USER MANUAL

FOXMAN-UN & FOX61x

DIRAC

DIRAC Server Operation

Document ID	1KHW029082	
Document edition	System Release:	R18
	Revision:	A
	Date:	2025-06-03

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

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 User Manual uses the following symbols:

STOP

Risk of operating trouble!
Indicates that an action may lead to operating trouble or loss of data.
→ Possible actions are given.

i

Please note:
Shows significant information.
→ Possible actions are given.

1.3 Document History

Table 1: Document history

Document ID	FOX61x Release	FOXMAN-UN Release	Rev.	Date	Changes since previous version
1KHW029082	R18	R18	A	Jun 2025	Updated version for the current system release.
1KHW029082	R17A	R17A	A	Sep 2024	Updated for the current system release. Minor updates and error corrections. Added new commands in section 9.1.4 and section 9.1.7.
1KHW029082	R16B	R16B	A	Jun 2023	Updated for the current system release.
1KHW029082	R16A	R16A	A	Aug 2022	Updated for the current system release.
1KHW029082	R15B	R15B	A	Jan 2022	Updated for the current system release.
1KHW029082	R15A	R15A	A	July 2021	Updated for the current system release.
1KHW029082	R14A	R14A	A	July 2020	Re-issued for the current system releases.
1KHW029082	R3B	R11B	A	Sept. 2019	First revision for the current system releases.

1.4 Target Audience

This User Manual 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

i

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

i

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

1.5 Definition of Terms

Table 2: Specific terms

Term	Explanation
SENC1 SENC1 unit	Designates the encryption unit SENC1-4, SENC1F4, SENC1-8 or SENC1F8 of FOX61x, or its representation in FOXMAN-UN. The unit can be plugged into a FOX61x subrack. Where certain features or characteristics apply to a specific encryption unit only, the SENC1-4, SENC1F4, SENC1-8 or SENC1F8 is named explicitly.
Core Unit	Designates the core and control unit of type 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.
dirac user	The user ‘dirac’ is the manager of the DIRAC key distribution system.
Board	In the SENC1 context a board is a SENC1 physical HW unit. The board is identified by a 10 to 13 digit number. Example: SENC1 board serial number: 4910764000
CE	Crypto Engine In the SENC1 context a CE is a Crypto Engine. A Functional Unit (FU) has two CEs: CE A and CE B. The Crypto Engine is identified by a 12 to 15 digit number which is composed of the 10 to 13 digits SENC1 board serial number, the Functional Unit number, and the Crypto Engine number. Examples: SENC1 board serial number: 4910764000 Functional Unit number: 1 or 2 Crypto Engine number: 1 (for CE A) or 2 (for CE B) CE ID: 491076400011, or 491076400012, or 491076400021, or 491076400022.
ENP	Ethernet Networking Package of FOXMAN-UN.
ESM	Ethernet Security Manager of FOXMAN-UN.
FU	Functional Unit In the SENC1 context a FU is a Functional Unit. A SENC1 unit has one (SENC1-4 and SENC1F4) or two (SENC1-8 and SENC1F8) FUs: FU 1, FU 2. The Functional Unit is identified by an 11 to 14 digit number which is composed of the 10 to 13 digits SENC1 board serial number and the Functional Unit number. Examples: SENC1 board serial number: 4910764000 Functional Unit number: 1 or 2 FU ID: 49107640001, or 49107640002.

Table 2: Specific terms (continued)

Term	Explanation
MK	Master Key Master Keys are generated and distributed whenever FOXMAN-UN deploys an encrypted tunnel, or on request of the DIRAC operator. Master Keys are generated for a particular Label Switched Path (LSP) and distributed to all MPLS tunnel end-points terminating this LSP.
NE	Network Element In the FOX61x context a NE is a subrack equipped with core and service units. In the SENC1/DIRAC context an FU behaves similar to an NE in certain aspects. Refer to the term “FU”.

2 Introduction

2.1 General

This document provides a detailed description of the DIRAC server.

The DIRAC system is composed of a server-side software, called “DIRAC server”, and several SENC1 boards operated in FOX61x NEs. The DIRAC system constitutes a security zone which is integrated with the ENP and ESM of FOXMAN-UN and/or FOXCST managing FOX61x network elements.

The DIRAC management network can be the same physical network as the FOXMAN-UN-FOX-61x NE management network since the DIRAC system has its own authentication and encryption means.

