IEEE 802.1X authentication with SCEP

Short Guide

Last edited: 2020-06-19

06-23 03:32

1. IEEE 802.1X authentication with SCEP support

Certificate-based logon with 802.1X

IEEE 802.1X is an IEEE standard for port-based Network Access Control in IEEE 802 networks. It provides an authentication mechanism for client devices (supplicants) wishing to attach to a LAN or WLAN. The supplicant provides credentials such as a digital certificate to an authenticator, and the authenticator forwards the credentials to an authentication server (RADIUS) for verification. The authenticator can be an IEEE 802.1X-capable Ethernet switch or wireless access point. If the authentication server determines the credentials are valid, the supplicant is allowed to access the protected side of the network.

As a RADIUS server, you can use the Microsoft Network Policy Server (NPS) or a freeware program such as freeRADIUS.

The supplicant is implemented as a software program. We support the free software **wpa_supplicant**.

The standard recommends the Extensible Authentication Protocol (EAP) or the PPP-EAP-TLS Authentication Protocol for authentication.

Certificate handling with SCEP

SCEP is a protocol designed to simplify secure and scalable issuing of certificates to network devices in large-scale environments.

With SCEP, the devices get their certificates themselves. To do this, they require a one-time password created by an authorized person. The client device can use this time-limited password (Windows: 60 minutes) to request a certificate from the SCEP service.

To prevent the certification authority (CA) from issuing arbitrary certificates with the one-time password, you can create a template in which you restrict the certificate classes.

The eLux implementation is based on the **OpenSCEP** project. The following description requires the use of Windows NDES.

2. Windows as SCEP server

Note
For Windows Server 2012 and later versions, NDES (Network Device Enrollment Service) is integrated in the Certification Authority (CA).
The described procedure is to be seen as an example and can vary depending on the version and environment.

Installing NDES

1. Install the server role **AD CS** with the **Network Device Enrolment Service** feature .
2. Set up a service account for NDES which must be authorized on the CA later on.
3. Enter the information for the certificate from the Registration Authority (RA) to issue a signing certificate for this enrollment process.
4. Define the key length.

The new virtual directories are displayed in the IIS console below the default website.

Configuring templates

The SCEP server uses templates for submission to the CA.

1. Set the LDAP name of the template in the registry:

   [HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\MSCEP

Default:	`IPSecIntermediateOffline`
EncryptionTemplate	*<templatename>*
GeneralPurposeTemplate	*<templatename>*
SignatureTemplate	*<templatename>*

2. Add the new template to the CA.
3. Configure the use of a one-time password in the registry (validity period, maximum number).

The one-time password allows a client that supports SCEP/NDES to contact the SCEP server directly and request a certificate. The client connects to the Windows SCEP server with the URL http://<CA_FQDN>/certsrv/mscep/mscep.dll

Configuring one-time password

Either

- disable passwords (option A):
  [`HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\MSCEP\EnforcePassword`]
  set to `0`

or

- define fixed password (option B):
  [`HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\MSCEP\UseSinglePassword`]

Permissions for NDES service account

- Set the permission to `full control`.

Modify SCEP application pool defaults

- Set **Load User Profile** option from `false` to `true`.

Requesting one-time passwords

1. Sign in to the SCEP Administrator website using your NDES service account:
   `http://<CA_FQDN>/certsrv/mscep_admin/`
2. Copy the challenge password to the configuration file `scep.ini`

3. Configuring SCEP for eLux clients

This is how you enable eLux clients to use SCEP for the certificate deployment:

1. Make sure that the eLux package **Network Access Control** and the included feature package **SCEP** are installed on the clients. This may require modifications of the image definition file on the web server via ELIAS.
2. To configure the SCEP agent, use the file `scep.ini`. Then select the Scout Enterprise feature Files configured for transfer to transfer the configuration file to the clients. For further information, see Configuring SCEP ini file.
3. Ensure that the clients have the correct time. We recommend that you configure a time server.

   The local time must match the time of the certificate authority.
4. To activate the SCEP agent, add the following entry to the `terminal.ini` file on the clients by using the Scout Enterprise feature **Advanced file entries**:

File	`/setup/terminal.ini`
Section	`Network`
Entry	`SCEP`
Value	`true`

   Please note that the terms are case-sensitive.
   For further information, see Advanced file entries in the **Scout Enterprise** guide.

