAN Aware Bundles

You can bundle VLANs that have already been created within a tenant into VLAN aware bundles. Each bundle consists of a range of VLANs that share the same MAC-VRF attributes, which you can define by overriding the default MAC-VRF attributes shared across tenants.

Figure 17-73: VLAN Aware Bundles



VLAN Aware Bundles

Configure a bundle of VLANs that share the same MAC-VRF attributes.

Workspace: New Workspace

Workspace created by cvpadmin

EVPN Services (Clone) / Arista / Bundle1

Configuration for

Bundle1

VLAN Range

Assign VLANS to this bundle with their VLAN IDs. Specify separate VLANs with a comma and series with a hyphen (e.g 1-9, 14, 23-40)

VLAN Range: Type value

Overide MAC-VRF Attributes

Enter values specific to this VRF to overide the default MAC-VRF attributes.

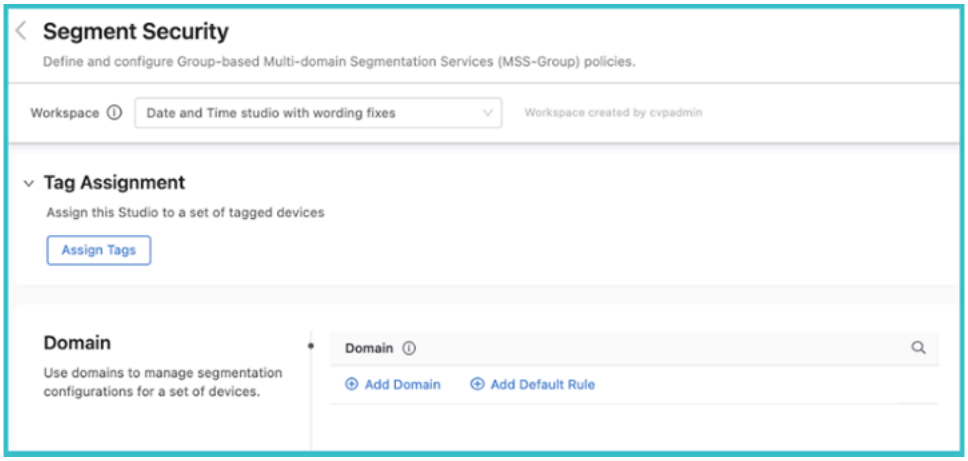
Route Distinguisher: Type value

Route Target: Type value

17.5.9 Segment Security

The Segment Security Studio enables you to separate your network into logical domains. Each domain contains a set of segments and policies that determine the forwarding behavior between segments. A segment describes a set of endpoints with identical security policies and network access privileges.

Figure 17-74: Segment Security



Segment Security

Define and configure Group-based Multi-domain Segmentation Services (MSS-Group) policies.

Workspace: Date and Time studio with wording fixes

Workspace created by cvpadmin

Tag Assignment

Assign this Studio to a set of tagged devices

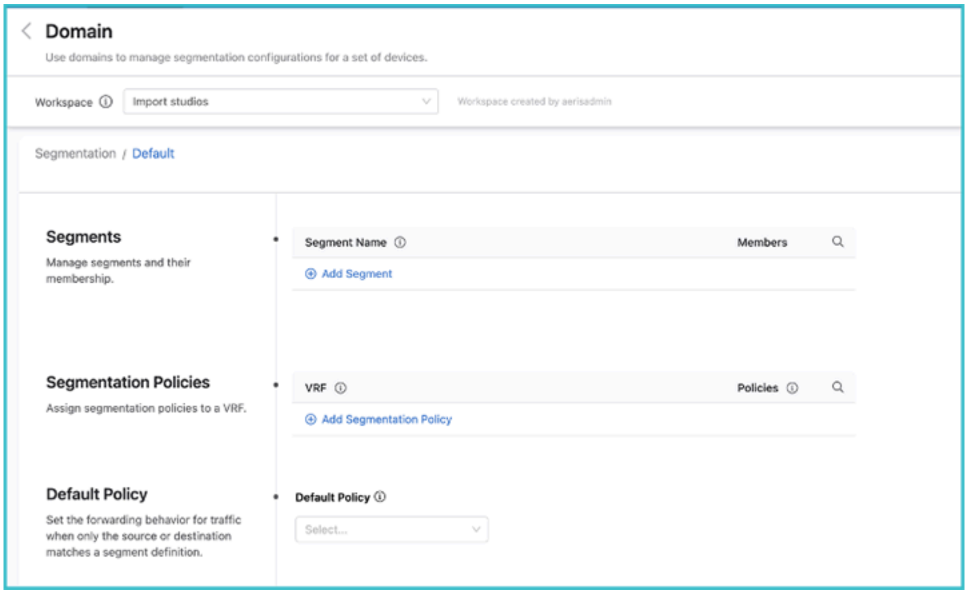
Domain

Use domains to manage segmentation configurations for a set of devices.

Domain

To create a segmentation domain, click **Add Domain** and enter a device tag query. A segmentation domain is identified by device tags, which gives you the ability to select a group of switches that form the domain. All devices in the same domain will be configured with identical segmentation policies.

Figure 17-75: Segment Security - Add Domain



Domain

Use domains to manage segmentation configurations for a set of devices.

Workspace: Import studios

Workspace created by aerisadmin

Segmentation / Default

Segments

Manage segments and their membership.

Segmentation Policies

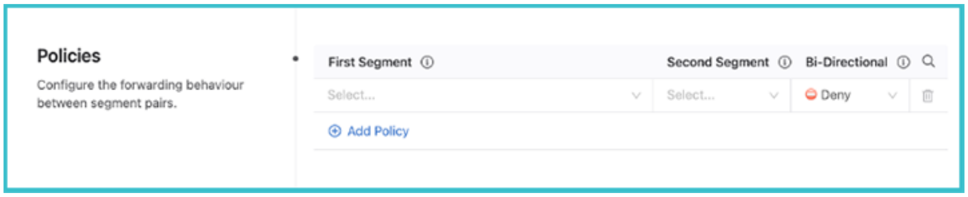
Assign segmentation policies to a VRF.

Default Policy

Set the forwarding behavior for traffic when only the source or destination matches a segment definition.

Once you have created the domain, click the arrow on the right, and the Policies screen will be displayed.

Figure 17-76: Segment Security - Policies



Policies

Configure the forwarding behaviour between segment pairs.

Enter a segment a name and identify its members. The segment membership is based upon either IPv4 or IPv6 prefixes, or both.

Next, set the security policies between segments. These policies apply to a single VRF. Configure segment policies for the VRF by clicking **View** underneath the Policies heading. Determine the relationship between pairs of segments inside the domain and the forwarding behavior of traffic between them.

17.6 MSS-G with Dynamic Configuration from Forescout

Using Forescout, an MSS-G configuration can be pushed automatically to CloudVision. This section covers the use of Forescout eyeSegment for policy definition and eyeSight for segment assignment. These systems produce an MSS-G configuration that is dynamic, and while visible on CloudVision, it bypasses the CLI on switches and will therefore not show up in the device running config.

There are two integration points from Forescout into Arista MSS-G:

- host to segment mapping in the Forescout console’s Policy Manager
- segment policy definition in Forescout eyeSegment

Both integration points are described below. Before deploying this integration, note that there is a terminology overlap:

- Arista MSS-G uses the terms “group” and “segment” interchangeably.
- The segments defined in the Forescout console under **Tools > Segment Manager** are static ranges designed to indicate areas of the network managed by Forescout and are unrelated to Arista MSS-G segments.
- The groups defined in the Forescout console Policy Manager are for organizing host/user/device taxonomy. Although it is possible through the Forescout Policy Manager to map each Forescout Group to an Arista MSS-G group, it is neither automatic nor required. In the majority of use cases, Forescout Groups will be hierarchical and not map directly to Arista MSS-G groups; instead, Arista MSS-G groups will be defined by Forescout Policies that may consider hosts/users/devices across several Forescout Groups.

Requirements

To configure MSS-G with Dynamic Configuration from Forescout the system must meet the following requirements:

On the Arista side:

- EOS 4.27.1F+
- TerminAttr 1.22+
- CloudVision 2022.1.1+.
- On the Forescout side it’s GA for Continuum 8.4.0, eyeSegment 5.18.0 (recommend 5.19.0), and the Forescout Arista MSS-G 1.0.0 module.

On the Forescout side:

- Continuum 8.4.0
- eyeSegment 5.18.0 (recommend 5.19.0)
- Forescout Arista MSS-G 1.0.0 module.

Limitations

Note the following limitations before configuring MSS-G with Dynamic Configuration from Forescout.

- Port matching: Policies are enforced based on IP address, and at this time there is no support for port or protocol matching.
- 60-segment limit: Arista CloudVision and EOS switches support a maximum of 60 segments.
- Single segmentation domain: All EOS switches participating in MSS-G receive all host-to-segment assignments transmitted from Forescout eyeSight to Arista CloudVision.
- Single VRF: The integration supports just a single Virtual Routing and Forwarding instance, or VRF. That VRF is configurable, but by default it uses the default VRF.
- Initial sync time: The initial transmission of host-to-segment assignments from CounterACT to CloudVision could take up to an hour, depending on the number of hosts, the number of CounterACT appliances, and the latency between CounterACT and CloudVision. It can be made much faster by enabling dynamic configuration on participating switches after CloudVision has received all initial segmentation configuration.
- Host scale: The integration supports up to 25,000 hosts in its initial phase. Enforcement point scale: The integration supports up to 100 enforcement points. Note that not all switches must be used as enforcement points. As long as traffic flows through an MSS-G capable enforcement point, policies will be enforced.
- Supported actions: Currently, the supported actions are forward and drop.
- IPv6: IPv6 is not currently supported in this integration.
- Wifi endpoints: To make the integration work with wireless clients, access points must be configured to forward traffic in the clear to an enforcement point.

17.6.1 Deployment Guidelines

- Subnets: eyeSight applies policies to single hosts, but users may assign all hosts within a subnet to a single segment using CloudVision Studios.

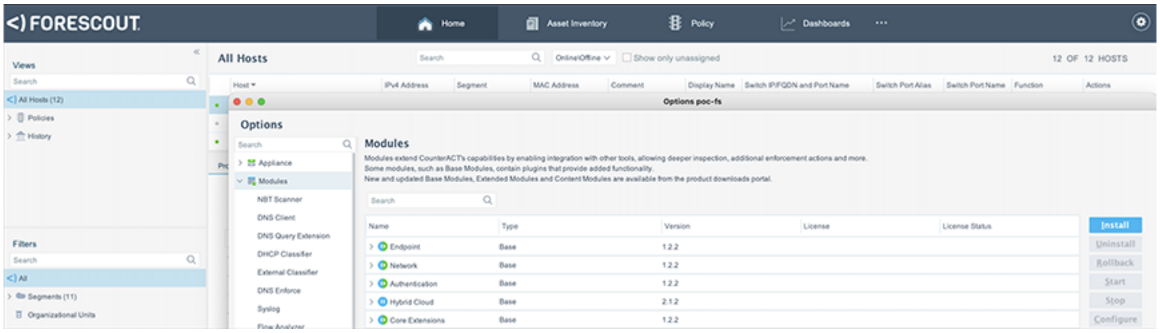
- Default forwarding behavior: Policies are enforced based on destination address. There are three cases.
  - The source and destination address each belong to a segment, and there is a segment-policy defined that determines the forwarding behavior for the packet. In this case, participating switches will enforce the configured segment policy.
  - The destination address does not belong to any segment. In this case, there is no MSS-G configuration to enforce, and the switch's actions will reflect whatever non-MSS-G configuration exists on the switch.
  - The destination address belongs to a segment, but either the source address does not or there is no segment policy to determine what action the switch should take. In this case the switch uses an “unspecified policy action” default, which could be DROP or FORWARD. This can be set in the eyeSegment MSS-G plugin.
- One segment per host: A host IP address can exist in only one Arista segment (e.g., an IT admin user cannot be in both a “user” and an “admin” segment simultaneously).
- Flat segment-policy hierarchy: eyeSegment policies destined for export to Arista CloudVision must not contain exceptions or make use of the “Any” group, eyeSegment virtual zones (e.g., Internal), or deleted zones. Improperly formed policies won't be exported.
- Bidirectional segment policies: Users should typically construct policies to forward or drop traffic in mirrored fashion (e.g., Zone A to Zone B Allow All and Zone B to Zone A Allow All). It is not strictly necessary to define rules both ways, but given the probability of bidirectional traffic, users will usually want to configure policies bidirectionally.
- Export to CloudVision: The export to CloudVision is disabled by default until eyeSegment version 5.19, but can be enabled via the fstool command. Starting with version 5.19 it is enabled by default.
- Resynchronization: Users must configure resynchronization per host-to-segment assignment policy or else CounterACT will never transmit host-to-segment assignments for hosts it learns while its connection to CloudVision is down. All deployments should use resync. Instructions for setting up resync can be found in the policy template.
- Policy export flap: Exporting policies from eyeSegment to MSS-G may result in a brief period of forwarding disruption as switches remove and then re-apply policies.
- Switch forwarding table partition: The EOS switches must have forwarding table partitions in place that allow for the desired host scale.
- A CloudVision certificate should be imported into Forescout Continuum's trusted certificates in order to secure the connection between Forescout Continuum and CloudVision.
- On 4GB switches there may not be sufficient memory to run dynamic MSS-G and sFlow.

17.6.2 Install the Arista MSS-G Module

Forescout's Arista MSS-G module adds the ability to connect to CloudVision and also assigns MSS-G segment ID in the policy manager.

The MSS-G module is an *.fpi file just like any other Forescout module.

Figure 17-77: Forescout MSS-G Module



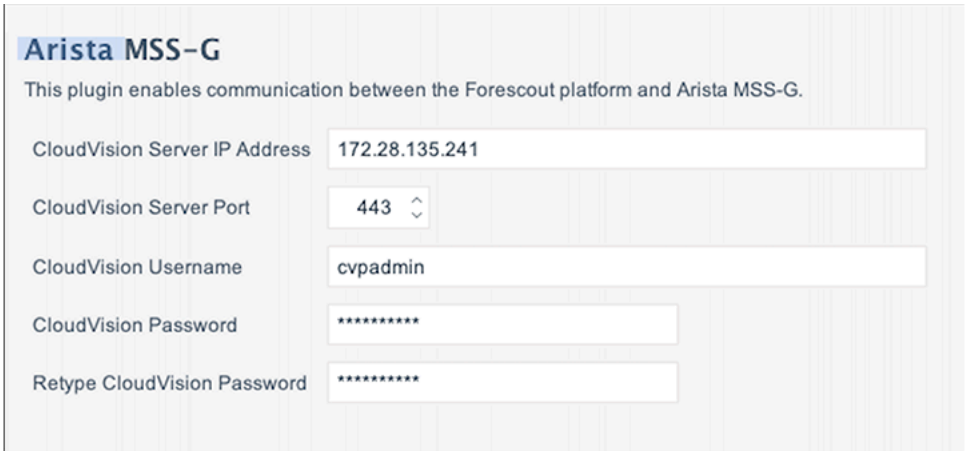
Modules

Modules extend CounterACT's capabilities by enabling integration with other tools, allowing deeper inspection, additional enforcement actions and more.
Some modules, such as Base Modules, contain plugins that provide added functionality.
New and updated Base Modules, Extended Modules and Content Modules are available from the product downloads portal.

Name	Type	Version	License	License Status
Endpoint	Base	1.2.2		
Network	Base	1.2.2		
Authentication	Base	1.2.2		
Hybrid Cloud	Base	2.1.2		
Core Extensions	Base	1.2.2		

Once installed, double-click on the Arista MSS-G module from the list and enter the CloudVision information:

Figure 17-78: Forescout - Arista MSS-G Plug-in



Arista MSS-G

This plugin enables communication between the Forescout platform and Arista MSS-G.

CloudVision Server IP Address: 172.28.135.241

CloudVision Server Port: 443

CloudVision Username: cvpadmin

CloudVision Password: **********

Retype CloudVision Password: **********

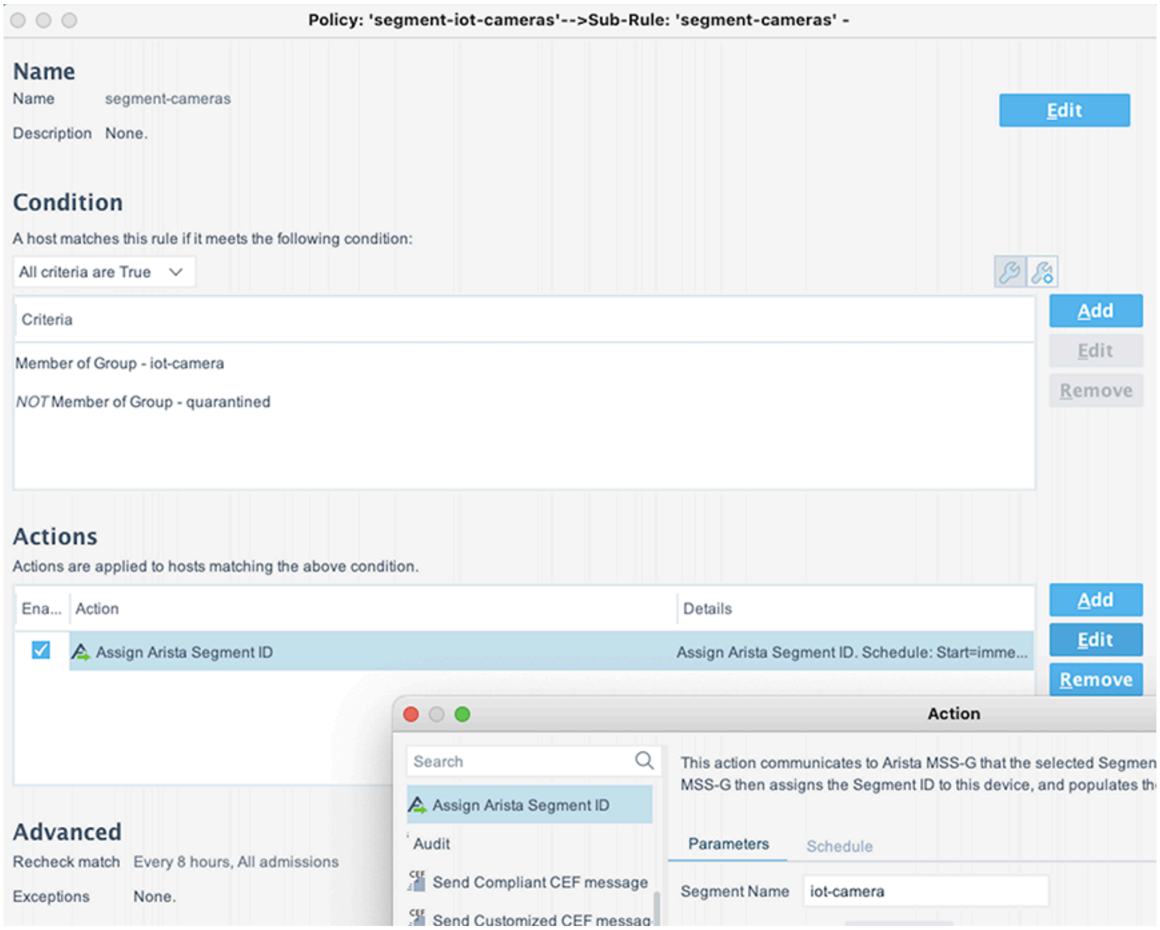
17.6.3 Specify Group Assignments with Forescout Policy Manager

The Forescout Policy Manager can be used to assign a user/host/device to an Arista MSS-G segment. This function is available as an action inside any Forescout policy. The conditions for classifying an endpoint to a group within the Forescout policy manager can be advanced combinations of many pieces of data, including DHCP vendor class, DNS event, SNMP system uptime, OS version, Active Directory group, and many other factors. In the example below, other policies (not shown) have classified cameras into the “IOT-Camera" Forescout group.

In the following example, another policy is defined that assigns the Arista Segment ID of “IOT-Camera” to all the members of the Forescout “IOT-Camera” group. Note that although the example shows a matching Forescout group and Arista MSS-G segment name, this is not required. However, if groups are defined on Forescout and segment policies are defined on CloudVision, then it is mandatory to have matching names.

Note: Group names configured on Forescout should not contain spaces.

Figure 17-79: Defining a Segment Policy



Policy: 'segment-iot-cameras'-->Sub-Rule: 'segment-cameras' -

Name

Name segment-cameras

Description None.

Condition

A host matches this rule if it meets the following condition:

All criteria are True

Criteria
Member of Group - iot-camera
NOT Member of Group - quarantined

Actions

Actions are applied to hosts matching the above condition.

Ena...	Action	Details
☑	Assign Arista Segment ID	Assign Arista Segment ID. Schedule: Start=imme...

Advanced

Recheck match Every 8 hours, All admissions

Exceptions None.

Action

This action communicates to Arista MSS-G that the selected Segmen

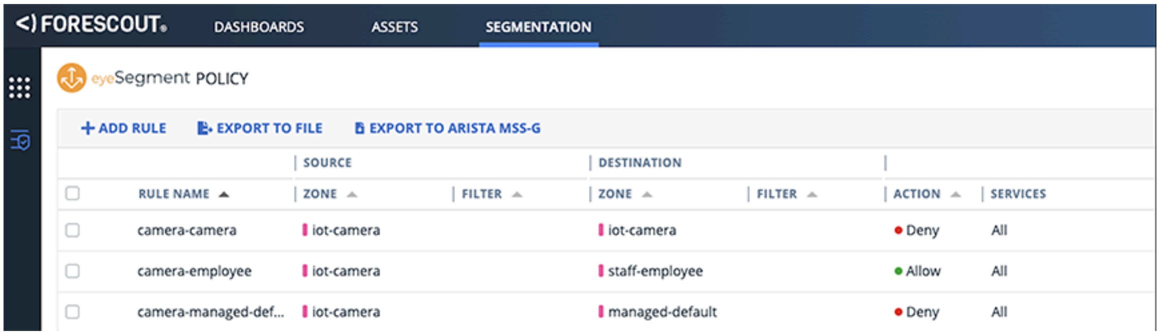
MSS-G then assigns the Segment ID to this device, and populates th

Segment Name iot-camera

17.6.4 Define segment policies in eyeSegment

The Forescout eyeSegment interface can be used to define Arista MSS-G Segment policies. The Zones listed in each eyeSegment policy must match with Arista MSS-G group names being used by Forescout Policy Manager or CloudVision to map IP addresses to groups. Forescout eyeSegment policies that are to be exported to CloudVision must use “All” in the services field.

Figure 17-80: Exporting eyeSegment policies into CloudVision



	SOURCE		DESTINATION			
RULE NAME	ZONE	FILTER	ZONE	FILTER	ACTION	SERVICES
camera-camera	iot-camera		iot-camera		● Deny	All
camera-employee	iot-camera		staff-employee		● Allow	All
camera-managed-def...	iot-camera		managed-default		● Deny	All

Select **Export to Arista MSS-G** to export eyeSegment policies into CloudVision. Check that the appropriate segment-policies show up in CloudVision’s network-wide **Network Segmentation** view. All Forescout eyeSegment policies must be exported at the same time. If a subset of policies is exported, previously exported eyeSegment policies not currently selected will be removed.

Enable OpenConfig on Arista switches

On participating, segmentation-enabled Arista devices, enable OpenConfig with the following commands:

```
>en
#conf
(config)#management api gnmi
(config-mgmt-api-gnmi)#transport grpc default
(config-gnmi-transport-default)#no shutdown
```

Enable Dynamic Configuration on Arista switches

Add the flag `–cvconfig=true` to the TerminAttr configuration on each participating switch:

```
(config)#daemon TerminAttr
(config-daemon-TerminAttr)#exec /usr/bin/TerminAttr -ingestgrpcurl=<address>:<
port> -cvcompression=gzip -ingestauth=token,/tmp/token … -cvconfig=true
(config-daemon-TerminAttr)#no shut
```

17.6.5 Forescout with Studios

You may add a segmentation configuration via both CVP Studios and Forescout, if desired. However, the configuration should be non-overlapping.

