

MACMON NAC WHITEPAPER

User-Login mit RADIUS-Authentifizierung
an Switches des Herstellers Hirschmann

Inhalt

1 Einleitung.....	2
2 Unterstützte Netzwerkgeräte des Herstellers Hirschmann Automation and Control GmbH.....	3
3 Konfigurationsschritte auf den Netzwerkgeräten.....	3
3.1 Konfiguration für Geräte mit HiOS und HiSecOS	3
3.1.1 Konfiguration über Web-GUI	3
3.1.2 Schnell-Konfiguration über Command Line Interface (CLI).....	4
3.2 Konfiguration für Geräte mit Classic-OS über das Command Line Interface (CLI).....	4
3.3 Konfiguration für Geräte mit Classic-Firewall Software über das Command Line Interface (CLI)	5
4 Konfiguration in macmon NAC	6
4.1 Grundvoraussetzungen	6
4.2 Erstellen und binden der RADIUS-Credentials	6
4.3 Erstellen einer RADIUS-Berechtigung	7
4.4 Erstellen einer RADIUS-Regel	9
Kontakt bei Hirschmann.....	10
Kontakt.....	10

Version: 1.0

1 Einleitung

Der Zugriff auf das Web-Interface oder das [Command Line Interface \(CLI\)](#) der [Managed Hirschmann Switches und Firewalls](#) erfordert eine vorherige [Authentifizierung](#) und [Autorisierung](#) des entsprechenden Benutzers.

Diese [Authentifizierung](#) kann entweder über das [lokale Benutzermanagement](#) auf dem jeweiligen Switch oder der Firewall selbst erfolgen oder aber zentralisiert über einen [RADIUS-Server](#).

Eine zentrale Benutzerverwaltung bietet erhebliche Vorteile, wie z.B.

- Höhere Sicherheit durch [Vermeidung von Standard-Logins und Passwörtern](#)
- Höhere Sicherheit durch [zentrales Erzwingen von Passwort-Richtlinien](#)
- Höhere Sicherheit durch [schnelle Reaktion bei einer Login-/Passwort-Offenlegung](#) oder beim [Aussperren unerwünschter Nutzer](#)
- Komfortables [Hinzufügen/Löschen von Benutzern](#) sowie [einfache Änderung von Passwörtern](#)

macmon NAC kann mit Hilfe des [integrierten RADIUS-Servers](#) die Aufgabe der [zentralen Benutzerverwaltung](#) übernehmen und Benutzer auf Basis des [konfigurierten Regelwerkes](#) autorisieren.

Dieser Leitfaden beschreibt, welche Einrichtungsschritte notwendig sind, um diese Funktion für Switches und Firewalls des Herstellers [Hirschmann Automation and Control GmbH](#) mit **macmon NAC** bereitzustellen. Die Switches und Firewalls werden so konfiguriert, dass in einem ersten Schritt die [Authentifizierung](#) und [Autorisierung über Radius](#) erfolgen soll. Als Fallback-Methode, falls die Kommunikation mit dem [Radius-Server](#) nicht möglich ist, erfolgt die [Authentifizierung](#) über den [lokal konfigurierten Benutzer „admin“](#).

HINWEIS: Die hier beschriebene Funktion ist in **macmon NAC** ausschließlich mit der [Lizenz für das Modul Switch-Viewer](#) verfügbar!



2 Unterstützte Netzwerkgeräte des Herstellers Hirschmann Automation and Control GmbH

- Switch-Modelle mit dem Betriebssystem HiOS und den Software-Levels L2E, L2S, L2A, L3S, L3A
- Switch-Modelle mit dem Betriebssystem Classic-OS und den Software-Levels L2P, L3E, L3P
- Firewall-Modelle mit dem Betriebssystem HiSecOS (z.B. EAGLE30 oder EAGLE40)
- Firewall-Modelle mit dem Betriebssystem Classic-Firewall (z.B. EAGLE One)

3 Konfigurationsschritte auf den Netzwerkgeräten

3.1 Konfiguration für Geräte mit HiOS und HiSecOS

3.1.1 Konfiguration über Web-GUI

Da die RADIUS-Authentifizierung mit **macmon NAC** durchgeführt wird, muss **macmon** als **RADIUS-Server** hinterlegt werden. Das konfigurierte **Secret** wird später für die RADIUS-Zugangsdaten in **macmon** verwendet.

