IEEE 802.1X authentication

Short Guide

Last edited: 2022-05-27

1. IEEE 802.1X authentication for eLux

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.

Note
For certificate enrollment and management, you can use SCEP which is supported by eLux.

Certificate-based logon with 802.1X and TPM 2.0

In combination with SCEP, private keys on TPM 2.0 devices can be stored in the TPM 2.0 module.[1] To further secure authentication, starting with eLux RP 6.2021, you have the option to have cryptographic keys generated inside the TPM 2.0 chip of a device. These keys can neither be displayed nor exported.

For further information, see Certificates for SCEP in the SCEP guide.

---

[1] ab eLux RP 6.7

2. Configuring 802.1X for eLux

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 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 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. Only LAN: In the Scout 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.

2.1. 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>"
    priority=6
    ca_cert="/setup/cacerts/scep/serverca.pem"
    client_cert="/setup/cacerts/scep/client.pem"
    private_key="/setup/cacerts/scep/client.key"
        }
```

   Add further entries according to your CA implementation.

   You can specify the certificate file and path in one of the following ways, for example if you access an external root certification authority. Note that only one file may be referenced via `ca_cert`. However, this file may contain several certificate entries.

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

   If the RADIUS certificate contains the NetBIOS name instead of the FQDN, you may use the following entry:

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

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

2. If you want to use TPM 2.0 via WLAN, add the following **engine** parameters for the network:[1]

```
...
network={
    ssid="WLAN-ABC"
    scan_ssid=1
    key_mgmt=WPA-EAP
    proto=WPA2
    eap=TLS
    engine=1            # Value must always be 1
    engine_id="tpm2tss"    # Private Key is taken from TPM 2.0 module
    dentity="__IDENTITY__"
    priority=6
    ca_cert="/setup/cacerts/scep/serverca.pem"
    client_cert="/setup/cacerts/scep/client.pem"
    private_key="/setup/cacerts/scep/client.key"    # Public part
}
```

3. To transfer the `wpa.conf` file to the clients, use the Scout 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** guide.

Use of multiple WiFi networks

- To use multiple SSIDs, set the **network** entry multiple times.

Example:

```
ctrl_interface=/var/run/wpa_supplicant
ctrl_interface_group=0
ap_scan=1
network=
{ ssid="" scan_ssid=1 key_mgmt=WPA-EAP eap=TLS identity="" priority=5 ca_cert="" ca_cert=""
client_cert="" private_key="" }
network=
{ ssid="" scan_ssid=1 key_mgmt=WPA-EAP eap=TLS identity="" priority=6 ca_cert="" ca_cert=""
client_cert="" private_key="" }
```

[1] from eLux RP 6 2103

Use of variables

For `identity` and `host name`, you can alternatively set variables:[1]

Spelling	Description	Other
`%IDENTITY%`	Common name from certificate	For compatibility reasons, the legacy spelling before eLux RP 6.9.100 (variable name in uppercase letters and 2 x 2 underscores is still supported. Example: `__IDENTITY__`
`%HOSTNAME%`	Hostname from `terminal.ini`	

Variables may also be used for a part of a value.[2] Prefixes and suffixes of a variable are pure strings that are passed through.
Example: `identity="host/%HOSTNAME%"`

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

[1] from eLux RP 6.9
[2] from wlandrivers 10.2, included from eLux RP 6.9.100 and eLux RP 6.10 onwards

2.2. WPA configuration via template (SCEP)

- 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%`[1] 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. For further information, see Configuring SCEP for eLux clients in the SCEP guide.
- There is no individual `/setup/scep/wpa.conf` file available.

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

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] Former spelling: `__IDENTITY__`
[2] see Configuring WPA supplicant

3. Diagnosis for 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** guide.

`/tmp/systemd-journal.log`	Network log file[1]

[1] for eLux RP 6.4 and later versions