appviewX

AppViewX EST Server Configuration Guide

Version: 2020.2.0

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	Configuration Guide AppViewX v20.2.0	May 2020

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: Introduction

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

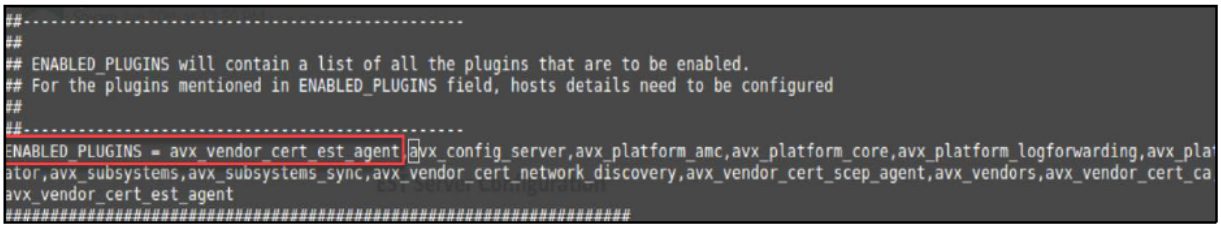
Before configuring the EST server, the user has to make the following changes:

- Make necessary changes in the <appviewx.conf> file (as shown in the below section).
- Create or upload the client authentication CA certificate.
- Disable the **Approval Required** option in the policy.

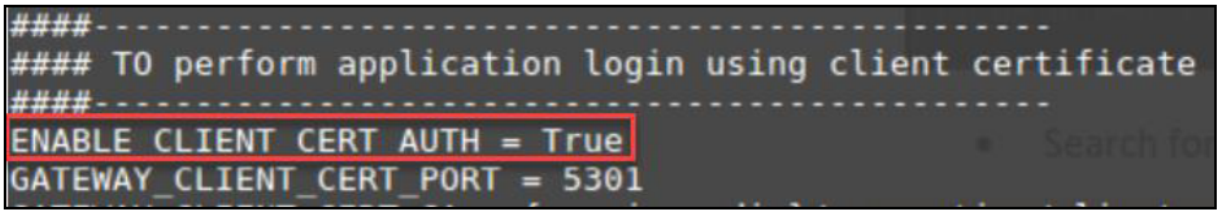
Modify appviewx.conf File

Open the terminal and go to the directory **vi /home/appviewx/appviewx/conf/** and open <appviewx.conf> file. The user has to make two changes in the <appviewx.conf> file as listed below.

- Search for **ENABLED_PLUGINS** and include **avx_vendor_cert_est_agent** at the beginning or end of the list as shown in the below image.



- Search for **ENABLE_CLIENT_CERT_AUTH** and change the value to **True**.



Note: By default, ENABLE_CLIENT_CERT_AUTH is **False** and the port is 5301.

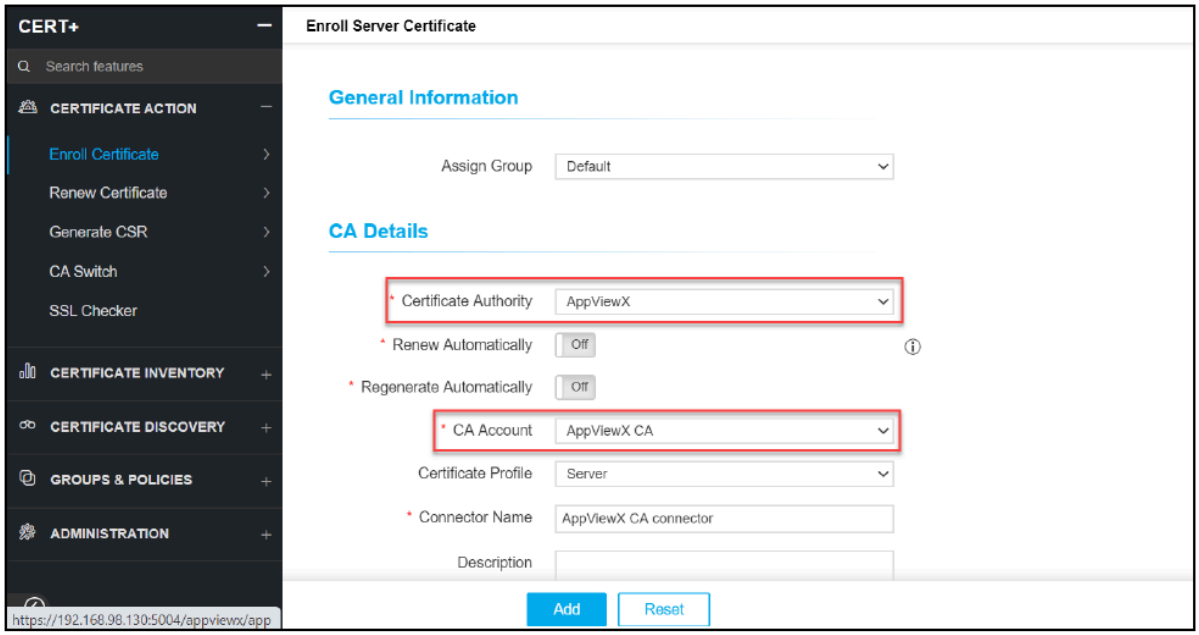
After making the above changes in the <appviewx.conf> file, execute the below commands respectively on the terminal.

