

APPLICATION NOTE

FOXMAN-UN

FreeRADIUS Integration

Document ID	1KHW029093	
Document edition	System Release:	R18
	Revision:	A
	Date:	2025-06-05

Copyright and confidentiality

Copyright in this document vests in Hitachi Energy.

Manuals and software are protected by copyright. All rights reserved. The copying, reproduction, translation, conversion into any electronic medium or machine scannable form is not permitted, either in whole or in part. The contents of the manual may not be disclosed by the recipient to any third party, without the prior written agreement of Hitachi Energy. An exception is the preparation of a backup copy of the software for your own use. For devices with embedded software, the end-user license agreement provided with the software applies.

This document may not be used for any purposes except those specifically authorized by contract or otherwise in writing by Hitachi Energy.

Disclaimer

This document contains information about one or more Hitachi Energy products and may include a description of or a reference to one or more standards that may be generally relevant to the Hitachi Energy products. The presence of any such description of a standard or reference to a standard is not a representation that all the Hitachi Energy products referenced in this document support all the features of the described or referenced standard. In order to determine the specific features supported by a particular Hitachi Energy product, the reader should consult the product specifications for that Hitachi Energy product. In no event shall Hitachi Energy be liable for direct, indirect, special, incidental, or consequential damages of any nature or kind arising from the use of this document, nor shall Hitachi Energy be liable for incidental or consequential damages arising from the use of any software or hardware described in this document.

Hitachi Energy may have one or more patents or pending patent applications protecting the intellectual property in the Hitachi Energy products described in this document. The information in this document is subject to change without notice and should not be construed as a commitment by Hitachi Energy. Hitachi Energy assumes no responsibility for any errors that may appear in this document.

All people responsible for applying the equipment addressed in this manual must satisfy themselves that each intended application is suitable and acceptable, including compliance with any applicable safety or other operational requirements. Any risks in applications where a system failure and/or product failure would create a risk for harm to property or persons (including but not limited to personal injuries or death) shall be the sole responsibility of the person or entity applying the equipment, and those so responsible are hereby requested to ensure that all measures are taken to exclude or mitigate such risks.

Products described or referenced in this document are designed to be connected and to communicate information and data through network interfaces, which should be connected to a secure network. It is the sole responsibility of the system/product owner to provide and continuously ensure a secure connection between the product and the system network and/or any other networks that may be connected.

The system/product owners must establish and maintain appropriate measures, including, but not limited to, the installation of firewalls, application of authentication measures, encryption of data, installation of antivirus programs, and so on, to protect these products, the network, its system, and interfaces against security breaches, unauthorized access, interference, intrusion, leakage, and/or theft of data or information.

Hitachi Energy performs functionality testing on released products and updates. However, system/product owners are ultimately responsible for ensuring that any product updates or other major system updates (to include but not limited to code changes, configuration file changes, third-party software updates or patches, hardware change out, and so on) are compatible with the security measures implemented. The system/product owners must verify that the system and associated products function as expected in the environment in which they are deployed. Hitachi Energy and its affiliates are not liable for damages and/or losses related to security breaches, any unauthorized access, interference, intrusion, leakage, and/or theft of data or information.

This document and parts thereof must not be reproduced or copied without written permission from Hitachi Energy, and the contents thereof must not be imparted to a third party nor used for any unauthorized purpose.

Contents

1 Purpose and Scope	4
2 Configure FOXMAN-UN	5
3 Configure PAM for RADIUS authentication module on FOXMAN-UN server.	6

1 Purpose and Scope

This application note describes how to set up the Pluggable Authentication Modules (PAM) to allow the FOXMAN-UN server to become a FreeRADIUS client for authentication requests to a FreeRADIUS Server.

2 Configure FOXMAN-UN

FOXMAN-UN shall be configured as follows for use of users/passwords for RADIUS authenticated users.



Please note:

“nemadm” in the scope of the feature described in this document is a default username used for RADIUS settings only. It is not related to the “nemadm” user who is the owner of FOXMAN-UN processes and files.

