

Base de connaissances > Products > Classic Switches > How to use Radius authentication to access switch management

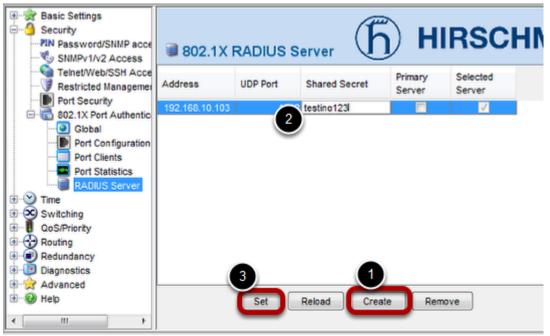
How to use Radius authentication to access switch management

- 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



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

ost	Configure RADIUS server host parameters.
ey sgauth	Configure the RADIUS key. Enable/Disable the message authenticator attribute
Isgauen	for this server.
rimary	Configure the primary RADIUS server.
etransmit imeout	Configure the retransmit value for the RADIUS server. Configure the RADIUS server timeout value.
THEORE	configure the Ampios server timeout value.
Hirschmann PowerMICE)	(Config)#radius server host ?
lect	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).

Pleae use following command:

radius server host auth 192.168.10.4 radius server key auth 192.168.10.4

Enable HTTPS

Basic Settings Security PIN Password/SNMP acce SNMPv1/v2 Access	
TeinetWeb/SSH Acce Restricted Managemen Port Security 802.1X Port Authentic Blobal Port Configuration Port Clients Port Statistics RADIUS Server	Configuration Telnet Server active Web Server(http) active Web Server(https) active HTTPS port number SSH Server active
Switching QoS/Priority QoS/Priority Routing Redundancy Joagnostics Advanced Help III	2 Set Reload

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

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

Optional: Configuration via CLI

(Hirschmann	PowerMICE)	#			
(Hirschmann					
(Hirschmann			https	Seblieb	
CH II S CHHam	TOWOTHIOL/	штр	neeps	301 401	

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>**