

How to use a BAT or a WLC as RADIUS Proxy

This How to explains step by step how to configure a BAT or a WLC as a RADIUS Proxy. You may need to refer to the following lessons for a complete working 802.1x environment (Supplicant - Authenticator - Server):

Environment without controller:

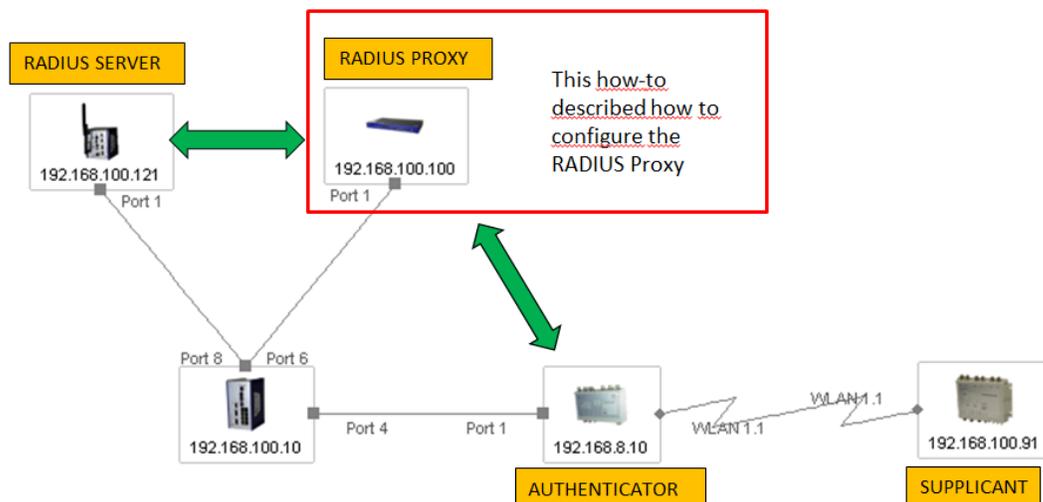
- How to configure an Open BAT as 802.1x supplicant
- How to configure an Open BAT as 802.1x authenticator
- How to use an Open BAT or a Controller as RADIUS Server and set up User accounts

Environment with controller to manage the APs:

- How to configure an Open BAT as 802.1x supplicant
- How to create a profile on a WLC and apply it on BAT Access points
- How to configure a Radius Profile on the WLC and include it in Logical settings
- How to use an Open BAT or a Controller as RADIUS Server and set up User accounts

These How to are complementary and use the following settings for the radius authentication: EAP - PEAP with MSCHAPv2 as tunnel method.

Representation



In our example, the authenticator is configured to send the RADIUS authentication requests to 192.168.100.100. 192.168.100.100 is a controller. We'll configure it as Proxy to forward the request to the real

RADIUS server at 192.168.100.121 (a BAT in our example)

It starts from the assumption that it was previously configured as a simple RADIUS server following the How-to :

- How to use an Open BAT or a Controller as RADIUS Server and set up User accounts

Concept

Forwarding and proxying of RADIUS requests is based on the concept of realms. A realm is a string that defines the validity range of user accounts. When explicitly specified, the realm is appended to the user name with an at-character as separation: **username@realm**

The **forwarding table** allows to define a list of RADIUS servers, each associated with a certain realm. The forwarding table is searched for the realm given along with a username; if no corresponding entry is found, the request is answered with an Access Reject.

An empty realm is internally interpreted as a local authentication request, i.e. the local RADIUS server will search its own database and will generate an answer.

To utilize realm handling, there are two particular realms beside the forwarding table:

- The **default realm** is the realm that will be used whenever a realm is given that has no configured forwarding server. Note that this realm itself has to be defined in the forwarding table; otherwise the access request will be rejected.
- The **empty realm** is the realm that will be used if a username without realm is given.

