How to use a WLC as SCEP server and an Open BAT as SCEP client

- 2018-02-21 - BAT, WLC (HiLCOS)

One of the characteristic of the WLC is to be a Certification Autorithy (CA).
It generates certificates and these certificates are used for a secure communication for example between the AP and the controller itself.
Most of the time it's done automatically for example when the controller applies a profile on an Access Point.
Automatically a configuration is also applied on the AP to manage the issuing and revocation of the certificates.
SCEP is used (Simple Certificate Enrollment Protocol).
Basically SCEP is designed to make the issuing and revocation of digital certificates as scalable as possible.
Using SCEP, devices or network users are be able to request their digital certificate electronically.

Managed AP have a SCEP configuration automatically applied when a profile is applied.
Then SCEP will take care of the revocation of the certificate and the device is able to request automatically a new certificate to the CA (the WLC) before the certificate expires.

But a manual configuration of SCEP in some cases is necessary:
For example if we want to use the WLC as radius server and Access clients as 802.1x supplicants using EAP/TLS

The AC need to get a certificate from the WLC (CA) and for that SCEP must be used because the only way for a WLC to generate a certificate is to use SCEP (we canno't somehow manually require the WLC to generate a certificate and then somehow manually install it on the AC like we can do using tools like XCA or OpenSSL)

It means that the AC, before than being used as 802.1x supplicant, has to request via SCEP a certificate to the WLC, in other words it needs to be able to reach the WLC via the network with the correct SCEP configuration. It will then get it's scertificate via SCEP. Then it can be used as 802.1x supplicant with EAP/TLS authentication (with the WLC as radius server).
SCEP will also take care to re-issue a new certificate before the certificates expires.

This how to explains step by step how to proceed to configure SCEP manually on a AC.

Representation

Preliminary steps

Give the BAT and the WLC an IP address (in our example: 192.168.1.130 and 192.168.1.100)

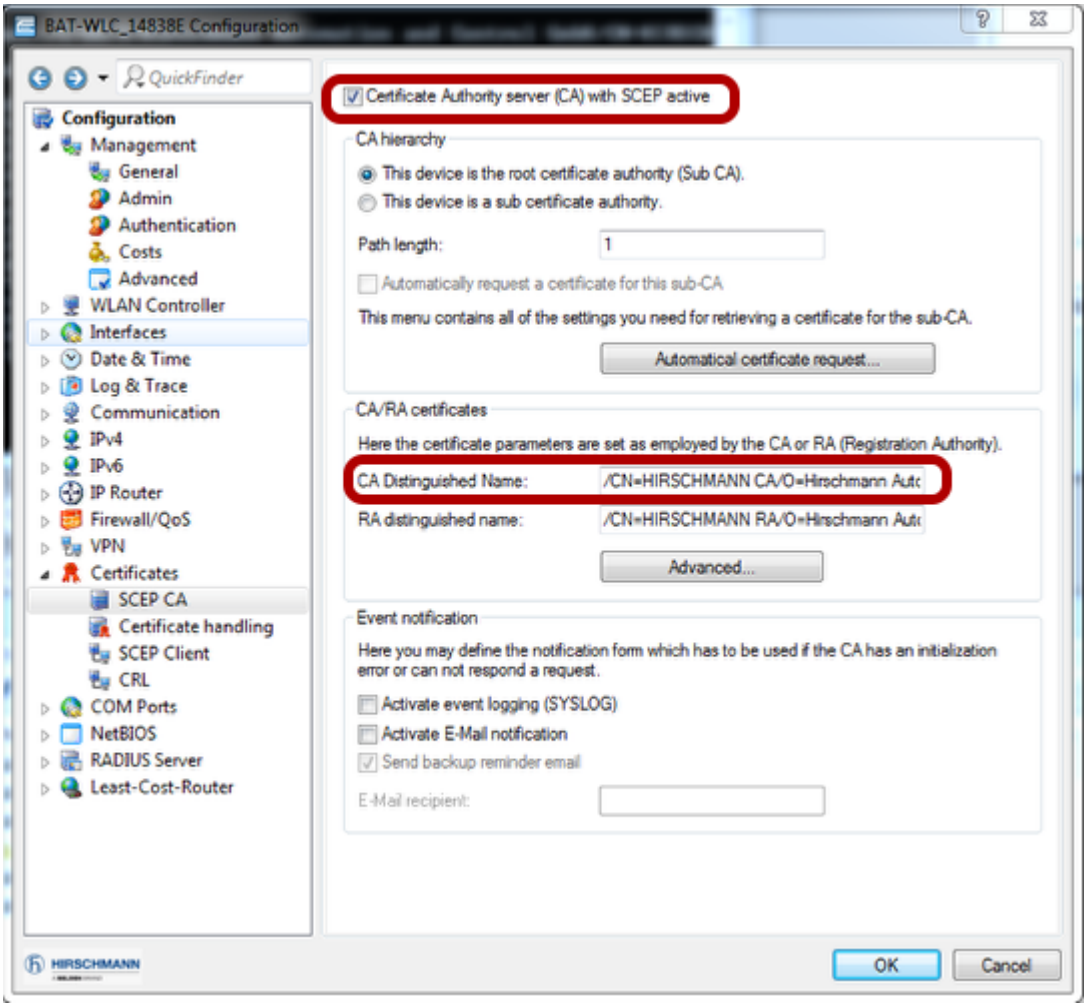
You can refer to the lesson ""How to give an Open BAT or a WLC an IP address""