Menüpunkt: *Network Security (Netzsicherheit) → RADIUS → Authentication Server*

☐	Index	Name	Address	Destination UDP port	Secret	Primary server	Active
☐	1	macmon	10.10.210.10	1,812	*****	☒	☒

Werden mehrere **RADIUS-Server** konfiguriert, entscheidet der **Index** darüber, in welcher Reihenfolge die **RADIUS-Server** angesprochen werden. Werden mehrere **RADIUS-Server** mit dem gleichen Namen versehen, entscheidet der aktivierte Haken bei **Primary Server (Primärer Server)** darüber, welcher Server innerhalb dieser Gruppe zuerst angesprochen wird.

Verbindungstatistiken können über den Menüpunkt *Network Security (Netzsicherheit) → RADIUS → Authentication Statistics (Authentication-Statistiken)* abgerufen werden.

Im nächsten Schritt wird überprüft, ob der **lokale Benutzer admin** eingerichtet wurde und aktiv ist. Die hier konfigurierte **Rolle/Berechtigung** und das Passwort gelten nur, wenn der Benutzer nach einem **RADIUS-Timeout** lokal authentifiziert wird.

Menüpunkt: *Device Security (Gerätesicherheit) → User Management (Benutzerverwaltung)*

☐	User name	Active	Password	Role	User locked	Policy check	SNMP auth type	SNMP auth password	SNMP encryption type	SNMP encryption password
☐	admin	☒	*****	administrator	☐	☐	hmacmd5	*****	des	*****

Um das **Switch-Login** mit Prüfung gegen den **RADIUS-Server** zu realisieren, müssen die standardmäßig verwendeten **Authentifizierungslisten** angepasst werden. In einer **Authentifizierungsliste** wird definiert, bei welcher Applikation die Authentifizierung mit welchen Methoden in welcher Reihenfolge ausgeführt werden soll.

In diesem Beispiel werden wir sowohl für den **Login über Telnet, Web-Interface oder SSH (defaultLogin-AuthList)**, als auch über den **Konsolenport (defaultV24AuthList)**, als erste Methode **RADIUS** konfigurieren und als zweite Methode die **lokale Authentifizierung**.

Menüpunkt: *Device Security (Gerätesicherheit) → Authentication List (Authentifizierungs-Liste)*

☐	Name	Policy 1	Policy 2	Policy 3	Policy 4	Policy 5	Dedicated applications	Active
☐	defaultDot1x8021AuthList	radius	reject	reject	reject	reject	8021x	✓
☐	defaultLoginAuthList	radius	local	reject	reject	reject	SSH,Telnet,WebInterface	✓
☐	defaultV24AuthList	radius	local	reject	reject	reject	Console(V24)	✓

3.1.2 Schnell-Konfiguration über 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 Konfiguration für Geräte mit Classic-OS über das Command Line Interface (CLI)

Bei Geräten mit [Classic-OS](#) erfolgt die Konfiguration über das [CLI](#). Um die passenden Befehle setzen zu können, muss sich das [CLI](#) im [Configure-Mode](#) befinden.

macmon NAC wird als **RADIUS-Server** hinterlegt und das [Shared-Secret](#) wird definiert:

```
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: *****
```

Als nächstes wird überprüft, ob der [lokale Benutzer admin](#) existiert:

```
show users
```

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

Im [Classic-OS](#) sind zwei [Authentifizierungslisten](#) voreingestellt:

```
show authentication
```

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

Die [defaultList](#) erlaubt nur eine [lokale Authentifizierung](#) und ist automatisch für alle lokal konfigurierten Benutzer (hier [admin](#)) vorkonfiguriert. Diese [defaultList](#) kann nicht modifiziert werden.

Die [radiusList](#) erlaubt standardmäßig nur die [Authentifizierung über RADIUS](#) und wird für alle unbekannten (nicht lokal konfigurierten) Benutzer angewendet.

Um nun für den [lokalen Benutzer admin](#) die [Authentifizierung über RADIUS](#) zu erzwingen, muss dieser Benutzer an die [radiusList](#) gebunden werden. Es erfolgt eine Warnmeldung!

```
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.

Nun muss für die [radiusList](#) als [zweite Authentifizierungsmethode](#) noch [local](#) konfiguriert werden.

```
(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 Konfiguration für Geräte mit Classic-Firewall Software über das Command Line Interface (CLI)

Bei Geräten mit [Classic-Firewall Software](#) erfolgt die Konfiguration über das CLI. Um die passenden Befehle setzen zu können, muss sich das CLI im [Configure-Mode](#) befinden.

macmon NAC wird als [RADIUS-Server](#) hinterlegt und das [Shared-Secret](#) wird definiert:

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

Als nächstes wird überprüft, ob der [lokale Benutzer admin](#) existiert:

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

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

In der [Classic-Firewall Software](#) sind [zwei Authentifizierungslisten](#) voreingestellt:

```
!*(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

Die [systemLoginDefaultList](#) erlaubt standardmäßig nur eine [lokale Authentifizierung](#) und ist automatisch für alle [lokal konfigurierten Benutzer](#) (hier [admin](#)) vorkonfiguriert.

Diese `systemLoginDefaultList` wird so modifiziert, dass als **erste Authentifizierungs-Methode** `RADIUS` und als **zweite Methode** `local` verwendet wird.

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

```
!*(Hirschmann EAGLE One) #show authentication
Authentication Login List      Method 1  Method 2  Method 3  Status
-----
systemLoginDefaultList      radius    local     none      active
userFirewallLoginDefaultList local     none      none      active
```

Damit diese **modifizierte Authentifizierungsliste** auch für unbekannte, d.h. **nicht lokal konfigurierte Benutzer** verwendet wird, muss diese noch als **Default-Liste für unbekannte Benutzer** definiert werden:

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

4 Konfiguration in macmon NAC

4.1 Grundvoraussetzungen

Die **macmon-Appliance** besitzt einen **integrierten RADIUS-Server**, welcher die **RADIUS-Anfragen** der **Hirschmann-Netzwerkgeräte** entgegennehmen und auf Grundlage des **macmon-Regelwerks** beantworten kann.

Bevor die nachfolgenden Schritte durchgeführt werden können, müssen zuvor diese Grundvoraussetzungen in macmon erfüllt worden sein:

- Anlegen der Hirschmann-Geräte als Netzwerkgeräte in macmon
- Einbinden der Identitätsquelle Active Directory
- Installation einer Lizenzdatei, welche das Switch-Viewer-Modul beinhaltet

4.2 Erstellen und binden der RADIUS-Credentials

Menüpunkt: *Settings* → *Credentials*

Über das Pulldown-Menü "**Create credentials**" werden Zugangsdaten vom Typ "**RADIUS-Secret**" angelegt. Hierbei wird das auf dem jeweiligen **Hirschmann-Gerät** konfigurierte **RADIUS-Secret** eingetragen.

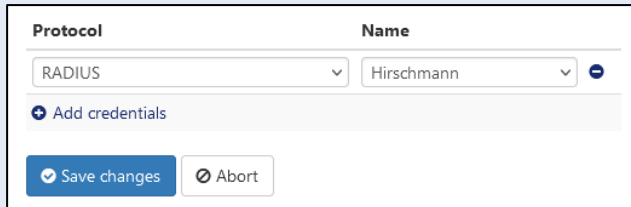
Edit RADIUS secret for 802.1X: Hirschmann (4)

Type	Value
Name	Hirschmann
Comment	
Secret	



Menüpunkt: [Network](#) → [Network devices](#) → [Hirschmann-Gerät](#) → [Action](#) → [Edit](#)

Über diesen Link wird das [Konfigurationsmenü des Netzwerkgerätes](#) aufgerufen. Im unteren Bereich, über die Schaltfläche "[Add credentials](#)", die erstellten [RADIUS-Zugangsdaten](#) hinzufügen und die Konfiguration speichern. Alternativ können die [RADIUS-Zugangsdaten](#) auch an eine [Netzwerkgerätegruppe](#) gebunden werden.



4.3 Erstellen einer RADIUS-Berechtigung

Hirschmann unterstützt spezielle [RADIUS-Attribute](#), um eine [definierte Berechtigung](#) für den angemeldeten [Switch-User](#) übergeben zu können. Diese [RADIUS-Attribute](#) werden von **macmon NAC** an den Switch gesendet. Der [Switch-User](#) erhält bei [erfolgreicher Authentifizierung](#) die entsprechende Berechtigung an der Benutzeroberfläche des Gerätes. Folgende [RADIUS-Attribute](#) werden unterstützt.

