CloudVision as-a-Service (CVaaS) Quick Start Guide

Arista Networks

www.arista.com

April 2021

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

Contents

1 CloudVision as-a-Service

CloudVision as-a-Service is an SaaS-based delivery for the Arista CloudVision management plane platform offering modern telemetry and analytics, network-wide automation, and orchestration. As a complement to the on-premises offering, the CloudVision as-a-Service platform offers cloud-based onboarding and feature delivery, using secure state-streaming to an Arista managed cloud-native architecture.

This document is intended to be a quick start guide for customers who seek to onboard to the CloudVision as-a-Service platform.

1.1 Onboarding at a Glance

Use the following steps and checklist to simplify the onboarding process.

1. Configure the CloudVision as-a-Service specific information in the respective authentication provider portal.
2. Log into the CloudVision as-a-Service using the provided Invitation URL.
3. Onboard an Authentication Provider.
4. Onboard Users.
5. Onboard EOS Devices.

Table 1: Checklist

	Checklist Item	Description
User Onboarding Prerequisites	Configure the CloudVision Service specific information in the authentication system.	Use the following information to provision the CloudVision as-a-Service in the supported authentication system. • Authorized origin: ***https://www.arista.io*** • Authorized callback URL: ***https://www.arista.io/api/v1/oauth***
	Invitation URL	Arista will provide you an invitation URL. **Valid for only 48 hours.**
	Authentication Details	For Google and Microsoft, no additional details are needed. For OneLogin, Okta, and other OAuth providers, please refer to the Authentication Details section.
Device Onboarding Prerequisites	EOS 4.20+	
	TerminAttr 1.11.1+	

	Checklist Item	Description
	Connectivity Requirements: Port 443 access to apiserver.arista.io:443	Refer to the Connectivity Details section for more information.

1.2 User Onboarding Prerequisites

Invitation URL

Use the Invitation URL provided by Arista for the initial login to the CloudVision as-a-Service. Note that this URL will only be accessible for up to 48 hours. Make sure to complete the authentication provider onboarding and user onboarding for the administrator account before the Invitation URL expires.

Note: If the invitation URL expires, please send an email to: cvaas-onboarding@arista.com

Authentication Details

Your OAuth administrator will need to configure CloudVision as-a-Service using the following OAuth information in their respective auth provider portal:

- Authorized origin: **https://www.arista.io**
- Authorized callback URL: **https://www.arista.io/api/v1/oauth**

For Okta, OneLogin and other OAuth providers, the following three pieces of information are required for successful CloudVision Service onboarding:

- OAuth Endpoint
- ClientID
- ClientSecret

Please refer to the respective OAuth provider documentation on how to obtain this information.

1.3 User Onboarding Workflow

Onboarding Authentication Providers

1. Once the CloudVision as-a-Service instance is set up, access the CloudVision Service using the provided **Invitation URL**.
2. Select a preferred authentication provider from the list.

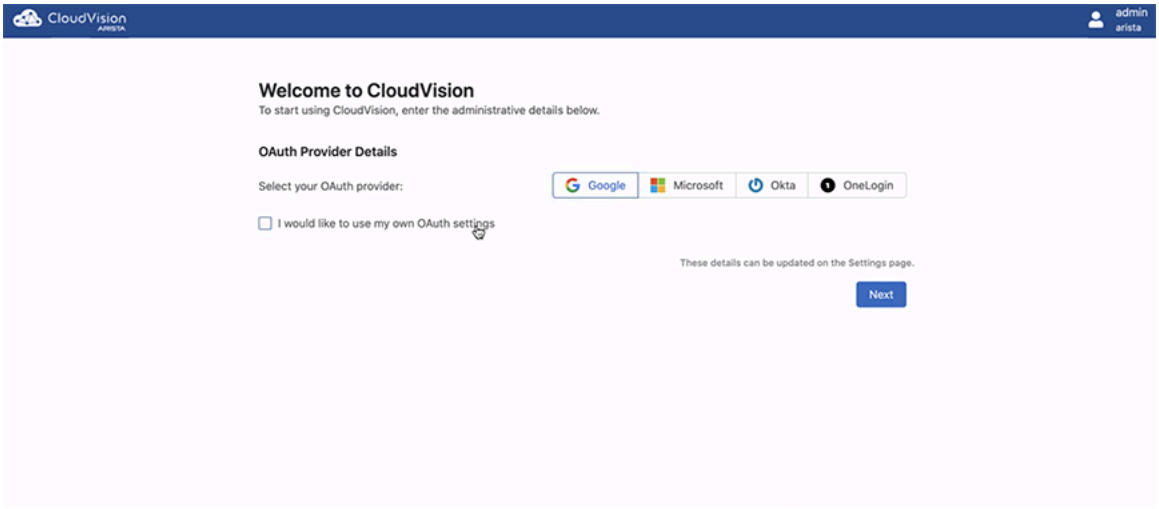

Figure 1: Welcome Screen - Select Preferred Authentication Provider

3. For Okta, OneLogin & other authentication methods, please fill out the **Endpoint/ClientID** and **ClientSecret** information.

