appviewX

CLMaaS Certificate Auto-Enrollment Guide

Version: 2022.1.0

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 2021.1.0	September 2021

About this Guide

This guide outlines the concepts as well as the steps for enabling and configuring the certificate auto-enrollment protocols: ACME, EST, and SCEP for the CLMaaS deployment of CERT+.

Audience

This guide is intended for AppViewX's customers.

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: Provisioning Certificate Auto-Enrollment for CLMaaS

Certificate Auto Enrollment allows users and devices to request and enroll for certificates automatically, without any user interaction required. This is a significant feature to be a part of your PKI strategy because the automated enrollment process helps to prevent disruptive situations that then require time- and effort-heavy remediations.

AppViewX's CLMaaS deployment enables IoT devices in the customer's premises to obtain certificates from AppViewX using certificate auto enrollment. Under this provision, IoT devices can send auto enrollment requests, in the form of a CSR file, to the AppViewX Cloud Connector using auto enrollment protocols. In response, AppViewX will create and send certificates based on the requirements defined in the CSR file, which the auto enrollment customer can download from AppViewX.

Auto enrollment protocols are standardized enrollment mechanisms accepted across a wide range of enterprise systems for device and application certificate enrollment. Systems leveraging auto enrollment protocols typically expect minimum to no admin intervention. Network devices such as routers-switches, DevOps tools, and Enterprise Mobility Management platforms are typical examples of such systems.

Under AppViewX's certificate auto enrollment implementation, IoT devices can send auto enrollment requests using one of the following certificate auto enrollment protocols:

- Automated Certificate Management Environment (ACME)
- Enrollment over Secure Transport (EST)
- Simple Certificate Enrollment Protocol (SCEP)

Note: If a customer has multiple AppViewX Cloud Connector instances up and running, auto enrollment protocols will have to be enabled for each instance individually.

Chapter 2: Prerequisites

- Configure the AppViewX Cloud Connector's FQDN/IP address during the auto enrollment configuration.

- Port requirements:

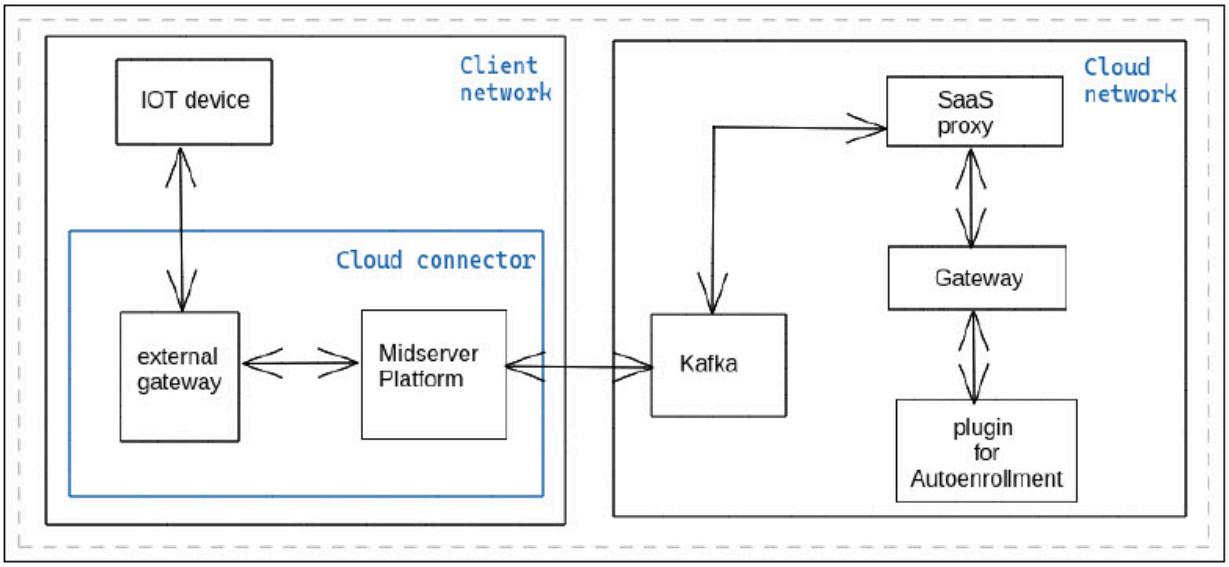
  The AppViewX auto enrollment gateway will be deployed on the AppViewX Cloud Connector, which is running in the customer's premises. This gateway will be used for establishing auto enrollment communication/validation from AppViewX to the auto enrollment clients.

  The following ports are used for this protocol communication:

Port no.	Description
30021	This port will receive the auto enrollment requests coming via EST.
30022	This port will receive the auto enrollment requests coming via SCEP.
30020	This port will receive the auto enrollment requests coming via ACME.

Chapter 3: Software Architecture

The diagram below shows the software architecture deployed to enable certificate auto enrollment in SaaS:



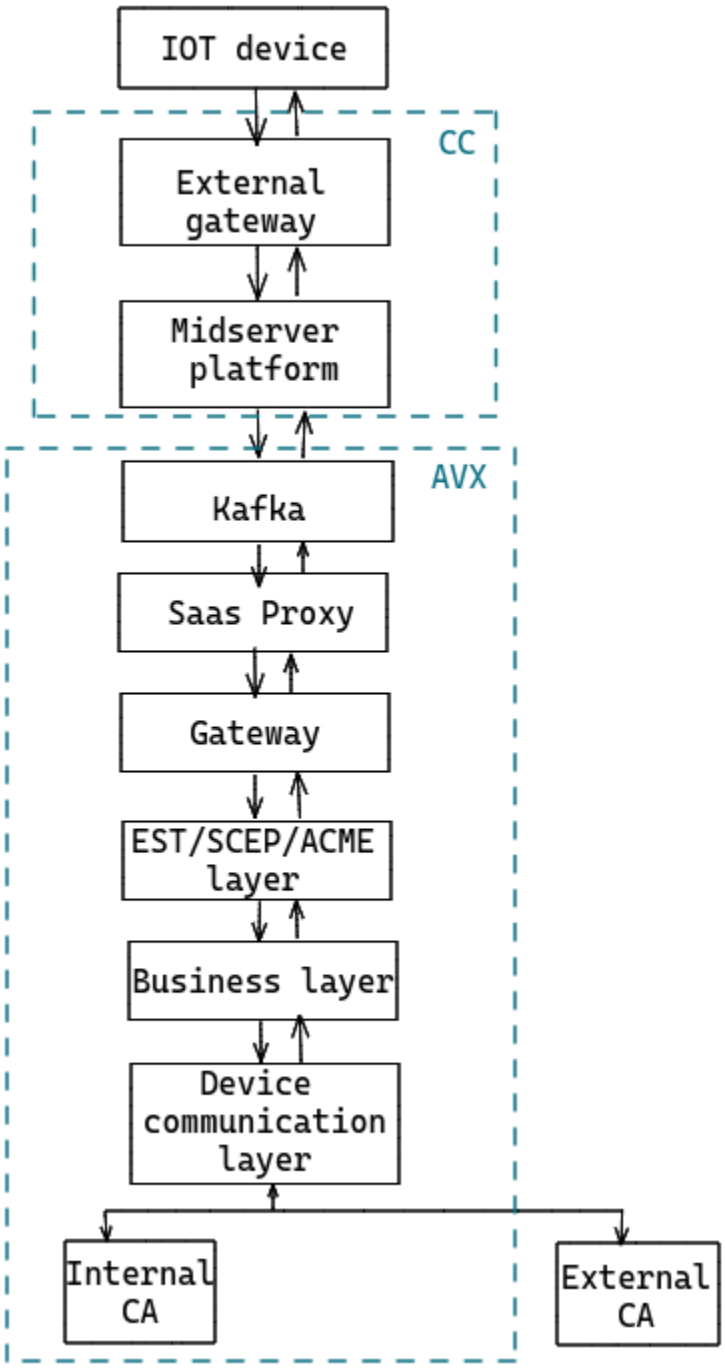
The key elements of this architecture are explained below:

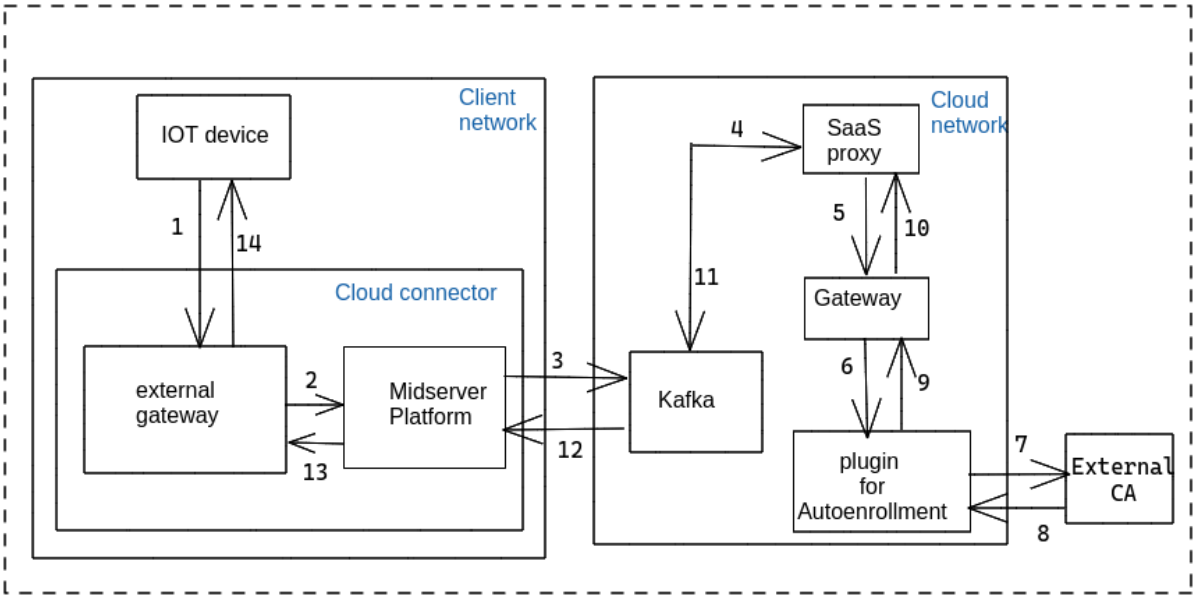
Element	Description
External gateway	The external gateway, which is a lightweight version of the AppViewX gateway, will run within the AppViewX Cloud Connector that will listen to incoming requests from IoT devices.
Mid server platform	The mid server platform will run as a jetty server that will expose the AppViewX transformers. The transformers will transform the EST/SCEP/ACME requests to standard action API endpoint format. The transformed API will be routed through the SaaS Proxy to hit the default gateway and cascade the request for processing.
SaaS proxy component	The SaaS proxy component will expose the transformed API that will capture the incoming auto enrollment requests and route it to the default gateway.

Chapter 4: Communication Flow

1. The IoT device submits a request for certificate auto enrollment.
2. The request is routed to the external gateway, which passes it on to the transformers exposed from the mid-server platform.
3. The transformers transform the EST/SCEP/ACME requests to standard action API endpoint format. The transformed API will hit the default gateway and cascade the request for processing.
4. The AppViewX Cloud Connector routes the request to the AppViewX instance on the cloud as an API call.

   From here, the auto enrollment request will follow AppViewX's default communication flow.
5. The enrolled certificate is cascaded back to the IoT device that requested it.





Chapter 5: Security Architecture

AppViewX secures all communication between the various entities involved in the certificate auto enrollment process.

The security architecture implemented is as follows:

Communication between	Secured using
AppViewX Cloud Connector and the AppViewX instance installed in the cloud	mTLS and AES encryption
IoT devices and the AppViewX Cloud Connector	EST, SCEP and ACME protocols
All AppViewX components	mTLS protocol
AppViewX instance installed in the cloud and external CA	HTTPS protocol

Chapter 6: Enabling Auto-Enrollment for AppViewX Cloud Connector Instance

Enabling Auto-Enrollment for AppViewX Cloud Connector Instance

AppViewX lets you enable the certificate auto enrollment feature for individual AppViewX Cloud Connector instances at the time of installation.

Note:

- If an instance of the AppViewX Cloud Connector is already installed, you will need to uninstall it. Enabling auto enrollment by upgrading an already installed instance will be a part of the future releases.
- If a patch is going to be applied for an FP1 AppViewX Cloud Connector instance, ensure that the Kafka proxy server is installed for the FP2 AppViewX Cloud Connector instance to work properly.

To enable auto-enrollment for an AppViewX Cloud Connector instance:

1. Download and install the latest version of the AppViewX Cloud Connector instance.
2. During installation, in response to the question **Do you need auto-enrollment of the certificate using EST/SCEP/ACME? (y/n)**, press **y**.
3. Press **Enter**.
4. In response to the question **Please choose one or more protocol (use comma separated numbers): 1)EST (MTLS) 2)SCEP (HTTP) 3)ACME (HTTPS)**, to enable the required protocol(s), enter a comma-separated list of numbers (from 1, 2, and 3).

> **Note:** If the Hashicorp Vault will be used to access the AppViewX Cloud Connector gateway, enter **3** to select the **ACME/HTTPS** protocol.

5. Proceed with the rest of the installation instructions.

- Enabling Auto-Enrollment for AppViewX Cloud Connector Instance
- Enabling Custom Authentication Certificates for EST

Enabling Custom Authentication Certificates for EST

Default AppViewX certificates are used for the handshake/authentication between the AppViewX Cloud Connector and the requesting IoT device.

For certificate auto enrollment via EST (that uses mTLS for communication), AppViewX enables customers to use custom certificates from a different CA, instead of the default AppViewX certificate. To do this:

1. Copy the custom certificate files in the **<installation package>/deps/** folder for the AppViewX Cloud Connector for which auto enrollment has been enabled.
2. Open the **appviewx.properties** file in the edit mode.
3. For the **EST_SERVER_ACCESS_CERT** field, enter the relative path of the custom certificate, with respect to the deps folder (in the AppViewX Cloud Connector installation package).
4. For the **EST_SERVER_ACCESS_KEY**, enter the relative path of the .key file for the custom certificate, with respect to the deps folder (in the AppViewX Cloud Connector installation package.
5. For the **EST_TRUSTED_CA_CERTS** field, enter a comma-separated list of .crt certificate sources to add them to the list of trusted certificate sources. A request will be valid only if the requested certificate belongs to a trusted source.
6. To apply the changes, navigate to the AppViewX Cloud Connector installation path and run the script: **./deps/utils/gateway_upgrade.sh**

Chapter 7: Configuring Certificate Auto Enrollment in AppViewX

Important: Ensure that the ACME/EST/SCEP agent is up and running in the AppViewX server.

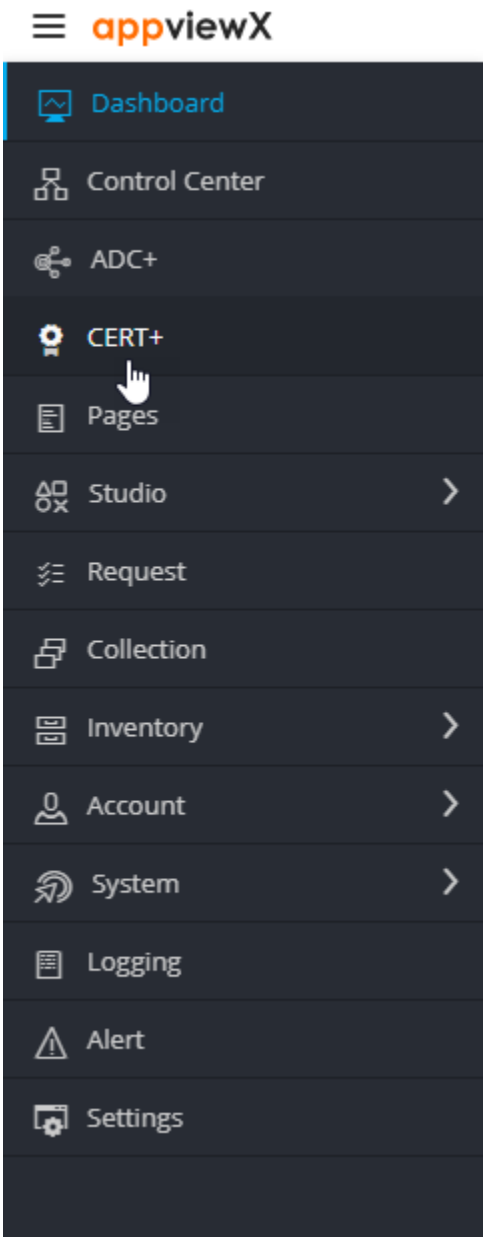
Before configuring certificate auto enrollment settings, ensure that the certificate policy for the CA profile that is tied to the ACME/EST/SCEP settings has auto approval enabled.

To do this:

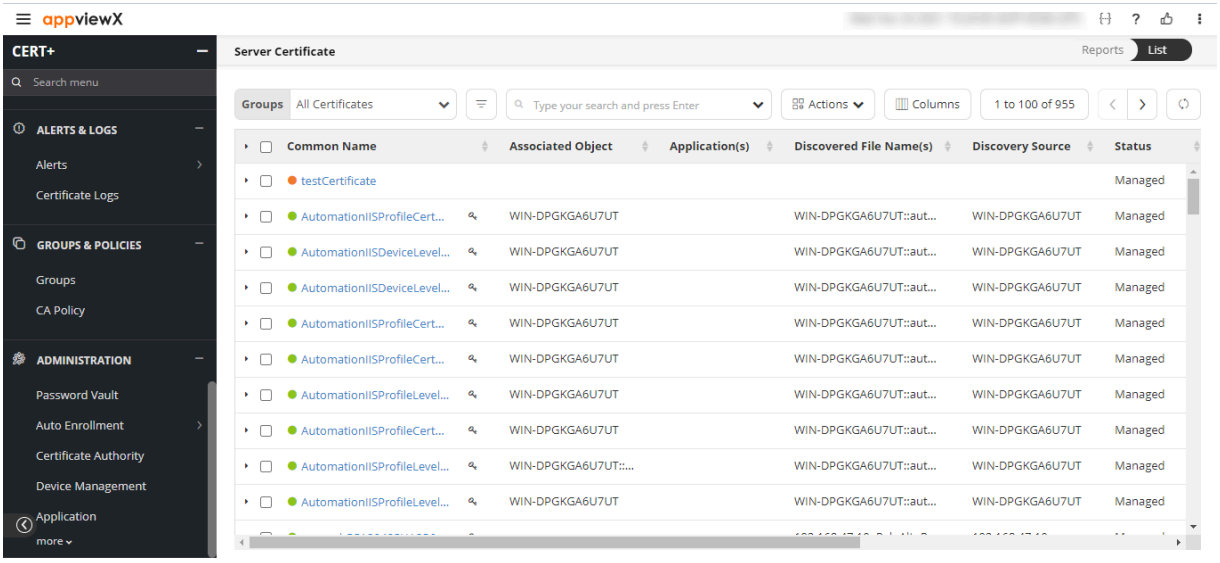
1. Login to AppViewX with your valid credentials.

   By default, the **Dashboard** is displayed.

2. From the top-right corner of the Dashboard, click ☰.
3. From the menu displayed, select **CERT+**.



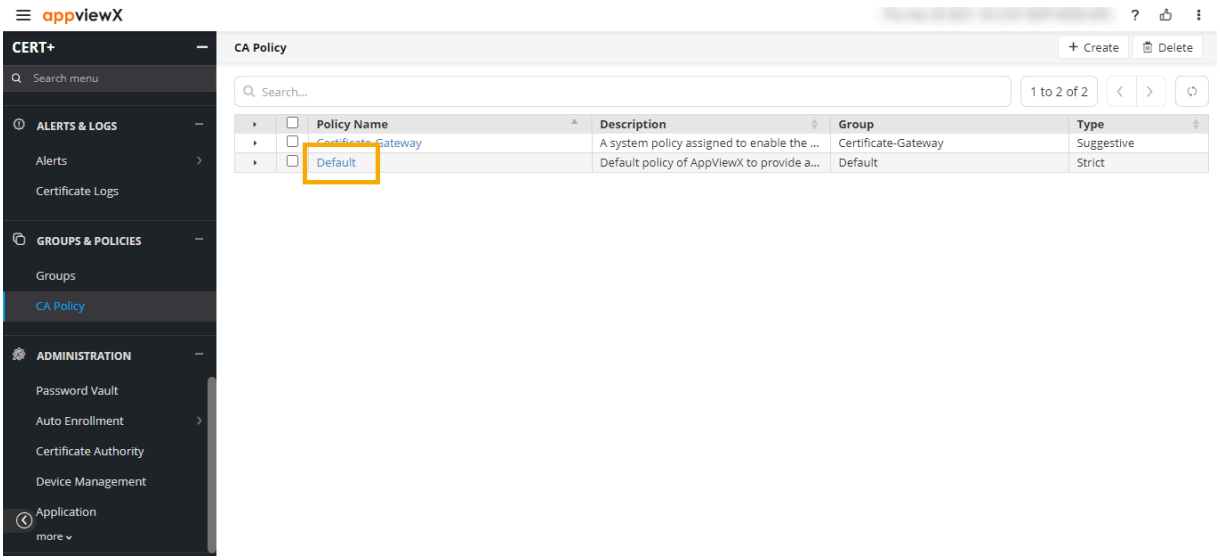
The CERT+ **Server Certificate** page is displayed.