One use-case is defining default policies. Forescout allows you to associate known hosts with segments, and will push segment-policies to CloudVision. However, it does not provide you a way to describe the desired forwarding behavior for unknown hosts. This may be important if, for example, you want to define the desired forwarding behavior between known hosts in the network and the Internet. In this case, you may define a segment with an IP prefix that captures the desired set of unknown hosts (possibly 0.0.0.0/0) and specify segment-policies between this default segment and other defined segments.

17.7 ISE/MSS-G Integration

ISE/MSS-G integration uses TrustSec data from Cisco ISE to create an MSS-G configuration to distribute to switches via CloudVision. The integration is implemented by an ISE provider that runs in the third-party collector. It maps TrustSec Security Groups (SGTs), Access Control Lists, and policies into MSS-Segments and policies. The integration is built on top of Cisco ISE’s External RESTful Services (ERS) and pxGrid APIs. Most of the integration is based on pxGrid and some information that is not available through pxGrid is loaded using the ERS REST APIs.

17.7.1 Prerequisites

The integration requires a few configurations in Cisco ISE. Refer to Cisco ISE documentation for configuration information.

- A pxGrid compatible license is necessary.
- The pxGrid service must be enabled.
- The ERS service must be enabled.
- There must be a user with ERS access permission.
- ISE certificates must contain Subject Alternative Name (SAN). Common Name based certificates will be rejected.

Note: Skipping CA validation is possible and may be used as a workaround if necessary.

Known Limitations

- Both ERS and pxGrid are needed.
- Dynamic IP prefix updates and rule changes may take up to 30 seconds to be updated in CloudVision.
- Layer-4 policies are not supported. Policies must be either accept-all or deny-all. ACL rules are limited to only `permit ip` and `deny ip`.
- Hostnames are not supported, i.e., static ISE configuration that is specified using hostnames will not be applied to CloudVision or to the switches and may cause issues to the integration.
- Setting up the ISE collector will clear all existing segmentation configuration in CloudVision.
- ISE SGT Mapping Groups are not supported.
- The MONITOR egress cell option is not supported.
- Only one Matrix configuration is supported.

17.7.2 Certificates for pxGrid integration

The ISE collector uses pxGrid as part of the integration with Cisco ISE. Client certificates are necessary to communicate with pxGrid. The certificates can be generated in the Cisco ISE web interface.

Verifying pxGrid is enabled in ISE:

1. Login as an administrator to the Cisco ISE web interface.
2. Navigate to **Administration** → **Deployment**.
3. Check the box called **pxGrid**.
4. Save changes.

Generating a Certificate

For information and instructions to generate certificates, refer to the official Cisco ISE documentation.

17.7.3 Configuring the ISE Collector

Before the ISE collector can be configured, it must be onboarded and enabled.

Enable Third Party Device Onboarding

1. Navigate to **Settings** (Gear icon on top right) → **General Settings.**
2. Enable **Third Party Device Onboarding**.
3. Enable **Onboard Cisco ISE Devices**.
4. Enable **Inventory Resource API**. This will show the onboarding in the User Interface.

From the Onboarding interface.

1. Navigate to **Device** → **Device Registration**.
2. Select the first tab **Device Onboarding**.
3. Under Onboard Non-EOS and Third Party Devices, select the template **Cisco ISE**.

Onboarding ISE

Complete the form and select **Onboard**.

- Cisco ISE URL (including protocol): https://ise-host.com

  Note: Use the fully qualified hostname. Include the protocol, such as https://.

- Cisco ISE Cert File: Upload the file COMMON_NAME_.cer

- Cisco ISE Key File: Upload the file client.key (decrypted)
- Cisco ISE CA File: Upload chain.cer

  Note: If deployment fails due to errors in validating the certificate, it may be because the Cisco ISE certificates do not specify the Subject Alternative Name option, which is required.
- pxGrid Port: Leave the default value (8910) or provide the port configured in ISE.
- pxGrid User: arista-ise-integration
- ERS Username: user_with_ers_permission
- ERS Password: password_for_user_above

Upon successful onboarding, the collector client will appear in the Cisco ISE user interface.

1. From **Administration** navigate to **pxGrid Services** and select **All Clients**.
2. Find the username in the table.
3. Check the relevant row.
4. Click **Approve** at the top of the table.
5. Allow up to one minute for the collector to notice the approval.
6. Data will start streaming to CloudVision. This may be checked in the telemetry browser in CloudVision:

   Dataset: analytics

   Path: /yang/arista/segmentation/config/domain
7. Devices onboarded to CloudVision with OpenConfig and MSS-G enabled will receive and apply the configurations.

Chapter 18

Using Snapshots to Monitor Devices

CloudVision enables you to monitor changes in the state of the devices in your network over time through the use of snapshots.

Note: Starting from *2018.2.0* release, snapshots UI is available as part of the **Device View** in **Telemetry**.

Sections in this chapter include:

18.1 About Snapshots

In CloudVision, the snapshot service runs as a scheduler to capture device snapshots periodically.

The information recorded in snapshots provides you with insights on the configuration, EOS image, and other aspects of the device. Snapshots are captured for individual devices (single switches) only.

18.2 Standard Information in Snapshots

The information recorded in the snapshot reflects the state of the device at the time snapshot was captured. A snapshot only contains outputs of custom commands that are part of a snapshot template. (You must select a snapshot template when you capture a snapshot.) See Defining Custom Snapshot Templates and Editing Custom Snapshot Templates for information on using snapshot templates.

When upgrading to the *2018.2* train, only snapshot templates are migrated but not previous snapshots. CloudVision stores migrated templates without any device list associated with them. Hence, they are marked as unscheduled. However, these templates can be used to capture snapshots before and after change controls.

18.3 How to Use Snapshots

In CloudVision, snapshot service schedules and periodically captures the outputs of commands that are specified in the template. The frequency of capturing command outputs is based on the scheduling frequency mentioned in the snapshot template. The information recorded in snapshots can provide you with insights on the configuration, EOS image, and other aspects of the device. Snapshots are captured for individual devices (single switches) only.

The main uses of snapshots are:

- Viewing snapshots to understand the state of a device at a given time, or over time.

- Comparing snapshots to see the change in state of a device between two points in time.
- Comparing snapshots to see the state of a device before and after a change control.

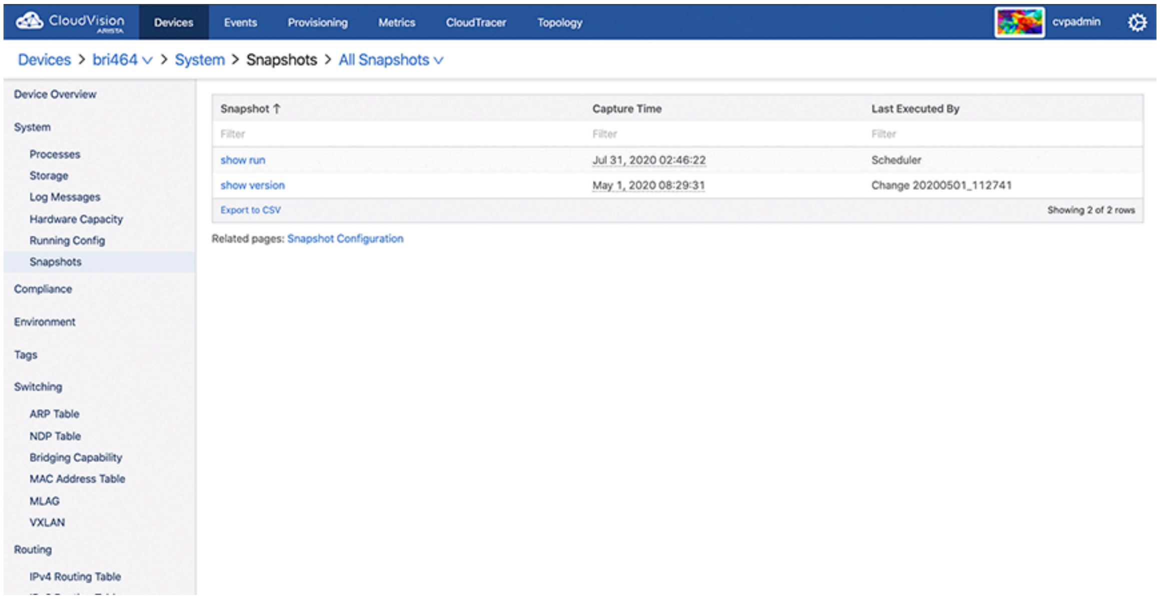
18.4 Accessing Snapshots

Snapshots are stored under the CVP dataset, which you can access any time for detailed analysis. The Snapshots page displays all valid snapshots created over time. Each valid snapshot provides the following additional information:

- **Name** - The name of the template (you assign the name when you create the template).
- **Capture Time** - The date and time when the snapshot was last captured.
- **Last Executed By** - The user that captured the snapshot.

It also allows navigating to snapshots of the corresponding snapshot template.

Figure 18-1: Snapshots Page



Snapshot ↑	Capture Time	Last Executed By
Filter	Filter	Filter
show run	Jul 31, 2020 02:46:22	Scheduler
show version	May 1, 2020 08:29:31	Change 20200501_112741

Export to CSV — Showing 2 of 2 rows

Related pages: Snapshot Configuration

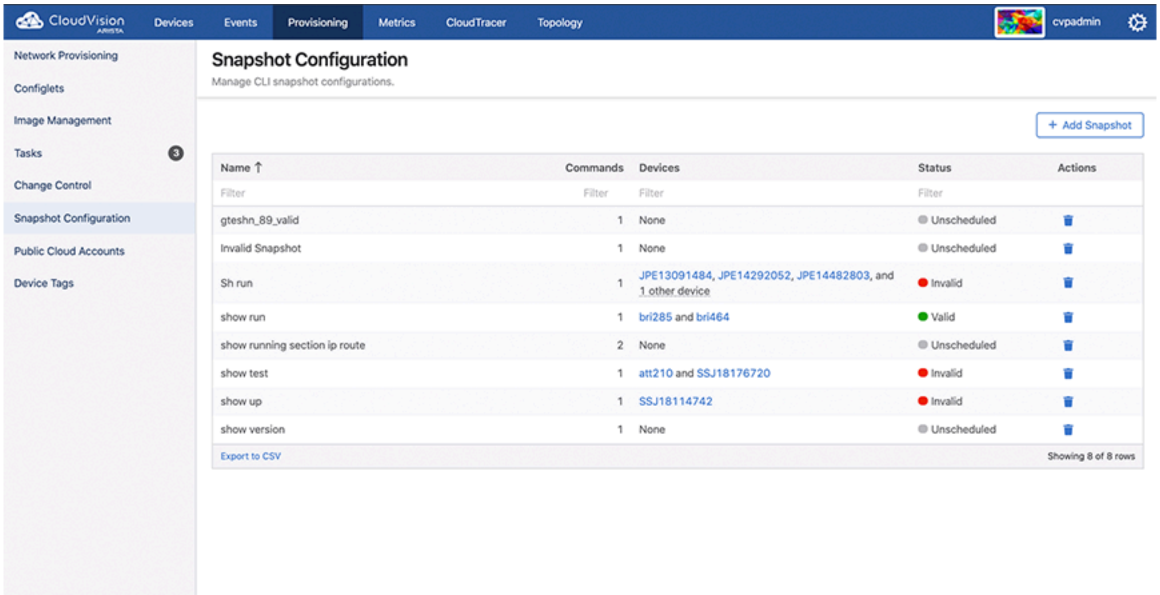
You can navigate to the Snapshots page through one of the following paths:

- **Inventory > Device_ID > Snapshots**
- **Network Provisioning** > Right-click on the required device > **Snapshot**.

18.5 Accessing Snapshot Configurations

The Snapshot Configuration page displays all snapshot templates created over time. It further allows you to edit current snapshot configuration, navigate to the Snapshots page, view the status of each snapshot configuration, and create a new custom snapshot configuration.

Figure 18-2: Snapshot Configuration Page



Snapshot Configuration

Manage CLI snapshot configurations.

Name ↑	Commands	Devices	Status	Actions
Filter	Filter	Filter	Filter	
gteshn_89_valid	1	None	● Unscheduled	🗑
Invalid Snapshot	1	None	● Unscheduled	🗑
Sh run	1	JPE13091484, JPE14292052, JPE14482803, and 1 other device	● Invalid	🗑
show run	1	bri285 and bri464	● Valid	🗑
show running section ip route	2	None	● Unscheduled	🗑
show test	1	att210 and SSJ18176720	● Invalid	🗑
show up	1	SSJ18114742	● Invalid	🗑
show version	1	None	● Unscheduled	🗑

Showing 8 of 8 rows

You can navigate to the Snapshot Configuration page through one of the following paths:

- **Inventory >** ***Device_ID*** **> Snapshots > Snapshot Configuration**
- **Network Provisioning** > Right-click on the required device > **Snapshot** > **Snapshot Configuration**.

18.6 Defining Custom Snapshot Templates

To ensure that snapshots contain the information you need for effectively monitoring changes in the state of devices over a certain period of time, CloudVision allows you to define custom snapshot templates.

A snapshot template defines commands, outputs of which need to be captured as part of the snapshot using that template. When you create a snapshot template, associate a list of devices, and set an execution frequency with it, the snapshot service starts capturing and storing snapshots for that template based on the scheduled frequency.

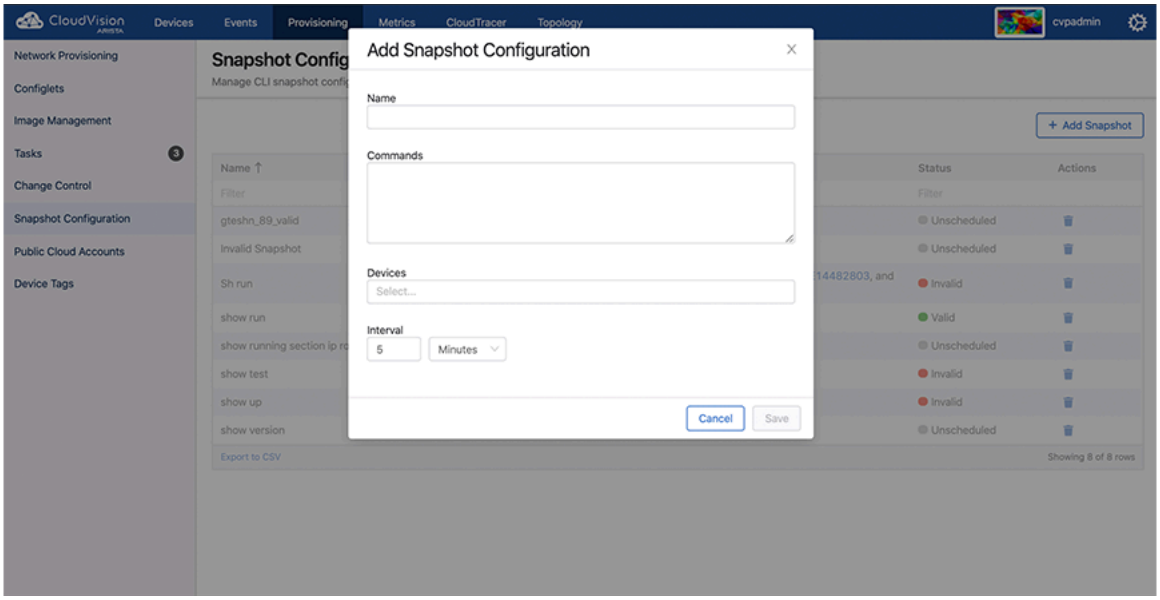
Complete the following steps to define a new custom snapshot template:

1. Navigate to **Inventory >** ***Device_ID*** **> Snapshots > Snapshot Configuration**.

   The Snapshot Configuration page displays currently available snapshot templates.
2. Click the **(or create a new configuration)** hyperlink at the lower right side of the page.

The **Snapshot Configuration** page displays the **Add Snapshot Configuration** section.

Figure 18-3: Add Snapshot Configuration Section



3. In the **Name** field, type the name of the custom snapshot template.
4. In the **Commands** field, enter the EOS CLI commands to be executed by the snapshot.
5. If necessary, click the **Devices** drop-down and select required devices.
6. Under **Interval**, Specify the frequency for capturing snapshots in either minutes, hours, or days.
7. Click **Save**.

   The Snapshot Configuration page immediately displays the latest configuration along with the list of current configurations.

   Note: A snapshot configuration that is created without a device is saved and marked as unscheduled. Snapshot templates with bash commands are marked as invalid. However, these unscheduled and invalid templates can still be selected while creating a Change Control to capture pre and post change control snapshots.

18.7 Editing Custom Snapshot Templates

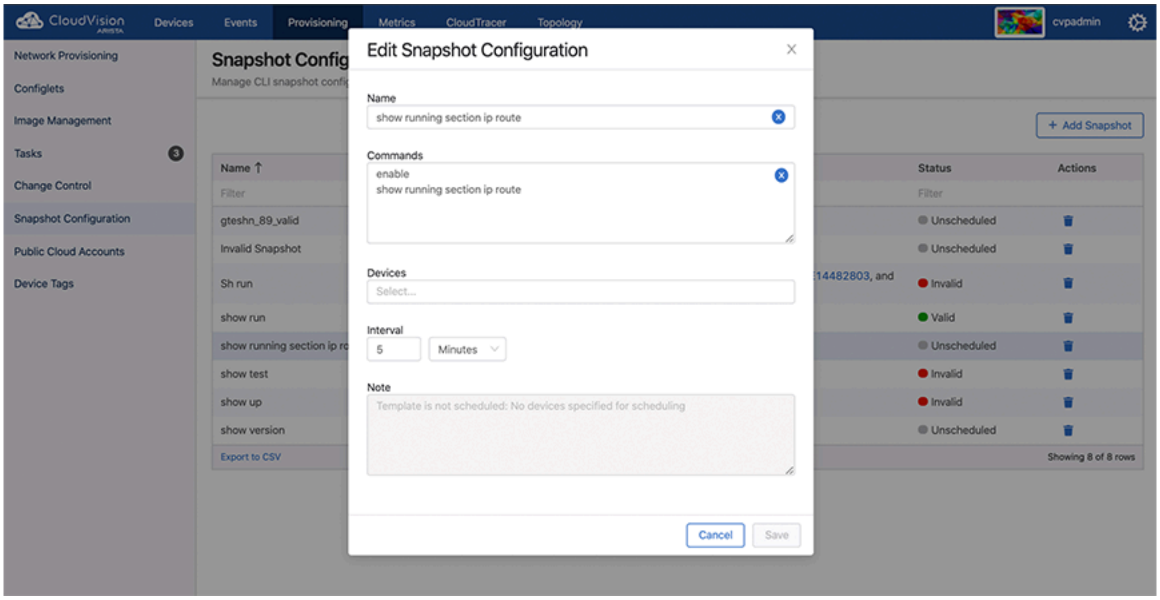
Complete the following steps to go to defined templates:

1. Navigate to **Inventory > *Device_ID* > Snapshots > Snapshot Configuration**.

   The Snapshot Configuration page displays currently available snapshot templates.

2. Click the snapshot name for editing the corresponding snapshot template..

Figure 18-4: Edit Snapshot Configuration Section



Edit Snapshot Configuration

Name: show running section ip route

Commands:

```
enable
show running section ip route
```

Devices: Select...

Interval: 5 Minutes

Note: Template is not scheduled: No devices specified for scheduling

Name ↑	Status	Actions
gteshn_89_valid	Unscheduled	
Invalid Snapshot	Unscheduled	
Sh run	Invalid	
show run	Valid	
show running section ip ro	Unscheduled	
show test	Invalid	
show up	Invalid	
show version	Unscheduled	

3. Modify the required information in corresponding fields.
4. Click **Save**.

18.8 Viewing Snapshots Differences

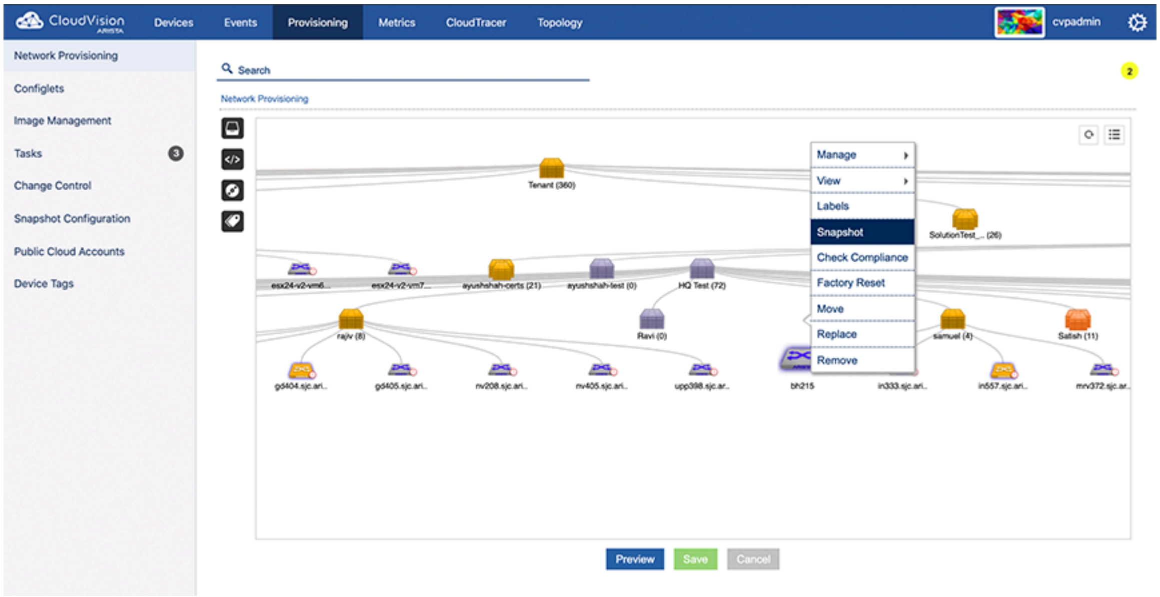
You can take snapshots of single devices only. The exact set of information and presentation of the information in the snapshot is determined by the snapshot template you choose when capturing the snapshot.

Complete the following steps to view snapshots of a device:

1. Go to the **Network Provisioning** page.
2. Locate the device for which you want to view snapshots.

3. Right-click on the device icon, then click **Snapshot**.

Figure 18-5: Initiate Viewing Snapshot



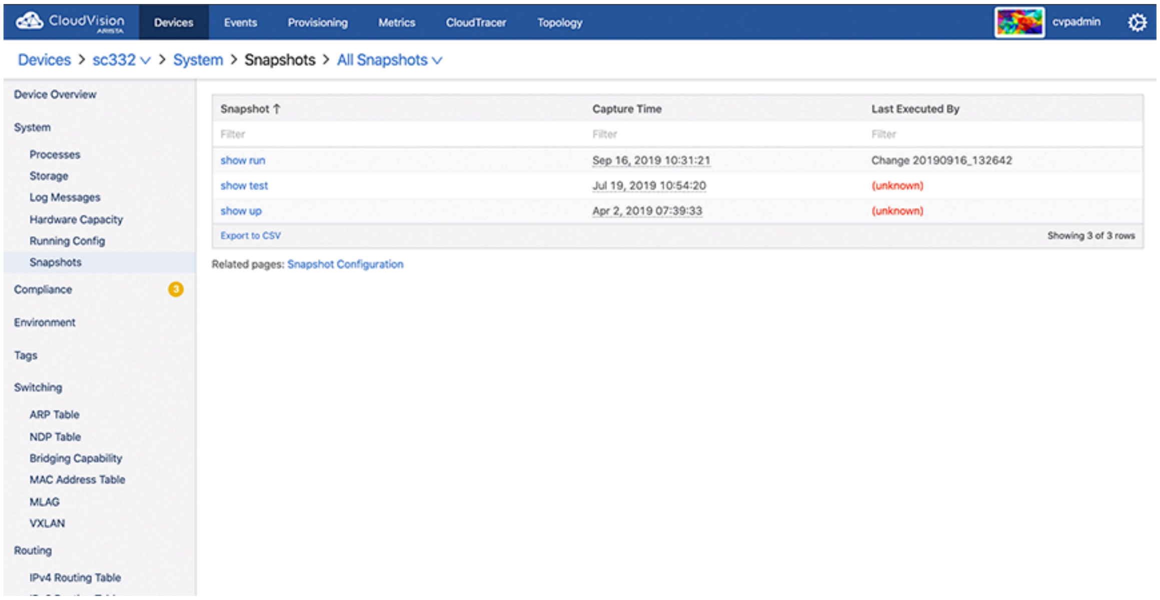
The **All Snapshots** page displays all valid snapshots.