Add the BAT in LANconfig

You can refer to the lesson ""How to discover a BAT or a WLC in LANconfig""

Make sure that the BAT AC can reach the WLC

Configuration of the WLC (1)



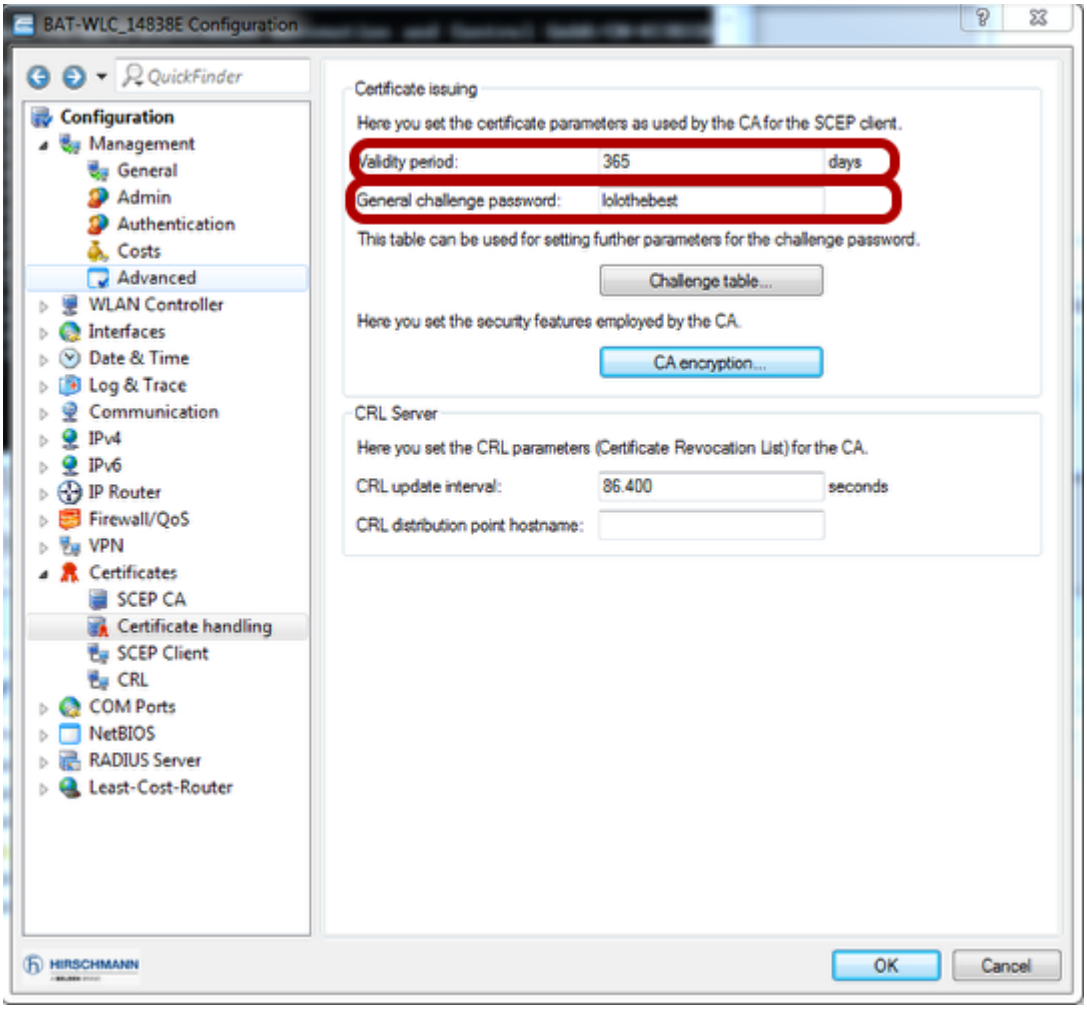
From LAN Config

Configuration > Certificates > SCEP CA

Activate the ""Certificate Authority server (CA) with SCEP active"".

Note the CA Distinguished Name, you'll need it for the BAT configuration (In our case: /CN=HIRSCHMANN CA/O=Hirschmann Automation and Control GmbH/C=DE)