4. In the CERT+ menu, scroll down to the **Groups & Policies** section and select **CA Policy**.

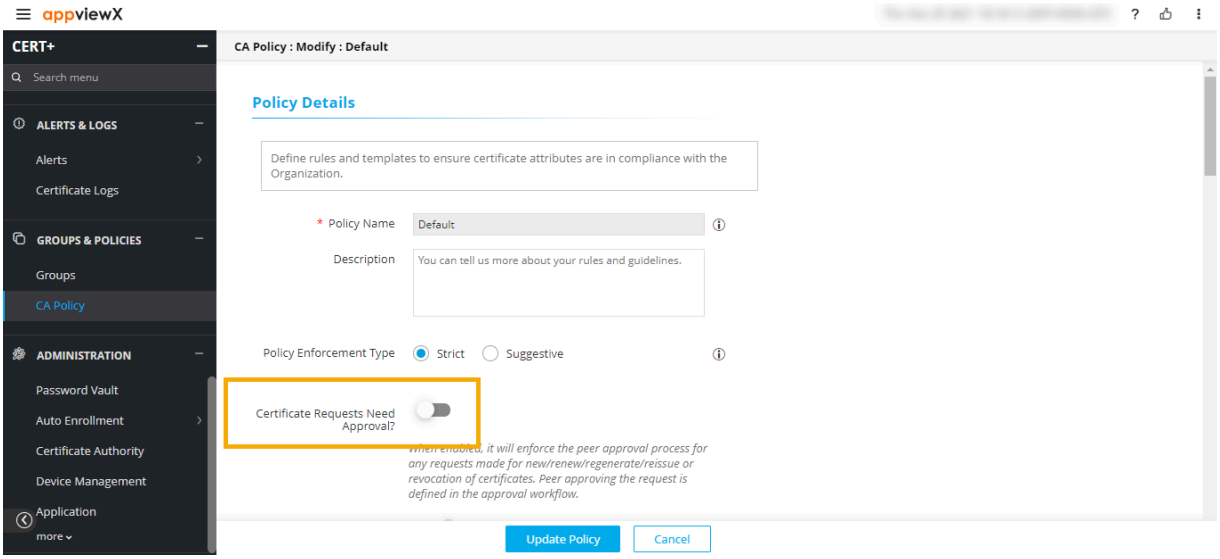
   The **CA Policy** page is displayed.

5. From the table displayed on the **CA Policy** page, click the **Default** policy name.



   The **CA Policy : Modify : Default** page is displayed.

6. On the **CA Policy : Modify : Default** page, enable the **Certificate Requests Need Approval** toggle button.



Chapter 8: Certificate Auto-Enrollment Protocols

- ACME
- EST
- SCEP

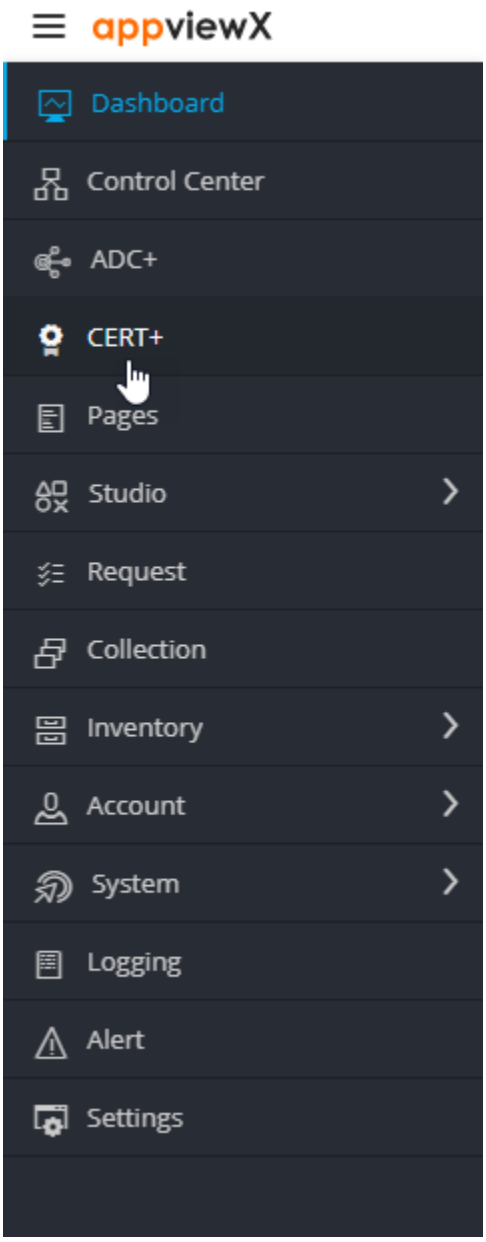
ACME

Automated Certificate Management Environment (ACME) is a communications protocol for automating the issuance of certificates and the domain validation procedures, allowing the automated deployment of Public Key Infrastructure (PKI) without user interaction.

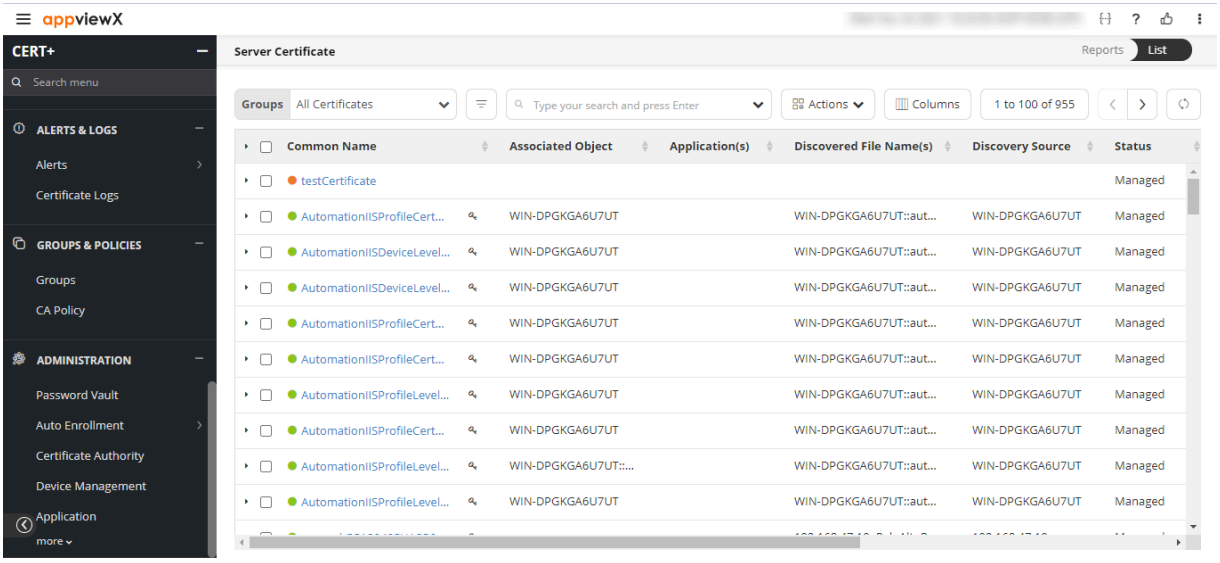
- Accessing the ACME Settings
- Enabling ACME for Auto-Enrollment

Accessing the ACME Settings

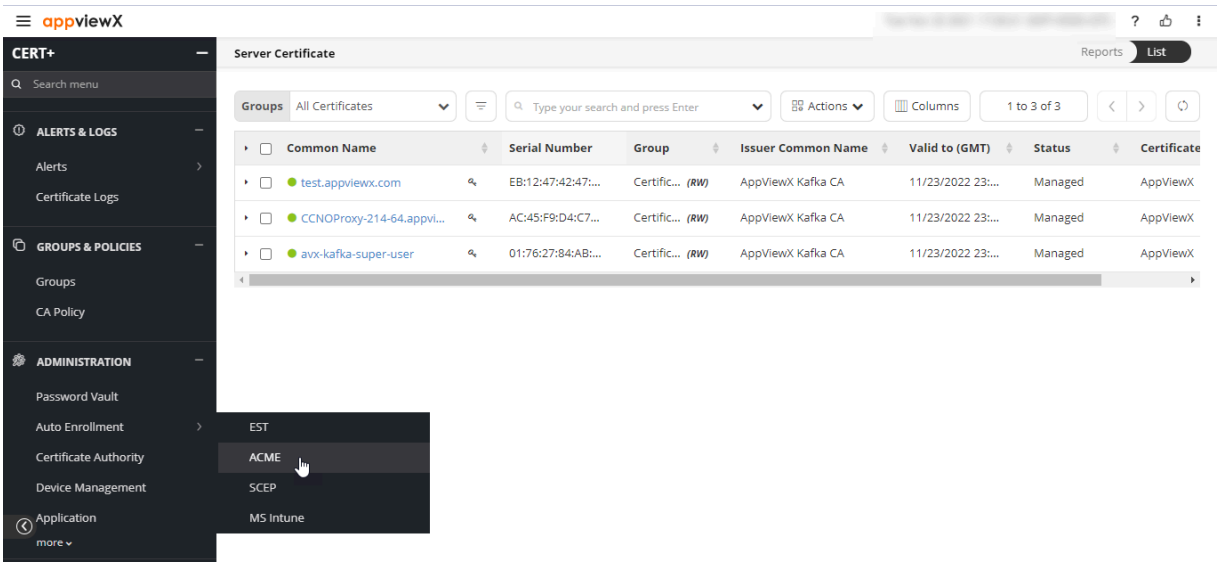
1. Login to AppViewX with your valid credentials.
   By default, the **Dashboard** is displayed.
2. From the top-right corner of the **Dashboard**, click ☰.
3. From the menu displayed, select **CERT+**.



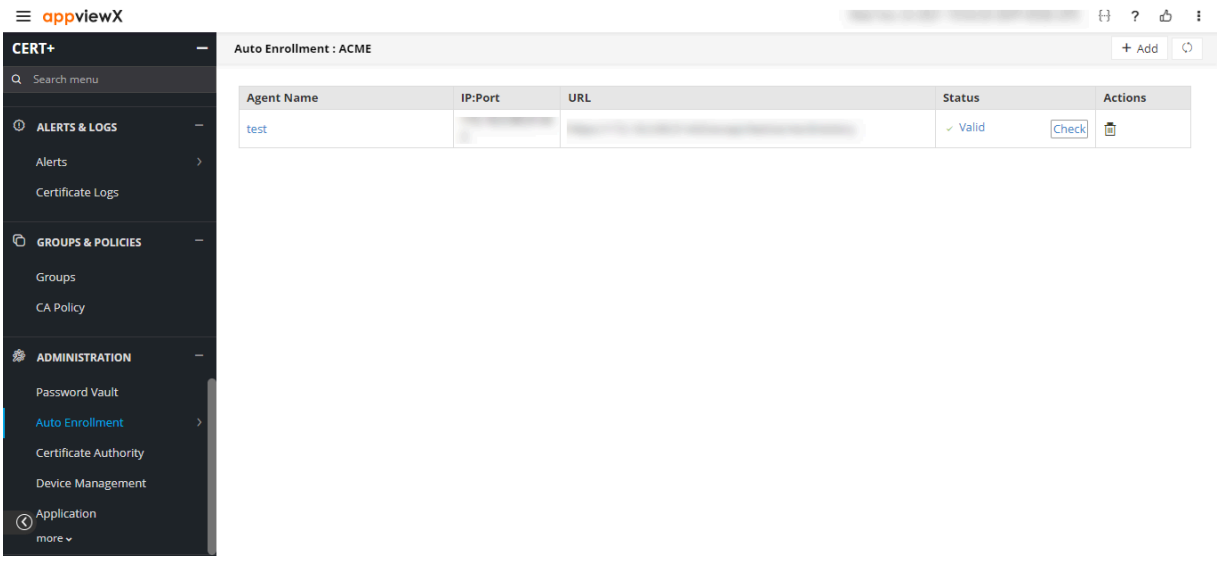
The CERT+ **Server Certificate** page is displayed.



4. In the CERT+ menu, scroll down to the **Administration** section and select **Auto Enrollment** > **ACME**.



The **Auto Enrollment : ACME** screen is displayed.

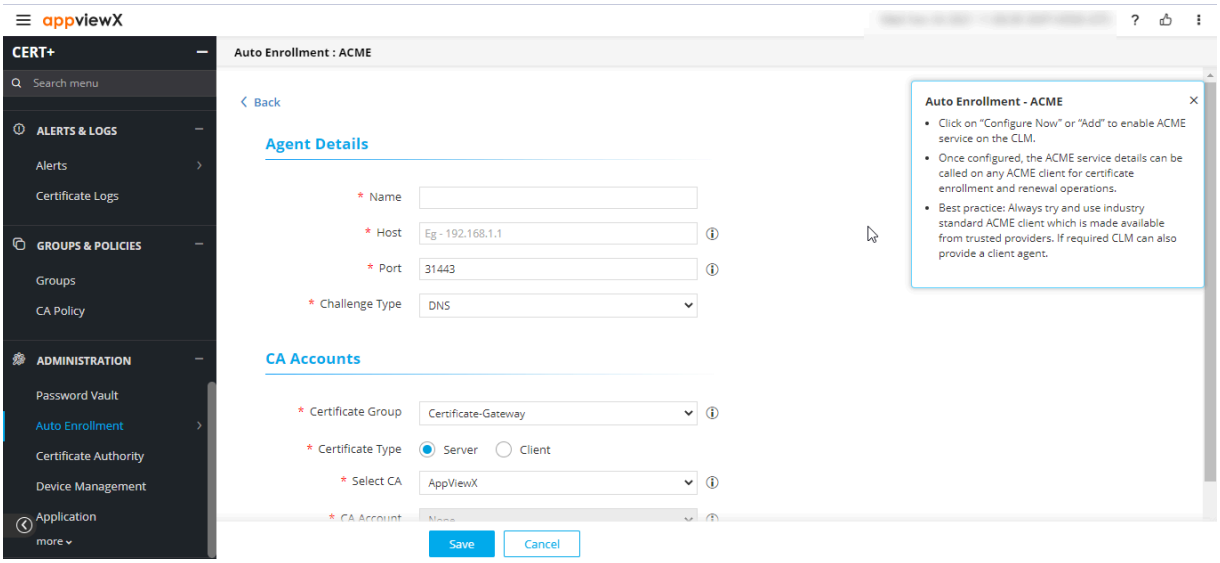


Enabling ACME for Auto-Enrollment

1. Navigate to the **Auto Enrollment : ACME** page.
2. To enable ACME for auto enrollment, click Configure Now or + Add.

> **Note:** The **Configure Now** button is displayed only if you are enabling your first ACME agent.

The **Auto Enrollment : ACME** page is updated to display the fields for enabling ACME.



3. Enter/Select the following details in the **Agent Details** section:

Field	Description
Name*	Enter a unique name for the ACME agent. **Note:** Only alphanumeric and the following special characters are allowed: period (.). hyphen (-), and underscore (_). The agent name cannot begin with a special character.
Host*	Enter the FQDN or IP address of the AppViewX Cloud Connector.
Port*	Enter the following port number: **30020**.
Challenge Type*	Select the preferred challenge type for ACME validation. The supported challenge types are: • DNS-01 • HTTP-01

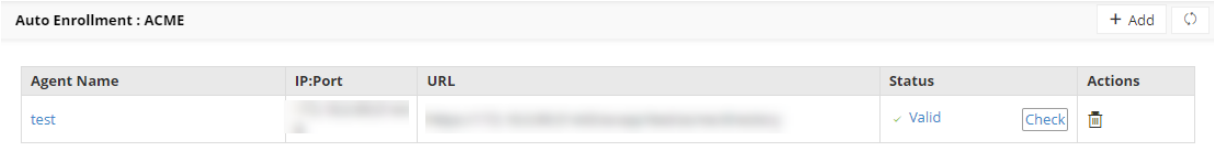
Note: Fields marked with red asterisk (*) symbol are mandatory.

4. Enter/Select the following **CA Accounts** details:

Field	Description
Certificate Group*	From the following options in the dropdown list, select a certificate group for managing certificates in the server/client inventory: • Certificate-Gateway • Default
Certificate Type*	Select a certificate type from the following options: • Server (default) • Client
Select CA*	From the dropdown list, select the Certificate Authority that the ACME agent will communicate with while performing the certificate auto enrollment actions.

Field	Description
CA Account*	From the dropdown list, select the Certificate Authority account that the ACME agent will communicate with while performing the certificate auto enrollment actions. **Note:** This dropdown list will be populated with valid values only when the CA account is added to the CA settings.
CA Connector Name*	Enter the CA connector name. This connector name will be shown in the holistic view for all the certificates issued through this ACME agent.
Certificate Validity*	Enter a validity period, in days, that will be applicable to all certificates issued through this ACME agent.

5. Click **Save**.
   The details of the ACME agent thus added are displayed on the main **Auto Enrollment : ACME** screen.



   The URL given here can be used for communication between the AppViewX ACME agent and the IoT device requesting auto-enrollment.

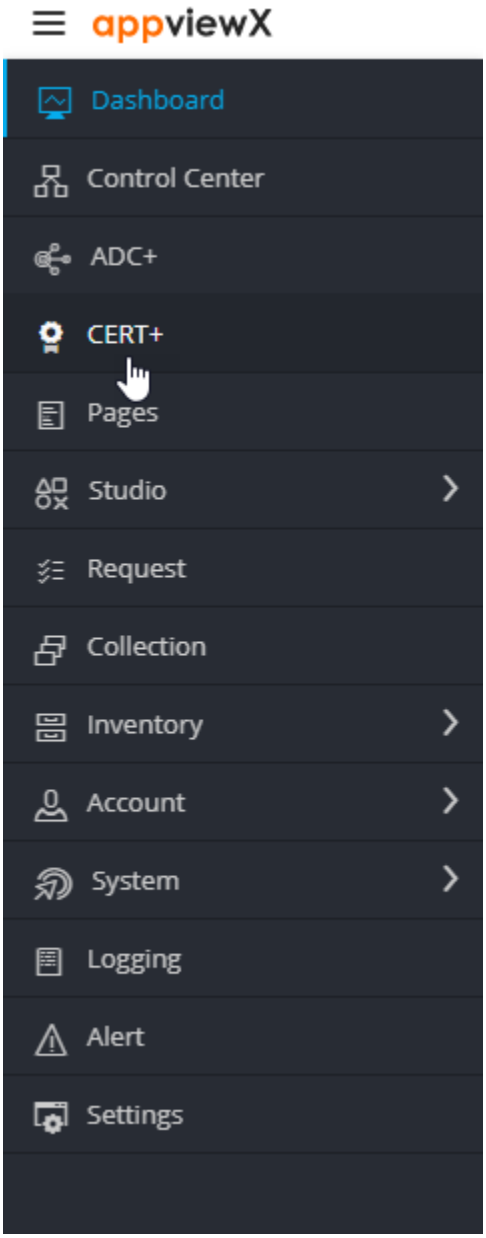
EST

The Enrollment over Secure Transport (EST) is a X.509 cryptographic certificate management protocol used to enable Public Key Infrastructure (PKI) clients to acquire client certificates and associated Certificate Authority (CA) certificates. AppViewX EST is compliant with RFC7030. AppViewX EST offers both, EST server and client functionalities with TLS-based authentication between the server and the client, as per the protocol.

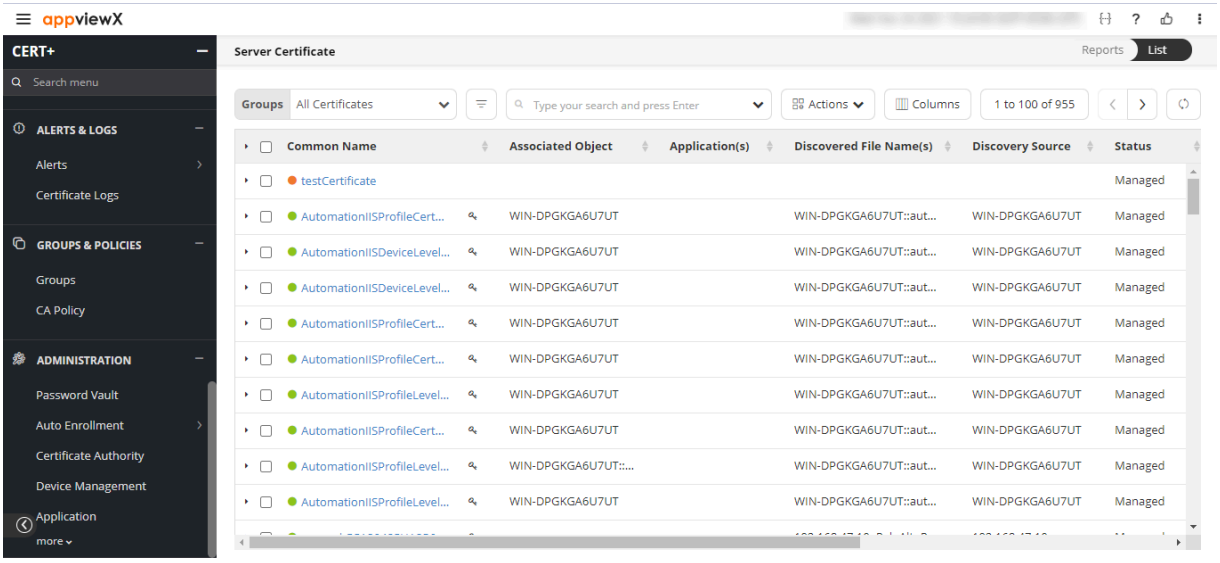
- Accessing the EST Settings
- Enabling EST for Auto Enrollment

Accessing the EST Settings

1. Login to AppViewX with your valid credentials.
   By default, the **Dashboard** is displayed.
2. From the top-right corner of the **Dashboard**, click ☰.
3. From the menu displayed, select **CERT+**.

