appviewX

CERT Solution Guide - EST Configuration Guide

Version: 2020.3.0

Copyright AppViewX, Inc.

External Reference Links

This product includes software developed by the CentOS Project (www.centos.org).

This product includes software developed by Red Hat, Inc. (www.redhat.com).

This product includes software developed by VMware, Inc. (www.vmware.com).

Contact Information

AppViewX, Inc.

222 Broadway, FL 19

New York, NY 10038

Email: info@appviewx.com

Web: www.appviewx.com

Contents

Preface

Revision History

Revision	Description	Date
1.0	Initial release of document for Release 2020.3.0	September 2020

About this Guide

This guide contains the predefined procedure for Enrollment over Secure Transport (EST) configuration.

Audience

This guide is intended for those who want to configure Enrollment over Secure Transport (EST) server.

Text Conventions

The following text conventions are used in this document:

Convention	Description
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`codeblock`	Indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Chapter 1: Overview

Enrollment over Secure Transport (EST) is a simple and functional certificate management protocol. EST works in the client-server model. AppViewX offers both EST server and client functionalities with TLS based authentication between the server and client as per the protocol. This document helps with the configuration of the EST in the AppViewX GUI.

Chapter 2: Prerequisites

Before configuring the EST server, the user has to make the following changes in the AppViewX server:

- Make sure that the <avx-platform-gateway-est> and <avx-vendor-cert-est-agent> services are running in the cluster.

> **Note:** If services are running, note the port number that is shown after 5301:<est_external_port>. This port must be configured in EST Settings UI.

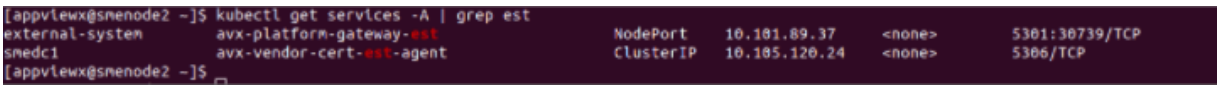
- Make sure that the namespace for below services are configured with respective data center (DC) names:
  - avx_platform_gateway_external=<dc name>
  - avx_vendor_cert_est_agent=<dc name>

Chapter 3: Enable EST Services

If EST services are not running, follow the steps to run the EST services:

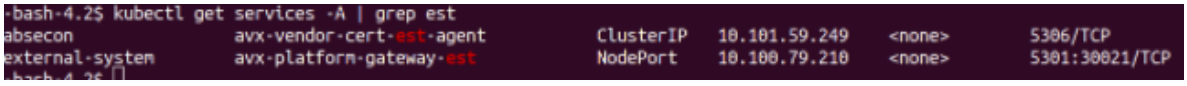
1. Open the terminal window.
2. Add the **avx_vendor_cert_est_agent** and **avx_platform_gateway_external** in **ENABLED_PLUGINS** in **appviewx.conf** that is available inside the scripts folder **</home/appviewx/appviewx_kubernetes/scripts>**.
3. Specify the data center (DC) where the gateway must be deployed.

4. Execute the command: `<plugins_install.sh>`
5. Verify the EST is enabled by executing the command: `<kubectl get services –A | grep est>`



6. Verify the plugin status and port number, do the steps as follows:
   a. Execute the `<kubectl get services -A | grep est>` command and make sure that the a**vx-vendor-cert-est-agent** and **avx-vendor-cert-est-agent** is running.
   b. Make sure that the port number is **5301:30021** in **avx-platform-gateway-est**.

> **Note:** The number **5301:30021** must be used in the UI configuration.



   c. Execute the `<kubectl get pods -n external-system -o wide>` command to identify the nodes running in the EST service. EST will be available on all the nodes where external system runs.

```
-bash-4.2$ kubectl get pods -n external-system -o wide
NAME                                    READY   STATUS         RESTARTS   AGE   IP              NODE
avx-platform-gateway-676f67587b-54jj8   1/1     Running        5          64d   10.244.198.136  trialnode2.appviewx.net
avx-platform-gateway-676f67587b-h6xrf   1/1     Running        4          62d   10.244.251.30   trialnode3.appviewx.net
avx-platform-gateway-676f67587b-tbqcs   0/1     NodeAffinity   0          64d   <none>          trialnode3.appviewx.net
-bash-4.2$
```

