How to use Radius authentication to access switch management

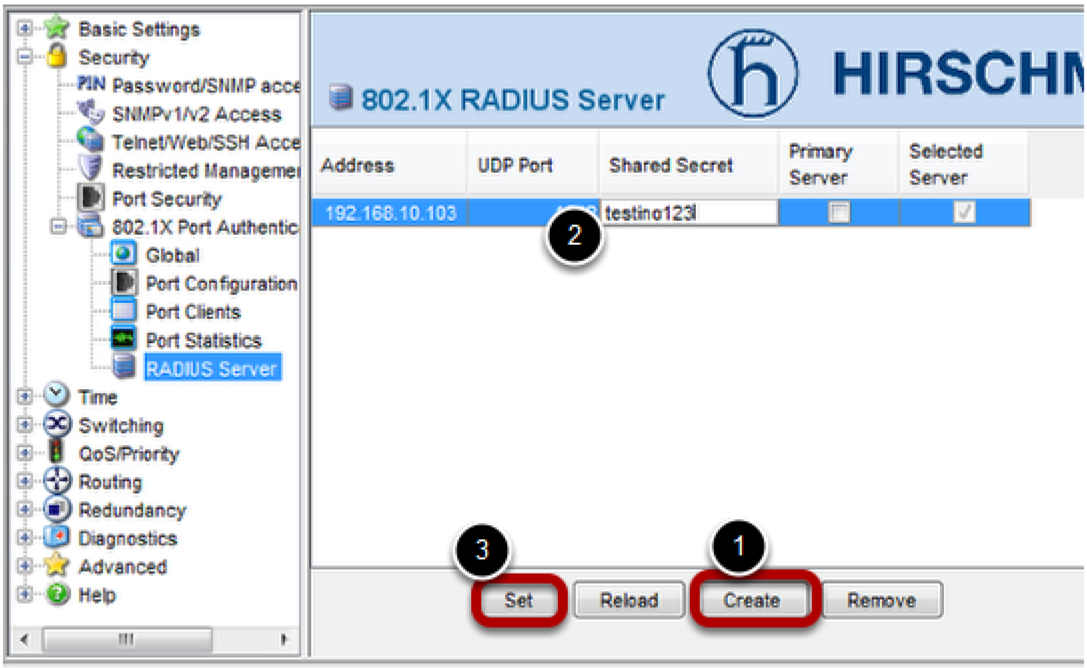
- 2024-03-06 - Classic Switches

This lesson describes how to configure radius for switch management access via telnet and webinterface.

The functionality is available as of release 7 for devices with L2P software and higher.

Note: For webinterface configuration make sure that the password consists 8 or more characters.

Configure Radius-Server



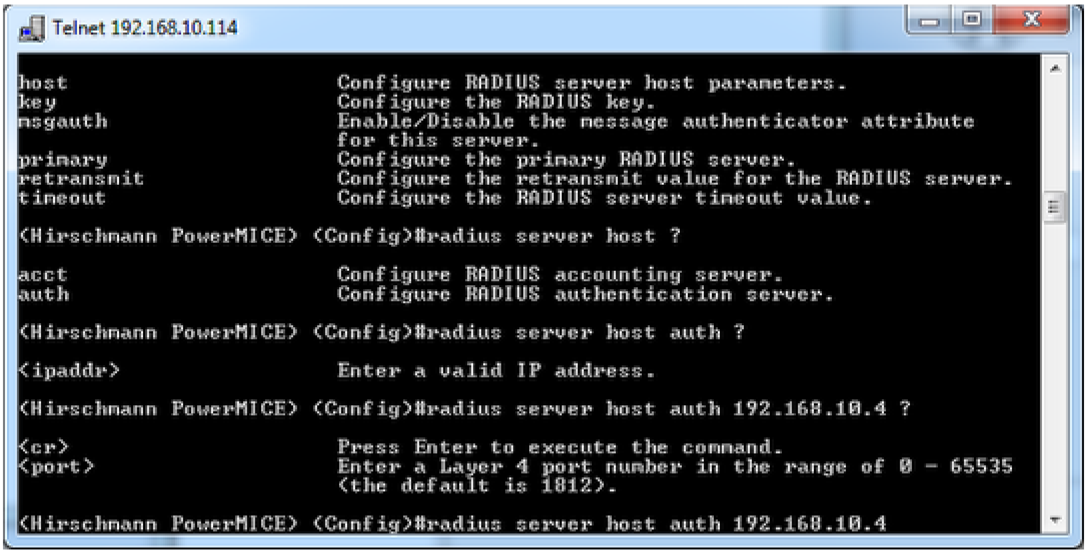
Address	UDP Port	Shared Secret	Primary Server	Selected Server
192.168.10.103	[illegible]	testino123	☐	☑

1.) Click on "Create" and enter IP-address of Radius-Server.

2.) Configure "Shared Secret". Please note that this field will be empty after the next step because of security reasons.

3.) Click on "Set" in order to send new configuration to switch agent.

