

Wissensdatenbank > Produkte > BAT > BAT, WLC (HiLCOS) > So verwenden Sie einen Open BAT oder WLC als RADIUS-Server und richten Benutzerkonten ein

# So verwenden Sie einen Open BAT oder WLC als RADIUS-Server und richten Benutzerkonten ein

- 2022-01-10 - BAT, WLC (HILCOS)

In dieser Lektion wird beschrieben, wie Sie die RADIUS-Serverfunktion für einen Open BAT oder einen WLC konfigurieren und Benutzerkonten einrichten.

Für eine vollständige 802.1x-Umgebung (Supplicant - Authenticator - Server) müssen Sie möglicherweise auch die folgenden Lektionen lesen:

Umgebung ohne Controller:

- How to configure an Open BAT as 802.1x supplicant
- How to configure an Open BAT as 802.1x authenticator

Umgebung mit Controller zur Verwaltung der 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

Diese Lektionen ergänzen sich und verwenden die folgenden Einstellungen für die Radiusauthentifizierung: EAP - PEAP mit MSCHAPv2 als Tunnelmethode.

Darstellung



Ein WLC oder ein Open BAT kann als RADIUS-Server verwendet werden. Die Menüs auf beiden sind identisch, jedoch ist bei Verwendung eines BAT der manuelle Upload eines Zertifikats erforderlich (Schritt in diesem Dokument beschrieben).

### Vorbereitende Schritte

Geben Sie dem BAT eine IP-Adresse (in unserem Beispiel: 192.168.1.150).

Siehe auch Lektion "So geben Sie einer Open BAT oder einem WLC eine IP-Adresse"

Fügen Sie den BAT in LANconfig hinzu

Siehe auch Lektion "So finden Sie eine BAT oder einen WLC in LANconfig"

Laden Sie ein Zertifikat auf den Server hoch (wenn Sie einen BAT als RADIUS-Server verwenden).



Dieser Schritt ist nicht erforderlich, wenn Sie einen Controller (WLC) als RADIUS-Server verwenden, da der Controller seine eigenen Zertifikate erstellen kann.

Wenn Sie jedoch einen BAT verwenden, müssen Sie dies manuell tun. Sie benötigen ein Zertifikat (PFX- oder P12-Dateien, diese Dateien enthalten einen privaten Schlüssel und das zugehörige Zertifikat).

Sie können die angehängte Datei zu Testzwecke verwenden

SSL-Zertifikate

(Passwort für die Zertifikate: hirschmann)

Dann klicken Sie in LAN-Config mit der rechten Maustaste auf den BAT, der als RADIUS-Server verwendet werden soll.

Configuration Management > Upload certificate or File ...

Wählen Sie die zu verwendende PFX- oder P12-Datei aus und wählen Sie als Zertifikattyp "EAP / TLS - Container als PKCS # 12-Datei" (normalerweise durch ein Kennwort geschützt).

> Open

Die Datei wird auf den BAT hochgeladen

Der Gerätestatus muss nach dem Hochladen "OK" sein

### Allgemeine Einstellungen

3 • R QuickFinder	RADIUS service		
Configuration	Authentication port:	1.812	
General	Accounting port:	0	
Admin Authentication	Accounting interim interval:	0	seconds
💑 Costs	RADSEC service		
Advanced Wireless LAN	RADSEC port:	0	
<ul> <li>Solution</li> <li>Date &amp; Time</li> <li>Log &amp; Trace</li> <li>Q Communication</li> <li>Q IPv4</li> <li>Q IPv6</li> <li>IP Router</li> </ul>			
<ul> <li>j (B) Log &amp; Trace</li> <li>j (P) Communication</li> <li>j (P) IP V4</li> <li>j (P) IP Nouter</li> </ul>	The data of the clients which s following tables. IPv4 clients Please keep in mind tha firewall to grant RADIU.	hall be communicate wit at a suitable inbound filte S server access for IPv6	h the server can be entered at the IPv6 clients IPv6 clients
<ul> <li>▷ Concernation</li> <li>▷ Q Communication</li> <li>♀ IPv4</li> <li>♀ IPv6</li> <li>♀ IPv6</li> <li>♀ IP Router</li> <li>▷ ♥ Firewall/QoS</li> <li>♥ VPN</li> </ul>	The data of the clients which s following tables. IPv4 clients Please keep in mind that firewall to grant RADIU:	thall be communicate wit at a suitable inbound filte S server access for IPv6	h the server can be entered at the IPv6 clients IPv6 clients IPv6 clients!
<ul> <li>▷ Context Inflet</li> <li>▷ Log &amp; Trace</li> <li>▷ ② Communication</li> <li>○ IPv4</li> <li>○ IPv6</li> <li>○ IP Router</li> <li>○ IP Router</li> <li>○ Firewall/QoS</li> <li>▷ VPN</li> <li>▷ Cont Ports</li> <li>○ Net8IOS</li> <li>□ Net8IOS</li> <li>□ RADIUS Server</li> </ul>	The data of the clients which is following tables.  IPv4 clients  Please keep in mind the firewall to grant RADIU: User database The data of the users which sh following table.	t a suitable inbound filte st a suitable inbound filte S server access for IPv6 nall be authenticated by t	h the server can be entered at the IPv6 clients r rule has to be created within the IPv6 i clients! the server can be entered at the 
Image: Constant and the second se	The data of the clients which is following tables.  IPv4 clients  Please keep in mind the firewall to grant RADIU. User database The data of the users which sh following table. The server will check authentice	thal be communicate with at a suitable inbound filte S server access for IPv6 hall be authenticated by the User table cation requests against the	h the server can be entered at the IPv6 clients r rule has to be created within the IPv6 clients! the server can be entered at the he following tables.

