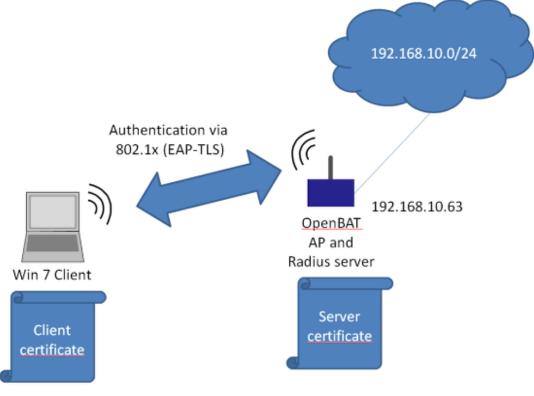


ナレッジベース > Products > BAT > BAT, WLC (HiLCOS) > How to set up 802.1x with EAP-TLS between Open BAT (as AP and Radius server) and Windows 7 client

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	2 🔳 🤉	-	telungen 192.	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	1	192.168.10.11	255.255.255.0	0.0.0.0	MAR 1040-4C4C4C4C99995MIN	HRHH	MACH-42F300
5 00:80:63:39:2E:A2		197 168 10 78	255 255 255 0	0.0.0	DS 30-2407T 1T 1SD AFHH	h	RS-392EA2
1 EC:E5:55:1E:64:26	Eigenschafte				×		RSP-ECE5551E6426
4 EC:E5:55:01:4B:C0	MAC-Adresse	EC:E5:55:D0:73	:20				RSP-ECE5550148C0
2 EC:74:BA:35:FD:9A	Name:	BAT-F_D07320				85	RSP-EC74BA36FD9A
8 EC:E5:55:68:1F:27	IP-Konfigura	IP-Konfiguration					RSB-681F27
3EC:E5:55:A4:B6:00	IP-Adresse: 192 . 168 . 10 . 63 Default setzen (192.168.10.23) MSP-ECE5554					MSP-ECE555A4B600	
	Netzmaske:	255 .	255 . 255		lt setzen (255.255.255.0)		
	Default Gateway: 0 . 0 . 0 . 0 Default setzen (0.0.0.0)						
	Als Voreinstellung speichern						
	Ok Abbrechen						
4			1	п			•
×							

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

🕣 🔻 🔎 QuickFinder	General				
Configuration	This is where you can pro	gram common settings for all wirely	ess LAN interfaces.		
Management	Country:	Europe	-		
General	ARP handling				
an perior accerting		- to d			
G Security	Indoor only mode activity				
Stations	Email address for WLAN	events:			
802.11i/WEP	Interfaces				
5 802.1X					
👗 WLC	This is where you can pro	gram physical and logical (MultiSS	ID) wireless LAN settings.		
AutoWDS	Physical WLA	N settings	Logical WLAN settings		
🔄 Trace					
😅 Wireless-IDS	Point-to-Point	Physical WLAN settings - W	Ablintedan 1	-9	
Interfaces	This is where you can g	Physical WLAN settings - W	LAN Intenace 1		
Date & Time Log & Trace	Operation Barlin Performance Client mode				
Communication	Common point-t	C			
Pv4	Extended settings	WLAN interface enabled			
2 IPv6	The following physical v	WLAN operation mode:	Access point -		
DIP Router	The following physical t	Broken LAN Ink detection:	None		
Firewall/QoS					
VPN	Bit rate serial P2P auto-	WLAN Interface Usage:	WLAN -		
Certificates					
COM Ports	Allow simultaneous (Link LED function:	Connection count -		
NetBIOS	Block time:				
Public-Spot			Jient signal strength' only makes sense in 'Client signal strength between this station and the co		
RADIUS Server	WLAN Link Status Log	point.			
Least-Cost-Router	Use this item to make the enables you to capture	Signal strength and thus faster the link LED blink	the connection quality is indicated by the blink s the better the connection is.	ing frequency. T	
	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 program common settings f	or all wireless I AN interfaces	
Wireless LAN	Country:		Europe	•
Band Steering Security Stations 802.11i/WEP	Indoor only me Email address for			
€ 802.1X			al (MultiSSID) wireless I AN settings	
Trace Wireless-IDS Interfaces	Datiest An Datiest	cal WLAN settings	Logical WLAN settings	
Date & Time Log & Trace Communication Interface:	ransmission Alarms	WLAN interface 1 - Network	:1	
9 IP√6	network enabled ame (SSID):	EAPtest		
Firewall/QoS Suppress S VPN	SID broadcast: er enabled	110		
NetBIOS	ount of clients: ent signal strength:	0	7.	