- *avx --initialize all*
- *avx --restart all*

Create the Client Authentication CA Certificate

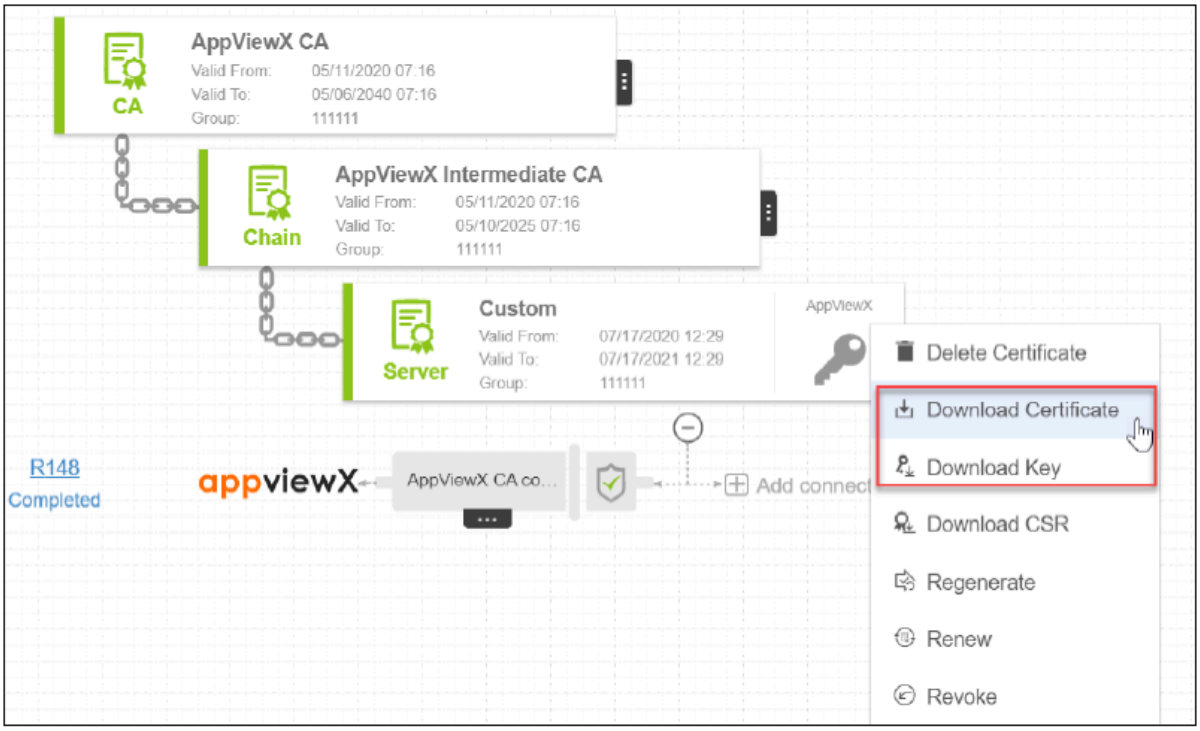
If the user does not have a client authentication CA certificate, the user can create one with the AppViewX CA. To create a client authentication CA certificate,

1. Log in to the AppViewX application with valid credentials.
2. Click the menu button.
3. Select **CERT+ > Certificate Action > Enroll Certificate > Server**.
4. On the **Enroll Server Certificate** details page, under **General Information** section, assign a group to the certificate.
5. Under **CA Details** section, select AppViewX from the **Certificate Authority** drop-down list and select AppViewX CA from the **CA Account** drop-down list. Fill in all other mandatory fields.