The client creates a WPA configuration file from the template `setup/scep/wpa.conf.scep`. However, if you have transferred an individual WPA configuration file to `/setup/scep/wpa.conf`, it has precedence.[1]

[1] for eLux RP 5.7.1000 and later versions

3.1. Certificates for SCEP

The following certificates are stored in `/setup/cacerts/scep` by the SCEP agent.

client.pem	Client certificate	
client.key	Private key of client certificate	for exception, see below
serverca.pem	Server CA certificate	
serverca.key	Server CA key	required to perform the request
serverca.sig	Server CA signature	required to perform the request

Thin Clients with TPM 2.0

– for eLux RP 6.7 and later versions –

If TPM 2.0 (Trusted Platform Module) is installed in the thin client, by default, the private key for the SCEP client certificate is not stored in the file system, but in the TPM 2.0 module. This is done automatically and does not require any special configuration.

The corresponding authentication procedures via WPA supplicant for wired Ethernet connections and via IEEE 802.1x for WLAN components consider both storage options for the SCEP private key - the file system and the TPM 2.0 module.

When you update your eLux version to a version with TPM 2.0 support, existing private keys for SCEP client certificates are moved from the file system to the TPM 2.0 module.

Client certificates continue to be stored in the file system. The rollout procedure, with which the clients initially receive the client certificates, is carried out exclusively via wired Ethernet connections. Existing certificates can be renewed both via wired Ethernet connections and via WLAN.

Deleting private SCEP key from TPM 2.0 module

- For the relevant devices, in the Scout Enterprise Console, use the **Remote factory reset** command with the option **Delete Scout Enterprise server address on device**.

Storing private SCEP key outside TPM 2.0 module

- To prevent the system from storing the private key for the SCEP client certificate inside the TPM 2.0 module, define the following `terminal.ini` entry:[1]

File	`/setup/terminal.ini`
Section	`Network`
Entry	`DisableSCEP2TPM`

[1] for eLux RP 6.9 and later versions

Value	`true`	By default, the value is `false`.

For further information, see Advanced file entries in the **Scout Enterprise** guide.

The private key file is then stored in the certificate store under `/setup/cacerts/scep` or in the directory defined in `scep.ini`.

3.2. Configuring the SCEP ini file

Note
You can use the example file on the clients to configure the SCEP agent:
`setup/scep/scep.ini.sample`

1. Create the text file `scep.ini` and insert the sections and entries described below.
2. To transfer the configuration file `scep.ini` to the clients to `setup/scep/`, use the Scout Enterprise feature Files configured for transfer. For further information, see Advanced device configuration > Files in the **Scout Enterprise** guide.

The certificate request is created from the `scep.ini` data. You can optionally extend the certificate request with additional attributes.[1] For further information, see "Extended SCEP certificate request" on page 11.

Sections and entries for `scep.ini`

Section	Entry	Description	Example
Admin	URI	SCEP server address (URI)	`URI=http://ca.w2k12.sampletec-01.com/certsrv/mscep/`
	PROXY	Proxy server (optional)	`PROXY=proxy.sampletec-01.com:3800`
	ReNew	Number of days before the certificate expires From this day on, the client tries to renew the certificate.	`ReNew=30`
	ExpireCheck	Time interval in days, how often the ReNew date is checked	`ExpireCheck=1`
	challengePassword	One-time password for the request Valid for 60 minutes once only The password is deleted after the certificates have been successfully transferred.	(A): `challengePassword=12345` (B): `challengePassword=<password requested via http://CA_FQDN/certsrv/mscep_admin/>`

[1] ab eLux RP 6.8

Note

For eLux RP 5 only: If you have deactivated the password in the registry (variant A), you must still specify a dummy value that is not evaluated.

