

## How to use an Open BAT or WLC as a RADIUS server and set up user accounts

- 2022-01-10 - BAT, WLC (HiLCOS)

This lesson describes how to configure the RADIUS Server function on an Open BAT or a WLC and set up user accounts.

You may need to refer to the following lessons for a complete working 802.1x environment (Supplicant - Authenticator - Server):

Environment without controller:

- [How to configure an Open BAT as 802.1x supplicant](#)
- [How to configure an Open BAT as 802.1x authenticator](#)

Environment with controller to manage the APs:

- [How to configure an Open BAT as 802.1x supplicant](#)
- How to create a profile on a WLC and apply it on BAT Acces points
- [How to configure a Radius Profile on the WLC and include it in Logical settings](#)

These How to are complementary and use the following settings for the radius authentication:

EAP - PEAP with MSCHAPv2 as tunnel method.

### **Representation**



A WLC or an Open BAT can be used as RADIUS Server.

The menus on both are identical but using a BAT the manual upload of a certificate is necessary (step described in this document).

### **Preliminary steps**

Give the BAT an IP address (in our example: 192.168.1.150)

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"

### **Upload a certificate on the server (if you use a BAT as RADIUS server)**







This step is not necessary if you use a controller as RADIUS Server because the controller is able to generate its own certificates.

But, if you use a BAT then you have to do it manually. You'll need a certificate (.pfx or .p12 files, these files contain a private key and its associated certificate).

You can use for testing the attached file

SSL\_certificates

(password for the certificates: hirschmann)

Then from LAN config, right clic on the BAT which has to be used as RADIUS server.

Configuration Management > Upload certificate or File ...

Select the .pfx or .p12 file you want to use and Select "EAP/TLS - Container as PKCS#12 file" as certificate type (it's usually protected by a password)

> Open

The file is uploaded on the BAT

Device status must be "OK" after the upload

## General settings



Configuration > RADIUS Server > General

Configure the authentication port: 1812

**Configure the RADIUS clients list (Authenticators IP address and shared secret)**



From the "General" dialog, select IPv4 clients

Create a new entry.

The new entry can be a single device (in our example it's only the device 192.168.1.140) but it could be a range of devices (the range is defined by the Netmask)

The shared secret will also be configured on the authenticator ( refer to the lesson "How to configure an Open BAT as 802.1x authenticator")

> OK

## Set up User accounts

From the "General" dialog, select "User table"

Create a new entry for each user.

In our case we use just one user: laurent

To enter the name of the user and a password (in our case: lolothebest) is enough

The name and the password will be used by the supplicant ( refer to the lesson "How to configure an Open BAT as 802.1x supplicant")

> OK

After loading the configuration, your device is ready to be used as RADIUS server

### **Check the status of the NAS (Network Access Server or Authenticator)**



HiLCOS Menu Tree 

**HiLCOS**  
 A BEL

[Logout](#)

HiLCOS Menu Tree

- 📁 Status
  - 📁 TCP-IP
    - 📁 RADIUS-Server
      - 📁 Access-Control

**Clients**

IP-Address	Last-Request	Last-Status-Request	NAS-Ident	Access-Requests	Status-Requests	Duplicate-Requests	Access-Accepts	Access-Rejects	Access-Challenges
127.0.0.1	5068	0	BAT-R_56AC14_4	0	0	0	2	0	2
192.168.1.140	5068	0	AP2_GROUP1	12	0	0	1	1	10

You can check it via the web interface

HiLCOS Menu Tree > Status > TCP-IP > RADIUS-Server > Access-Control

**Check the authentication of clients**



## HiLCOS Menu Tree

- [Status](#)
- [TCP-IP](#)
- [RADIUS-Server](#)

**Log-Table**

Index	Time	Event
<a href="#">18</a>	12/08/2014 12:01:07	sent RADIUS accept for user id 'support' to 192.168.1.140
<a href="#">17</a>	12/08/2014 12:01:07	sent RADIUS challenge for user id 'support' to 192.168.1.140

You can see the result of the authentication tries in the Log-Table available via the Web interface under

HiLCOS Menu Tree > Status > TCP-IP > RADIUS-Server > Log-Table.

More information can be available if if we use RADIUS Accounting (not described in this How-to).

## Conteúdo Relacionado

- [How to configure an Open BAT as an 802.1x supplicant](#)
- [How to configure an Open BAT as an 802.1x authenticator](#)
- [How to configure a Radius Profile on the WLC and include it in Logical settings](#)