Configuration of the WLC (2)



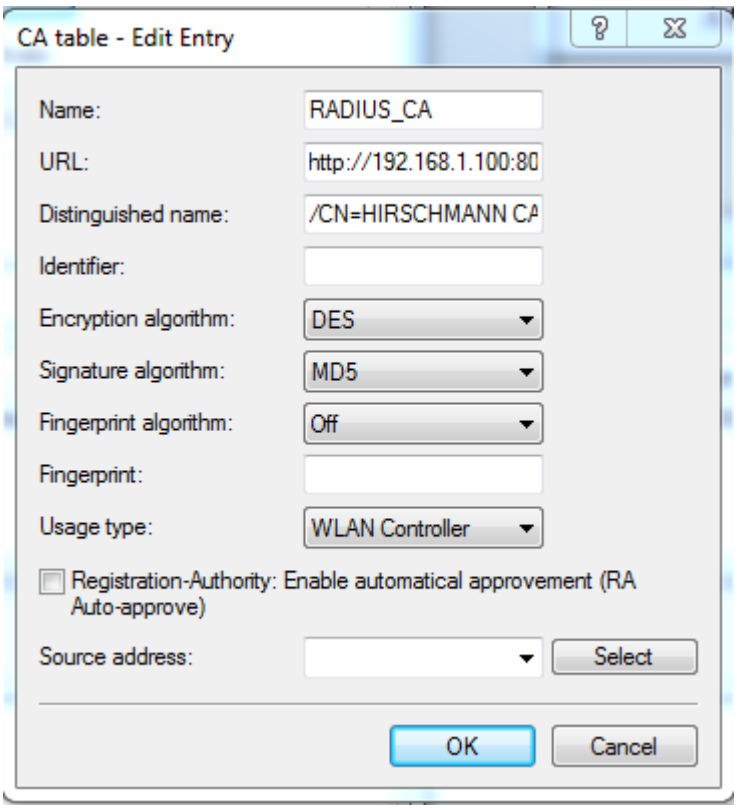
Configuration > Certificates > Certificate handling

Indicate a validity period for the certificates to issue.

Set a challenge password for the SCEP clients (in our example we set a general one but specific ones for each client can be set in the challenge table)

If a password is already existing, don't modify it. It means that this challenge is already used by other SCEP clients.

Configuration of the BAT (1)



