

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

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

Example

[root@CE340 home] # openss1 req -out sha256.csr -key 340.key -new -sha256
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
Country Name (2 letter code) [XX]:
State or Province Name (full name) [] 💳
Locality Name (eg, city) [Default City]:
Organization Name (eg, company) [Default Company Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:340com
Email Address []:email
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []
An optional company name []:xxxx
[root@CE340 home]#
[root@CE340 home]#
[root@CE340 home]#
[root@CE340 home]# 1s
340.key api.txt lost+found sha256.csr ssid.txt user
[root@CE340 home]#

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:

Page Info - https://	Certificate Viewer:"340.
General Media Permissions Security Website Identity Website: Owner: This website does not supply ownership in Vesified here CN-	General Details Certificate Hierarchy 340.
Privacy & History Have I visited this website prior to today? Yes Is this website storing information (cookies) on my computer? Yes Have I saved any passwords for this website? Yes Technical Details Connection Encrypted (TLS_ECDHE_RSA_WITH_AES_128 The page you are viewing was encrypted before being tran Encryption makes it difficult for unauthorized people to vie computers. It is therefore unlikely that anyone read this pa	Certificate Eields a340 a Certificate Version Serial Number Certificate Signature Algorithm Issuer aValidity Not Before Field Yalue PKCS #1 SHA-256 With RSA Encryption Export
	Close

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.

<u>Note</u>

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>/0=<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 ~]# opensal 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, 0=____, CN=340.____.com/emailAddress=_____@c____.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



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



Page Info - https://www.auth/?next=%2F	Certificate Viewer:"340.
Ganaral Madia Decemistions	General Details
Website Identity Website: Owner: This website does not supply ownersh	ip it
remed by.	Certificate Fields
Privacy & History Have I visited this website prior to today? Is this website storing information (cookies) on my computer? Have I saved any passwords for this website? Technical Details Connection Encrypted (TLS_ECDHE_RSA_WITH_AES_	Yes Certificate Version Serial Number Yes Certificate Signature Algorithm Issuer aValidity Not Before Field Value EXEC at 1 SB-256 Mith. PSA Encreant ion
The page you are viewing was encrypted before being Encryption makes it difficult for unauthorized people to computers. It is therefore unlikely that anyone read this	Egport
	Çlose
ver Manager Reles Reles Active Directory Certificate Services Active Directory Certificate Services Certificate Templates (Revoked Certificates Fonding Requests Fonding Requests Certificate Templates Certificate Templat	Issued Certificates Request ID Request IN Binary Certificate Certificate Template Serial Number Certificate Effective Date 2 WINAUTH/WIN BEGIN CERTI Domain Controller (611bbf39000 5/20/2015 9:35 AM 3 WINAUTH/admin BEGIN CERTI Exchange Enrollmen 6141f6d0000 5/20/2015 10:16 AM 4 WINAUTH/admin BEGIN CERTI CEP Encryption (CE 6141f6d0000 5/20/2015 10:26 AM 5 WINAUTH/admin BEGIN CERTI CEP Encryption (CE 614930a000 5/20/2015 10:26 AM 6 WINAUTH/admin BEGIN CERTI CEP Encryption (CE 614930a000 5/20/2015 10:26 AM 7 WINAUTH/WIN BEGIN CERTI CA Exchange (CAEx 126/447000 5/20/2015 8:32 AM 9 WINAUTH/WIN BEGIN CERTI Cross Certification A 1368350000 5/27/2015 8:40 AM 10 WINAUTH/WIN BEGIN CERTI Cross Certification A 136835000 5/27/2015 8:40 AM 111

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

Server Manage

E

Đ

E DNS S E File Se Web S