FOXMAN-UN needs two user classes for access to the node: Manager and Session Manager. For this access FOXMAN-UN uses two dedicated users which are defined with default settings and can be changed in `/opt/nem/etc/nem.conf`:

Table 1:

User class	Default		nem.conf tag	
	username	password	username	password
Manager	nemadm	nemadm	nem_remote_auth_admin_user	nem_remote_auth_admin_user_pwd
Session Manager	sessionmanager	sessionmanager	nem_remote_auth_session_user	nem_remote_auth_session_user_pwd

To adapt these default usernames/passwords to user/passwords which are available on installation side the following steps have to be executed:

- 1 Create encrypted passwords with stringtool
`/opt/nem/bin/stringtool <password >`

Example:

```
$ /opt/nem/bin/stringtool nemadm
7E1C4B1DE2EA7879
```

```
$ /opt/nem/bin/stringtool session
B261E2B152ECADD7EF40733064D77107
```

- 2 Insert usernames and passwords into nem.conf

```
nem_remote_auth_admin_user mymanageruser
nem_remote_auth_admin_user_pwd 7E1C4B1DE2EA7879
nem_remote_auth_session_user mysessionmanageruser
nem_remote_auth_session_user_pwd B261E2B152ECADD7EF40733064D77107
```

- 3 Restart FOXMAN-UN by entering the two commands: “nemstop” followed by “nemstart”.

Also see a sample setup in the user manual [1KHW002414] FOXMAN-UN under Linux, section “Configuration for RADIUS Authenticated Users”.

3 Configure PAM for RADIUS authentication module on FOXMAN-UN server

The following preconditions need to be satisfied:

- FOXMAN-UN is correctly installed and configured on RedHat 9.6 (64 bit).
- FreeRADIUS server is installed and configured on Linux server.
- Spare 64 bit Linux machine is installed and configured.

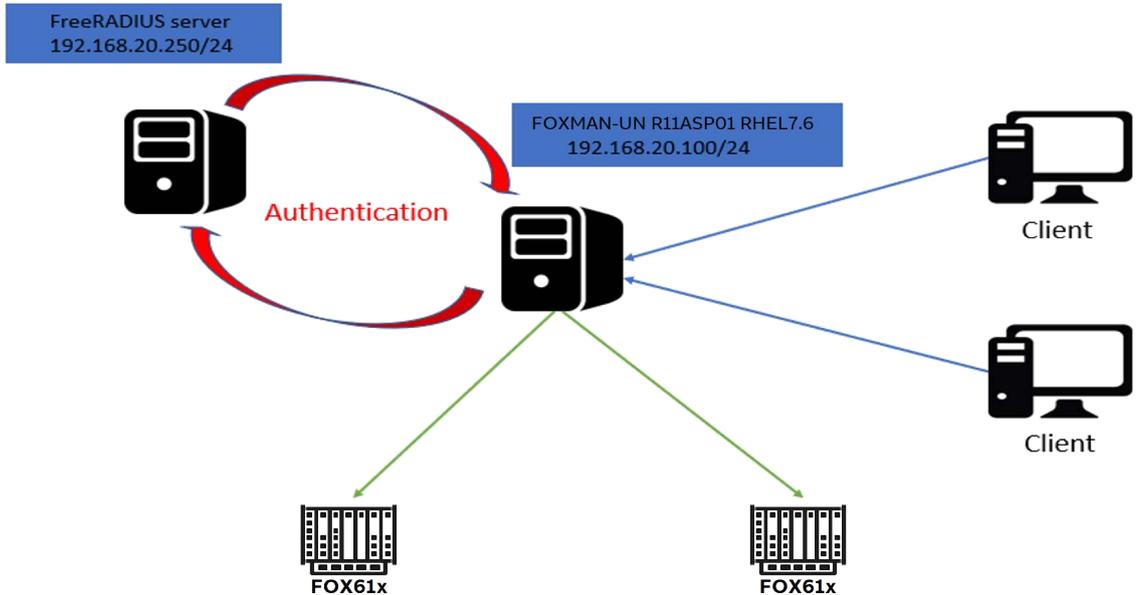


Figure 1: Basic setup (example)