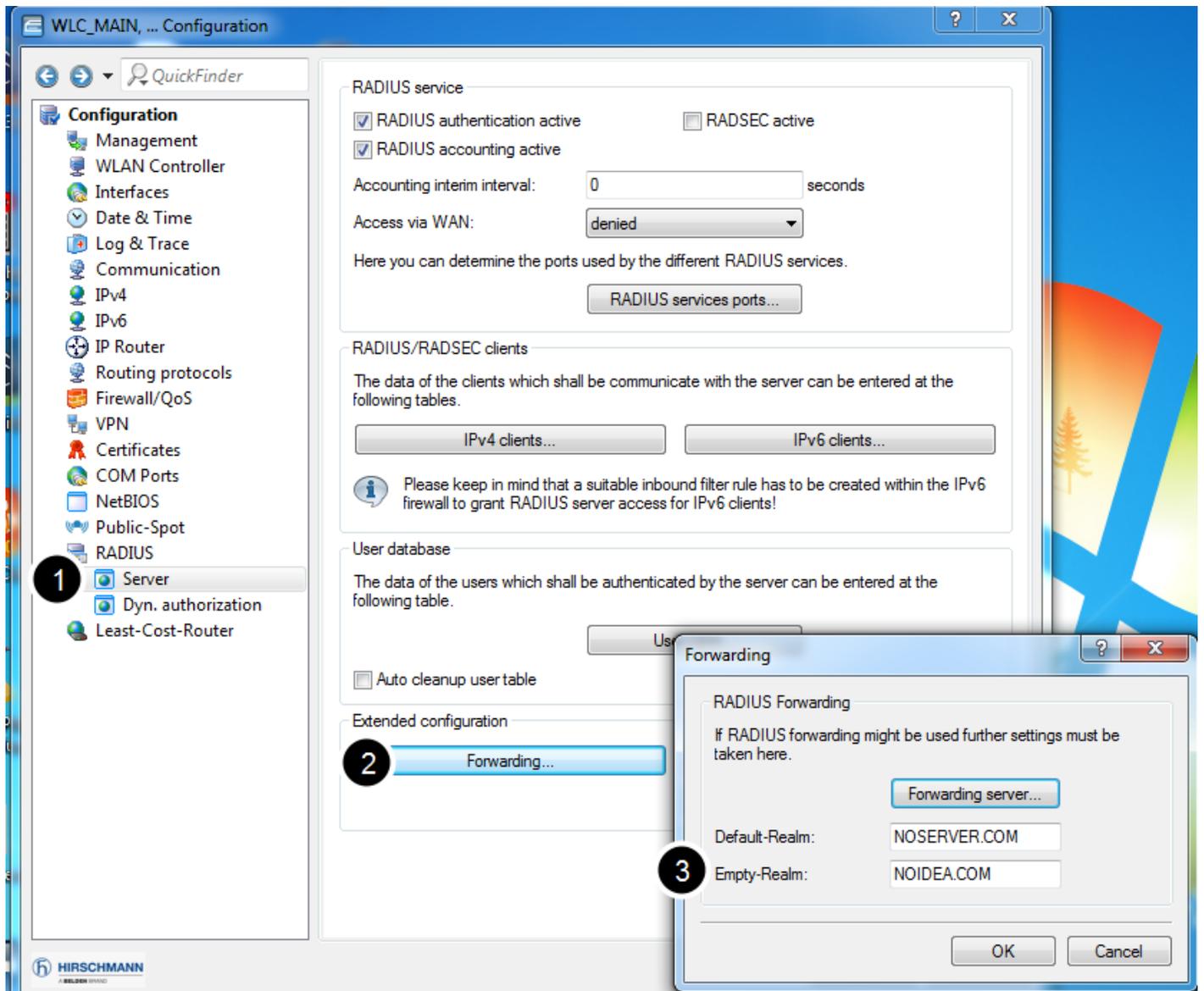
The **default configuration** of the local RADIUS server is an empty forwarding table, and both the default and empty realm are left empty. This means that **all requests will be handled locally**, and the realm will effectively be ignored.

To use the local RADIUS server as a pure **forwarder/proxy**, set both the default and empty realm to a realm that is configured in the forwarding table.

In our example the supplicant doesn't include any realm in its name.