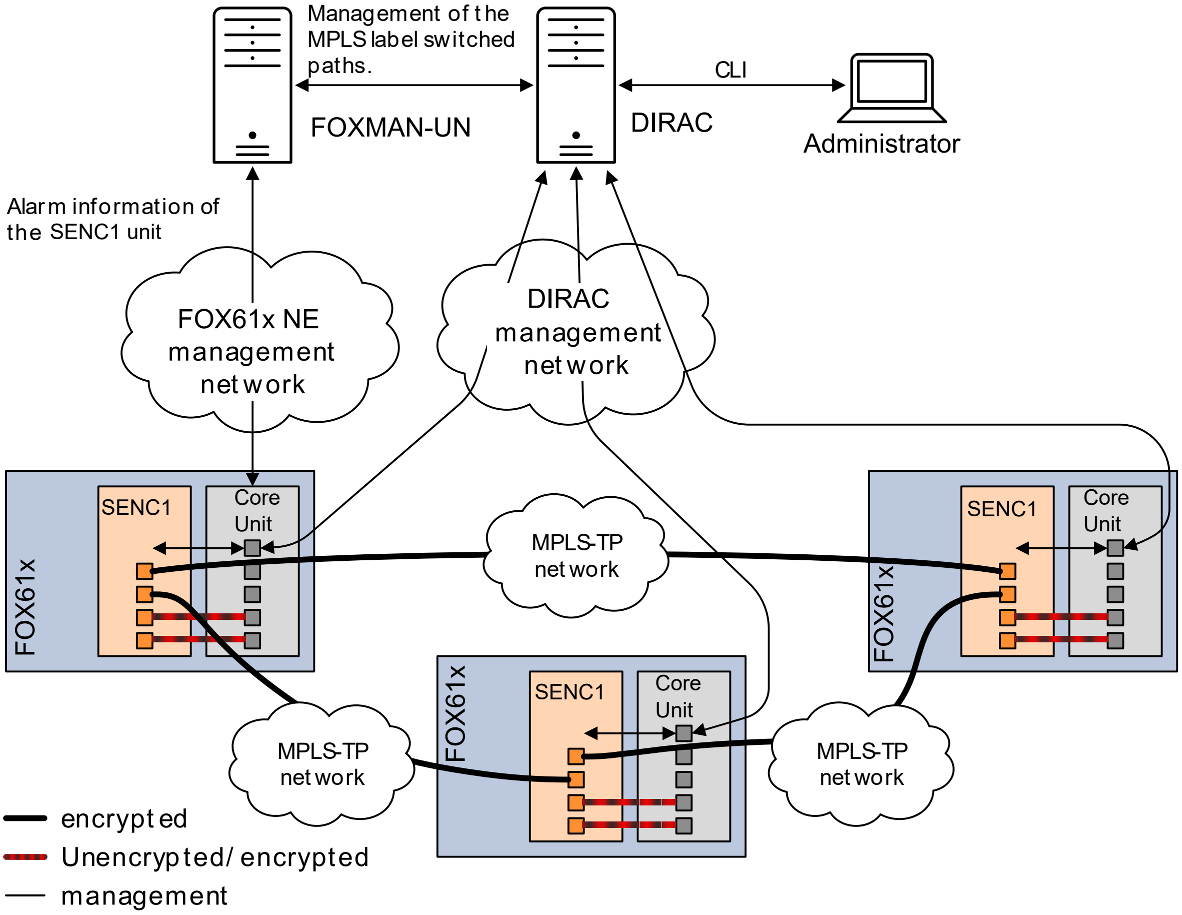


Figure 1: Encryption with the MPLS application using SENC1 and DIRAC server

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 has a command line interface (CLI) through which it is managed. In addition there is a secure interface between the network management system FOXMAN-UN and the DIRAC server in order to synchronize paired information (Crypto Engine identifiers, encrypted MPLS tunnels and tunnel endpoints, DIRAC server alarm status) between both systems.

The communication between the DIRAC server and FOXMAN-UN is done via a REST interface, based on HTTPS.

The DIRAC server also forwards the MPLS tunnels crypto configuration information from the FOXMAN-UN to all SENC1 Crypto Engines in the DIRAC system via secured channels over Ethernet or MPLS-TP links, depending on the preferred configuration.

SENC1 boards are the HW units that provide encryption in the FOX61x network element. The SENC1-4 and SENC1F4 boards have one Functional Unit with two Crypto Engines. The SENC1-8 and SENC1F8 boards have two Functional Units with two Crypto Engines each, i.e. four Crypto Engines in total. One Crypto Engine is equipped with two Ethernet interfaces. It encrypts and decrypts bidirectional user traffic. For more information on SENC1 units refer to [1KHW029028] FOX61x User Manual “SENC1-4, SENC1F4, SENC1-8, SENC1F8”.

The enrollment of SENC1 units and the establishment of trust between the DIRAC server and the SENC1 Crypto Engines is done by the crypto officer via FOXMAN-UN/ESM. The FOXMAN-UN/ESM use the GRPC channel (see below) to set up crypto configurations for MPLS tunnels.

The communication between the DIRAC server and the SENC1 Functional Units is based on the encrypted GRPC protocol (management channel). The certificates used for the GRPC encryption are created on the DIRAC server and on the SENC1 Functional Units and are automatically exchanged between the DIRAC server and the SENC1 Functional Units.

The user traffic interfaces of the SENC1 Crypto Engines are interconnected with 1 Gbit/s or 10 Gbit/s secure channels over a MPLS-TP network. For details refer to [1KHW029028] FOX61x User Manual “SENC1-4, SENC1F4, SENC1-8, SENC1F8”.

The alarm status of the SENC1 boards is collected by the core units of the FOX61x network elements and forwarded via the FOX61x NE management network to the network management system FOXMAN-UN and to FOXCST.

2.2 DIRAC Main Components

Figure 2 illustrates the topology of the DIRAC System and the main components of the DIRAC server.

