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

Arista Networks

www.arista.com

May 2022
<table>
<thead>
<tr>
<th>Headquarters</th>
<th>Support</th>
<th>Sales</th>
</tr>
</thead>
<tbody>
<tr>
<td>5453 Great America Parkway</td>
<td>+1 408 547-5502</td>
<td>+1 408 547-5501</td>
</tr>
<tr>
<td>Santa Clara, CA 95054</td>
<td>+1 866 476-0000</td>
<td>+1 866 497-0000</td>
</tr>
<tr>
<td>USA</td>
<td><a href="mailto:support@arista.com">support@arista.com</a></td>
<td><a href="mailto:sales@arista.com">sales@arista.com</a></td>
</tr>
<tr>
<td>+1 408 547-5500</td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="http://www.arista.com">www.arista.com</a></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© Copyright 2022 Arista Networks, Inc. All rights reserved. The information contained herein is subject to change without notice. The trademarks, logos and service marks ("Marks") displayed in this documentation are the property of Arista Networks in the United States and other countries. Use of the Marks are subject to Arista Network’s Term of Use Policy, available at [www.arista.com/en/terms-of-use](http://www.arista.com/en/terms-of-use). Use of marks belonging to other parties is for informational purposes only.
Contents

1 CloudVision as-a-Service ................................................................................................. 1
  1.1 Onboarding at a Glance ............................................................................................... 1
  1.2 Checklist ..................................................................................................................... 1
  1.3 User Onboarding Prerequisites ................................................................................... 3
    1.3.1 Invitation URL ....................................................................................................... 3
    1.3.2 Authentication Details .......................................................................................... 5
  1.4 User Onboarding Workflow ......................................................................................... 7
    1.4.1 Onboarding Authentication Providers .................................................................. 8
    1.4.2 Onboarding User Accounts ................................................................................ 13
    1.4.3 Login to CloudVision .......................................................................................... 14
  1.5 Device Onboarding Prerequisites ............................................................................... 15
    1.5.1 Software Requirements ....................................................................................... 15
    1.5.2 Connectivity Requirements .................................................................................. 16
  1.6 Device Onboarding Workflow ..................................................................................... 17
    1.6.1 Onboarding Devices: ZTP as-a-Service ............................................................... 17
    1.6.2 Onboarding Devices: Token-Based Authentication ............................................. 21
  1.7 Connecting CloudVision Wifi Tenant ......................................................................... 24
  1.8 Troubleshooting ........................................................................................................ 26
    1.8.1 Troubleshooting Connectivity Issues ..................................................................... 26
    1.8.2 Troubleshooting Device Onboarding Issues ........................................................ 27
    1.8.3 Troubleshooting Streaming Telemetry Latency Issues ......................................... 27
    1.8.4 Troubleshooting Switch Provisioning and Configuration Issues .......................... 28
  1.9 Automation with CloudVision as-a-Service ............................................................... 29
  1.10 CloudVision as-a-Service Support ......................................................................... 32
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.

1.2 Checklist

<table>
<thead>
<tr>
<th>Checklist Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User Onboarding Prerequisites</strong></td>
<td></td>
</tr>
<tr>
<td>Configure the CloudVision Service specific information in the authentication system.</td>
<td>Use the following information to provision the CloudVision as-a-Service in the supported authentication system.</td>
</tr>
<tr>
<td>• Authorized origin: <strong><a href="https://www.arista.io">https://www.arista.io</a></strong></td>
<td></td>
</tr>
<tr>
<td>• Authorized callback URL: <strong><a href="https://www.arista.io/api/v1/oauth">https://www.arista.io/api/v1/oauth</a></strong></td>
<td></td>
</tr>
<tr>
<td>Invitation URL</td>
<td>Arista will provide you an invitation URL. <strong>Valid for only 48 hours.</strong></td>
</tr>
<tr>
<td>Authentication Details</td>
<td>For Google and Microsoft, no additional details are needed. For OneLogin, Okta, and other OAuth providers, please refer to the Authentication Details section.</td>
</tr>
<tr>
<td><strong>Device Onboarding Prerequisites</strong></td>
<td></td>
</tr>
<tr>
<td>EOS 4.22+</td>
<td></td>
</tr>
<tr>
<td>TerminAttr 1.15.3+</td>
<td></td>
</tr>
<tr>
<td>Checklist Item</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Connectivity Requirements: Port 443 access to apiserver.arista.io &amp; <a href="http://www.arista.io">www.arista.io</a></td>
<td>Refer to the Connectivity Details section for more information.</td>
</tr>
<tr>
<td>Valid NTP server configuration</td>
<td>To configure NTP use the following command:</td>
</tr>
<tr>
<td></td>
<td>switch(config)#ntp server &lt;vrf&gt; &lt;vrf-name&gt; &lt;ntp server&gt;</td>
</tr>
</tbody>
</table>