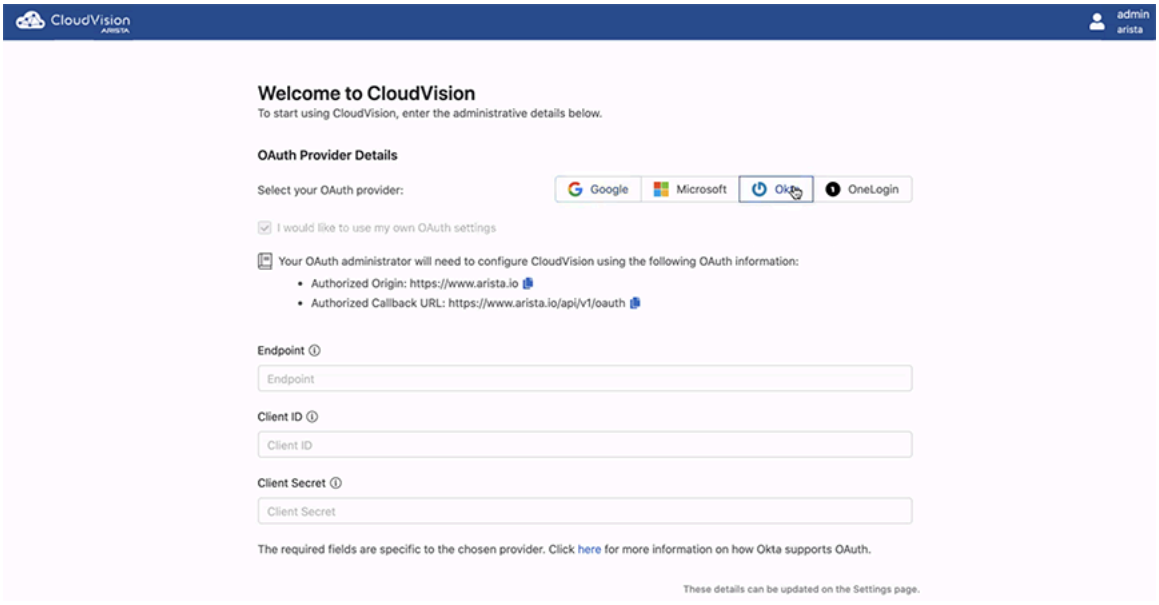

Figure 2: Provider Details

Note: To make changes to authentication providers after the initial onboarding process, navigate to **Access Control** > **Providers** and select the **Add Provider** button.

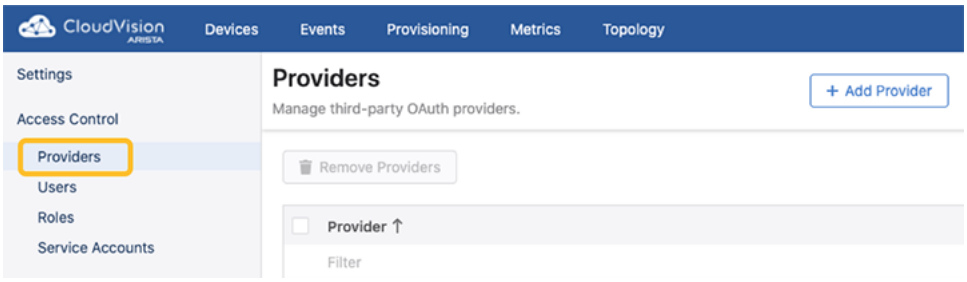

Figure 3: Access Control - Providers

Onboarding User Accounts

After the authentication provider is set up, add the admin user account in the User Information screen.

