

Base de connaissances > Products > BAT > BAT, WLC (HiLCOS) > How to use Radius to access the BAT's agent

How to use Radius to access the BAT's agent

- 2018-02-21 - BAT, WLC (HiLCOS)

General information



BAT uses so named ""**Privilege Levels**"" to define different access rights of a user to the agent. Those levels are defined as:

- 1: User, read-only
- 3: User, write-only
- 5: Admin, read only, no trace rights
- 7: Admin, read and write, no trace rights
- 9: Admin, read-only
- 11: Admin, read and write
- 15: Supervisor

All other values are mapped to ""no access"".

Additional to the ""Privilege Levels"" you can define so named **""Functional Rights""**. A functional right could be e.g. the right to use a specific wizard within WEB-interface.

Open LANconfig configuration dialog

BAT-R_56AB24 Configuration			3 X
G Configuration Management Management Management Mathemication Admin Authemication Costs Advanced Wireless LAN Interfaces Date & Time Log & Trace Communication PV4 IPv6 PV6	Device Login Authentical Select the method for au Authentication via: RADIUS authentication Specify the attribute to b Access rights via: Specify if accounting da Accounting: Configure the RADIUS of	ation Uthenticating users while accessing the device. Internal administrator table be used by the RADIUS server for transmitting access rights Provider specific attribute ta shall be transmitted via RADIUS. No Example Comparison of the following table. RADIUS servers	• •
Firewall/QoS			

- Open LANconfig dialog
- Click on ""Configuration Management Authentication"" in the left hand menu
- Click on ""RADIUS servers..."" to configure the Radius servers.

Configure Radius Servers

			Cano	
		RADIUS servers -	New Entry	8 ×
		Profile name:	2 RASPBERRY)
		Backup profile:		- Select
QuickFinder	Add	Edit Server address:	3 192.168.10.216	•
	_	Port:	1.812	
		Secret:	4	Show
			Generate password	F
		Source address:		- Select
		Protocol:	RADIUS	•

- 1. Press ""Add..."" to open the Radius Servers dialog.
- 2. Enter Profile name
- 3. Enter IP-address of your Radius server
- 4. Enter shared secret defines on your Radius server
- 5. Press ""OK""

Specify the Radius Attribute to be used

BAT-R_56A824 Configuration	
 QuickFinder Configuration Management General Admin Authentication Costs Advanced Wireless LAN Interfaces Date & Time Log & Trace Communication IPv6 IPv6 IPv6 IP Reacters 	Device Login Authentication Select the method for authenticating users while accessing the device. Authentication via: Internal administrator table RADIUS authentication Specify the attribute to be used by the RADIUS server for transmitting access rights. Access rights via: Provider specific attribute Specify if accounting data shall b Provider specific attribute Management privilege level attribute No Configure the RADIUS servers in the following table. RADIUS servers

Management privilege level attribute

Use ""**Management privilege level attribute**"" if you don't want to assign functional access rights to any user and you don't use Radius attribute 136 for other devices in the network.

If you use ""**Management privilege level attribute**"", configuration of Radius server is more easy cause you then can use standard Radius attribute 136 (Management-Privilege-Level).

Here is an example of freeradius users file:

testuser Cleartext-Password := ""testpassword"" User-name == ""testuser"", Service-Type := NAS-Prompt-User, Service-Type := Administrative-User, Management-Privilege-Level := ""15""

This testuser will have supervisor rights because of Management-Privilege-Level 15.

Provider specific attribute

If you use Radius attribute 136 for other devices in the network or you want to assign functional access rights to a user then choose **""Provider specific attribute""**. This is the default value.

In this case you have to use two vendor-specific Radius attributes using **vendor ID 2356**.

Access rights ID: 11 Function rights ID: 12

For freeradius these vendor-specific attributes have to be defined in a file which has to be included in /etc/freeradius/dictionary. In the following example the file is named /etc/freeradius/dictionary.hirschmann. In this case please add the red line into /etc/freeradius/dictionary. It should then look like:

.....

The filename given here should be an absolute path.
#
\$INCLUDE /usr/share/freeradius/dictionary
\$INCLUDE /etc/freeradius/dictionary.hirschmann

The file /etc/freeradius/dictionaly.hirschmann file should look like:

-*- text -*#
#
dictionary.hirschmann
#
originally by
""J.S. "" <>
#
VENDOR Hirschmann 2356
BEGIN-VENDOR Hirschmann
Attributes
ATTRIBUTE Hirschmann-Access-Rights 11 integer
ATTRIBUTE Hirschmann-Function-Rights 12 integer
END-VENDOR Hirschmann

An example for a users file could be:

```
network Cleartext-Password := ""hirschmann""
User-name == ""network"",
Hirschmann-Access-Rights := ""1"",
Hirschmann-Function-rights := ""67"",
```

This is how the values for ""Hirschmann-Functional-Rights"" can be calculated:

- 1. Open the console of the BAT.
- 2. Change to the directory **Setup** > **Config** > **Admins**.
- 3. The command set? shows you the current mapping of the function rights to the corresponding hexadecimal code (e.g. Device-Search (0x80)).
- 4. To combine function rights, you add their hex values together.
- 5. Convert the hexadecimal value to a decimal number.
- 6. By using this decimal value in the function rights ID, you can transfer the corresponding rights.

In above example the user ""network"" gets functional rights for Basic-Wizard (0x1) Security-Wizard (0x2) Time-Setting (0x40)

Sum: 43 (HEX) = 67 (DEZ)