Note:

You can also navigate to the **All Snapshots** page through **Telemetry > Devices > *Device_ID* > Snapshots**.

4. Click on the snapshot template name for viewing the corresponding snapshot.

Figure 18-6: All Snapshots Page



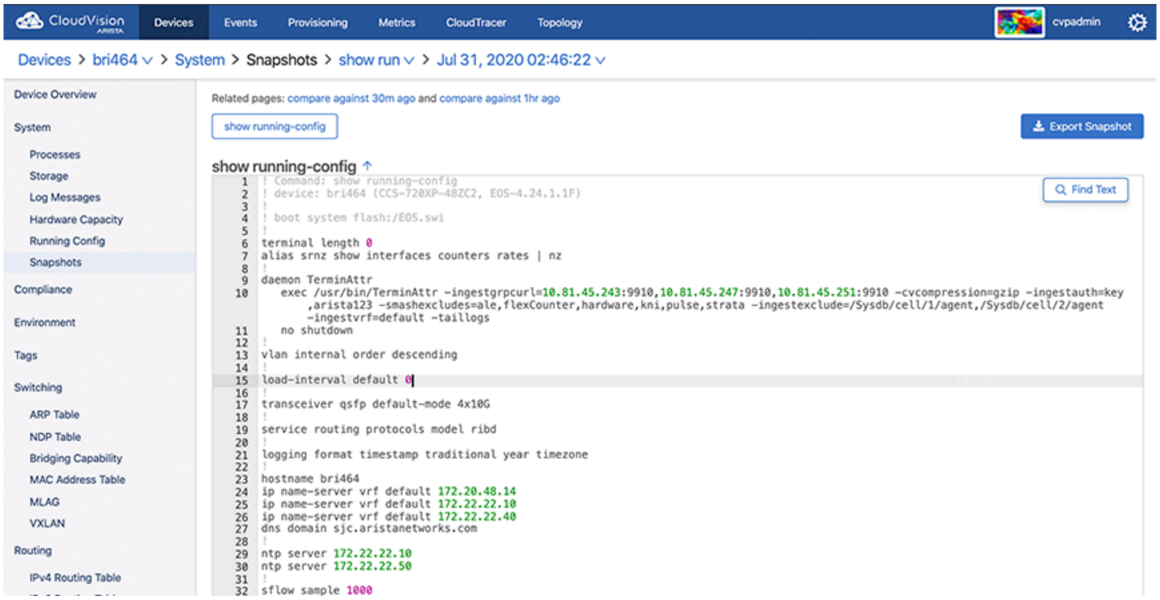
Snapshot ↑	Capture Time	Last Executed By
Filter	Filter	Filter
show run	Sep 16, 2019 10:31:21	Change 20190916_132642
show test	Jul 19, 2019 10:54:20	(unknown)
show up	Apr 2, 2019 07:39:33	(unknown)

Export to CSV   Showing 3 of 3 rows

Related pages: Snapshot Configuration

5. Click the date and time breadcrumb for viewing all snapshots of the corresponding template.

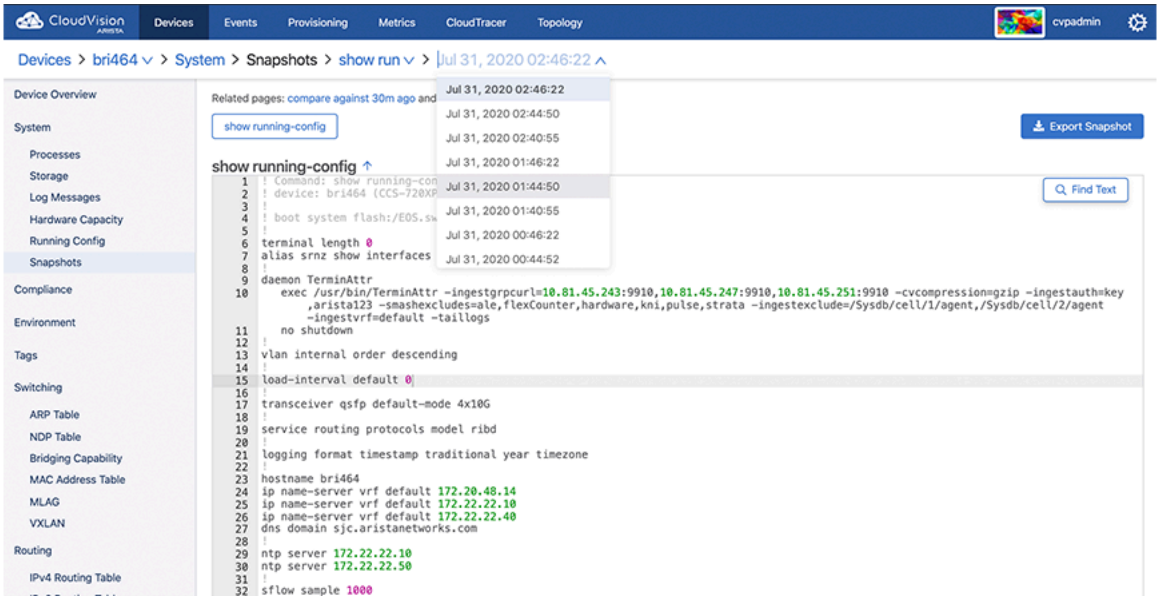
Figure 18-7: View All Snapshots



```
! Command: show running-config
! device: bri464 (CCS-720XP-48ZC2, EOS-4.24.1.1F)
!
! boot system flash:/EOS.swi
!
terminal length 0
alias srnz show interfaces counters rates | nz
!
daemon TerminAttr
   exec /usr/bin/TerminAttr -ingestgrpcurl=10.81.45.243:9910,10.81.45.247:9910,10.81.45.251:9910 -cvcompression=gzip -ingestauth=key
       ,arista123 -smashexcludes=ale,flexCounter,hardware,kni,pulse,strata -ingestexclude=/Sysdb/cell/1/agent,/Sysdb/cell/2/agent
       -ingestvrf=default -taillogs
   no shutdown
!
vlan internal order descending
!
load-interval default 0
!
transceiver qsfp default-mode 4x10G
!
service routing protocols model ribd
!
logging format timestamp traditional year timezone
!
hostname bri464
ip name-server vrf default 172.20.48.14
ip name-server vrf default 172.22.22.10
ip name-server vrf default 172.22.22.40
dns domain sjc.aristanetworks.com
!
ntp server 172.22.22.10
ntp server 172.22.22.50
!
sflow sample 1000
```

6. Click the required snapshot to view the corresponding output.

Figure 18-8: Select Snapshot

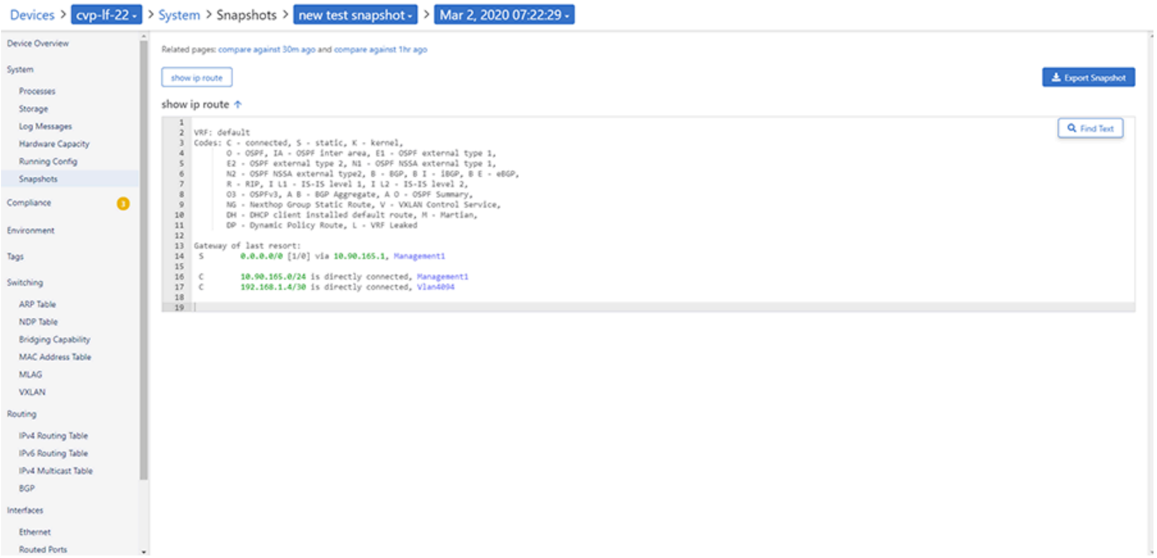


```
! Command: show running-con
! device: bri464 (CCS-720XP
!
! boot system flash:/EOS.sw
!
terminal length 0
alias srnz show interfaces
!
daemon TerminAttr
   exec /usr/bin/TerminAttr -ingestgrpcurl=10.81.45.243:9910,10.81.45.247:9910,10.81.45.251:9910 -cvcompression=gzip -ingestauth=key
       ,arista123 -smashexcludes=ale,flexCounter,hardware,kni,pulse,strata -ingestexclude=/Sysdb/cell/1/agent,/Sysdb/cell/2/agent
       -ingestvrf=default -taillogs
   no shutdown
!
vlan internal order descending
!
load-interval default 0
!
transceiver qsfp default-mode 4x10G
!
service routing protocols model ribd
!
logging format timestamp traditional year timezone
!
hostname bri464
ip name-server vrf default 172.20.48.14
ip name-server vrf default 172.22.22.10
ip name-server vrf default 172.22.22.40
dns domain sjc.aristanetworks.com
!
ntp server 172.22.22.10
ntp server 172.22.22.50
!
sflow sample 1000
```

7. Click Compare against a previous time for viewing corresponding snapshot differences.

8. The page displays corresponding snapshot differences.

Figure 18-9: Compare Snapshots



Related pages: compare against 30m ago and compare against 1hr ago

show ip route

```

VRF: default
Codes: C - connected, S - static, K - kernel,
       O - OSPF, IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type2, B - BGP, B I - iBGP, B E - eBGP,
       R - RIP, I L1 - IS-IS level 1, I L2 - IS-IS level 2,
       O3 - OSPFv3, A B - BGP Aggregate, A O - OSPF Summary,
       NG - Nexthop Group Static Route, V - VXLAN Control Service,
       DH - DHCP client installed default route, M - Martian,
       DP - Dynamic Policy Route, L - VRF Leaked

Gateway of last resort:
 S        0.0.0.0/0 [1/0] via 10.90.165.1, Management1

 C        10.90.165.0/24 is directly connected, Management1
 C        192.168.1.4/30 is directly connected, Vlan4094

```

Note: Snapshot differences are displayed in color codes to quickly identify significant changes in the state of the device over time. Click the Split tab for viewing snapshot differences in different windows.

Chapter 19

Backup & Restore, Upgrades, DNS NTP Server Migration

This document provides details on how to perform backup and restore operations and upgrading CloudVision Portal (CVP).

- Backup and Restore
- Upgrading CloudVision Portal (CVP)
- DNS / NTP Server Migration

19.1 Backup and Restore

CloudVision Portal (CVP) enables you to backup and restore the complete CVP provisioning dataset, including containers, devices, configlets, images, and configlet / image assignments. You can use commands to backup and restore CVP data.

Arista provides a simple script at /cvpi/tools/backup.py which is scheduled by default to run daily to backup CVP data, and retain the last 5 backups in /data/cvpbackup/. Backing up and restoring data saves information about the CVP instance to a tgz file, and then restores the information from the tgz file to a new CVP instance. The CVP commands provide all of the functionality required to complete backup and restore operations.

Note: It is a good practice to regularly create and export backups to ensure that you have an adequate supply of backup files available to you that you can use to restore CVP data.

Note: There is no backup or restore of the Telemetry analytics dataset.

The current CVP release does not support restoring backups taken from previous CVP releases. If you would like to restore a backup from a previous CVP release, install the previous release, restore the backup, and then upgrade to the current release. After you have successfully upgraded to the current release, take another backup so that you can directly restore that into current main release in the future.

For more information, see:

- Requirements for Multi-node Installations
- Using CVPI Commands to Backup and Restore CV-CUE Data
- Using CVPI Commands to Backup and Restore CVP Provisioning Data

19.1.1 Requirements for Multi-node Installations

The basic requirements for backup and restore operations are the same for single-node installations and multi-node installations.

19.1.2 Using CVPI Commands to Backup and Restore CV-CUE Data

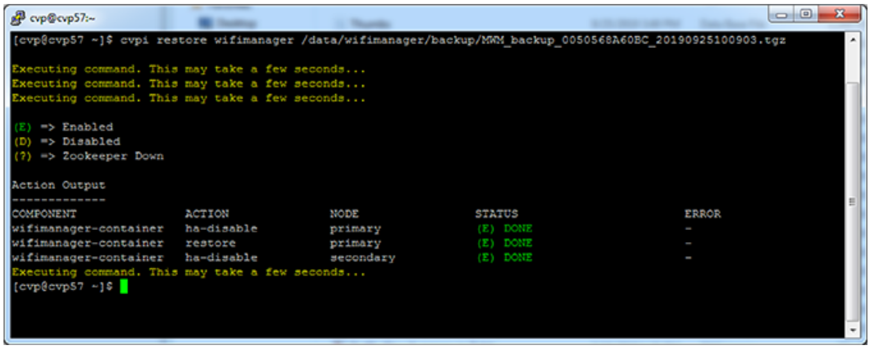
Arista recommends to back up wifimanager regularly and especially before performing any upgrades.

- Restore CV-CUE Data
- RMA

19.1.2.1 Restore CV-CUE Data

You can restore wifimanager from a backup using the `cvpi restore wifimanager </path/to/backup/file>` command.

Figure 19-1: Restore CV-CUE Data



```
[cvp@cvp57 ~]$ cvpi restore wifimanager /data/wifimanager/backup/MWM_backup_0050568A60BC_20190925100903.tgz

Executing command. This may take a few seconds...
Executing command. This may take a few seconds...
Executing command. This may take a few seconds...

(E) => Enabled
(D) => Disabled
(?) => Zookeeper Down

Action Output
-------------
COMPONENT                 ACTION          NODE            STATUS                 ERROR
wifimanager-container     ha-disable      primary         (E)  DONE              -
wifimanager-container     restore         primary         (E)  DONE              -
wifimanager-container     ha-disable      secondary       (E)  DONE              -
Executing command. This may take a few seconds...
[cvp@cvp57 ~]$ 
```

Note: For a CV cluster, you can run this command only on the primary node. If no backup was carried out before the upgrade, you can use a scheduled backup under the `/data/wifimanager/data/data/backup` directory to restore wifimanager.

19.1.2.2 RMA

For RMA or recovery issues, contact support-wifi@arista.com.

Note: Back up wifimanager on any node before submitting it for an RMA. When the node is re-deployed post-RMA, you can restore earlier wifimanager data from a backup that you have stored elsewhere.

19.1.3 Using CVPI Commands to Backup and Restore CVP Provisioning Data

Backup and restore are CVPI functionalities of CVPI components.

Note:

The default directory to save and restore backup data files is `/data/cvpbackup`.

The default directory for backup/restore log files is `/cvpi/logs/cvpbackup`.

The default directory for temporary files during backup/restore is `/data/tmp/cvpbackup`.

The following commands are used to backup and then restore the containers, devices, configlets, images, and configlet or image assignments that are defined in CVP.

Note: When restoring devices, use the username and password that can access the devices being registered.

19.1.3.1 Backup CVP Provisioning Data

Use the `cvpi backup` command for saving a copy of CVP data as backup.

```
cvpi backup cvp
```

Note: To check the progress of the backup, read the latest `backup_cvp.*.log file in /cvpi/logs/cvpbackup`.

This command creates the backup files for the CVP component.

```
[cvp@cvp108 bin]$ cvpi backup cvp
```

19.1.3.2 Restore CVP Provisioning Data

Use the `cvpi restore` command to restore backup files for the CVP component.

```
cvpi restore cvp cvp.timestamp.tgz eosimages.timestamp.tgz
```

The `cvp.<timestamp>.tgz` parameter contains provisioning data from the DataBase (DB) of the CVP application. The `cvp.eosimages.<timestamp>.tgz` parameter contains EOS images and extensions stored in the DataBase (DB) of the CVP application.

Note: To check the progress of the restore, read the latest `restore_cvp.*.log file in /cvpi/logs/cvpbackup`.

This command restores the backup files of the CVP component.

```
[cvp@cvp108 bin]$ cvpi restore cvp cvp.2019.1.0.tgz cvp.eosimages
.2019.1.0.tgz
```

Note:

To check the progress of the backup, tail `-f/cvpi/logs/cvpbackup/backup_cvp.20190606020011.log`.

CVP backup creates two backup files in the /data/cvpbackup directory for restoration. The `eosimages.tgz` is generated only when it differs from the currently available copy of the `eosimages.tgz`, and is an optional parameter for restore if the CVP system already contains the same EOS image.

The `cvpi backup` command can be run anytime and does not disrupt the cvp application. However, the `cvpi restore` command will stop the cvp application and disrupt the service for the duration of the restore. If the restore is from a backup on a different CVP system to a new CVP system, it may also be required to on-board the EOS devices or restart the Terminattr daemons on the EOS devices after the restore.

19.1.3.2.1 Troubleshooting CVP Restore Failure of Provisioning Data

If the cvpbackup directory does not exist in /data when copying the restore files to a newly built VM, you must create it and assign the ownership to the cvp user and group in either of the following two ways:

- Login as cvp user and create the cvpbackup directory

  Use the `su cvp` command to login as cvp user and the `mkdir -p /data/cvpbackup` command to create the cvpbackup directory.
- Create the folder as root and change the ownership

  Use the `mkdir -p /data/cvpbackup` command to create the folder as root and the `chown -R cvp:cvp /data/cvpbackup/` command to change the ownership of cvpbackup directory and its files to cvp user and group.

Verifying the Ownership of cvpbackup Directory

Use one of the following commands to verify the ownership of cvpbackup directory:

- **ls**

  This example verifies the ownership of cvpbackup directory using the `ls` command.

  ```
  [root@cvp-2019 data]# ls -l /data/ | grep cvpbackup
  drwxrwxr-x. 2 cvp cvp 236 Mar 16 02:01 cvpbackup
  ```

- **stat**

  This example verifies the ownership of cvpbackup directory using the `stat` command.

  ```
  [root@cvp-2019 data]# stat /data/cvpbackup/ | grep Access
  Access: (0775/drwxrwxr-x) Uid: (10010/ cvp) Gid: (10010/ cvp)
  ```

Verifying the Ownership of Files Inside the cvpbackup Directory

The following example verifies the ownership of files inside the cvpbackup directory using the `ls` command:

```
[root@cvp-2019 data]# ls -l /data/cvpbackup
total 18863972
-rw-rw-r-- 1 cvp cvp 6650171 Mar 14 02:01 cvp.20200314020004.tgz
-rw-rw-r-- 1 cvp cvp 9642441292 Mar 14 02:08 cvp.eosimages.20200314020002.tgz
```

Correcting the Ownership of cvpbackup Directory Files

Use the chown command to correct the ownership of cvpbackup directory files.

```
chown cvp:cvp cvp.<timestamp>.tgz cvp.eosimages.<timestamp>.tgz
```

The `cvp.<timestamp>.tgz` parameter contains provisioning data from the DataBase (DB) of the CVP application. The `cvp.eosimages.<timestamp>.tgz` parameter contains EOS images and extensions stored in the DataBase (DB) of the CVP application.

This example changes the ownership of all cvpbackup directory files.

```
[root@cvp-2019 data]# chown cvp:cvp cvp.20200319020002.tgz cvp.eosimages
.20200314020002.tgz
```

19.2 Upgrading CloudVision Portal (CVP)

Note: While upgrading CVP, refer to the latest release notes available at Arista Software Download page; and upgrade procedures.

Devices under management must:

- be running supported EOS version
- have supported TerminAttr version installed
- have the TerminAttr agent enabled and successfully streaming telemetry to CVP.

The following steps can be taken at any point on an existing cluster as part of preparing for an upgrade to the current version:

1. Upgrade existing CVP clusters to the latest CVP release
2. Upgrade all EOS devices under management to the supported release train.

3. For devices running EOS releases prior to *4.20*, ensure that the eAPI unix domain socket is enabled with the following configuration:

```
management api http-commands
   protocol unix-socket
```

4. Install supported TerminAttr on all EOS devices under management.
5. Enable state streaming from all EOS devices under management by applying the **SYS_StreamingTelemetry** configlet and pushing the required configuration to all devices.
6. Ensure that all devices are successfully streaming to the CVP cluster.
7. Ensure that all devices are in image and config compliance.
8. Complete regular backups. Complete a final backup prior to upgrade.
9. Ensure that all tasks are in a terminal state (Success, Failed, or Canceled).
10. Ensure that all Change Controls are in a terminal state.

Note: After the cluster is upgraded to the latest CVP release, systems running unsupported TerminAttr versions fail to connect to the CVP cluster. These devices will have to be first upgraded to a supported TerminAttr version by re-onboarding them from the CloudVision UI. You cannot rollback a device to a time before it was running the supported TerminAttr version.

The upgrade from the previous CVP release to the current CVP release trains include data migrations that can take several hours on larger scale systems.

- Upgrades
- CVP Node RMA
- CVP / EOS Dependencies
- Upgrade CV-CUE As Part of a CV Upgrade

19.2.1 Upgrades

Upgrades do not require that the VMs be redeployed, and do not result in the loss of logs. .

The CVP cluster must be functional and running to successfully complete an upgrade. As a precaution against the loss of CVP data, it is recommended that you backup the CVP data before performing an upgrade. To upgrade CVP to the current release, you must first upgrade CVP to the supported release that supports an upgrade to the current release. For more information, refer the CVP release notes at Arista Software Download page.

Note: Centos updates (`yum update` commands) outside of CVP upgrades are not supported.

- Verifying the health of CVP before performing upgrades
- Upgrading from version 2018.1.2 (or later)

19.2.1.1 Verifying the Health of CVP before Performing Upgrades

Upgrades should only be performed on healthy and fully functional CVP systems. Before performing the upgrade, make sure that you verify that the CVP system is healthy.

Complete the following steps to verify the health of CVP.

1. Enter into the Linux shell of the primary node as **cvp user**.
2. Execute the `cvpi status all` command on your CVP:

   This shows the status of all CVP components.
3. Confirm that all CVP components are running.
4. Log into the CVP system to check functionality.

   Once you have verified the health of your CVP installation, you can begin the upgrade process.

