

Knowledgebase > Products > BAT > BAT, WLC (HiLCOS) > How to configure an Open BAT as an 802.1x authenticator

How to configure an Open BAT as an 802.1x authenticator - 2022-01-10 - BAT, WLC (HiLCOS)

This lesson describes how to configure an Open BAT as 802.1x authenticator. You may need to refer to the following lessons for a complete working 802.1x environment (Supplicant - Authenticator - Server):

- How to configure an Open BAT as 802.1x supplicant

- How to use an Open BAT or a Controller as RADIUS Server and set up User accounts

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

EAP - PEAP with MSCHAPv2 as tunnel method.

Representation

× Preliminary steps

Give the BAT an IP address (in our example: 192.168.1.140) 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""

Configure the BAT as an Access Point

You can refer to the lesson ""How to configure an Open BAT as Access Point"" but only



×

Configuration > Wireless LAN > 802.1X > RADIUS servers > Add

Give an name to identify the server (this name is only used locally on the Authenticator) Indicate the IP address of the server (in our example: 192.168.1.150)

Indicate the server port and the shared secret. They will have to match with the ones

configured on the RADIUS server



×

Configuration > Wireless LAN > 802.11i/WEP > WPA or Private WEP settings Select the relevant network (in our case Wireless LAN 1 - Network 1) and Edit In the new dialog make sure that the encryption is activated. Select as Method: 802.11i (WPA)-802.1x

In the passphrase field, enter the name of the RADIUS server (the one configured in the precedent step)

> 0K

This Access Point is now ready to be used as authenticator or NAS (Network Access Server)

 How to use a 	<u>n Open BAT or WLC as a RADIUS :</u>	server	<u>and set up us</u>	<u>ser accoun</u>	<u>ts</u>
BAT_AUTH Configuration		6.84	×		
G O • R QuickFinder	802.11 (WPA/AES) / Wred Equivalent Privacy		WPA or Private WEP settings - Edit Entry		
Configuration	onfiguration You should select 802.11 Enhanced Security with Advanced Encryption Standard (WPA/AES) or at least Wired Equivalent Privacy (WEP) to ensure that all information be transmitted in encrypted form.		Interface: Wreless LAN 1 - Network 1		
a 🍓 Management			C Encryption activated		
Admin	Here, you can program encryption settings for earth insical wireless LAN network (MultiSSID				_
🕹 Costs 2 WP		EP settings	Method / Key 1 length:	802.11i (WPA)-802.1	•
Advanced	Here, you can specify the WEP group keys 2 to 4, that are commonly used	2 to 4, that are commonly used by the logical		SERVER_150	Show
2 General	General			Generate password	
Band Steering A Security	HEP Group	neya	WPA version:	WPA2	-
Stations	Stations Edended settings		WPA1 session key type:	ТКІР	-
802.11/WEP	the station table or via 802.1x, you can select here the group key used for the disease.	WPA2 session key type:	ALS	× .	
🕹 WLC	Vi AN error lan	manelies	WPA rekeying cycle:	0	seconds
AutoWDS	TOT YOUR ANY		WPA2 key management.	Standard	-
PA or Private WEP settings		(D)	Users EAP method.	165	•
Interface Encryption	Method / Key 1 WPA version WPA1 key type WPA2 key type Rekey, cycle	A OK	Pre-authentication		
Wreless LAN 1 - Network 1 Activated Wreless LAN 2 - Network 1 Activated	802.119 (WPA) PSK WPA2 T32P AES Disconds 802.119 (WPA) PSK WPA2 TX2P AES Disconds	E Cance	OKC (Opportunistic Key	y Caching) activated	
Wireless LAN 1 - Network 2 Activated	802.11 (MPA)-P5K 10PA2 TKIP AES 0 seconds		Authentication:	Open system (recom	*
Wreless LAN 1 - Network 3 Activated Wreless LAN 1 - Network 4 Activated	802.13 (WPA) PSK WPAZ TKIP AES 0 seconds 802.13 (WPA) PSK WPAZ TKIP AES 0 seconds		Default key:	Key 1	¥
Wreless LAN 1 - Network 5 Activated Wreless LAN 1 - Network 6 Activated	802.13 (VPA) PSK UPA2 TKP AE5 0 seconds 802.13 (VPA) PSK UPA2 TKP AE5 0 seconds	-	Encrypt mgmt. frames:	No	•
* [
R QuickFinder	3 146			OK	Cancel
			U		

Related Content