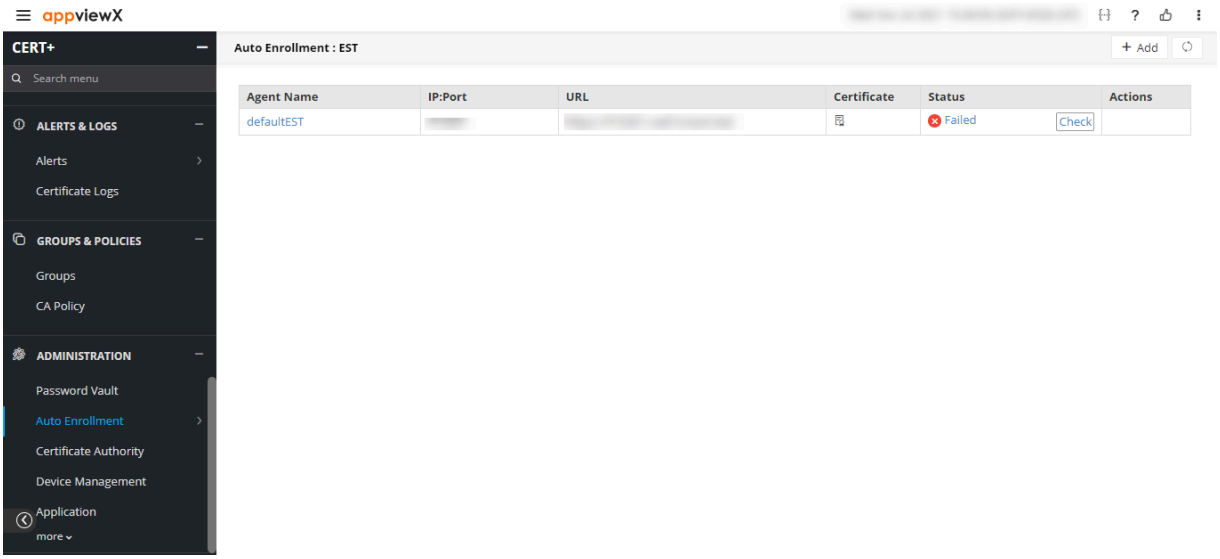


The CERT+ **Server Certificate** page is displayed.



4. In the CERT+ menu, scroll down to the **Administration** section and select **Auto Enrollment** > **EST**.

   The **Auto Enrollment : EST** screen is displayed.

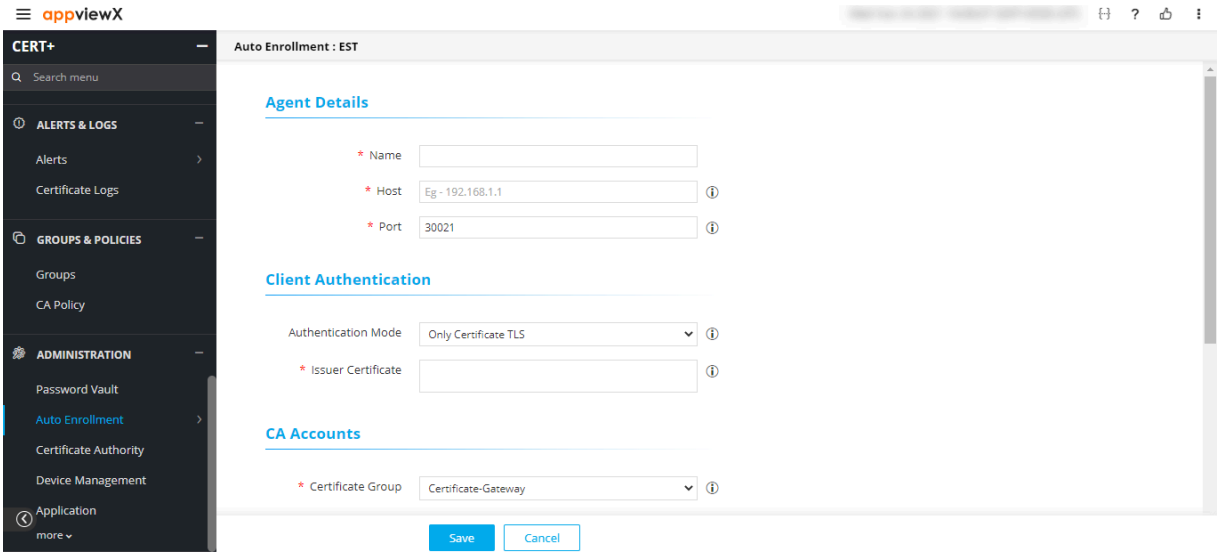


Enabling EST for Auto Enrollment

1. Navigate to the **Auto Enrollment : EST** page.
2. To enable EST for auto enrollment, click + Add.

Note: An EST agent is already created, by default. You can choose to edit the settings of this default EST agent for your requirements instead of creating a new one.

The **Auto Enrollment : EST** page is updated to display the fields for enabling EST.



3. Enter/Select the following details in the **Agent Details** section:

Field	Description
Name*	Enter a unique name for the EST agent. **Note:** Only alphanumeric and the following special characters are allowed: period (.). hyphen (-), and underscore (_). The agent name cannot begin with a special character.
Host*	Enter the FQDN or IP address of the AppViewX Cloud Connector
Port*	Enter the following port number: **30021**

Note: Fields marked with red asterisk (*) symbol are mandatory.

4. Enter/Select the following **Client Authentication** details:

Field	Description
	To authenticate clients during communication, select an authentication mode from the following options:Only Certificate TLSOnly certificate TLS-based client authentication will be performed. • Certificate TLS with HTTP as fallback If certificate TLS fails during client authentication, HTTP-based authentication will be performed as a fallback. • Both Certificate TLS and HTTP Both, certificate TLS-based as well as HTTP-based client authentication, will be performed one after the other. **Note:** The second authentication mode is performed after the successful completion of the first one.
Authentication Mode	Enter the common name for the CA that will be used for authenticating the client certificate. **Tip:** Enter up to three characters of the common name for a list with matching values to be displayed. You can then select the issuer certificate from this list. **Note:** Only issuer certificates that are available in the root or intermediary certificates' inventory will be shown for selection in the above mentioned list.

5. Enter/Select the following **CA Accounts** details:

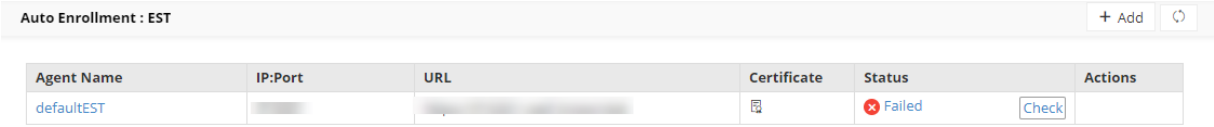
Field	Description
Certificate Group*	From the following options in the dropdown list, select a certificate group for managing certificates in the server/client inventory: • Certificate-Gateway • TestGroup • WOApprovalGroup

Field	Description
	• Default • CreateCertGroup
Certificate Type*	Select a certificate type from the following options: • Server (default) • Client
Select CA*	From the dropdown list, select the Certificate Authority that the EST agent will communicate with while performing the certificate auto enrollment actions.
CA Account*	From the dropdown list, select the Certificate Authority account that the EST agent will communicate with while performing the certificate auto enrollment actions. **Note:** This dropdown list will be populated with valid values only when the CA account is added to the CA settings.
CA Certificate*	Enter the name of the issuer certificate that will be used for signing the CSR by the Certificate Authority. **Tip:** Enter up to three characters of the certificate name for a list with matching values to be displayed. You can then select the issuer certificate from this list. **Note:** Only issuer certificates that are available in the root or intermediary certificates' inventory will be shown for selection in the above mentioned list
CA Connector Name*	Enter the CA connector name. This connector name will be shown in the holistic view for all the certificates issued through this EST agent.
Certificate Validity*	Enter a validity period, in days, that will be applicable to all certificates issued through this EST agent.

6. Enter/Select the following **Advanced Settings**:

Field	Description
Include Truststore Certificates*	Depending on whether you want to share the Truststore certificates with the client during authentication, select Yes (default) or No.
Retry Count*	Enter the maximum number of calls the EST agent will trigger to collect a certificate from AppViewX till it is received. Minimum value: 5 Maximum value: 99
Retry Frequency*	Enter the duration in seconds for which the EST agent will wait between triggering the calls. Minimum value: 10 Maximum value: 99

7. Click **Save**.
   The details of the EST agent thus added are displayed on the main **Auto Enrollment : EST** screen.



   The URL given here can be used for communication between the AppViewX EST agent and the IoT device requesting auto enrollment.

SCEP

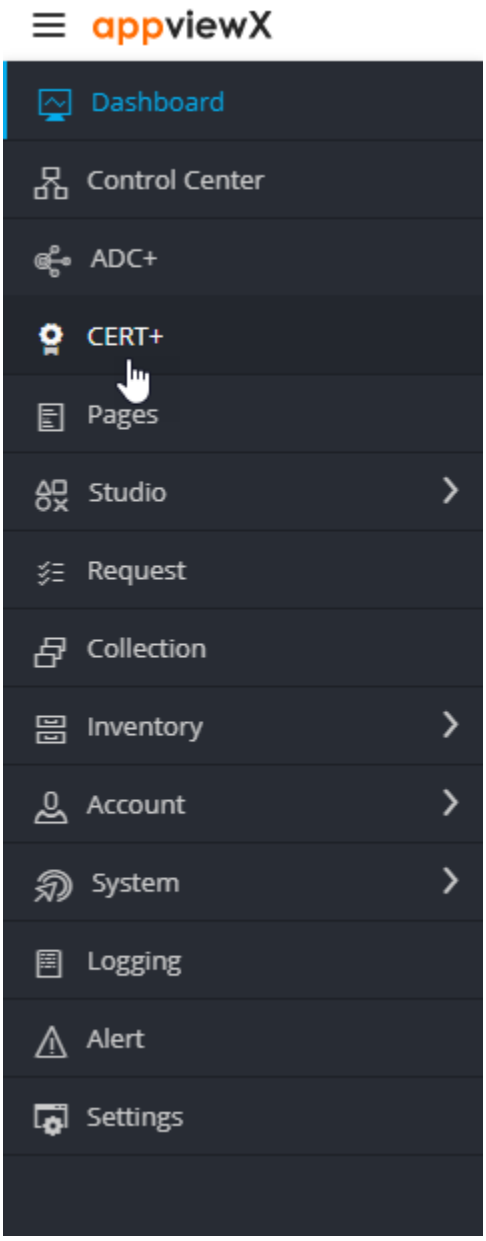
The Simple Certificate Enrollment Protocol (SCEP) allows devices to easily enroll for a certificate by using a URL and a shared secret key to communicate with a Public Key Infrastructure (PKI).

- Accessing the SCEP Settings
- Enabling SCEP for Auto-Enrollment

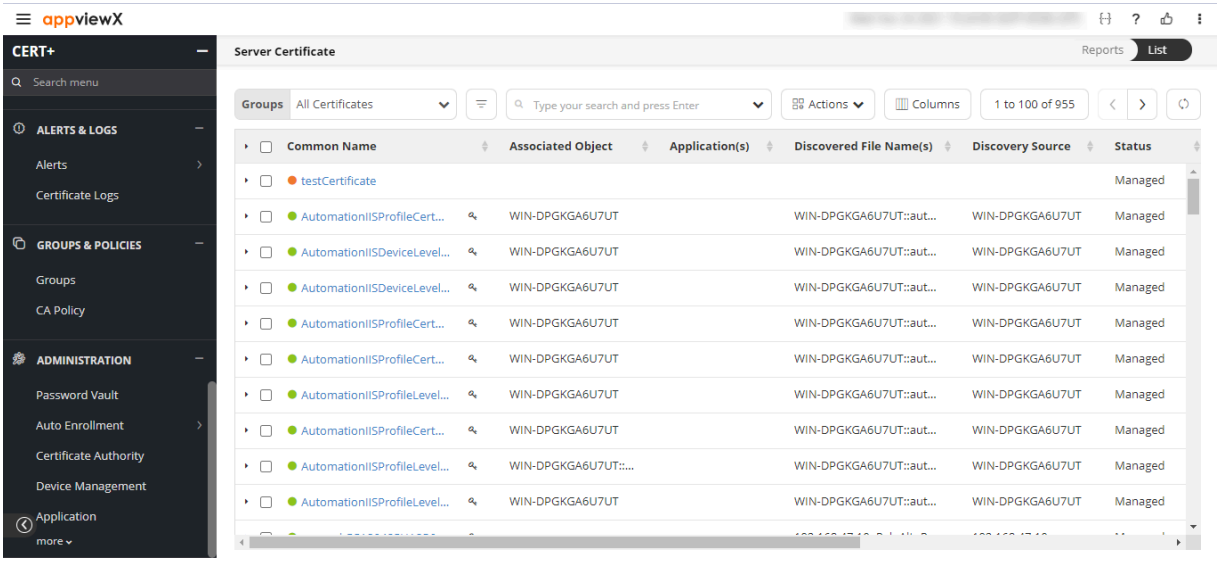
Accessing the SCEP Settings

1. Login to AppViewX with your valid credentials.
   By default, the **Dashboard** is displayed.

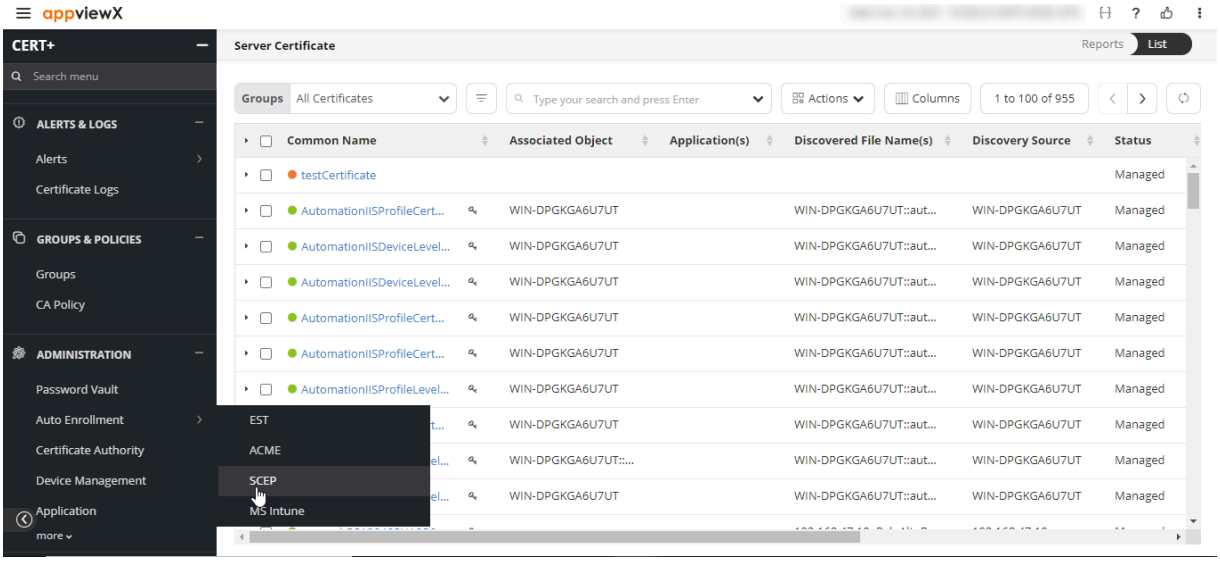
2. From the top-right corner of the **Dashboard**, click ☰.
3. From the menu displayed, select **CERT+**.



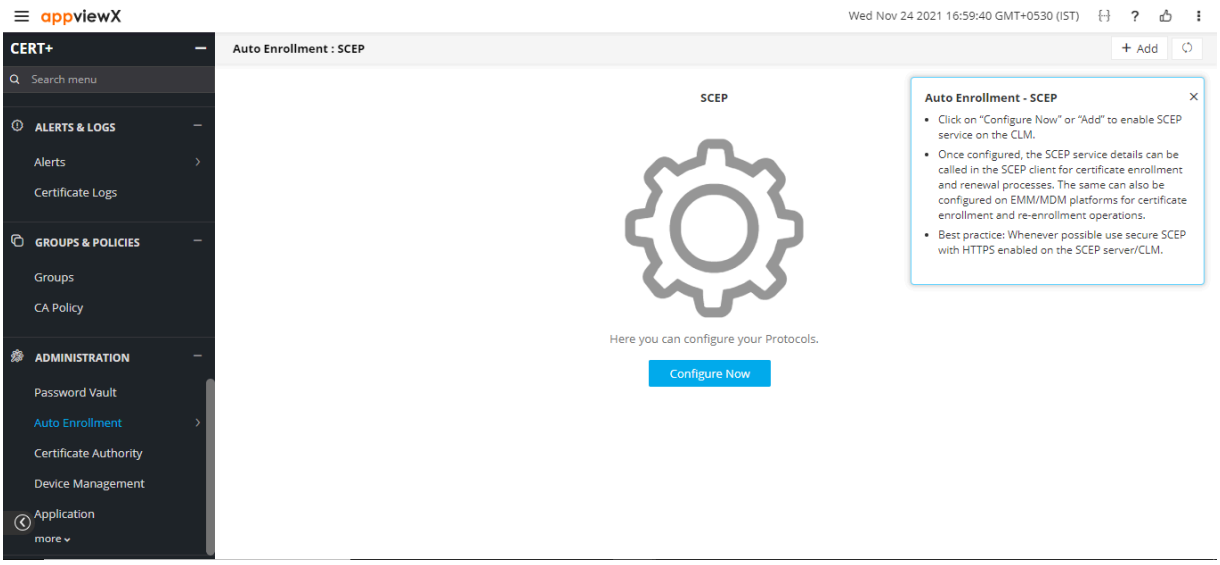
The CERT+ **Server Certificate** page is displayed.



4. In the CERT+ menu, scroll down to the **Administration** section and select **Auto Enrollment** > **SCEP**.



The **Auto Enrollment : SCEP** page is displayed.

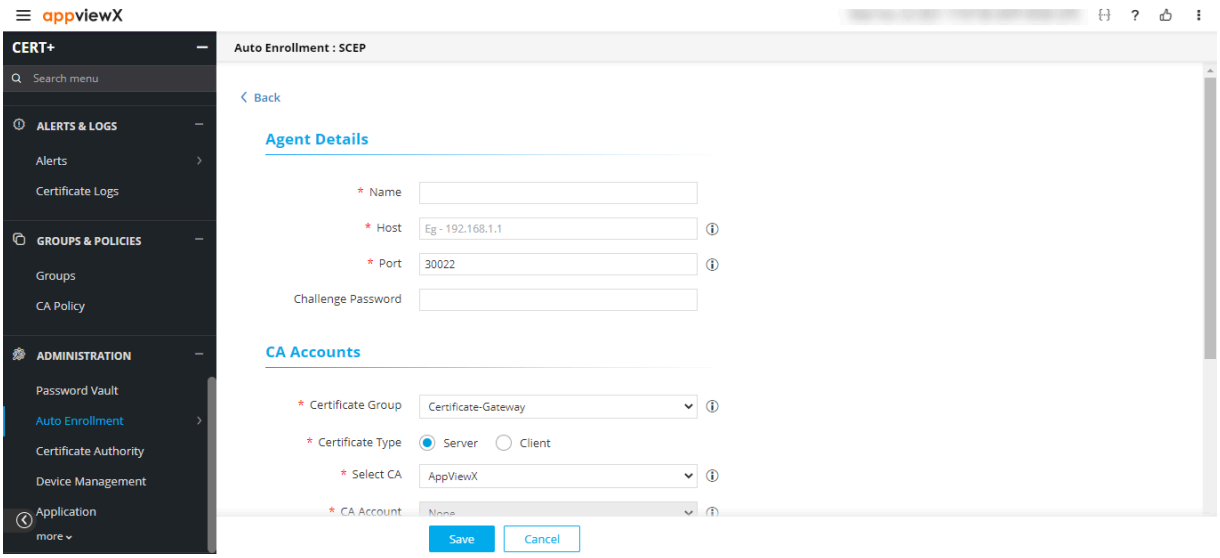


Enabling SCEP for Auto-Enrollment

1. Navigate to the **Auto Enrollment : SCEP** page.
2. To enable SCEP for auto enrollment, click Configure Now or + Add.

> **Note:** The **Configure Now** button is displayed only if you are enabling your first SCEP agent.

The **Auto Enrollment : SCEP** page is updated to display the fields for enabling SCEP.



3. Enter/Select the following details in the **Agent Details** section:

Field	Description
Name*	Enter a unique name for the SCEP agent. **Note:** Only alphanumeric and the following special characters are allowed: period (.). hyphen (-), and underscore (_). The agent name cannot begin with a special character.
Host*	Enter the FQDN or IP address of the AppViewX Cloud Connector.
Port*	Enter the following port number: **30022**
Challenge Password	Configure the challenge password that will be used for enrolling certificates.

