

知识库 > Products > BAT > BAT, WLC (HiLCOS) > How to set up 802.1x with EAP-TLS between Open BAT (as AP and Radius server) and Windows 7 client

How to set up 802.1x with EAP-TLS between Open BAT (as AP and Radius server) and Windows 7 client

- 2023-11-17 - BAT, WLC (HiLCOS)

This lesson describes how an OpenBAT can be configured as AP using its own radius server and providing an EAP-TLS connection for a Windows 7 client and how to create certificates for this use with XCA.



×

This is the network which will be configured in this Howto.

This configuration and this topology is an example only. It can be modified according to customers needs.-

Configure OpenBAT

HiDiscovery							
Datei Bearbeiten Optio	nen ?	a 🔊	•			_	
Signal Eigenschaften V	WWW Telnet Pi	ng Neu-Scan Eins	tellungen	168.10.4: ASIX AX887	728 US82.0 to Fast Ethern	•	
Id MAC-Adresse	Schreibbar	IP-Adresse A	Netzmaske	Default Gateway	Produkt		Name
6 EC:E5:55:D0:73:20	V.		0.0.0.0		BAT-F		BAT-F_D07320
7 EC:E5:55:42:F3:00	\checkmark	192.168.10.11	255.255.255.0	0.0.0.0	MAR 1040-4C4C4C4C99995MM	(HRHH	MACH-42F300
5 00:80:63:39:2E:A2		197 168 10 78	255 255 255 0	0.0.0	DS 30-3407T 1T 1SD AFHH	h	RS-392EA2
1 EC:E5:55:1E:64:26	Eigenschafte	en			×		RSP-ECE5551E6426
4 EC:E5:55:01:4B:C0	MAC-Adresse	: EC:E5:55:D0:73	20				RSP-ECE555014BC0
2 EC:74:BA:36:FD:9A	Name:	BAT-F_D07320				8S	RSP-EC74BA36FD9A
8 EC:E5:55:68:1F:27	IP-Konfigura	tion					RSB-6B1F27
3 EC:E5:55:A4:B6:00	IP-Adresse:	192 .	168 . 10	. 63 Defau	lt setzen (192.168.10.23)		MSP-ECE555A4B600
	Netzmaske:	255 .	255 . 255	. Defau	it setzen (255.255.255.0)		
	Default Gate	eway: 0.	0.0	. 0 De	efault setzen (0.0.0.0)		
			Als Voreinste	ellung speichern			
			Ok	Abbrechen			
4			1	n			
×							

Use HiDiscovery to assign a IP-address to the BAT. The PC is locally connected.

🕤 🔹 H2 QuickFinder	General			
Configuration	This is where you can pro	gram common settings for all wire	ess LAN interfaces.	
Management	Country:	Europe	•	
General	TT LOOL			
e deneral	ARP handing			
G Security	indoor only mode activ	aleo		
5 Stations	Email address for WLAN e	events:		
802.11i/WEP	. Interfaces			
🍓 802.1X	There is a			
💩 WLC	This is where you can pro	gram physical and logical (MultiSS	D) wreless LAN settings.	
AutoWDS	Physical WLA	N settings	Logical WLAN settings	
Trace				
B Wireless-IDS	Point-to-Point	Physical WI AN settings - W	AN interface 1	
Date & Time	This is where you can p	- Filysical free of seconds - fi	continuente a	
log & Trace	Common point4	Operation Radio Performance	e Client mode	
Communication		THE WE AN interfaces applied		
Pv4	Extended settings	V LAW Intellace enabled		
2 IPv6	The following physical v	WLAN operation mode:	Access point -	
DIP Router		Broken LAN Ink detection:	None -	
Firewall/QoS		WI AN Interface Lisage:	WI AN	
VPN	Bit rate serial P2P auto-	the of the local charge.	intern .	
Certificates	It May sim Assesses			
COM Ports	M Now sinutarious	Link LED function:	Connection count -	
Public Spot	Block time:	The link-LED function 1	Tient signal strength' only makes sense in "Tier	nt mode' WLAN
RADIUS Server	-WLAN Link Status Loo	operation. It denotes the	e signal strength between this station and the o	connected acces
Least-Cost-Router	Horitical Courter Court	point. Signal strength and thus	the connection quality is indicated by the blin	king frequency. T
	enables you to capture	faster the link LED blink	s the better the connection is.	
	WLAN Link Status I			

