Importing the SHA2 Certificate

This appendix describes importing the SHA2 certificate to the Cisco Edge 340 Series. The details of creating, getting, or generating the certificate are not provided in this document.

There are two ways to import the SHA2 certificate in CE340:

- Certificate API, page D-1
- SCEP API, page D-3

Certificate API

The Cisco Edge 340 Series support certificate generated from Non-SCEP server as well.

Certificate API user should have key file of certificate with it.

Note Make sure to provide hostname of CE340 in Common Name Field while creating or getting certificate.

Following are the steps to insert certificate using Certificate API:

Step 1 To generate the Key and CSR from the CE340 CLI:

i. `# openssl genrsa -out key_name.key 2048`

Example

```
[root@CE340 home]# openssl genrsa -out 340.key 2048
Generating RSA private key, 2048 bit long modulus
.....................................................................................
..............+++
.....................................................................+++
e is 65537 (0x10001)
[root@CE340 home]# pwd
/home
[root@CE340 home]# ls
340.key  api.txt  lost+found  ssid.txt  user
[root@CE340 home]#
```

ii. `# openssl req -out sha256.csr -key key_name.key -new -sha256`

Example

Step 2 Generate the certificate from the CA server using CE340 CSR.

Step 3 To load the certificate from the local storage, use the following command:

```
# curl -k -X PUT -u root:aDMIN123# https://127.0.0.1/api/v3/import/certificate/nginx
--form key=@<path to certificate key file> --form crt=@<path to crt file>
```

Example

```
curl -k -X PUT -u root:aDMIN123# https://127.0.0.1/api/v3/import/certificate/nginx --form
key=@/home/tmp/server.key --form crt=@/home/tmp/server.crt
```

Upon success the # prompt will be shown on the screen after the above command is executed.

Upon failure the generic failure message will be shown on the screen and then the # prompt will be shown.

Step 4 To load the certificate from a remote server, use the following command:

```
# curl -k -X PUT -u root:aDMIN123# https://127.0.0.1/api/v3/import/certificate/nginx
--form key=<link location of remote server key file> --form crt=<link location of remote
server crt file>
```

Example

```
curl -k -X PUT -u root:aDMIN123# https://127.0.0.1/api/v3/import/certificate/nginx --form
key=http://10.107.3.155:8080/server.key --form crt=http://10.107.3.155:8080/server.crt
```

Upon success the # prompt will be shown on the screen after the above command is executed.

Upon failure the generic failure message will be shown on the screen and then the # prompt will be shown.

Step 5 To verify that the newly loaded certificate is inserted, use the follow the command:

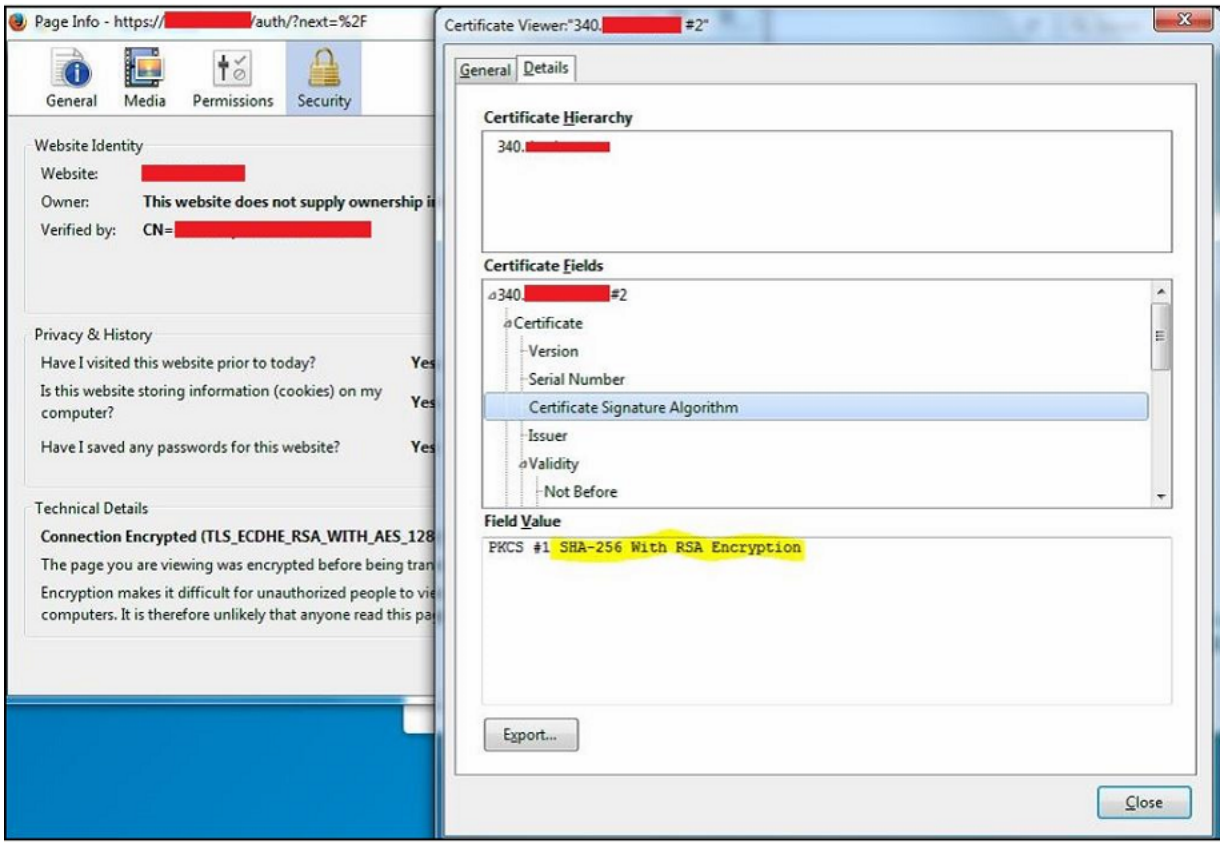
```
# curl -k -X GET -u root:aDMIN123# https://127.0.0.1/api/v3/import/certificate/nginx
```