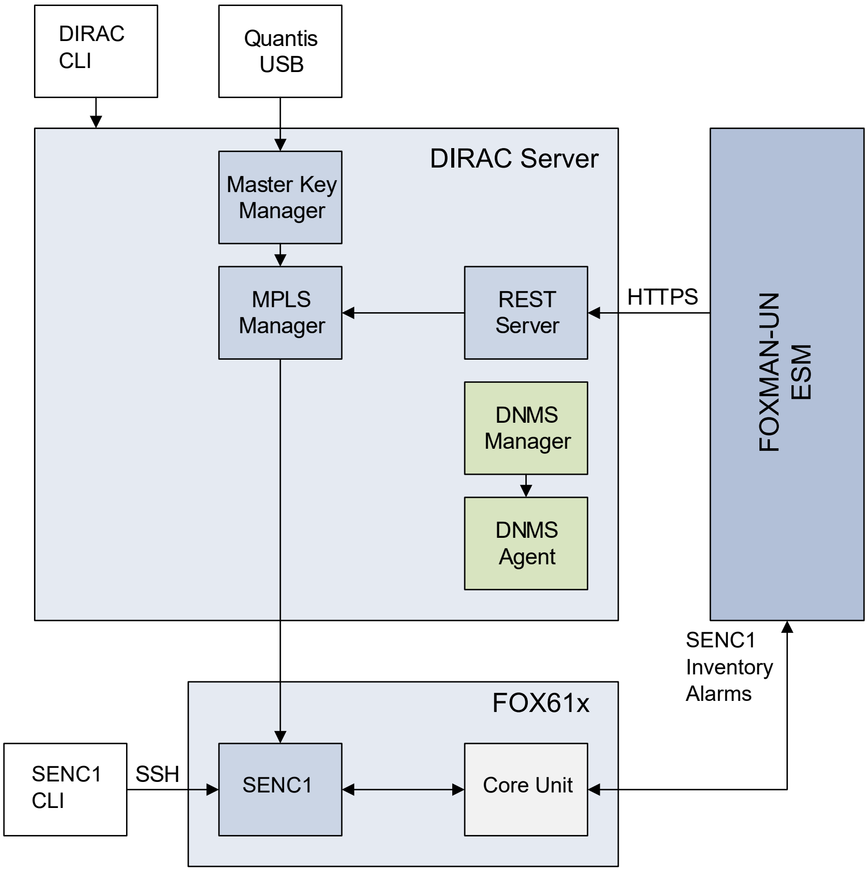


Figure 2: DIRAC server main components

2.2.1 DIRAC System

The DIRAC system is composed of the following components:

- The DIRAC server, running on a Linux physical or virtual machine. The DIRAC server is managed with the DIRAC CLI and via its REST interface. Typically the DIRAC server is deployed as add-on to the FOXMAN-UN and is running on the same physical and/or virtual Linux machine as the FOXMAN-UN.
- The SENC1 units, operated in FOX61x network elements. The SENC1 units basic configuration is done using FOXCST and FOXMAN-UN. Once a unit is deployed in a FOX61x network element the SENC1 is managed with the FOXMAN-UN ESM:
  - via the DIRAC server for the setup of crypto configurations for MPLS tunnels, and
  - via the FOX61x core unit for the configuration of the SENC1 unit and port parameters.

i

Please note:
The configuration of the Layer 2 protocol packet encryption is done in the ESM of FOXMAN-UN or via the DIRAC CLI. FOXMAN-UN ESM provides the full functionality for L2 encryption setup.

The FOXMAN-UN (as shown in Figure 2), running on a Linux machine, is not part of the DIRAC system. The FOXMAN-UN applies encryption profiles to MPLS tunnels that fit to crypto configurations used on the SENC1 Crypto Engines.

2.2.2 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.
- 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).

  Master Keys can be renewed on request by the DIRAC user.
- The MPLS manager, maintaining a database with all deployed SENC1 Crypto Engines and MPLS segments and tunnel endpoints.

  The MPLS manager communicates with the FOXMAN-UN via a REST (Representational State Transfer) interface over HTTPS.

  The MPLS manager communicates with the SENC1 Functional Units via an encrypted GRPC protocol. GRPC encryption is done using a private certificate. Exchanging the public certificates establishes trust.

  The MPLS manager forwards the crypto configuration for the MPLS tunnels from the FOXMAN-UN to the involved SENC1 Crypto Engines:
  - Involved Crypto Engine endpoints;
  - MPLS labels to be used in outgoing and incoming direction;
  - Crypto Profile to be applied (encrypt/discard/bypass, authentication);
  - Master Key to be used for the Session Key encryption;
  - Session Key renewal rate.

i

Please note:
The configuration of the Layer 2 protocol packet encryption (PTP and ESMC) is preferably done with the FOXMAN-UN ESM.

- 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 manager monitors the status of the SENC1 management channel.

- The DNMS agent, providing the DIRAC server fault management and the logging of DIRAC server events.

