HITACHI
Inspire the Next

INSTALLATION INSTRUCTION

FOXMAN-UN & FOX61x DIRAC

DIRAC Server Installation

Hitachi Energy

Document ID	1KHW029081	
Document edition	FOXMAN-UN System Release:	R18
	Revision:	A
	Date:	2025-10-10

Copyright and confidentiality

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 Preface 4
1.1 Precautions and Safety 4
1.2 Symbols and Notations 4
1.3 Target Audience 4
1.4 Definition of Terms 4

2 Introduction 5
2.1 General 5
2.2 HW Requirements 5

3 Installation 6
3.1 Prerequisites 6
3.2 Procedures 6
3.3 Verification 8
3.4 DIRAC - FOXMAN-UN Integration 9

4 Annex 11
4.1 Document History 11
4.2 Associated Documents 11

1 Preface

1.1 Precautions and Safety

Before you handle any equipment you must comply with the safety advices.

Adherence to the safety instructions ensures compliance with the safety requirements as defined in IEC 62368-1 (Audio/video, information and communication technology equipment - Part 1: Safety requirements).

Please refer to the following document:

[1KHW002497] FOX61x Operating Instruction “Precautions and safety”.

1.2 Symbols and Notations

This Installation Instruction uses the following symbols:

Risk of operating trouble!

Indicates that an action may lead to operating trouble or loss of data.

→ Possible actions are given.

Please note:

Shows significant information.

→ Possible actions are given.

1.3 Target Audience

This Installation Instruction is targeted at persons who are entrusted with the provisioning, operation and administration of the system.

The persons targeted are

- the provisioning personnel, and/or
- the operation and administration personnel

Please note:

The above personnel roles correspond to the “User Role”, “Maintenance Role” and “Crypto Officer Role” as defined in FIPS 140-2.

Please note:

Only instructed and skilled personnel as per IEC 62368-1 may provision and maintain the system.

1.4 Definition of Terms

Table 1: Specific terms

Term	Explanation
SENC1	Designates the encryption unit SENC1 with its instantiations SENC1-4, SENC1F4, SENC1-8 or SENC1F8 of FOX61x.
Core Unit	Designates the core and control unit CESM1, CESM1-F, CESM2, CESM2-F or CESM3 of FOX61x. Where certain features or characteristics apply to a specific core unit only, the CESM1, CESM1-F, CESM2, CESM2-F or CESM3 is named explicitly.

2 Introduction

2.1 General

This document provides a description for the installation of a DIRAC server.

The DIRAC system is composed of a server-side software, called “DIRAC server”, and several SENC1 boards that are operated in FOX61x network elements.

The DIRAC server is a centralized key management system and is responsible for the generation and distribution of the Master Keys used by the SENC1 Crypto Engines. The random numbers required for the Master Keys are generated by a Quantis USB device, attached to the DIRAC server.

The DIRAC server provides the following hardware and software components:

- The Quantis USB device, delivering the quantum random numbers required for the Master Keys. This device is a third party product manufactured by ID QUANTIQUE (IDQ).
- The Master Key Manager, distributing the Master Keys generated by the Quantis USB device to the Crypto Engines which are used as MPLS tunnel endpoints for a bidirectional label switched path (LSP).
- The MPLS manager, maintaining a database with all deployed SENC1 Crypto Engines and MPLS tunnel endpoints.
- The DNMS manager, maintaining a database with all deployed SENC1 Functional Units with their identifier and IP address. The DNMS database is populated by the DIRAC user.
- The DNMS agent, providing the DIRAC server fault management and the logging of DIRAC server events.