Certificate	CNTYPE	Type (`autoip|ip|dns|autodns|dnsfqdn|email`) `autoip` The IP address of the device is used as **CN**. `ip` The IP address you specify as **CN** in the `scep.ini` (see next option) is used. `dns` The name you specify as **CN** in the `scep.ini` (see next option) is used. `autodns` The host name specified in the `terminal.ini` is used as **CN**. `dnsfqdn`[1] The host name specified in the `terminal.ini` with the domain name appended is used as **CN**. `email` The email address you specify as **CN** in the `scep.ini` (see next option) is used.	`CNTYPE=email`
	CN	Certificate/Name Is filled by the system for `CNTYPE=autoip|autodns|dnsfqn`	`CN=userxxx@sampletec-01.com`

	OU
	ORGANIZATION
	LOCALITY
	STATE
		Certificate/Attribute (optional)	`OU=TestLab`
			`ORGANIZATION=SampleTec`
			`LOCALITY=Karlsruhe`
			`STATE=BW`

[1] for eLux RP 6.7 and later versions

	OU1[1] OU2 OU3 OU4 OU5 OU6	Further attributes for up to 6 OUs[2] (optional) The OUs specified here can be used for a certificate request.	OU1=Testlab OU2=KA_QA OU3=KA_DEV
	COUNTRY	Certificate/Country	`COUNTRY=DE`
	KEYLEN	Key length (from certificate template) The maximum length is `2048`. Incorrect key length leads to event log entry **Incorrect Challenge Password**	`KEYLEN=2048`
	CertStore[3]	The certificate store can be freely selected from eLux RP 6.8 onwards.	`CertStore=/setup/cacerts/scep`

Note
If a thin client has a TPM 2.0 module built in, the private key for the SCEP client certificate is only stored in the TPM 2.0 module if you specify the default path `/setup/cacerts/scep`.

[1]for eLux RP 6.8 and later versions
[2]for eLux RP 6.8 and later versions
[3]for eLux RP 6.8 and later versions

3.3. Extended SCEP certificate request

– for eLux RP 6.8 and later versions –

Note
This function is only necessary if you want to configure the SCEP agent with additional attributes that are not set via `scep.ini`

The certificate request is created from the values in the `scep.ini` file and is available on the device in the file `setup/scep/clientreq.conf.in`. This file is already installed with SCEP as a template and has the following entries by default:

```
[req]
prompt=no
distinguished_name=req_distinguished_name
string_mask=nombstr
attributes=req_attributes

[req_attributes]
challengePassword=__CHALLENGEPASSWORD__

[req_distinguished_name]
C=__COUNTRY__
ST=__STATE__
L=__LOCALITY__
O=__ORGANIZATION__
OU=__OU__
1.OU=__OU1__
2.OU=__OU2__
3.OU=__OU3__
4.OU=__OU4__
5.OU=__OU5__
6.OU=__OU6__
CN=__CN__

[__X509V3__]
subjectAltName=critical,__CNTYPE__:__ALTNAME__
```

The fields marked with underscores are macros and are replaced by the values from `scep.ini`.

If the attributes provided in the `scep.ini` are sufficient for your purposes, there is no need to edit the `clientreq.conf.in` file.

Extending certificate request with additional attributes

1. Get the `setup/scep/clientreq.conf.in` file installed with SCEP from a device, for example by using the **Diagnostics** feature.

2. Edit the file. Add any other openSSL sections and attributes. For further information, see https://www.openssl.org/docs/man1.0.2/man1/openssl-req.html
3. Transfer the file to the relevant clients to `setup/scep/clientreq.conf.in` by using the Scout Enterprise feature **Files configured for transfer**.

Note

This file - and not the `scep.ini` - is the source for the certificate request. Only delete fields that you do not need!.

4. Configuring 802.1X

Note
802.1X can be configured for LAN or WLAN. The procedure differs in the location of the configuration file and in some parameters. For further information, see Configuring WPA supplicant.

1. Make sure that the eLux package **WLAN drivers** and the included feature package **WPA supplicant** are installed on the clients. This may require modifications of the image definition file on the web server via ELIAS.
2. Transfer the required certificates to the clients to `/setup/cacerts` by using the Scout Enterprise feature Files configured for transfer.

   Note
   The certificates of your RADIUS environment require the FQDN for the Common Name (CN).

3. Configure the file `wpa.conf`, and then transfer the configuration file to the clients by using the Scout Enterprise feature Files configured for transfer. For further information, see Configuring WPA supplicant.
4. If you use SCEP, alternatively generate the file `wpa.conf` from the template `wpa.conf.scep`. For further information, see WPA configuration via template.
5. In the Scout Enterprise Console, for the relevant OU, in the device configuration under **Network > LAN > Advanced > IEEE 802.1X authentication**, select the **Activate** option.

If the configuration is correct and the required certificates are rolled out, you can use devices on the 802.1X port.

