appviewX

CERT Solution Guide - EST Client Configuration Guide

Version: 2020.3.0

Copyright AppViewX, Inc.

External Reference Links

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

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

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

Contact Information

AppViewX, Inc.

222 Broadway, FL 19

New York, NY 10038

Email: info@appviewx.com

Web: www.appviewx.com

Contents

Preface

Revision History

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

About this Guide

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

Audience

This guide is intended for those who want to install the EST agent on a client machine to perform enrollment tasks on certificates.

Text Conventions

The following text conventions are used in this document:

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

Chapter 1: Overview

Enrollment over Secure Transport (EST) is a simple and functional certificate management protocol. EST works in the client-server model. AppViewX offers both EST server and client functionalities with TLS based authentication between the server and client as per the protocol. EST client installed in Linux, Windows, and Mac OS platforms supports certificate enrollment and re-enrollment for both machine and user authentication certificates. This document helps with the installation of the EST agent on a client machine that allows you to perform enrollment tasks on certificates.

Tip: You can download the EST client agent from release.appviewx.com.

Chapter 2: Installation of the EST Agent in Windows Machine

Install EST Agent

To install the EST agent in the Windows machine:

1. Admin can download the **EST Client** <*.zip*> file to a directory that has no access restriction to other user accounts.
2. After extracting the <*.zip*> file, run the <*ScheduleEST.exe*> program in the **Scheduler** folder. You can run manually or can be automated using PowerShell or other methods.
3. This will create two tasks in **Task Scheduler:**
   - **AppViewX-AutoEnrollment:** to get the certificate for the machine.
   - **AppViewX-UserAutoEnrollment:** to get the certificate for the user.
4. After the task creation, when a user logs in, it automatically triggers both the tasks.
5. The EST Client will check CSR values against certificates in the store. If a certificate is available with the same CSR values, it verifies certificate **IssuerName** with IssuerName set in the configuration file.
6. If it matches, then checks the certificate **expiry date** and **DaysBeforeExpiry** configured in the configuration file.
   - If **DaysBeforeExpiry** is higher than days to certificate expiry date, the task will trigger the program to perform a certificate re-enrollment.
   - If a certificate is not available with the same CSR values or the IssuerName is different, it will enroll as a new certificate.