3 Functions and Specifications

The DIRAC server provides the following functions:

Table 3: DIRAC server - system features

Feature	Rating or standard	Release[1]
Operable with encryption units	- SENC1-4 - SENC1F4 - SENC1-8 - SENC1F8	r2a
Maximum number of supported encryption units	150 SENC1 Functional Units with 2 Crypto Engines each	r2a
Maximum number of supported MPLS tunnels	150’000 MPLS tunnels with 300’000 tunnel endpoints on 300 SENC1 Crypto Engines (1000 tunnel endpoints per Crypto Engine)	r2a
Management channel to the network management system FOXMAN-UN	REST (Representational State Transfer) interface over HTTPS, user authentication using certificates. For MPLS tunnel crypto configuration setup in SENC1 from FOXMAN-UN.	r2a
Management communication channel between DIRAC server and encryption units	GRPC protocol. GRPC encryption using certificates.	r15a
Master Key generation	Quantis USB device attached to the Linux server	r2a
Support for SFTP and SSH public key authorization when connecting to an FU.		r17a
Support for software download and management (incl. via ESW distribution wizard).		r17a

1. refers to the DIRAC SW version shown in the DIRAC CLI.

Table 4: DIRAC server - management

Feature	Rating or standard	Release[1]
Management interface	DIRAC server CLI	r2a
Manager privileges	dirac user for all management operations, no root privileges	r2a
Improved usability of management interface	DIRAC server CLI	r15a

1. refers to the DIRAC SW version shown in the DIRAC CLI.

4 DIRAC Functional Description

4.1 DIRAC Operator Roles

The implementation of the DIRAC system is compliant with FIPS 140-2 security level 2. This means:

- The cryptographic module employs role-based authentication to control access to the module.
- The cryptographic module is not required to authenticate the individual identity of the operator.

The cryptographic module supports the following authorized roles for operators:

- “User Role”:

  The user role performs general security services, including cryptographic operations and other approved security functions.

  The “User Role” in case of the DIRAC system corresponds to the scope of the currently identified FOXMAN-UN user when using the FOXMAN-UN ESM.

  The “User Role” in case of the DIRAC system corresponds to the scope of the DIRAC administrator when using the DIRAC CLI.
- “Crypto Officer Role”:

  The crypto officer role performs cryptographic initialization or management functions, e.g. module initialization, input/output of cryptographic keys, and audit functions.

  The “Crypto Officer Role” in case of the DIRAC system corresponds to the actual scope of the DIRAC CLI (= ‘dirac’ user) and SENC1 CLI (= ‘admin’ user) commands, and to the scope of the SENC1 maintainer user.

Above roles are implemented using the “dirac” user account.

4.2 DIRAC System Interfaces

The DIRAC system interfaces are located between the SENC1 unit and the DIRAC server, and between the DIRAC server and the FOXMAN-UN.

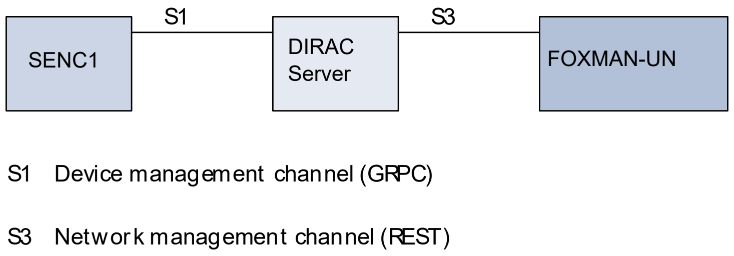

S1
S3
SENC1
DIRAC Server
FOXMAN-UN
S1 Device management channel (GRPC)
S3 Network management channel (REST)

Figure 3: DIRAC system interfaces

S1: Device management channel

The device management channel is based on GRPC. The supported commands are:

- Create Tunnel Endpoint
- Delete Tunnel Endpoint
- Push Master Key
- Refresh Master Key

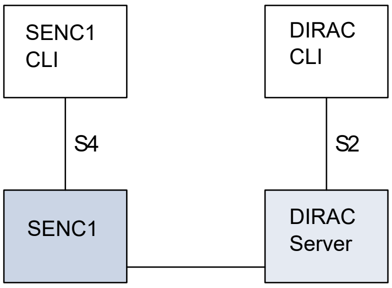
S3: Network management channel

The network management channel allows the FOXMAN-UN to “program” the DIRAC server via the DIRAC Management Module without knowing the secrets (Master Key value, passwords, SENC1 certificates).

4.3 DIRAC User Interfaces

Advanced users can communicate with the DIRAC system by means of two Command Line Interfaces (CLI):

- CLI for the DIRAC server
- CLI for the SENC1 Functional Units.



S4	SENC1 CLI (SSH)
S2	DIRAC CLI (SSH)

Figure 4: DIRAC system user interfaces

S4: SENC1 CLI

The SENC1 CLI provides the configuration, update and audit of any SENC1 Functional Unit individually. The protocol of this channel is based on SSH. The SENC1 CLI is to be used by advanced users only.

S2: DIRAC CLI

The DIRAC CLI allows the DIRAC user to configure the DIRAC server, and to access and modify the Key Management parameters. The protocol of this channel is based on SSH. The DIRAC CLI is to be used by advanced users only.

4.4 DIRAC Key Management

Master Keys are used by the SENC1 Crypto Engines to encrypt the Session Keys. Master Keys are generated by the Quantis USB device attached to the DIRAC server, and distributed to the SENC1 Crypto Engines. For the installation of the Quantis device please refer to [1KHW029081] User Manual “DIRAC - DIRAC Server Installation”.