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.

	Interface settings Specify login setting	gs for each local area network i	interface.
Wireless LAN		(Interfaces
General Band Steering Security Stations 802.1X WEC AuguMDS	(name is DEFAULT LAN networks (to b	e authentication of the wireles). In addition, you can define yo	is LAN networks in a central RADIUS server our own RADIUS server for specific wireless phrase of the logical wireless LAN network), river can be specified. RADIUS servers
AutoWDS			
RADIUS servers			8 23
	e port bootop server a	ource addr	ОК
		RADIUS servers - New	Cancel Entry
		RADIUS servers - New Name:	Entry P
	Default server	RADIUS servers - New Name: Server address:	Entry Cancel
		RADIUS servers - New Name: Server address: Server port:	Entry 8 2
QuickFinder		RADIUS servers - New Name: Server address:	Cancel
QuickFinder		RADIUS servers - New Name: Server address: Server port:	Entry ? *
QuickFinder COM Ports NetBIOS Public-Spot RADIUS Server		RADIUS servers - New Name: Server address: Server port: Secret: Backup server:	Entry Cancel Entry Cancel Entry Cancel Entry Concellent E
QuickFinder COM Ports NetBIOS Public-Spot RADIUS Server		RADIUS servers - New Name: Server address: Server port: Secret: Backup server:	Entry Entry MY RADIUS 127.0.0.1 1.812 Generate password Show Generate password Show Generate password Show Generate password Show Cancel

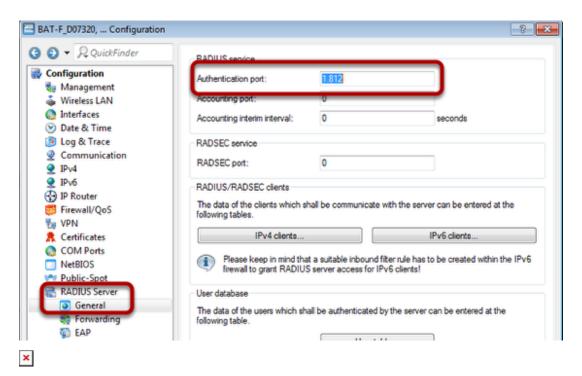
×

Proceed to menu "Wireless LAN - 802.1X"

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

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

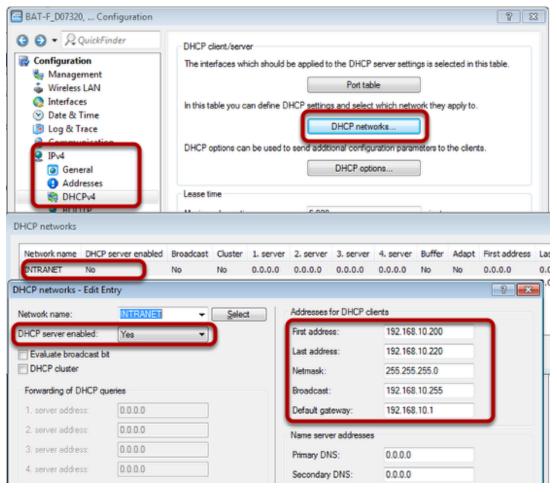
Fill in the fields. Leave the "Secret" field blank



Proceed to menu "RADIUS Server - General"