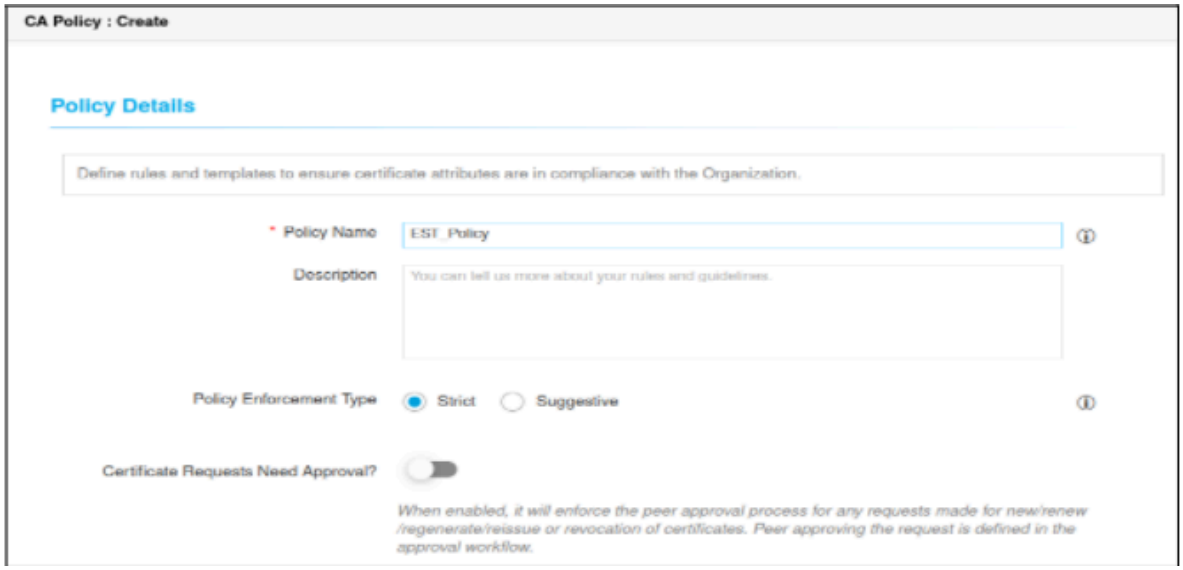
d. Ping to the node names to get IP addresses.

```
-bash-4.2$ ping trialnode2.appviewx.net
PING trialnode2.appviewx.net (192.168.61.82) 56(84) bytes of data.
64 bytes from trialnode2.appviewx.net (192.168.61.82): icmp_seq=1 ttl=64 time=0.225 ms
64 bytes from trialnode2.appviewx.net (192.168.61.82): icmp_seq=2 ttl=64 time=0.098 ms
^C
--- trialnode2.appviewx.net ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.098/0.161/0.225/0.064 ms
-bash-4.2$ ping trialnode3.appviewx.net
PING trialnode3.appviewx.net (192.168.61.83) 56(84) bytes of data.
64 bytes from trialnode3.appviewx.net (192.168.61.83): icmp_seq=1 ttl=64 time=0.149 ms
64 bytes from trialnode3.appviewx.net (192.168.61.83): icmp_seq=2 ttl=64 time=0.206 ms
64 bytes from trialnode3.appviewx.net (192.168.61.83): icmp_seq=3 ttl=64 time=0.114 ms
^C
```

7. [Optional] Create a separate group for EST if required or else use the Default Group, where the **Certificate Request Needs Approval** should be disabled for the associated CA Policy.

8. Create a CA policy and associate with group. For more details, refer to the **CERT+ Admin Guide.**

a. Disable **Certificate Requests Need Approval?** in the **Policy Details** page.



b. To configure a policy with AppViewX details, click **AppViewX** in the **Certificate Authority** pane on the left side of the screen.
c. In the CA detail section, select **CA Accounts** from the dropdown list.
d. Add validity, and then click **Add**.
e. Select bit length as 2048 and above (AppViewX Client supports 2048 RSA)
f. Select ECDSA curves based on requirement.
g. Select the hash function as SHA-256 and above.
h. Click **Save CA Details**.
i. Select the Group that is created earlier and update policy.

9. Upload a client authentication issuer certificate in AppViewX application.
   a. By default, AppViewX EST Client software (Windows/Linux/Mac) will have an Authentication Certificate Encoded within the software (which will be encrypted and kept within Client software), user will never have direct access to it and this will be used for agent to communicate with AppViewX EST Server.
   b. For initial validation, you can use the default encoded authentication certificates in the Client software and issuer certificate. The file will be available in a common share folder with the following file name.
      i. The file name **<AppViewXIntermediateCA_D2 E3 B6 15 EE E6 2D 4C 1D 99 AC 11 6D 47 B5 CD.crt>**
      ii. Upload the above file in the respective AppViewX environment and trust it in EST Settings.
      iii. To upload a certificate, log in to AppViewX application with valid credentials.
      iv. Click the menu button located in the upper left corner of the screen.