From LAN Config

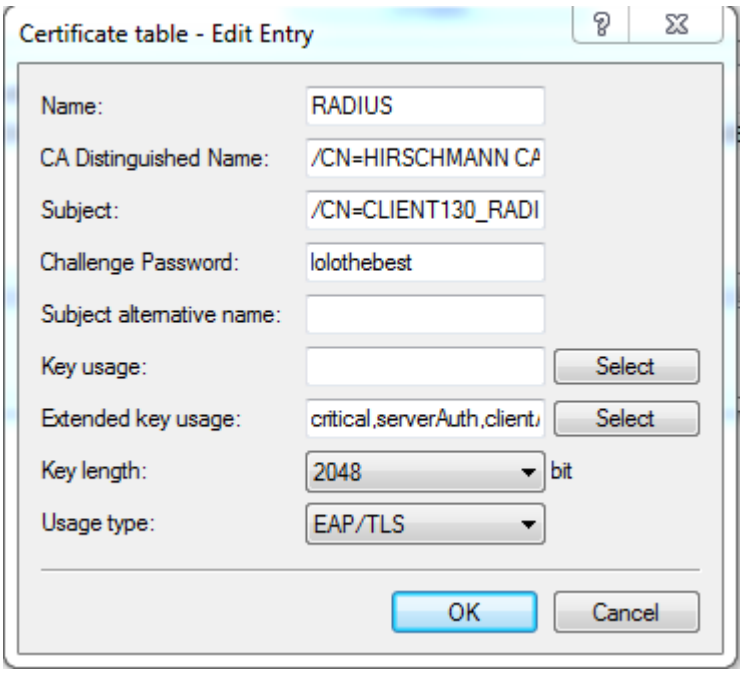
Configuration > Certificates > SCEP Client > CA table > Add

Create an entry as shown above with the following settings:

URL: http://192.168.1.100:80/cgi-bin/pkiclient.exe

Distinguished name: /CN=HIRSCHMANN CA/O=Hirschmann Automation and Control GmbH/C=DE

Configuration of the BAT (2)



Configuration > Certificates > SCEP Client > certificate table > Add

Create an entry as shown above with the following settings:

CA Distinguished name: /CN=HIRSCHMANN CA/O=Hirschmann Automation and Control GmbH/C=DE

Subject: /CN=CLIENT130_RADIUS/O=Hirschmann Automation and Control GmbH/C=DE

Give the same challenge password as the one configured on the WLC (in our examople: lolothebest)

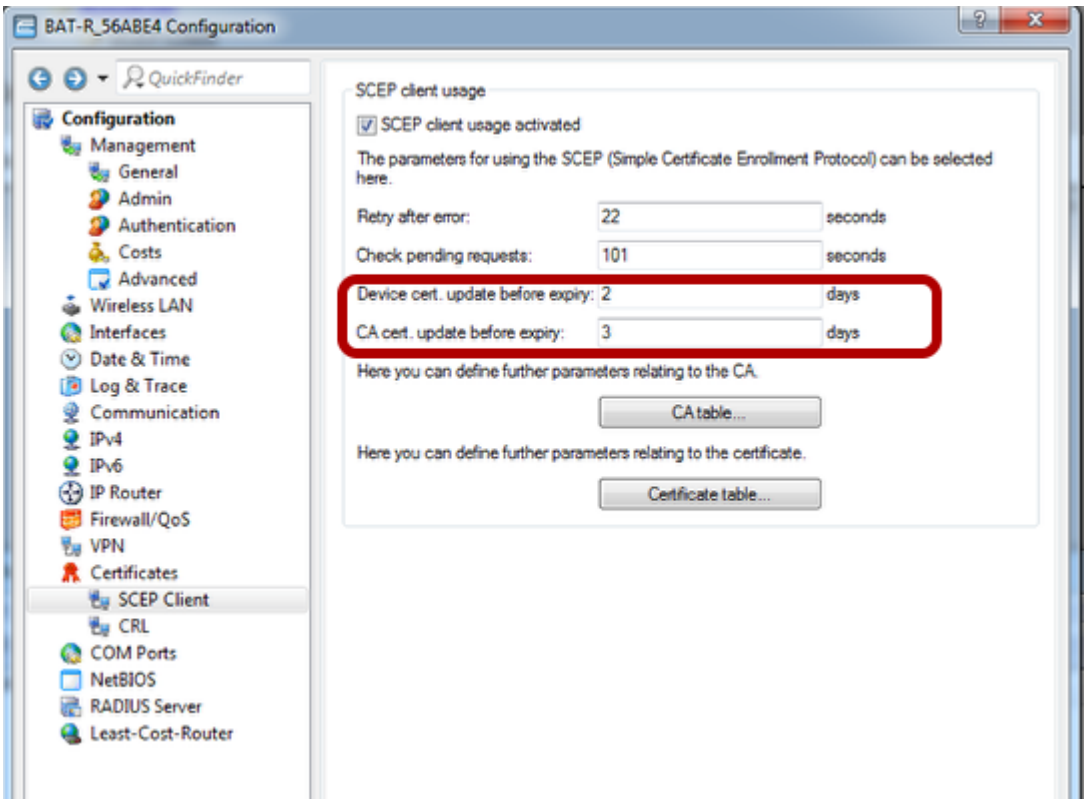
For the key usage select: critical,serverAuth,clientAuth