   - Upgrading CloudVision Portal (CVP)

19.2.1.2 Upgrading from version 2018.1.2 (or later)

Use this procedure to complete the fast upgrade of CVP to the current version of CVP.

Pre-requisites:

Before you begin the upgrade procedure, make sure that you have:

- Verified the health of your CVP installation (see Verifying the health of CVP before performing upgrades.
- Verified that you are running version 2018.1.2 or later.

Complete the following steps to perform the upgrade.

1. SSH as root into the primary node.
2. Run these commands:
   a. **`rm -rf /tmp/upgrade`** (to remove data from old upgrades if already present)
   b. **`mkdir /data/upgrade`**
   c. **`ln -s /data/upgrade /tmp/upgrade`**
   d. **`scp/wget cvp-upgrade-<version>.tgz`** to the /data/upgrade directory.
3. Run the **`su cvpadmin`** command to trigger the shell.
4. Select the upgrade option from the shell.

   Note: On a multi-node cluster, upgrade can be performed only on the primary node. Upgrading to the current version may take up to 30 minutes.

   Note: If an issue occurs during an upgrade, you will be prompted to continue the upgrade once the issue is resolved.

   Note: Upgrade to 2021.1.0 and newer requires the configuration of a kubernetes cluster network. You will be prompted during the upgrade to enter the private IP range for the kubernetes cluster network. For this reason, a separate, unused network addressing should be provided when configuring CVP.

   Users will see this prompt while running the upgrade:

   ```
   This upgrade requires to configure kubernetes cluster network.
   Please enter private ip range for kubernetes cluster network :
   ```

   The `cvpi env` command will show kubernetes cluster related parameters. KUBE_POD_NETWORK and KUBE_SERVICE_NETWORK are the two subnetworks derived from KUBE_CLUSTER_NETWORK. KUBE_CLUSTER_DNS is the second IP address from KUBE_SERVICE_NETWORK.

   Note: KUBE_CLUSTER_NETWORK is the kubernetes private IP range and this should not conflict with CVP nodes, device interface IPs, cluster interface IPs, or switch IPs. In addition, do not use link-local or the subnet reserved for loopback purposes or any multicast IP addresses. The subnet length for KUBE_CLUSTER_NETWORK needs to be less than or equal to 20.

19.2.2 CVP Node RMA

Use this procedure to replace any node of a multi-node cluster. Replacing nodes of multi-node cluster involves removing the node you want to replace, waiting for the remaining cluster nodes to recover, powering on the replacement node, and applying the cluster configuration to the new node.

When you replace cluster nodes, you must replace only **one node at a time**. If you plan to replace more than one node of a cluster, you must complete the entire procedure for each node to be replaced.

When replacing a node the CloudVision VM that comes with the new CVA might not be the same version as the one running on the other nodes. For more information on redeploying with the correct version refer to: **https://www.arista.com/en/qsg-cva-200cv-250cv/cva-200cv-250cv-redeploy-cvp-vm-tool**

Check that the XML file is similar as on the other appliances. This can be checked using the `virsh dumpxml cvp` command.

Note: It is recommended that you save the CVP cluster configuration to a temporary file, or write down the configuration on a worksheet. The configuration can be found in `/cvpi/cvp-config.yaml`.

1. Power off the node you want to replace (primary, secondary, or tertiary).
2. Remove the node to be replaced.
3. Allow all components of the remaining nodes to recover.

   The remaining nodes need to be up and settled before continuing to step 4.
4. Use the `cvpi status all` command to ensure that remaining nodes are healthy. You will see some services are reported as “NOT RUNNING” due to not all pods for those services being online. This is expected while a node is offline.

```
[root@node2 ~]# cvpi status all

Executing command. This may take some time...
Completed 227/227 discovered actions

secondary       components total:147 running:108 disabled:12 not running:27
tertiary        components total:112 running:103 disabled:9
primary         NODE DOWN


Action Output
-------------

COMPONENT                  ACTION              NODE                STATUS
              ERROR

aaa                        status              secondary           NOT
 RUNNING            Only 2/3 pod(s) ready

ambassador                 status              secondary           NOT
 RUNNING            Only 2/3 pod(s) ready

apiserver                  status              secondary           NOT
 RUNNING            Only 2/3 pod(s) ready

audit                      status              secondary           NOT
 RUNNING            Only 2/3 pod(s) ready

clickhouse                 status              secondary           NOT
 RUNNING            Only 2/3 pod(s) ready

cloudmanager               status              secondary           NOT
 RUNNING            Only 2/3 pod(s) ready

coredns                    status              secondary           NOT
 RUNNING            Only 2/3 pod(s) ready

device-interaction         status              secondary           NOT
 RUNNING            Only 2/3 pod(s) ready

elasticsearch-recorder     status              secondary           NOT
 RUNNING            Only 2/3 pod(s) ready

elasticsearch-server       status              secondary           NOT
 RUNNING            Only 2/3 pod(s) ready

enroll                     status              secondary           NOT
 RUNNING            Only 2/3 pod(s) ready
```

```
flannel                    status              secondary          NOT
 RUNNING            Only 2/3 pod(s) ready

ingest                     status              secondary          NOT
 RUNNING            Only 2/3 pod(s) ready

inventory                  status              secondary          NOT
 RUNNING            Only 2/3 pod(s) ready

kafka                      status              secondary          NOT
 RUNNING            Only 2/3 pod(s) ready

label                      status              secondary          NOT
 RUNNING            Only 2/3 pod(s) ready

local-provider             status              secondary          NOT
 RUNNING            Only 2/3 pod(s) ready

nginx-app                  status              secondary          NOT
 RUNNING            Only 2/3 pod(s) ready

prometheus-node-exporter   status              secondary          NOT
 RUNNING            Only 2/3 pod(s) ready

prometheus-server          status              secondary          NOT
 RUNNING            Only 0/1 pod(s) ready

radius-provider            status              secondary          NOT
 RUNNING            Only 2/3 pod(s) ready

script-executor            status              secondary          NOT
 RUNNING            Only 2/3 pod(s) ready

script-executor-v2         status              secondary          NOT
 RUNNING            Only 2/3 pod(s) ready

service-clover             status              secondary          NOT
 RUNNING            Only 2/3 pod(s) ready

snapshot                   status              secondary          NOT
 RUNNING            Only 2/3 pod(s) ready

tacacs-provider            status              secondary          NOT
 RUNNING            Only 2/3 pod(s) ready

task                       status              secondary          NOT
 RUNNING            Only 2/3 pod(s) ready
```

5. Power on the replacement node.
6. Log in as *cvpadmin*.
7. Enter the cvp cluster configuration.

```
CentOS Linux 7 (Core)
Kernel 3.10.0-957.1.3.el7.x86_64 on an x86_64

localhost login: cvpadmin
Last login: Fri Mar 15 12:24:45 on ttyS0
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
Enter a command
[q]uit [p]rint [s]inglenode [m]ultinode [r]eplace [u]pgrade
```

```
>r
Please enter minimum configuration to connect to the other peers
*Ethernet interface for the cluster network: eth0
*IP address of eth0: 172.31.0.216
*Netmask of eth0: 255.255.0.0
*Default route: 172.31.0.1
*IP address of one of the two active cluster nodes: 172.31.0.161
 Root password of 172.31.0.161:
```

8. Wait for the RMA process to complete. No action is required.

```
Root password of 172.31.0.161:
External interfaces, ['eth1'], are discovered under /etc/sysconfig/network-
scripts
These interfaces are not managed by CVP.
Please ensure that the configurations for these interfaces are correct.
Otherwise, actions from the CVP shell may fail.
Running : /bin/sudo /sbin/service network restart
[  334.001886] vmxnet3 0000:0b:00.0 eth0: intr type 3, mode 0, 9 vectors
 allocated
[  334.004577] vmxnet3 0000:0b:00.0 eth0: NIC Link is Up 10000 Mbps
[  334.006315] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[  334.267535] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
[  348.252323] vmxnet3 0000:13:00.0 eth1: intr type 3, mode 0, 9 vectors
 allocated
[  348.254925] vmxnet3 0000:13:00.0 eth1: NIC Link is Up 10000 Mbps
[  348.256504] IPv6: ADDRCONF(NETDEV_UP): eth1: link is not ready
[  348.258035] IPv6: ADDRCONF(NETDEV_CHANGE): eth1: link becomes ready
Fetching version information
Run cmd: sudo -u cvp -- ssh 172.31.0.156 cat /cvpi/property/version.txt 0.18
Fetching version information
Run cmd: sudo -u cvp -- ssh 172.31.0.216 cat /cvpi/property/version.txt
 10.19
Fetching version information
Run cmd: sudo -u cvp -- ssh 172.31.0.161 cat /cvpi/property/version.txt 0.16
Running : cvpConfig.py tool...
[  392.941983] vmxnet3 0000:0b:00.0 eth0: intr type 3, mode 0, 9 vectors
 allocated
[  392.944739] vmxnet3 0000:0b:00.0 eth0: NIC Link is Up 10000 Mbps
[  392.946388] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[  393.169460] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
[  407.229180] vmxnet3 0000:13:00.0 eth1: intr type 3, mode 0, 9 vectors
 allocated
[  407.232306] vmxnet3 0000:13:00.0 eth1: NIC Link is Up 10000 Mbps
[  407.233940] IPv6: ADDRCONF(NETDEV_UP): eth1: link is not ready
[  407.235728] IPv6: ADDRCONF(NETDEV_CHANGE): eth1: link becomes ready
[  408.447642] Ebtables v2.0 unregistered
[  408.935626] ip_tables: (C) 2000-2006 Netfilter Core Team
[  408.956578] ip6_tables: (C) 2000-2006 Netfilter Core Team
[  408.982927] Ebtables v2.0 registered
[  409.029603] nf_conntrack version 0.5.0 (65536 buckets, 262144 max)
Stopping: ntpd
Running : /bin/sudo /sbin/service ntpd stop
Running : /bin/sudo /bin/systemctl is-active ntpd
Starting: ntpd
Running : /bin/sudo /bin/systemctl start ntpd.service
Waiting for all components to start. This may take few minutes.
Run cmd: su - cvp -c '/cvpi/bin/cvpi -v=3 status zookeeper' 0.45
Run cmd: su - cvp -c '/cvpi/bin/cvpi -v=3 status zookeeper' 0.33
Checking if third party applications exist
Run cmd: su - cvp -c '/cvpi/zookeeper/bin/zkCli.sh ls /apps | tail -1' 0.72
Running : cvpConfig.py tool...
Stopping: cvpi-check
Running : /bin/sudo /sbin/service cvpi-check stop
Running : /bin/sudo /bin/systemctl is-active cvpi-check
Starting: cvpi-check
Running : /bin/sudo /bin/systemctl start cvpi-check.service
```

9. Continue waiting for the RMA process to complete. No action is required.

```
[Fri Mar 15 20:26:28 UTC 2019] :
Executing command. This may take some time...

(E) => Enabled
(D) => Disabled
(?) => Zookeeper Down

Action Output
-------------
COMPONENT           ACTION              NODE                STATUS
    ERROR
hadoop              cluster             tertiary            (E) DONE

hbase               cluster             tertiary            (E) DONE

Executing command. This may take some time...

(E) => Enabled
(D) => Disabled
(?) => Zookeeper Down

Action Output
-------------
COMPONENT           ACTION              NODE                STATUS
    ERROR
aerisdiskmonitor    config              primary             (E) DONE

aerisdiskmonitor    config              secondary           (E) DONE

aerisdiskmonitor    config              tertiary            (E) DONE

apiserver           config              primary             (E) DONE

apiserver           config              secondary           (E) DONE

apiserver           config              tertiary            (E) DONE

cvp-backend         config              primary             (E) DONE

cvp-backend         config              secondary           (E) DONE

cvp-backend         config              tertiary            (E) DONE

cvp-frontend        config              primary             (E) DONE

cvp-frontend        config              secondary           (E) DONE

cvp-frontend        config              tertiary            (E) DONE

geiger              config              primary             (E) DONE

geiger              config              secondary           (E) DONE

geiger              config              tertiary            (E) DONE

hadoop              config              primary             (E) DONE
hadoop              config              secondary           (E) DONE

hadoop              config              tertiary            (E) DONE

hbase               config              primary             (E) DONE

hbase               config              secondary           (E) DONE

hbase               config              tertiary            (E) DONE

kafka               config              primary             (E) DONE

kafka               config              secondary           (E) DONE

kafka               config              tertiary            (E) DONE

zookeeper           config              primary             (E) DONE

zookeeper           config              secondary           (E) DONE

zookeeper           config              tertiary            (E) DONE

Executing command. This may take some time...
secondary       89/89 components running
primary         78/78 components running
Executing command. This may take some time...
COMPONENT           ACTION              NODE                STATUS
    ERROR
Including: /cvpi/tls/certs/cvp.crt
Including: /cvpi/tls/certs/cvp.key
Including: /etc/cvpi/cvpi.key
Including: /cvpi/tls/certs/kube-cert.pem
Including: /data/journalnode/mycluster/current/VERSION
Including: /data/journalnode/mycluster/current/last-writer-epoch
Including: /data/journalnode/mycluster/current/last-promised-epoch
Including: /data/journalnode/mycluster/current/paxos
Including: /cvpi/tls/certs/ca.crt
Including: /cvpi/tls/certs/ca.key
Including: /cvpi/tls/certs/server.crt
Including: /cvpi/tls/certs/server.key
mkdir -p /cvpi/tls/certs
mkdir -p /data/journalnode/mycluster/current
mkdir -p /cvpi/tls/certs
mkdir -p /etc/cvpi
mkdir -p /cvpi/tls/certs
mkdir -p /cvpi/tls/certs
mkdir -p /cvpi/tls/certs
mkdir -p /data/journalnode/mycluster/current
mkdir -p /cvpi/tls/certs
mkdir -p /data/journalnode/mycluster/current
mkdir -p /data/journalnode/mycluster/current
mkdir -p /cvpi/tls/certs
Copying: /etc/cvpi/cvpi.key from secondary
rsync -rtvp 172.31.0.161:/etc/cvpi/cvpi.key /etc/cvpi
Copying: /cvpi/tls/certs/cvp.crt from secondary
rsync -rtvp 172.31.0.161:/cvpi/tls/certs/cvp.crt /cvpi/tls/certs
Copying: /cvpi/tls/certs/server.key from secondary
rsync -rtvp 172.31.0.161:/cvpi/tls/certs/server.key /cvpi/tls/certs
Copying: /cvpi/tls/certs/ca.crt from secondary
rsync -rtvp 172.31.0.161:/cvpi/tls/certs/ca.crt /cvpi/tls/certs
Copying: /cvpi/tls/certs/cvp.key from secondary
rsync -rtvp 172.31.0.161:/cvpi/tls/certs/cvp.key /cvpi/tls/certs
Copying: /cvpi/tls/certs/ca.key from secondary
rsync -rtvp 172.31.0.161:/cvpi/tls/certs/ca.key /cvpi/tls/certs
```

```
Copying: /data/journalnode/mycluster/current/last-writer-epoch from
 secondary
rsync -rtvp 172.31.0.161:/data/journalnode/mycluster/current/last-writer-
epoch /data/journalnode/mycluster/current
Copying: /cvpi/tls/certs/kube-cert.pem from secondary
Copying: /cvpi/tls/certs/server.crt from secondary
rsync -rtvp 172.31.0.161:/cvpi/tls/certs/server.crt /cvpi/tls/certs
Copying: /data/journalnode/mycluster/current/VERSION from secondary
rsync -rtvp 172.31.0.161:/data/journalnode/mycluster/current/VERSION /data/
journalnode/mycluster/current
Copying: /data/journalnode/mycluster/current/paxos from secondary
rsync -rtvp 172.31.0.161:/data/journalnode/mycluster/current/paxos /data/
journalnode/mycluster/current
Copying: /data/journalnode/mycluster/current/last-promised-epoch from
 secondary
rsync -rtvp 172.31.0.161:/data/journalnode/mycluster/current/last-promised-
epoch /data/journalnode/mycluster/current
rsync -rtvp 172.31.0.161:/cvpi/tls/certs/kube-cert.pem /cvpi/tls/certs
Starting: cvpi-config
Running : /bin/sudo /bin/systemctl start cvpi-config.service
Starting: cvpi
Running : /bin/sudo /bin/systemctl start cvpi.service
Running : /bin/sudo /bin/systemctl start cvpi-watchdog.timer
Running : /bin/sudo /bin/systemctl enable docker
Running : /bin/sudo /bin/systemctl start docker
Running : /bin/sudo /bin/systemctl enable kube-cluster.path
```

10. Enter "q" to quit the process after the **RMA process is complete!** message is displayed.

```
Waiting for all components to start. This may take few minutes.
[  560.918749] FS-Cache: Loaded
[  560.978183] FS-Cache: Netfs 'nfs' registered for caching
Run cmd: su - cvp -c '/cvpi/bin/cvpi status all --cluster' 48.20
Run cmd: su - cvp -c '/cvpi/bin/cvpi status all --cluster' 2.73
Run cmd: su - cvp -c '/cvpi/bin/cvpi status all --cluster' 7.77
Run cmd: su - cvp -c '/cvpi/bin/cvpi status all --cluster' 2.55
Run cmd: su - cvp -c '/cvpi/bin/cvpi status all --cluster' 2.23
Run cmd: su - cvp -c '/cvpi/bin/cvpi status all --cluster' 2.64
Run cmd: su - cvp -c '/cvpi/bin/cvpi status all --cluster' 2.59
Run cmd: su - cvp -c '/cvpi/bin/cvpi status all --cluster' 2.07
Run cmd: su - cvp -c '/cvpi/bin/cvpi status all --cluster' 2.70
Run cmd: su - cvp -c '/cvpi/bin/cvpi status all --cluster' 2.51
Run cmd: su - cvp -c '/cvpi/bin/cvpi status all --cluster' 2.57
Run cmd: su - cvp -c '/cvpi/bin/cvpi status all --cluster' 2.40
Run cmd: su - cvp -c '/cvpi/bin/cvpi status all --cluster' 2.24
Waiting for all components to start. This may take few minutes.
Run cmd: su - cvp -c '/cvpi/bin/cvpi -v=3 status all' 9.68
RMA process is complete!
[q]uit [p]rint [e]dit [v]erify [s]ave [a]pply [h]elp ve[r]bose
>q
```

11. Use the `cvpi status all` command to ensure that the cluster is healthy.

```
[cvp@cvp87 ~]$ cvpi status all


Executing command. This may take some time...
Completed 215/215 discovered actions
primary  components total:112 running:104 disabled:8
secondary  components total:122 running:114 disabled:8
tertiary  components total:97 running:91 disabled:6
```

When a node is RMA'd, the other nodes will replicate their state via HDFS to the new node. We can track this in real time by issuing the following command:

```
watch -n 30 "hdfs dfsadmin -report | grep 'Under replicated'"
```

Once the count of "Under replicated" blocks hits 0, data synchronization to the new node is complete.

The disk usage on the new node will also grow as the blocks are replicated and the RMA'd node will have a similar disk space utilization as the other nodes once the operation has finished successfully.

19.2.3 CVP / EOS Dependencies

To ensure that CVP can provide a base level of management, all EOS devices must be running at least EOS versions *4.17.3F* or later. To ensure device compatibility supported EOS version advice should be sought from the Arista account team.

CVP should not require any additional EOS upgrades to support the standard features and functions in later versions of the appliance. Newer features and enhancements to CVP may not be available for devices on older code versions.

Refer to the latest Release Notes for additional upgrade/downgrade guidance.

Related topics:

- Upgrades
- CVP Node RMA

19.2.4 Upgrade CV-CUE As Part of a CV Upgrade

In case of a CV upgrade, services go through the following steps:

1. Services or service containers (such as CV-CUE) are stopped.
2. Existing container images are deleted.
3. New component RPMs are installed.
4. The server is rebooted and all services are started again.

   A service on CV is upgraded only if its version is different from the pre-upgrade version (CV stores its pre-upgrade state to decide this). The wifimanager component follows a similar process. When CV boots up after an upgrade, wifimanager starts and upgrades only if the CV upgrade has resulted in a new wifimanager version. The following actions precede every wifimanager **start** operation:

   a. `load`: Loads the wifimanager container image into docker when CV boots up for the first time after an upgrade.
   b. `init`: Initializes wifimanager before the start. The wifimanager `init` is versioned *init-8.8.0-01*, for example. The `init-<version>` handler initiates a wifimanager upgrade if needed. Thus, if the wifimanager version has not changed after the CV upgrade, the wifimanager upgrade is not invoked. If the wifimanager version has changed, then a wifimanager upgrade is called before its start.

   Note: Load and init are internal actions to the wifimanager start operation; they are not run separately. The CV-CUE service might take longer to start than other CV services.

19.3 DNS / NTP Server Migration

You can migrate your DNS / NTP server after you have completed your initial deployment of CloudVision. Migrating the DNS / NTP server is typically done if you want to or need to change the DNS / NTP server that CloudVision currently uses.

For example, if the current CloudVision DNS / NTP server was intentionally isolated during the initial CloudVision installation, you need to migrate the server to make it accessible by external resources.

Note: Following the DNS / NTP Server Migration procedure may cause the CVP server to be unavailable for some time after using the commands.

19.3.1 How to Modify the DNS and NTP Configuration

The process for modifying the DNS / NTP server after the completion of the initial CloudVision installation involves updating the DNS and NTP server entries on each cluster node and modifying the `/cvpi/cvp-config.yaml` file (on each node) to reflect the updates to the server entries.

Pre-requisites

Before you begin the migration process, make sure that:

- The IP addresses and hostnames (fqdn) of the nodes must not change.
- For each node, make sure that:
  - At least one DNS server entry is present in the /cvpi/cvp-config.yaml file.
  - The DNS server that corresponds to the DNS server entry in the `/cvpi/cvp-config.yaml` file can be accessed by the cluster throughout the migration process. (The reason for this is that any changes made to resolv.conf take effect immediately upon saving the file.)
- The time difference between the old NTP server and new NTP server should be negligible.
- The old NTP server and new NTP server should be in same time zone.

Note: Following the DNS / NTP Server Migration procedure may cause the CVP server to be unavailable for some time after using the commands.

Complete these steps to modify the DNS / NTP server.

1. On each node, edit the `/cvpi/cvp-config.yaml` file to reflect the changes to the DNS and NTP server entries that need to be made,
2. To read the `/cvpi/cvp-config.yaml` file and restart the network service, run the `/cvpi/tools/cvpConfig.py -y /cvpi/cvp-config.yaml -n node`*`X`* command on each node where *X* is the respective node number.
3. Restart the CVP components for all kubernetes pods to re-mount the `/etc/resolv.conf` file: `cvpi -v=3 stop all && cvpi -v=3 start all`

   Related topics:

   - Backup and Restore

Chapter 20

Supplementary Services

This document provides configurations steps and examples for supplementary setup procedures for CloudVision Portal (CVP).

- HTTPS Certificates Setup
- Customizing TLS and SSH Ciphers
- DHCP Service for Zero Touch Provisioning (ZTP) Setup
- RADIUS or TACACS Authentication Setup
- Background Tasks
- Resetting cvpadmin Password System Recovery
- Optional SAN IP field in CVP Certificate
- Rotating Internal Certificate Authority

20.1 HTTPS Certificates Setup

CVP uses nginx to front and terminate all HTTPS connections. To support HTTPS, the server must be configured with a certificate. A self-signed certificate is generated at first bootup.