Note: Fields with red asterisk (*) symbol are mandatory.

4. Enter/Select the following **CA Accounts** details:

Field	Description
Certificate Group*	From the following options in the dropdown list, select a certificate group for managing certificates in the server/client inventory: • Certificate-Gateway • TestGroup • WOApprovalGroup • Default • CreateCertGroup
Certificate Type*	Select a certificate type from the following options: • Server (default) • Client
Select CA*	From the dropdown list, select the Certificate Authority that the SCEP agent will communicate with while performing the certificate auto enrollment actions.

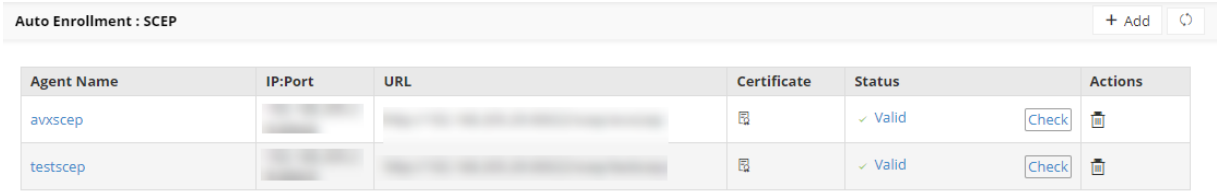
Field	Description
CA Account*	From the dropdown list, select the Certificate Authority account that the SCEP agent will communicate with while performing the certificate auto enrollment actions. **Note:** This dropdown list will be populated with valid values only when the CA account is added to the CA settings.
Server Certificate*	Enter the common name for the server certificate that will be used for authentication. **Tip:** Enter up to three characters of the certificate name/serial number for a list with matching values to be displayed. You can then select the server certificate from this list. **Note:** Only server certificates that are available in the root or intermediary certificates' inventory will be shown for selection in the above mentioned list.
CA Connector Name*	Enter the CA connector name. This connector name will be shown in the holistic view for all the certificates issued through this SCEP agent.
Certificate Validity*	Enter a validity period, in days, that will be applicable to all certificates issued through this SCEP agent.

5. Enter/Select the following **Advanced Settings**:

Field	Description
Include Truststore Certificates*	Depending on whether you want to transfer the Truststore certificates along with the end certificate to the end device, select Yes (default) or No.
Retry Count*	Enter the maximum number of calls the SCEP agent will trigger to collect a certificate from AppViewX till it is received. Minimum value: 5 Maximum value: 99
Retry Frequency*	Enter the duration in seconds for which the SCEP agent will wait between triggering the calls.

Field	Description
	Minimum value: 10 Maximum value: 99
Certificate Poll Type*	To poll the issued certificate from the SCEP agent to the subsystem certificate plugin, select a certificate poll type from the following options: • Issuer and Subject (default) • Transaction ID

6. Click **Save**.
   The details of the SCEP agent thus added are displayed on the main **Auto Enrollment : SCEP** screen.



   The URL given here can be used for communication between the AppViewX SCEP agent and the IoT device requesting auto enrollment.

Chapter 9: EST Configuration

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.

AppViewX EST Client Security

AppViewX EST Clients provides two levels of security:

- Encrypts the authentication data using Installer Generator.
- Creates DATA-CHALLENGE during the installation using unique machine parameters and agent gets executed only when DATA-CHALLENGE decryption is successful.

AppViewX EST Installer Generator

Traditional EST Enrollment methods like curl or wget will have an Authentication Certificate kept open in the user machine.

AppViewX provides a solution to this using AppViewX Installer Generator Software, which encrypts the complete authentication data to a Single DATA file and during the installation we need to copy only the DATA file to the user machine. This restricts the user from reading or modifying authentication DATA.

AppViewX EST Installer

During the Installation of the AppViewX EST Client, it creates an encrypted DATA-CHALLENGE secret, which contains unique machine parameters and, in each execution, it triggers a request only when DATA-CHALLENGE decryption is successful. This protects agents from copying and executing from another machine.

Configuring AppViewX EST Server

Prerequisites

Verify EST Server Status (Enabled/Disabled)

1. Make sure that the EST plugin and external gateway are configured with respective data center (DC) names, in **appviewx.conf** file under **<appviewx_kubernetes/scripts directory>**:
   - **avx_platform_gateway_external=<dc name>**
   - **avx_vendor_cert_est_agent=<dc name>**

   Note: These changes must be made before configuring the EST Agent Configurations in UI.

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

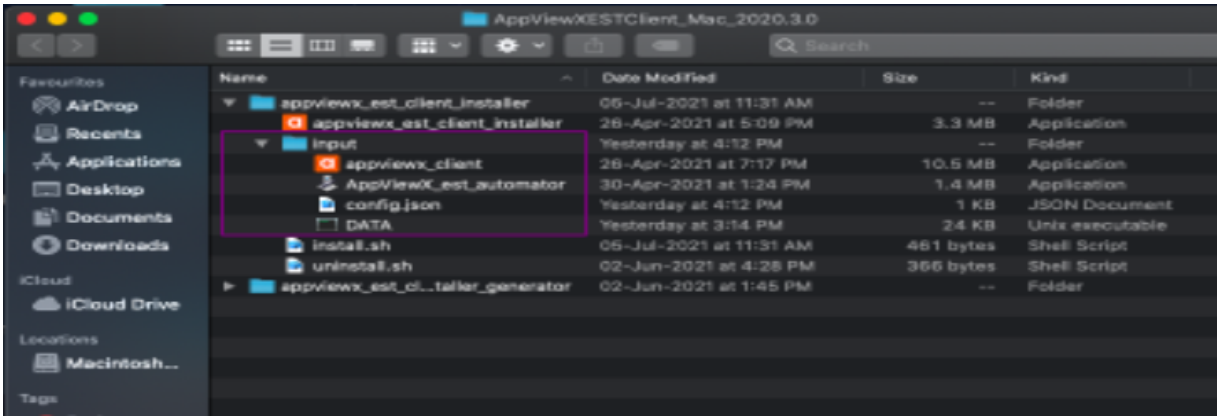
```
[appviewx@smenode2 ~]$ kubectl get services -A | grep est
external-system        avx-platform-gateway-est                NodePort    10.101.89.37    <none>        5301:30739/TCP
smedc1                 avx-vendor-cert-est-agent               ClusterIP   10.105.120.24   <none>        5306/TCP
[appviewx@smenode2 ~]$
```

Note: if services are running, then note the port number that is shown after 5301: <est_external_port>. This port needs to be configured in EST Settings UI.

Enable EST Services

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

1. Open the terminal window.
2. Ensure **avx_vendor_cert_est_agent** is up and running in the EKS cluster.
3. When you install Cloud Connector, you are prompted with **Do you need Auto-enrollment of the certificate using EST/SCEP/ACME?**. Type **y** to continue.
4. You are prompted with **Please choose one or more protocol**. Type **1** to choose EST protocol.

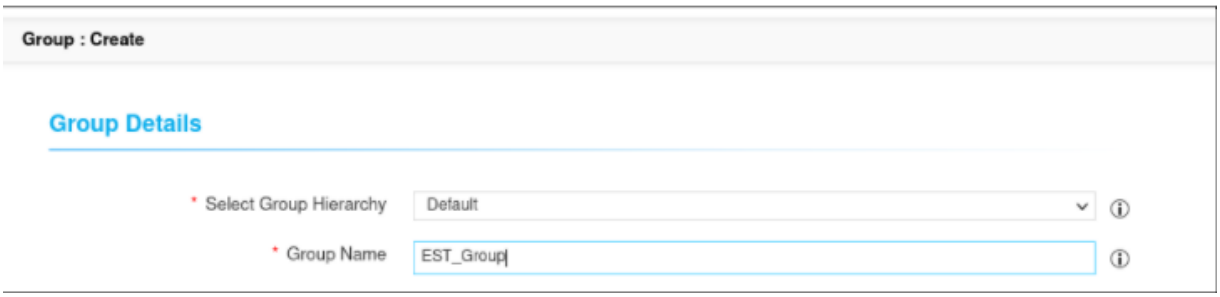


A message that auto enrollment is successful for protocol appears.

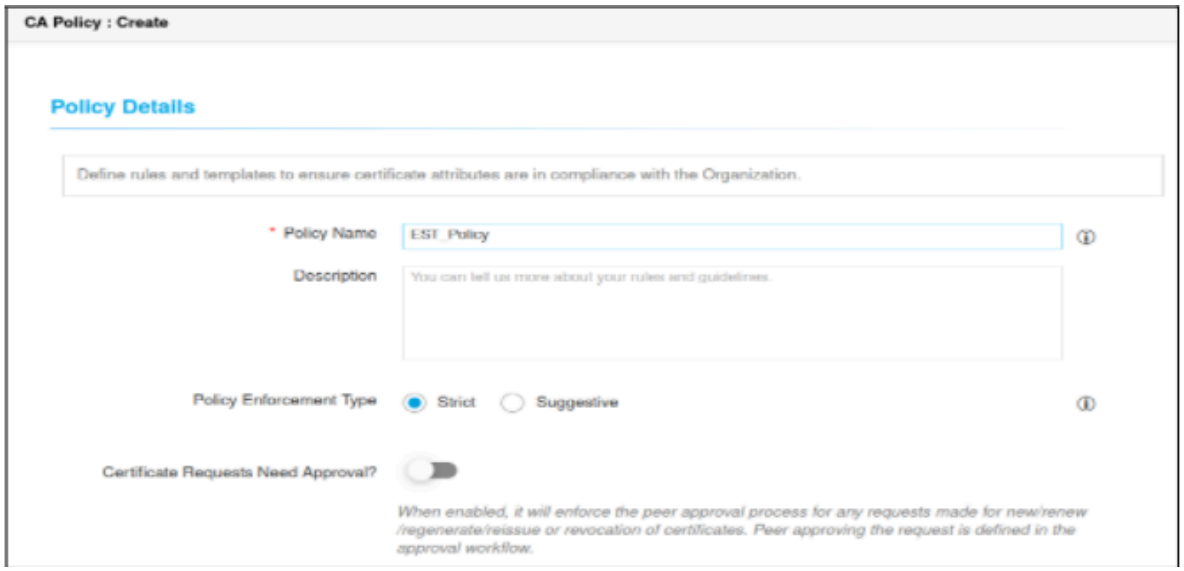
5. Verify the plugin status and port number:
   a. Execute the `<kubectl get services -A | grep est>` command and make sure that the **avx-vendor-cert-est-agent** is running in Cloud Connector.
   b. Make sure that the port number is **5301:30021** in **avx-platform-gateway-est**.

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

6. [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.



7. 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.

8. 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*.

Create Client Authentication Certificate Using AppViewX CA

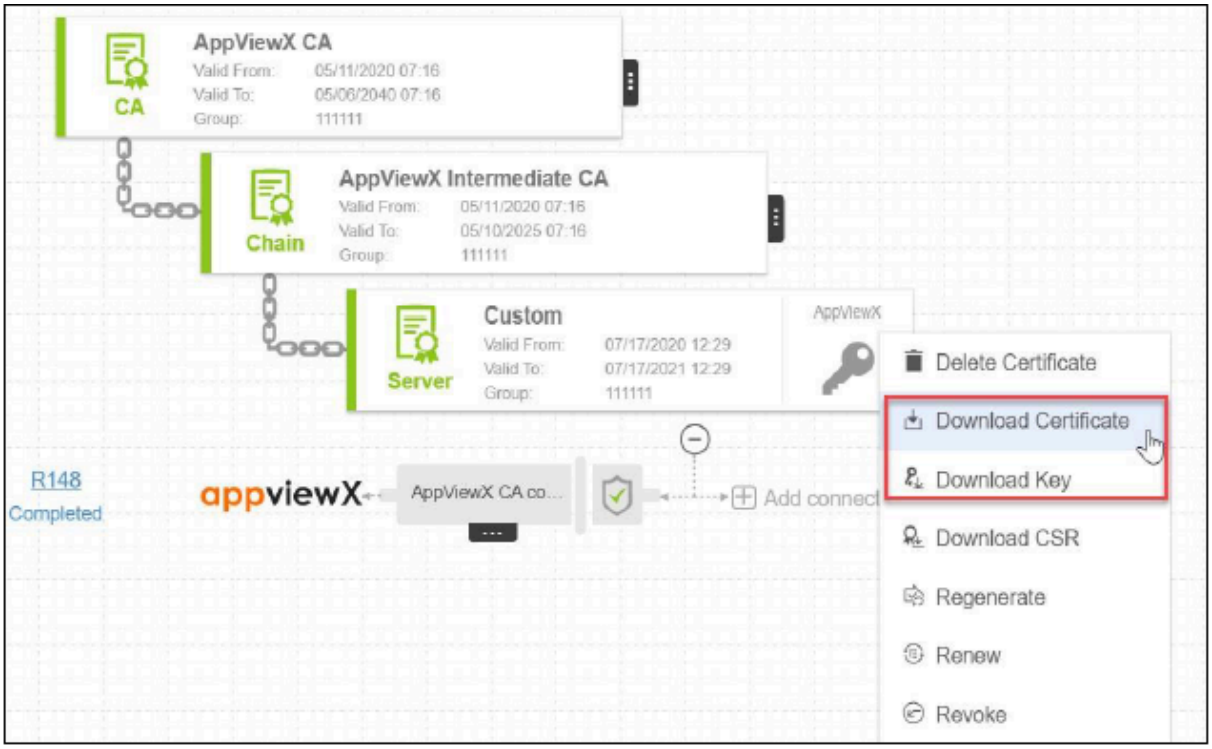
If the user does not have a client authentication AppViewX CA certificate, user can use AppViewX CA. To use a client authentication AppViewX CA certificate:

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.

EST UI Configuration

To configure the EST server:

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. Select **Administration** > **Auto-Enrollment** > **EST**.

On the EST list view page, **defaultEST** is displayed by default.

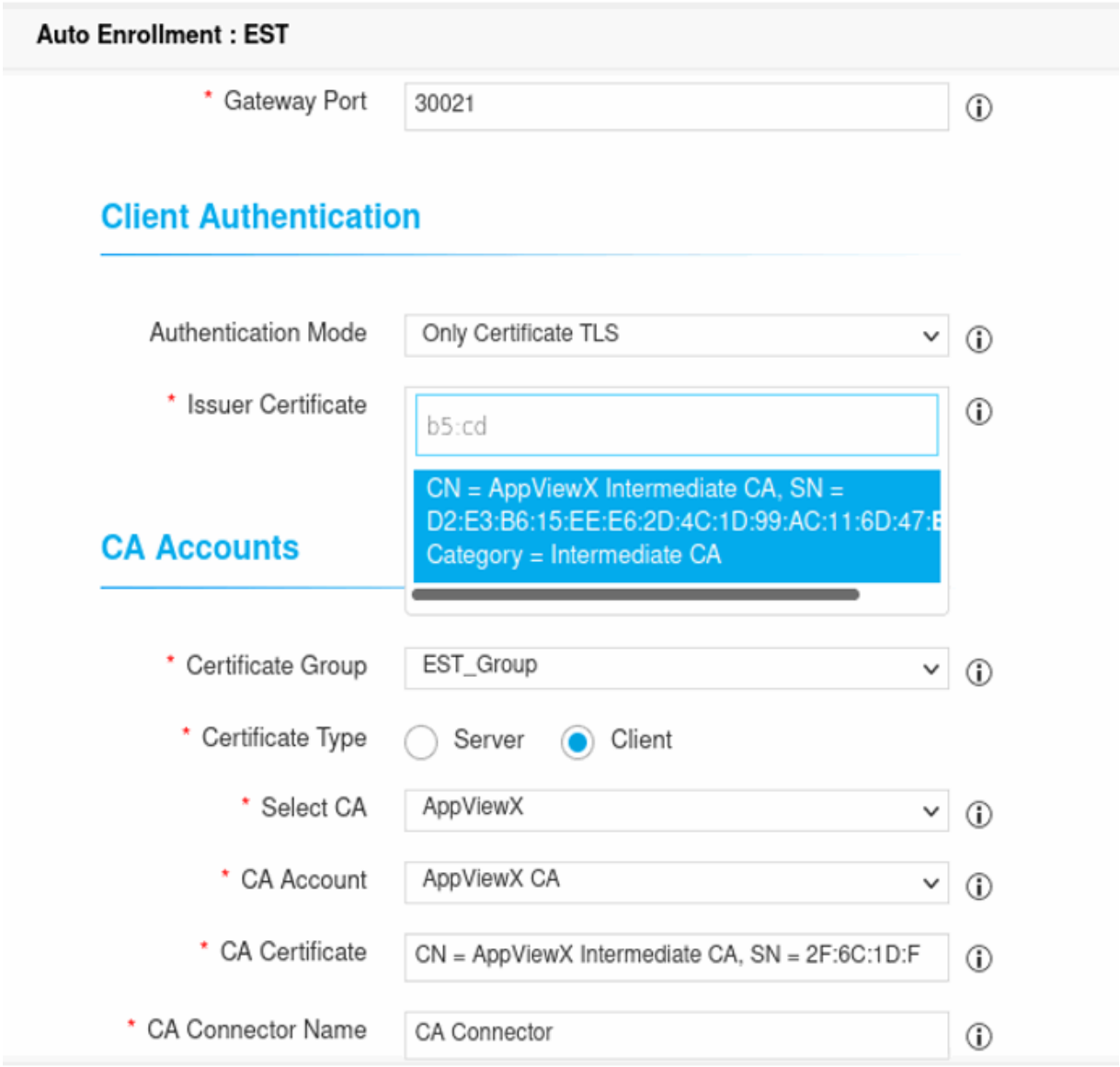
5. Click **+ Add** icon on the top-right.
6. On the EST details page, under the **Agent Details** section, enter the Name, IP Address (Cloud Connector where EST is enabled) and 30021 (gateway port).
7. Under the **Client Authentication** section, select an **Authentication Mode** from the drop- down list.
   - Only Certificate TLS (If you are using AppViewX EST client) - During client authentication, only certificate TLS based authentication will be performed.
   - Certificate TLS with HTTP as Fallback - During client authentication, when the certificate TLS fails, HTTP based authentication will be performed as a Fallback.
   - Both Certificate TLS and HTTP - During client authentication, both certificate TLS and HTTP based authentication will be performed respectively after the successful completion of the other.
8. If the user selects **Certificate TLS with HTTP as Fallback** or **Both Certificate TLS** and **HTTP** mode, the user will be prompted to enter the username and password along with the option to select the **HTTP Authentication Mode**.

   Note: HTTP authentication mode is not supported in AppViewX EST agent.

9. Select an HTTP Authentication Mode: **Basic** or **Digest**
   - **Basic** - During client authentication, only the username and password values will be considered for the HTTP based authentication.
   - **Digest** - During client authentication, along with the username and password, nonce and realm values will be supported.

   Note: This is the same certificate that was uploaded in the **Upload the Client Authentication CA Certificate** section.

10. Select the **Issuer Certificate** by entering the first three letters of the certificate name or serial number.



11. Under the **CA Settings** section, select the **Certificate Group** from the drop-down list.
12. Select the Certificate Type as **Client** or **Server** based on the requirement.
13. Select the **CA** and **CA Account** from the respective drop-down lists. At present, AppViewX supports only AppViewX CA, EJBCA, and Microsoft CA.
14. In the **CA Certificate** field, enter the certificate name and in the **CA Connector Name** field, enter a name for the CA Connector.
15. In the **Certificate Validity** field, enter the number of days.
16. Under the **Advanced Settings** section, select the **Yes** or **No** radio button to include or exclude truststore certificates. You can choose an option whether to share the trust store certificate with the client during the get CA operation.

17. Enter the **Retry Count** and **Retry Frequency** in the respective fields.
18. Click **Save.**

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

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>

Best Practices for EST Server

The following are the best practices:

- For auto-enrollment, create a separate certificate group and CA policy in AppViewX.
- Enable auto-renewal in the AppViewX policy.
- During policy creation, select only required bit-length (minimum 2048 bit).
- For machine enrollment, define an expected domain name in the CA policy for machine CSR (for example, *.appviewx.com) to avoid issuing certificates for different domain machines.
- Recommended to use TLS authentication with AppViewX EST clients.
- Recommended to use only private/internal CA as trusted for client authentication (Not recommended to use public CA as trusted to validate clients).
- Select appropriate certificate type: **Server** or **Client** (Select Server only if it is a server certificate and Client for machine and user certificates).

- The recommended validity for the issued certificate is one year.
- Use the trusted CA-signed certificate in a gateway for EST URL.

Adding External CA Trust Certificate for EST Client Authentication

By default, Cloud Connector is started with the default AppViewX intermediate and AppViewX root certificates.

If a certificate from a different CA has to be used instead of AppViewX's default certificate, you must update the relative path of the certificates in the **appviewx.properties** file, which will be in the **<Cloud_Connector_folder>/deps/** directory.

To add any other intermediate or root CAs:

1. Copy the files of the certificate and paste them in the **<Cloud_Connector_folder>/deps/** directory in a desired location.
2. Update the following fields by passing the relative paths of the respective files that were placed in the directory in Step 1.
   EST_TRUSTED_CA_CERTS=<relativepath_after_deps>,<relativepath_after_deps>

Update SSL Certificate for EST-HTTPS Communication

To update SSL certificate for EST-HTTPS communication:

1. By default, there will be a self-signed Certificate available in the location.
2. If a custom certificate is needed instead of the default self-signed certificate, you must update the relative path of the certificates in the **appviewx.properties** file, which will be in the **<Cloud_Connector_folder>/deps/** directory.
3. Copy the files of the certificate and paste them in the **<Cloud_Connector_folder>/deps/** directory in a desired location.
4. Update the following fields by passing the relative paths of the respective files that were placedin the directory in Step 3.