Configuration	Authentication method The server and the method	of authentication can be cho	osen here.
🤹 Management 💩 Wireless LAN	Default method:	TLS	-
 Interfaces Date & Time Log & Trace Communication IPv4 	Tunnel server:	e subject name towards the R/	ADIUS user table
	Default tunnel method		
9 IPv6	TTLS default:	MD5	-
P Router	PEAP default:	MSCHAPv2	•
WPN	Timeouts		
Certificates COM Ports	Reauth period:	0	seconds
NetBIOS	Retransmit timeout:	0	seconds
RADIUS Server General Forwarding			

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

file Edit Device Group	View Tools He	dp				
777 00 1	' 🖌 🖻 🖬 🖬	🏷 🗖 🛛 🥙 🚱 🔍 QuickFinder				
😂 Hirschmann LANconfig	Name	Comment Cl	uster Name	Address	Location	Device Statu
	@BAT-F_D07320	-1		192.168.10.63		Ok
		Configure		Ctrl+O		
		Setup Wizard		Ctrl+W		
		Quick Rollback		Ctrl+Q		
		Check		Ctrl+F5		
		Configuration Management		•	Print	Ctrl+P
-		Firmware Management		,	Save as File	Ctrl+S
		WEBconfig / Console Session		•	Restore from File	Ctrl+R
		Monitor Device			Save Script as File	
		Monitor Device Temporarily		Ctrl+M	Restore Script from File	
		Monitor WLAN Device			Save Certificate as File	_
		Create Trace Output			N Upload Certificate or File	
		Set Date/Time		T		
		Activate Software Option				
	*	Activate Configuration Synchronizati	on Settings			
Date Time	Name	Add to Wireless ePaper Server				

Rightclick on the OpenBAT within LANconfig

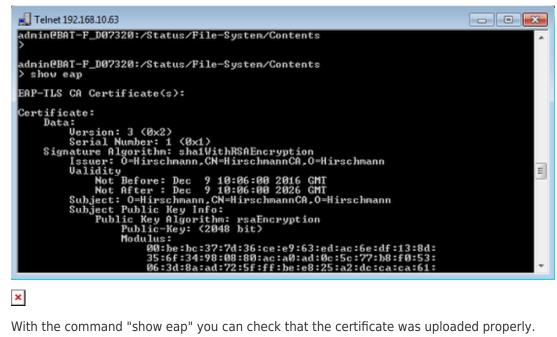
Use menu "Configuration Management - Upload Certificate or File...". A new window will open.

Restore C	ertificate to BAT-F_D07320				×
Suchen in:	📃 Desktop	•	G 🖻	⊳ 😥	
D D	ateiordner				•
T	ient.txt extdokument 51 KB		N		
PI	HirschmannBAT.p12 Privater Informationsaustau 3,49 KB				
PI	irschmannClient.p12 rivater Informationsaustau 36 KB				
si Aerea	suer tvt				Ŧ
Dateiname:	HirschmannBAT.p12			Öffne	en
Dateityp:	Certificate Files		-	Abbrec	hen
Certificate	EAP/TLS - Container as PKCS#	#12 file (*,	pfx, *.p12	[requires pa	BS: 🔻
Cert. password	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.

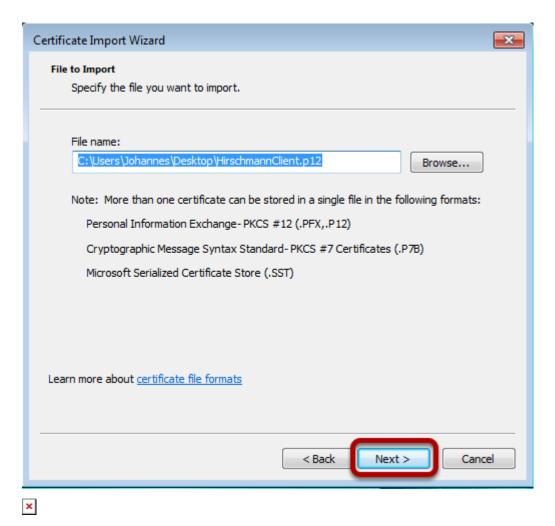


With the command "show eap" you can check that the certificate was uploaded properly.