2.2 HW Requirements

The DIRAC server runs on a Linux machine. The specific requirements for the Linux environment are:

- OS: RedHat Enterprise Linux version 9.6 is required for R18;
- Server HW as defined in the FOXMAN-UN R18 Release Notes.
- The DIRAC server software is installed on the same HW (or VM) as the FOXMAN-UN R18 core software.
- As a prerequisite to the server HW it is required to provide the following:
  - at least 2 additional CPU cores with respect to the FOXMAN-UN core installation;
  - at least 8 GB of RAM in addition to the FOXMAN-UN core installation;
  - one free USB 2.0 (or higher) port for connecting the Quantis USB device.

3 Installation

3.1 Prerequisites

The DIRAC server software is provided either via an installer script, or via an RPM only. To install the software you need

- root permission on the server machine,
- the DIRAC server software package that is containing the installer (installation script and RPM, or RPM only),
- a Quantis USB (QRNG) device, and
- a valid license option to operate the DIRAC server software must be installed beforehand.

The DIRAC server software should be installed on the same machine as FOXMAN-UN. Installation on a separate machine is not recommended.

3.2 Procedures

Install the DIRAC server software

Proceed as follows:

1. Login as ‘root’ user on the Linux server machine.
2. Open a terminal.
3. Identify the folder where the DIRAC server software installer has been made available.
4. Start the DIRAC server software installation:
   - Mount the installation medium containing the DIRAC server software RPM (nem-dirac-keymgr-18.0.0-n.el8-x86_64.rpm) as local repository (as described in the FOXMAN-UN installation manual), go to the NEM_ADDON folder, then enter

     ```
     ./install_dirac.sh
     ```
5. Wait until the installation process is successfully concluded.
6. At the end of installation procedure, NEM administrators will be automatically added to dirac group and offered to log out and log back in for the change to take effect. In case such user chooses not to do so right away, they still must log out and log back in before attempting to start DIRAC, i.e., before running 'nemstart'.

Result: The DIRAC server software is installed. The user ‘dirac’ is created.

Please note:
The SSH remote access to the server for user ‘dirac’ is restricted.

End of instruction

Define a password for the user ‘dirac’

Proceed as follows:

1. On the machine where the DIRAC server software is installed open a terminal
2. Log in as user ‘root’ and set the password:

```
passwd dirac
Changing password for user dirac.
New password:
Retype new password:
```

```
passwd: all authentication tokens updated successfully.
```

→ The password for the user ‘dirac’ is defined.

End of instruction

Install the Quantis USB device

Please note:
The Quantis USB device installation is a mandatory step in the DIRAC server installation, provided you have chosen to use this device as random number generator. The DIRAC server will not be fully operable without such a device. If this device is not installed, a Linux built-in software random number generator will be used.

Proceed as follows:

1. Login as ‘root’ user on the Linux server machine.
2. Check the availability of USB 2.0 on the Linux server machine:
   - Open a terminal.
   - List USB devices by entering the following command:
     ```
     lsusb
     ```
   - Verify that at least one device with USB version 2.0 (or later) is available, e.g.:
     ```
     Bus 002 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
     ```
3. Install the library ‘libusb’ if not yet installed.
   - If missing, the RPM can be downloaded from “https://rpmfind.net/linux/RPM/centos-stream/9/appstream/x86_64/libusb-0.1.7-5.el9.x86_64.html”.
   - Install the package via
     ```
     yum install libusb
     ```
4. Extract the Quantis libraries QuantisRNG-2.x.y-Linux-amd64.tar.bz2, provided with the Quantis device, to /usr/lib64:
   ```
   sudo tar --strip-components=2 -C /usr/lib64 -xjvf QuantisRNG-2.x.y-Linux-amd64.tar.bz2 QuantisRNG-2.x.y-Linux-amd64/lib64
   ```
   Instead of 2.x.y use the real version available.
   Example:
   ```
   sudo tar --strip-components=2 -C /usr/lib64 -xjvf QuantisRNG-2.12.0-Linux-amd64.tar.bz2 QuantisRNG-2.12.0-Linux-amd64/lib64
   ```
5. Manually create the file /etc/udev/rules.d/idq-quantis-rhel.rules with the following content, making sure to save the file after creation:
   ```
   #Quantis USB
   SUBSYSTEM=="usb", ATTR{idVendor}=="0aba", ATTR{idProduct}=="0102", OWNER="dirac", GROUP="dirac", MODE="0660"
   ```
6. Reload the udev daemon with the updated rules:
   ```
   udevadm control --reload-rules
   ```
7. As user ‘dirac’ verify that you belong to the group ‘dirac’ by entering the groups command and checking the output:
   ```
   groups
   dirac
   ```
   In any case we recommend to reboot your machine now.
8. Identify the USB port supporting USB 2.0 (or later).
9. Plug in the Quantis USB device to the USB 2.0 (or later) port.
10. Identify and check the Quantis USB device:
    ```
    lsusb -d 0aba:0102 -v
    ```

```
[...]
iManufacturer  1 id Quantique
iProduct       2 Quantis USB
[...]
```

