

MACMON NAC WHITE PAPER

Logging in to Hirschmann Switches
with RADIUS Authentication

Contents

1 Introduction.....	2
2 Supported network devices from Hirschmann Automation and Control GmbH.....	3
3 Configuration steps on network devices.....	3
3.1 Configuration for devices with HiOS and HiSecOS.....	3
3.1.1 Configuration in the web GUI	3
3.1.2 Quick configuration via command line interface (CLI)	4
3.2 Configuration for devices with Classic OS via the command line interface (CLI).....	4
3.3 Configuration for devices with Classic Firewall software via the command line interface (CLI).....	5
4 Configuration in macmon NAC.....	6
4.1 Basic requirements.....	6
4.2 Create and bind the RADIUS credentials.....	6
4.3 Creating a RADIUS permission.....	7
4.4 Creating a RADIUS rule	9
Contact at Hirschmann.....	10
Contact.....	10

Version: 1.0

1 Introduction

To access the web interface or [command line interface \(CLI\)](#) of Hirschmann managed switches and firewalls, the user must first be [authenticated](#) and [authorized](#).

[Authentication](#) can be performed either using the [local user management](#) on the switch or firewall itself, or via a centralized **RADIUS Server**.

Centralized user management offers significant benefits, for example:

- Increased security by [avoiding standard user names and passwords](#)
- Increased security due to [centralized password policies](#)
- Increased security due to the ability to [respond rapidly in the event of user name/password disclosure](#) or the [locking out of unwanted users](#)
- Convenient [adding/deletion of users](#) and [easy changing of passwords](#)

macmon NAC can use the [integrated RADIUS Server](#) to perform [central user management](#) and authorize users based on the [configured policies](#).

This guide describes the setup steps necessary to provide this function for switches and firewalls from [Hirschmann Automation and Control GmbH](#) in conjunction with **macmon NAC**. The switches and firewalls are configured so that [authentication](#) and [RADIUS authorization](#) take place first. As a fallback method, if communication with the **RADIUS Server** is not possible, the [locally configured "admin" user](#) can be used for [authentication](#).

NOTE: The feature described here is only available in **macmon NAC** with a [license](#) for the **Switch Viewer** module!



2 Supported network devices from Hirschmann Automation and Control GmbH

- Switch models with the HiOS operating system and software levels L2E, L2S, L2A, L3S, L3A
- Switch models with the Classic OS operating system and software levels L2P, L3E, L3P
- Firewall models with the HiSecOS operating system (e.g. EAGLE30 or EAGLE40)
- Firewall models with the Classic Firewall operating system (e.g. EAGLE One)

3 Configuration steps on network devices

3.1 Configuration for devices with HiOS and HiSecOS

3.1.1 Configuration in the web GUI

Since **RADIUS authentication** is performed with **macmon NAC**, **macmon** must be entered as the **RADIUS Server**. The configured **secret** is used later for the **RADIUS credentials** in **macmon**.

Menu item: *Network Security → RADIUS → Authentication Server*

<input type="checkbox"/>	Index	Name	Address	Destination UDP port	Secret	Primary server	Active
<input type="checkbox"/>	1	macmon	10.10.210.10	1,812	*****	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

If several **RADIUS Servers** are configured, the **index** decides the order in which the **RADIUS Servers** are addressed. If several **RADIUS Servers** have the same name, the server with the **Primary Server** checkbox selected is addressed first.

Connection statistics can be retrieved from the menu item *Network Security → RADIUS → Authentication Statistics*.

The next step is to check whether the **admin local user** has been set up and is active.

The **role/permission** and password configured here apply only if the user is authenticated locally after a **RADIUS timeout**.

Menu item: *Device Security → User Management*

<input type="checkbox"/>	User name	Active	Password	Role	User locked	Policy check	SNMP auth type	SNMP auth password	SNMP encryption type	SNMP encryption password
<input type="checkbox"/>	admin	<input checked="" type="checkbox"/>	*****	administrator	<input type="checkbox"/>	<input type="checkbox"/>	hmacmd5	*****	des	*****

In order to implement the **switch login** with verification against the **RADIUS Server**, the default **authentication lists** must be adapted. An **authentication list** defines in which application the authentication is to be performed, with which methods, and in which order.

In this example, we will configure **RADIUS** as the first method and **local authentication** as the second method for both **login via telnet**, **web interface** or **SSH** (defaultLogin-AuthList), and via the **console port** (defaultV24AuthList).