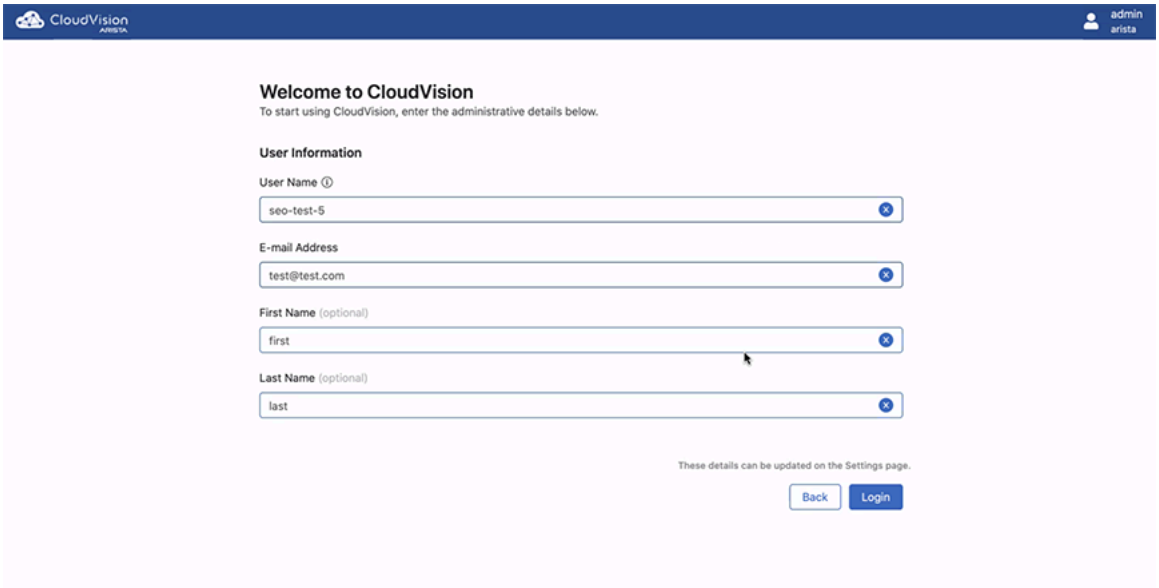

Figure 4: User Information Screen

Note: To make changes or add new users to CloudVision after the initial on-boarding, navigate to **Access Control** > **Users** under the CloudVision Settings.

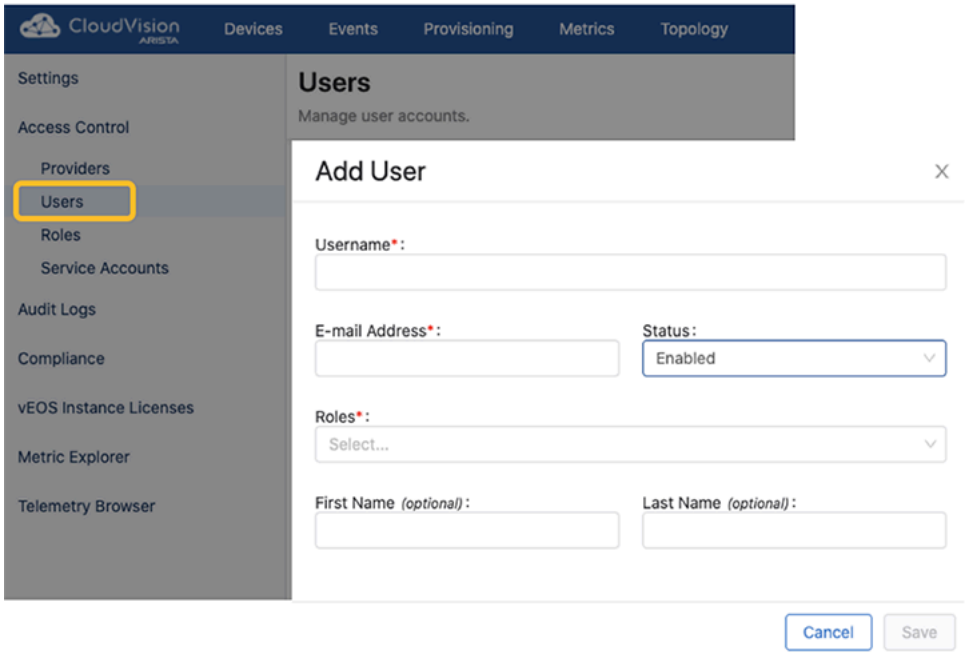

Figure 5: Add User

Login to CloudVision

1. After selecting **Finish** you will get redirected to https://arista.io.
2. Enter the name of the *Organization* that was provided during the initial cluster setup. You can find the organization name in the welcome email.
3. Select the provider and login using the user account created in the previous section.

Figure 6: CloudVision Login

1.4 Device Onboarding Prerequisites

Software Requirements

Current minimum software requirements are:

- EOS 4.20+
- TerminAttr 1.11.1+ (TerminAttr is the Streaming Telemetry Agent that is responsible for streaming the telemetry data to the CloudVision Service.)