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

14. For more information, refer to Enroll a Certificate.



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

Upload the Client Authentication CA Certificate

If the user has a Client Authentication CA certificate, the user can upload it. To upload a client authentication CA certificate,

1. Click the menu button.
2. Select **CERT+ > Certificate Inventory > Upload**.
3. On the Upload Certificate page, click the **Browse** button and choose the client authentication CA certificate.
4. Click **Upload**.
5. The uploaded certificate is available in the Intermediate/Root inventory **(CERT+ > Certificate Inventory)**.

> **Restriction:** AppViewX server only supports AppViewX Root and Intermediate CA certificates for authentication.

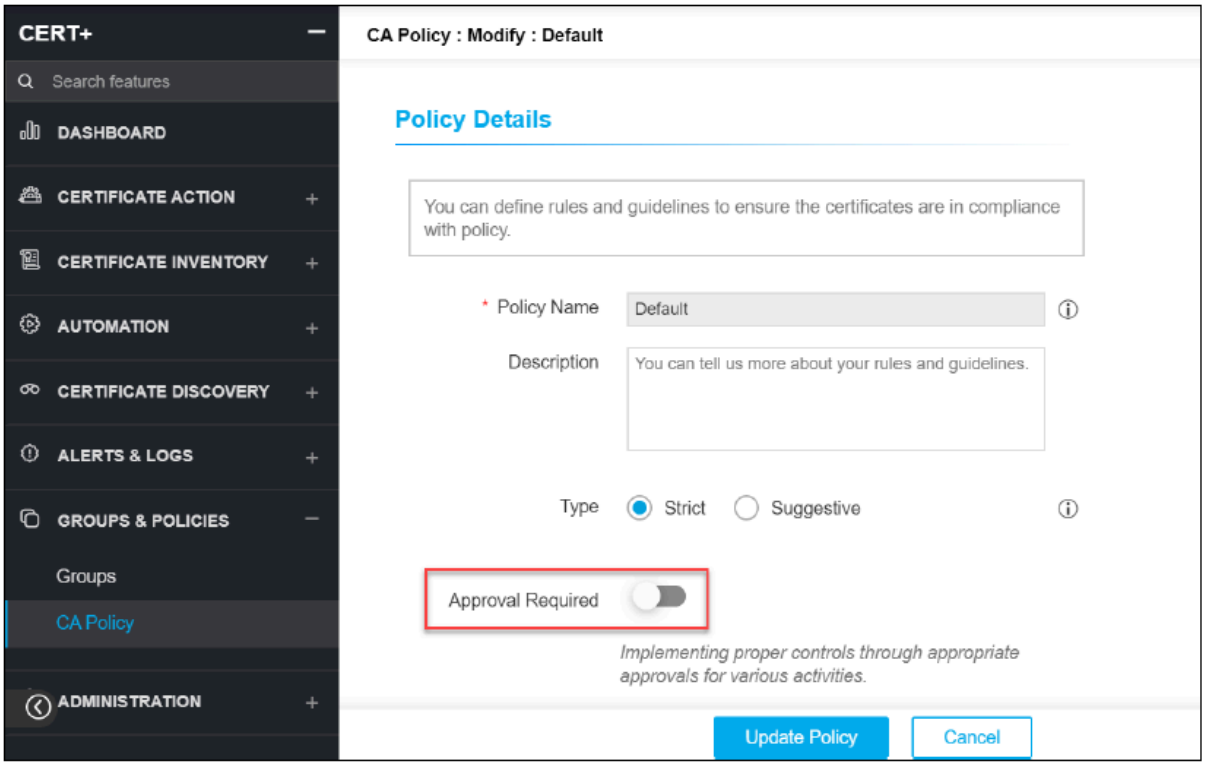
Disable the Policy Approval Required

The user has to disable the approval required option in the policy before configuring the EST. To disable the approval required option,

1. Click the menu button.
2. Select **CERT+ > Groups & Policies > CA Policy**.
3. On the CA Policy list view page, select the respective policy.
4. On the policy details page, disable the **Approval Required** toggle.

> **Note:** By default, **Approval Required** toggle is enabled.

> **Important:** Make sure the respective certificate group is associated with the respective policy under **Groups & Policies > Groups**.



5. Click **Update Policy**.

6. To know about certificate groups, refer to Create a Certificate Group.

> **Important:** If the Approval Required is enabled, the incoming enrollment request will be in the pending status which may require manual approval.