Menu item: [Device Security](#) → [Authentication List](#)

<input type="checkbox"/>	Name	Policy 1	Policy 2	Policy 3	Policy 4	Policy 5	Dedicated applications	Active	
<input type="checkbox"/>	defaultDot1x8021AuthList	radius	reject	reject	reject	reject	8021x	✓	
<input type="checkbox"/>	defaultLoginAuthList	radius	local	reject	reject	reject	SSH,Telnet,WebInterface	✓	
<input type="checkbox"/>	defaultV24AuthList	radius	local	reject	reject	reject	Console(V24)	✓	

3.1.2 Quick configuration via command line interface (CLI)

```
enable
configure
radius server auth add 1 ip 10.10.210.10
radius server auth modify 1 name macmon primary enable status enable secret *****
authlists set-policy defaultLoginAuthList radius local reject reject reject
authlists set-policy defaultV24AuthList radius local reject reject reject
```

3.2 Configuration for devices with Classic OS via the command line interface (CLI)

For devices with [Classic OS](#), the configuration is done in the [CLI](#). To set the appropriate commands, the [CLI](#) must be in [Configure mode](#).

macmon NAC is entered as the **RADIUS Server** and the [shared secret](#) is defined:

```
radius server host auth <IP-address of macmon appliance>
radius server primary <IP-address of macmon appliance>
radius server key auth <IP-address of macmon appliance>
Enter secret (25 characters max): *****
Re-enter secret: *****
```

The next step is to check whether the [admin local user](#) exists:

```
show users
```

User Name	User Access Mode	SNMPv3 Access Mode	SNMPv3 Authentication	SNMPv3 Encryption
admin	Read/Write	Read/Write	MD5	DES

In the [Classic OS](#), two [authentication lists](#) are predefined:

```
show authentication
```

Authentication Login List	Method 1	Method 2	Method 3
defaultList	local	undefined	undefined
radiuslist	radius	reject	reject

The [defaultList](#) only allows [local authentication](#) and is automatically preconfigured for all locally configured users (here [admin](#)). This [defaultList](#) cannot be modified.

By default, the [radiuslist](#) only allows [authentication via RADIUS](#) and is applied to all unknown (not locally configured) users.

To force the [admin local user](#) to [authenticate via RADIUS](#), this user must be bound to the [radiusList](#). A warning message is issued!

```
users login admin radiuslist
```

Note: when assigning a list to the 'admin' account, include an authentication method that allows administrative access even when remote authentication is unavailable.

Now you still have to [locally](#) configure the [radiuslist](#) as the [second authentication method](#).

```
(Config)#authentication login radiuslist radius local reject
```

```
show authentication
```

Authentication Login List	Method 1	Method 2	Method 3
defaultList	local	undefined	undefined
radiuslist	radius	local	reject

3.3 Configuration for devices with Classic Firewall software via the command line interface (CLI)

For devices with [Classic Firewall software](#), the configuration is done in the [CLI](#). To set the appropriate commands, the [CLI](#) must be in [Configure mode](#).

macmon NAC is entered as the **RADIUS Server** and the [shared secret](#) is defined:

```
!*(Hirschmann Eagle One) (config)#radius server 1 modify ip-address <ip-address> secret <shared secret>
!*(Hirschmann Eagle) (config)#radius server 1 status enable
```

The next step is to check whether the [admin local user](#) exists:

```
!*(Hirschmann EAGLE One) #show users
```

User Name	User Access Mode	SNMPv3 Authentication	SNMPv3 Encryption	User Active
admin	Read/Write	MD5	DES	Yes

In the [Classic Firewall software](#), two authentication lists are predefined:

```
!*(Hirschmann EAGLE One) #show authentication
```

Authentication Login List	Method 1	Method 2	Method 3	Status
systemLoginDefaultList	local	none	none	active
userFirewallLoginDefaultList	local	none	none	active

By default, the [systemLoginDefaultList](#) only allows [local authentication](#) and is automatically preconfigured for all [locally configured users](#) (here [admin](#)).

This `systemLoginDefaultList` is modified to use `RADIUS` as the **first authentication method** and `local` as the **second method**.

```
!(Hirschmann EAGLE One) (config)#authentication login systemLoginDefaultList set radius local
```

```
!(Hirschmann EAGLE One) #show authentication
Authentication Login List
-----
systemLoginDefaultList      radius    local    none     active
userFirewallLoginDefaultList local     none     none     active
```

In order for this **modified authentication list** to be used also for unknown, i.e. **not locally configured users**, this must still be defined as a **default list for unknown users**:

```
!(Hirschmann EAGLE One) (config)#authentication login systemLoginDefaultList default
```

4 Configuration in macmon NAC

4.1 Basic requirements

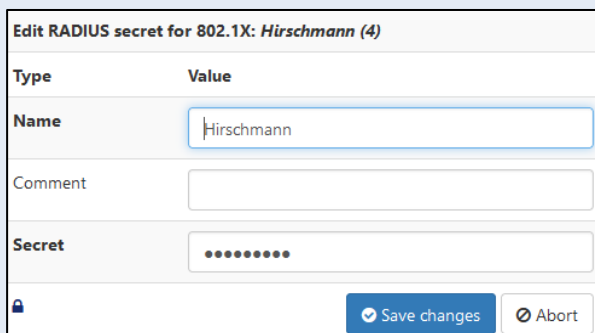
The **macmon appliance** has an **integrated RADIUS Server** which can receive and respond to the **RADIUS requests** from the **Hirschmann network devices** according to the **macmon policies**. Before the following steps can be carried out, these basic requirements must be met in macmon:

- The Hirschmann devices must be created as network devices in macmon
- The Active Directory identity store must be integrated
- You must install a license file that includes the Switch Viewer module

4.2 Create and bind the RADIUS credentials

Menu item: *Settings* → *Credentials*

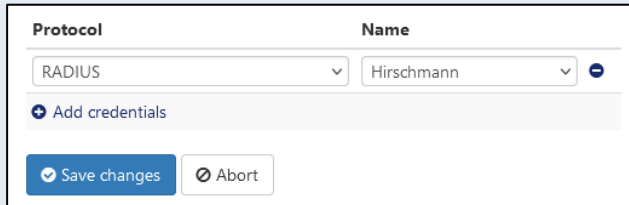
The **"Create credentials"** pulldown menu is used to create **"RADIUS secret"** credentials. In this case, enter the **RADIUS secret** configured on the respective **Hirschmann device**.



Type	Value
Name	<input type="text" value="Hirschmann"/>
Comment	<input type="text"/>
Secret	<input type="password" value="....."/>

Menu item: [Network](#) → [Network devices](#) → [Hirschmann device](#) → [Action](#) → [Edit](#)

This link opens the [configuration menu for the network device](#). At the bottom, use the “[Add credentials](#)” button to add the created [RADIUS credentials](#) and save the configuration. Alternatively, the [RADIUS credentials](#) can also be bound to a [network device group](#).



4.3 Creating a RADIUS permission

Hirschmann supports special [RADIUS attributes](#) in order to be able to pass on a [defined permission](#) for the logged-in [switch user](#). These [RADIUS attributes](#) are sent to the switch by **macmon NAC**. The [switch user](#) is given the corresponding permissions for the device’s GUI once [authentication](#) is successful. The following [RADIUS attributes](#) are supported.

Note that [HiOS/HiSecOS](#) currently only supports attributes for the [user roles](#) [Guest](#), [Operator](#) and [Administrator](#).

HIOS/HiSecOS

Role	Service type	Value	Permission
Guest	NAS prompt	7	Read only
Operator	Login	1	Write, without security settings
Administrator	Administrative	6	Write, including security settings

Classic OS/Classic Firewall

Right	Service type	Value	Permission
Read-only	NAS prompt	7	Read only
Read-write	Administrative	6	Write

Menu item: [Policies](#) → [RADIUS \(non NAC\)](#) → [Permission](#)

The **Add permission** button creates a [new permission](#). A successful authorization is guaranteed by the value **True/Yes** in the **Authorized** field. The **Add element** button selects the **Service-Type** [attribute](#). In the **Value** field, select the desired [permission](#) in the switch's GUI (see above). We recommend that you choose a descriptive [name](#) for the [RADIUS permission](#) that includes the [role](#).

AuthenticationRulesPermissions

AttributesValue

Name

admin_user

Common

AttributeValue

Authorized *

✓ True / Yes

RADIUS attributes

AttributeValue

Service-Type

✓ 6

+ Add element

Required parameters are marked with an asterisk (*)

✓ Save changes

✗ Abort

4.4 Creating a RADIUS rule

Menu item: Policies → RADIUS (non NAC) → Rules

A **rule** links **authorized users** with the **previously created RADIUS permission**. Clicking the button **Add rule** creates a new **rule**. The **Condition** field defines the **authorized users**. For example, you might want to enter an **Active Directory** group. That is the only real benefit of this function. The rule is dynamic, and changes to the **AD group** automatically affect the **authorization when logging in** to the **Hirschmann devices**.

In the **Assign permission** field, the name of the previously created **RADIUS permission** is selected.

Authentication

Rules

Permissions

◀ Back to rule list

Action ▾

Create rule

Name

Switch_Login_Hirschmann

Description

Active

☒

Conditions

AND

☒ User

Identity store groups

Contains

(

"SwitchAdmins"

)

Assign permission

admin_user

Contact at Hirschmann

Hirschmann Automation and Control GmbH
Stuttgarter Strasse 45-51
72654 Neckartenzlingen, Germany

Phone: +49-7127-14-0

Website: <https://www.belden.com/support/technical-product-support-main>

www.beldensolutions.com

www.blog.beldensolutions.com

Contact

macmon secure GmbH
Alte Jakobstraße 79-80 | 10179 Berlin | Germany

Phone.: +49 (0) 30 23 25 777 – 0
nac@macmon.eu

www.macmon.eu