The guidelines to import a certificate are:

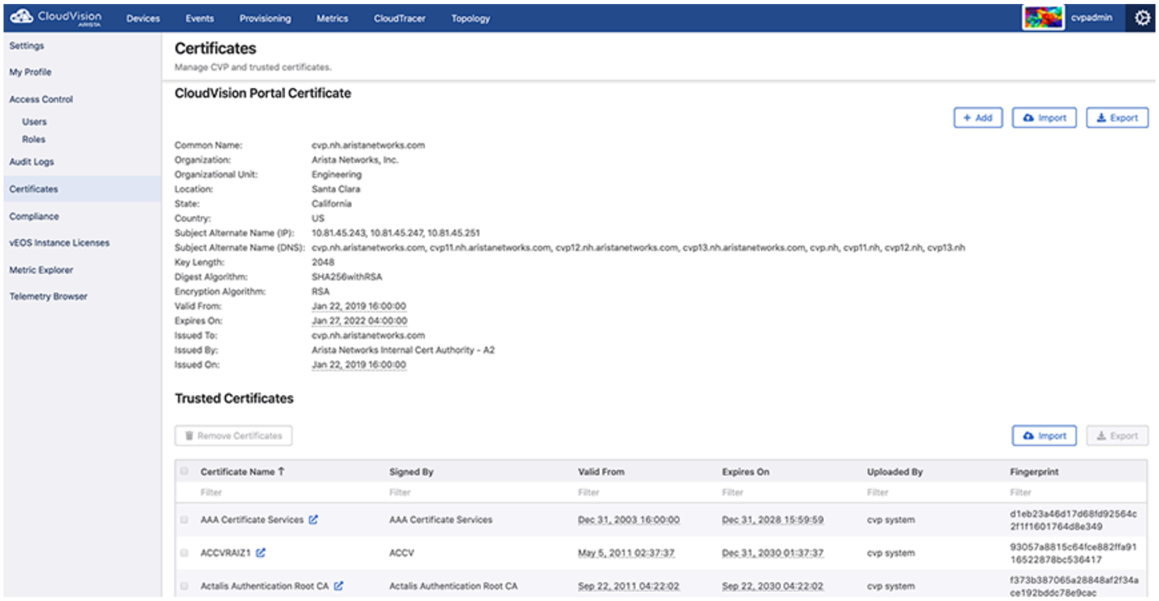
- Correctly fill the Subject Alternate Name (SAN) IP and DNS fields in both signed and self-signed certificates:
    - The SAN IP field must contain the IP addresses of all CVP cluster nodes; and the IP address of any IP load balancer used in front of CVP.
    - The SAN DNS field must contain the Fully Qualified Domain Name (FQDN) of the following elements:
        - All CVP cluster nodes
        - Any Canonical Names (CNAMES) and round-robin DNS names
        - Any IP load balancer used in front of CVP

    Note: Zerotouch Provisioning (ZTP) and REST API calls can fail if signed certificates are uploaded without appropriate data in SAN fields.
- When importing a CVP certificate signed by an internal Certificate Authority (CA), the uploaded file must sequentially contain the full trust chain of PEM-encoded certificates like a server certificate, all intermediate certificates (if available), and a root certificate.
- Leave an empty line between every two certificates when importing multiple certificates into a single file.

    Note: Do not leave an empty line at the end of the file.
- If the server certificate is self-signed then the server and root certificates are one-and-the-same, so only that single certificate is required.
- CVP does not support wildcard certificates.

To install an HTTPS certificate, navigate to the Settings page (Click on the gear icon) > **Certificates** (See the figure below).

Figure 20-1: Certificates Page



Certificates

Manage CVP and trusted certificates.

CloudVision Portal Certificate

Common Name: cvp.nh.aristanetworks.com
Organization: Arista Networks, Inc.
Organizational Unit: Engineering
Location: Santa Clara
State: California
Country: US
Subject Alternate Name (IP): 10.81.45.243, 10.81.45.247, 10.81.45.251
Subject Alternate Name (DNS): cvp.nh.aristanetworks.com, cvp11.nh.aristanetworks.com, cvp12.nh.aristanetworks.com, cvp13.nh.aristanetworks.com, cvp.nh, cvp11.nh, cvp12.nh, cvp13.nh
Key Length: 2048
Digest Algorithm: SHA256withRSA
Encryption Algorithm: RSA
Valid From: Jan 22, 2019 16:00:00
Expires On: Jan 27, 2022 04:00:00
Issued To: cvp.nh.aristanetworks.com
Issued By: Arista Networks Internal Cert Authority - A2
Issued On: Jan 22, 2019 16:00:00

Trusted Certificates

□	Certificate Name ↑	Signed By	Valid From	Expires On	Uploaded By	Fingerprint
	Filter	Filter	Filter	Filter	Filter	Filter
□	AAA Certificate Services	AAA Certificate Services	Dec 31, 2003 16:00:00	Dec 31, 2028 15:59:59	cvp system	d1eb23a46d17d68fd92564c 2f1f1601764d8e349
□	ACCVRAIZ1	ACCV	May 5, 2011 02:37:37	Dec 31, 2030 01:37:37	cvp system	93057a8815c64fce882ffa91 16522878bc536417
□	Actalis Authentication Root CA	Actalis Authentication Root CA	Sep 22, 2011 04:22:02	Sep 22, 2030 04:22:02	cvp system	f373b387065a28848af2f34a ce192bddc78e9cac

Install the certificate using one of the following methods:

- Generating and Installing Self-Signed Certificate
- Installing Public Certificate
- Creating a CSR

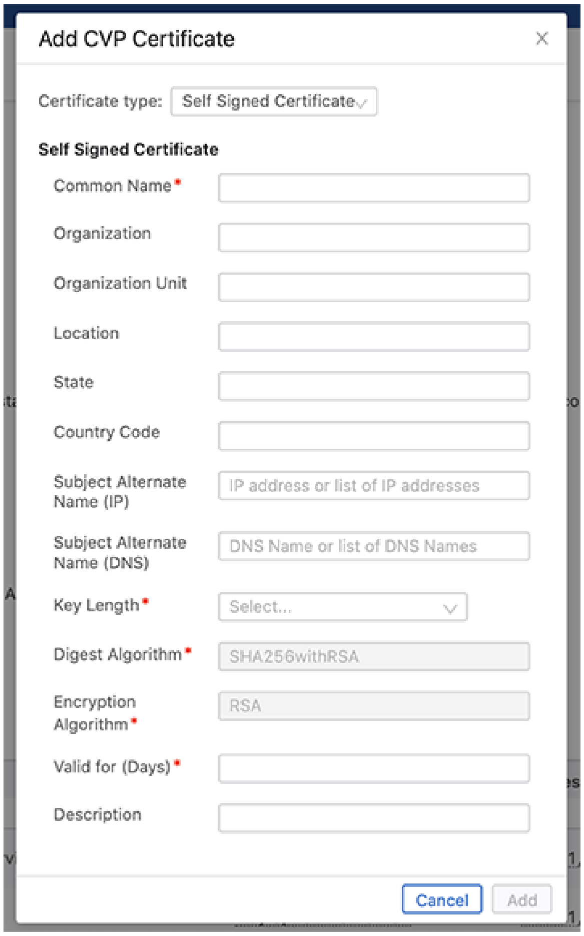
20.1.1 Generating and Installing Self-Signed Certificate

Perform the following steps to generate and install a self-signed certificate:

1. On the Certificates page, click **+ Add**.

CVP opens the **Add CVP Certificate** pop-up window. See the figure below.

Figure 20-2: Add CVP Certificate Pop-Up Window



Add CVP Certificate

Certificate type: Self Signed Certificate

Self Signed Certificate

Common Name*

Organization

Organization Unit

Location

State

Country Code

Subject Alternate Name (IP): IP address or list of IP addresses

Subject Alternate Name (DNS): DNS Name or list of DNS Names

Key Length*: Select...

Digest Algorithm*: SHA256withRSA

Encryption Algorithm*: RSA

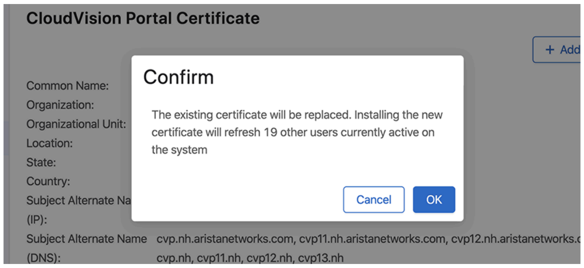
Valid for (Days)*

Description

2. Select **Self Signed Certificate** from the **Certificate Type** drop-down menu.
3. Provide the required information.
4. Click **Add**.

   CVP opens the **Confirm** pop-up window informing that the existing certificate will be replaced. See the figure below.

Figure 20-3: Confirm Pop-Up Window



CloudVision Portal Certificate

Common Name:
Organization:
Organizational Unit:
Location:
State:
Country:
Subject Alternate Na
(IP):
Subject Alternate Name (DNS): cvp.nh.aristanetworks.com, cvp11.nh.aristanetworks.com, cvp12.nh.aristanetworks.c
cvp.nh, cvp11.nh, cvp12.nh, cvp13.nh

Confirm

The existing certificate will be replaced. Installing the new certificate will refresh 19 other users currently active on the system

5. Click **OK**.

   CVP replaces the certificate and restarts the nginx service.

Note: When CVP is restarted, add an exception in the browser for the new certificate.

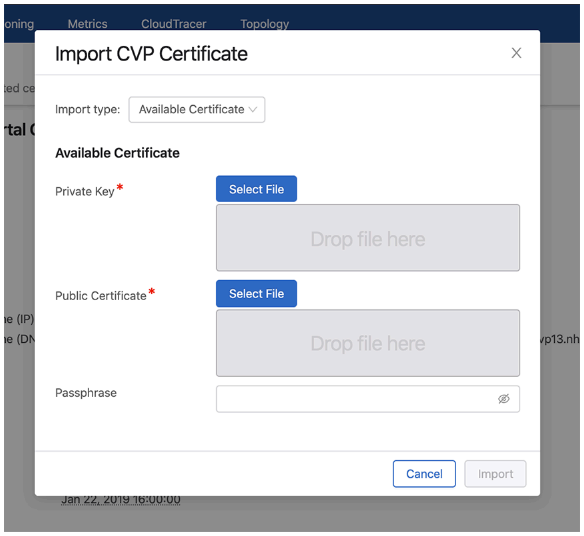
20.1.2 Installing Public Certificate

Perform the following steps to install a public certificate:

1. On the Certificates page, click **Import**.

   CVP opens the **Import CVP Certificate** pop-up window. See the figure below.

   Figure 20-4: Import CVP Certificate Pop-Up Window



Import CVP Certificate

Import type: Available Certificate

2. Select **Available Certificate** from the **Import type** drop-down menu.
3. Upload private key and public certificate.
4. (Optional) Provide passphrase.
5. Click **Import**.

   CVP replaces the certificate and restarts the nginx service.

   Note: When CVP is restarted, add an exception in the browser for the new certificate.

20.1.3 Creating a CSR

A server Certificate Signing Request (CSR) file can be created by either your internal CA (along with an associated server key) or via CVP.

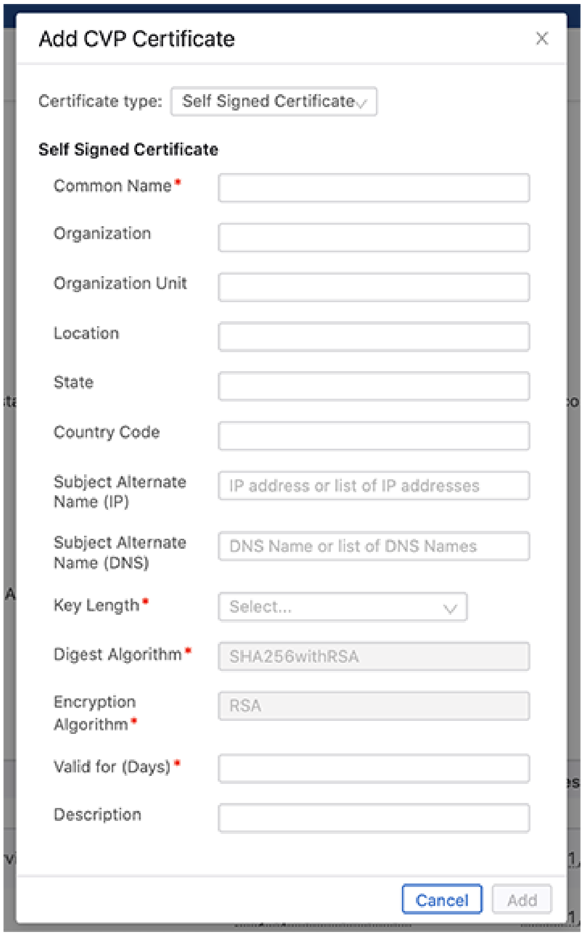
Perform the following steps to create a CSR:

1. On the Certificates page, click **+ Add**.

   CVP opens the **Add CVP Certificate** pop-up window.
2. Select **Certificate Signing Request** from the **Certificate Type** drop-down menu.

See the figure below.

Figure 20-5: Add CVP Certificate Dialogbox for CSR



Add CVP Certificate

Certificate type: Self Signed Certificate

Self Signed Certificate

Common Name*

Organization

Organization Unit

Location

State

Country Code

Subject Alternate Name (IP): IP address or list of IP addresses

Subject Alternate Name (DNS): DNS Name or list of DNS Names

Key Length*: Select...

Digest Algorithm*: SHA256withRSA

Encryption Algorithm*: RSA

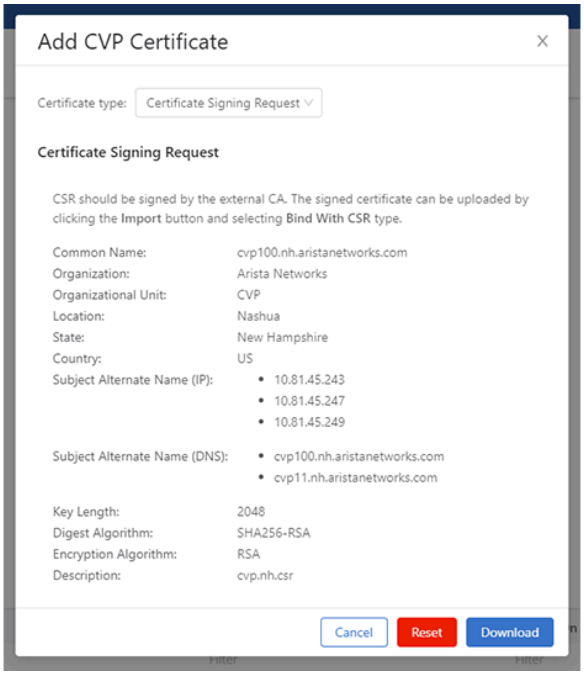
Valid for (Days)*

Description

3. Provide the required information in all fields.
4. Click **Add**.

CVP opens the **Add CVP Certificate** dialog box displaying the complete CSR information. See the figure below.

Figure 20-6: Add CVP Certificate Dialogbox with CSR Details



Certificate type: Certificate Signing Request

Certificate Signing Request

CSR should be signed by the external CA. The signed certificate can be uploaded by clicking the **Import** button and selecting **Bind With CSR** type.

Common Name: cvp100.nh.aristanetworks.com
Organization: Arista Networks
Organizational Unit: CVP
Location: Nashua
State: New Hampshire
Country: US
Subject Alternate Name (IP):
- 10.81.45.243
- 10.81.45.247
- 10.81.45.249

Subject Alternate Name (DNS):
- cvp100.nh.aristanetworks.com
- cvp11.nh.aristanetworks.com

Key Length: 2048
Digest Algorithm: SHA256-RSA
Encryption Algorithm: RSA
Description: cvp.nh.csr

5. Click **Download** to download the CSR file.

   Note: The CA provides the root key (For example, `myCA.key`) and and root certificate (For example, `myCA.pem`).

6. Create a configuration file to define the SAN fields.

   Example:

```
bash-4.2# cat cvp100.nh.aristanetworks.com.ext
authorityKeyIdentifier=keyid,issuer
basicConstraints=CA:FALSE
keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherm
ent
subjectAltName = @alt_names

[alt_names]
DNS.1 = cvp100.nh.aristanetworks.com
DNS.2 = cvp100.nh
DNS.3 = cvp11.nh.aristanetworks.com
DNS.4 = cvp11.nh
DNS.5 = cvp12.nh.aristanetworks.com
DNS.6 = cvp12.nh
DNS.7 = cvp13.nh.aristanetworks.com
DNS.8 = cvp13.nh
IP.1 = 10.81.45.243
IP.2 = 10.81.45.247
IP.3 = 10.81.45.251
```

7. Run the following command to generate a signed certificate from the downloaded CSR file.

```
openssl x509 -req -in downloaded_file -CA root_certificate -CAkey root_key -
CAcreateserial
```

```
-out updated_certificate_filename -days validity_period_in_days -sha256 -
extfile SAN_DNS_IP_ext_filename
```

Example:

```
openssl x509 -req -in CSR.csr -CA myCA.pem -CAkey myCA.key -CAcreateseri
al -out cvp100.nh.aristanetworks.com.gui2.crt -days 365 -sha256 -extfile
 cvp100.nh.aristanetworks.com.ext
```

8. Edit the new certificate file to add the root certificate at the end of the file.

Example:

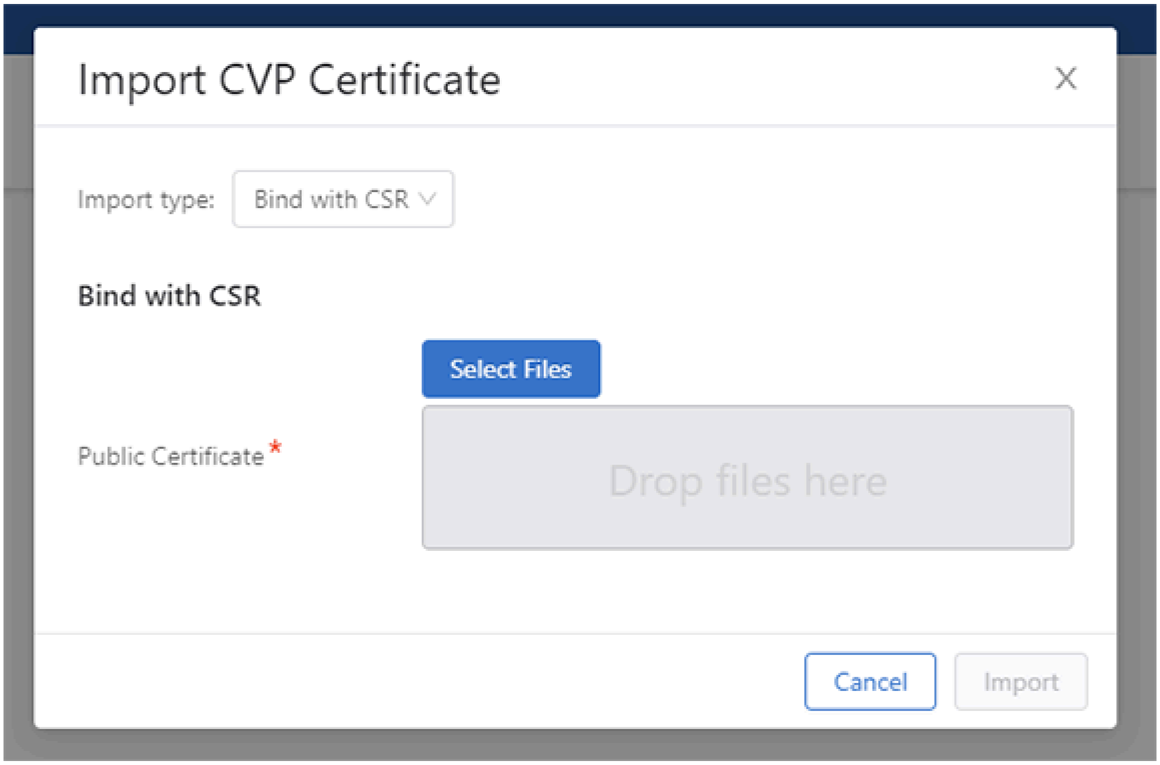
```
bash-4.2# cat cvp100.nh.aristanetworks.com.gui2.crt
-----BEGIN CERTIFICATE-----
MIIEqz2N2cDEzLm5oLmFyaXN0YW5ldHdvcmtzLmNvbYIIY3ZwMTMubmiHBApRLfOH
[snip]
Ta7HF9MPgnc5XOlVN2PRWkEuPN1JFEuj7xute41NuTBmnqoAeuhdTbVpxuBEeoY=
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
MIID6zCCAtOgAwIBAgIJANW5kelAXMzhMA0GCSqGSIb3DQEBCwUAMIGLMQswCQYD
[snip]
2QoyIITDLQor1I/2z+RDHWCx8wEiYrsYkyzZDm/7NeGqfygXjnVJwfJBjtjpB8Y=
-----END CERTIFICATE-----
bash-4.2#
```

Note: In case of intermediate certificates, add them between the new certificate and the root certificate.

9. In the CVP, click on the gear icon > **Certificates**.
10. Click **Import**.

CVP opens the **Import CVP Certificate** dialog box.

Figure 20-7: Import CVP Certificate to Bind with CSR



Import CVP Certificate

Import type: Bind with CSR

Bind with CSR

Public Certificate *

11. Select **Bind with CSR** in the **Import type** dropdown menu.
12. In the **Public Certificate** section, click **Select files**.
13. Navigate and select the edited crt file.
14. Click **Import**.

20.1.4 Renewing the Certificate Authority

Note: The device communication will be disrupted when these steps are executed.

The Certificate Authority (CA) in the on-premise CVP can be renewed with the following steps:

1. SSH into the primary.
2. Reset the Certificate Authority (CA) and stop apiserver and ingest with the following commands.

```
yes | cvpi reset ca-init-v1
cvpi stop ingest
cvpi stop apiserver
```

3. Renew CA and aeris admin certificates with the following commands.

```
cvpi init ca-init-v1
/cvpi/apps/aeris/bin/create-admin-cert.sh
```

4. Restart all stopped components.

```
cvpi start all
```

5. Re-onboard all devices from the Device Onboarding page.

20.2 Customizing TLS and SSH Ciphers

CVP uses nginx to front and terminate all HTTPS connections. To support HTTPS, the server must be configured with a certificate. A selfsigned certificate is generated at first bootup.

- Configuring Custom TLS Ciphers
- Configuring Custom SSH Ciphers
- Strong KEX Algorithm

20.2.1 Configuring Custom TLS Ciphers

Complete these steps to configure custom TLS ciphers.

Nginx, the web server software, uses TLS ciphersuites that are considered safe to use, but may not meet the security standards of certain organizations. It is possible to change the settings used by adding or changing **ssl_ciphers** in **/etc/nginx/conf.d/cvpi-server.conf** (pre 2021.2.0) or **/etc/nginx/conf.d/servers/cvpi-server.conf** (post 2021.2.0) under the server block.

1. Using the appropriate path for your version of CloudVision, create a file that contains all of the SSL ciphers you need. Any open SSL cipher string can be used.
   - **/etc/nginx/conf.d/cvpi-server.conf** (pre 2021.2.0)
   - **/etc/nginx/conf.d/servers/cvpi-server.conf** (post 2021.2.0)
2. Run the following command to make sure the configuration does not contain any errors:

   ```
   /usr/sbin/nginx -t -c  /etc/nginx/conf.d/cvpi-server.conf
   ```

   or

   ```
   /usr/sbin/nginx -t -c  /etc/nginx/conf.d/servers/cvpi-server.conf
   ```

3. Run the following command to reload nginx with the updated configuration.

   ```
   systemctl reload nginx
   ```

20.2.2 Configuring Custom SSH Cipher

Complete these steps to configure custom SSH ciphers.

Note: Upgrading CVP removes custom SSH ciphers. You must reconfigure SSH ciphers after the upgrade.

