Configuring SCEP and Obtaining and Enrolling the Certificate

Cisco Edge 340 Series supports Simple Certificate Enrollment Protocol (SCEP) since software Release 1.2 patch 12.

Components Used

The information in this document is based on these software and hardware versions:

- Windows 2008 server
- Server with a Certificate Authority (CA) available
- Cisco Edge 340

Note The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any commands.

Note For more information on the SCEP server configuration, see http://social.technet.microsoft.com/wiki/contents/articles/9063.network-device-enrollment-service-ndes-in-active-directory-certificate-services-ad-cs.aspx

To configure SCEP and obtain and enroll the certificate, follow these steps:

Step 1 Establish a secure shell (SSH) connection with the CE340.

Step 2 Apply the SCEP patch image.

For detailed information about applying the patch 1.2.0.12, see the release notes for patch 12.

Step 3 Create a text file with SCEP server information as following:

```
[root@340 home]# cat api.txt
{
  "module": "http",
  "managed": "true",
  "url": "http://<SCEP_Server_IP>/CertSrv/mscep/mscep.dll",
  "challenge_password": "",
  "params": {
      "keysize": 2048,
```

```
      "subject":
  "/C=IN/ST=Bangalore/O=Example/CN=test.example.com/emailAddress=admin@example.com"
  }
}
```

Parameter	Description
module	Specifies the module to be enabled. Currently, the only supported value is web server: http.
managed	Specifies whether or not need SCEP manage.
url	Specifies CA server URL. For example: http://10.75.212.202/CertSrv/mscep/mscep.dll”
challenge_password	(Optional) The value of this field depends on the server settings. For example, if EnforcePassword=0, this field need to be empty.
params	CSR and private key related parameters.

Parameter	Description
keysize	The value is 2048, 4096, or 8192.
subject	Certificate subject. For example, `/C=<Country Name>/ST=<State>/L=<Locality Name>/O=<Organization Name>/CN=<Common Name>` Supported subjects are as following:

Subject Key Name	Description
C	Country name
ST	State
L	Locality name
O	Organization name
CN	Common name
OU	Organization unit
emailAddress	Email address

Return Value	Description
“”	Success.
Others	Exceptions.

Step 4 Set 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
```

Step 5 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
```

Step 6 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
```

Step 7 Certificate will be saved.

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

Step 8 Check the certificate in CE340.

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

Step 9 Restart the nginx server or reboot the device.

```
# service nginx restart
```

Step 10 Certificate can be checked in the CE340 browser as well as in the NDES server issued certificates.

Table C-1 Supported Methods and SCEP Server

	NDES (Windows 2008)	NDES (Windows 2003)
getca	Supported	Supported
enroll	Supported	Supported
getcert	Supported	Supported
getcrl	Not supported	Supported