Software can be downloaded from: https://www.arista.com/en/support/software-download. Streaming Telemetry Agent is available under the **CloudVision** -> **CloudVision Portal**:

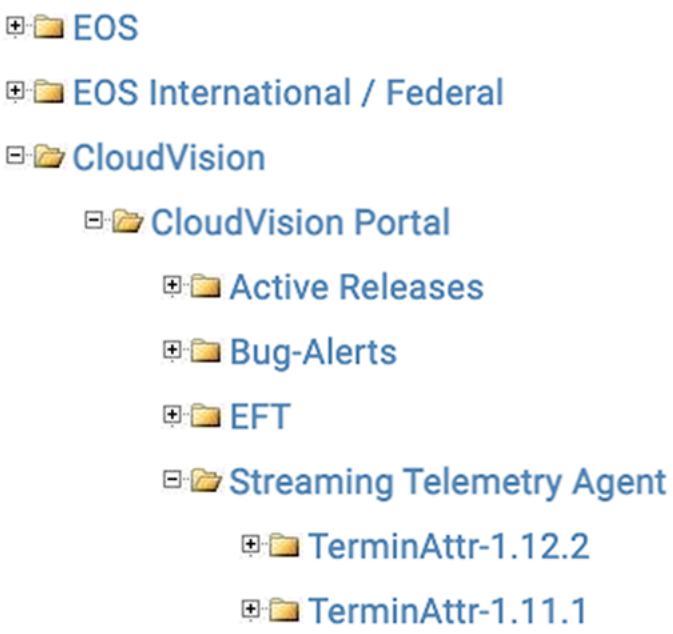

Figure 7: Software Download

Connectivity Requirements

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

Verify connectivity to CloudVision Service using the curl command:

```
HQ-DC-leaf1#bash
[admin@HQ-DC-leaf~]$ curl apiserver.arista.io:443
curl: (52) Empty reply from server
```

Troubleshooting

1. Verify proper DNS resolution:

```
HQ-DC-leaf1#bash nslookup apiserver.arista.io
NOTE: If this is unsuccessful please check your DNS server
 configuration. If no DNS servers present please add the "ip name-
server" configuration as follows:
HQ-DC-leaf1(config)# ip name-server 8.8.8.8
```

2. If you have multiple VRFs configured, first change the VRF context:

```
[admin@HQ-DC-leaf~]$ sudo ip netns exec ns-MGMT curl apiserver.ari
sta.io:443
```

1.5 Device Onboarding Workflow

Onboarding Devices: Token-Based Authentication requires the following steps

1. Onboard devices
2. Create and use token for onboarding
3. Provision devices

Step 1: Onboard devices

To onboard the devices, navigate to: **Devices** -> **Inventory** -> **Add Devices** -> **Onboard Devices**

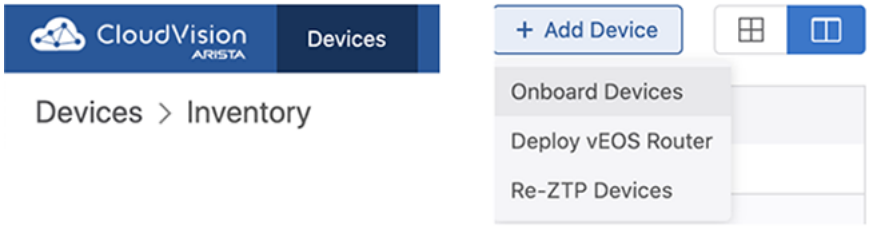

Figure 8: Onboard Devices

Step 2: Create and use token for onboarding

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

Note: The same token can be used to onboard multiple devices. CloudVision Service will use the device serial number to correctly identify the device.

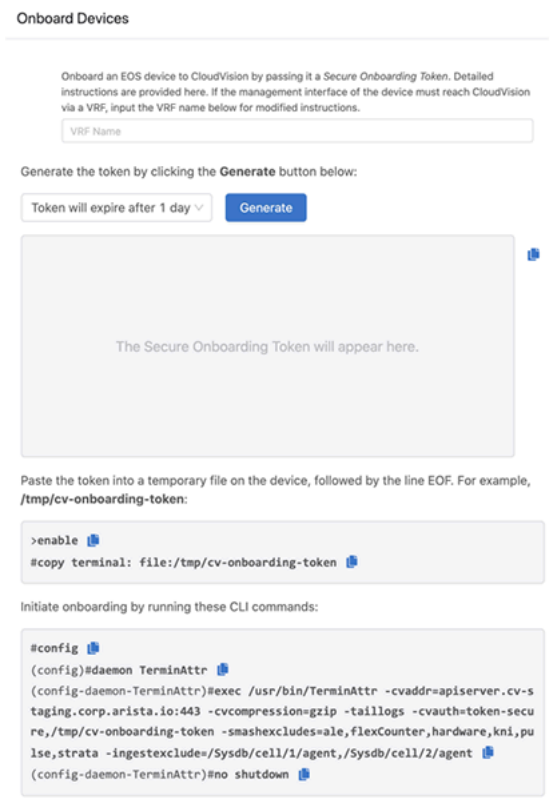

Figure 9: Generate a Token

Step 3: Provision devices

After successfully onboard the devices, they should appear under the **Devices** tab.