4.1. Configuring WPA supplicant

Note
You can use the example files on the clients to configure the WPA supplicant:
`setup/scep/wpa.conf.*`

1. Create an individual `wpa.conf` configuration file.

   By default, the file contains the following information:

```
ctrl_interface=/var/run/wpa_supplicant
ctrl_interface_group=0
ap_scan=0
network={
   key_mgmt=IEEE8021X
   eapol_flags=0
   eap=TLS
   identity="Common Name as specified in certificate"
   ca_cert="/setup/cacerts/scep/serverca.pem"
   client_cert="/setup/cacerts/scep/client.pem"
   private_key="/setup/cacerts/scep/client.key"
   }
```

   Note
   For `identity`, you can alternatively set the host name of the device via a variable:[1]
   `identity="__HOSTNAME__"`
   Correct spelling: Two underscores followed by the word `HOSTNAME` (all uppercase) followed by two more underscores.

   Add further entries according to your CA implementation, for example, if you access an external root certification authority:

```
ca_cert="/setup/cacerts/<root_extern>.pem"
ca_cert="/setup/cacerts/<intermediate_extern>.pem"
ca_cert="/setup/cacerts/<subordinate_intern>.pem"
ca_cert="/setup/cacerts/<radius>.ssl"
```

   If the RADIUS certificate contains the NetBIOS name instead of the FQDN, use the following entries:

```
ca_cert="/setup/cacerts/<intermediate>.pem"
ca_cert="/setup/cacerts/<root>.pem"
```

[1] from eLux RP 6.9

Important

The spelling and case-sensitivity of the certificate file names must be identical to the names of the transferred certificate files.

2. To transfer the `wpa.conf` file to the clients, use the Scout Enterprise feature **Files configured for transfer**. Use the following destination:

LAN	`setup/scep/`
WLAN	`setup/wlan/`

For further information, see Advanced device configuration > Files in the **Scout Enterprise** guide.

For further information on configuring 802.1X for WLANs, see WPA support in the **Scout Enterprise** guide.

4.2. WPA configuration via template

– only if SCEP is used –

Note

The following information is related to 802.1X configuration of LANs.

If you use SCEP, you can benefit from the template file `setup/scep/wpa.conf.scep` provided on the clients:

```
ctrl_interface=/var/run/wpa_supplicant
ctrl_interface_group=0
ap_scan=0
network={
   key_mgmt=IEEE8021X
   eapol_flags=0
   eap=TLS
   identity="__IDENTITY__"
   ca_cert="/setup/cacerts/scep/serverca.pem"
   client_cert="/setup/cacerts/scep/client.pem"
   private_key="/setup/cacerts/scep/client.key"
   }
```

Note

The __IDENTITY__ variable is replaced by the CN of the client certificate.

The client evaluates this template and creates the `wpa.conf` file if the following requirements are met:

- SCEP is configured in the `terminal.ini` file of the client.
- There is no individual `/setup/scep/wpa.conf` file available.[1]

If required, modify the template and transfer it to the clients to `setup/scep/wpa.conf.scep`. To do so, use the Scout Enterprise feature Files configured for transfer. Note that if you have an individual `/setup/scep/wpa.conf` file,[2] it has precedence.[3]

Note

The `wpa.conf` file generated from the template is created in a temporary directory and can only be viewed via the diagnostic files.

[1] for eLux RP 5.7.1000 and later versions

[2] see Configuring WPA supplicant

[3] for eLux RP 5.7.1000 and later versions

5. Diagnosis for SCEP and 802.1X

Show client certificate in a shell

- Use the following command:
  `openssl x509 -in /setup/cacerts/scep/client.pem -noout -text`

All information about the certificate is displayed.

View log files

1. For the relevant OU, in the device configuration, enable enhanced logging.
2. Request the diagnostic files. For further information, see Requesting diagnostic files in the **Scout Enterprise** guide.

`/var/log/messages`	Kernel log file[1]
`/tmp/systemd-journal.log`	Network log file[2]
`/setup/logs/scepagent.log`[3]	Log file of the SCEP agent, contains last certificate transfer This file is not included in the template `#System`, but must be defined in an individual template. For further information, see Configuring diagnostic files in the **Scout Enterprise** guide.

[1] relevant up to eLux RP 6.3
[2] for eLux RP 6.4 and later versions
[3] temporary version under `/var/log/scepagent.log`