

Wissensdatenbank > Produkte > BAT > BAT, WLC (HiLCOS) > So richten Sie 802.1x mit EAP-TLS zwischen Open BAT (als AP- und Radius-Server) und Windows 7-Client ein

So richten Sie 802.1x mit EAP-TLS zwischen Open BAT (als AP- und Radius-Server) und Windows 7-Client ein

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

In dieser Lektion wird beschrieben, wie ein OpenBAT mit einem eigenen Radius-Server als AP konfiguriert werden kann, wobei eine EAP-TLS-Verbindung für einen Windows 7-Client bereitgestellt wird, und wie Zertifikate für diese Verwendung mit XCA erstellt werden.



×

Dies ist das Netzwerk, das in diesem Howto konfiguriert wird.

Diese Konfiguration und diese Topologie ist nur ein Beispiel. Es kann nach Kundenwunsch modifiziert werden.

OpenBAT konfigurieren

d MAC-Adresse	Schreibbar	IP-Adresse A	Netzmaske	Default Gateway	Produkt		Name
6 EC:E5:55:D0:73:20	V	0.0.0.0	0.0.0.0	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 1040-4C4C4C4C99995MM	RHH	MACH-42F300
5 00:80:63:39:2E:A2		197 168 10 28	255 255 255 0	0.0.0.0	DS 30-7407T 1T 1SD AFHH		RS-392EA2
1 EC:E5:55:1E:64:26	Eigenschaft	en			×		RSP-ECE5551E64
4 EC:E5:55:01:4B:C0	MAC-Adresse	: EC:E5:55:D0:73	:20				RSP-ECE55501480
2 EC:74:BA:36:FD:9A	Name:	BAT-F_D07320				3S	RSP-EC74BA36FD
8 EC:E5:55:68:1F:27	IP-Konfigura	tion					RSB-681F27
3 EC:E5:55:A4:B6:00	IP-Adresse: 192 . 168 . 10 . 63 Default setzen (192.168.10.23)						MSP-ECE555A486
	Netzmaske:	255 .	255 . 255	. Defau	lt setzen (255.255.255.0)		
	Default Gat	eway: 0.	0.0	. 0 De	efault setzen (0.0.0.0)		
			Als Voreinste	ellung speichern			
			Ok	Abbrechen			

Verwenden Sie HiDiscovery, um dem BAT eine IP-Adresse zuzuweisen. Der PC ist lokal angeschlossen.

R QuickFinder	General			
Configuration	This is where you can pro	gram common settings for all wirele	ss LAN interfaces.	
Management	Country:	Europe	•	
🤶 General	ARP handling			
Bur band seering	Indoor only mode activ	vated		
Security Stations	Email address for WLAN	events:		
802.11i/WEP 802.1X	Interfaces			
👗 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			-
Interfaces	This is where you can g	Physical WLAN settings - Wi	LAN Interface 1	
🕑 Date & Time		Operation Radio Performance	e Client mode	
Log & Trace	Common point4			
2 Communication	E an de de arreste	WLAN interface enabled		
2 IPv4	Extended settings	WI AN operation mode:	Access point	
₽ IPv6	The following physical v	The set operation mode.	Access pors	
DIP Router		Broken LAN link detection:	None 👻	
Firewall/QoS		WLAN Interface Lisage:	WI AN	
VPN	Bt rate serial P2P auto-		in the second se	
Certificates				
COM Ports	Allow simultaneous (Link LED function:	Connection count -	
NetBIOS	Block time:			
Public-Spot		The link-LED function 'O	lient signal strength' only makes sense in	Client mode' WLAN
RADIUS Server	-WLAN Link Status Log	 operation. It denotes the point. 	signal strength between this station and t	he connected acces
Least-Cost-Router	Use this item to make the enables you to capture	Signal strength and thus faster the link LED blinks	the connection quality is indicated by the the better the connection is.	blinking frequency.
	WLAN Link Status I			

Verwenden Sie den Access-Point im WLAN-Betriebsmodus. Optional können Sie alternative