   EST_SERVER_ACCESS_CERT=<relativepath_after_deps>

   EST_SERVER_ACCESS_KEY=<relativepath_after_deps>

Gateway - EST Log

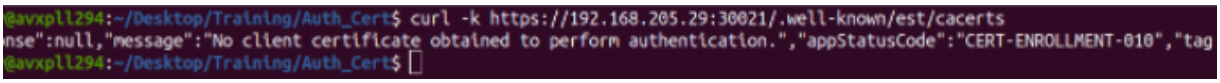
To access the EST logs:

1. Access the terminal window.
2. Go to **<Cloud Connector_Installed_Path>/deps/logs** directory and find file with the name format **<avx-mid-server-gateway-<full pod name>-MTLS.log>**. For example, **<avx-mid-server-gateway-74d6df94b6-km6px-MTLS.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 **avx-mid-server-gateway-MTLS-<yyyy-mm-dd>.log.** For example, **<avx-mid-server-gateway-MTLS- 2021-03-17.log>**.
   - Execute the following command in the AppViewX cluster: `kubectl exec -it <avx-vendor-cert-est-agent pod_name> -n <namespace> -- bash` and move to the logs folder to check the pod logs.

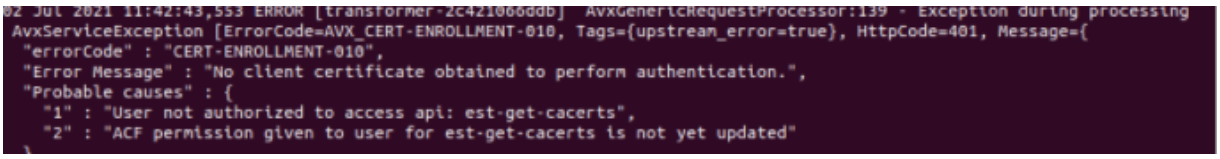
Verification of EST Server

To verify the EST server:

1. Access the terminal window.
2. Execute the `<kubectl get pods -A | grep est>` command and get the pod name.
3. Execute the following command in the AppViewX cluster: `kubectl exec -it <avx-vendor-cert-est-agent pod_name> -n <namespace> -- bash` and move to the logs folder to check the pod logs.
4. Access CACerts URL from the browser or try CURL from another machine to the Cloud Connector IP.



5. Check the log file.



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

Testing EST Enrollment by using CURL

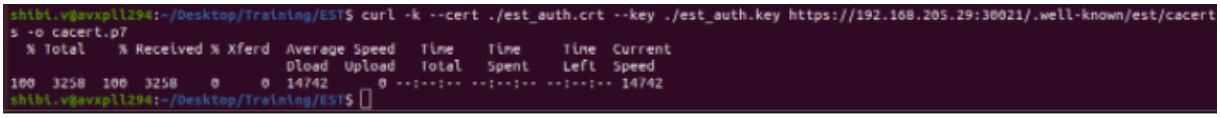
To test the EST enrollment:

1. After the successful verification, create a test folder in the Linux client machine.
2. Copy the <**est_auth.crt**> and <**est_auth.key**> to any directory.

3. Generate the CSR in the same folder/directory with <openssl> command.

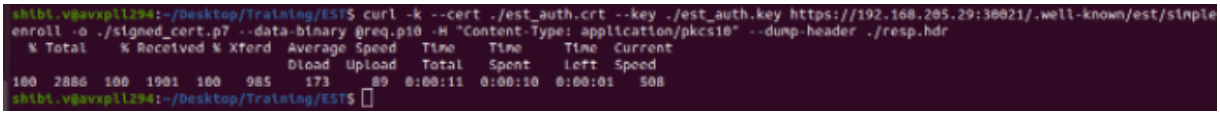
   `openssl req -new -newkey rsa:2048 -nodes -keyout rsakey.key -out req.p10`

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.

Configuring AppViewX EST Clients

- Installation and Configuration of EST Client in Windows Machine
- Installation of the EST Client Agent in Linux Machine
- Installation of the EST Client in Mac System

Installation and Configuration of EST Client in Windows Machine

Prerequisites

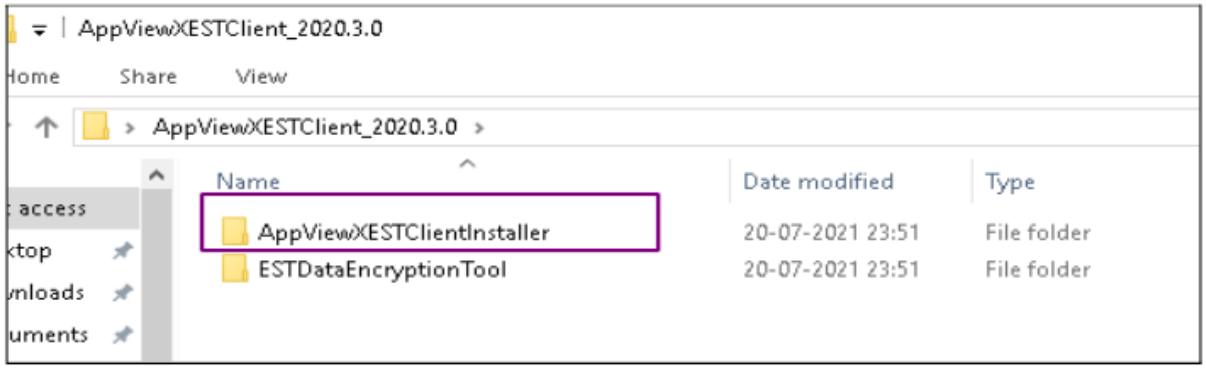
Prerequisites for the EST Client agent installation on a Windows machine:

- Configure EST server in AppViewX.
- Admin access is required to modify the configuration file.
- The minimum <.Net> version required is v4.5.2.
- OS Requirements (Windows: v7.0, v8.0, and v10.0).
- Installation Steps

Installation Steps

To install and configure the EST client:

1. Get the EST client software from the AppViewX release portal.
2. Extract **<AppViewX_EST_Windows_Client_2020.3.0.zip>** file.

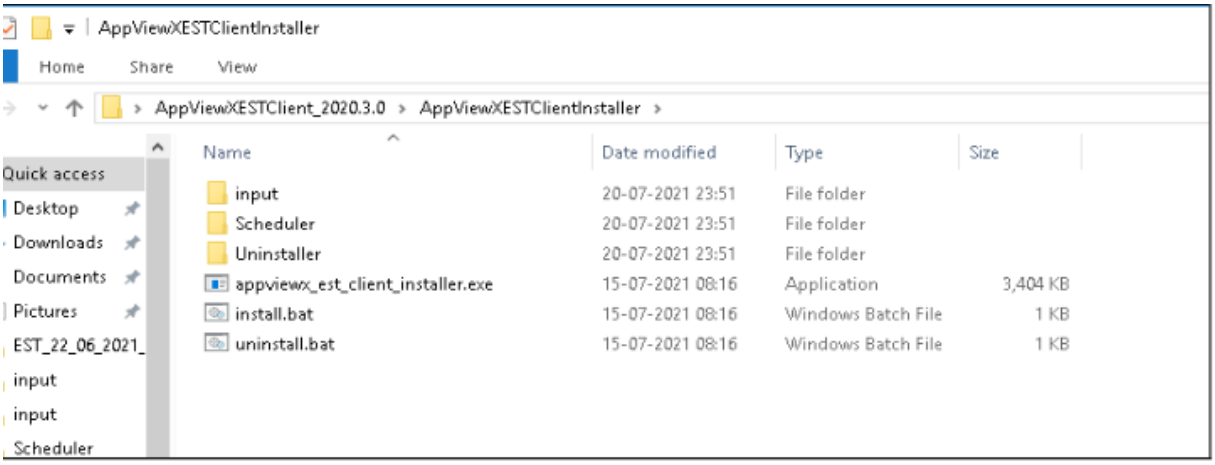


3. Copy the **AppViewXESTClientInstaller** to the user machine.

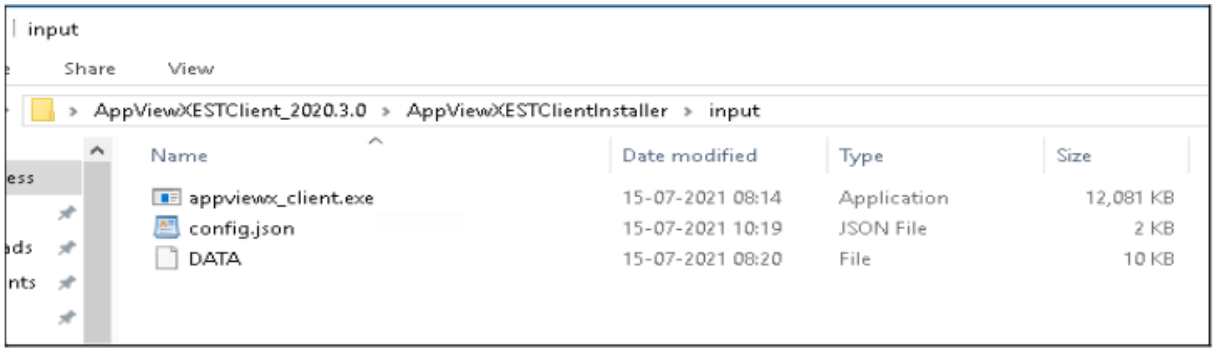
Note: For the initial validation of EST server and client functionality, you can use agent software as it is (this can the reduce the time required to test the feature). Once the validation is successful, you can change Authentication Certificate using the below mentioned documents:

- For Server Side, refer Configuring AppViewX EST Server section.
  - Upload Client Authentication Issuer Certificate In AppViewX.
- For Client Side, refer EST DataEncryption Tool section.

4. The **AppViewXESTClientInstaller** folder contains the following files:



5. The **input** folder contains the following details:

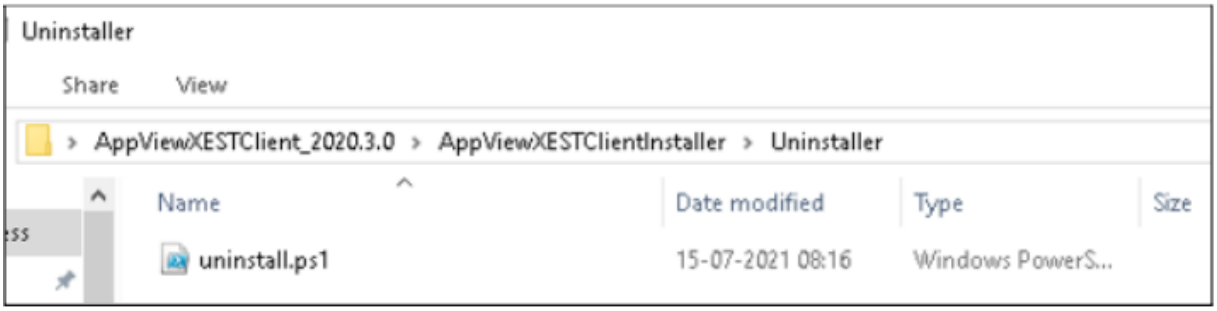


- <**appviewx_client.exe**> - Client software binary (after installation which will get copied to C:/)
- <**config.json**> - Contains configuration files required for enrollment (for Configuration details refer Section 8 edit the configuration file
- The **DATA** file contains the following details:
  - Contains encrypted Authentication Data. Users will not have direct access that is encrypted by using EST DataEncryption Tool.
  - If you are using the same Agent software, need not to update the default DATA file.
  - Encrypted DATA file contains client authentication certificate signed by AppViewXIntermediateCA_D2 E3 B6 15 EE E6 2D 4C 1D 99 AC 11 6D 47 B5 CD.
  - CA Certificate file is uploaded in the Same Drive and you can upload this as the Trusted CA in EST UI Settings. For the Detailed Server Configuration steps, refer to the EST DataEncryption Tool section.

6. The **Scheduler** folder contains the following details:

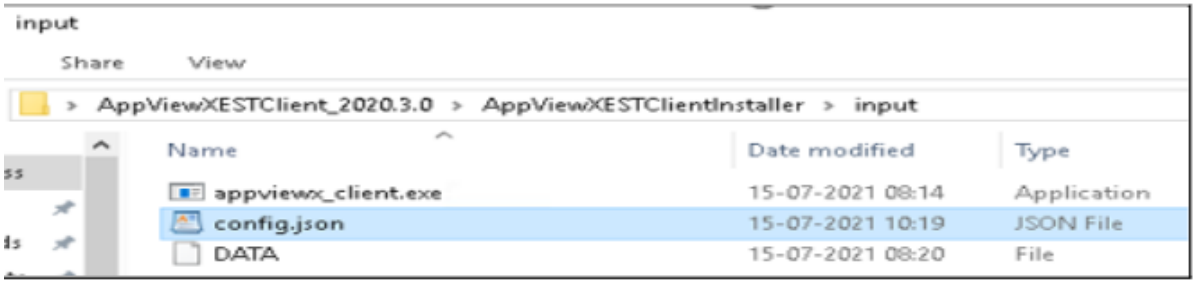
- <**triggerJobSystem.ps1**> - PowerShell Script for creating machine enrollment schedule task. Default trigger is at User LogOn.
- <**triggerJobUsers.ps1**> - PowerShell Script for creating user enrollment schedule task. Default trigger is at User LogOn.

7. The **Uninstaller** folder contains the following details:



- <**uninstall.ps1**> - PowerShell script for uninstalling the AgentSoftware.
- <**appviewx_est_client_installer.exe**> - Binary for Installing the Agent (do not trigger directly as it is handled in install.bat).
- <**install.bat**> - Script to install agent into the machine.
- <**uninstall.bat**> - Script to uninstall agent in from machine.

8. To edit the configuration file, do the steps as follows:
   - Open the **<config.json>** in the input folder.



The following table describes the string details.

String	Description
Hostname	EST Server hostname/IP
Port	30021 is default for AppViewX 20.3 FP5 and above.
Path_seg	AppViewX EST Agent name configured in UI (if you are using default EST, do not EST agent name).

Note: It is not mandatory to have all the types in the config file. You can keep only the type you require and delete the rest.

For example, if the requirement is to enroll only User CERT, then delete “machine” and “Others” from the list.

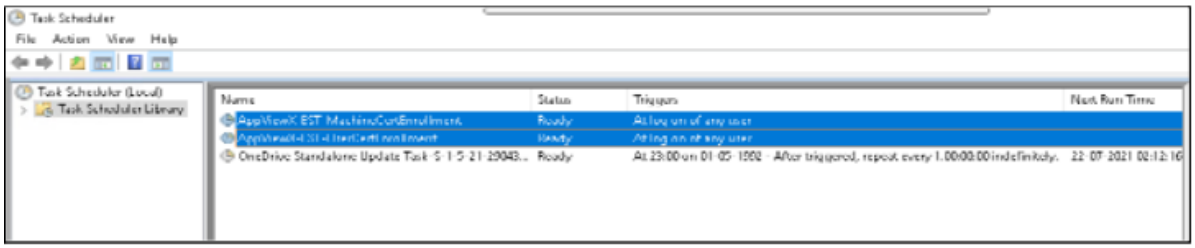
```
    "certificates": [
        {
            "certificate_id": 1,
            "certificate_type": "user",
            "reenrollment_trigger_before_no_of_days_of_expiry": 30        },
        {
            "certificate_id": 2,
            "certificate_type": "machine",
            "reenrollment_trigger_before_no_of_days_of_expiry": 30        },
        {
            "certificate_id": 3,
            "certificate_type": "others",
            "reenrollment_trigger_before_no_of_days_of_expiry": 30,
            "common_name":"sample.commonname.com",
            "store_name": "user",
            "san_dns_names":["sample.san1.com","sample.san2.com"],
            "san_ip_addresses":["10.1.1.1","10.1.1.2"],
            "certificate_country": "US",
            "certificate_province": "Washington",
            "certificate_locality": "Seattle",
            "certificate_organization": "AppViewX Inc",
            "certificate_organization_unit": "Engineering",
            "signed_pem_file_name": "",
            "private_key_file_name": "",
            "cacert_file_name": ""
        }
    ]
}
```

The following table describes the string details:

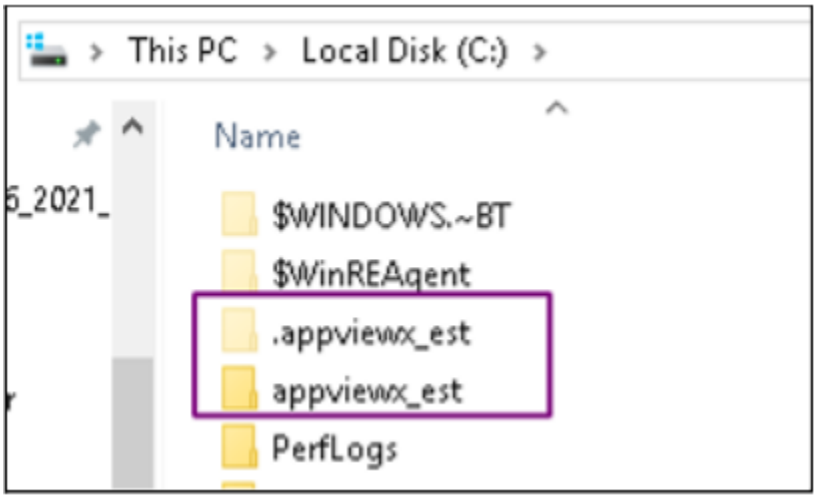
String	Description
Certificate_type	**user:** Generates Logged in Username as CN for the CSR and installs Certificate in User Personal Store (gets logged in username using <**powershell>** command).

String	Description
Certificate_type	**machine:** Generates Machine as CN for the CSR and installs certificate in user personal store (gets machine name using <**hostname**> command).
Certificate_type	**others:** Generates configured common_name as CN for the CSR and installs certificate in the store. • **Store_name: user** installs another certificate type into the user's personal store. • **Store_name: machine** installs another certificate type into the machine store.

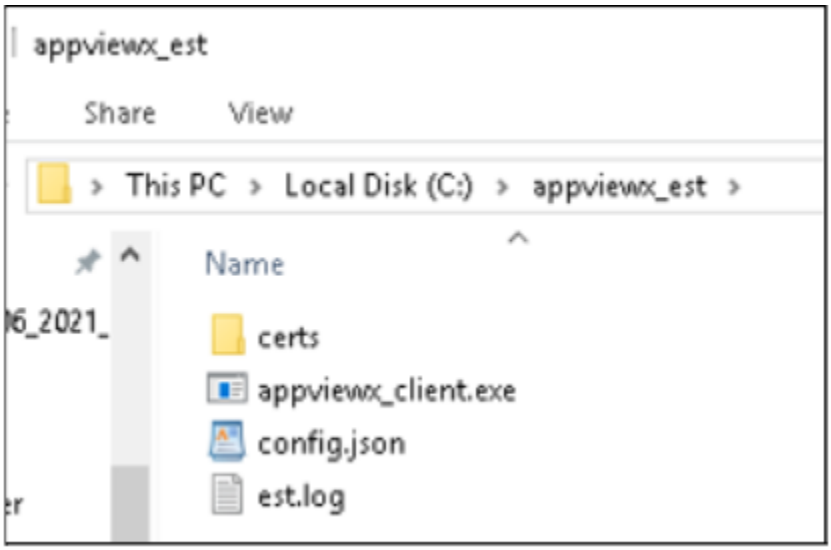
9. To install the agent software, do the steps as follows:
   - Open the **AppViewXinstaller** folder and then select the <**install.bat**> file.
   - Right-click **<install.bat>** file, and then select **Run as administrator**.
     - It creates Machine and User Enrollment tasks in the Windows Task Scheduler.
     - Encrypts the software with machine unique parameters and copies to <**C:/Drive**>.
10. Verify the following steps are completed after installations.
    - Machine and User enrollment tasks need to be created in the task scheduler.



    - Files must be copied to <**C:/Drive**>.



- Validate the copied configuration file in **<C:/appviewx_est/config.json>**.