The Quantis USB device is connected to the DIRAC server. Master Keys are generated and distributed whenever FOXMAN-UN deploys an encrypted segment/tunnel, or on DIRAC user request.

When a new Master Key for a specific LSP is requested the following operations are performed:

- The MPLS Manager checks the existence of the LSP.
- The MPLS Manager gets the list of endpoints corresponding to this LSP.
- The MPLS Manager requests a new Master Key from the Quantis USB device.
- The MPLS Manager distributes the new Master Key to the Crypto Engines according to Figure 5.
- The MPLS Manager gives back the result to the user.

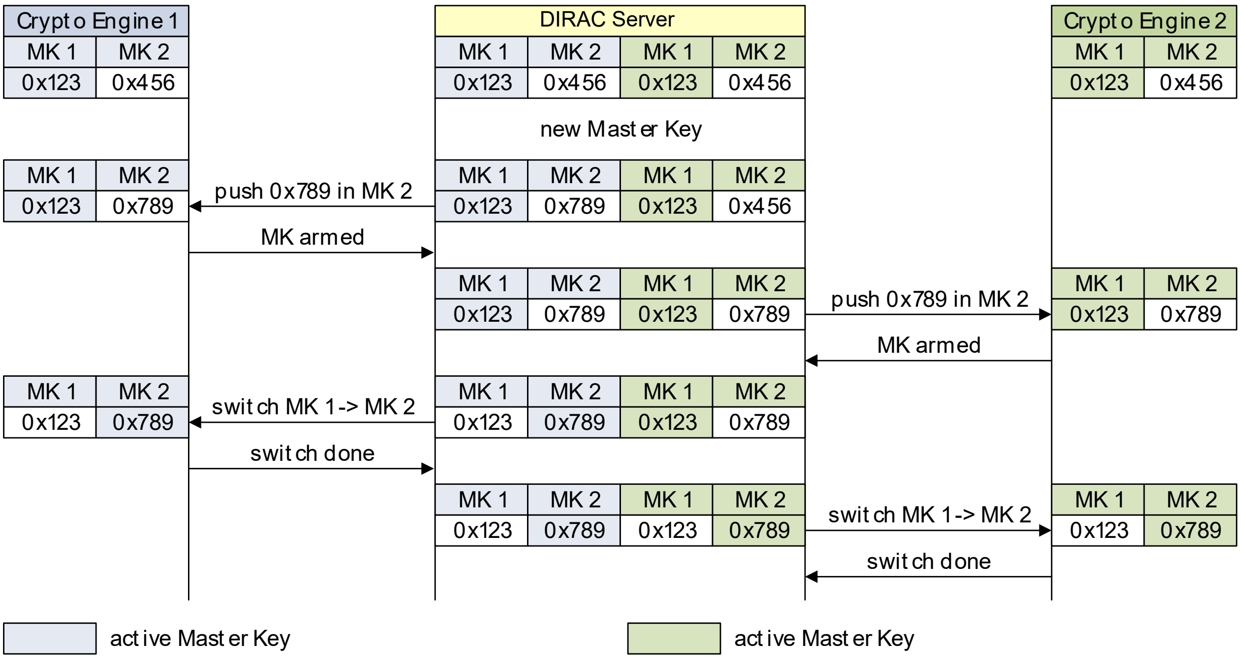


Figure 5: Master Key distribution and activation

The Quantis USB device is supervised by the DIRAC server. The Quantis USB status is checked every minute by the DIRAC server. A QRNG alarm is raised …

- if the Quantis USB device is not available, or
- if the Quantis USB device does not deliver a new Master Key on request.

4.5 DIRAC Information Model

The DIRAC server manages and stores persistently information about Functional Units, Crypto Engines, Crypto Segments, and Crypto Configurations.

4.5.1 Functional Units

The Functional Unit list shows all added (enrolled) SENC1 Functional Units in the DIRAC server.

The command “functional-unit --list” displays following information:

- Id - Functional Unit identifier
- FU - Functional Unit number within SENC1 card: 1 or 2
- Name - name of the Functional Unit specified during adding (enrollment) to DIRAC
- IP Address - IP address of the Functional Unit
- Hardware - SENC1 hardware variant
- Software - SENC1 ESW version
- Status - communication status with the Functional Unit

For a detailed description of the CLI commands output see section 9.1.3 Functional Unit Commands (on page 45).

4.5.2 Crypto Engines

The Crypto Engine list shows all Crypto Engines available in the DIRAC system. In order to make a Crypto Engine available in the DIRAC system the Functional Unit (of the SENC1 card) to which the Crypto Engine belongs to has to be added (enrolled) in DIRAC; see SENC1 FU Enrollment.

The command “crypto-engine --list” displays a table with the following parameters:

- CE ID - SENC1 Crypto Engine identifier
- Engine - SENC1 Crypto Engine number within Functional Unit (1 or 2)
- Dci - DIRAC configuration index
- Sci - SENC1 Crypto Engine configuration index
- Status - management channel connection status

For a detailed description of the CLI commands output see section 9.1.2 Crypto Commands (on page 44).