Radioeinstellungen usw. vornehmen

QuickFinder	General			
Configuration Management	This is where yo	u can program common settings	s for all wireless LAN interfaces.	
Wireless LAN	Country:		Europe	•
🧕 General	ARP handling	9		
Band Steering	indoor only m	node activated		
Security Stations	Email address fo	r WLAN events:		
802.11i/WEP 802.1X	Interfaces This is where yo	u can program physical and log	ical (MultiSSID) wireless I AN eettings	
AutoW/DS				
	Phys	ical WLAN settings	Logical WLAN settings	
B Wireless-IDS	Delet to Delet			
🔕 Interfaces 🛛 🔚 Log	ical WLAN settings - WL	AN interface 1 - Network 1	? 💌	
S Date & Time Netwo	ork Transmission Alarms	1	_	_
Dog & Trace		1411 ANU		
IPv4	nace:	WLAN Interface 1 - Netwo	nk 1	
IP√6 IP√ IP√6 IP√ IP√6 IP√ IP√	WLAN network enabled			
IP Router Net	work name (SSID):	EAPtest		
Firewall/QoS Sup	press SSID broadcast:	NO		_
Certificates	MAC filter enabled			
COM Ports Max	imum count of clients:	0		
NetBIOS	mal client einnal etreorth	0	*	
IN NORTH				

Konfigurieren Sie die SSID





Weiter zum Menü "Wireless LAN - 802.11i / WEP"

Verwenden Sie die Schaltfläche "WPA oder Private WEP-Einstellungen ...". Ein neues Fenster wird geöffnet

Doppelklick auf die erste Zeile

Stellen Sie sicher, dass "Verschlüsselung aktiviert" aktiviert ist

Wählen Sie als Methode "802.11i (WPA) -802.1x"

Lassen Sie das Passphrase-Feld leer.

BAT-F_D07320, Configuration		8 8
Configuration	Interface settings Specify login settings for each local area network interface. Interfaces Authentication via RADIUS You can manage the authentication of the wireless LAN networks in a central RADIUS set (name is DEFAULT). In addition, you can define your own RADIUS server for specific wire LAN networks to be entered in place of the passphrase of the logical wireless LAN netwo For each RADIUS server listed here, a backup server can be specified. RADIUS servers	srver sless rk).
RADIUS servers	RADIUS servers - New Entry	
QuickFinder COM Ports NetBIOS Public-Spot RADIUS Server Least-Cost-Router	Add Server address: 127.0.0.1 Server port: 1.812 Secret: Image: Comparison of the symbol comparison of the sy	r the section.
(b) HIRSCHMANN	OK Can	

×

Weiter zum Menü "Wireless LAN - 802.1X"

Verwenden Sie die Schaltfläche "RADIUS servers ...". Ein neues Fenster wird geöffnet.

Verwenden Sie die Schaltfläche "Add". Ein neues Fenster wird geöffnet.

Füllen Sie die Felder aus. Lassen Sie das "Secret" Feld leer

V + P2 QuickFinder	RADIUS sendoe		
Configuration Management	Authentication port:	1.812	
Wireless LAN	Accounting port:	0	
Interfaces Date & Time	Accounting interim interval:	0	seconds
Log & Trace	RADSEC service		
Communication	RADSEC port:	0	
Pv4			
♥ IPv4 ♥ IPv6 ♥ IP Router ♥ Firewall/QoS ► VPN	RADIUS/RADSEC clients The data of the clients which s following tables.	hall be communicate wit	h the server can be entered at the
♥ IPV4 ● IPv6 ● IP Router ■ Firewall/QoS ● VPN R Certificates	RADIUS/RADSEC clients The data of the clients which s following tables.	hall be communicate wit	h the server can be entered at the

Weiter mit Menü "RADIUS-Server - General"

Verwenden Sie "1812" als "Authentication Port".

