How to create a WLC cluster

[19.11.2015]

This lesson describes step by step how to create a WLC cluster.

In our example we create a cluster with 2 controllers (WLCs) located in the same LAN.
WLC_MAIN with IP address 192.168.1.10/24
WLC_BACKUP with IP address 192.168.1.100/24

The lessons also details the additional parameter to configure if the controllers were in 2 different LANs

LANConfig is used for the controller configuration

Introduction

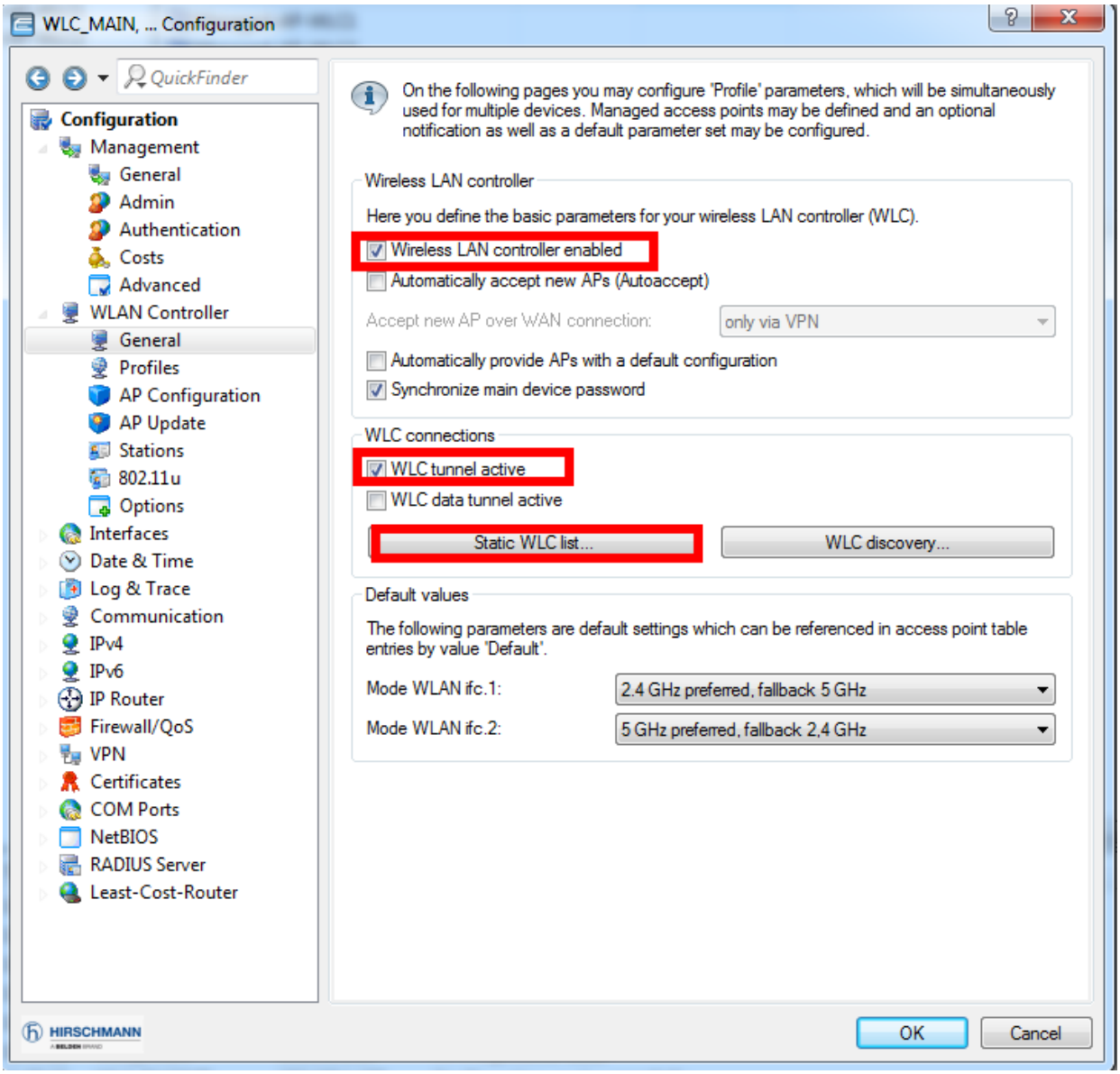
In order to operate multiple WLAN controllers in a WLC cluster, they must all have identical configurations. This also includes the certificates used within the WLC cluster. The solution lies in establishing a certificate hierarchy, also known as a CAhierarchy: This involves defining the CA of a WLC as the root-CA. The other WLCs retrieve this certificate for their (sub-) CA.