**ZTP as-a-Service Prerequisites**

For User-Generated Token with USBKey or Bootstrap Script:
- EOS-4.25.5 or
- EOS-4.26.1

No platform dependency for the USB Key and Bootstrap Script method. Supported in all Hardware Platforms.

For Embedded Token Support:
- EOS-4.26.1

Supported with specific platforms. Please refer to the Platform-Specific Feature Set Guide.
1.3 User Onboarding Prerequisites

1.3.1 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 reach out to cvaas-onboarding@arista.com or if urgent please contact Arista TAC.
Organizations that have a user registered within CloudVision as-a-Service, can use the new self-service feature to obtain an invitation link, if they have forgotten their password.

Figure 1: Request Invitation Link

**Request Invitation Link**

Request an invitation link to access CloudVision to be sent to your email address by filling out the information below.

The provided email address must be associated with a user registered with your organization.

If you encounter any issues, please contact [Arista TAC](#).

**Organization Name**

[Input field]

**Email Address**

[Input field]

[Submit] [Cancel]

Figure 2: CloudVision Login

**CloudVision Login**

**Organization**

<Your Organization> [Enter]

If you are unable to login and already have an account with your organization or are the registered administrator for this cluster, you can request an invitation link [here](#).

To create an account within your organization, contact your network administrator.

If your organization is new to CloudVision, sign up [here](#).
1.3.2 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.

For more detailed information please refer to: https://www.arista.com/en/support/toi/cvp-2021-2-0/14834-aaa-providers-oauth-and-saml-support
1.4 User Onboarding Workflow
1.4.1 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 3: Welcome Screen - Select Preferred Authentication Provider*
3. For Okta, OneLogin & other authentication methods, please fill out the **Endpoint/ClientID** and **ClientSecret** information.

**Figure 4: Provider Details**

![OAuth Provider Details](image)

- **Select your OAuth provider:**
  - Google
  - Microsoft
  - Okta
  - OneLogin

- **Endpoint**

- **Client ID**

- **Client Secret**

- **Your OAuth administrator will need to configure CloudVision using the following OAuth information:**
  - **Authorized Origin:** https://www.okta.com
  - **Authorized Callback URL:** https://www.okta.com/api/v1/oauth

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

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

**Figure 5: Access Control - Providers**

![Access Control Providers](image)
1.4.1.1 Onboarding SAML Providers

Use the following procedure to add a SAML provider.

1. Get the CloudVision specific SAML metadata from your cluster by going to a URL: https://www.arista.io/api/v1/saml_sp_metadata

   **Note:** To download this file you need to either already be logged into the CloudVision cluster or access the cluster through the Invitation URL.

2. In the metadata, you will need the **entityID** at the top of the file and the **Location** at the bottom of the file when configuring your SAML provider.