The left navigation pane appears.

v. Click **CERT+** > **Certificate Inventory**.

vi. Click **Upload** > **CA Certificate**.

vii. Select CA, and then upload the file.

- Note the Serial Number **B5:CD** of the CA Certificate (This needs to be added as **Issuer Certificate in EST Client Authentication Configuration** later).
- If you want to use non AppViewX Certificate as the Issuer CA for EST Authentication. Refer the **EST Server Update FP5 Authenticate with External CA guide** and section Adding External CA Trust Certificate for EST Client Authentication
- Description: TLS Authentication handshake is happening in the GW and by default GW is holding only AppViewX Intermediate and AppViewX Root in the EST_TRUSTED_CA_CERTS, AppViewX GW will be sending these Certificates as the DN(Distinguished Name) response to the Clients.
- During TLS Handshake Client validates whether the DN response from server contains the CA Certificate with Signed Client's Authentication Certificate. If not, client will not send the authentication Certificate to the Server, assuming this is not the right server.

Note: OCSP and CRL Validation of Client Authentication Certificate for EST request is disabled by default in AppViewX. To enable reach out to AppViewX Support (support@appviewx.com).

If it is getting enabled, make sure OCSP or CRL responder is reachable from AppViewX to validate the client certificate status; else all the client enrollment requests will fail with the status *OCSP or CRL responder is not reachable*.

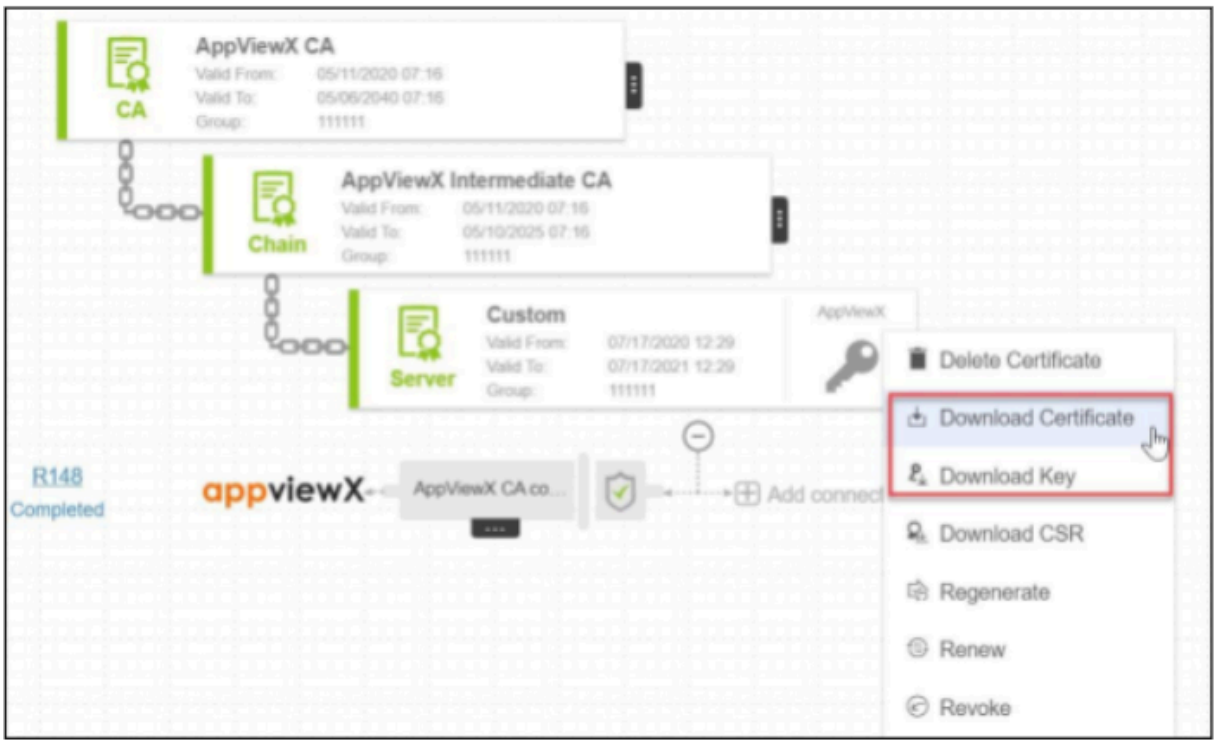
Chapter 4: Create Client Authentication Certificate Using AppViewX CA

If the user does not have a client authentication AppViewX CA certificate, user can use AppViewX CA. To use a client authentication AppViewX CA certificate:

1. Log in to the AppViewX application with valid credentials.
2. Click the menu button.
   The left navigation pane appears.
3. Click **CERT+.**
   The CERT+ left navigation pane appears.
4. Expand **CERTIFICATE Inventory.**
5. Select **Enroll Certificate,** and then **Server.**
   The **Enroll Server Certificate** page appears.
6. In the **General Information** section of the **Enroll Server Certificate** page, select the desired **Assign Group** from the dropdown list.