This how-to shows you the configuration steps which are necessary for setting up a CAhierarchy. As examples, the configuration is done using two WLCs:
WLC_MAIN (192.168.1.10) represents the device with the root-CA;
WLC_BACKUP (192.168.1.100) is the device which obtains a certificate from the root-CAin order to issue further certificates as a sub-CA.

Preliminary step

Give the controllers an IP address
    -> Refer to the lesson "How to give an Open BAT or a WLC an IP address ?" if necessary
- Discover the WLCs in LANconfig
    --> Refer to the howto: "How to add a BAT or a WLC in LANconfig" if necessary
- Set the time on the WLCs
    --> Refer to the howtos "How to set the date and time on an Open BAT or a WLC" if necessary

Enable the clustering on the WLCs

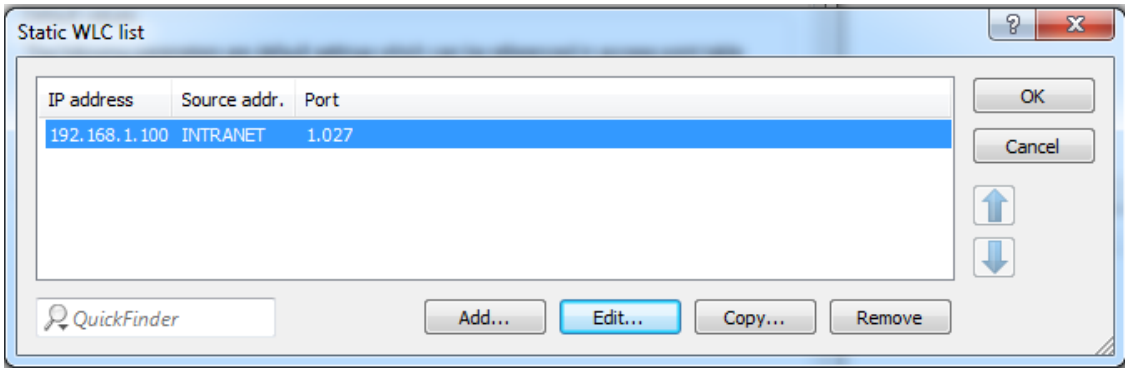


Via LANConfig:
Configuration > WLAN Controller > General
- Check the box "Wireless LAN controller enabled"
- Check the box "WLC" tunnel active

We must now make sure that the WLCs find each other, there are 3 options:
1/ If they are in the same LAN, "WLC discovery" can be used.
2/ If they are in different LANs, Check additionnally "WLC data tunnel active" and enter them statically in "Static WLC list..."
3/ If they are in the same LAN but you prefer to enter them statically, let the box "WLC data tunnel active" unchecked and enter them statically in "Static WLC list..."