   **Figure 6: Metadata**

   ```xml
   <EntityDescriptor
     xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
     version="2.0"
     id="entityID"
     issueInstant="2012-07-06T14:36:01Z"
     metadataLocation="https://www.arista.io/api/v1/saml_sp_metadata">
     <KeyDescriptor
       xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
       use="signing"/>
     <KeyDescriptor
       xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
       use="encryption"/>
     <SPSSODescriptor
       xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
       ID="spID"
       version="2.0"
       Service">
     </SPSSODescriptor>
   </EntityDescriptor>
   
   <IdentityProviderDescriptor
     xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
     service="assertionConsumerService"
     binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
     location="/api/v1/saml legislators">"title"=""</IdentityProviderDescriptor>
   </EntityDescriptor>

3. Proceed with your organization’s SAML provider configuration. Refer to the SAML provider documentation for further information. Use the **Location** URL and **entityID** URLs obtained in Step 2 to complete the registration process.

   For Example: In Octa fill out Single sign on URL with the **Location** URL and the Audience URL (SP Entity ID) with the **entityID** URL.

4. Gather the **Identity Provider metadata** from your SAML Provider configuration. You will need this information in the next step when setting up the SAML provider in CloudVision.

5. Navigate to **Access Control > Providers**. To add a new SAML provider, click the **Add SAML Provider** button.

   **Figure 7: Providers**
6. Fill out the other necessary information (from Step 4) to onboard the SAML provider.

**Figure 8: Add SAML Provider**

Please refer to the respective OAuth Provider documentation for specific details. Some examples can be found here: [https://www.arista.com/en/support/toi/cvp-2021-2-0/14834-aaa-providers-oauth-and-saml-support](https://www.arista.com/en/support/toi/cvp-2021-2-0/14834-aaa-providers-oauth-and-saml-support)

**Note:** To make changes to authentication providers after the initial onboarding process navigate to **Access Control > Providers** under the CloudVision Settings.

**Figure 9: Access Control - Providers**

### 1.4.1.2 Arista Provided SAML Provider

Customers can request an Arista provided SAML provider if they do not have a SSO provider in the organization. An SSO Provider is mandatory for CloudVision Service login, no local login option is supported.
You can request an Arista Provided SAML provider option called “Launchpad” through your Arista account representative.

Once you have the Launchpad authentication configured, you can configure Launchpad as a provider:

Please use the following settings to configure Launchpad as a SAML provider:

- **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
1.4.2 Onboarding User Accounts

Once the authentication provider is set up, add the admin user account in the User Information screen. Make sure the email address matches with the email address maintained in the SSO.

Figure 10: User Information Screen

![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.

Note: Please note that IDP-initiated SAML SSO login is not supported. Login at www.arista.io.

Figure 11: Add User

![Add User Screen]
1.4.3 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 12: CloudVision Login**
1.5  Device Onboarding Prerequisites

Connectivity Requirements
EOS devices need to be able to connect to www.arista.io & apiserver.arista.io on port 443.

Verify connectivity to CloudVision Service using the Ncat command:

HQ-DC-leaf1#bash
[admin@HQ-DC-leaf~]$ nc -zv www.arista.io 443
Ncat: Version 7.50 ( https://nmap.org/ncat )
Ncat: Connected to 35.221.29.186:443.
Ncat: 0 bytes sent, 0 bytes received in 0.08 seconds.
[admin@HQ-DC-leaf~]$ nc -zv apiserver.arista.io 443

If you have multiple VRFs configured, change the VRF context. For eg. to change the VRF Context for a VRF named “MGMT”:

[admin@HQ-DC-leaf~]$ sudo ip netns exec ns-MGMT nc -zv www.arista.io 443

Troubleshooting
1. Verify proper DNS resolution:

HQ-DC-leaf1#bash
[admin@HQ-DC-leaf~]$ 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 nc -zv apiserver.arista.io 443

1.5.1  Software Requirements

Current minimum software requirements are:

• EOS 4.22+
• TerminAttr 1.15.3+ (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 13: Software Download

- EOS
- EOS International / Federal
- CloudVision
  - CloudVision Portal
    - Active Releases
    - Bug-Alerts
    - EFT
  - Streaming Telemetry Agent
    - TerminAttr-1.12.2
    - TerminAttr-1.11.1

1.5.2 Connectivity Requirements

EOS devices need to be able to connect to www.arista.io & apiserver.arista.io on port 443.

Verify connectivity to CloudVision Service using the Ncat command:

```
HQ-DC-leaf1#bash
[admin@HQ-DC-leaf~]$ nc -zv www.arista.io 443
Ncat: Version 7.50 (https://nmap.org/ncat)
Ncat: Connected to 35.221.29.186:443.
Ncat: 0 bytes sent, 0 bytes received in 0.08 seconds.
```

```
[admin@HQ-DC-leaf~]$ nc -zv apiserver.arista.io 443
```

If you have multiple VRFs configured, change the VRF context. For eg. to change the VRF Context for a VRF named “MGMT”:

```
[admin@HQ-DC-leaf~]$ sudo ip netns exec ns-MGMT nc -zv www.arista.io 443
```
1.6 Device Onboarding Workflow

Select the device onboarding option appropriate for your configuration:

- **Onboarding Devices: Zero Touch Provisioning (ZTP) as-a-Service**
  - ZTP as-a-Service: Using a USB Key
  - ZTP as-a-Service: Using a Bootstrap Script
  - Using Hardware Authentication with ZTP as-a-Service
- **Onboarding Devices: Token-Based Authentication**

1.6.1 Onboarding Devices: ZTP as-a-Service

Arista’s Zero Touch Provisioning is used to configure a switch without user intervention. Built to fully leverage the power of Arista’s Extensible Operating System (EOS), ZTP as-a-Service provides a flexible solution to onboard EOS devices into CloudVision as-a-Service.

**Requirements:**

- DHCP Server: EOS device should be able to reach arista.io by obtaining valid IP settings from a DHCP server
- EOS Version: The device should be running **EOS version 4.25.5 or 4.26.1** or newer.
- Permit ZTP in CloudVision as-a-Service Cluster: ZTP as-a-Service should be enabled in the CVaaS cluster via: **Provisioning > Zero Touch Provisioning > Manage Permitted Devices**

**Figure 14:** Zero Touch Provisioning: Manage Permitted Devices

**Note:** ZTP can be enabled globally for all devices or it can be managed per-device level using Serial Numbers.
• Add a compliance token required for ZTP:

Figure 15: Compliance Screen

- Navigate to the “Settings -> Compliance” section.
- Follow the link on the page to go to your arista.com dashboard and copy the token.
- Paste the token on the CVaaS Compliance page and click Save.

ZTP as-a-Service Options:

• Using a USB Key
• Using Bootstrap Script
• Using Embedded Token
• Using Hardware Authentication with ZTP as-a-Service

1.6.1.1 ZTP as-a-Service: Using a USB Key

A USB key can be used to provide the onboarding token and other information required for the ZTP process. Please follow the below steps to enable ZTP as-a-Service using a USB Key.

Step 1: Log in to the CloudVision as-a-Service cluster and generate a token using Devices > Onboard Devices > Generate.

Figure 16: Onboard Devices: Generate the Token

Generate the Token

Generate the token by clicking the Generate button below:

Token will expire after 1 week

Generate

The secure onboarding token will appear here.

Note: The same token can be used to onboard multiple devices. No need to generate multiple tokens.

Step-2: Prepare a USB key.
- Create a directory called `ztp` inside the USB.
- Copy the token generated in step-1 into a file named `token.tok` in `ztp` directory.
- Create a file named `ztpConfig.yaml` (`ztp/ztpConfig.yaml`) and add the following content:

The configuration (`/mnt/usb1/ztp/ztpConfig.yaml`) should look like this:

```yaml
bootstrapUrl: 'https://www.arista.io/ztp/bootstrap'
serverCaCertificate: ../../../etc/pki/tls/certs/ca-bundle.crt
enrollmentToken: token.tok
version: '1.0'
```

**Note:** Please use the following regional CVaaS URLs for the bootstrap field depending on your specific CVaaS region:

- **US:** https://www.arista.io/ztp/bootstrap
- **EU:** https://www.cv-prod-euwest-2.arista.io/ztp/bootstrap
- **JP:** https://www.cv-prod-apnortheast-1.arista.io/ztp/bootstrap
- **AU:** https://www.cv-prod-ausoutheast-1.arista.io/ztp/bootstrap

**Step-3:** Setup a DHCP server to serve routable IP settings (Note: Device should be able to reach `apiserver.arista.io`).

Example configuration for DHCPD:

```bash
subnet 10.10.10.128 netmask 255.255.255.128 {
    range 10.10.10.170 10.10.10.185;
    option domain-name "test.aristanetworks.com";
    option routers 10.10.10.129;
    option domain-name-servers 10.10.10.6;
    option ntp-servers time.google.com;