Chapter 3: EST Configuration

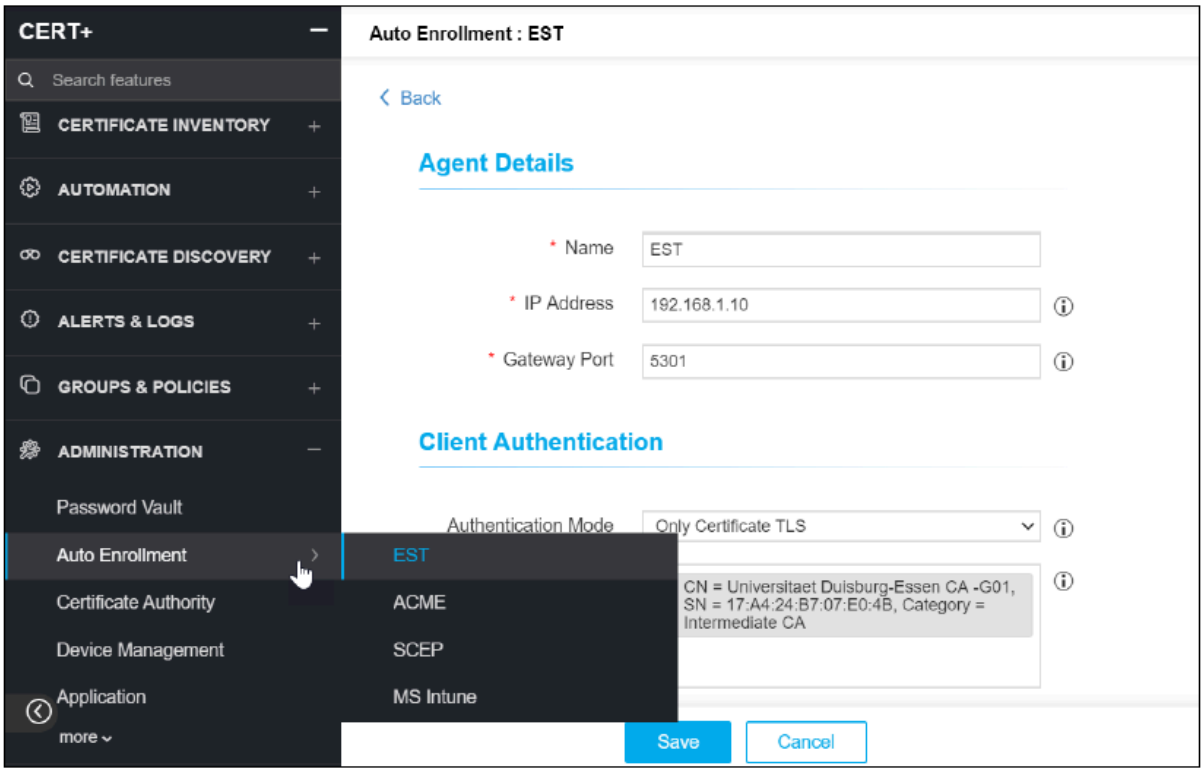
To configure the EST server,

1. Click the menu button.
2. Select **CERT+ > Administration > Auto-Enrollment > EST**.
3. On the EST list view page, **defaultEST** is displayed by default. Click **+ Add** icon on the top-right.
4. On the EST details page, under the **Agent Details** section, enter the Name, IP Address, and the Gateway Port.

   Note: By default, the Gateway Port is 5301.

5. Under the **Client Authentication** section, select an **Authentication Mode** from the drop-down list.
   - Only Certificate TLS – 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.
6. 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**.
7. 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.
8. Select the **Issuer Certificate** by entering the first three letters of the certificate name or serial number. (This is the same certificate that was uploaded in **Upload the Client Authentication CA Certificate** section).
9. Under the **CA Settings** section, select the **Certificate Group** from the drop-down list.
10. Select the Certificate Type as **Client** or **Server** based on the requirement.
11. Select the **CA** and **CA Account** from the respective drop-down lists. At present, AppViewX supports only AppViewX CA, EJBCA, and Microsoft CA.
12. In the **CA Certificate** field, enter the certificate name and in the **CA Connector Name** field, enter a name for the CA Connector.

13. In the **Certificate Validity** field, enter the number of days.



14. 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 authentication.
15. Enter the **Retry Count** and **Retry Frequency** in the respective fields.
16. Click **Save**.

Supported Operations

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

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/.well-known/est

For AppViewX Enrollment - https://est.appviewx.com/.well-known/est/appviewx/simpleenroll

For AppViewX Re-enrollment - https://est.appviewx.com/.well-known/est/appviewx/simplereenroll