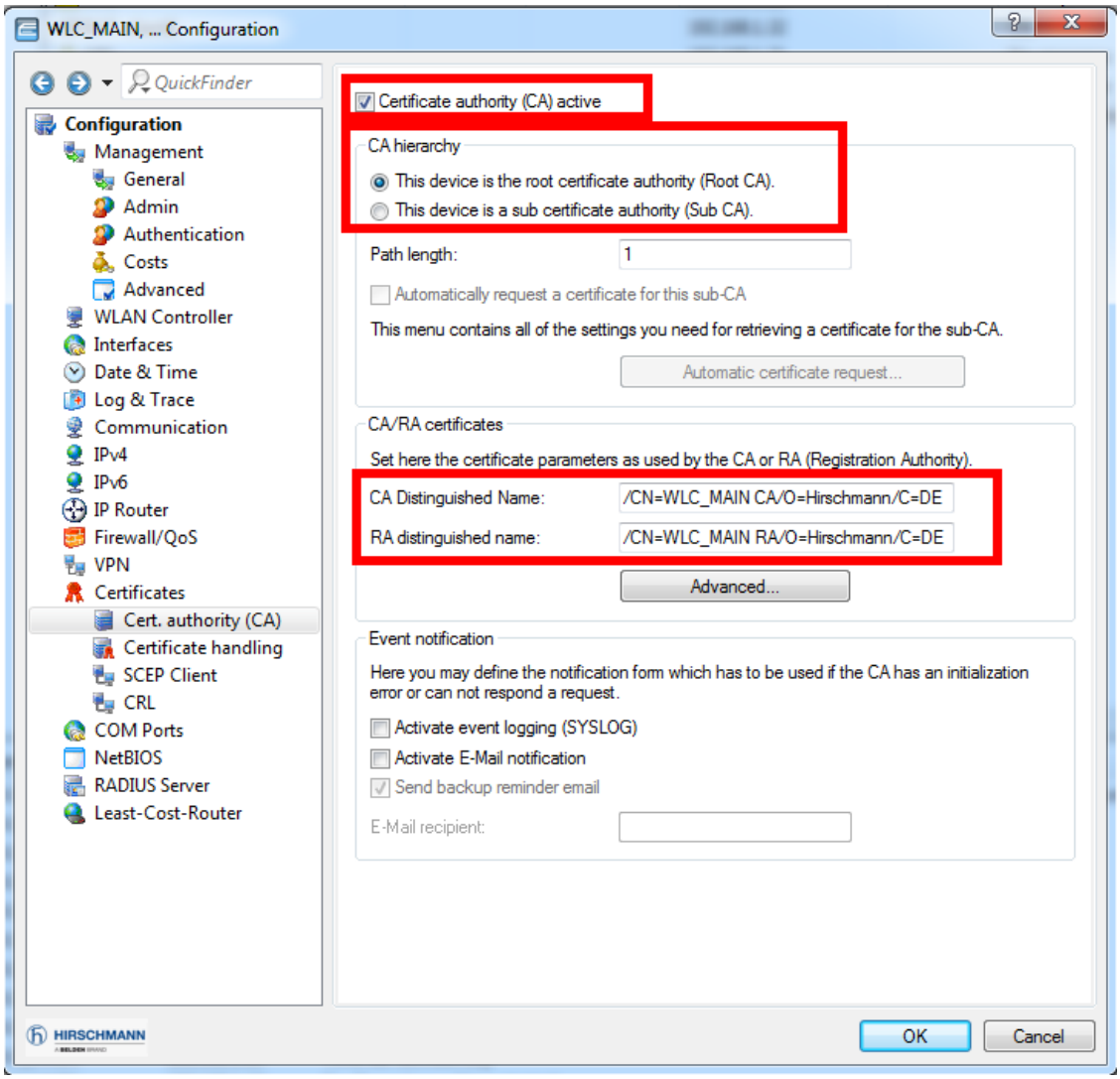
In our example they are in the same LAN but we prefer to enter them statically (Option 3) we select then "Static WLC list..."