Configuration > RADIUS Server > General Konfigurieren Sie den Authentication Port: 1812

Konfigurieren Sie die Liste der RADIUS-Clients (IP Adresse Authenticator und Shared Secret)

Paddress Netmask	Protocols			ОК
192.168.1.140 255.255.255.25	5 RADIUS			Cancel
		IPv4 clients - Edit Entry		8 ×
	_	IP address:	192.168.1.140	
QuickFinder		Netmask:	255.255.255.255	
	7118a 15a	Protocols:	RADIUS -	
EAP	Auto clea	Client secret:	support	Show

Wählen Sie im Dialogfeld "General" IPv4-Clients aus

Erstellen Sie einen neuen Eintrag.

Der neue Eintrag kann ein einzelnes Gerät sein (in unserem Beispiel ist dies nur das Gerät 192.168.1.140), es kann sich jedoch auch um eine Reihe von Geräten handeln (der Bereich wird durch die Netzmaske definiert).

Das Shared Secret wird auch auf dem Authenticator konfiguriert (siehe Lektion "So konfigurieren Sie eine Open BAT als 802.1x-Authenticator").

> 0K

Benutzerkonten einrichten

Entry active			Passphrase (optional):		Show
Name / MAC address:	laurent			Generate password	]
Case sensitive usemame	e check		TX bandwidth limit:	0	kbit/s
Password:	lolothebest V Show	<i>(</i>	RX bandwidth limit:	0	kbit/s
	Generate password		Station mask		
VLAN ID:	0		Calling station:		1
Comment:		^	Called station:		j
			Validity/Expiry		
Canada an Anna an			Expiry type:	Relative & absolute 🔹	]
Service type.	Any 🔹		Relative expiry:	0	seconds
Protocol restriction for aut	hentication		Absolute expiry:	00:	00:00
PAP	CHAP		V Multiple login		
V MSCHAP	MSCHAPVZ		Max. concurrent logins:	0	-
If here are made no restrictions, all authentication		Time budget:	0	seconds	
protocols will be a	lowed automatically!		Volume budget:	0	byte
Shell privilege level:	0				

Wählen Sie im Dialogfeld "General" die Option "User Table" aus.

Erstellen Sie für jeden Benutzer einen neuen Eintrag.

In unserem Fall verwenden wir nur einen Benutzer: laurent

Zur Eingabe des Benutzernamens und eines Passworts, in unserem Fall: lolothebest

Der Name und das Kennwort werden vom Supplicant verwendet (siehe Lektion "So konfigurieren Sie einen Open BAT als 802.1x-Supplicant").

#### > 0K

Nach dem Laden der Konfiguration ist Ihr Gerät bereits als RADIUS-Server konfiguriert

Überprüfen Sie den Status des NAS (Network Access Server oder Authenticator).

HiLCOS Menu Tree							(	ĥ)	н
🗐 Logout								U	ABE
HiLCOS Menu Tree Status TCP-IP RADIUS-Server Access-Control Clients									
IP-Address	Last-Request	Last-Status- Request	NAS-Ident	Access- Requests	Status- Requests	Duplicate- Requests	Access- Accepts	Access- Rejects	Access- Challen
127 0 0 1	5068	0	BAT-R 56AC14	4	0	0	2	0	2
192.168.1.140	5068	0	AP2_GROUP1	12	0	0	1	1	10

Sie können es über die Weboberfläche überprüfen

HiLCOS-Menübaum> Status> TCP-IP> RADIUS-Server> Access Control

## Überprüfen Sie die Authentifizierung der Clients

HiLCOS Menu Tree	HIRSCHMANN A BELDEN BRAND
HiLCOS Menu Tree Status <u>TCP-IP</u> <u>RADIUS-Serv</u>	<u>er</u>
Log-Table	
Index Time	Event
18 12/08/2014 12:01:07 17 12/08/2014 12:01:07	sent RADIUS accept for user id support to 192.168.1.140
12/06/2014 12:01:07	sent roadios chanenge for user to support to 192, 166, 1, 140

Das Ergebnis der Authentifizierungsversuche finden Sie in derLog-Tabelle, das über das Webinterface verfügbar ist unter:

HiLCOS-Menübaum> Status> TCP-IP> RADIUS-Server> Log-Tabelle.

Weitere Informationen können verfügbar sein, wenn Sie RADIUS Accounting verwenden (in

dieser Lektion nicht beschrieben).

Ähnliche Inhalte

- So konfigurieren Sie eine Open BAT als 802.1x-Supplicant
- So konfigurieren Sie eine Open BAT als 802.1x-Authenticator
- How to configure a Radius Profile on the WLC and include it in Logical settings