    host Switch-01 {
        hardware ethernet 94:8e:11:22:02:33;
        fixed-address 10.10.10.181;
        option host-name "Switch-01";
        option bootfile-name "tftp://none";
    }
}
```

**Step-4:** Plug in the USB to the EOS device and boot up into the ZTP provisioning mode. (The USB key will be mounted on the `/mnt/usb1` directory).

**Note:** If the device is not in the ztp mode delete the following files and reboot: `rm /mnt/flash/startup-config` & `rm /mnt/flash/zerotouch-config`

At this point, the ZTP process should begin and the device should show up under the **Provisioning > Zero Touch Provisioning**.

**Step-5:** Once properly registered the device should also show up in the **Undefined Container** on the Network Provisioning page. Move the device into a named container and apply appropriate configlets. After submitting the change control the device should reboot and complete the ZTP as-a-Service process.

**Note:** Same USB key and token can be used to onboard multiple EOS devices. Make sure the token has not expired before proceeding.

### 1.6.1.2 ZTP as-a-Service: Using a Bootstrap Script

ZTP as-a-Service can be enabled via a custom bootstrap script and using a DHCP server option to point to that bootstrap script. This method is an alternative to the previously mentioned USB method and might be more appropriate when onboarding a large number of devices.
Please follow the below steps to enable ZTP as-a-Service using a Bootstrap Script.

**Step-1:** Log in to the CloudVision as-a-Service cluster and generate a token using Devices > Onboard Devices > Generate.

**Step-2:** Prepare a bootstrap script and host it on an HTTP server. A sample script can be obtained by through: https://github.com/aristanetworks/cloudvision-ztpaas-utils

**Note:** If you are using a Windows machine, please watch out for the unnecessary characters when downloading this file. To troubleshoot whether unwanted characters are presented in the downloaded bootstrap script file, login to the switch bash prompt and open the file using: vi / tmp/zt-download command.

Make sure to provide the updated token information and other information in the bootstrap script.

For example:

```
############## USER INPUT ##############
cvAddr = "www.cv-staging.corp.arista.io"
enrollment_token = "eyJhbGciOiJSUzI1Nixxx..."
############## USER INPUT ##############
```

**Step-3:** Direct the DHCP server to point to the bootstrap script via option-67/bootfile-name option:

For example:

```
subnet 10.10.1.1 netmask 255.255.255.0 {
  range 10.10.1.1 10.10.1.253;
  option domain-name "dev.aristanetworks.com";
  option routers 10.10.1.250;
  option domain-name-servers 10.10.1.5;
  option ntp-servers time.google.com;

  host leaf-1A {
    hardware ethernet fc:bd:67:aa:22:33;
    fixed-address 10.10.1.180;
    option host-name "leaf-1A";
    option bootfile-name "http://10.10.1.10:8000/bootstrap.py";
  }
}
```

**Step-3:** Boot up the EOS device into ZTP provisioning mode.

At this point, the ZTP process should begin and the device should be displayed in Provisioning > Zero Touch Provisioning.

**Step-4:** Once properly registered the device should also show up in the Undefined Container on the Network Provisioning page. Move the device into a named container and apply appropriate configlets. After submitting the change control the device should reboot and complete the ZTP as-a-Service process.

**Note:** Same bootstrap script and token can be used to onboard multiple EOS devices. Make sure the token has not expired before proceeding.

### 1.6.1.3 ZTP as-a-Service: Using Embedded Token

For newer EOS devices which have the embedded token support, ZTP as-a-Service can be performed by configuring the DHCP server to provide the bootstrap URL.

**Note:** EOS version should be 4.26.1 or newer.

**Note:** For devices that have the Embedded Token support please refer to the Platform-Specific Feature Set Guide (ZTP Platform support for CloudVision as-a-Service).
You can use following command to verify whether the device has the Embedded token support:

```
Leaf-1A#show hardware eeprom
<truncated>
ZtpToken: xxxx
```

According to your specific CVaaS region please use the following regional CVaaS URLs in the DHCP server bootfile-name option (Option-67).

- **US**: https://www.arista.io/ztp/bootstrap
- **EU**: https://www.cv-prod-euwest-2.arista.io/ztp/bootstrap
- **JP**: https://www.cv-prod-apnortheast-1.arista.io/ztp/bootstrap
- **AU**: https://www.cv-prod-ausoutheast-1.prod.arista.io/ztp/bootstrap

**Example:**