   Config.jsonFile

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <configSections>
    <section name="log4net" type="log4net.Config.Log4NetConfigurationSectionHandler,log4net" />
  </configSections>
  <appSettings>
    <add key="ESTEnabled" value="Yes" />
    <add key="SystemAutoEnrollment" value="Yes" />
    <add key="UserAutoEnrollment" value="No" />
    <add key="SystemAccounts" value="SYSTEM,SERVICE" />
    <add key="SubjectName" value="CN=www.test1-app.com,O=appviewx,OU=cert,ST=NY,C=US" />
    <add key="DynamicCN" value="Yes" />
    <add key="DynamicComputerName" value="Yes" />
    <add key="ESTEnrollURL" value="https://enroll.appviewx.com:5301/.well-known/est/simpleenroll"/>
    <add key="ESTReEnrollURL" value="https://enroll.appviewx.com:5301/.well-known/est/simplereenroll"/>
    <add key="ValidateRevocation" value="Yes" />
    <add key="SkipSSLValidation" value="No" />
    <add key="DeltaCRL" value="Yes" />
    <add key="SkipSSLError" value="No" />
    <add key="IssuerName" value="AppViewX Intermediate CA" />
    <add key="ESTCertFile" value="data\admin.txt" />
    <add key="ESTCertEnc" value="data\enc.txt" />
    <add key="DaysBeforeExpiry" value="25" />
    <add key="CertFile" value="data\admin.p12" />
    <add key="CertEnc" value="data\ps.txt" />
```

Configuration Fields Description

File	Description
ESTEnabled	Denotes the EST Client is enabled or not
SystemAutoEnrollment	Specifies the auto-enrollment of the system is enabled
UserAutoEnrollment	Specifies the auto-enrollment of the user is enabled
SystemAccounts	Denotes the system accounts
SubjectName	Specifies CSR properties an Admin can enter manually for certificate enrolment
DynamicCN	Specifies the dynamic common name to fetch from the AD for the user certificate
DynamicComputerName	Specifies to fetch FQDN value of the machine and use as a common name for the machine certificate
ESTEnrollURL	Denotes the enrollment URL of the EST Client
ESTReEnrollURL	Denotes the re-enrollment URL of the EST Client

File	Description
ValidateRevocation	Enable/disable the validate revocation parameter
SkipSSLValidation	Enable/disable the skip SSL validation parameter
DeltaCRL	Enable/disable the delta CRL parameter
SkipSSLError	Enable/disable the skip SSL error parameter
IssuerName	Denotes the certificate issuer name
ESTCertFile	Denotes the encrypted authentication certificate location and the file name.
ESTCertEnc	Denotes the encrypted file which contains the password of the authentication certificate.
DaysBeforeExpiry	Specifies the number of days before the certificate expiry to trigger re-enrollment calls.
CertFile	Denotes the name of the authentication certificate file(.p12)
CertEnc	Denotes the name of the text file which contains the password of .p12 file (this will be removed after encryption)
AppViewXGatewayUrl	Not using this parameter
PushBatchSize	Not using this parameter
PortNumber	Not using this parameter
CertificateStatus	Not using this parameter
Vendor	Not using this parameter

Best Practices

- Use the **FQDN** in EST Enroll and Re-enroll URL configuration instead of server IP.
- Enable the **Dynamic CN** and Computer Name to get a specific machine's and user's name in CSR.
- In the case of Microsoft CA, the auto-enrollment template has to be configured with option DN supplied in the request.
- Enable the **ValidateRevocation** to check the revocation status of the EST server URL.
- Change the **SkipSSLValidation** and **SkipSSLError** to No to validate the server URL.
- Change the **DeltaCRL** to **Yes**.

- Provide the exact **CN Name** of the issuer.
- The above configuration enforces the server validation before sending the certificate request or authentication data.
- Make sure that the authentication data is encrypted and stored in the data folder.
- Change AppViewX default authentication certificate that is shipped along with the product. After you update the authentication certificate, run the task in the scheduler to encrypt the certificate and password file.

Chapter 3: Installation of the EST Client Agent in Linux Machine

Install the EST Agent

To install the EST agent in the Linux machine:

1. Go to the **EST Client Installer Generator** folder.
2. You can find **bin**, **Input**, **Output** folders, and <*appviewx_est_client_installer_generator*> and <*README.md*> files.
3. Click the **Input** folder.
   - You can find CA certificate <*ca.crt*>, authentication certificate <*est_auth.crt*>, authentication key <*est_auth.key*>, and <*secure_config.json*> files.

File	Description
ca.crt	Certificate of CA who signed the certificate presented by the server during TLS authentication.
est_auth.crt	The certificate used by the client for the client authentication on the server.
est_auth.key	Key of the est_auth.crt
secure_config.json	List of configurations set by the PKI admin to override configuration fields set by the user in (/home/<user>/appviewx_est/config.json). <*secure_config*> files details will not be accessible by the user.

   - If you have an authentication certificate and a key, replace it with this.
   - Provide the authentication certificate and the key and admin can configure values inthe <*secure_config.json*> file.
4. From the **EST Client Installer Generator** folder, open the terminal and run the **<appviewx_est_client_installer_generator>** file by executing the installer generator command:
   `/appviewx_est_client_installer_generator-i ./input -o ./output`
5. Executing the above command reads the list of files available in the input folder,encrypts, and generates a <*DATA*> file in the **Output** folder.

6. Copy the <*DATA*> file from the **Output** folder of the **EST Client Installer Generator** to the **Input** folder of the **EST Client Installer**.
7. Go to the **EST Client Installer** folder.
8. You can find **bin** and **Input** folders, and <*appviewx_est_client_installer*> and <*README.md***>** files.
9. Click the **Input** folder.
   - You can find **<***appviewx_est_client*>, <*config.json*>, and <*DATA*> file (file copied from the Installer Generator output folder).

File	Description
config.json	A user can make changes to server details, certificate install location, and CSR values.

   - You can configure values in the <*config.json*> file if required.
10. From the **EST Client Installer** folder, open the terminal and run the <*appviewx_est_client_installer*> file by executing the installer command *./appviewx_est_client_installer -i./input.*
11. Executing the above command creates **appviewx_est** and **.appviewx_est** folders with all the files required in the **Home** </home/user/> directory.
12. To execute the **appviewx_est_client** periodically, make an entry in the cron. For example, *10* * * ** *export PATH=$PATH:/sbin:/usr/sbin;/home/user/appviewx_est/appviewx_est_client.*
13. Alternatively, you can add cron details in the <*installer3.sh*> available in the **bin** folder to install the **appviewx_est** (move to the bin folder and execute) with cron entry.
    - Above installation creates the following folders:
      - ~/appviewx_est
      - ~/.appviewx_est
    - Adds a cron entry for invoking the **appviewx_est_client** for every hour at 10th minute (user can customize cron based on schedule requirement).
14. Go to the **Home** folder (/home/user/) and click the **appviewx_est** folder.
15. You can find **certs** folder, <*appview_est_client*>, <*config.json*>, and <*est.log*> files.
16. Execute the **EST Client** with the command: `./appviewx_est_client.`
17. Executing the above command enrolls the configuration and stores the certificate in the **certs** folder.

Note:

- Output path for certificates and the key can be configured in the **<config.json>** file.
- **certificate_install_path, signed_pem_file_name,signed_p12_file_name, private_key_file_name, cacert_file_name** can be configured locally in the **<config.json>** file before the installation.

Config.jsonFile