Use Access-Point as WLAN operation mode. Optionally you can choose alternative Radio settings etc.

BAT-F_D07320, Configuration				8 8
G ⊙ ▼ ♀ QuickFinder	General This is where you	can ninniam common settings f	or all wireless I AN interfaces	
Say Management Wireless LAN General	Country:		Europe	•
 Band Steering Security Stations 	Email address for	ode activated WLAN events:		
© 802.11i/WEP 802.1X WLC	Interfaces This is where you	can program physical and logic	al (MultiSSID) wireless I AN settions	
AutoWDS Trace Wireless-IDS Trace	Physic Delet to Delet	cal WLAN settings	Logical WLAN settings	
Date & Time Log & Trace	Fransmission Alarms	IN INCENSEE 1 - NELWORK 1	8	
Communication Interface: IPv4 IPv6 Network 0	network enabled	WLAN interface 1 - Network		F
Firewall/QoS Suppress	SSID broadcast:	NO		
Certificates COM Ports Maximum NetBIOS Misimal ali	count of clients:	0	\$y	
Public-Spot	oni agna siongin;	v	4	

Configure the SSID





×

Proceed to menu "Wireless LAN - 802.11i/WEP"

Use button "WPA or Private WEP settings...". A new window will open

Doubleclick on first line

Make sure that "encryption activated" is checked

Choose "802.11i (WPA)-802.1x" as "Method

Leave the passphrase field blank.

QuickFinder Configuration	Interface settings Specify login setting	s for each local area network i	interface.		
Wireless LAN	Interfaces				
Ceneral Control Contr	Authentication via F You can manage th (name is DEFAULT LAN networks to b For each RADIUS a	RADIUS e authentication of the wireless). In addition, you can define yo e entered in place of the passp server listed here, a backup ser	s LAN networks in a central RADIUS server our own RADIUS server for specific wireless phrase of the logical wireless LAN network). rver can be specified. RADIUS servers		
AutoWDS					
RADIUS servers			8 2		
Name Server address Serv	er port Backup server S	ource addr	ОК		
Name Server address Serv	er port Backup server S	RADIUS servers - New I	Cancel		
Name Server address Serv	er port Backup server S	RADIUS servers - New I Name:	Entry		
Name Server address Serv	er port Backup server S Default server	RADIUS servers - New I Name: Server address: Server address:	OK Cancel		
Name Server address Serv	er port Backup server S	RADIUS servers - New I Name: Server addrese: Server port: Secret:	Entry		
Name Server address Serv	er port Backup server S Default server Add	RADIUS servers - New I Name: Server address: Server port: Secret:	OK Cancel		
Name Server address Serv P QuickFinder COM Ports NetBIOS Public-Spot RADIUS Server Least-Cost-Router	Per port Backup server S	RADIUS servers - New I Name: Server address: Server port: Secret: Backup server:	Cancel		
Name Server address Serv	Default server Add	RADIUS servers - New I Name: Server addrese: Server port: Secret: Backup server: (1) The device deter destination networe address should b Source address (red):	CACCE Cancel Entry Provide the correct source IP address for the ork automatically. If a certain source IP address for the ork automatically. If a certain source IP address for the ork automatically. If a certain source IP address for the ork automatically. If a certain source IP address for the ork automatically. If a certain source IP address for the ork automatically. If a certain source IP address for the ork automatically. If a certain source IP address for the ork automatically. If a certain source IP address for the ork automatically. If a certain source IP address for the ork automatically. If a certain source IP address for the ork automatically. If a certain source IP address for the ork automatically or directly.		
Name Server address Serv	Default server Add	RADIUS servers - New I Name: Server address: Server port: Secret: Backup server: I) The device deter destination netwo address should b Source address (opt.):	CACCE		

×

Proceed to menu "Wireless LAN - 802.1X"

Use button "RADIUS servers...". A new window will open.