Client side: Install the certificates



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



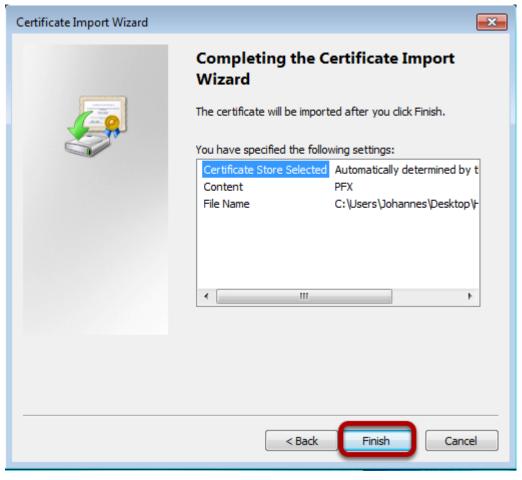
The wizard will show the path of the certificate. Use button "Next".

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	!

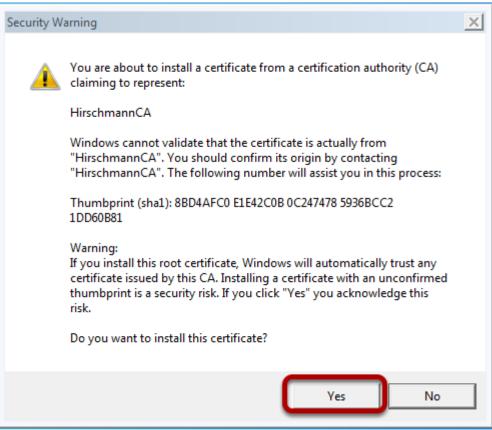
Enter the password of the certificate and click on "Next".

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.					
O 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					
x					

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)	tems Network and Sharing Center	• ∮•	Search Control Panel	م
Control Panel Home Manage wireless networks Change adapter settings Change advanced sharing settings	View your basic network inforr WIN7VM (This computer) View your active networks Network	nation and set	up connections	See full map
×	Change your networking settings Set up a new connection or ne Set up a wireless, broadband, a	twork	vPN connection; or set up	

Open the window to manage Wireless networks

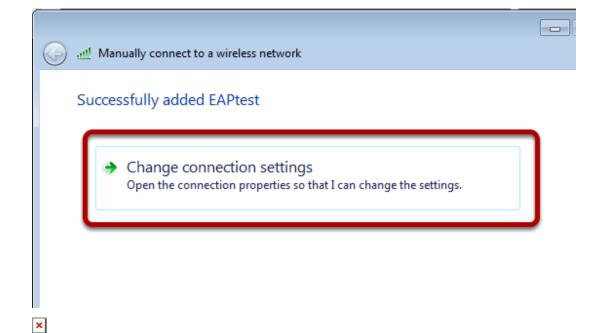
G 🗣 📶 « Network and Internet) Manage Wireless Networks 🔹 🍕 Search Manage Wireless N
Manage wireless networks that use (Wireless Network Connection) Windows tries to connect to these networks in the order listed below.
Add Adapter properties Profile types Network and Sharing Center
×

Click "Add" to create a new entry.

() all Manually connect to a	wireless network					
How do you want to	add a network?					
This creates a new for the network of	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 hoc network This creates a temporary network for sharing files or an Internet connection					
×						
Use option "Manualle create						
🕝 🏨 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 automatically						
Connect even if the network is not broadcasting Warning: If you select this option, your computer's privacy might be at risk.						
wanning, ir you sele	at this option, your computer a 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 Use simple certificate selection (Recommended) Validate server certificate 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 Microsoft Root Certificate Authority
4
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.