1. Edit the `/etc/cvpi/sshd_config` to include custom ciphers and MAC definitions.
2. Run the following command to make sure the configuration does not contain any errors:

   ```
   sshd -t -f /etc/cvpi/sshd_config
   ```

3. Run the following command to reload sshd with the updated configuration.

   ```
   systemctl reload sshd
   ```

20.2.3 Strong KEX Algorithm

1. Modify the file***/etc/cvpi/sshd_config*** Below are all the ciphers and key exchange methods that can be used on CVP. You can remove those methods which the customer does not want, You can keep the following lines at the end of the file ***/etc/cvpi/sshd_config***

```
Ciphers chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,ae
s128-gcm@openssh.com,aes256-gcm@openssh.com

KexAlgorithms curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-
nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-
exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-s
ha512,diffie-hellman-group14-sha256,diffie-hellman-group14-sha1
```

2. Save the file and validate the syntax of the file using the command `sshd -t -f /etc/cvpi/sshd_config`. After running this command, it should throw any error.
3. Reload the sshd service by issuing `systemctl reload sshd` and after that verify whether the sshd service came up by checking the output of `systemctl status sshd`. Now the weak key exchange algorithms will have gone away.

20.3 DHCP Service for Zero Touch Provisioning (ZTP) Setup

The ZTP process relies on a DHCP server to get devices registered with CVP. The DHCP server can be on the CVP, but is more commonly an external DHCP server.

1. Ensure the DHCP server is installed (it is installed by default in CVP).

```
rpm -qa | grep dhcp
dhcp-common-4.1.1-43.P1.el6.x86_64
dhcp-4.1.1-43.P1.el6.x86_64
```

2. Edit the `/etc/dhcp/dhcpd.conf` file to include the option bootfile-name, which provides the location of the script that starts the ZTP process between CVP and the device.

   In this example, DHCP is serving the *172.31.0.0/16* subnet.

   Note: The *172.31.5.60* is the IP address of a CVP node, and it is recommended to use the HTTPS URL to point to the bootstrap file. This ensures that the specified devices, after they ZTP, will show up under the undefined container of the specified CVP.

```
[root@cvp1-dhcp dhcp]# cat dhcpd.conf
#
# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp*/dhcpd.conf.sample
#   see 'man 5 dhcpd.conf'
#
subnet 172.31.0.0 netmask 255.255.0.0 {
  range 172.31.3.212 172.31.5.214;
  option domain-name "sjc.aristanetworks.com";
}
host esx21-vm20 {
  option dhcp-client-identifier 00:0c:29:f9:21:99;
  fixed-address 172.31.3.211;
  option bootfile-name "https://172.31.5.60/ztp/bootstrap";
}
host esx21-vm22 {
  option dhcp-client-identifier 00:0c:29:d1:64:e1;
  fixed-address 172.31.3.213;
  option bootfile-name "https://172.31.5.60/ztp/bootstrap";
}
```

3. Restart the DHCP service after any configuration changes with the `service dhcpd restart` command.

4. Configure dhcpd to start on system boot with the `chkconfig dhcpd on` command.

Related topics:

- RADIUS or TACACS Authentication Setup
- Background Tasks
- Resetting cvpadmin Password
- HTTPS Certificates Setup

20.4 RADIUS or TACACS Authentication Setup

1. Edit the client file `/etc/raddb/clients.conf` by adding the following:

```
# CVP
client 172.31.0.0/16 {
        secret = cvpsecret
```

2. To add more, enter the following.

```
# Arista Networks
client 172.17.0.0/16 {
        secret = cvpsecret
}
client 172.18.0.0/16 {
        secret = cvpsecret
}
client 172.20.0.0/16 {
        secret = cvpsecret
}
client 172.22.0.0/16 {
        secret = cvpsecret
}
```

The default `clients.conf` file will have a section for local host. The user should either delete the whole section or comment it out. If CVP will be connecting to RADIUS on local host. You have to add a client entry for *127.0.0.0/16* (same as above).

1. Edit the users file `/etc/raddb/users` by adding the following:

```
# CVP
cvpuser Cleartext-Password := "cvpuser"
        Service-Type = NAS-Prompt-User

start radiusd:  sudo service radiusd start
enable radiusd on boot: sudo chkconfig radiusd on
```

2. If RADIUS is not working, run the server in debug mode.

```
# service radiusd stop
# /usr/sbin/radiusd -X -f
```

RADIUS will now run on the terminal with verbose output. This will let you know if RADIUS is receiving auth requests and what failure is being hit for the request. After you are done debugging, Control-C the process and start radiusd as a service.

Note: You may have to either disable iptables or firewall.serviced depending on the OS version. You could also configure it to allow traffic on ports 1812 and 1813 on the Radius server.

Related topics:

- Background Tasks

- Resetting cvpadmin Password
- HTTPS Certificates Setup
- DHCP Service for Zero Touch Provisioning (ZTP) Setup

20.5 Background Tasks

CloudVision provides command-line tools that can be executed from the linux shell or scheduled as cronjobs either on a CVP node or on an external server, for the following tasks:

- Compliance checks
- Snapshots
- Backups

The tools are available by default on the CVP nodes in the `/cvpi/tools/` directory. The tools can be used on an external linux server by downloading the `cvp-tools-<version> .tgz` from https://www.arista.com to the external linux server.

Detailed help on the tool is available by using the –h option with the tool:

```
cvpi/tools/compliance.py -h
cvpi/tools/backup.py -h
```

Related topics:

- Resetting cvpadmin Password
- HTTPS Certificates Setup
- DHCP Service for Zero Touch Provisioning (ZTP) Setup
- RADIUS or TACACS Authentication Setup

20.5.1 Scheduling and Viewing Cronjobs

To schedule cronjobs to perform periodic compliance checks or snapshots, insert commands into the crontab using the following command:

```
crontab -e
```

Note: When inserting commands to schedule cronjobs, you only need to do this on one node of the cluster.

Example

To schedule a periodic compliance check and snapshot to be performed hourly on the tenant container, and a backup to be performed daily at 2:00 am, insert the following lines into the crontab file on the primary node if not already present. In this example, the user is named “**me**” and the password is “**pwd**”.

```
0 * * * * /cvpi/tools/compliance.py --user me --password pwd --containers
 tenant
0 2 * * * /cvpi/tools/backup.py --limit 5
```

To see the active cronjobs, use the following command:

```
crontab -l
```

To view the console outputs of the cronjobs tail, view (open) the following log file:

```
tail -f /var/log/cron
```

Related topics:

- Resetting cvpadmin Password
- HTTPS Certificates Setup
- DHCP Service for Zero Touch Provisioning (ZTP) Setup
- RADIUS or TACACS Authentication Setup

20.6 Resetting cvpadmin Password

If the *cvpadmin* password is lost or forgotten, you can reset it from any of the CVP nodes using the following steps.

1. Log into a CVP node Linux shell as root user.
2. Execute the following command:

```
/cvpi/tools/update-mgmt-password -password <new password>
```

Note: Do not set the new password to the string "*cvpadmin*".

Related topics:

- HTTPS Certificates Setup
- DHCP Service for Zero Touch Provisioning (ZTP) Setup
- RADIUS or TACACS Authentication Setup
- Background Tasks

20.7 Optional SAN IP field in CVP Certificate

ZTP boot can be done without specifying the SAN IP in the certificate’s field. If the certificate is issued by a public CA without a SAN IP, it will require us to use CVP’s FQDN to set up a secure connection. Using an IP address you can set up a secure connection with CVP, because the ZTP app now resolves the DNS name to the correct IP address. Although the SAN IP field in the certificate is now optional, DNS is still mandatory.

20.7.1 Creating a certificate without SAN IP

Go to settings and click on certificate Click on +Add, to add the new certificate Certificate form, asking for details will appear Fill the details without specifying SAN IPs

1. From Settings select Certificate.
2. Click on **+Add**, to add the new certificate.
3. Complete the Certificate form, without specifying a SAN IP address.
4. Click **OK** at the prompt will confirming that a SAN IP has not been provided.
5. Clicking **OK** on the next prompt stating the existing certificate will be replaced.
6. Proceed with the ZTP boot process.

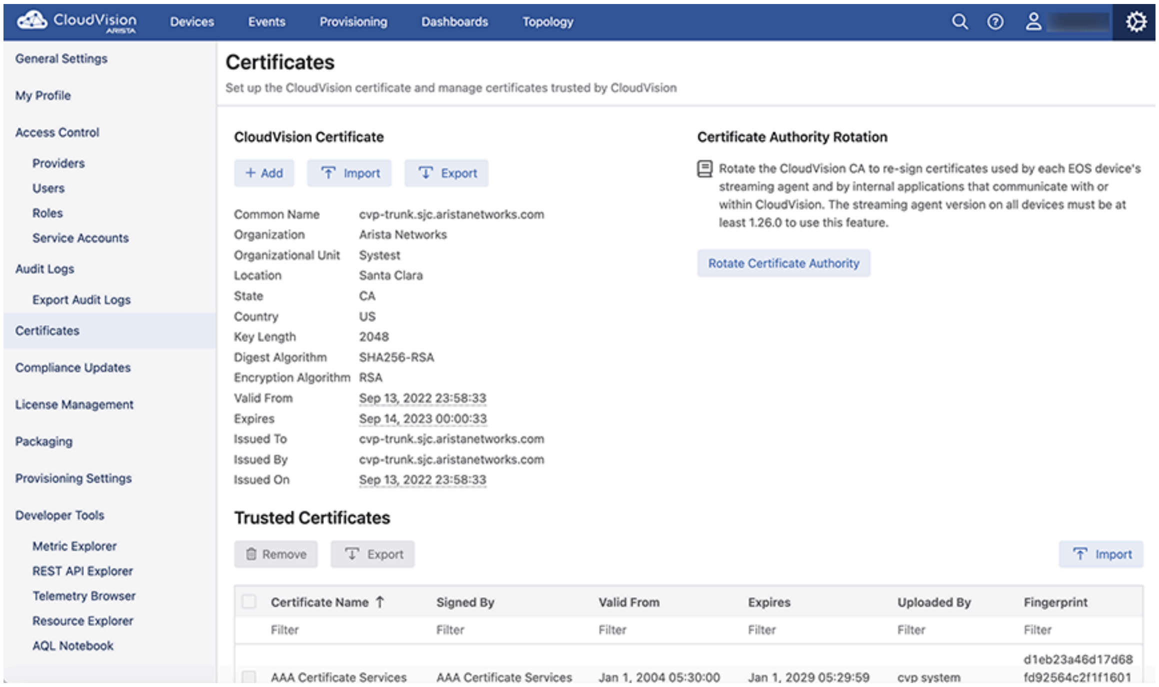
20.8 Rotating Internal Certificate Authority

The streaming agent used by EOS devices and other applications that communicate with each other in CloudVision uses mutual TLS certificates signed by a local certificate authority (CA). To prevent the CA from expiring in the future, you should rotate the CA. Once rotated, by default, the CA becomes valid for a hundred years. This process re-signs the certificates used by each EOS device's streaming agent and internal applications that communicate with CloudVision. The streaming agent version on all devices must be at least 1.26.0 to use this feature.

You get the first notification through an event message around 90 days prior to the certificate expiry.

To rotate a certificate, go to **Settings** (gear icon) > **Certificates** on the CloudVision portal. The CA rotation process takes several minutes, and it is necessary to plan a maintenance window before rotating a CA. See the images below.

Figure 20-8: Certificate Authority Rotation page



Certificates

Set up the CloudVision certificate and manage certificates trusted by CloudVision

CloudVision Certificate

Common Name	cvp-trunk.sjc.aristanetworks.com
Organization	Arista Networks
Organizational Unit	Systest
Location	Santa Clara
State	CA
Country	US
Key Length	2048
Digest Algorithm	SHA256-RSA
Encryption Algorithm	RSA
Valid From	Sep 13, 2022 23:58:33
Expires	Sep 14, 2023 00:00:33
Issued To	cvp-trunk.sjc.aristanetworks.com
Issued By	cvp-trunk.sjc.aristanetworks.com
Issued On	Sep 13, 2022 23:58:33

Certificate Authority Rotation

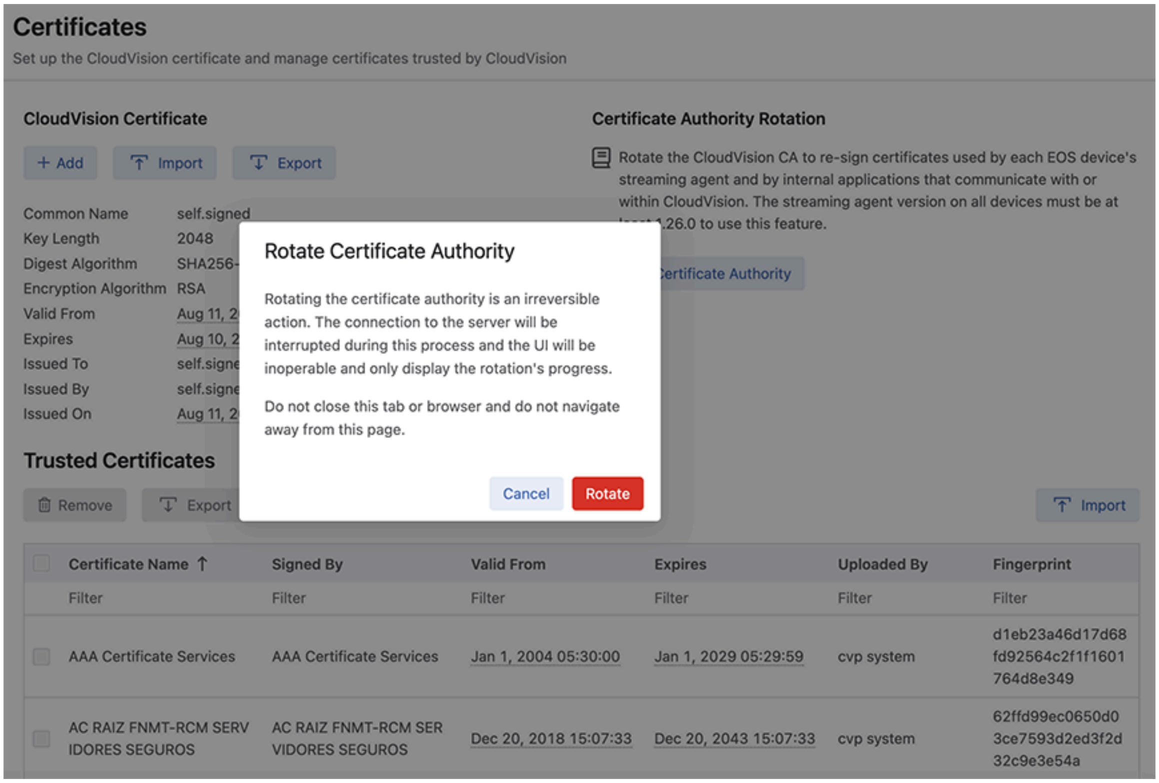
Rotate the CloudVision CA to re-sign certificates used by each EOS device's streaming agent and by internal applications that communicate with or within CloudVision. The streaming agent version on all devices must be at least 1.26.0 to use this feature.

Trusted Certificates

□	Certificate Name ↑	Signed By	Valid From	Expires	Uploaded By	Fingerprint
	Filter	Filter	Filter	Filter	Filter	Filter
□	AAA Certificate Services	AAA Certificate Services	Jan 1, 2004 05:30:00	Jan 1, 2029 05:29:59	cvp system	d1eb23a46d17d68 fd92564c2f1f1601

Click **Rotate Certificate Authority**.

Figure 20-9: Confirmation Page to Rotate CA



Certificates

Set up the CloudVision certificate and manage certificates trusted by CloudVision

CloudVision Certificate

Common Name	self.signed
Key Length	2048
Digest Algorithm	SHA256-
Encryption Algorithm	RSA
Valid From	Aug 11, 2
Expires	Aug 10, 2
Issued To	self.signe
Issued By	self.signe
Issued On	Aug 11, 2

Certificate Authority Rotation

Rotate the CloudVision CA to re-sign certificates used by each EOS device's streaming agent and by internal applications that communicate with or within CloudVision. The streaming agent version on all devices must be at l.26.0 to use this feature.

Rotate Certificate Authority

Rotating the certificate authority is an irreversible action. The connection to the server will be interrupted during this process and the UI will be inoperable and only display the rotation's progress.

Do not close this tab or browser and do not navigate away from this page.

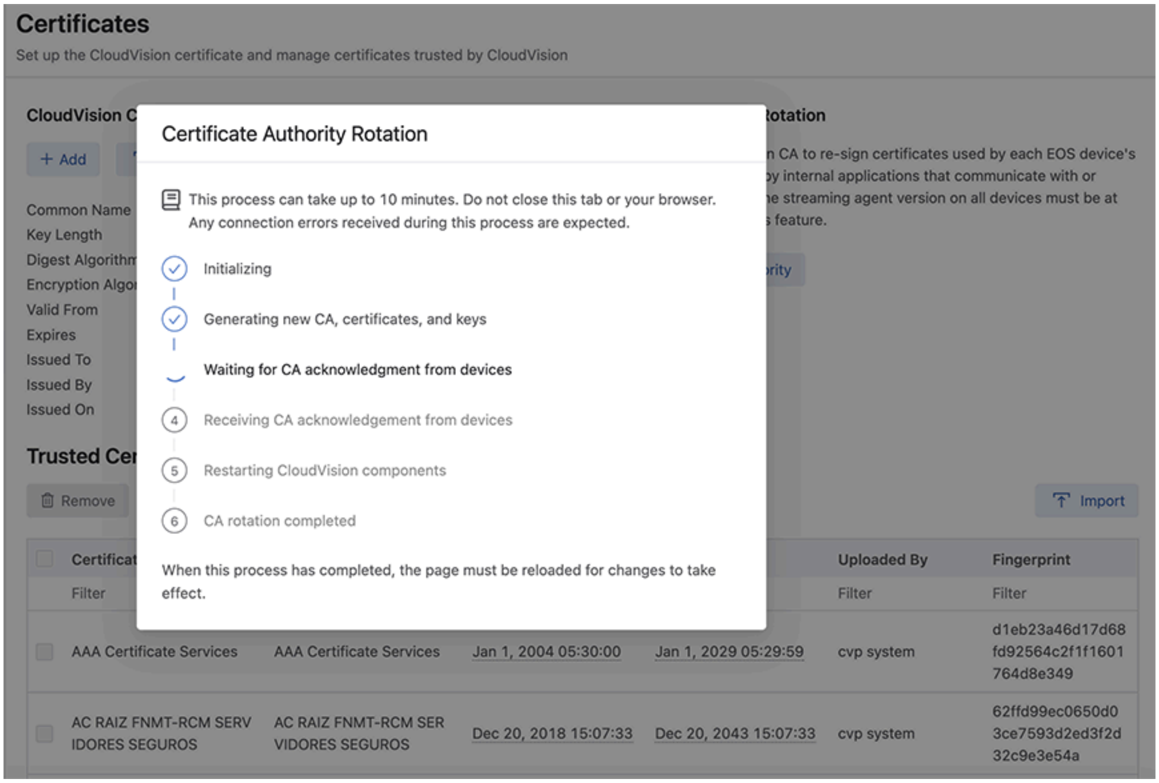
Trusted Certificates

Certificate Name ↑	Signed By	Valid From	Expires	Uploaded By	Fingerprint
Filter	Filter	Filter	Filter	Filter	Filter
AAA Certificate Services	AAA Certificate Services	Jan 1, 2004 05:30:00	Jan 1, 2029 05:29:59	cvp system	d1eb23a46d17d68fd92564c2f1f1601764d8e349
AC RAIZ FNMT-RCM SERVIDORES SEGUROS	AC RAIZ FNMT-RCM SERVIDORES SEGUROS	Dec 20, 2018 15:07:33	Dec 20, 2043 15:07:33	cvp system	62ffd99ec0650d03ce7593d2ed3f2d32c9e3e54a

Click **Rotate**.

Note: During this process, the CloudVision portal becomes inaccessible, and the page displays only the progress of the rotation. Do not close the window or the browser, and do not navigate away from the page. The rotation process takes several minutes (more than 10 minutes). Wait until the rotation process is completed when the browser tab gets refreshed. See image below.

Figure 20-10: CA Rotation Status Window



Certificates

Set up the CloudVision certificate and manage certificates trusted by CloudVision

Certificate Authority Rotation

This process can take up to 10 minutes. Do not close this tab or your browser. Any connection errors received during this process are expected.

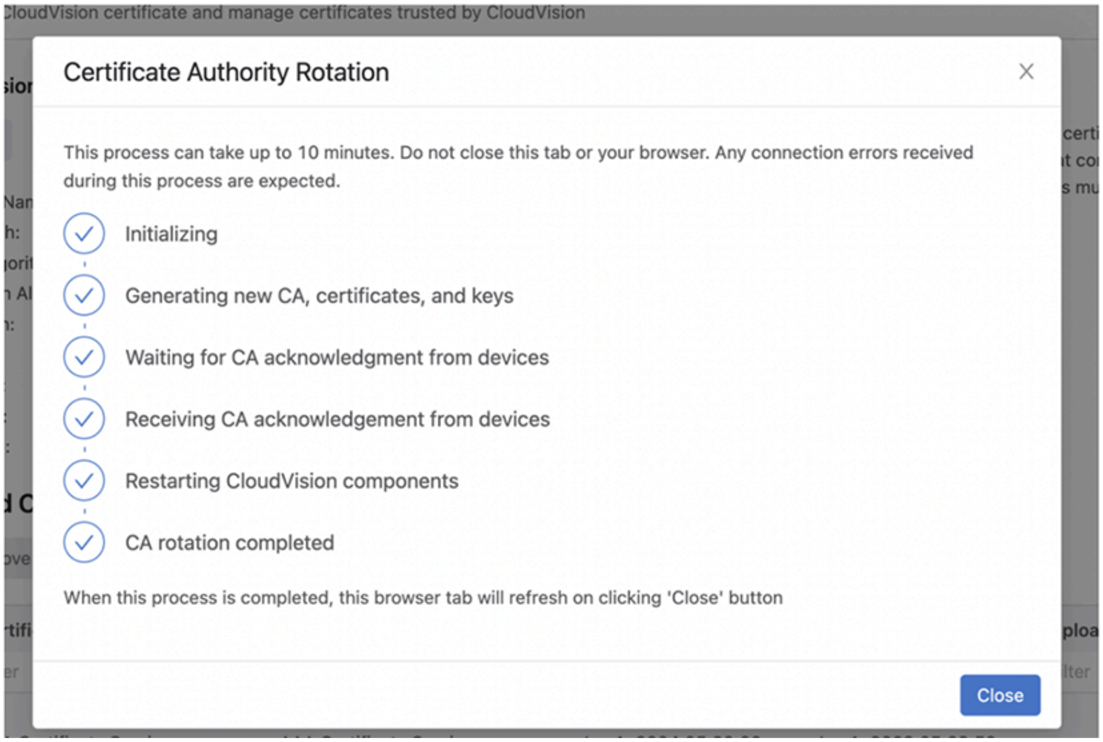
- ✓ Initializing
- ✓ Generating new CA, certificates, and keys
- Waiting for CA acknowledgment from devices
- 4 Receiving CA acknowledgement from devices
- 5 Restarting CloudVision components
- 6 CA rotation completed

When this process has completed, the page must be reloaded for changes to take effect.

Certificat				Uploaded By	Fingerprint
Filter				Filter	Filter
AAA Certificate Services	AAA Certificate Services	Jan 1, 2004 05:30:00	Jan 1, 2029 05:29:59	cvp system	d1eb23a46d17d68fd92564c2f1f1601764d8e349
AC RAIZ FNMT-RCM SERVIDORES SEGUROS	AC RAIZ FNMT-RCM SERVIDORES SEGUROS	Dec 20, 2018 15:07:33	Dec 20, 2043 15:07:33	cvp system	62ffd99ec0650d03ce7593d2ed3f2d32c9e3e54a

Once the rotation process is complete, click **Close** at the bottom of the page.