Use button "Add". A new window will open.

Fill in the fields. Leave the "Secret" field blank



Proceed to menu "RADIUS Server - General"

 QuickFinder Configuration 	Authentication method	of authentication can be cho	osen here.
🍓 Management 🎄 Wireless LAN 🔕 Interfaces	Default method: Tunnel server:	TLS	
 Date & Time Log & Trace Communication IPv4 IPv6 	For EAP/TLS check th	e subject name towards the RA	ADIUS user table
	TTLS default:	MD5	▼
Firewall/QoS	Timeouts	MSCHAPVZ	•
Certificates	Reauth period:	0	seconds
	Retransmit timeout:	0	seconds
RADIUS Server			
EAP			

Proceed to menu "RADIUS Server - EAP" Choose "TLS" as "Default method".



Proceed to menu "IPv4 - DHCPv4"

Use button "DHCP networks...". A new window will open.

Doubleclick on the first line (INTRANET). A new window will open.

Enable DHCL server and configure relevant IP settings.

Now the configuration of the OpenBAT is finished.

Upload Server Certificate to OpenBAT

e Edit Device Group View	Tools Help				
≩ 🧝 ସ 🔍 🔍 🖉 🖉	🖻 🖾 🏷 🗖 🕶 🔍	QuickFinder			
Hirschmann LANconfig Name	Comm	nent Cluster Name	Address	Location	Device State
@ B4	T-F_D07320		192.168.10.63		Ok
	Configure		Ctrl+O		
	Setup Wiza	ard	Ctrl+W		
	Quick Rolls	back	Ctrl+Q		
	Check		Ctrl+F5		
	Configurat	ion Management	•	Print	Ctrl+P
-	Firmware N	Management	•	Save as File	Ctrl+S
	WEBconfig	/ Console Session	,	Restore from File	Ctrl+R
	Monitor De	evice		Save Script as File	
	Monitor De	evice Temporarily	Ctrl+M	Restore Script from File	
	Monitor W	LAN Device		Save Certificate as File	_
	Create Trac	ce Output		Upload Certificate or File	
	Set Date/Ti	ime			
	Activate So	oftware Option			
1	Activate Co	onfiguration Synchronization Settings			
	Add to Win	ulara albanas Canasa			

Rightclick on the OpenBAT within LANconfig

Use menu "Configuration Management - Upload Certificate or File...". A new window will open.

🚰 Restore	Certificate to BAT-F_D07320			×
Suchen in:	🧮 Desktop	- G 🕽	š 📂 🛄 🔻	
	Dateiordner			•
	client.txt Textdokument 2,51 KB	N		
5	HirschmannBAT.p12 Privater Informationsaustau 3,49 KB	4		
5	HirschmannClient.p12 Privater Informationsaustau 3,36 KB			
للمعمعا	issues by			Ŧ
Dateiname:	HirschmannBAT.p12		Öffner	
Dateityp:	Certificate Files	•	Abbrech	en
Certificate	EAP/TLS - Container as PKCS	#12 file (*.pfx, *.p1	2 [requires pas	× –
Cert. passwo	Replace existing file of this ty	/pe		

×

Choose the relevant file Choose "EAP/TLS - Container as PKCS#12 file" Enter the password

The certificate will be uploaded.



With the command "show eap" you can check that the certificate was uploaded properly.

