appviewx

CERT Solution Guide SCEP Configuration 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 2022.1.0	June 2022

About this Guide

This guide contains the pre-defined procedure for the Simple Certificate Enrolment Protocol (SCEP) configuration

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 the text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`codeblock`	Indicates commands with a paragraph, URLs, codes in examples, text that appears on the screen, or text that you enter.

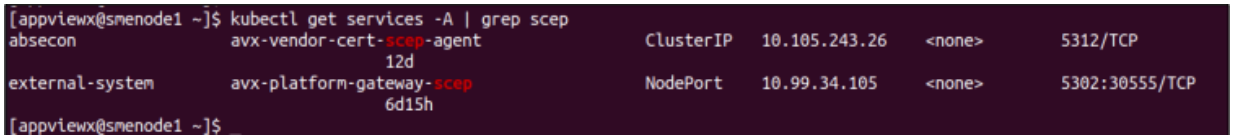
Chapter 1: Overview

The SCEP protocol services can be configured in AppViewX to enable the communications between the client (device endpoints) and AppViewX northbound services that processes the client requests such as certificate enrolment and renewal. Once the protocol service gets enabled, AppViewX will act as a RA in receiving and serving the client requests. The protocol must be enabled as HTTP service.

Chapter 2: Prerequisites

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

- Make sure that the and services are running in the cluster.



> **Note:** If services are running, note the port number that is shown after 5302:< scep_external_port>. This port number needs to be configured in SCEP Settings GUI.

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

Chapter 3: Enable SCEP Services

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

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

```
ENABLED_PLUGINS=appviewx_dependencies,avx_commons,avx_crontab,avx_config_server,avx_platform_core,avx_platform_amc,avx_platform_q
ueue,avx_platform_gateway,avx_platform_gateway_external,avx_platform_web,avx_subsystems,avx_vendors,avx_subsystems_sync,avx_visua
l_page_builder,avx_vendor_cert_network_discovery,avx_vendor_cert_scep_agent,avx_vendor_cert_intune_agent,avx_vendor_cert_est_agen
t,avx_vendor_cert_acme_agent
SSH_OTHER_USER=appviewx

avx_commons=absecon
avx_config_server=absecon
avx_platform_core=absecon
avx_platform_queue=absecon
avx_subsystems=absecon
avx_subsystems_sync=absecon
avx_vendors=absecon
avx_platform_gateway=absecon
avx_platform_web=absecon
avx_platform_amc=absecon
avx_platform_gateway_external=absecon
avx_visual_page_builder=absecon
avx_vendor_cert_network_discovery=absecon
avx_vendor_cert_scep_agent=absecon
avx_vendor_cert_intune_agent=absecon
avx_vendor_cert_est_agent=absecon
avx_vendor_cert_acme_agent=absecon
```

4. Execute the command <plugins_install.sh>
5. Verify the SCEP is enabled using command.

```
[appviewx@smenode1 ~]$ kubectl get services -A | grep scep
absecon               avx-vendor-cert-scep-agent               ClusterIP   10.105.243.26    <none>        5312/TCP
                                 12d
external-system       avx-platform-gateway-scep                NodePort    10.99.34.105     <none>        5302:30555/TCP
                                 6d15h
[appviewx@smenode1 ~]$
```

Chapter 4: Generate SCEP Registration Authority (RA)

To generate SCEP registration authority,

1. Log in to the **AppViewX** application with valid credentials.
2. Click on 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 asrequired.
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 a certificate, 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**.

Chapter 5: Configure SCEP via AppViewX GUI

To configure the SCEP via GUI,

1. Log in to the **AppViewX** application with valid credentials.
2. Click on the menu button.
   The left navigation pane appears.
3. Click **CERT+**.
   The **CERT+** left navigation pane appears.
4. Navigate to **Inventory** > **Certificate** > **Auto enrolment** > **SCEP**.
5. Click the **Add** button.
6. On the SCEP details page, under the **Agent Details** section, enter the Name, IP Address (node's IP address where SCEP plugin is running), and the Gateway Port.

   Note: Use the port number that is appearing when you enable SCEP services

7. Set the SCEP password in the Challenge Password field.
8. Under the **CA Accounts** section, select the **Certificate Group** from the drop-down list.
9. Select the Certificate Type as **Client** or **Server** based on the requirement.
10. Select the **CA** and **CA Account** from the respective drop-down lists. At present, AppViewX supports only AppViewX CA, EJBCA, and Microsoft CA.
11. In the **Server Certificate** field, upload the RA certificate that is created in the AppViewX using respective CA.
12. In the **CA Connector Name** field, enter the desired connector name.
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 get CA operation.
15. Enter the **Retry Count** and **Retry Frequency** in the respective fields.
16. Select the required **Certificate Poll Type** (select the **Issuer and Subject** or **Transaction ID**).
17. Click **Save**.
18. Once saved, AppViewX will generate and populate the SCEP URL in the GUI, which can be used for establishing the SCEP service. Multiple SCEP services can be configured in AppViewX GUI with the same VMware and unique SCEP agent names.