This command will display the newly inserted certificate. Upon success the # prompt will be shown on the screen after the above command is executed.

Step 6 After loading the new certificate, restart the nginx server by executing the following command:

```
# service nginx restart
```

Step 7 Check the certificate in GUI as following:



SCEP API

Follow these steps to get certificate from the NDES server:

Step 1 Upgrade or reimage the device with the new 1.2.0.19 patch.

Step 2 Connect to the CE340 via SSH.

Step 3 Create a file named as `api.txt` by using the text editor present in CE340.

Following is a sample file. Please change the values in **bold** and *italic* according to your requirement.

Note Make sure to provide hostname of CE340 in Common Name Field while creating or getting certificate.

```
{
"module": "http",
"managed": "true",
"url": "http://<SCEP-Server-ip>/CertSrv/mscep/mscep.dll",
"challenge_password": "<SamplePassword>",
"params": {
"keysize": 2048,
"subject":
"/C=<country-name>/ST=<state-name>/O=<organization-name>/CN=<device-hostname>/emailAddress
=email@yourcompnay.domain"
}
}
```

Step 4 Execute the following command at the same location where `api.txt` was created to configure the SCEP server information:

```
# curl -X PUT -u root:aDMIN123# -H "Content-Type:application/json" -d @api.txt
http://127.0.0.1/api/v3/system/scep
```

Upon success the # prompt will be shown on the screen after the above command is executed.

Upon failure the generic failure message will be shown on the screen and then the # prompt will be shown.

Step 5 Verify that the certificate request file and private key are generated:

```
# openssl req -in /usr/local/share/cpgmgt-service/scep/keystore/http/csr/server.csr -noout
- text
```

```
[root@test-340 ~]# openssl req -in /usr/local/share/cpgmgt-service/scep/keystore/http/csr/server.csr -noout -text
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=IN, ST=KA, O=[redacted], CN=340.[redacted].com/emailAddress=[redacted]@[redacted].com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c8:a0:85:ea:23:9e:7e:29:ae:5b:47:8e:40:ed:
                    6d:84:d0:c0:5a:ae:c6:0a:fa:71:fd:63:79:27:12:
                    0e:d6:de:22:87:ad:67:96:8e:01:1a:80:f1:b9:c3:
```

Step 6 Call get_ca:

```
# curl -X PUT -u root:aDMIN123# -H "Content-Type:application/json" -d
'{"method":"getca","module":"http"}' http://127.0.0.1/api/v3/system/scep/command
```

Upon success the # prompt will be shown on the screen after the above command is executed.

Upon failure the generic failure message will be shown on the screen and then the # prompt will be shown.

Step 7 Call enroll:

```
# curl -X PUT -u root:aDMIN123# -H "Content-Type:application/json" -d
'{"method":"enroll","module":"http"}' http://127.0.0.1/api/v3/system/scep/command
```

Upon success the # prompt will be shown on the screen after the above command is executed.

Upon failure the generic failure message will be shown on the screen and then the # prompt will be shown.

Step 8 Make sure the certificate is generated and saved locally on CE340:

```
# ls /usr/local/share/cpgmgt-service/scep/keystore/http/cert server.crt
```

Step 9 Make sure that relevant or valid details are present in the certificate:

```
# openssl x509 -in /usr/local/share/cpgmgtservice/scep/keystore/http/cert/server.crt -text
```

```
[root@test-340 cert]# openssl x509 -in /usr/local/share/cpgmgt-service/scep/keystore/http/cert/server.crt -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            13:b7:23:c8:00:01:00:00:00:0e
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: DC=com, DC=[redacted], DC=[redacted], CN=[redacted]-CA
        Validity
            Not Before: May 28 12:19:09 2015 GMT
            Not After : May 27 12:19:09 2017 GMT
        Subject: C=IN, ST=KA, O=[redacted], CN=340.[redacted].com/emailAddress=[redacted]@[redacted].com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c8:a0:85:ea:23:9e:7e:29:ae:5b:47:8e:40:ed:
```

Step 10 Restart the nginx server or reboot the device. This step will insert the SCEP certificate in CE340.

```
[root@test-340 cert]# service nginx restart
Redirecting to /bin/systemctl restart  nginx.service
[root@test-340 cert]#
```

Step 11 Check the certificate in GUI as well as in NDES server to ensure that the correct certificate is inserted.