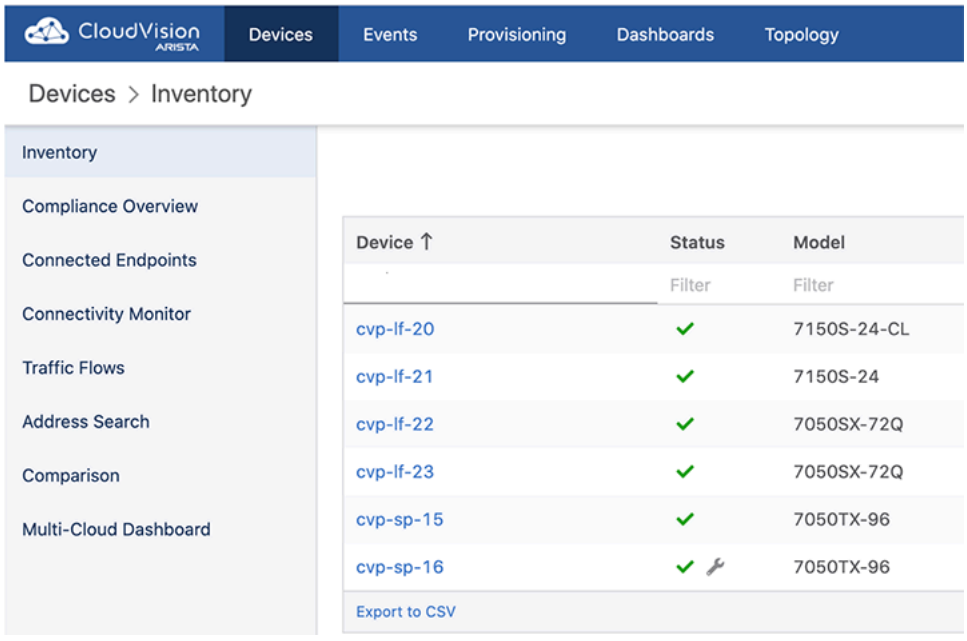

Figure 10: Devices - Inventory

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

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

For example: Assuming *john.smith@company.com* is the email address used to login to CloudVision as-a-Service you need to have *john.smith* as a user configured in the device (or in TACACS+ server):

```
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.

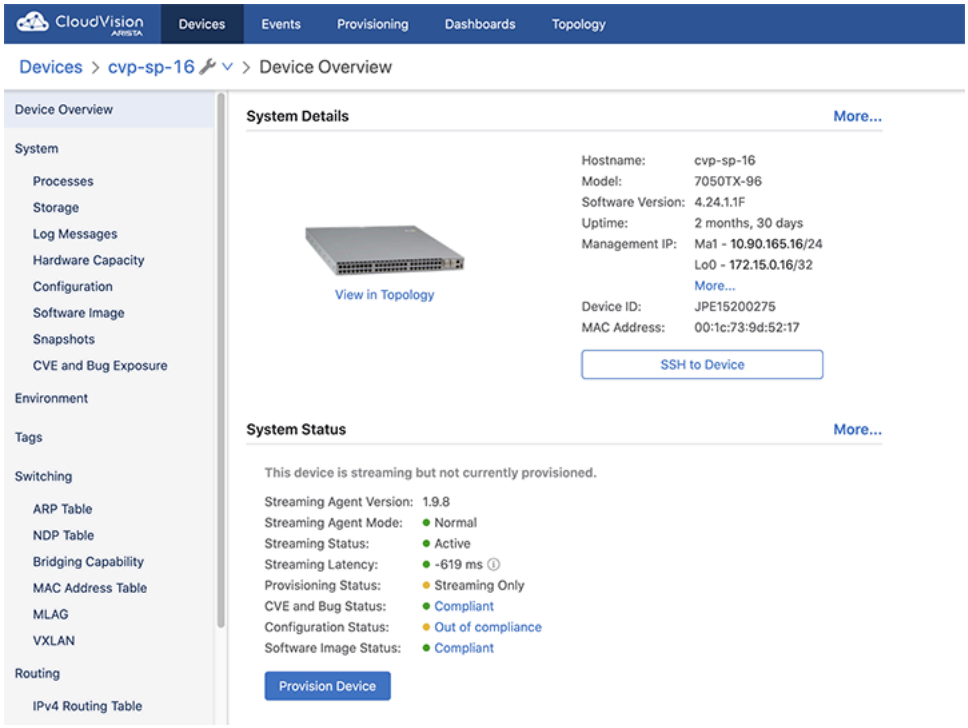

Figure 11: Device Overview

1.6 Troubleshooting

1.6.1 Troubleshooting Connectivity Issues

Verify connectivity to CloudVision Service

Verify connectivity to CloudVision Service using the curl command:

```
HQ-DC-leaf1#bash
[admin@HQ-DC-leaf~]$ curl apiserver.arista.io:443
curl: (52) Empty reply from server
```

If you have multiple VRFs configured, first change the VRF context:

```
[admin@HQ-DC-leaf~]$ sudo ip netns exec ns-MGMT
curl apiserver.arista.io:443
```

Verify proper DNS resolution

```
HQ-DC-leaf1#bash nslookup apiserver.arista.io
```

Note: If this is unsuccessful please check your DNS server configuration. If no DNS servers present please add the *ip name-server* configuration as follows:

```
HQ-DC-leaf1(config)# ip name-server 8.8.8.8
```

1.6.2 Troubleshooting Device Onboarding Issues

TerminAttr Agent Version issues

One of the common causes for Device Onboarding issues is the Streaming Telemetry agent (aka: TerminAttr agent) version incompatibilities. Please verify the switch TerminAttr agent version is greater than or equal to the supported agent version for CloudVision Service.

Other issues

- TerminAttr agent log files might provide additional information to enhance the troubleshooting process. You can access the TerminAttr logs using following command:

```
Switch-01#bash ls /var/log/agents/TerminAttr-*
/var/log/agents/TerminAttr-2223
Switch-01#bash cat /var/log/agents/TerminAttr-2223

===== Output from /usr/bin/TerminAttr ['-cvaddr=apiserver.cv-sta
ging.corp.arista.io:443', '-cvcompression=gzip', '-cvvrf=MGMT',
 '-taillogs', '-cvauth=token-secure,/tmp/cv-onboarding-token', '-
smashexcludes=ale,flexCounter,hardware,kni,pulse,strata', '-ingestexclu
de=/Sysdb/cell/1/agent,/Sysdb/cell/2/agent'] (PID=2223) started Mar 14
 21:01:03.638345 ===
I0314 21:01:03.666579    2223 libmain.go:94] TerminAttr Version:
 v1.13.3 go1.15.8 386
```

1.6.3 Troubleshooting Streaming Telemetry Latency Issues

NTP Issues: If the switch clock is too far off the actual timing, this can lead in to streaming latency related problems. Verify NTP settings using `show ntp status`.

To configure NTP use the command: `switch(config)#ntp server <vrf> <vrf-name> time.google.com`

https://www.arista.com/en/um-eos/eos-system-clock-and-time-protocols

1.6.4 Troubleshooting Switch Provisioning and Configuration Issues

If the **Provision Device** is failing, or if any configuration or change control actions are failing, please make sure the current user's user account that is used to login to the CloudVision as-a-Service exists in the EOS device.

For example: Assuming *john.smith@company.com* is the email address used to login to CloudVision as-a-Service you need to have *john.smith* as a user configured in the device (or in TACACS+ server):
`sw(config)#username john.smith privilege 15 <nopassword/secret>`

If you have TACACS+ configured for authentication, in order for CloudVision 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.

Following sample switch configuration shows how to configure commonly used CloudVision features such as **sflow/aaa-authentication**. Please refer to the EOS user manual (https://www.arista.com/en/um-eos/eos-overview) for more information.

