

Base de Conhecimento > Products > BAT > BAT, WLC (HiLCOS) > How to use an Open BAT or WLC as a RADIUS server and set up user accounts

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

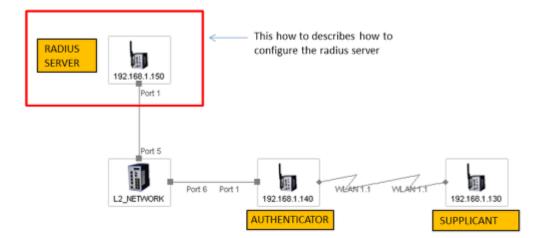
Environment with controller to manage the APs:

- 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).

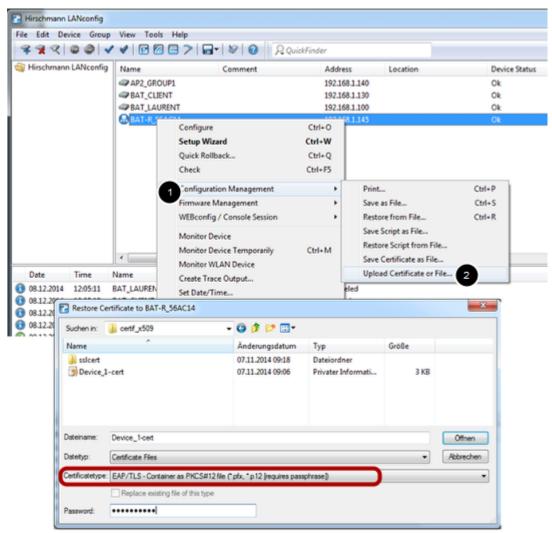
Preliminary steps

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

BAT-RADIUS_SRV Configuration		-	<u>ଥାଲେ</u> 🕺		
G 🕘 🗸 🔍 QuickFinder	RADIUS service				
Configuration	Authentication port:	1.812			
Seneral	Accounting port:	0			
Admin Authentication	Accounting interim interval:	0	seconds		
💑 Costs	RADSEC service				
Advanced Wireless LAN	RADSEC port:	0			
Q Interfaces O Date & Time Date & Time D G & Trace Q Communication	RADIUS/RADSEC clients The data of the clients which shall be communicate with the server can be entered at the following tables.				
⊳ 👤 IPv4	IPv4 clients		IPv6 clients		
 IPv6 IP Router IF rewall/QoS 	Please keep in mind that a suitable inbound filter rule has to be created within the IPv6 firewall to grant RADIUS server access for IPv6 clients!				
VPN	User database				
R Certificates @ COM Ports Transformed Ports NetBIOS	The data of the users which shall be authenticated by the server can be entered at the following table.				
RADIUS Server General					
 General Forwarding EAP Options 	The server will check authentic		-		

Configuration > RADIUS Server > General

Configure the authentication port: 1812

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

IP address Netmask	Protocols			ОК
192.168.1.140 255.255.255				Cancel
< Q QuickFinder G EAP G Options Least-Cost-Router	V Use the	C	192.168.1.140 255.255.255.255 RADIUS support Generate password	Show
			ОК	Cancel

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")

> 0K

Set up User accounts

Entry active			Passphrase (optional):		Show
Name / MAC address:	laurent			Generate password]
Case sensitive usemame	e check		TX bandwidth limit:	0	kbit/s
Password:	Iolothebest V Sho	v	RX bandwidth limit:	0	kbit/s
	Generate password		Station mask		
VLAN ID:	0		Calling station:		
Comment:		*	Called station:		1
			Validity/Expiry		
Service type:			Expiry type:	Relative & absolute -]
Service type.	Any 🔻		Relative expiry:	0	seconds
Protocol restriction for aut	hentication		Absolute expiry:	00:	00:00
V PAP	CHAP		Multiple login		
V MSCHAP EAP	MSCHAPv2		Max. concurrent logins:	0	•
If here are made no restrictions, all authentication protocols will be allowed automatically!		Time budget:	0	seconds	
		Volume budget:	0	byte	
Shell privilege level:	0				

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")

> 0K

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

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

HiLCOS Me	nu Tree						(6	н
Logout								IJ	ABE
IP-Address	Last-Request	Last-Status- Request	NAS-Ident	Access- Requests	Status- Requests	Duplicate- Requests			
	5068	0	BAT-R 56AC14	4	0	0	2	0	2
127 0 0 1	2000								-

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	(h) HIRSCHMANN
Logout	A BELDEN BRAND
HiLCOS Menu Tree Status TCP-IP RADIUS-Serv Log-Table	<u>er</u>
Index Time	Event
18 12/08/2014 12:01:07	sent RADIUS accept for user id 'support to 192.168.1.140
12/08/2014 12:01:07	sent RADIUS challenge for user id 'support' to 192.168.1.140
You can see the result of th	e 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