G ⊙ ▼ R QuickFinder	Authentication method The server and the method	of authentication can be cho	osen here.	
 Management Wireless LAN Interfaces Date & Time Log & Trace Communication IPv4 IPv6 IP Router 	Default method: Tunnel server: For EAP/TLS check the Default tunnel method TTLS default: PEAP default:	TLS e subject name towards the R/ MD5 MSCHAPv2	ADIUS user table	
 Priewal/ Gos VPN Certificates COM Ports NetBIOS RADIUS Server General Forwarding EAP Options 	Timeouts Reauth period: Retransmit timeout:	0	seconds	

Weiter zum Menü "RADIUS Server - EAP"

Wählen Sie "TLS" als "Default Method".

🔄 BAT-F_D07320, Configu	uration								8	3
G 🕤 🗸 R QuickFinder	DHC	P cliant /sec								ור
Configuration	The	interfaces u	voi deich choudd	he applied to		encourt entities	on in colu	i ni hato	his table	
Sa Management	ine	intendoes v	mich should	be applied to	othe Dhur	server setur	igs is see	ected in t	nis table.	
line wireless LAN					Port tak	ole				
Interfaces	in th	is table you	can define D	HCP setting	s and select	t which netw	ork they	apply to.		
🕑 Date & Time					DHCP onto	undra.				
Dog & Trace					DHCF New	runs				
5 IPv4	DHO	P options c	an be used t	o send addit	ional config	uration parar	neters to	the clien	te.	
General					DHCP opt	ions				
Addresses							-			
S DHCPv4	Leas	e time								
DHCP networks - Edit Entry	No No	No	0.0.0.0	2. server	0.0.0.0	4. server	No	No	0.0.0.0	0.0
Network name:	TRANET	- Sek	ict 🛛	Addresses	for DHCP cl	ients			_	
DHCP server enabled: Y	es	-		First addres	99:	192.168	10.200			ŀ
Evaluate broadcast bit				Last addre	SS:	192.168	10.220			
DHCP cluster				Netmask:		255.255	255.0			-
Forwarding of DHCP queries				Broadcast		192.168	10.255			
1. server address: 0.	0.0.0			Default gat	teway:	192.168	.10.1			
2. server address: 0.	0.0.0			Name serve	er addresse:	,		_		
2. server address: 0. 3. server address: 0.	0.0.0			Name serve Primary DN	er addresse: VS:	s 0.0.0.0				

Weiter mit Menü "IPv4 - DHCPv4"

Verwenden Sie die Schaltfläche "DHCP networks ...". Ein neues Fenster wird geöffnet.

Doppelklicken Sie in der ersten Zeile (INTRANET). Ein neues Fenster wird geöffnet.

Aktivieren Sie den DHCP-Server und konfigurieren Sie die relevanten IP-Einstellungen.

Damit ist die Konfiguration des OpenBAT abgeschlossen.

Laden Sie das Serverzertifikat auf den OpenBAT hoch

😤 🕱 🥄 🖾 🥥 🗸	View Tools Help	R QuickFind	ler			
Hirschmann LANconfig	Name	Comment	Cluster Name	Address	Location	Device Status
E	BAT-F_007320	Configure Setup Wizard Quick Rollback Check		197.168.10.63 Ctrl+O Ctrl+W Ctrl+Q Ctrl+F5		Ok
		Configuration Management Firmware Management WEBconfig / Console Session		;	Print Save as File Restore from File	Ctrl+P Ctrl+S Ctrl+R
		Monitor Device Monitor Device Temporarily Monitor WLAN Device Create Trace Output Set Date/Time Activate Software Option		Ctrl+M	Save Script as File Restore Script from File Save Certificate as File Nupload Certificate or File	>
Data Tara M	<	Activate Configuration Synchroni Add to Wireless ePaper Server	ization Settings			

Klicken Sie mit der rechten Maustaste auf den OpenBAT in LANconfig

Verwenden Sie das Menü "Configuration Management –Upload Certificate or File...". Ein neues Fenster wird geöffnet.