```
!
daemon TerminAttr
   exec /usr/bin/TerminAttr -cvaddr=apiserver.customer1.corp.arista
.io:443 -cvcompression=gzip -cvvrf=MGMT <truncated>
   no shutdown
!
hostname Leaf-7050SX3-211
ip name-server vrf MGMT 10.240.48.6
!
ntp server vrf MGMT time.google.com
!
aaa authorization exec default local
!
username admin privilege 15 role network-admin secret <>
username john.smith privilege 15 role network-admin secret <>
!
vrf instance MGMT
!interface Management1
   vrf MGMT
   ip address 10.240.129.211/25
!
ip route vrf MGMT 0.0.0.0/0 10.240.129.129
!
!
sflow sample 16,384
sflow polling-interval 120
sflow destination 127.0.0.1
sflow source-interface Loopback0
sflow run
!
interface Loopback0
!
interface Management1
   vrf MGMT
   ip address 10.240.129.211/25
!
```

1.7 Automation with CloudVision as-a-Service

Generating a Service Account Token

In order to access the CloudVision as-a-Service and send API requests **Service Account Token** is needed. Navigate to the **Settings** -> **Access Control** -> **Service Accounts** to add a Service Account.

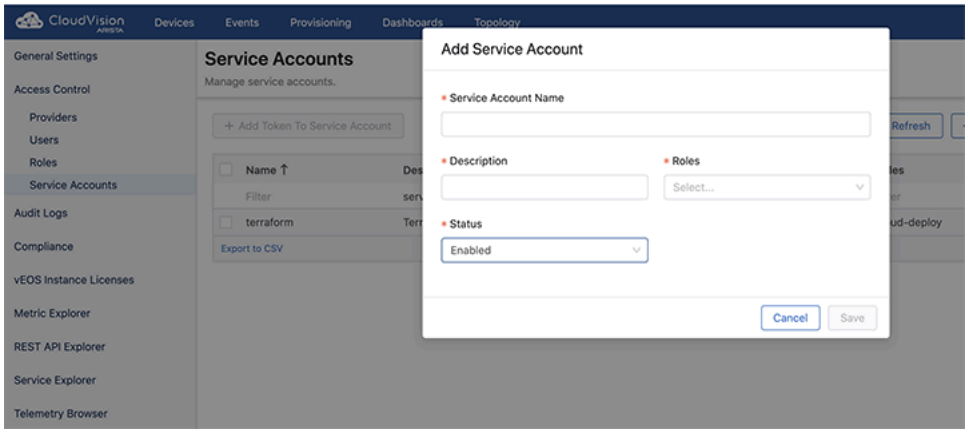

Figure 12: Add Service Account

Use the **Generate Service Account Token** section to create a new token by providing a description and an expiration date. This token can be used to send API calls to the CloudVision Service instance.

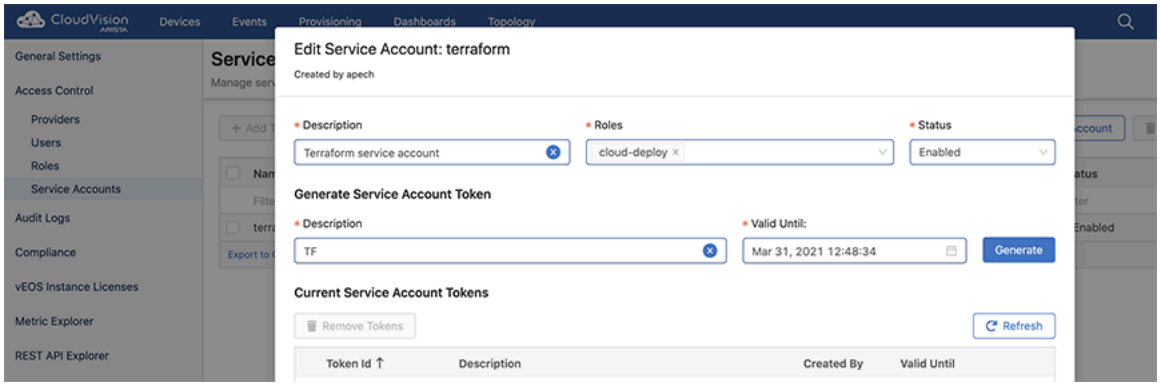

Figure 13: Edit Service Account Token

Note: The token will only be shown once. Make sure to copy this to a local file. During automation this token file will be used to send API calls to the CloudVision Service.

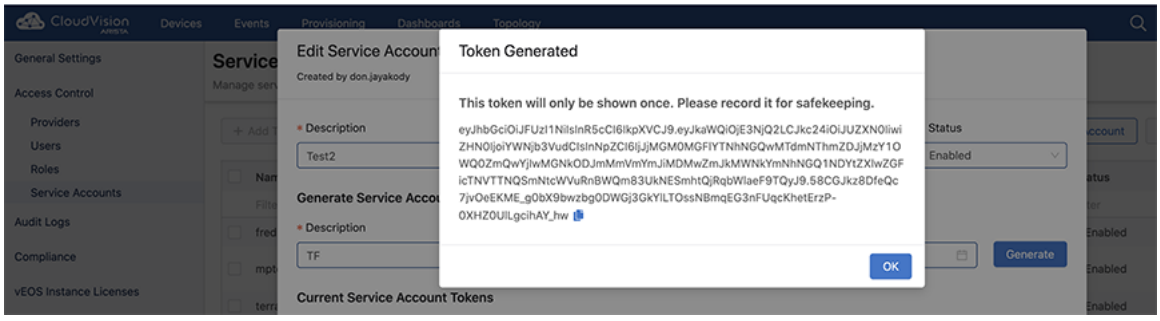

Figure 14: Token Generated

Accessing CloudVision Service REST API

You can access the CloudVision Service REST API swagger-ui by navigating to: **Settings** -> **REST API Explorer**.

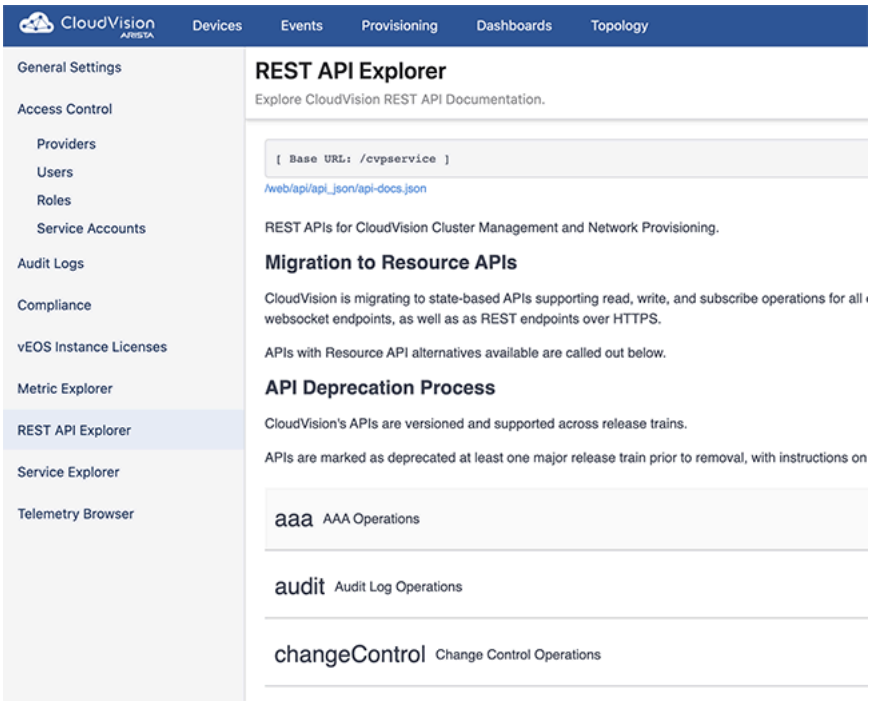

Figure 15: REST API Explorer

Sending API Calls

Using Curl

With the service account token you would be able to login properly & query the APIs:

Note: For this example create a file called *token* and copy & paste the service account token in there.