Figure 20-11: CA Rotation Complete Status



CloudVision certificate and manage certificates trusted by CloudVision

Certificate Authority Rotation

This process can take up to 10 minutes. Do not close this tab or your browser. Any connection errors received during this process are expected.

- ✓ Initializing
- ✓ Generating new CA, certificates, and keys
- ✓ Waiting for CA acknowledgment from devices
- ✓ Receiving CA acknowledgement from devices
- ✓ Restarting CloudVision components
- ✓ CA rotation completed

When this process is completed, this browser tab will refresh on clicking 'Close' button

The browser tab refreshes, and the CA rotation is completed. The new CA is now valid for one hundred years and devices are automatically re-enrolled.

If you see any errors during the CA rotation process, you can retry the rotation. If the rotation process fails after multiple retries, then you must contact Arista Support team (TAC) for a resolution.

Chapter 21

Troubleshooting and Health Checks

If you encounter an issue when using CloudVision appliance, check to see if there are troubleshooting steps for the issue.

- System Recovery
- VM Redeployment
- Health Checks
- Resource Checks

21.1 System Recovery

System recovery should be used only when the CVP cluster has become unusable and other steps, such as performing a `cvpi watchdog off, cvpi stop all, and then, cvpi start all, cvpi watchdog` on have failed. For example, situations in which, regardless of restarts, a `cvpi status all` continues to show some components as having a status of UNHEALTHY or NOT RUNNING.

There are two ways to completely recover a CVP cluster:

- VM Redeployment
- CVP Re-Install without VM Redeployment

Note: A good backup is required to proceed with either of these system recoveries.

21.1.1 CVP Re-Install without VM Redeployment

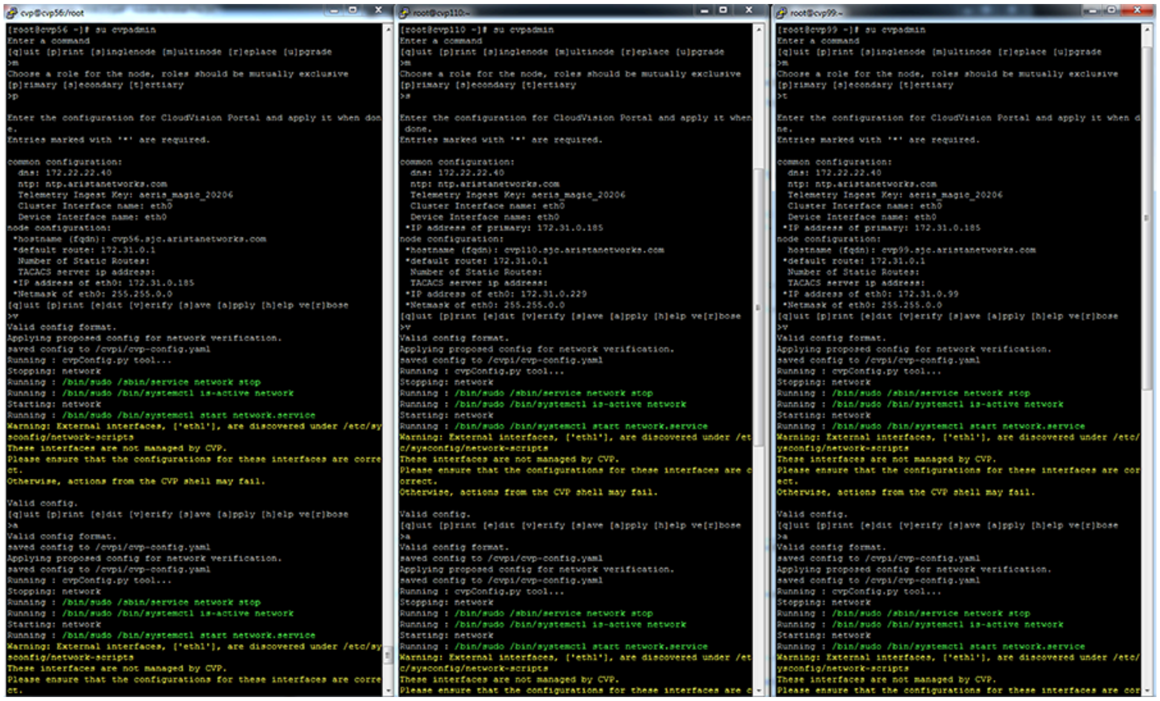
Complete these steps:

1. Run `cvpReInstall` from the Linux shell of the primary node. This may take 15 minutes to complete.

```
[root@cvp99 ~]# cvpReInstall
0.Log directory is /tmp/cvpReinstall_17_02_23_01_59_48
Existing /cvpi/cvp-config.yaml will be backed up here.
….
….
Complete!

CVP configuration not backed up, please use cvpShell to setup the cluster

CVP Re-install complete, you can now configure the cluster
```

2. Re-configure using the procedure in Shell-based Configuration. Log into the Linux shell of each node as **cvpadmin** or **su cvpadmin**.

   Figure 21-1: cvp-shell-login



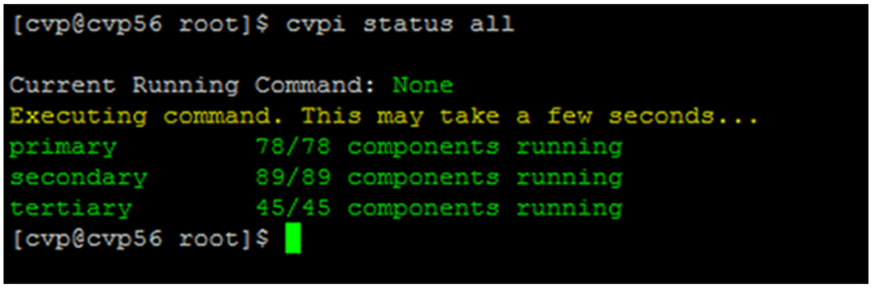
```
[root@cvp56 ~]# su cvpadmin
Enter a command
[q]uit [p]rint [s]inglenode [m]ultinode [r]eplace [u]pgrade
>m
Choose a role for the node, roles should be mutually exclusive
[p]rimary [s]econdary [t]ertiary
>p

Enter the configuration for CloudVision Portal and apply it when don
e.
Entries marked with '*' are required.

common configuration:
  dns: 172.22.22.40
  ntp: ntp.aristanetworks.com
  Telemetry Ingest Key: aeris_magic_20206
  Cluster Interface name: eth0
  Device Interface name: eth0
node configuration:
 *hostname (fqdn): cvp56.sjc.aristanetworks.com
 *default route: 172.31.0.1
  Number of Static Routes:
  TACACS server ip address:
 *IP address of eth0: 172.31.0.185
 *Netmask of eth0: 255.255.0.0
[q]uit [p]rint [e]dit [v]erify [s]ave [a]pply [h]elp ve[r]bose
>v
Valid config format.
Applying proposed config for network verification.
saved config to /cvpi/cvp-config.yaml
Running : cvpConfig.py tool...
Stopping: network
Running : /bin/sudo /sbin/service network stop
Running : /bin/sudo /bin/systemctl is-active network
Starting: network
Running : /bin/sudo /bin/systemctl start network.service
Warning: External interfaces, ['eth1'], are discovered under /etc/sy
sconfig/network-scripts
These interfaces are not managed by CVP.
Please ensure that the configurations for these interfaces are corre
ct.
Otherwise, actions from the CVP shell may fail.

Valid config.
[q]uit [p]rint [e]dit [v]erify [s]ave [a]pply [h]elp ve[r]bose
>a
Valid config format.
saved config to /cvpi/cvp-config.yaml
Applying proposed config for network verification.
saved config to /cvpi/cvp-config.yaml
Running : cvpConfig.py tool...
Stopping: network
Running : /bin/sudo /sbin/service network stop
Running : /bin/sudo /bin/systemctl is-active network
Starting: network
Running : /bin/sudo /bin/systemctl start network.service
Warning: External interfaces, ['eth1'], are discovered under /etc/sy
sconfig/network-scripts
These interfaces are not managed by CVP.
Please ensure that the configurations for these interfaces are corre
ct.
```

```
[root@cvp110 ~]# su cvpadmin
Enter a command
[q]uit [p]rint [s]inglenode [m]ultinode [r]eplace [u]pgrade
>m
Choose a role for the node, roles should be mutually exclusive
[p]rimary [s]econdary [t]ertiary
>s

Enter the configuration for CloudVision Portal and apply it when
 done.
Entries marked with '*' are required.

common configuration:
  dns: 172.22.22.40
  ntp: ntp.aristanetworks.com
  Telemetry Ingest Key: aeris_magic_20206
  Cluster Interface name: eth0
  Device Interface name: eth0
 *IP address of primary: 172.31.0.185
node configuration:
 *hostname (fqdn): cvp110.sjc.aristanetworks.com
 *default route: 172.31.0.1
  Number of Static Routes:
  TACACS server ip address:
 *IP address of eth0: 172.31.0.229
 *Netmask of eth0: 255.255.0.0
[q]uit [p]rint [e]dit [v]erify [s]ave [a]pply [h]elp ve[r]bose
>v
Valid config format.
Applying proposed config for network verification.
saved config to /cvpi/cvp-config.yaml
Running : cvpConfig.py tool...
Stopping: network
Running : /bin/sudo /sbin/service network stop
Running : /bin/sudo /bin/systemctl is-active network
Starting: network
Running : /bin/sudo /bin/systemctl start network.service
Warning: External interfaces, ['eth1'], are discovered under /et
c/sysconfig/network-scripts
These interfaces are not managed by CVP.
Please ensure that the configurations for these interfaces are c
orrect.
Otherwise, actions from the CVP shell may fail.

Valid config.
[q]uit [p]rint [e]dit [v]erify [s]ave [a]pply [h]elp ve[r]bose
>a
Valid config format.
saved config to /cvpi/cvp-config.yaml
Applying proposed config for network verification.
saved config to /cvpi/cvp-config.yaml
Running : cvpConfig.py tool...
Stopping: network
Running : /bin/sudo /sbin/service network stop
Running : /bin/sudo /bin/systemctl is-active network
Starting: network
Running : /bin/sudo /bin/systemctl start network.service
Warning: External interfaces, ['eth1'], are discovered under /et
c/sysconfig/network-scripts
These interfaces are not managed by CVP.
Please ensure that the configurations for these interfaces are c
```

```
[root@cvp99 ~]# su cvpadmin
Enter a command
[q]uit [p]rint [s]inglenode [m]ultinode [r]eplace [u]pgrade
>m
Choose a role for the node, roles should be mutually exclusive
[p]rimary [s]econdary [t]ertiary
>t

Enter the configuration for CloudVision Portal and apply it when d
ne.
Entries marked with '*' are required.

common configuration:
  dns: 172.22.22.40
  ntp: ntp.aristanetworks.com
  Telemetry Ingest Key: aeris_magic_20206
  Cluster Interface name: eth0
  Device Interface name: eth0
 *IP address of primary: 172.31.0.185
node configuration:
  hostname (fqdn): cvp99.sjc.aristanetworks.com
 *default route: 172.31.0.1
  Number of Static Routes:
  TACACS server ip address:
 *IP address of eth0: 172.31.0.99
 *Netmask of eth0: 255.255.0.0
[q]uit [p]rint [e]dit [v]erify [s]ave [a]pply [h]elp ve[r]bose
>v
Valid config format.
Applying proposed config for network verification.
saved config to /cvpi/cvp-config.yaml
Running : cvpConfig.py tool...
Stopping: network
Running : /bin/sudo /sbin/service network stop
Running : /bin/sudo /bin/systemctl is-active network
Starting: network
Running : /bin/sudo /bin/systemctl start network.service
Warning: External interfaces, ['eth1'], are discovered under /etc/
ysconfig/network-scripts
These interfaces are not managed by CVP.
Please ensure that the configurations for these interfaces are cor
ect.
Otherwise, actions from the CVP shell may fail.

Valid config.
[q]uit [p]rint [e]dit [v]erify [s]ave [a]pply [h]elp ve[r]bose
>a
Valid config format.
saved config to /cvpi/cvp-config.yaml
Applying proposed config for network verification.
saved config to /cvpi/cvp-config.yaml
Running : cvpConfig.py tool...
Stopping: network
Running : /bin/sudo /sbin/service network stop
Running : /bin/sudo /bin/systemctl is-active network
Starting: network
Running : /bin/sudo /bin/systemctl start network.service
Warning: External interfaces, ['eth1'], are discovered under /etc/
ysconfig/network-scripts
These interfaces are not managed by CVP.
Please ensure that the configurations for these interfaces are cor
```

3. Issue a `cvpi status all` command to ensure all components are running.

   Figure 21-2: Example output of cvpi status all command



```
[cvp@cvp56 root]$ cvpi status all

Current Running Command: None
Executing command. This may take a few seconds...
primary          78/78 components running
secondary        89/89 components running
tertiary         45/45 components running
[cvp@cvp56 root]$ 
```

4. Login to the CVP GUI as `cvpadmin/cvpadmin` to set the cvpadmin password.
5. From the **Backup & Restore** tab on the **Setting** page, restore from the backup.

   Related topics:

   - Health Checks
   - Resource Checks

21.2 VM Redeployment

Complete the following steps:

1. Delete all the CVP VMs.
2. Redeploy the VMs using the procedures in CloudVision Portal (CVP) Setup.
3. Issue a `cvpi status all` command to ensure all components are running.
4. Login to the CVP GUI as `cvpadmin/cvpadmin` to set the cvpadmin password.

5. From the **Backup & Restore** tab on the **Setting** page, restore from the backup.

21.3 Health Checks

The following table lists the different types of CVP health checks you can run, including the steps to use to run each check and the expected result for each check.

Component	Steps to Use	Expected Result
Network connectivity	`ping -f` across all nodes	No packet loss, network is healthy.

HBase	`hbase hbck 2>&1 | grep "Status\\|Table"`	The status is provided. A good system will return a status of "okay" `2021-11-11 15:06:31,066 INFO [main] util.HBaseFsck: getTableDescriptors == tableNames => [__test-table_ne652.aristanetworks.com__, aeris_v2, hbase:namespace]`
		`Number of Tables: 3`
		`Table hbase:meta is okay. Table _test-table_ne652.aristanetworks.com_ is okay. Table aeris_v2 is okay. Table hbase:namespace is okay.`
		`Status: OK`

Check time is in sync between nodes	On all nodes run `date +%s`	UTC time should be within a few seconds of each other (typically less than one second). Up to 10 seconds is allowable.
I/O slowness issues	The disk I/O throughput is at an unhealthy level (too low).	Use the `cvpi resources` command to find out whether the disk I/O throughput is at a **healthy level** or **unhealthy level**. The disk I/O throughput reported in the command output is measured by the Virtual Machine. See Running Health Checks for an example of the output of the `cvpi resources` command.

- Running Health Checks

21.3.1 Running Health Checks

Run the `cvpi resources` command to execute a health check on disk bandwidth. The output of the command indicates whether the disk bandwidth is at a healthy level or unhealthy level. The threshold for healthy disk bandwith is 20MBS.

The possible health statuses are:

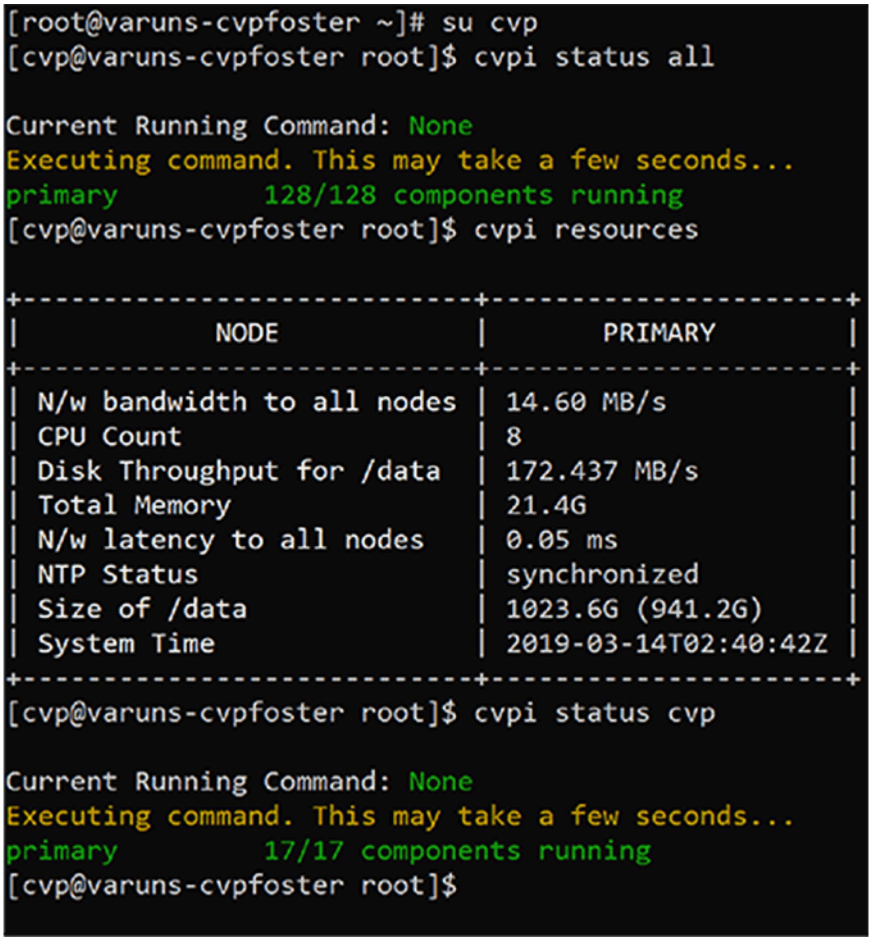
- **Healthy** - Disk bandwidth above 20MBs

- **Unhealthy** - Disk bandwidth at or below 20MBs

The output is color coded to make it easy to interpret the output. Green indicates a healthy level, and red indicates an unhealthy level (see the example below).

This example shows output of the `cvpi resources` command. In this example, the disk bandwidth status is healthy (above the 20MBs threshold).

Figure 21-3: Example output of cvpi resources command



```
[root@varuns-cvpfoster ~]# su cvp
[cvp@varuns-cvpfoster root]$ cvpi status all

Current Running Command: None
Executing command. This may take a few seconds...
primary         128/128 components running
[cvp@varuns-cvpfoster root]$ cvpi resources


+----------------------------+----------------------+
|            NODE            |       PRIMARY        |
+----------------------------+----------------------+
| N/w bandwidth to all nodes | 14.60 MB/s           |
| CPU Count                  | 8                    |
| Disk Throughput for /data  | 172.437 MB/s         |
| Total Memory               | 21.4G                |
| N/w latency to all nodes   | 0.05 ms              |
| NTP Status                 | synchronized         |
| Size of /data              | 1023.6G (941.2G)     |
| System Time                | 2019-03-14T02:40:42Z |
+----------------------------+----------------------+
[cvp@varuns-cvpfoster root]$ cvpi status cvp

Current Running Command: None
Executing command. This may take a few seconds...
primary         17/17 components running
[cvp@varuns-cvpfoster root]$
```

Related topics

- Resource Checks

21.4 Resource Checks

CloudVision Portal (CVP) enables you to run resource checks on CVP node VMs. You can run checks to determine the current data disk size of VMs that you have upgraded to CVP version 2017.2.0, and to determine the current memory allocation for each CVP node VM.

Performing these resource checks is important to ensure that the CVP node VMs in your deployment have the recommended data disk size and memory allocation for using the Telemetry feature. If the resource checks show that the CVP node VM data disk size or memory allocation (RAM) are below the recommended levels, you can increase the data disk size and memory allocation.

These procedures provide detailed instructions on how to perform the resource checks and if needed, how to increase the CVP node VM data disk size and CVP node VM memory allocation.

- Running CVP node VM Resource Checks
- Increasing Disk Size of VMs Upgraded to CVP Version 2017.2.0
- Increasing CVP Node VM Memory Allocation

21.4.1 Running CVP node VM Resource Checks

CloudVision Portal (CVP) enables you to quickly and easily check the current resources of the primary, secondary, and tertiary nodes of a cluster by running a single command. The command you use is the `cvpi resources` command.

Use this command to check the following CVP node VM resources:

- Memory allocation
- Data disk size (storage capacity)
- Disk throughput (in MB per second)
- Number of CPUs

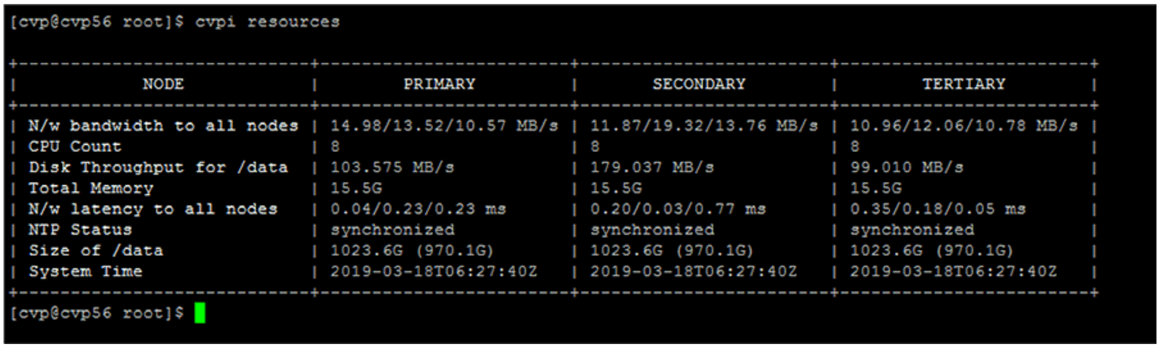
Complete the following steps to run the CVP node VM resource check.

1. Login to one of the CVP nodes as **root**.
2. Execute the `cvpi resources` command.

   The output shows the current resources for each CVP node VM

   - If the total size of sdb1 (or vdb1) is approximately 120G or less, you can increase the disk size to 1TB (seeIncreasing Disk Size of VMs Upgraded to CVP Version 2017.2.0).
   - If the memory allocation is the default of 16GB, you can increase the RAM memory allocation (see Increasing CVP Node VM Memory Allocation).

   Figure 21-4: Using the cvpi resource command to run CVP node VM resource checks



```
[cvp@cvp56 root]$ cvpi resources

+---------------------------+----------------------+----------------------+----------------------+
|           NODE            |       PRIMARY        |      SECONDARY       |       TERTIARY       |
+---------------------------+----------------------+----------------------+----------------------+
| N/w bandwidth to all nodes | 14.98/13.52/10.57 MB/s | 11.87/19.32/13.76 MB/s | 10.96/12.06/10.78 MB/s |
| CPU Count                 | 8                    | 8                    | 8                    |
| Disk Throughput for /data | 103.575 MB/s         | 179.037 MB/s         | 99.010 MB/s          |
| Total Memory              | 15.5G                | 15.5G                | 15.5G                |
| N/w latency to all nodes  | 0.04/0.23/0.23 ms    | 0.20/0.03/0.77 ms    | 0.35/0.18/0.05 ms    |
| NTP Status                | synchronized         | synchronized         | synchronized         |
| Size of /data             | 1023.6G (970.1G)     | 1023.6G (970.1G)     | 1023.6G (970.1G)     |
| System Time               | 2019-03-18T06:27:40Z | 2019-03-18T06:27:40Z | 2019-03-18T06:27:40Z |
+---------------------------+----------------------+----------------------+----------------------+
[cvp@cvp56 root]$
```

21.4.2 Increasing Disk Size of VMs Upgraded to CVP Version 2017.2.0

If you already upgraded any CVP node VMs running an older version of CVP to version 2017.2.0, you may need to increase the size of the data disk of the VMs so that the data disks have the 1TB disk image that is used on current CVP node VMs

CVP node VM data disks that you upgraded to version 2017.2.0 may still have the original disk image (120GB data image), because the standard upgrade procedure did not upgrade the data disk image. The standard upgrade procedure updated only the root disk, which contains the Centos image along with rpms for CVPI, CVP, and Telemetry.