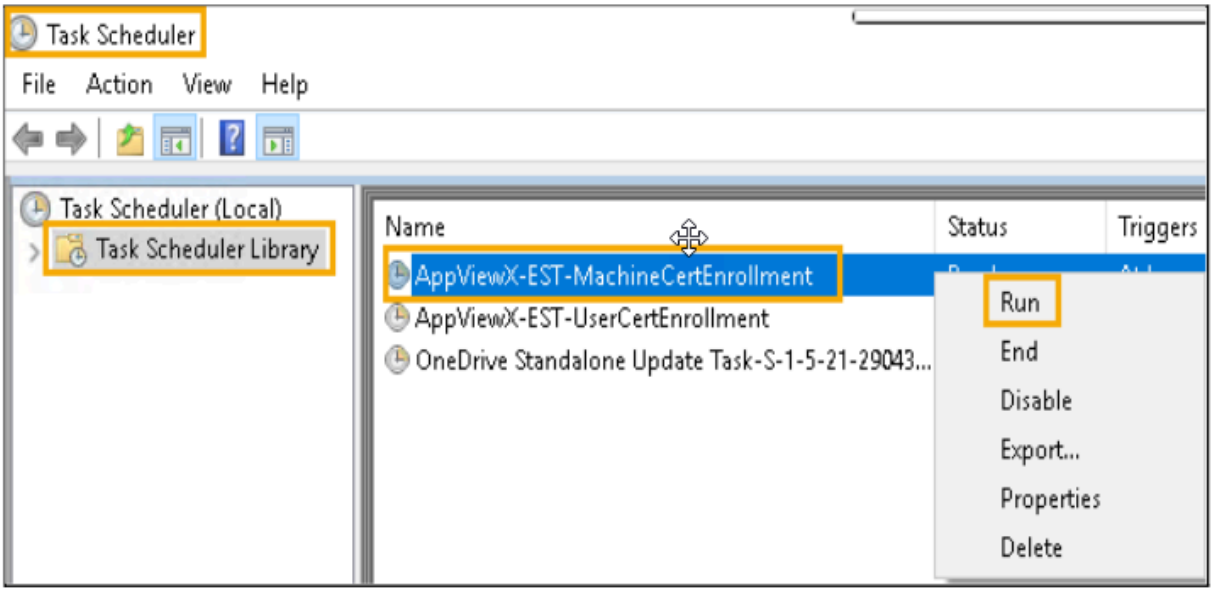
- It should contain the same configuration that is pushed using the <*install.bat*> method <**AppViewXESTClient_2020.3.0\AppViewXESTClientInstaller\input**>.

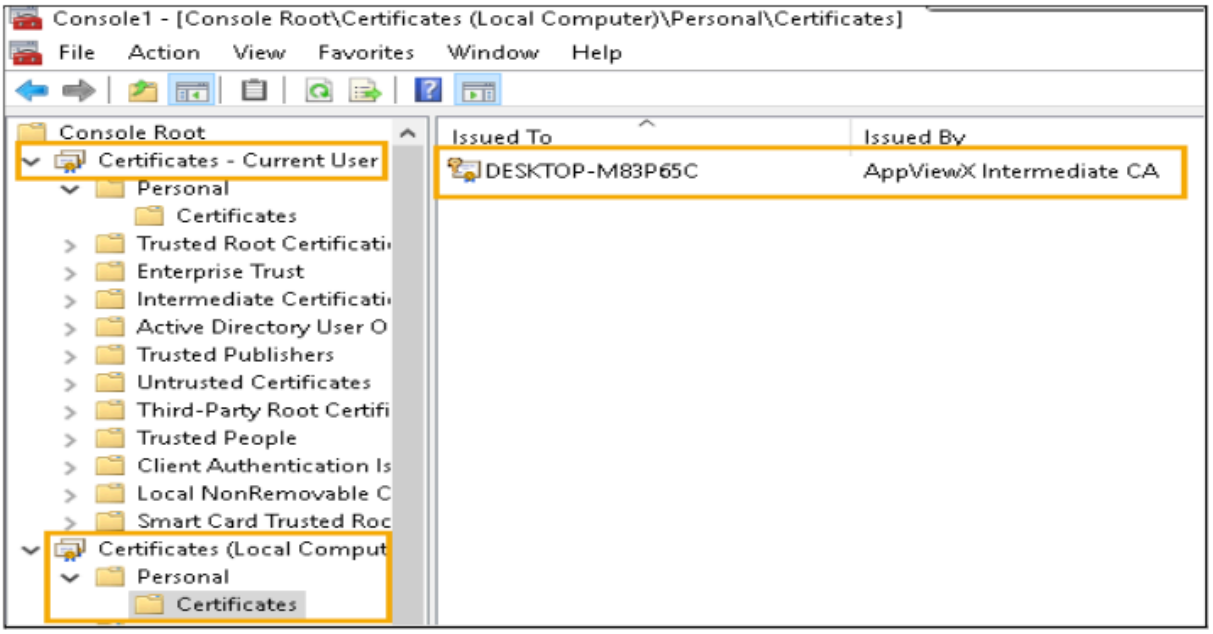
11. To trigger the enrollment task, do the steps as follows:

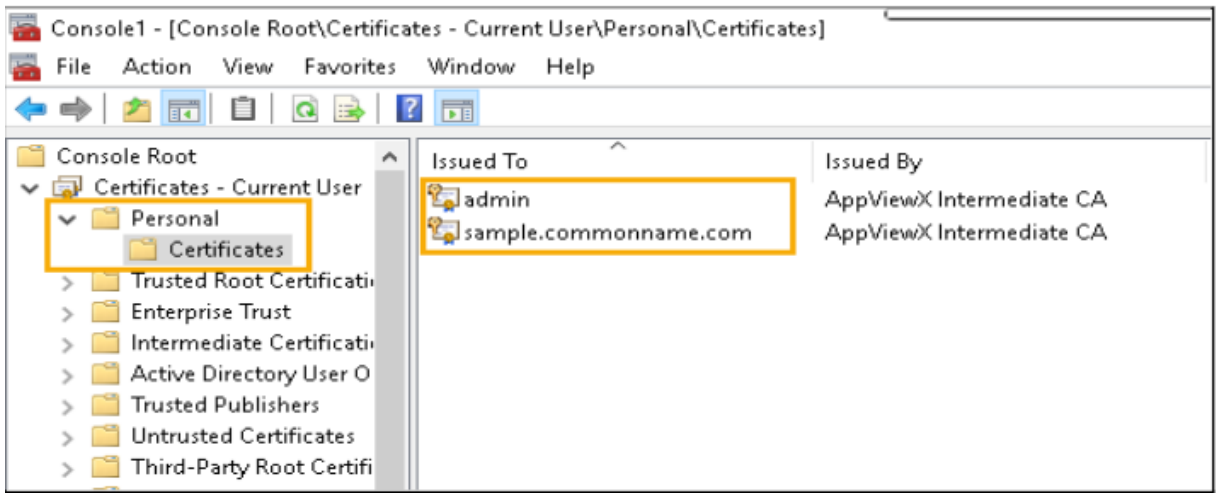
    This agent can either trigger automatically when a user logs in or manually from the Task Scheduler.

    - Open the task scheduler library, and then select the <**AppViewX-EST-MachineCertEnrollment**> file.
    - Right-click the <**AppViewX-EST-MachineCertEnrollment**> file, and then click **Run** to run the tasks.

    Note: The certificates will be installed in the store within 30 seconds.







Installation of the EST Client Agent in Linux Machine

This section covers the installation procedures for the EST client agent on a Linux machine to perform certificate enrollment tasks.

Prerequisites

Crontab should be available for the installing user. Cron acts as a scheduler to trigger an enrolment task in a Linux machine. If it is not enabled, the user should execute the agent manually. To schedule it, execute the command: `<./appviewx_est_client_installer -cron "10 * * * *"; >.`

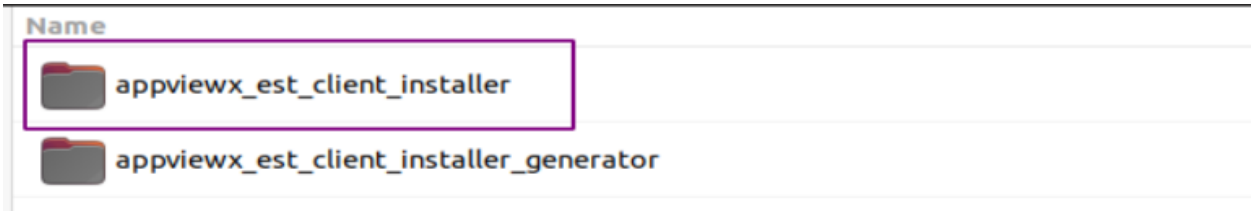
OS Requirements

Supported OS and their versions are mentioned in the following table:

OS	Versions
Redhat	v7.3 and later
Ubuntu	v18.04 and later
CentOS	v7.0 and later
Debian	v10.0 and later
FreeBSD	v12.1 and later
Fedora	v29.0 and later
Mint	v18.2 and later

Installation Steps

Step 1: Download and Extract Agent Software



Note: The **appviewx_est_client_installer** is the only folder needed on the client machine.

1. Use **Appviewx_est_client_installer_generator** only for encrypting authentication data. (In this package, it is already done and encrypted **DATA** is available in **appviewx_est_client_installer/input** folder).
2. If you use this Agent software as it is, you need not to update the default DATA file.

   This Encrypted DATA file contains Client Authentication Certificate Signed by **AppViewXIntermediateCA_D2 E3 B6 15 EE E6 2D 4C 1D 99 AC 11 6D 47 B5 CDI**.

   This CA Certificate file is uploaded in the same drive and you can upload this as the Trusted CA in EST UI Settings
3. For the Detailed Server Configuration Steps, refer to Step 5: Upload Client Authentication Issuer Certificate in AppViewX in Configuring AppViewX EST Server.
4. To generate a new data file, refer Section, EST DataEncryption Tool.

Step 2: Edit Client's Configuration File and Add Server Details

1. Open **appviewx_est_client_installer/input/config.json**.
2. Under EST Servers, update as mentioned below:
   - Server hostname/ip
   - Port number
   - path_seg (AgentName needs to be added here, if user wish to get certificates via a particular Agent configured in AppViewX)

```
{
        "est_servers": [

                {
                        "certificate_type": "user",
                        "host_name": "pm-apvx-1.lab.appviewx.net",
                        "port": 30021,
                        "path_seg": ""
                },
                {
                        "certificate_type": "machine",
                        "host_name": "pm-apvx-1.lab.appviewx.net",
                        "port": 30021,
                        "path_seg": ""
                },
                {
                        "certificate_type": "others",
                        "host_name": "pm-apvx-1.lab.appviewx.net",
                        "port": 30021,
                        "path_seg": ""
        }
        ],
```

3. Under Certificates, mention required fields:
   a. **Certificate_id** and **certificate_type** are the only mandatory fields.
   b. Other fields are optional.
   c. **Certificate_type: user is** automatically fetched a currently logged in user name as the CN.
   d. **Certificate_type: machine automatically** fetches machine name as the CN.
   e. **Certificate_type: others**:any CN, SAN DNS, or SAN IP can be given.
   f. **Certificate and Key Location**: By default, Certificates are stored in to **/home/<username>/ appviewx_est/certs** folder as pem file.

```
"certificates": [
        {
                "certificate_id": 1,
                "certificate_type": "user",
                "certificate_country": [""],
                "certificate_province": [""],
                "certificate_locality": [""],
                "certificate_organization": [""],
                "certificate_organization_unit": [""],
                "reenrollment_trigger_before_no_of_days_of_expiry": 25,
                "signed_pem_file_name": "",
                "private_key_file_name": "",
                "cacert_file_name": ""
        },
        {
                "certificate_id": 2,
                "certificate_type": "machine",
                "certificate_country": [""],
                "certificate_province": [""],
                "certificate_locality": [""],
                "certificate_organization": [""],
                "certificate_organization_unit": [""],
                "reenrollment_trigger_before_no_of_days_of_expiry": 25,
                "signed_pem_file_name": "",
                "private_key_file_name": "",
                "cacert_file_name": ""
        },
        {
            "certificate_id": 3,
            "certificate_type": "others",
            "reenrollment_trigger_before_no_of_days_of_expiry": 30,
            "signed_pem_file_name": "",
            "private_key_file_name": "",
            "cacert_file_name": "",
            "common_name":"test.test.con",
            "san_dns_names":["*.google.co.in","*.google.in","google.co.in","google.in"],
            "san_ip_addresses":["192.168.98.215","192.168.98.215"],
                        "additional_cert_formats":["pkcs12"]
        }
```

Step 3: Install Linux EST Client

To install the Linux EST client:

1. Open terminal **in appviewx_est_client_installer**.
2. Execute `./appviewx_est_client_installer`.

```
shibi.v@avxpll294:~/Desktop/Training/EST/New/AppViewX_EST_Agent_Linux_2021/appviewx_est_client_installer$ ./appviewx_est_client_installer
constants.EST_HOME_VISIBLE :  /home/shibi.v/appviewx_est logFile :  est.log
Creating folder  /home/shibi.v/.appviewx_est
Creating folder  /home/shibi.v/appviewx_est
Creating folder  /home/shibi.v/appviewx_est/certs
Created Folders
EST Client installed successfully
shibi.v@avxpll294:~/Desktop/Training/EST/New/AppViewX_EST_Agent_Linux_2021/appviewx_est_client_installer$
```

Client is automatically installed in the User **Home** folder.

Step 4: Trigger Enrollment Request

To trigger enrollment request:

1. Go to **User Home/appviewx_est**.
2. Execute the command: `./appviewx_client est auto.`

```
shibi.v@avxpll294:~/appviewx_est$ ./appviewx_client est auto
Making Enrollment
Initiating Call  avxpll294.appviewx.com machine
Added a Certificate to Keystore ID : 4, SerialNumber : 3244B2045AB9F3AE55FFB1E4F1A005AC
Agent Execution Completed
shibi.v@avxpll294:~/appviewx_est$
```

The enrolled certificate gets stored in the AppViewX Client's local keystore.

Step 5: Verification of Supported Commands in AppViewX Client

To verify:

Go to **Home/appviewx_client/certs**. Type --help to see supported commands.

```
shibi.v@avxpll294:~/appviewx_est$ ./appviewx_client --help
Usage:
  appviewx_client [command]

Available Commands:
  est         est protocol based certificate enrollment and reenrollment
  help        Help about any command
  keystore    keystore ( Only for linux )
  version     version

Flags:
  -h, --help   help for appviewx_client

Use "appviewx_client [command] --help" for more information about a command.
shibi.v@avxpll294:~/appviewx_est$
shibi.v@avxpll294:~/appviewx_est$
```

```
shibi.v@avxpll294:~/appviewx_est$ ./appviewx_client keystore -h
keystore ( Only for linux )

Usage:
  appviewx_client keystore [command]

Available Commands:
  download    download get the list of certificates
  list        list get the list of certificates

Flags:
  -h, --help   help for keystore

Use "appviewx_client keystore [command] --help" for more information about a command.
shibi.v@avxpll294:~/appviewx_est$
```

Command to verify certificates stored in keystore:

```
shibi.v@avxpll294:~/appviewx_est$ ./appviewx_client keystore list
+-------------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------+
|ID    |Common Name              |SerialNumber                                |Download Type  |Created Date
 |Expiry Date                   |
+-------------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------+
|0     |avxpll294.appviewx.com   |5C4DD353A41B97C4FC819A72DEA777F3            |p12            |Thu Jun  2 20:48:41 2022
 |Fri Jun  2 15:17:26 2023      |
|1     |avxpll294.appviewx.com   |DCE76DBDF369B0175F64C7A4AC3A88E2            |p12            |Thu Jun  2 20:51:01 2022
 |Fri Jun  2 15:19:45 2023      |
|2     |avxpll294.appviewx.com   |4D6F0008EDABA70311B0CEB0FF3F335C            |p12            |Thu Jun  2 20:51:45 2022
 |Fri Jun  2 15:20:30 2023      |
|3     |avxpll294.appviewx.com   |A13462C94DA04574C4555574328B0CDA            |p12            |Thu Jun  2 20:55:20 2022
 |Fri Jun  2 15:24:04 2023      |
|4     |avxpll294.appviewx.com   |3244B2045AB9F3AE55FFB1E4F1A005AC            |p12            |Fri Jun  3 11:44:45 2022
 |Sat Jun  3 06:13:29 2023      |
+-------------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------+
shibi.v@avxpll294:~/appviewx_est$
```

Command to download certificates stored in keystore:

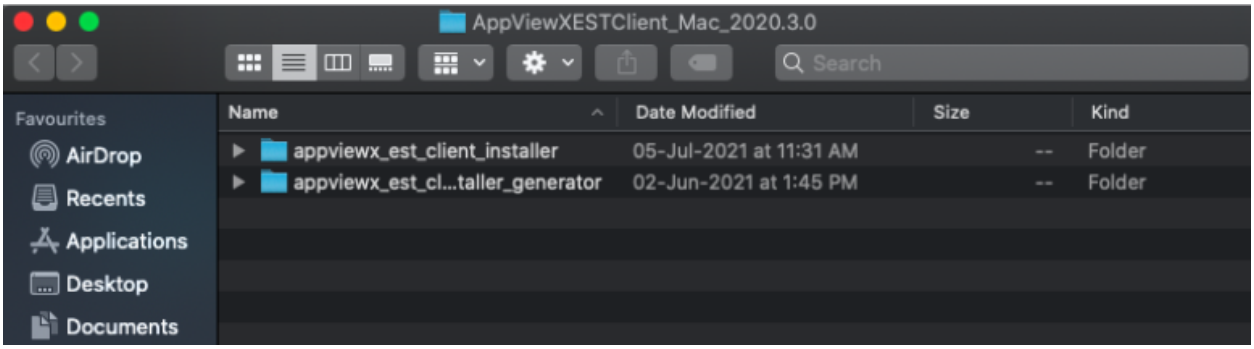
```
shibi.v@avxpll294:~/appviewx_est$ ./appviewx_client keystore download -h
download get the list of certificates

Usage:
  appviewx_client keystore download [flags]

Flags:
      --filepath string   filepath to store the certificate
  -h, --help              help for download
      --id string         id to download the certificate
      --password string   password for the PFX File
shibi.v@avxpll294:~/appviewx_est$
```

```
shibi.v@avxpll294:~/appviewx_est$ ./appviewx_client keystore download --filepath ./machine_cert.p12 --id 3 --password P@ssw0rd
+-------------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------+
|ID    |Common Name              |SerialNumber                                |Download Type  |Created Date
 |Expiry Date                   |
+-------------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------+
|0     |avxpll294.appviewx.com   |5C4DD353A41B97C4FC819A72DEA777F3            |p12            |Thu Jun  2 20:48:41 2022
 |Fri Jun  2 15:17:26 2023      |
|1     |avxpll294.appviewx.com   |DCE76DBDF369B0175F64C7A4AC3A88E2            |p12            |Thu Jun  2 20:51:01 2022
 |Fri Jun  2 15:19:45 2023      |
|2     |avxpll294.appviewx.com   |4D6F0008EDABA70311B0CEB0FF3F335C            |p12            |Thu Jun  2 20:51:45 2022
 |Fri Jun  2 15:20:30 2023      |
|3     |avxpll294.appviewx.com   |A13462C94DA04574C4555574328B0CDA            |p12            |Thu Jun  2 20:55:20 2022
 |Fri Jun  2 15:24:04 2023      |
|4     |avxpll294.appviewx.com   |3244B2045AB9F3AE55FFB1E4F1A005AC            |p12            |Fri Jun  3 11:44:45 2022
 |Sat Jun  3 06:13:29 2023      |
+-------------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------+

Download Success
shibi.v@avxpll294:~/appviewx_est$
```

Installation of the EST Client in Mac System

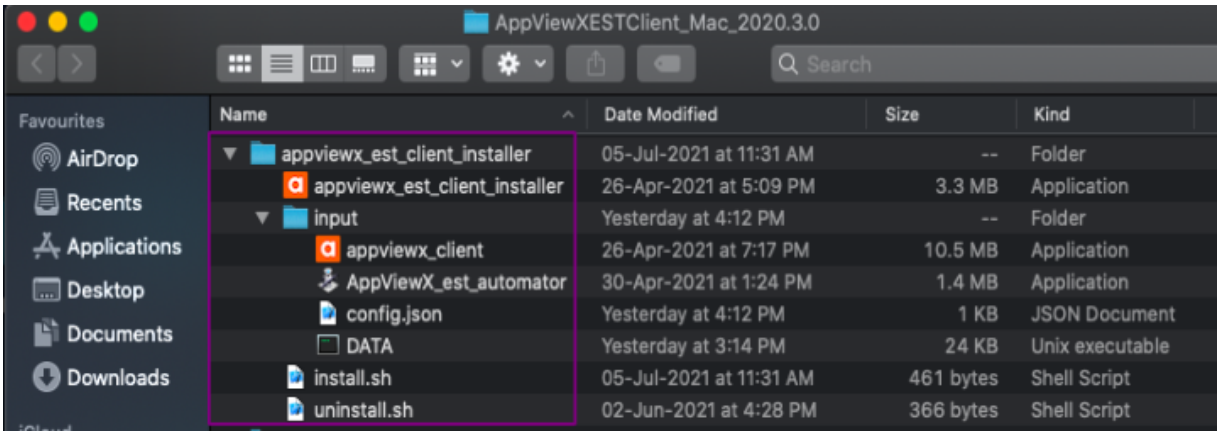
Step 1: Download and Extract the File

Download the file **AppViewXESTClient_Mac.zip** from Release Portal and extract it.