Optional: Configuration via CLI



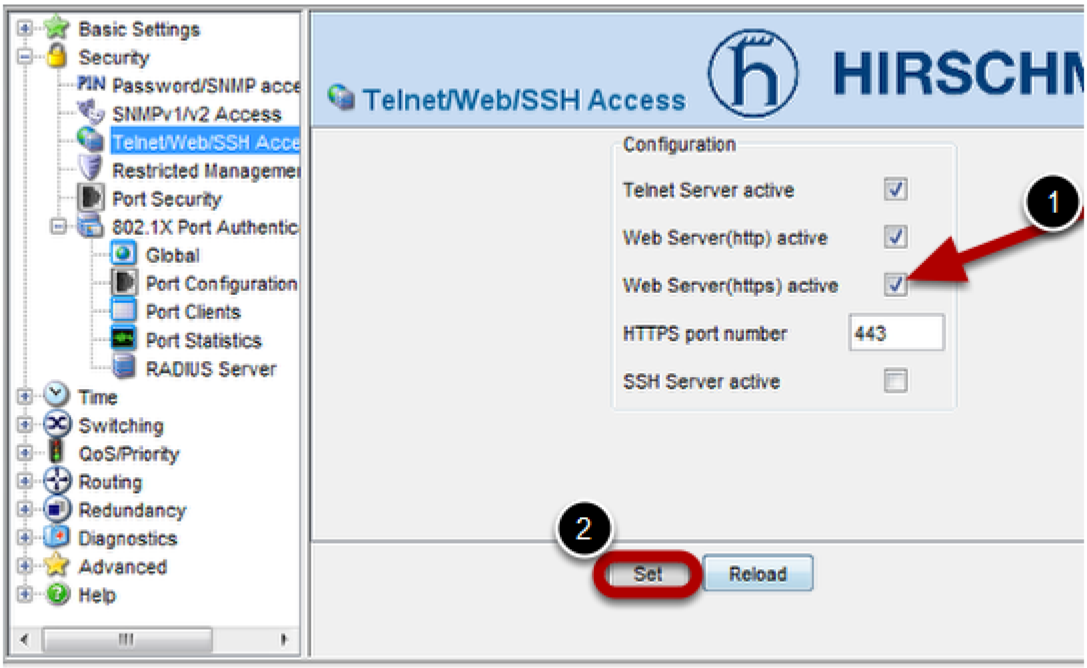
```
host                     Configure RADIUS server host parameters.
key                      Configure the RADIUS key.
msgauth                  Enable/Disable the message authenticator attribute
                         for this server.
primary                  Configure the primary RADIUS server.
retransmit               Configure the retransmit value for the RADIUS server.
timeout                  Configure the RADIUS server timeout value.

(Hirschmann PowerMICE) (Config)#radius server host ?

acct                     Configure RADIUS accounting server.
auth                     Configure RADIUS authentication server.

(Hirschmann PowerMICE) (Config)#radius server host auth ?

<ipaddr>                 Enter a valid IP address.

(Hirschmann PowerMICE) (Config)#radius server host auth 192.168.10.4 ?

<cr>                     Press Enter to execute the command.
<port>                   Enter a Layer 4 port number in the range of 0 - 65535
                         (the default is 1812).

(Hirschmann PowerMICE) (Config)#radius server host auth 192.168.10.4
```

Pleae use following command:

radius server host auth 192.168.10.4

radius server key auth 192.168.10.4

Enable HTTPS



Configuration

Telnet Server active ☑

Web Server(http) active ☑

Web Server(https) active ☑

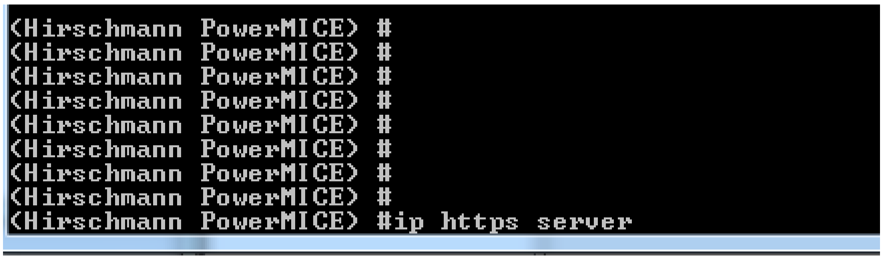
HTTPS port number 443

SSH Server active ☐

It is necessary to enable HTTPS in order to use radius for access switch agent via WEB-interface.

1.) Enable HTTPS
2.) Click on "**Set**" in order to send new configuration to switch agent.

Optional: Configuration via CLI



```
(Hirschmann PowerMICE) #
(Hirschmann PowerMICE) #
(Hirschmann PowerMICE) #
(Hirschmann PowerMICE) #
(Hirschmann PowerMICE) #
(Hirschmann PowerMICE) #
(Hirschmann PowerMICE) #
(Hirschmann PowerMICE) #
(Hirschmann PowerMICE) #ip https server
```

Please use following command:

ip https server

Please note that this command is used in enable mode, not in configure mode.

More CLI commands

After above steps all non local configured users will be authenticated by radius-server. All local configured users (like "admin" and "user") will be authenticated by local switch database.

More modifications are possible by using so named "Authentication Lists". Following commands will be helpful:

Show Authentication Lists per user
show users authentication

Show Authentication List definition
show authentication

Change preconigured Authentication List named "radiuslist".
After this modificatiion all users will be authenticated by radius server, and only if configured server is not available local database will be used.

authentication login radiuslist radius local

Configuration of Authentication List used for all non local users.

users defaultlogin <listname>