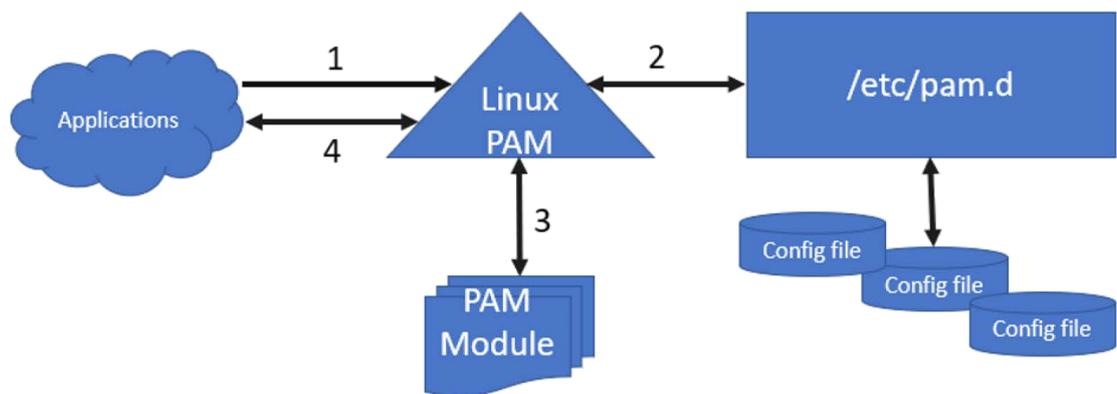


Figure 2: Relations of modules

The FreeRADIUS PAM software for client authentication is available at https://freeradius.org/sub_projects/



Figure 3: Download of pam_radius-release_3_0_0.tar.gz

Since FOXMAN-UN R18 is a 64-bit application installation the additional PAM shared library is required at 64 bit for full support of user authentication.

To compile the PAM module in the correct way it is better to use a spare 64 bit Linux environment with the required software gcc and pam-devel at 64 bit installed.

Installation and setup instruction

Proceed as follows:

1. Install additional software gcc and pam-devel for library configuration on spare 64 bit Linux server.
 - mount the DVD or the ISO image of your Linux 64-bit OS as Local Repository and enable the repository as per Linux 64-bit OS System Administration manual.
 - as root:

```
#yum install gcc pam-devel
```

```
Dependencies resolved.
```

```
=====
Package           Architecture      Version
=====
Installing:
gcc                x86_64            gcc-11.5.0-5.el9_5
pam-devel          x86_64            pam-devel-1.5.1-22.el9_5
Installing for dependencies:
cpp                x86_64            cpp-11.5.0-5.el9_5
glibc-devel        x86_64            glibc-devel-2.34-125.el9_5
glibc-headers      x86_64            glibc-headers-2.34-125.el9_5
kernel-headers     x86_64            kernel-headers-5.14.0-503.33.1.el9_5
libasan             x86_64            libasan-11.5.0-5.el9_5
libatomic          x86_64            libatomic-11.5.0-5.el9_5
=====
```

```
Transaction Summary
```

```
Install 2 Packages (+6 Dependent packages)
```

```
Total download size: 39 M
```

```
Installed size: 55M
```

2. Transfer the pam_radius-release_3_0_0.tar.gz to the /opt folder on spare 64-bit Linux server.
3. Create the 64-bit shared library for PAM authentication

- as root:

Extract the files

```
#tar -zxvf pam_radius-release_3_0_0.tar.gz
```

- Configure the library

```
#cd /opt/pam_radius-release_3_0_0
```

```
#!/configure
```

```
checking build system type... x86_64-unknown-linux-gnu
checking host system type... x86_64-unknown-linux-gnu
checking target system type... x86_64-unknown-linux-gnu
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... none needed
[...]
checking for the compiler flag "-Wdocumentation"... no
checking if building with -DNDEBUG... no
configure: creating ./config.status
config.status: creating src/config.h
```

```
#make
```

```
cc -Wall -fPIC -c src/pam_radius_auth.c -o pam_radius_auth.o
src/pam_radius_auth.c: In function 'pam_private_session':
src/pam_radius_auth.c:1300:6: warning: variable 'ctrl' set but not used [-Wunused-but-set-variable]
```

```

int ctrl;
^
cc -Wall -fPIC -c src/md5.c -o md5.o
cc -shared pam_radius_auth.o md5.o -lpam -o pam_radius_auth.so