Enter the "other" WLC address in the static WLC list



On WLC_MAIN, enter the IP address of WLC_BACKUP: 192.168.1.100
On the WLC_BACKUP enter the IP address of WLC_MAIN: 192.168.1.10
The port in use per default is 1027

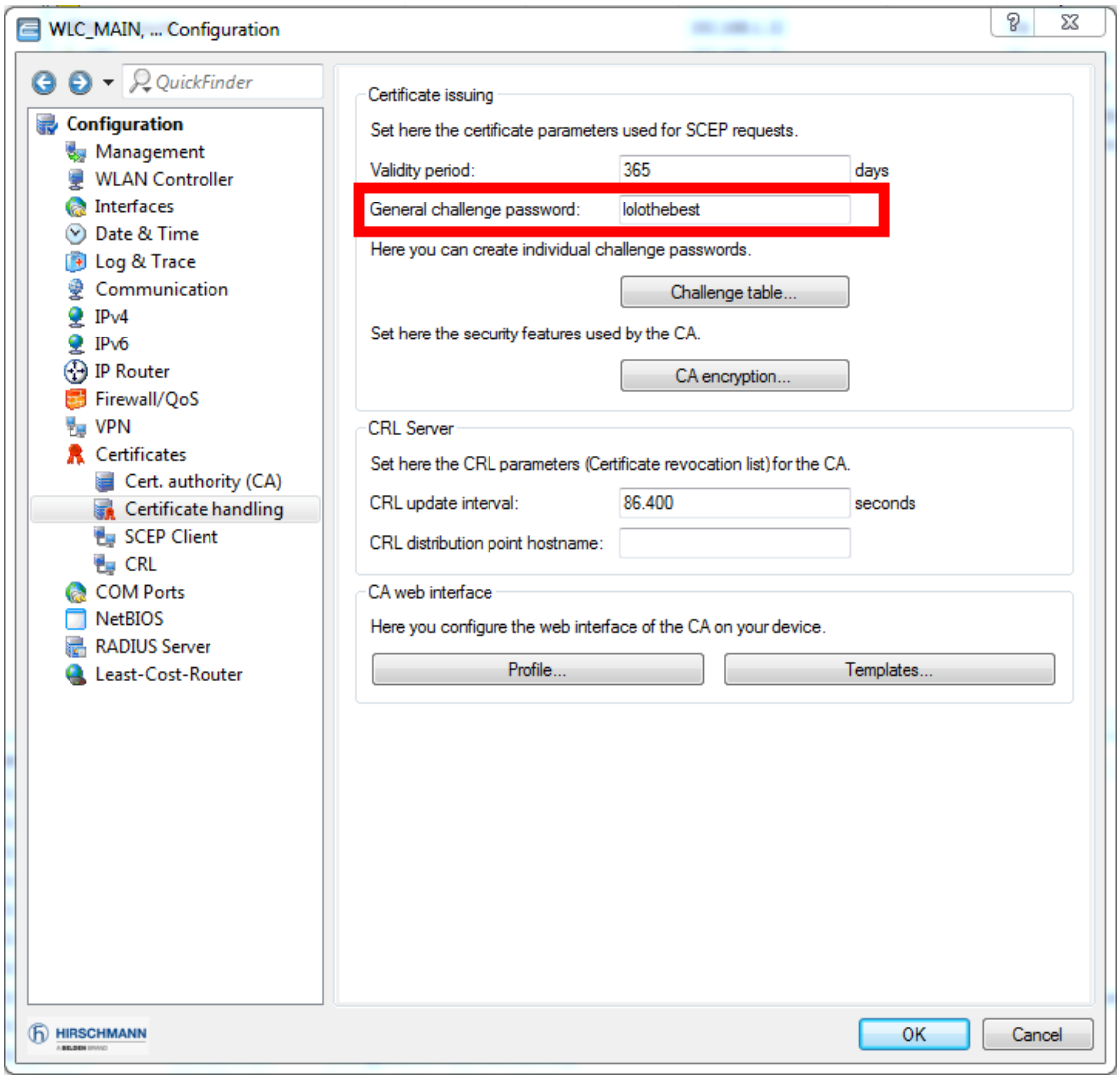
Configure WLC_MAIN as Root CA



Configuration > Certificates > Cert. authority (CA)
- Check the box "Certificates authority (CA) active
- In the CA hierarchiy menu, select "This device is the root certificate authority (Root CA).
- In the menu CA/RA certificates, customize the name of the certificate authority (CA) and the registration authority (RA)