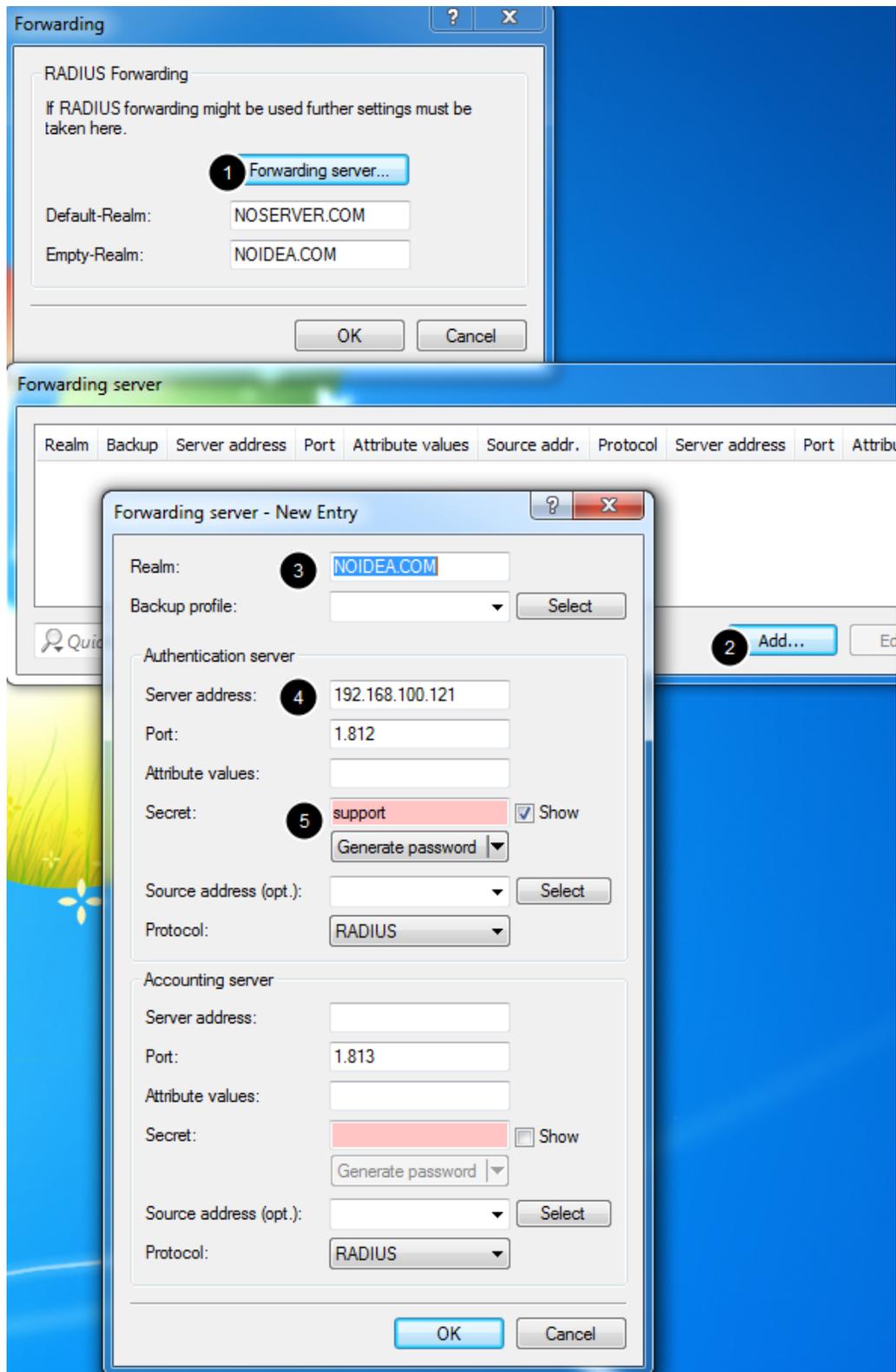
A default realm will be added by the RADIUS Proxy and request will be forwarded to the corresponding RADIUS server

Define an empty realm



- 1/ Select Configuration > RADIUS > Server
- 2/ Clic on the menu Forwarding
- 3/ Enter an Empty-Realm, in our example: NOIDEA.COM

Define a forwarding server



- 1/ From the Forwarding Window, select "Forwarding server"
- 2/ Add a new server
- 3/ Enter the Realm you defines previously as "Empty Realm"

4/ Enter the IP address of the RADIUS the request should be forwarded to

5/ Enter the secret shared with the RADIUS server

> OK

Check the logs

Logs on the RADIUS

HiLCOS Menu Tree
Status
TCP-IP
RADIUS-Server

Log-Table

Index	Time	Event
85	01/13/2020 14:32:05	sent RADIUS accept for user id 'client2' to 192.168.100.100
1	01/13/2020 14:32:05	sent RADIUS challenge for user id 'client2' to 192.168.100.100

Logs on the Proxy

HiLCOS Menu Tree
Status
TCP-IP
RADIUS-Server

Log-Table

Index	Time	Event
174	01/13/2020 14:31:39	sent RADIUS accept for user id 'client2' to 192.168.8.10
2	01/13/2020 14:31:39	sent RADIUS challenge for user id 'client2' to 192.168.8.10

From this point you can check the authentication attempts on the Proxy and on the RADIUS under:

HiLCOS Menu Tree > Status > TCP-IP > RADIUS-Server > Log-Table

1/ The RADIUS sent a challenge to the Proxy for client2

2/ The proxy Relayed the challenge to the NAS

3/ The RADIUS sent an accept to the WLC for client2

4/ The proxy relayed the accept to the NAS