4.5.3 Crypto Segments and Crypto Configurations

In the DIRAC system:

- a Crypto Segment item defines the encryption for a specific MPLS tunnel;
- a Crypto Configuration item defines the encryption for a specific MPLS tunnel endpoint executed by a specific Crypto Engine.

The command “crypto-segment --list” displays following information:

- Segment - Crypto Segment Identifier
- Status - status of Crypto Segment
- Profile - crypto profile [0..5]
- Layer - layer/protocol for which Crypto Segment is used: MPLS or LAYER2
- Active Master Key - hash key (first 32 digits in hex) of the Active Master Key
- Activated At - date&time when the Active Master Key was activated

The command “crypto-configuration --list” displays following information:

- Ce Id - SENC1 Crypto Engine identifier for which the Crypto Configuration is used
- Segment - Crypto Segment Identifier
- Label In - LSP label in incoming direction
- Label Out - LSP label in outgoing direction
- L2 - if the Crypto Configuration is used for L2 encryption: yes/no
- Vlan - if the Crypto Configuration is based on VLAN subinterfaces: yes/no
- Profile - crypto profile
- Active Master Key - hash key (first 32 digits in hex) of the Active Master Key
- Activation Time - date&time when the Active Master Key was activated
- Fallback Master Key - hash key (first 32 digits in hex) of the Fallback Master Key

For a detailed description of the CLI commands output see section 9.1.2 Crypto Commands (on page 44).

4.6 DIRAC Server Alarms

The DIRAC server provides one alarm to inform the FOXMAN-UN about its status.

The following alarm is available:

- Certificate is about to expire (eDpmAlarmCertificateIsAboutToExpire)
- Certificate has expired (eDpmAlarmCertificateIsExpired)
- Random number generator is not operational (eDpmAlarmQrngIsNotQuantum)
- Detected random number generator is not Quantum (eDpmAlarmQrngIsNotOperational)

The alarms can be polled by the FOXMAN-UN, or the DIRAC server can asynchronously send the alarm indication to the FOXMAN-UN.

5 DIRAC Installation

For the installation of the DIRAC server please refer to [1KHW029081] User Manual “DIRAC - DIRAC Server Installation”.

6 DIRAC Commissioning

Once the DIRAC server is installed the following configuration operations have to be performed.

6.1 DIRAC Server Status Check

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.

Check the DIRAC server status

→ Check the version and status. Proceed as follows:

1. Log in as dirac user on the Linux machine.
2. Open a terminal.
3. Connect to the DIRAC server:

```
$ /opt/dirac/bin/Cli.sh
==================================================
DIRAC CLI
Version: 17.1.0
(c) 2021-2024 Hitachi Energy. All rights reserved.
==================================================
```

4. Check the DIRAC server version. The version should match the installed server version:

```
dirac> version
Build Version: 17.1.0

dirac>
```

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

```
dirac> status
 Process name:     diracserverd
 Process Id:       3493530
 Process state:    active
 Process substate: running
 Running since:    Wed 2024-04-03 13:20:39 CEST
 Server status:    active
 QRNG source:      Quantis (S/N not available)
 QRNG status:      OK
```

Result: The DIRAC server version and status are checked.

End of instruction

6.2 Opening Ports

An important aspect of firewalls is the ports and protocols that will be able to communicate with external applications. It is assumed that FOXMAN-UN and DIRAC are running on the same host. However, make sure that any firewall between the DIRAC server and the SENC1 units lets pass the management traffic.

The following table shows the protocols used for management traffic with the DIRAC server.

Table 5: Protocols used for management traffic with the DIRAC server

Protocol	Application / service	Port number	Comments
TCP/HTTPS	GRPC	9009	Used by the DIRAC server to access the SENC1 Functional Unit.
TCP	SSH	22	Used by the DIRAC CLI SSH client as destination port for the SSH session (initiated by the SSH client).
HTTP	REST	443	Used for the management communication between the DIRAC server and FOXMAN-UN. Not relevant for the firewall settings if FOXMAN-UN and DIRAC are running on the same host.

For more information related to opening ports please refer to [1KHW028522] FOX61x User Manual “Management Communication” and to [1KHW029012] FOXMAN-UN in Firewalled Environment, Application Note.

7 SENC1 Commissioning

For detailed information on the commissioning of a SENC1 Functional Unit FOXCST and FOXMAN-UN/ESM please refer to the SENC1 user manual [1KHW029028].

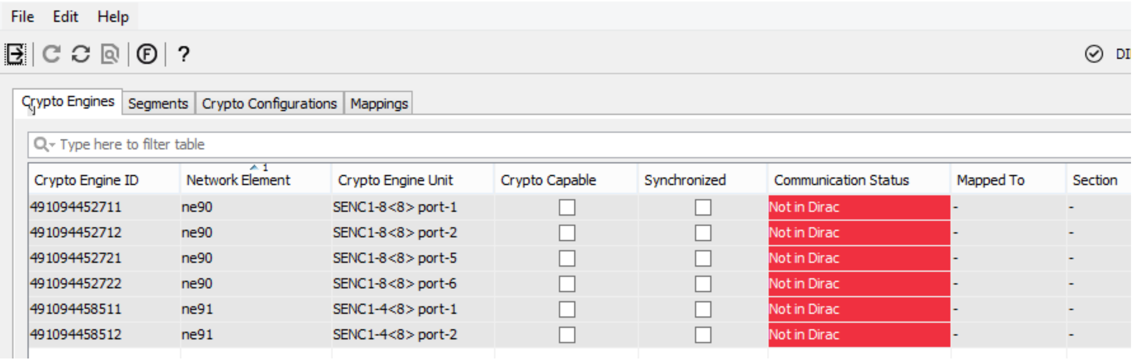
This section describes in short the following activities:

- Enroll FU (SENC1 FU Enrollment);
- Disenroll FU (SENC1 FU Disenrollment);
- FU SW Upgrade (FU Software Upgrade);
- L2 encryption (L2 Encryption);
- Master Key refresh (Master Key Refresh).