In our example for the CA: /CN=WLC_MAIN CA/O=Hirschmann/C=DE
For the RA: /CN=WLC_MAIN RA/O=Hirschmann/C=DE

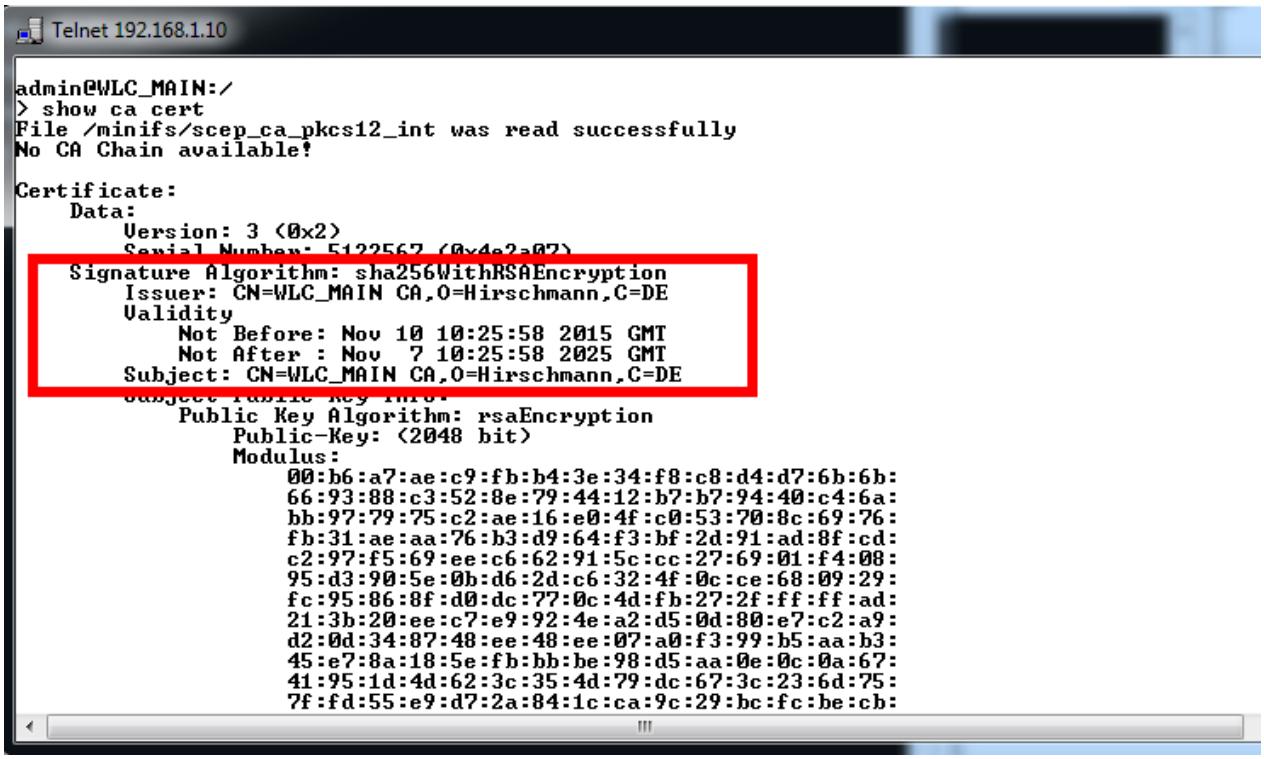
Set a challenge password on WLC_MAIN



Configuration > Certificates > Certificate handling
Set a General challenge password (in our example: lolothebest")