   Note: By default, the Default option is selected.

7. In the **CA Details** section, select/enter the details as required.
8. Select a **CSR Generation** mode: AppViewX, Upload CSR, HSM, or Endpoint.
9. Under the **CSR Parameters** section, enter a Common Name for the certificate.
10. While creating certificates, you can attach supporting documents by uploading it in the **Attachment** section.
11. Click **Add** to generate the certificate. The certificate holistic view with the newly created CSR appears.
12. Click **Submit**.
13. On the submit dialog box, enter relevant comments and click **Yes**.
14. Click **Refresh** on the top-right to refresh the holistic view. Now, a chain of certificates is displayed.
15. Hover over the vertical eclipse icon on the certificate and download the Certificate and Key.



Note: The user has to trust the AppViewX Intermediate CA certificate and select this certificate as **Issuer Certificate** during the EST configuration.

Chapter 5: EST Configuration

- Supported Operations

Supported Operations

The AppViewX EST agent supports three operations as shown in the below table.

Supported Operation	Operation Path
Distribution of CA certificates	/cacerts
Enrollment of clients	/simpleenroll
Re-enrollment of clients	/simplereenroll

Chapter 6: Best Practices

Example URLs

- For default: <https://est.appviewx.com:<port_number>/.well-known/est>
- For AppViewX Enrollment: <https://est.appviewx.com:<port_number/.well-known/est/appviewx/simpleenroll>
- For AppViewX Re-enrollment: <https://est.appviewx.com:<port_number/.well- known/est/appviewx/simplereenroll>

Chapter 7: Adding External CA Trust Certificate for EST Client Authentication

- By default, AppViewX Intermediate and AppViewX Root will be available in the location with filenames **default_inter.crt, default_root.crt**
- Execute the command

```
[appviewx@pesrv07-arch-94-20 ~]$ kubectl describe secret client-cacerts-est -n external-system
Name:         client-cacerts-est
Namespace:    external-system
Labels:       <none>
Annotations:
Type:         Opaque

Data
====
default_inter.crt:  1505 bytes
default_root.crt:   1281 bytes
[appviewx@pesrv07-arch-94-20 ~]$
```

- Add below plugins in the ENABLED_PLUGINS list

ENABLED_PLUGINS=appviewx_dependencies,avx_platform_gateway_external,avx_platform_gateway

```
# Comma seperated values of absolute paths of certs
#EST_TRUSTED_CA_CERTS=/home/appviewx/appviewx_kubernetes/scripts/digicert.crt
```

- Run `./plugins_install.sh`

Chapter 8: Change SSL Certificate for EST-HTTPS Communication

1. By default, there will be self-signed certificate available in the location.
2. Add below plugins in the ENABLED_PLUGINS list

   ENABLED_PLUGINS=appviewx_dependencies,avx_platform_gateway_external,avx_platform_gateway

```
# Please specify the absolute paths of files for the labels below
# EST_SERVER_ACCESS_CERT=
# EST_SERVER_ACCESS_KEY=
# Comma seperated values of absolute paths of certs
#EST_TRUSTED_CA_CERTS=/home/appviewx/appviewx_kubernetes/scripts/digicert.crt
```

3. Run `./plugins_install.sh`

```
[appviewx@pesrv07-arch-94-20 ~]$ kubectl describe secret server-tls-est -n external-system
Name:         server-tls-est
Namespace:    external-system
Labels:       <none>
Annotations:
Type:         kubernetes.io/tls

Data
====
tls.crt:  1046 bytes
tls.key:  1704 bytes
```

Chapter 9: Gateway - EST Logs

To access the EST logs:

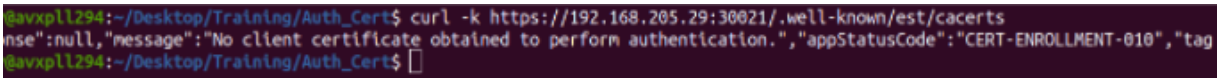
1. Access the terminal window.
2. Go to **<Installed_Path>/logs** directory and find with the name format **<avxgw-MTLS-<yyyy-mm-dd>.log>**. For example, **<avxgw-MTLS-2021-03-17.log>**.
   - If the file size exceeds 100 MB, it will be rolled over and the latest logs will be available in the latest file that is named with an incrementing counter starting from 1 such as **avxgw-MTLS-<yyyy-mm-dd>.<incrementing_counter>.log.** For example, **<avxgw-MTLS- 2021-03-17.1.log>**.
   - EST Plugin Logs:

     </home/appviewx/appviewx/logs/avx-vendor-cert-est-agent-<pod_name>.log>

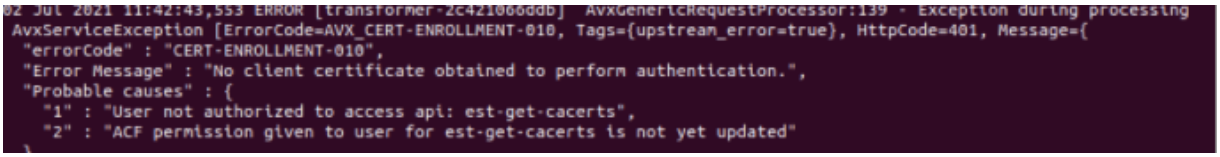
Chapter 10: Verification of the EST Server

To verify the EST server:

1. Access the terminal window.
2. Go to **<appviewx/logs>** directory and execute the `<kubectl get pods -A | grep est>` command.
3. Go to **-f <pod_name>.log** directory.
4. Access CACerts URL from browser or try curl from another machine.



5. Check the log file.



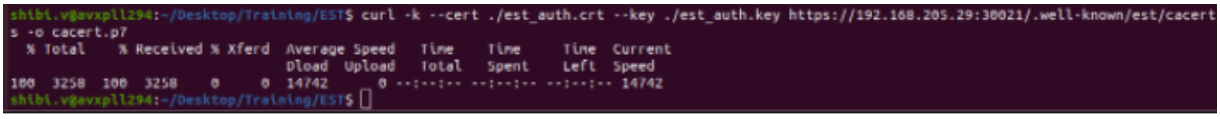
The response indicates that the EST is listening on port and trying to do Certificate Authentication with Client.

Chapter 11: Testing EST Enrollment by using CURL

To test the EST enrollment:

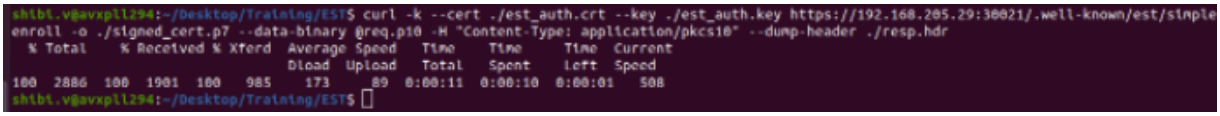
1. After the successful verification, create a test folder in the Linux client machine.
2. Copy the <**est_auth.crt**> and <**est_auth.key**> from the common share directory https://drive.google.com/drive/folders/1K4G5L8yB5TOvvLCAPjNC3lQWBWtlWua0
3. Generate the CSR in the same folder with <openssl> command.

   `openssl req -new -newkey rsa:2048 -nodes -keyout rsakey.key -out req.p10`
4. Trigger GetCA certs request using CURL command (update server IP and Pathseg depends on Server Config).
5. Make sure that the authentication CERT and Key is present in same location **<curl -k --cert ./est_auth.crt --key ./est_auth.key** *https://<server_ip>:30021/.well-known/est/cacerts -o cacert.p7*.
   You will receive <cacert.p7> file with Configured CA Certificate in Step 9.



6. Convert the received CA Certificate to pem <openssl base64 -d -in cacert.p7 | openssl pkcs7 -inform DER -outform PEM -print_certs -out cacert.pem>.
7. Trigger enrollment request by using CURL and make sure that the authentication Cert, Key, and CSR are present in same location.

   <curl -k --cert ./est_auth.crt --key ./est_auth.key https://192.168.205.29:30021/.well-known/est/simpleenroll -o ./signed_cert.p7 --data-binary @req.p10 -H "Content-Type: application/pkcs10" --dump-header ./resp.hdr>



8. Verify the content of **<signed_cert.p7>**.

9. Convert the enrolled p7 Certificate in to pem:

```
<openssl base64 -d -in signed_cert.p7 | openssl pkcs7 -inform DER -outform PEM -print_certs -out signed_cert.pem>
```

Note: Make sure that you have received **<cacert.p7>** file with Configured CA Certificate.