Chapter 6: SCEP Service Flow

- SCEP Service Flow

SCEP Service Flow

Once the AppViewX SCEP service gets configured and enabled, the client can start requesting for the certificate enrolments using this service. The entire certificate enrolment process has been mentioned below:

- Certificate Enrollment
- EST Enrollment
- AppViewX Server URL Details

Certificate Enrollment

For enrolling a certificate using the AppViewX SCEP services, the following processes will be executed which are based on the client vendors:

- Get CA Certificate
- Request a Challenge Passphrase
- Certificate Enrollment
- Enrollment Using SCEP Client
- Enrollment using Cisco Router

Get CA Certificate

During certificate enrolment request from the client, get CA certificate process will be executed first through the AppViewX enabled SCEP service. Some client vendors do not support get CA certificate process and this process will be skipped.

During this process execution, the client will request the user defined CA certificate from AppViewX. As the response to the client, AppViewX will share the user selected CA certificates, during the SCEP GUI configuration

Note: If the user has selected any intermediate certificate, in the response, AppViewX will share the complete chain of trust store certificates will be shared with the client. This CA certificate will be used for encrypting the data for further communication.

Request a Challenge Passphrase

This is an optional value only few client will use. During the certificate enrolment request, some clients will also send the challenge password along with the CSR (Certificate Signing Request). The SCEP service will validate this value against the challenge password value provided during respective SCEP service configuration in AppViewX GUI. If both the password value match, the enrolment process will be proceeded further.

Certificate Enrollment

During this process, the client will share the CSR (Certificate Signing Request) to AppViewX through SCEP service. AppViewX will forward the CSR to the user selected CA during its respective SCEP service configuration in AppViewX GUI. Once the CSR has been signed by the CA successfully, AppViewX will receive the signed certificate, create the chain of trust of certificates in the holistic view and push the certificate to the client as the response through the SCEP service. During push operation, the application connector for SCEP will be created and displayed in the holistic view.

Enrollment Using SCEP Client

Step 1

Get Enrollment URL from AppViewX Cert+ Auto enroll SCEP Page:

Step2

Generate Private kay and CSR with passphrase

Openssl Eg: openssl genrsa -out enrollment.key 2048 && openssl req -new -key enrollment.key -out enrollment.csr

Step3

Initiate GetCA Request

sscep getca -c -u

Eg:sscep getca -c ca-cert -u http://192.168.66.50:5250/services/scep/cert-scep/app

Step4

Request for Certificate:

sscep enroll -u <scep_url> -k ./<key_file> -r ./<csr_file> -c <ca_cert_file> -l

./<output_certificate>

Example:sscep enroll -u http://192.168.66.50:5250/services/scep/cert-scep/app -k ./enrollment.key -r ./enrollment.csr -c ca-cert-1 -l ./cert1.crt

Enrollment using Cisco Router

To enroll using Cisco router,

1. Configure using the Cisco Router Trustpoint.

   Cisco Router Trustpoint Configuration:

   crypto pki trustpoint scep-test

   enrollment url http://192.168.66.50:5250/services/scep/cert-scep

   fqdn SCEP_DEMO_Cisco_Router.avxdevcert.com

   subject-name CN=SCEP_DEMO_Cisco_Router

```
CSR_67_50#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
CSR_67_50(config)#
CSR_67_50(config)#crypto pki trustpoint scep-test
CSR_67_50(ca-trustpoint)#$//192.168.66.50:5250/services/scep/cert-scep
CSR_67_50(ca-trustpoint)# fqdn SCEP_DEMO_Cisco_Router.avxdevcert.com
CSR_67_50(ca-trustpoint)# subject-name CN=SCEP_DEMO_Cisco_Router
CSR_67_50(ca-trustpoint)#
```

2. Initiate GetCA Request from Router.

```
CSR_67_50(config)#crypto pki authenticate scep-test
Trustpoint 'scep-test' is a subordinate CA and holds a non self signed cert
Certificate has the following attributes:
       Fingerprint MD5: 0FB963B4 A5540CA6 7A462211 F6194AE8
      Fingerprint SHA1: 8ECAB98C 317286E1 BFF83C3B A2010DCC C0967E6C

% Do you accept this certificate? [yes/no]:
```

3. Initiate Enrollment Request.

```
CSR_67_50(config)#crypto pki enroll scep-test
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.

Password:
Re-enter password:

% The subject name in the certificate will include: CN=scep_router_test
% The subject name in the certificate will include: SCEP_DEMO_Cisco_Router.avxdevcert.com
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose scep-test' commandwill show the fingerprint.

CSR_67_50(config)#
```