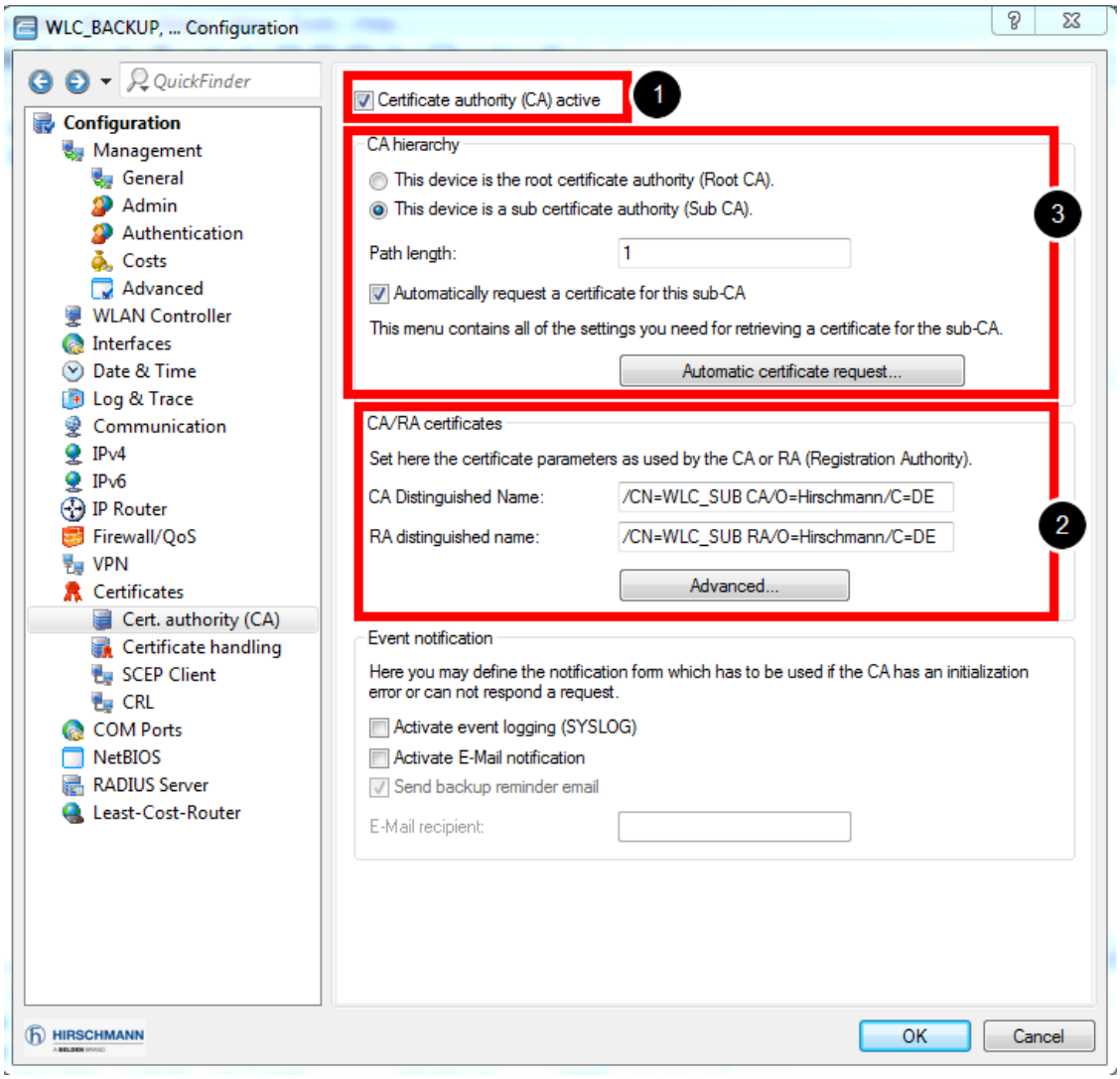
This password is used when certificates must be issued via SCEP (Simple Certificate Enrollment Protocol) which is the case when configuring 2 controllers in a cluster.