```

- The procedure generates under the directory /opt/pam_radius-release_3_0_0 the shared library pam_radius_auth.so compiled at 64-bit.
- As root, transfer the 'pam_radius_auth.so' to the FOXMAN-UN server on /lib64/security/ path

```

verify ownership: root:root
and permit: 755

```

- As root, configure the required modules per application in /etc/pam.d/ on FOXMAN-UN server by adding the following line to the required applications file:

```

auth [success=done auth_err=die default=ignore] pam_radius_auth.so
auth include system-auth

```

- Note:
This configuration allows the login even if RADIUS server is not reachable or RADIUS service is down; the primary authentication is via RADIUS and alternative is system-auth.
- For FOXMAN-UN application

```

nem-auth

```

- Make a backup copy:

```

#cp /etc/pam.d/nem-auth /etc/pam.d/original_nem-auth

```

- Edit the files and save the configuration:

```

#vim /etc/pam.d/nem-auth

```

```

##PAM-1.1
#NEM authentication

```

```

auth [success=done auth_err=die default=ignore] pam_radius_auth.so
auth include system-auth
auth required pam_nologin.so
account required pam_unix.so
password include system-auth
session include system-auth
session required pam_limits.so
session optional pam_console.so

```

- Restart the application to load the new configuration:
 - as a NEM administrator, execute:

```

#nemstop
#nemstart

```

- Create the server configuration file for the RADIUS server connection.

- As root, create the FreeRADIUS configuration directory under /etc

```

#mkdir /etc/raddb/

```

- use the file under /opt/pam_radius-release_3_0_0/pam_radius_auth.conf as a template and copy to /etc/raddb with server name.

```

#cp pam_radius_auth.conf /etc/raddb/server
#chmod go-rwx /etc/raddb/server

```

7. As root, configure the Radius Server to provide the authentication service to the FOXMAN-UN server. According to your FreeRADIUS server setup, users and clients can be defined on database or files. In this procedure it has been defined on file basis:

- Two files need to be configured:

- For RHEL:

```
/etc/raddb/clients.conf
/etc/raddb/users
```

- as an example, based on figure 1, the FreeRADIUS server is 192.168.20.250 and FOXMAN-UN server is 192.168.20.100.

- Append in the client.conf the following section where secret is the secret key that server and client use for the FreeRADIUS Authentication. The client IP is the FOXMAN-UN IP, the short name is a description, you can use the FOXMAN-UN hostname. Example:

```
#vim /etc/raddb/clients.conf
```

```
client 192.168.20.100/24 {
secret = testing123
shortname = FOXMAN-UNR18
nastype = other
require_message_authenticator = no
}
```

- Put at the beginning of the users file, before any comment line, the FOXMAN-UN's users that need to authenticate by FreeRADIUS server. In a basic installation, these are nemadm for FOXMAN-UN application and root for the server administration. Example:

```
#vim /etc/raddb/users
```

```
nemadm Cleartext-Password := "nemadm"
root Cleartext-Password := "TrA%18gz"
#
# Configuration file for the rlm_files module.
# Please see rlm_files(5) manpage for more information.
#
```

8. As root, configure the FOXMAN-UN server to connect to the FreeRADIUS server.

- Edit the /etc/raddb/server file and add a line with the IP address of FreeRADIUS server and the secret key as configured in client.conf file above) for the FOXMAN-UN server.
- As example from [Figure 1: Basic setup \(example\)](#):

```
# vim /etc/raddb/server
# server[:port]shared_secret timeout (s)
192.168.20.250 testing123 3
```

Result: You have successfully set up the PAM modules.

End of instruction

Hitachi Energy Ltd
Bruggerstrasse 72
5400 Baden - Switzerland

Phone: please refer to <https://www.hitachienergy.com/contact-us/Customer-Connect-Center>
(Customer Connect Center)

Email: communication.networks@hitachienergy.com

www.hitachienergy.com/communication-networks