Result: The Quantis USB device is installed.

End of instruction

3.3 Verification

Before starting the commissioning of the DIRAC server, check the correct version of the installed DIRAC server and the status of the DIRAC server modules.

Verify the DIRAC server status

→ Check the DIRAC server version and status. Proceed as follows:

1. On the DIRAC server, open a terminal as user ‘dirac’, or open a terminal and switch to user ‘dirac’:

   ```
   su dirac
   Password:
   ```

2. Start the DIRAC target services by entering the command:

   ```
   dirac> diracstart
    Starting DIRAC target services

   Done.
   ```

3. Start the CLI:

   ```
   /opt/dirac/bin/Cli.sh
   ```

   or just

   ```
   Cli.sh
   ```

4. Check the DIRAC server version. If the “version” or “status” commands return an error message like “Connection Error: Unable to connect to the server”, restart the DIRAC server via the command “dirac-restart”. The version should match the installed server version R18:

   ```
   dirac> version
   Cli:    18.0.0
   Server: 18.0.0
   ```

5. Check the DIRAC server status. All modules should be “Active”:

   ```
   dirac> status
    Process name:     diracserverd
    Process Id:       18679
    Process state:    active
    Process substate: running
    Running since:    Wed 2024-08-03 11:55:37 CEST
    Server status:    active
    QRNG source:      Quantis
    QRNG status:      OK
   ```

6. Verify that the QRNG is able to generate random numbers by using the --generate command.
7. Exit from the CLI by entering the command:

```
dirac> exit
```

Result: The DIRAC server version and status are verified.

End of instruction

For commissioning and operation of the DIRAC server refer to [1KHW029082] User Manual “DIRAC Server Operation”.

3.4 DIRAC - FOXMAN-UN Integration

After successful installation of the DIRAC server the communication between FOXMAN-UN and DIRAC is set up so that the FOXMAN-UN Ethernet Security Manager recognizes a working DIRAC server over the REST interface. To enable communication between the two systems, keys and certificates are exchanged...

- (recommended setup:) automatically during installation if FOXMAN-UN core and DIRAC server are installed on the same machine and DIRAC server is installed after the FOXMAN-UN core - see instructions “Set up communication between DIRAC and FOXMAN-UN” further below;
- (not recommended:) manually by the server administrator if the DIRAC server and FOXMAN-UN core are installed on different machines, or if FOXMAN-UN is installed after the DIRAC server - see instructions “Exchange certificates between DIRAC and FOXMAN-UN” and “Set up communication between DIRAC and FOXMAN-UN” below.