Verify that WLC_MAIN has created the certificate correctly



Per Telnet it's possible to check that the certificate was created successfully.
Connect per telnet and type the command: show ca cert

Configure WLC_BACKUP as Sub CA



Configuration > Certificates > Cert. authority (CA)

1/ Check the box "Certificates authority (CA) active

2/ In the menu CA/RA certificates, customize the name of the certificate authority (CA) and the registration authority (RA)

In our example for the CA: /CN=WLC_SUB CA/O=Hirschmann/C=DE

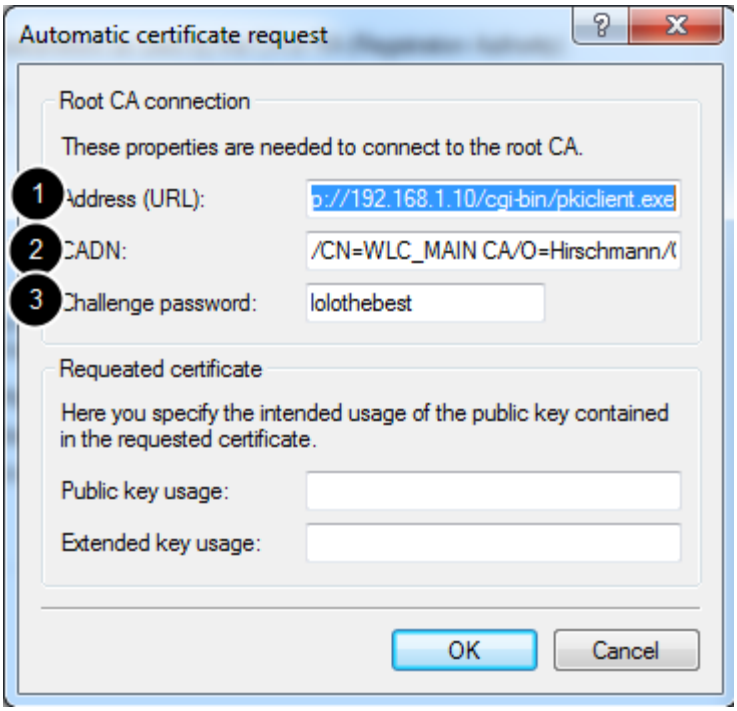
For the RA: /CN=WLC_SUB RA/O=Hirschmann/C=DE

3/ In the CA hierarchiy menu, select "This device is a sub certificate authority (Sub CA).

Check the box "Automatically request a certificate for this sub-CA

Go in the menu "Automatic certificate request..."

Enter the settings to retrieve certificates on the Root CA



1/ As Address, enter: http://[IP address of the Root CA]/cgi-bin/pkiclient.exe
in our exmaple: http://192.168.1.10/cgi-bin/pkiclient.exe

2/ As CADN, enter the name of the CA (as configure on WLC_MAIN at the step "Configure WLC_MAIN as Root CA")
in our example: /CN=WLC_MAIN CA/O=Hirschmann/C=DE

3/ Enter the password configured previously on the WLC_MAIN at the step "Set a challenge password on WLC_MAIN"