Zu beachten ist, dass on [HiOS/HiSecOS](#) zurzeit nur Attribute für die [Benutzerrollen](#) [Guest](#), [Operator](#) und [Administrator](#) unterstützt werden.

HiOS/HiSecOS

Rolle	Service-Type	Wert	Berechtigung
Guest	NAS Prompt	7	nur lesend
Operator	Login	1	schreibend, ohne Sicherheitseinstellungen
Administrator	Administrative	6	schreibend, auch Sicherheitseinstellungen

Classic-OS/Classic Firewall

Recht	Service-Type	Wert	Berechtigung
Read-only	NAS Prompt	7	nur lesend
Read-Write	Administrative	6	schreibend

Menüpunkt: Policies → RADIUS (non NAC) → Permission

Über die Schaltfläche **Add permission** wird eine **neue Berechtigung** erstellt. Eine erfolgreiche Autorisation gewährleistet der Wert **True/Yes** im Feld **Authorized**. Über die Schaltfläche **Add element** wird das **Attribut Service-Type** ausgewählt. Der zu setzende Wert im Feld **Value** entspricht der gewünschten **Berechtigung** an der Benutzeroberfläche des Switches (siehe oben). Es empfiehlt sich einen **sprechenden Namen** für die **RADIUS-Berechtigung** zu wählen, welcher die **Rolle** beinhaltet.

Authentication

Rules

Permissions

Attributes	Value
Name	admin_user

Common

Attribute	Value
Authorized *	☒ True / Yes

RADIUS attributes

Attribute	Value
Service-Type	☒ 6

[Add element](#)

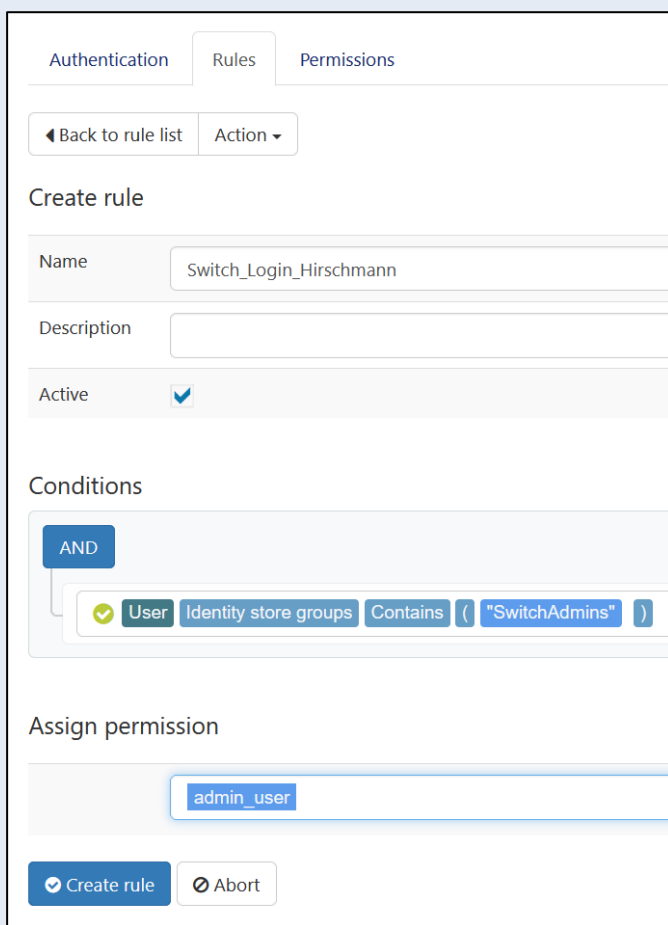
Required parameters are marked with an asterisk (*)

4.4 Erstellen einer RADIUS-Regel

Menüpunkt: Policies → RADIUS (non NAC) → Rules

Über eine **Regel** werden **berechtigte User** mit der **zuvor erstellten RADIUS-Berechtigung** verknüpft. Ein Klick auf den Button **Add rule** erstellt eine neue **Regel**. Im Feld **Condition** werden die **berechtigten User** definiert. Hier empfiehlt es sich z. B. eine Gruppe des **Active Directory** zu hinterlegen. Damit wird der große Vorteil dieser Funktion ausgeschöpft. Die Regel ist dynamisch und Änderungen an der **AD-Gruppenmitgliedschaft** wirken sich automatisch auf die **Berechtigung beim Login** an den **Hirschmann-Geräten** aus.

Im Feld **Assign permission** wird der Namen der zuvor erstellen **RADIUS-Berechtigung** ausgewählt.



The screenshot shows the 'Create rule' form in the macmon interface. The form is divided into three tabs: 'Authentication', 'Rules' (selected), and 'Permissions'. Below the tabs are two buttons: 'Back to rule list' and 'Action'. The 'Create rule' section contains a 'Name' field with the value 'Switch_Login_Hirschmann', a 'Description' field, and an 'Active' checkbox which is checked. The 'Conditions' section shows a logical operator 'AND' followed by a condition: 'User Identity store groups Contains ("SwitchAdmins")'. The 'Assign permission' section has a dropdown menu with 'admin_user' selected. At the bottom are two buttons: 'Create rule' and 'Abort'.

Kontakt bei Hirschmann

Hirschmann Automation and Control GmbH
Stuttgarter Straße 45-51
72654 Neckartenzlingen

Telefon: +49-7127-14-0

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

www.beldensolutions.com

www.blog.beldensolutions.com

Kontakt

macmon secure GmbH
Alte Jakobstraße 79-80 | 10179 Berlin

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

www.macmon.eu