Exchange certificates between DIRAC and FOXMAN-UN

Keys and certificates for the DIRAC REST interface are generated during the DIRAC installation and stored in the folder /etc/pki/dirac. The following two files are relevant for the next steps:

- nem.pem
- nem.crt

As the server administrator (you will need root permission to do this),

Proceed as follows: (applicable only if the DIRAC server and FOXMAN-UN core are installed on different machines)

1. Copy the DIRAC key from the DIRAC machine:

   ```
   /etc/pki/dirac/nem.pem
   ```

   to the following folder on the FOXMAN-UN machine:

   ```
   /opt/nem/etc/enpsec/
   ```

2. Copy the DIRAC certificate from the DIRAC machine:

   ```
   /etc/pki/dirac/nem.crt
   ```

   to the following folder on the FOXMAN-UN machine:

   ```
   /opt/nem/etc/enpsec/
   ```

3. Change the ownership of the two copied files on the FOXMAN-UN machine:

   ```
   cd /opt/nem/etc/enpsec/
   chown nemadm:nem nem.pem
   chown nemadm:nem nem.crt
   ```

4. Verify that the following two entries in the file “/opt/nem/etc/enpsec/dpmprop.cfg” are present:

   ```
   clientCertificateFile=nem.crt
   privateKeyFile=nem.pem
   ```

Result: The DIRAC - FOXMAN-UN certificates are in place.

End of instruction

Set up communication between DIRAC and FOXMAN-UN

Proceed as follows:

1. Login as ‘root’ user on the FOXMAN-UN server
2. Verify that the DIRAC server can be addressed from FOXMAN-UN; the following entry in the file “/opt/nem/etc/enpsec/dpmprop.cfg” is required when DIRAC server is installed on the same machine as FOXMAN-UN:

   ```
   enpsec_hostname=localhost
   ```

   If the DIRAC server is on a different machine “localhost” needs to be replaced by the host-name of the DIRAC server, e.g.

   ```
   enpsec_hostname=mydiracserver
   ```

3. Make sure the following entry is present in the file “/etc/hosts”:

   ```
   127.0.0.1 localhost localhost.localdomain localhost4
   localhost4.localdomain4
   ```

4. Log in to FOXMAN-UN and open the Ethernet Security Manager application from the NEM Desktop (menu: Application - Ethernet Security Manager...).
5. Verify the DIRAC communication status in the upper right corner of the Ethernet Security Manager dialog window. The status should show an OK mark  and the text “DIRAC local-host:9343” or a text similar to “DIRAC mydiracserver.company.com:9343”.

   If this is not the case you may need to reboot the DIRAC server software by entering the command “dirac-restart” in the DIRAC CLI (as user dirac).
   Optionally, but only recommended if necessary due to its wider impact, restart the NEM core and/or NEM base services by entering the command “nembasestop”, followed by “nemstart” in a terminal (as a NEM administrator).

Result: The DIRAC - FOXMAN-UN communication via the REST interface is up and run-ning.

End of instruction

4 Annex

4.1 Document History

Table 2: Document history

Hitachi Energy Document ID	FOX61x Release	FOXMAN-UN Release	Rev.	Date	Changes since previous version
1KHW029081	R18	R18	A	Oct 2025	Updated version for the current system release.
1KHW029081	R17A	R17A	A	Oct 2024	Updated version for the current system release.
1KHW029081	R16B	R16B	A	Aug 2023	Updated version for the current system release.
1KHW029081	R16A	R16A	A	Aug 2022	Updated version for the current system release.
1KHW029081	R15B	R15B	B	Feb 2022	Corrected Quantis USB device installation procedure.
1KHW029081	R15B	R15B	A	Jan 2022	Updated version for the current system release.
1KHW029081	R15A	R15A	A	Jun 2021	Updated version for the current system release.
1KHW029081	R14A	R14B	A	Jan 2021	Updated version for the current system release.
1KHW029081	R14A	R14A	A	July 2020	Re-issued for the current system releases.
1KHW029081	R3B	R11B	A	Sept 2019	First revision for the current system releases.

4.2 Associated Documents

[1KHW002499] Release Note “FOXMAN-UN”

[1KHW002497] FOX61x Operating Instruction “Precautions and safety”

[1KHW029082] User Manual “DIRAC Server Operation”

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

Document ID: 1KHW029081 R18 Rev. A