Client side: Install the certificates



Doubleclick on the Client certificate. A new window will open. Click on "Next"



The wizard will show the path of the certificate. Use button "Next".

Certificate Import Wizard	×
Password To maintain security, the private key was protected with a password.	
Type the password for the private key.	
Password:	
Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.	
Mark this key as exportable. This will allow you to back up or transport your keys at a later time.	
☑ Include all extended properties.	
Learn more about protecting private keys	
< Back Next > Cance	!

Enter the password of the certificate and click on "Next".

Certificate Import Wizard				
Certificate Store Certificate stores are system areas where certificates are kept.				
Windows can automatically select a certificate store, or you can specify a location for the certificate.				
Output Automatically select the certificate store based on the type of certificate				
Place all certificates in the following store				
Certificate store: Browse				
Learn more about <u>certificate stores</u>				
< Back Next > Cancel				

Stay with default settings. The place to store the certificate will be selected automatically. Click on "Next".



Click on "Finish".



1

Confirm to install the certificate.

Configure the wireless network

~~~				
🔾 🖓 🦉 👯 « All Control Panel )	Items   Network and Sharing Center	•	Search Control Panel	Q
Control Panel Home Manage wireless networks Change advanced sharing settings	View your basic network info WIN7VM (This computer) View your active networks Network Public network	ormation and s	set up connections	See full map
×	Change your networking settings — Set up a new connection o Set up a wireless, broadbar	r network Id, dial-up, ad hoc,	or VPN connection; or set up	a router or access

Open the window to manage Wireless networks

G 🗣 🛃 « Network and Internet ) Manage Wireless Networks 🔹 🍕 Search Manage Wireless N
Manage wireless networks that use (Wireless Network Connection) Windows tries to connect to these networks in the order listed below.
Add Adapter properties Profile types Network and Sharing Center

Click "Add" to create a new entry.

() all Manually connect to a	wireless network				
How do you want to	add a network?				
Manually cree This creates a new for the network of security key (if ap	Manually create a network profile This creates a new network profile or locates an existing network and saves a profile for the network on your computer. You need to know the network name (SSID) and security key (if applicable).				
Create an ad This creates a ter	hoc network nporary network for sharing files or an Internet connection				
×					
Use option "Manualle create	e a network profile".				
🚱 ݵ Manually connect to a	wireless network				
Enter information for	r the wireless network you want to add				
Network name:	EAPtest				
Security type:	WPA2-Enterprise				
Encryption type:	AES				
Security Key:	Hide characters				
Start this connection	nautomatically				
Connect even if the network is not broadcasting					
wanning, ir you sele	ce chis option, your computer's privacy might be at lisk.				
	Next Cancel				

Enter the previously configured SSID

Choose WPA2-Enterprise" as "Security type" and "AES" as "Encryption Type". Click "Next"



Click on "Change connection settings"

EAPtest Wireless Network Properties
Connection Security
Security type: WPA2-Enterprise
Encryption type: AES
Choose a network authentication method: Microsoft: Smart Card or other certificat Settings Remember my credentials for this connection each
time I'm logged on
Advanced settings
OK Cancel
×

In tab "Security" choose "Microsoft Smartcard..." and press the button "Settings"

Smart Card or other Certificate Properties
When connecting: Use my smart card Use a certificate on this computer Validate server certificate selection (Recommended) Connect to these servers:
Trusted Root Certification Authorities:  DigiCert Assured ID Root CA DigiCert High Assurance EV Root CA Equifax Secure Certificate Authority Geo Trust Global CA Geo Trust Global CA HirschmannCA HirschmannCA Microsoft Root Certificate Authority
۲
View Certificate Do not prompt user to authorize new servers or trusted certification
Use a different user name for the connection
OK Cancel

Check "Validate server certificate" and choose the relevant certificate. Close all configuration dialaogs with button "OK"



Click on the WLAN icon in the taskbar and choose the relevant WLAN (EAPtest) to connect to.