Verification after Enrollment

```
CSR_67_50(config)#do sh crypto pki certificates scep-test
Certificate
  Status: Available
  Certificate Serial Number (hex): 3272BE7B534C7EED
  Certificate Usage: General Purpose
  Issuer:
    cn=avx_intermediate_ca
  Subject:
    Name: SCEP_DEMO_Cisco_Router.avxdevcert.com
    hostname=SCEP_DEMO_Cisco_Router.avxdevcert.com
    cn=SCEP_DEMO_Cisco_Router
  CRL Distribution Points:
    http://192.168.66.50/controller/avxcrl?crlFileName=212469579805591063.crl
  Validity Date:
    start date: 13:28:51 IST Jul 9 2019
    end   date: 13:28:51 IST Jul 8 2020
  Associated Trustpoints: scep-test

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 02F2D7F505E38617
  Certificate Usage: Signature
  Issuer:
    c=US
    st=Washington
    l=Seattle
    o=AppViewX Inc
    cn=AppViewX Intermediate CA
  Subject:
    cn=avx_intermediate_ca
  CRL Distribution Points:
    http://192.168.66.50/controller/avxcrl?crlFileName=975242343495596841.crl
  Validity Date:
    start date: 12:59:15 IST Jul 9 2019
    end   date: 14:12:06 IST Jul 6 2024
  Associated Trustpoints: scep-test est_test
  Storage: nvram:US#8617CA.cer

CSR_67_50(config)#
```

EST Enrollment

EST Enrollment Using Curl

1. Add Authentication Certificate and Key in the location
2. Generate CSR in the location using Openssl

Eg: openssl genrsa -out enrollment.key 2048 && openssl req -new -key enrollment.key

3. Initiate GeCACert Request using Curl
   - curl --cert <auth_cert>--key <auth_key>https://<ip>:<port>/.well-known/est/cacerts - o <output_ca_p7>

     Convert Recived p7 Certificate in to pem using openssl

   - openssl base64 -d -in <output_ca_p7>| openssl pkcs7 -inform DER -outform PEM - print_certs -out <output_ca_cert_pem>

   Example

   - curl --cert est_auth.crt --key est_auth.key --cacert 192-168-96-22.pem https://192.168.66.50:5301/.well-known/est/cacerts -o cacerts.p7 Convert Recived p7 Certificate in to pem using openssl
   - openssl base64 -d -in cacerts.p7 | openssl pkcs7 -inform DER -outform PEM -print_certs -out cacerts.pem
4. Initiate Enrollment Request
   - curl -k --cert <aith_cert>--key <auth_key> <simpleenroll_url> --data-binary @ <csr_file>-H "Content-Type: application/pkcs10" -o <signed_cert.p7>

     Convert Signed p7 Certificate in to pem using openssl

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

   Example

   - curl -k --cert est_auth.crt --key est_auth.key https://<ip>:<port>/.wellknown/est/simpleenroll --data-binary @ <csrfile.csr>-H "Content-Type: application/pkcs10" -o output.p7

     Convert Recived p7 Certificate in to pem using openssl

   - openssl base64 -d -in output.p7 -out output.decode | openssl pkcs7 -inform DER - outform PEM -in output.decode -print_certs -out est_signed.pem

AppViewX Server URL Details

For default EST instance in AppViewX, it will be listening on below URLs for the Operation paths: https://<IP>:<port>/.well-known/est/<operational_path>

Example: https://est.appviewx.com:<port>/.well-known/est/cacerts for getting ca certificate https://est.appviewx.com:<port>/.well-known/est/simpleenroll for Enrollment

For other EST instance in AppViewX, it will be listening on below URLs for the Operation paths with path segments: https://<IP>:<port>/.well-known/est/<agent_name>/<operational_path>

Example:

https://est.appviewx.com:<port>/.well-known/est/agent1/cacerts for getting ca certificate https://est.appviewx.com:<port>/.well-known/est/agent1/simpleenroll for Enrollment

1. Save Gateway Certificate in the location where libest is running
2. Save Authentication Certificate and Key in the location (in this example name is est_auth.crt, est_auth.key)
3. Set the environment variable using below command:

   export EST_OPENSSL_CACERT=appviewx_gw.crt (**appviewx_gw.crt** is the public certificate of the AppViewX Gateway where EST is listening)

4. **Getca** certificate from EST server (defaultEST instance) with TLS authentication. (Authentication certificates are already placed in the client folder)

   ./estclient -g -s est.appviewx.com -p 5301 -o certs -c est_auth.crt -k est_auth.key

5. Enroll request

   ./estclient -e -s est.appviewx.com -p <port>-o certs -c est_auth.crt -k est_auth.key --pemoutput --common-name myclient3 -w 15

6. Enroll request for other EST instances

   ./estclient -e -s est.appviewx.com -p <port>-o certs -c est_auth.crt -k est_auth.key --pemoutput --common-name myclient3 --path-seg <agent_name> -w 15