7.1 SENC1 FU Enrollment

If required, pre-enrollment in a secure room is done as described in the SENC1 user manual, section “SENC1 Basic Setup in a Secure Room”.

After adding an FOX61x with an assigned SENC1 HW unit, or, alternatively, adding/assigning a SENC1 HW unit to an FOX61x already managed by FOXMAN-UN, the related SENC1 FUs will appear in the FOXMAN-UN ESM “Crypto Engines” tab.



Crypto Engine ID	Network Element	Crypto Engine Unit	Crypto Capable	Synchronized	Communication Status	Mapped To	Section
491094452711	ne90	SENC1-8<8> port-1	□	□	Not in Dirac	-	-
491094452712	ne90	SENC1-8<8> port-2	□	□	Not in Dirac	-	-
491094452721	ne90	SENC1-8<8> port-5	□	□	Not in Dirac	-	-
491094452722	ne90	SENC1-8<8> port-6	□	□	Not in Dirac	-	-
491094458511	ne91	SENC1-4<8> port-1	□	□	Not in Dirac	-	-
491094458512	ne91	SENC1-4<8> port-2	□	□	Not in Dirac	-	-

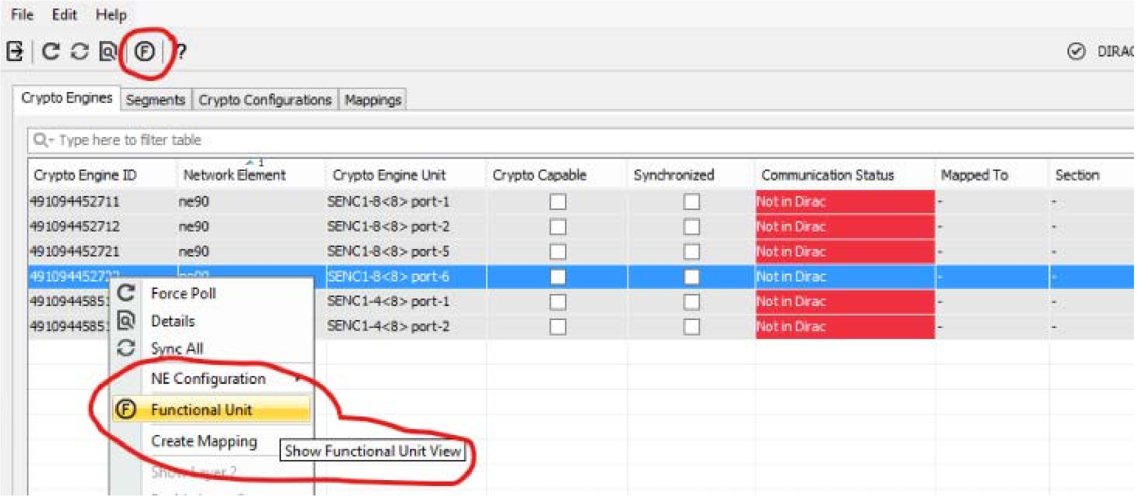
Figure 6: ESM, Crypto Engines tab

For each SENC1 HW unit you will see 2 or 4 Crypto Engines, depending on the type of SENC1 HW.

All SENC1 HW units that are assigned will be shown in the ESM. The respective Crypto Engines will appear with a communication status “Not in Dirac” as long as they have not been defined in DIRAC.

The procedure to add a SENC1 HW unit to DIRAC and to do the initial configuration of the unit is called “Enroll procedure”, or “Add to Dirac”.

This procedure can be started from the “Functional Unit View” (FU View) dialog window. The FU View can be invoked via icon bar (Icon with an “F”) or from the context menu (Functional Unit) on a Crypto Engine entry in the Crypto Engines table.