```
bash-3.2$ curl -X GET --header 'Accept: application/json'
'https://www.cv-staging.corp.arista.io/cvpservice/configlet/getC
onfigletByName.do?name=CloudTracer'
-b access_token=`cat token`
{"key":"configlet_843806b0-a015-491b-af2b-12486a38d05f","name":"CloudTr
acer"}
```

Using Python

Python based CVPRAC module (https://github.com/aristanetworks/cvprac) provides a REST API client for Cloudvision. Install CVPRAC using **pip** or directly from the source as described in the Installation section. To send API calls to the CloudVision Service using CVPRAC module set the **is_cvaas** option to **True** as follows.

Note: Token is needed to send API calls to the CloudVision Service. Obtain a token using a Service Account as shown in the previous section.

```
>>> from cvprac.cvp_client import CvpClient;
>>> clnt = CvpClient()
>>> clnt.connect(nodes=['www.cv-staging.corp.arista.io'], username='',
 password='',
is_cvaas=True, cvaas_token='eyJhbGciOi<truncated>')
```

```
>>> print(clnt.api.get_configlet_by_name('CloudTracer')){'key':
 'configlet_843806b0-a015-491b-af2b-12486a38d05f', 'name': 'CloudTracer',
 'reconciled': False, 'config': 'monitor connectivity\n host aws-us-
east-1\n
ip 52.216.227.10\n, <truncated> 'typeStudioConfiglet': False}
```

Using Ansible

Starting with the release 2.1.1 Ansible CVP supports CloudVision as-a-Service.

CloudVision Ansible bundle can be downloaded from here: https://github.com/aristanetworks/ansible-cvp. To authenticate with a CloudVision as-a-Service instance update the authentication steps as follows:

```
# Default Ansible variables for authentication
ansible_host: < IP address or hostname to target >
ansible_user: cvaas # Shall not be changed. ansible will switch to cvaas
 mode
ansible_ssh_pass: < User token to use to connect to CVP instance >
ansible_connection: httpapi
ansible_network_os: eos
```

For additional details please refer to: https://github.com/aristanetworks/ansible-cvp/pull/235

1.8 CloudVision as-a-Service Support

If you require any assistance during the onboarding process please reach out to cvaas-onboarding@arista.com. For other support related questions please contact support@arista.com.