```
{
    "est_servers": [
        {
            "certificate_type": "auth",
            "host_name": "est.appviewx.com",
            "port": 5301,
            "path_seg": "authca",
            "validate_server_cert": false,
            "server_url_ca_cert": ""
        },
        {
            "certificate_type": "machine",
            "host_name": "est.appviewx.com",
            "port": 5301,
            "path_seg": "ejbca",
            "validate_server_cert": false,
            "server_url_ca_cert": ""
        },
        {
            "certificate_type": "user",
            "host_name": "est.appviewx.com",
            "port": 5301,
            "path_seg": "ejbca",
            "validate_server_cert": false,
            "server_url_ca_cert": ""
        }
    ],
    "certificates": [
        {
            "certificate_id": 1,
            "certificate_type": "auth",
            "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",
            "reenrollment_trigger_before_no_of_days_of_expiry": 1000,
            "signed_pem_file_name": "/home/shibi.v/appviewx_est/certs/LinuxOS.pem",
            "private_key_file_name": "/home/shibi.v/appviewx_est/certs/LinuxOS.key",
            "cacert_file_name": "/home/shibi.v/appviewx_est/certs/LinuxOS_ca_avx.pem"
        },
        {
            "certificate_id": 3,
            "certificate_type": "user",
            "reenrollment_trigger_before_no_of_days_of_expiry": 1000,
            "signed_pem_file_name": "/home/shibi.v.pem",
            "private_key_file_name": "/home/shibi.v.key",
            "cacert_file_name": "/home/shibi.v_ca_avx.pem"
        }
    ],
    "log_limit_number_of_lines": 10
}
```


Configuration Fields Description

File	Description
certificate_type	Denotes the type of certificate(like authentication, machine, and user)
host_name	Denotes the hostname of the EST server
port	Denotes the port of the EST server
path_seg	Denotes the path segment/agent name of the EST server
validate_server_cert	Setting true will enable the CA Certificate Validation in TLS
server_url_ca_cert	EST Client's TLS transaction CA Certificate pool will include this file along with System Certificate Pool and ca.crt
certificate_id	Denotes the unique id of the certificate
reenrollment_trigger_ before_no_of_days_of_expiry	Denotes the number of days before re-enrollment to be triggered
signed_pem_file_name	Specifies the path to save the certificate
private_key_file_name	Specifies the path to save the private key
cacert_file_name	Specifies the path to save the CA certificate of the server

Secure_config.jsonFile

```
{
    "certificates": [
        {
            "certificate_id":1,
            "certificate_type": "machine",
            "certificate_country": [
                "IN"
            ],
            "certificate_province": [
                "TN"
            ],
            "certificate_locality": [
                "City"
            ],
            "certificate_organization": [
                "Limited"
            ],
            "certificate_organization_unit": [
                "IT"
            ]
        },
        {
            "certificate_id":2,
            "certificate_type": "user",
            "certificate_country": [
                "IN"
            ],
            "certificate_province": [
                "TN"
            ],
            "certificate_locality": [
                "City"
            ],
            "certificate_organization": [
                "Limited"
            ],
            "certificate_organization_unit": [
                "IT"
            ]
        }
    ]
}
```

Best Practices

- 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 <*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.
- Update the crontab for the scheduled execution of the agent software for validity check and renewal.