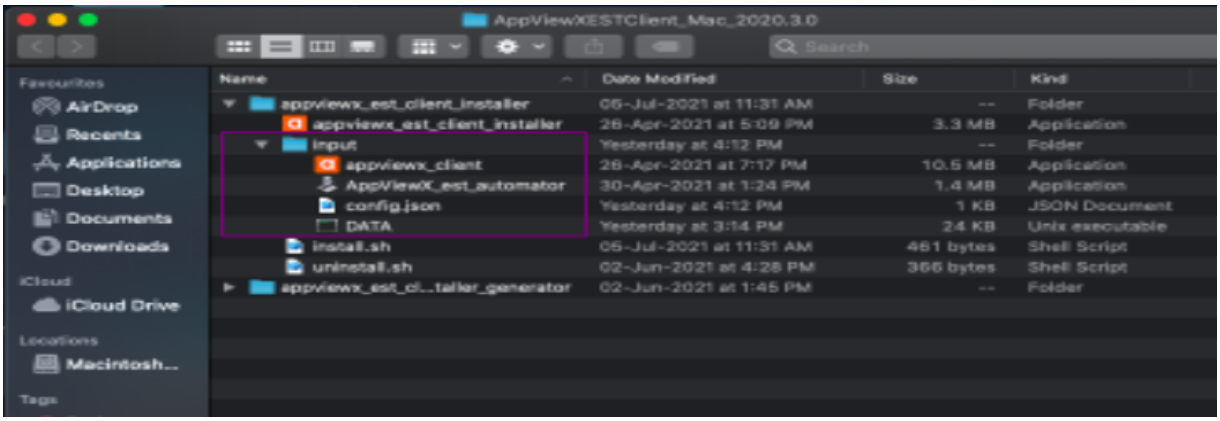


Step 2: Copy appviewx_est_client_installer Folder to the User Machine

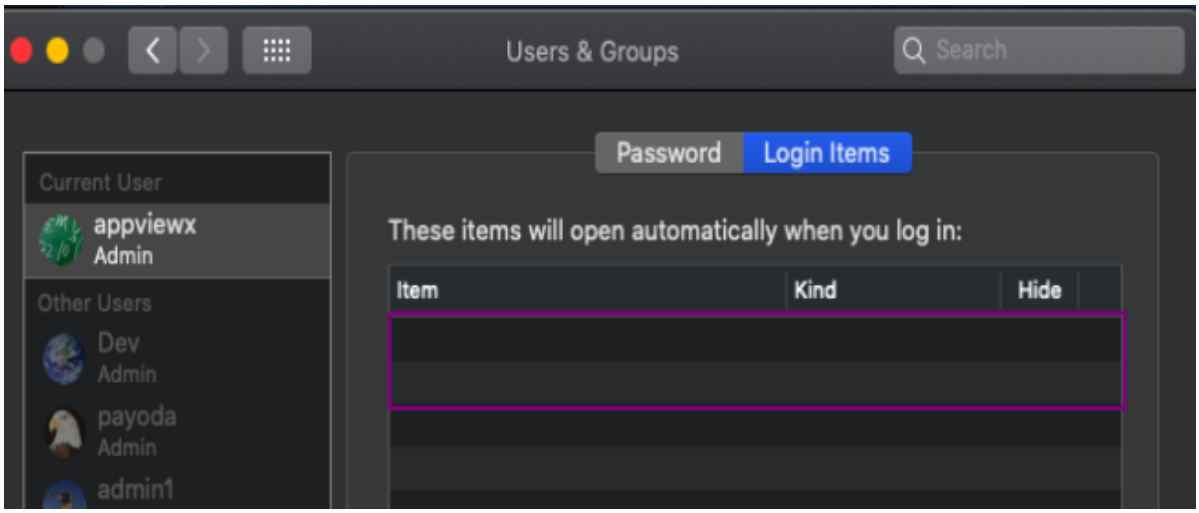
1. Description on Folder Structure:



2. Description on Input folder:



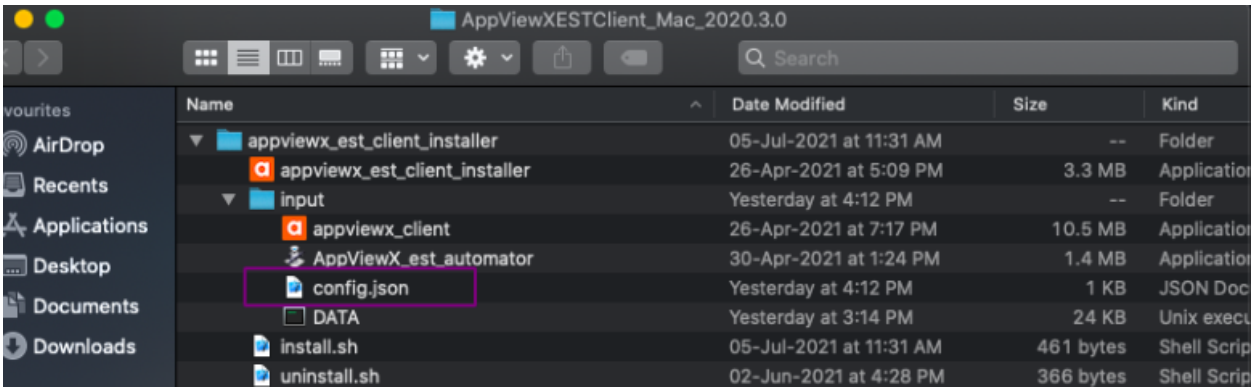
- **appviewx_client.app**: Client software binary (after installation which will get copied to User Home Folder).
- **AppViewX_est_automator.app**: Automator App which adds in to Users Login Items after Installation (Installation is covered in Step4, this triggers Agent Execution during User Login).



- **Config.json:** Contains configuration files required for enrollment (for Configuration details refer to Step 3).
- **DATA:** Contains encrypted Authentication Data. (User will never have direct access to it, which we are encrypting Using **appviewx_est_client_installer_generator**).
- **Appviewx_est_client_installer.app:** Binary for Installing the Client (no need to trigger directly. It is handled in **install.bat**).
- **Install.sh:** Script to install EST Client into Machine.
- **uninstall.sh:** Script to Uninstall EST Client from Machine.

Step 3: Edit the Configuration File

Open **config.json** in the input folder (Open with text editor).



- **Hostname**: EST Server hostname/IP.
- **Port**: 30021 is default for AppViewX 20.3 FP5 and above.
- **Path_seg**: AppViewX EST Agent name configured in GUI. (If using Default EST, leave it as empty. However, make sure the Policy associated with the Default Group has the “Certificate needs auto approval” option disabled.)

config.json

```
{
    "est_servers": [

                {
                        "certificate_type": "user",
                        "host_name": "pm-apvx-1.lab.appviewx.net",
                        "port": 30021,
                        "path_seg": ""
                },
                {
                        "certificate_type": "machine",
                        "host_name": "pm-apvx-1.lab.appviewx.net",
                        "port": 30021,
                        "path_seg": ""
                }
    ],
    "certificates": [

                {
                        "certificate_id": 1,
                        "certificate_type": "user",
                        "certificate_country": [""],
                        "certificate_province": [""],
                        "certificate_locality": [""],
                        "certificate_organization": [""],
                        "certificate_organization_unit": [""],
                        "reenrollment_trigger_before_no_of_days_of_expiry": 25,
                        "signed_pem_file_name": "",
                        "private_key_file_name": "",
                        "cacert_file_name": "",
                        "additional_cert_formats": ["pkcs12"],
                        "trust-ca": true

                },
                {
                        "certificate_id": 2,
                        "certificate_type": "machine",
                        "certificate_country": [""],
                        "certificate_province": [""],
                        "certificate_locality": [""],
                        "certificate_organization": [""],
                        "certificate_organization_unit": [""],
                        "reenrollment_trigger_before_no_of_days_of_expiry": 25,
                        "signed_pem_file_name": "",
                        "private_key_file_name": "",
                        "cacert_file_name": "",
                        "additional_cert_formats": ["pkcs12"],
                        "trust-ca": true
                }     ],
    "log_limit_number_of_lines": 10
}
```

Note: It is not mandatory to have all the types in the config file. Keep only the required type and delete the rest. For example, if requirement is to Enroll Only User Cert, then delete *machine* and *Others* from the list.

- **Certificate_type**: “user”: Generates Logged In Username as CN for the CSR and installs Certificate in User Personal Store (gets logged in user’s username using <**powershell>** command).
- **Certificate_type**: “machine”: Generates Machine’s name as CN for the CSR and installs Certificate in User Personal Store (gets machine name using <**hostname**> command).
- Set other Certificate attributes as mentioned above.

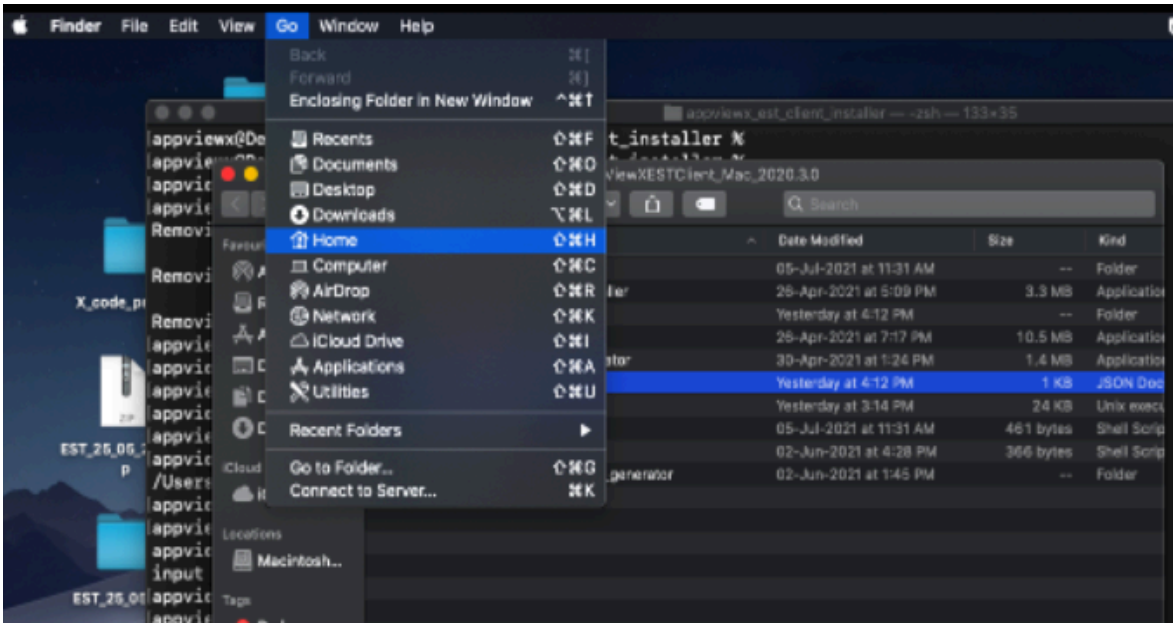
Step 4: Install the Agent Software

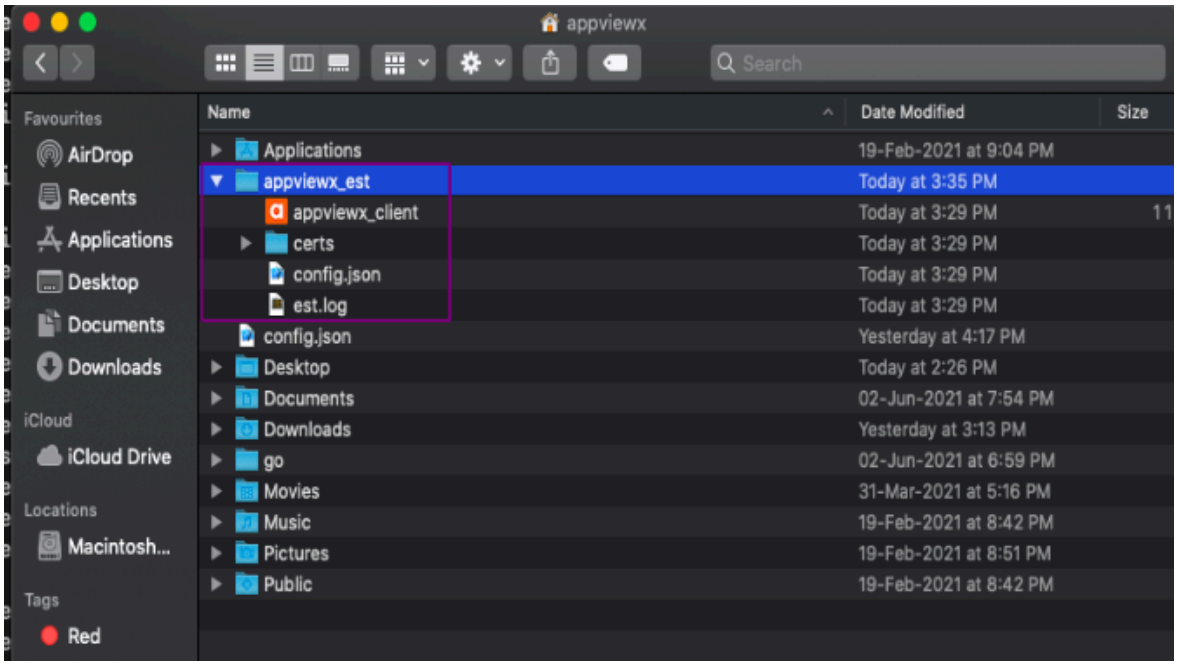
1. Open terminal in the **appviewx_est_cient_installer** folder.
2. Run the **install.sh** file.

```
appviewx@Devs-MacBook-Air appviewx_est_client_installer %
appviewx@Devs-MacBook-Air appviewx_est_client_installer % pwd
/Users/appviewx/Desktop/AppViewXESTClient_Mac_2020.3.0/appviewx_est_client_installer
appviewx@Devs-MacBook-Air appviewx_est_client_installer %
appviewx@Devs-MacBook-Air appviewx_est_client_installer % ls
appviewx_est_client_installer.app       install.sh
input                                   uninstall.sh
appviewx@Devs-MacBook-Air appviewx_est_client_installer %
appviewx@Devs-MacBook-Air appviewx_est_client_installer % ./install.sh
Installing EST Agent Software
constants.EST_HOME_VISIBLE :  /Users/appviewx/appviewx_est logFile :  est.log
Creating folder  /Users/appviewx/.appviewx_est
Creating folder  /Users/appviewx/appviewx_est
Creating folder  /Users/appviewx/appviewx_est/certs
Created Folders
EST Client installed successfully

Copying AppViewX_est_automator to Applications

Adding AppViewX_est_automator in the Startup
login item UNKNOWN
appviewx@Devs-MacBook-Air appviewx_est_client_installer %
```

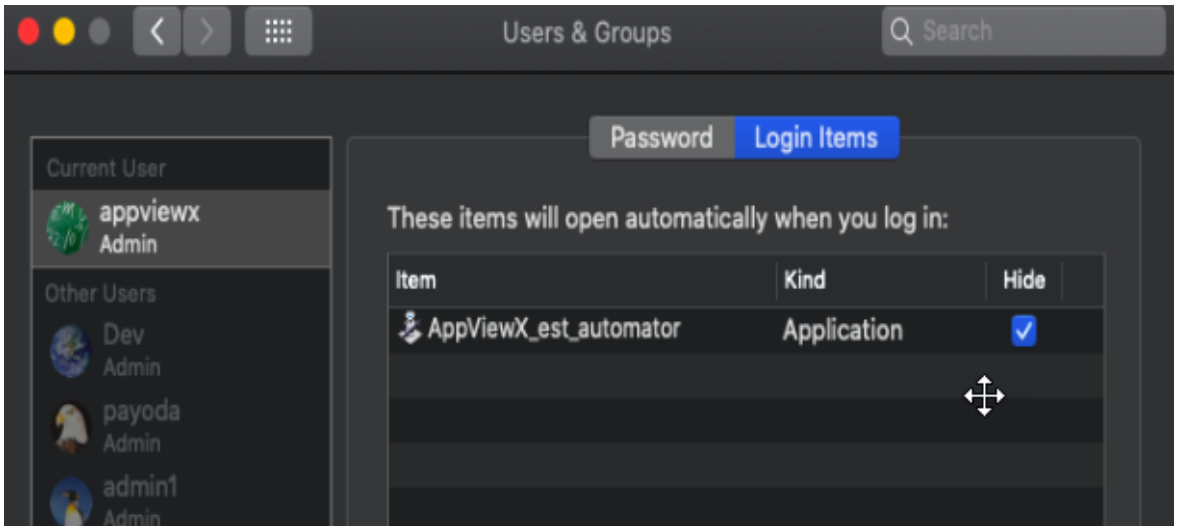
Execution Details:

- Encrypts the Software with Machine Unique parameters and Copies to Users Home folder.
- Installs **AppViewX_est_automator** in the **Users Login Items** (So that it can trigger agent when User logs in):
  - Verify the files copied to user Home folder. Navigate to **Finder**> **Go** > **Home Folder**:

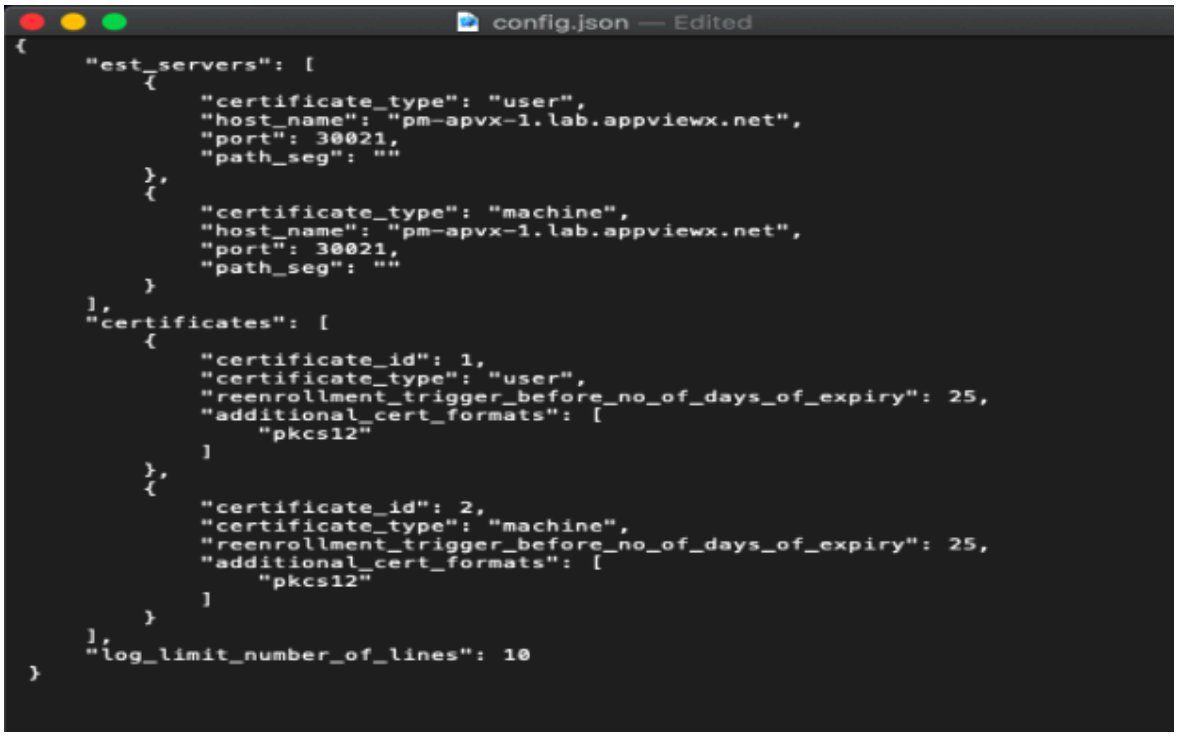




- Verify **AppViewX_est_automator** in **Login Items.** Go to **System Preferences** > **Users & Groups** > **Login Items**



- Validate the Copied Configuration file in **/home/<user>/appviewx_est/config.json**.