Restore Co	ertificate to BAT-F_D07320				×
Suchen in:	📃 Desktop	-	G 🗊	▼ 🏷	
D D	ateiordner				
CI	l ient.txt extdokument 51 KB				
H Pi	l irschmannBAT.p12 rivater Informationsaustau 49 KB		2º		
Pi 3,	l irschmannClient.p12 rivater Informationsaustau 36 KB				
51	cilec tvt				-
Dateiname:	HirschmannBAT.p12			Öffner	1
Dateityp:	Certificate Files		•	Abbrech	ien
Certificate	EAP/TLS - Container as PKCS	#12 file (*.p	fx, *.p12	(requires pa	St 🔻
Cert. password	Replace existing file of this t	уре			

×

Wählen Sie die entsprechende Datei aus

Wählen Sie "EAP / TLS - Container as PKCS # 12 file"

Geben Sie das Passwort ein

Das Zertifikat wird hochgeladen.



×

Mit dem Befehl "show eap" können Sie überprüfen, ob das Zertifikat ordnungsgemäß hochgeladen wurde.

Client-Seite: Installieren Sie die Zertifikate



Doppelklicken Sie auf das Client-Zertifikat. Ein neues Fenster wird geöffnet.

Klicken Sie auf "Next"



Der Assistent zeigt den Pfad des Zertifikats an.

Betätigen Sie die Schaltfläche "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 > Cancel	
×	

Geben Sie das Passwort des Zertifikats ein und klicken Sie auf "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.	
 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	

Bleib bei den Standardeinstellungen. Der Ort zum Speichern des Zertifikats wird automatisch ausgewählt.

Klicken Sie auf "Next"



Klicken Sie auf "Finish"



1

Bestätigen Sie, um das Zertifikat zu installieren.

Konfigurieren Sie das drahtlose Netzwerk

🔾 🖓 😨 📽 All Control Panel	Items + Network and Sharing Center		Search Control Panel	Q
Control Panel Home Manage wireless networks Change adapter settings Change advanced sharing	View your basic network inform	nation and se	et up connections	e See full map
settings	View your active networks Network Public network	A	Cor Access type: Internet Connections: 💡 Local Area	nnect or disconnect
	Change your networking settings Set up a new connection or ne Set up a wireless, broadband, o	twork dial-up, ad hoc, o	or VPN connection; or set up	a router or access
×	noint.			

Öffnen Sie das Fenster, um drahtlose Netzwerke zu verwalten

Good ⊂ Image Wireless Networks - 4y Search Manage Wireless Networks
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
×

Öffnen Sie das Fenster, um drahtlose Netzwerke zu verwalten

() all Manually connect to a	wireless network		
How do you want to	add a network?		
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		
×			
Verwenden Sie die Option "	Manually create network profile"		
G 🔐 Manually connect to a	wireless network		
Enter information for 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.			
	Next Cancel		

Geben Sie die zuvor konfigurierte SSID ein

Wählen Sie WPA2-Enterprise als "Security type" und "AES" als "Encryption type"

Click "Next"



Klicken Sie auf "Change connection settings"

EAPtest Wireless Network Properties		
Connection Security		
Security type:	WPA2-Enterprise	
Encryption type:	AES	
Choose a network au Microsoft: Smart Car Remember my cre time I'm logged or Advanced settings	thentication method: d or other certificat Settings dentials for this connection each	
	OK Cancel	
×		

In der Registerkarte "Security" wählen Sie "Microsoft Smartcard..." und klicken auf die Schaltfläche "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 GeoTrust Global CA Equifax CA		
GIL Cyber Hast Global Root FirschmannCA Microsoft Hoor Authority		
Microsoft Root Certificate Authority		
View Certificate Do not prompt user to authorize new servers or trusted certification		
Use a different user name for the connection		
OK Cancel		

Aktivieren Sie "Validate server certificate" und wählen Sie das entsprechende Zertifikat aus. Schließen Sie alle Konfigurationsdialoge mit der Schaltfläche "OK"



Klicken Sie in der Taskleiste auf das WLAN-Symbol und wählen Sie das entsprechende WLAN (EAPtest) aus, zu dem Sie eine Verbindung herstellen möchten.