Note: It is recommended that each CVP node have 1TB of disk space reserved for enabling CVP Telemetry. If the CVP nodes in your current environment do not have the recommended reserved disk space of 1TB, complete the procedure below for increasing the disk size of CVP node VMs.

Pre-requisites

Before you begin the procedure, make sure that you:

- Have upgraded to version 2017.2.0. You cannot increase the data disk size until you have completed the upgrade to version 2017.2.0 (see How to Modify the DNS and NTP Configuration).
- Have performed the resource check to verify that the CVP node VMs have the data disk size image of previous CVP versions (approximately 120GB or less). See Running CVP node VM Resource Checks.

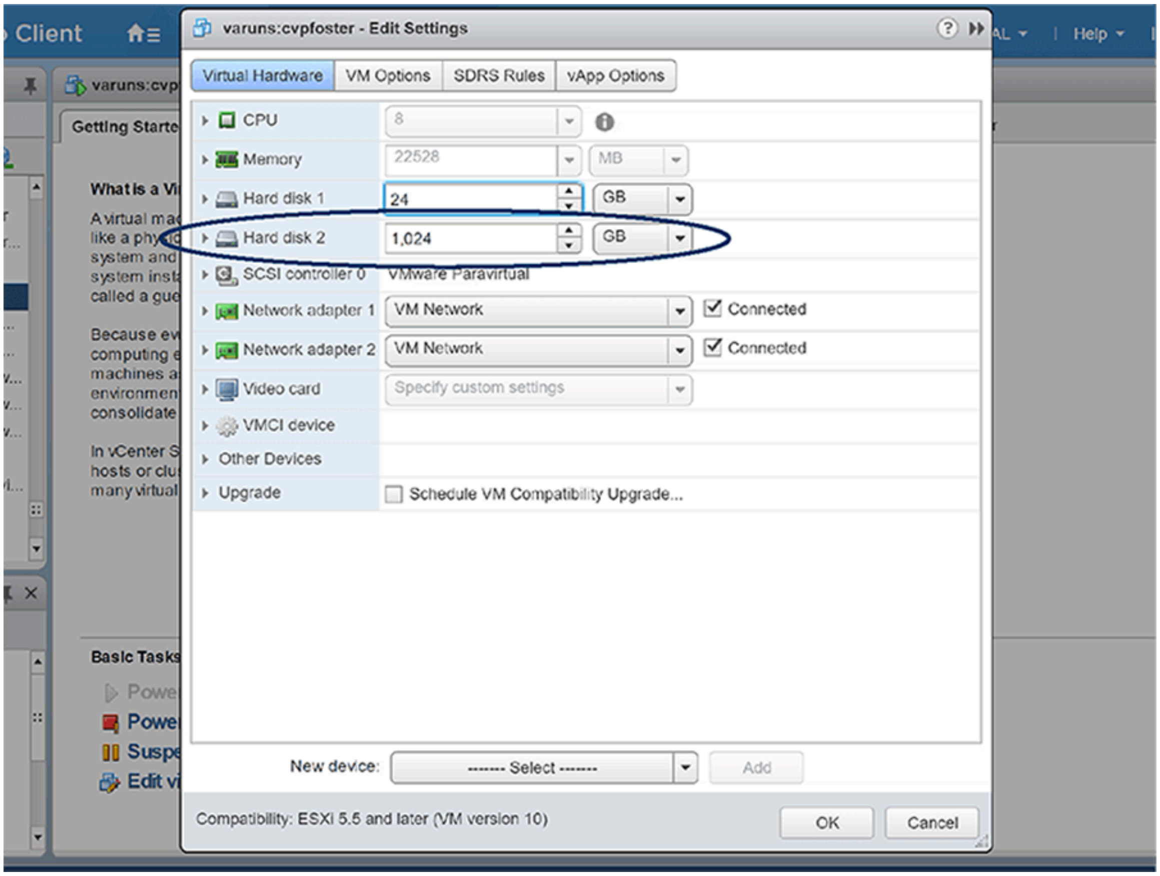
Procedure

Complete the following steps to increase the data disk size.

1. Turn off cvpi service by executing the `systemctl stop cvpi` command on all nodes in the cluster. (For a single-node installation, run this command on the node.)
2. Run the `cvpi -v=3 stop all` on the primary node.
3. Perform a **graceful power-off** of all VMs.

   Note: You do not need to unregister and re-register VMs from vSphere Client or undefine and redefine VMs from kvm hypervisor.
4. Do the following to increase the size of the data disk to 1TB using the hypervisor:
   - **ESX**: Using vSphere client, do the following:
     a. Select the **Virtual Hardware** tab, and then select **hard disk 2**.
     b. Change the setting from 120GB to **1TB**.
     c. Click **OK**.
   - **KVM**: Use the `qemu-img resize` command to resize the data disk from 120GB to 1TB. Be sure to select **disk2.qcow2.**

Figure 21-5: Using vSphere to increase data disk size



varuns:cvpfoster - Edit Settings

Virtual Hardware | VM Options | SDRS Rules | vApp Options

CPU: 8

Memory: 22528 MB

Hard disk 1: 24 GB

Hard disk 2: 1,024 GB

SCSI controller 0: VMware Paravirtual

Network adapter 1: VM Network ☑ Connected

Network adapter 2: VM Network ☑ Connected

Video card: Specify custom settings

VMCI device

Other Devices

Upgrade: □ Schedule VM Compatibility Upgrade...

New device: ------- Select ------- Add

Compatibility: ESXi 5.5 and later (VM version 10)

OK Cancel

5. Power on all CVP node VMs, and wait for all services to start.
6. Use the `cvpi status all` command to verify that all the cvpi services are running.

7. Run the `/cvpi/tools/diskResize.py` command on the primary node. (Do not run this command on the secondary and tertiary nodes.)
8. Run the `df -h /data` command on all nodes to verify that the /data is increased to approximately 1TB.
9. Wait for all services to start.
10. Use the `cvpi -v=3 status all` command to verify the status of services.
11. Use the `systemctl status cvpi` to ensure that cvpi service is running.

21.4.3 Increasing CVP Node VM Memory Allocation

If the CVP Open Virtual Appliance (OVA) template currently specifies the default of 16GB of memory allocated for the CVP node VMs in the CVP cluster, you need to increase the RAM to ensure that the CVP node VMs have adequate memory allocated for using the Telemetry feature.

Note: It is recommended that CVP node VMs have 32GB of RAM allocated for deployments in which Telemetry is enabled.

You can perform a rolling modification to increase the RAM allocation of every node in the cluster. If you want to keep the service up and available while you are performing the rolling modification, make sure that you perform the procedure on only one CVP node VM at a time.

Once you have completed the procedure on a node, you repeat the procedure on another node in the cluster. You must complete the procedure once for every node in the cluster.

Pre-requisites

Before you begin the procedure, make sure that you:

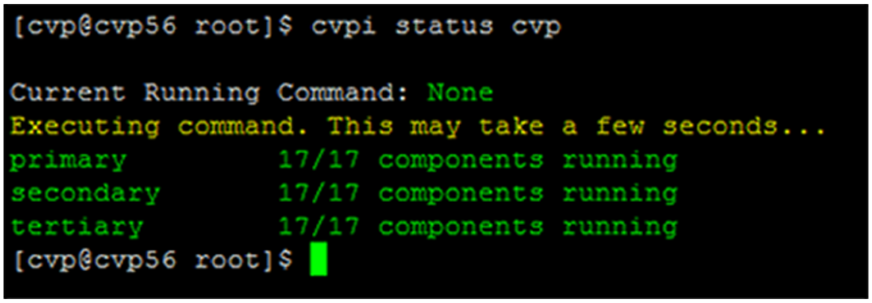
- Have performed the resource check to verify that the CVP node VMs have the default RAM memory allocation of 16GB (see Running CVP node VM Resource Checks).
- Make sure that you perform a GUI-based backup of the CVP system and copy the backup to a safe location (a location off of the CVP node VMs). The CVP GUI enables you to create a backup you can use to restore CVP data.

Procedure

Complete the following steps to increase the RAM memory allocation of the CVP node VMs.

1. Login to a CVP node of the cluster as **cvp user**.
2. Using the `cvpi status cvp shell` command, make sure that all nodes in the cluster are operational.

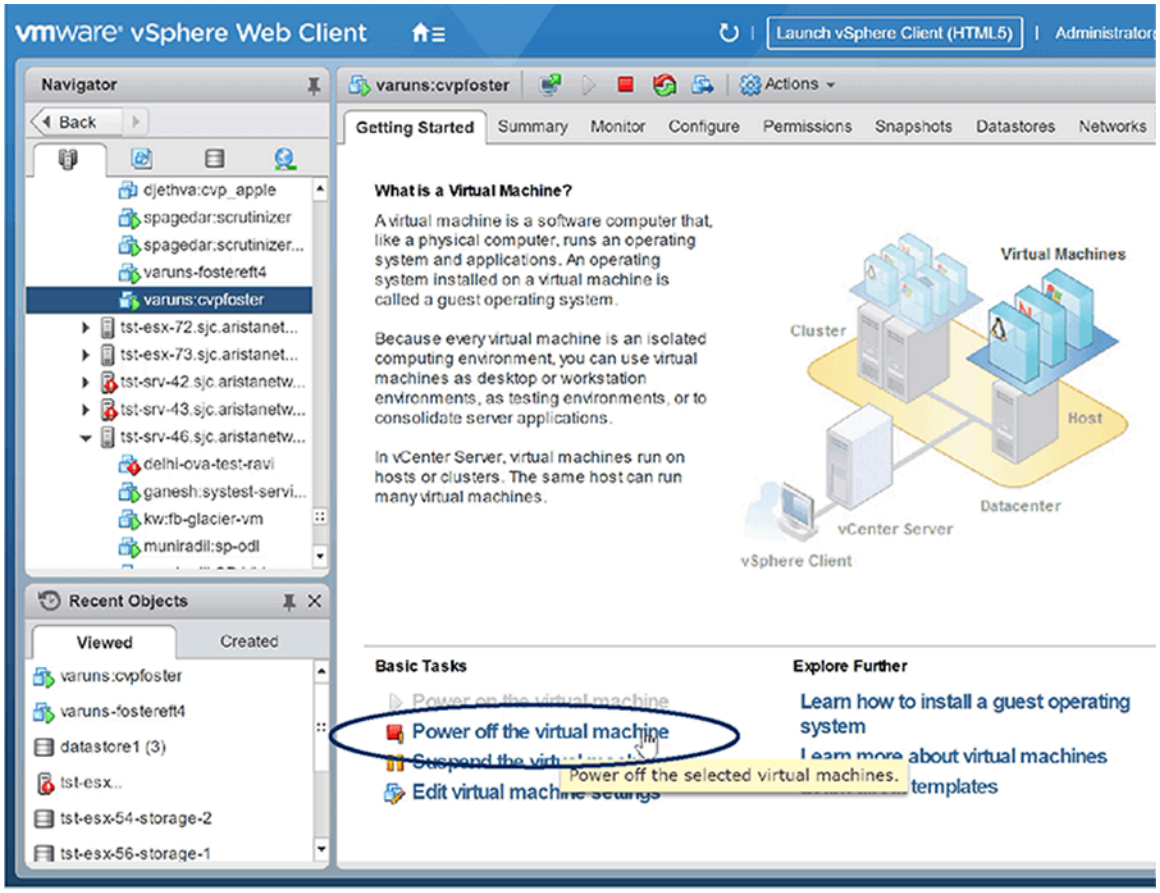
Figure 21-6: cvpi status cvp shell command



```
[cvp@cvp56 root]$ cvpi status cvp

Current Running Command: None
Executing command. This may take a few seconds...
primary          17/17 components running
secondary        17/17 components running
tertiary         17/17 components running
[cvp@cvp56 root]$
```

3. Using vSphere client, shutdown one CVP node VM by selecting the node in the left pane, and then click the **Power off the virtual machine** option.

Figure 21-7: Power off the virtual machine



What is a Virtual Machine?

A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. An operating system installed on a virtual machine is called a guest operating system.

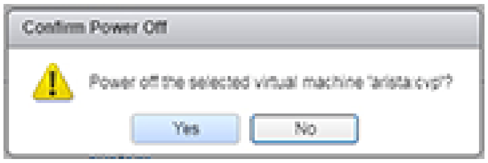
Because every virtual machine is an isolated computing environment, you can use virtual machines as desktop or workstation environments, as testing environments, or to consolidate server applications.

In vCenter Server, virtual machines run on hosts or clusters. The same host can run many virtual machines.

Power off the selected virtual machines.

4. Click to confirm powering off the virtual machine.

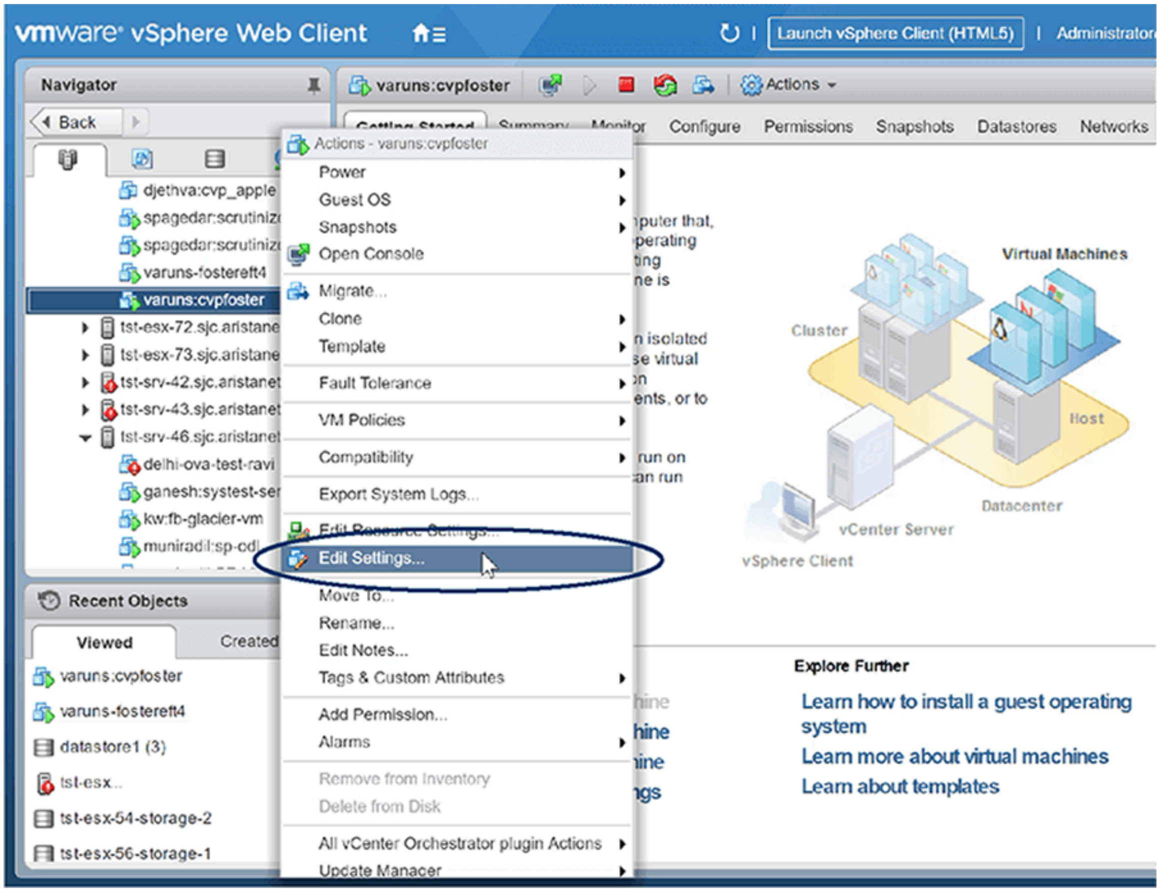
Figure 21-8: Powering off confirmation


Confirm Power Off

Power off the selected virtual machine "arista.cvp"?

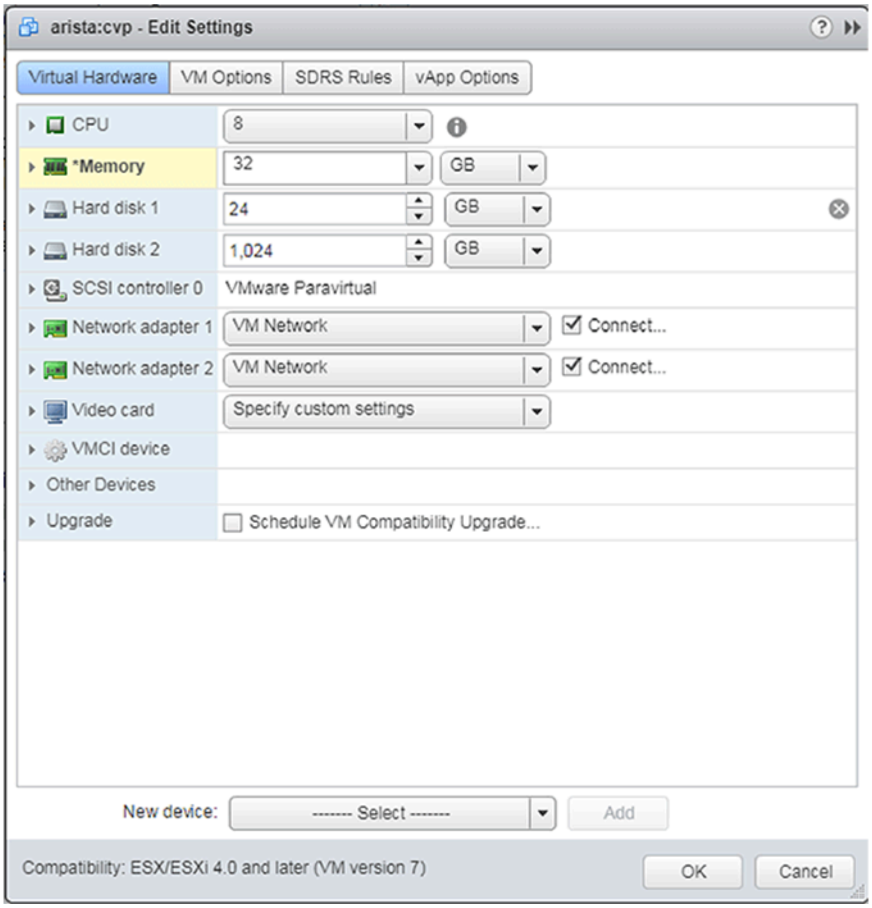
5. On the CVP node VM, increase the memory allocation to 32GB by right-clicking the node icon, and then choose **Edit Settings**.

Figure 21-9: Edit Settings



The **Edit Resource Settings** dialog appears.

Figure 21-10: Edit Resources Settings



CPU	8		
*Memory	32	GB	
Hard disk 1	24	GB	
Hard disk 2	1,024	GB	
SCSI controller 0	VMware Paravirtual		
Network adapter 1	VM Network	☑ Connect...	
Network adapter 2	VM Network	☑ Connect...	
Video card	Specify custom settings		
VMCI device			
Other Devices			
Upgrade	□ Schedule VM Compatibility Upgrade...		

New device: ------- Select ------- Add

Compatibility: ESX/ESXi 4.0 and later (VM version 7)

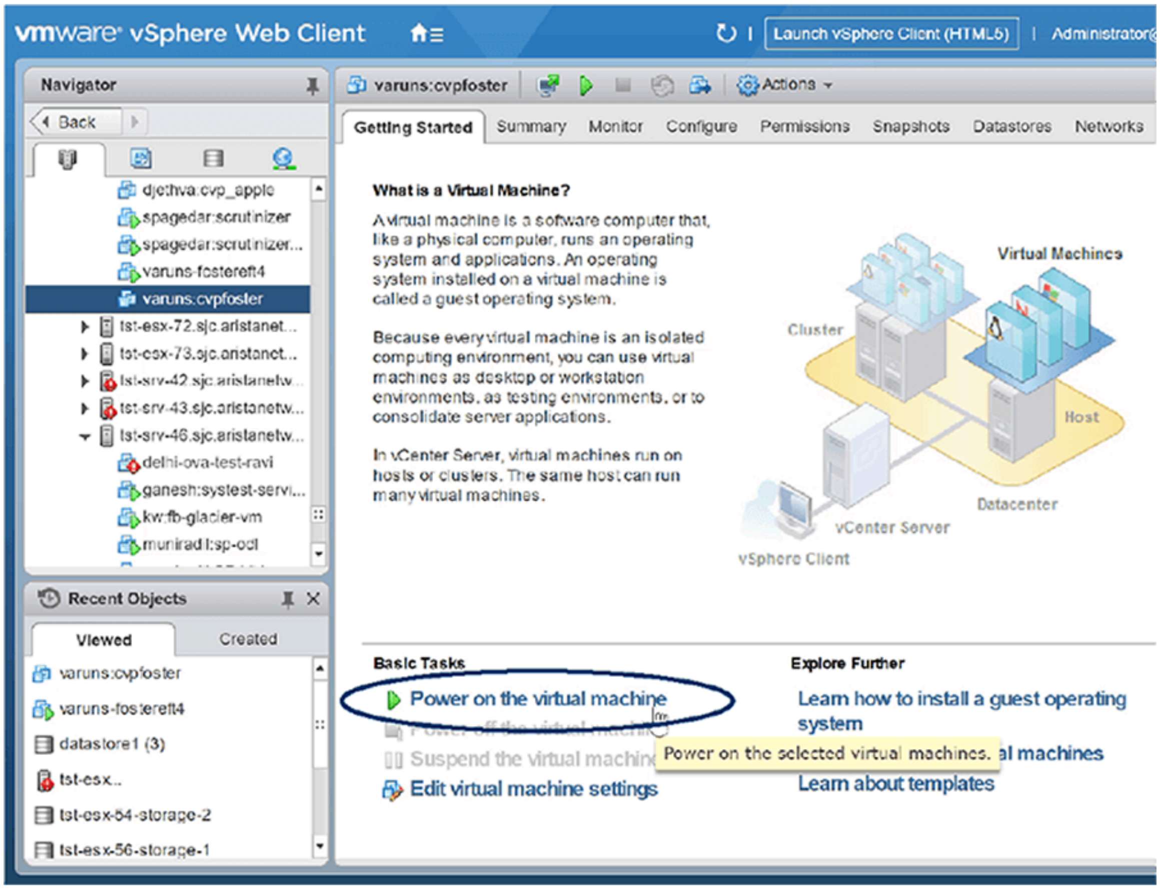
6. Do the following to increase the memory allocation for the CVP node VM:

- Using the **Memory** option, click the up arrow to increase the size to **32GB**.
- Click the **OK** button.

The memory allocation for the CVP node VM is changed to 32GB. The page refreshes, showing options to power on the VM or continue making edits to the VM properties.

7. Click the **Power on the virtual machine** option.

Figure 21-11: Power on the virtual machine



What is a Virtual Machine?

A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. An operating system installed on a virtual machine is called a guest operating system.

Because every virtual machine is an isolated computing environment, you can use virtual machines as desktop or workstation environments, as testing environments, or to consolidate server applications.

In vCenter Server, virtual machines run on hosts or clusters. The same host can run many virtual machines.

Power on the selected virtual machines.

8. Wait for the cluster to reform.
9. Once the cluster is reformed, repeat **step 1 through step 7** one node at a time on each of the remaining CVP node VMs in the cluster.

Related topics:

- System Recovery
- Health Checks