Note: This should contain the me configuration as the one pushed using **install.sh** method (**AppViewXESTClient_2020.3.0\AppViewXESTClientInstaller\input**)

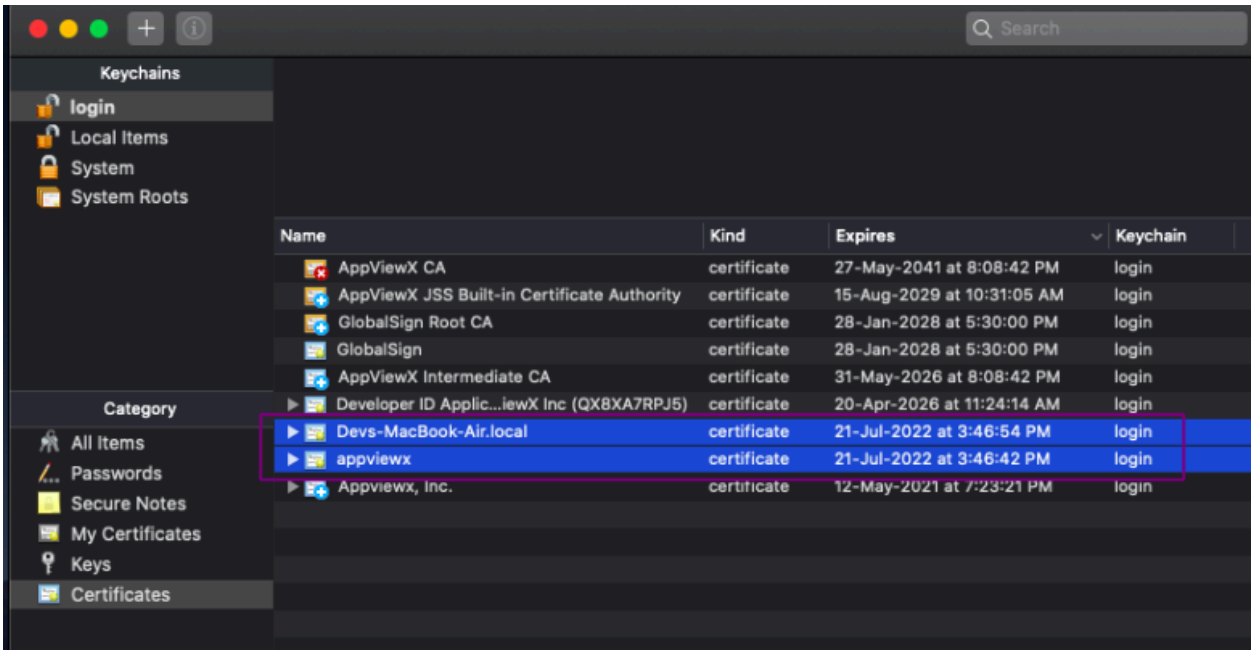
Step 5: Trigger Enrollment Request

This Agent can either trigger automatically when user logs in or manually from terminal using below command:

```
~/appviewx_est/appviewx_client.app/Contents/MacOS/appviewx_client est auto
```

```
appviewx@Devs-MacBook-Air appviewx_est % ~/appviewx_est/appviewx_client.app/Contents/MacOS/appviewx_client est auto
Initiating Enrollment Call  appviewx user
Initiating Enrollment Call  Devs-MacBook-Air.local machine
Agent Execution Completed
appviewx@Devs-MacBook-Air appviewx_est %
```

Step 6: Verify Machine and User Certificates Installed in Login Keychain



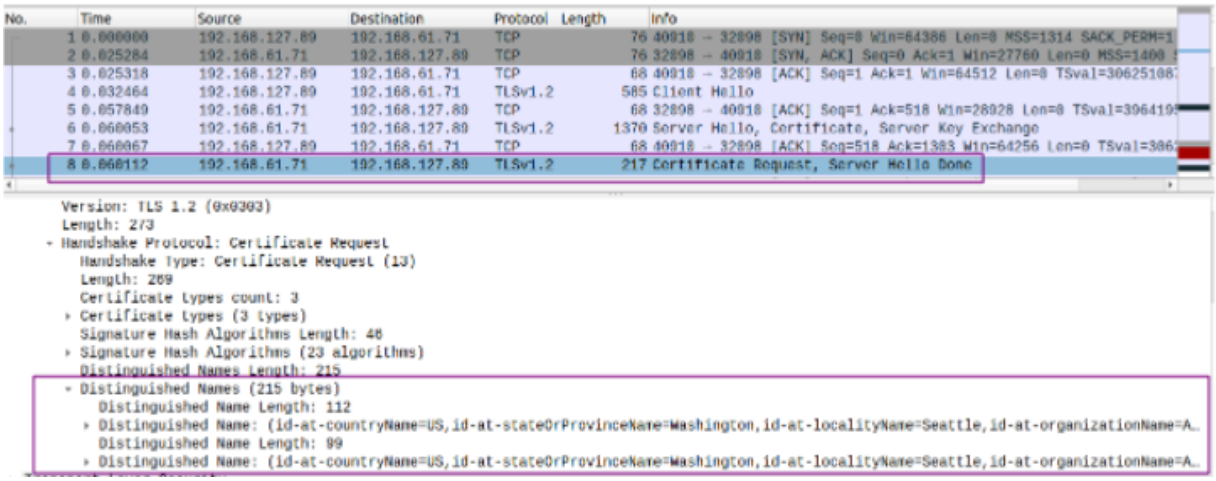
Troubleshooting

- Common Errors and Troubleshooting
- Error Codes

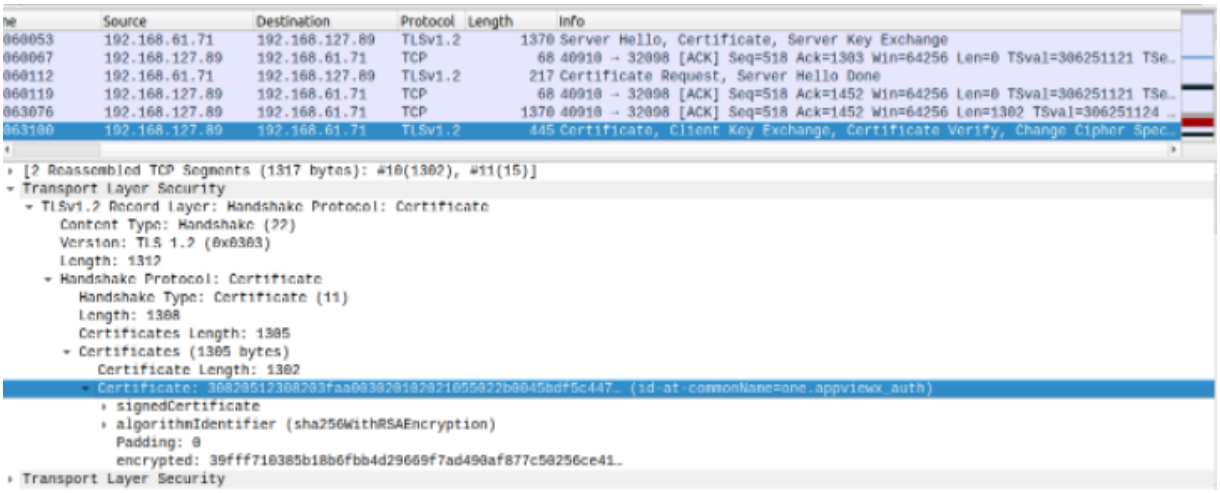
Common Errors and Troubleshooting

Error Code: 401 Unauthorized

1. Make sure Client is sending the Authentication Certificate (Try enrollment request from curl using the same Client certificates).
2. Check the trusted CA added in the EST agent settings to validate whether Client Authentication Certificate is signed by Same CA.
3. If the authentication certificate is signed by CA Other than AppViewX CA, make sure it is added in the trusted CA list from the CLI (Refer section, Adding External CA Trust Certificate for EST Client Authentication in the document).
4. Do a TCP dump and analyze the TLS transactions between Server and Client and make sure client is receiving Distinguished Name of Trusted CA's.



5. In the TCP dump, make sure Client is sending the Authentication Certificate in the Certificate Response field.



500-Internal Server Error

1. Make sure EST Service is running in AppViewX Server.
2. Check the EST Server Status (Refer Section, Verify EST Server Status (Enabled/Disabled)).
3. Check the EST Enrollment using Curl (Refer Section, Testing EST Enrollment by using CURL)

Error Codes

S. No	Status Code	Error Codes	Error Messages	Description

1	500 - Internal Server Error	CERT-ENROLLMENT-001	Agent settings is not found (or) invalid for this agent	When there is no agent found for EST with the specified name.
2	500 - Internal Server Error	CERT-ENROLLMENT-002	Agent settings is not valid	When EST agent settings are in valid.
3	401 - Unauthorized	CERT-ENROLLMENT-003	Authentication failed for the auto enrollment protocol	TLS / Basic / Digest authentication failed for the provided authentication parameters.
4	401 - Unauthorized	CERT-ENROLLMENT-006	Provided NONCE is invalid	• When TLS and HTTP auth is selected but the input does not contain any Basic auth value. • When TLS and HTTP auth is selected but the input does not contain any Digest auth value. Here Nonce is sent in the WWW-Authenticate header as per RFC.
5	500 - Internal Server Error	CERT-ENROLLMENT-007	Failure while creating nonce	When creating Nonce to send to client in case of Digest HTTP authentication
6	500 - Internal Server Error	CERT-ENROLLMENT-008	Certificate conversion failed	While converting the certificate contents to PKCS7 format which is to be sent as a response to the client.
7	500 - Internal Server Error	CERT-ENROLLMENT-009	Error while converting to JSON	Error during map to JSON conversion.
8	401 - Unauthorized	CERT-ENROLLMENT-010	No client certificate obtained to perform authentication.	When a client certificate is not found in the request to perform the TLS authentication.
9	500 - Internal Server Error	CERT-EST-001	Unable to get certificates requested by the client device	Could not obtain the certificates which were requested from the agent.
10	500 - Internal Server Error	CERT-EST-003	Certificate cannot be obtained after polling from the agent.	Certificate cannot be obtained even after retrying for the provided amount of time interval.

11	500 - Internal Server Error		CSR parameters already available for selected CA.	When there is already a request present in the certificate inventory and a similar CSR is obtained for enrollment/ re enrollment.
12	500 - Internal Server Error	CERT-ENROLLMENT-PROTOCOL-1020	Certificate enrollment failed for the provided csr.	• Check for the request id of the submitted CSR for further details. • Certificate or the certificate creation request may not be found to retrieve the certificate. • Exception while fetching work order mapping for the transaction id.
13	404 - Not Found	CERT-ENROLLMENT-PROTOCOL-1019	Certificate enrollment request does not exist. Please check the request sent from the AppViewX agent	The request from the EST agent is not found when received in subsystem certificate NB.
14	401 - Unauthorized	CERT-ENROLLMENT-PROTOCOL-1014	Authentication failed for the autoenrollment protocol.	When TLS authentication fails.
15	500 - Internal Server Error	CERT-ENROLLMENT-PROTOCOL-1005	Error while fetching policy settings for an agent	When obtaining group or policy details.
16	400 - Bad Request	CERT-SCEP-1011	Unable to extract CSR in the SCEP request	Occurs when the CSR extraction fails.
17	404 - Not Found	CERT-SCEP-1012	Policy is not associated with given certificate group	When the certificate policy for the provided agent is not present.
18	404 - Not Found	CERT-SCEP-1013	Group policy does not have the given certificate authority	All the error from 18 to 29 would be to validate the CSR parameters against policy
19	404 - Not Found	CERT-SCEP-1014	Group policy does not have the given hash function	NA

20	404 - Not Found	CERT-SCEP-1015	Group policy does not have the given key type	NA
21	404 - Not Found	CERT-SCEP-1016	Group policy does not have the given key length	NA
22	400 - Bad Request	CERT-SCEP-1017	Given common name must ends with as per the common name defined in group policy	NA
23	400 - Bad Request	CERT-SCEP-1018	Given common name cannot be same as common name defined in group policy	NA
24	400 - Bad Request	CERT-SCEP-1019	Given organization must match with organization defined in group policy	NA
25	400 - Bad Request	CERT-SCEP-1020	Given organization unit must match with organization unit defined in group policy	NA
26	400 - Bad Request	CERT-SCEP-1021	Given locality must match with locality defined in group policy	NA
27	400 - Bad Request	CERT-SCEP-1022	Given state must match with state defined in group policy	NA
28	400 - Bad Request	CERT-SCEP-1023	Given country must match with country defined in group policy	NA

29	404 - Not Found	CERT-SCEP-1024	Group policy does not have the given certificate type	NA
30	400 - Bad Request	CERT-CSR-0002	Failed to parse CSR, please validate the content.	CSR content is not proper while uploading it for submission
31	404 - Not Found	CERT-CA-0001	CA settings are not available.	CA setting selected in EST settings is not found
32	404 - Not Found	CERT-KEY-0003	Certificate/private key retrieval failed.	DAO exception while fetching certificate.
33	417 - Expectation Failed	CERT-CSR-0005	Csr submission failed. ${ERROR_MSG}	Custom error message from CA.

Best Practices for Client

- To define the mandatory CSR parameters, update the **<secure_config.json>** file in the **Installer Generator** folder.
- Add trusted CA-signed certificate, key, and EST URL's CA certificate to the **input** folder of **Installer Generator** and encrypt the files using the installer generator program.
- Use FQDN in EST Enroll and Re Enroll URL configuration instead of mentioning server IP in the configuration.
- To validate EST URL's certificate with a trusted CA certificate, update the **validate_server_cert** parameter to **yes** in the **<config.json>** file.
- After the software installation, delete the **Installer** folder from the machine. The installer installs agent software in the **home** folder and it is recommended to delete the **Installer** from the machine.

EST DataEncryption Tool

Introduction

This tool is used for Encrypting the Authentication data (est_auth.crt, est_auth.key) and secure Config file.

Description for est_auth.crt and est_auth.key

AppViewX EST Server uses TLS Based authentication for validating the Clients. So Client should present an Authentication Certificate during the Enrollment process as per the RFC of EST and Server will validate the Certificate against Trusted CA Configured in EST UI.

If the issuer trusted by AppViewX EST signs the Certificate presented by the Client during initial handshake, server will further proceed with the Enrollment process, else it will reject the request.

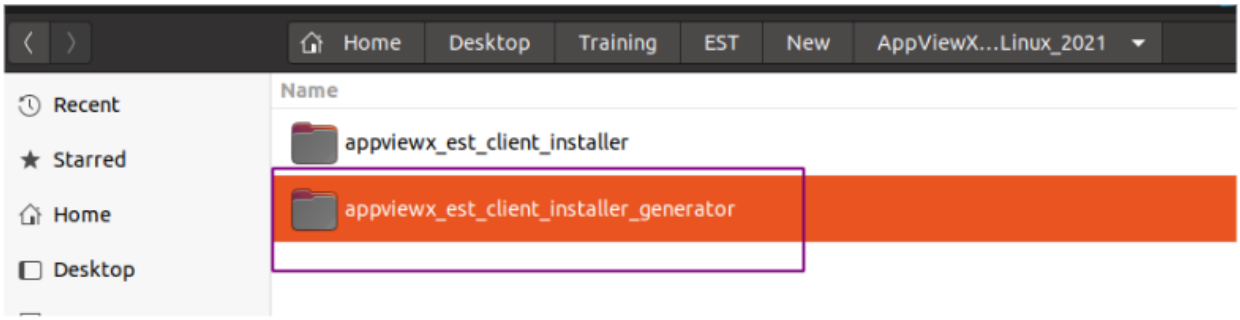
So, the security of this Authentication Certificate present in the Client Machines are crucial and we use AppViewX EST DataEncryption or (**appviewx_est_installer_generator**) for the encryption.

The execution steps are the same for Windows/Linux/Mac OS.

This operation typically executed by PKI Admin before provisioning Agent software with Updates DATA File in the input folder of **appviewx_est_installer** to the user.

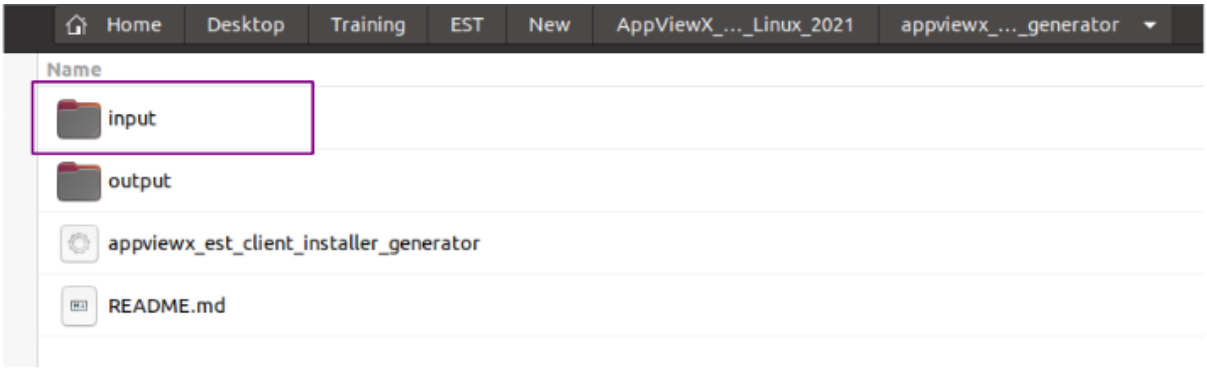
Encryption Step

In all the ZIP files, you can see a folder called **appviewx_est_client_installer_generator**.

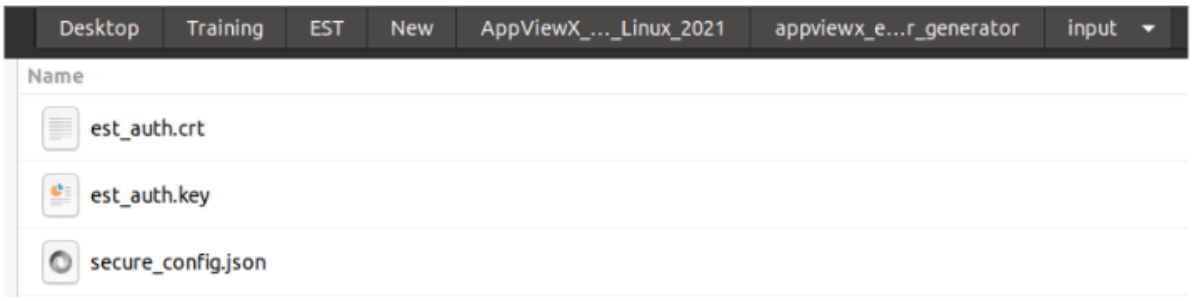


Step 1: Place Files in the Input Folder

1. Open the **input** folder.



2. Place the Authentication Certificate, Key, and **secure_config.json** file inside **input** folder.

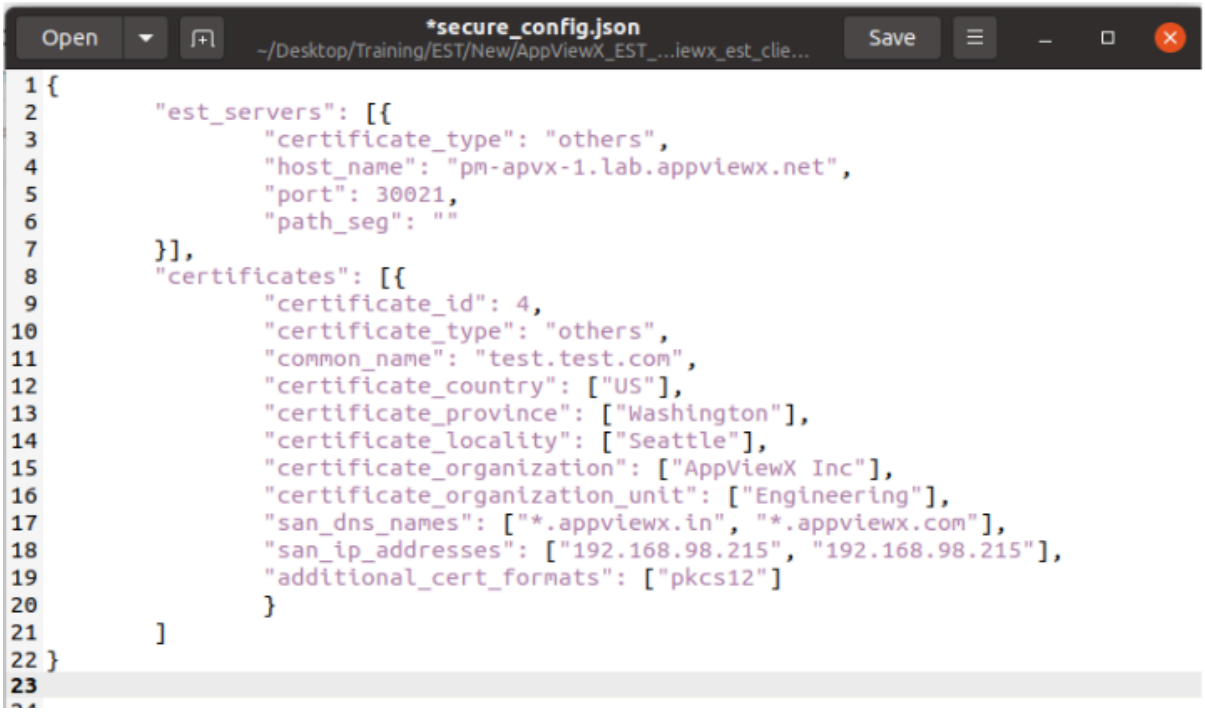


Note: The filenames should be same **est_auth.crt, est_auth.key, secure_config.json** (optional file).

Secure_config.json: Description:

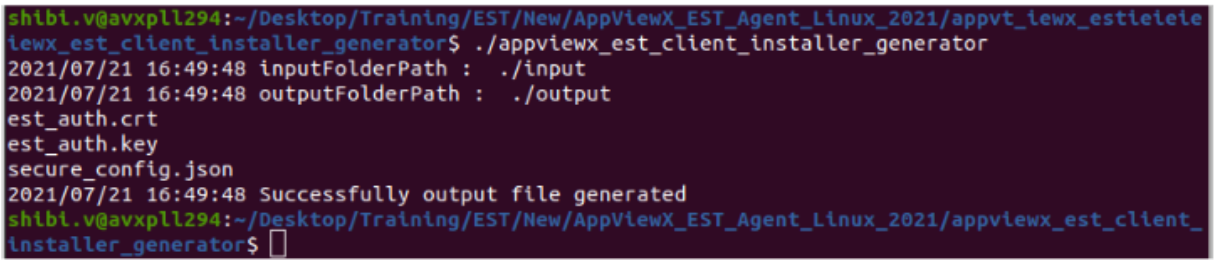
This file even can be left empty.

This is used where administrators want to hard Code certain values and to override the User inputs if they try to edit certain configs, Admin can set the Values in secure config and along with authentication DATA secure_config also will get encrypted and added in DATA file.



Step 2: Execution of Encryption Tool

1. Open the terminal at **appviewx_est_client_installer_generator** tool.
2. Execute using **./appviewx_est_client_installer_generator**.



New DATA file is generated in the output folder **appviewx_est_client_installer_generator/output**.

Step 3: Use a New DATA File in *appviewx_est_installer* Input Folder

- Copy and paste a new DATA file at the input folder of **appviewx_est_installer**.