```
subnet 10.10.1.1 netmask 255.255.255.0 {
  range 10.10.1.1 10.10.1.253;
  option domain-name "dev.aristanetworks.com";
  option routers 10.10.1.250;
  option domain-name-servers 10.10.1.5;
  option ntp-servers time.google.com;

  host leaf-1A {
    hardware ethernet fc:bd:67:aa:22:33;
    fixed-address 10.10.1.180;
    option host-name "leaf-1A";
    option bootfile-name "https://www.arista.io/ztp/bootstrap";
  }
}
```

**Note:** By default, a device will be mapped to the primary CVaaS tenant of the customer. For customers that have multiple CVaaS tenants, in order to update the device to tenant mapping for a device please create a support ticket.

### 1.6.1.4 Using Hardware Authentication with ZTP as-a-Service

During ZTP as-a-Service using both USB & Bootstrap Script methods, it is possible to enable an additional layer of authentication using the **Hardware Authentication** feature. EOS devices should have a Trusted Platform Module (TPM) chip onboard for Hardware Authentication to work. Hardware authentication can be enabled globally (for all the devices) or on a per-device basis.

To enable Hardware Authentication, navigate to the **Provisioning > Zero Touch Provisioning > Manage Permitted Devices**.

### 1.6.2 Onboarding Devices: Token-Based Authentication

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 17: 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 18: Generate a Token

Onboard Devices

Onboarding an OUI device to CloudVision by passing it a Secure Onboarding Token. Detailed instructions are provided here. If the management interface of the device must reach CloudVision via a VIP, input the VIP name below for modified instructions.

VIP Name

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, followed by the line EOF. For example, /tmp/cv-onboarding-token:

```
#enable
#copy terminal: file:/tmp/cv-onboarding-token
```

Initiate onboarding by running these CLI commands:

```
```
```
Step 3: Provision devices

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

**Figure 19: 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 20: Device Overview

1.7 Connecting CloudVision Wifi Tenant

To connect your CloudVision Wifi tenant to CloudVision as a Service, to enable wifi visibility within CloudVision as a Service you must create a new key within the administrative section of the wifi portal. This enables viewing of the Wifi devices in Compliance view, Device view and Topology.

Provisioning and management of wifi devices must be done on the Wifi portal.

Instructions:

1. Go to your Launchpad portal, and navigate Admin, then click on New Key.

2. Create your key and save the Key ID and Value.
3. Go to CloudVision Service (Arista.io) and log in. Click the settings wheel on the upper right side of the screen. In General settings, you can add the Wifi Cloud Connector.

   a. Click the settings wheel upper right.
   b. Click the settings wheel upper right and select the Wifi Cloud Connector configuration button.
   c. Input the URL, Key ID, and Value.
      - **URL**: launchpad.wifi.arista.com (do not include https:// or trailing /)
      - **KeyID**: from Launchpad
      - **Key Value**: from Launchpad.

   **Note**: Once the Key value has been saved in CloudVision, this field will show the encrypted value, if you need to add the key again, you must copy it from the LaunchPad portal.

   ![Figure 22: Launch Pad - Settings](image-url)
1.8 Troubleshooting

1.8.1 Troubleshooting Connectivity Issues

Verify connectivity to CloudVision Service

Verify connectivity to CloudVision Service using the Ncat command:

```
HQ-DC-leaf1# bash
[admin@HQ-DC-leaf~]$ nc -zv apiserver.arista.io 443
Ncat: Version 7.50 ( https://nmap.org/ncat )
Ncat: Connected to 35.221.29.186:443.
Ncat: 0 bytes sent, 0 bytes received in 0.08 seconds.
[admin@HQ-DC-leaf~]$ nc -zv www.arista.io 443
```

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

```
[admin@HQ-DC-leaf~]$ sudo ip netns exec ns-MGMT nc -zv 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
```
1.8.2 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.

Connectivity Issues

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 nc -zv apiserver.arista.io 443

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-staging.corp.arista.io:443', '-cvcompression=gzip', '-cvvrf=MGMT', '-taillogs', '-cvauth=token-secure,/tmp/cv-onboarding-token', '-smashexcludes=ale,flexCounter,hardware,kni,pulse,strata', '-ingestexcludes=/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:
v1.15.3 golang 386

1.8.3 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

1.8.4 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.

```bash
! 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
!
```
1.9 Automation with CloudVision as-a-Service

Generating a Service Account Token

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

**Figure 23: 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 24: 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 25: 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 26: REST API Explorer**

![REST API Explorer](image)

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

**Using Python**

Python based CVPRAC module ([https://github.com/aristanetworks/cvprac](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.

```python
>>> 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

```python
>>> 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, <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](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](https://github.com/aristanetworks/ansible-cvp/pull/235)
1.10 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.