Apply the settings

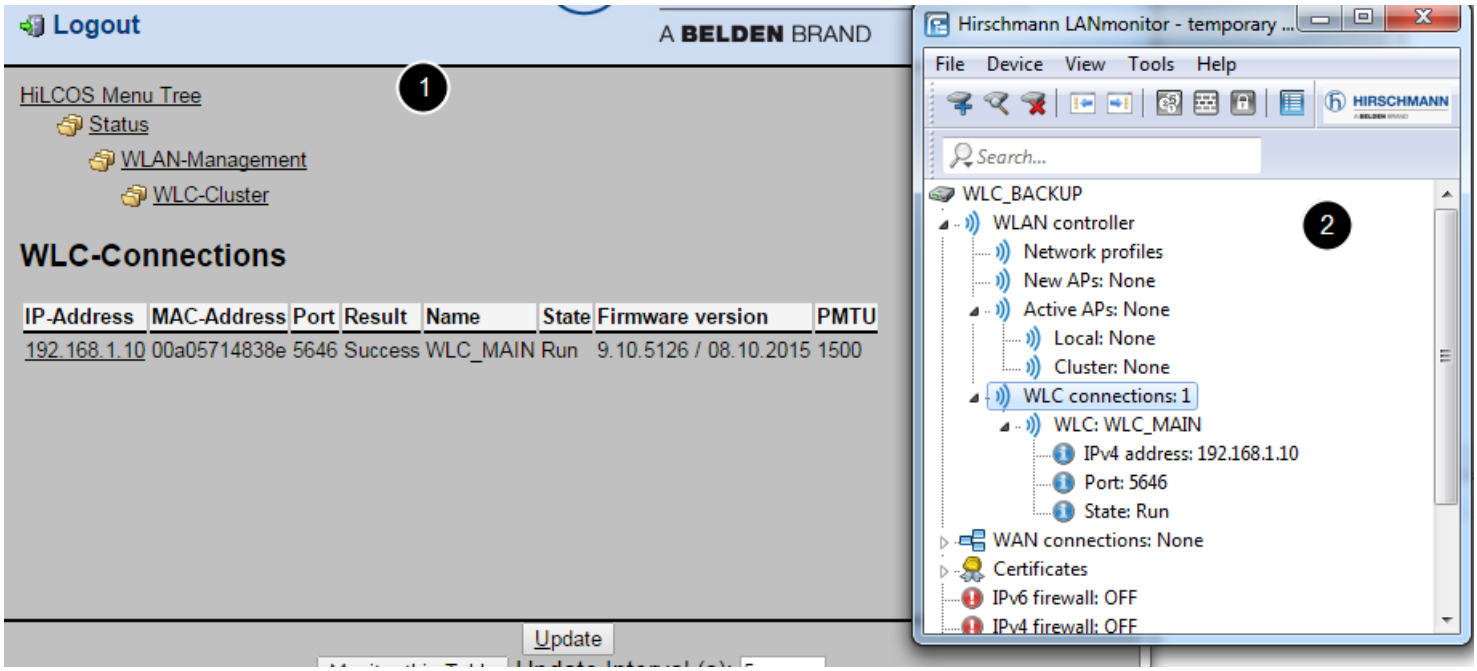
Verify that WLC_BACKUP has retrieved the certificate correctly from the Root CA

```
admin@WLC_BACKUP:/
> show ca cert
File /minifs/scep_ca_pkcs12_int was read successfully
Stack consists of 2 certificates, showing only CA certificates

Certificate 1:

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 5122567 (0x4e2a07)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN=WLC_MAIN CA,O=Hirschmann,C=DE
        Validity
            Not Before: Nov 10 10:25:58 2015 GMT
            Not After : Nov  7 10:25:58 2025 GMT
        Subject: CN=WLC_MAIN CA,O=Hirschmann,C=DE
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b6:a7:ae:c9:fb:b4:3e:34:f8:c8:d4:d7:6b:6b:
                    66:93:88:c3:52:8e:79:44:12:b7:b7:94:40:c4:6a:
                    bb:97:79:75:c2:ae:16:e0:4f:c0:53:70:8c:69:76:
                                    .
                                    .
                                    .
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 5122571 (0x4e2a0b)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN=WLC_MAIN CA,O=Hirschmann,C=DE
        Validity
            Not Before: Nov 10 10:51:02 2015 GMT
            Not After : Nov  7 10:25:58 2025 GMT
        Subject: CN=WLC_SUB CA,O=Hirschmann,C=DE
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:bf:c1:90:c0:fb:a2:c0:e6:07:9a:70:bd:14:b7:
                    62:ee:94:7f:1d:de:df:68:88:c4:be:56:5e:91:5e:
                    5f:e9:d1:d6:d9:65:38:e3:17:90:f1:5f:70:fd:d2:
```

Open a Telnet session on WLC_BACKUP and type de command: show ca cert

2 certificates will be displayed. The first one is the certificate of the root CAthe second one is the certificate of the sub-CA.

Verify that the cluster is active



Check that the controllers recognise the other members of the cluster
1/ Via the Web interface under:
HiLCOS Menu Tree > Status > WLAN Management > WLC-Cluster > WLC-Connections

2/ Or via LanMonitor under
WLAN Controller > WLC connections