Key lenght: 2048 bit

Usage type. EAP/TLS

> OK

Configuration of the BAT (3)



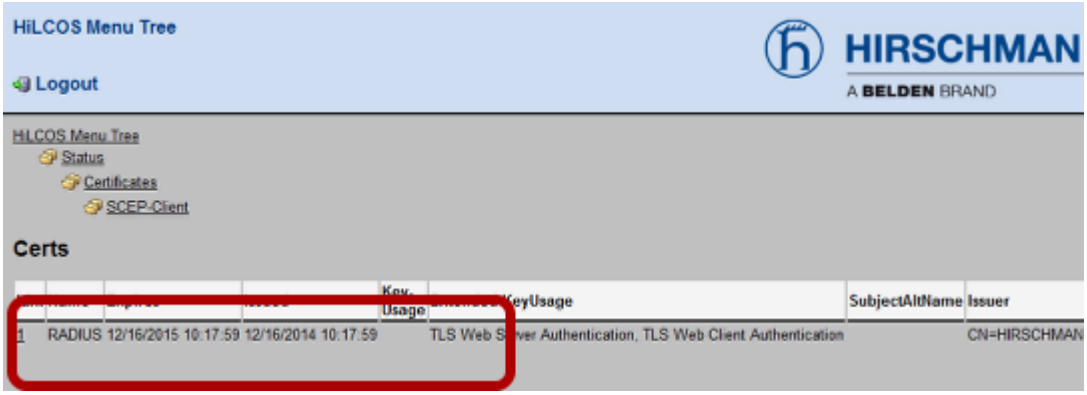
Configuration > Certificates > SCEP Client

Define when the certificate must be updated before its expiration.

> OK

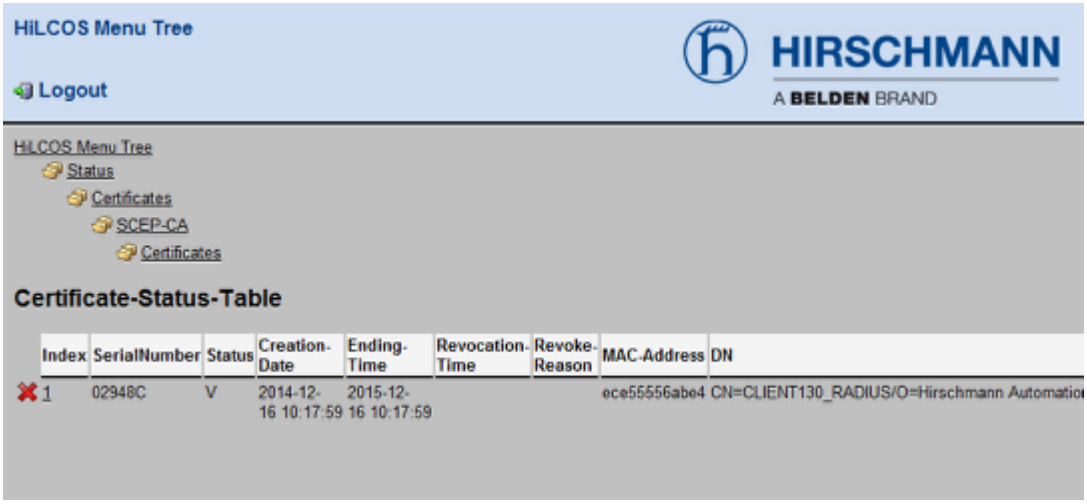
When the configuration is applied on the client the the certificate request and issuing and exchange are automatically done through the network

Checking on the BAT



You can check in the web interface that the client got its certificate

Checking on the WLC



You can check in the web interface that the WLC issued the certificate.

The BAT has now a certificate which can be used for a 802.1x EAP/TLS authentication on the WLC configured as radius server.