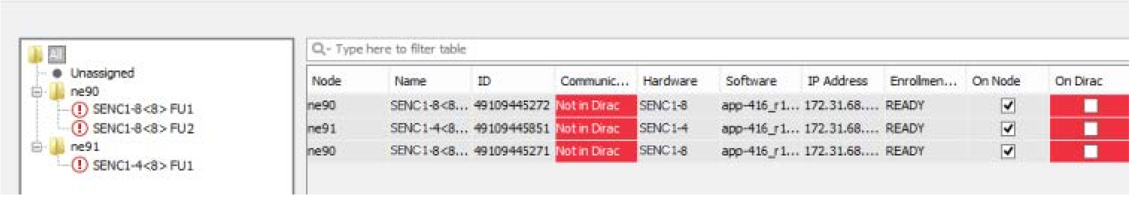


Crypto Engine ID	Network Element	Crypto Engine Unit	Crypto Capable	Synchronized	Communication Status	Mapped To	Section
491094452711	ne90	SENC1-8<8> port-1	□	□	Not in Dirac	-	-
491094452712	ne90	SENC1-8<8> port-2	□	□	Not in Dirac	-	-
491094452721	ne90	SENC1-8<8> port-5	□	□	Not in Dirac	-	-
4910944527[illegible]	[illegible]	SENC1-8<8> port-6	□	□	Not in Dirac	-	-
49109445851		SENC1-4<8> port-1	□	□	Not in Dirac	-	-
49109445851		SENC1-4<8> port-2	□	□	Not in Dirac	-	-

Figure 7: ESM - options to open FU View

In the FU View you see all FUs detected by FOXMAN-UN.

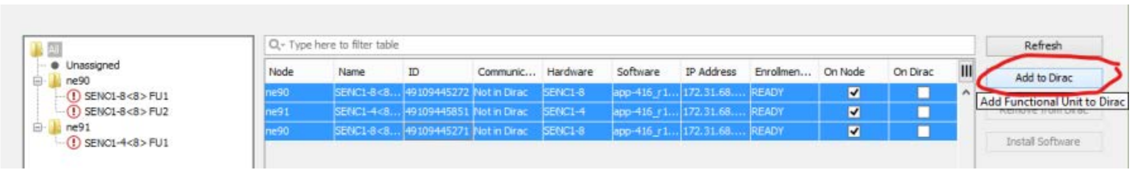
Before the enrollment procedure you will see the units with a red warning, indicating that the unit was not yet enrolled:



Node	Name	ID	Communic...	Hardware	Software	IP Address	Enrollmen...	On Node	On Dirac
ne90	SENC1-8<8...	49109445272	Not in Dirac	SENC1-8	app-416_r1...	172.31.68....	READY	☑	□
ne91	SENC1-4<8...	49109445851	Not in Dirac	SENC1-4	app-416_r1...	172.31.68....	READY	☑	□
ne90	SENC1-8<8...	49109445271	Not in Dirac	SENC1-8	app-416_r1...	172.31.68....	READY	☑	□

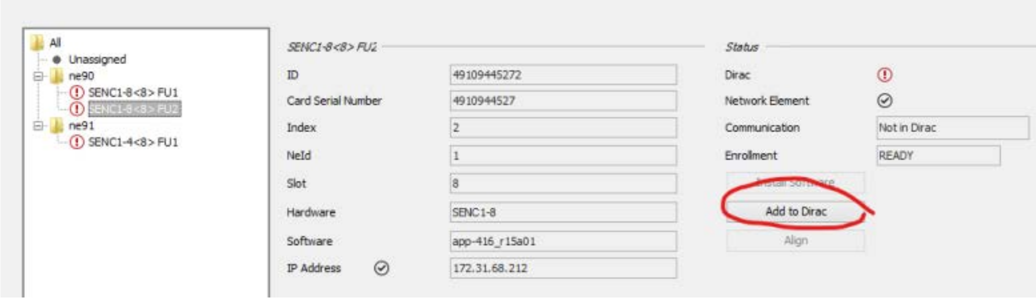
Figure 8: ESM - FU View

In order to invoke the enrollment procedure you can select in such a list all units you want to enroll and click on the “Add to Dirac” button, or you can select one specific FU (viewing the details of such FU) and click on the “Add to Dirac” button.



Node	Name	ID	Communic...	Hardware	Software	IP Address	Enrollmen...	On Node	On Dirac
ne90	SENC1-8<8...	49109445272	Not in Dirac	SENC1-8	app-416_r1...	172.31.68....	READY	☑	□
ne91	SENC1-4<8...	49109445851	Not in Dirac	SENC1-4	app-416_r1...	172.31.68....	READY	☑	□
ne90	SENC1-8<8...	49109445271	Not in Dirac	SENC1-8	app-416_r1...	172.31.68....	READY	☑	□

Figure 9: ESM - “Add to Dirac” button for several CEs



SENC1-8<8> FU2

ID	49109445272
Card Serial Number	4910944527
Index	2
NeId	1
Slot	8
Hardware	SENC1-8
Software	app-416_r15a01
IP Address	172.31.68.212

Status

Dirac	ⓘ
Network Element	✓
Communication	Not in Dirac
Enrollment	READY

Figure 10: ESM - “Add to Dirac” button for single CE

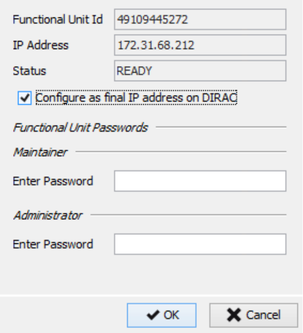
A dialog to provide missing data and to confirm the execution of the enrollment procedure will appear then on the screen.

This dialog is slightly different depending on the current enrollment status of the FU:

- If Enrollment Status of FU is “Factory Default”, then you are requested to provide NEW passwords to protect the access to the unit via ssh (two times to protect against typos).
- In any other case, you are requested to introduce the current password of the units, in order to perform the operations.

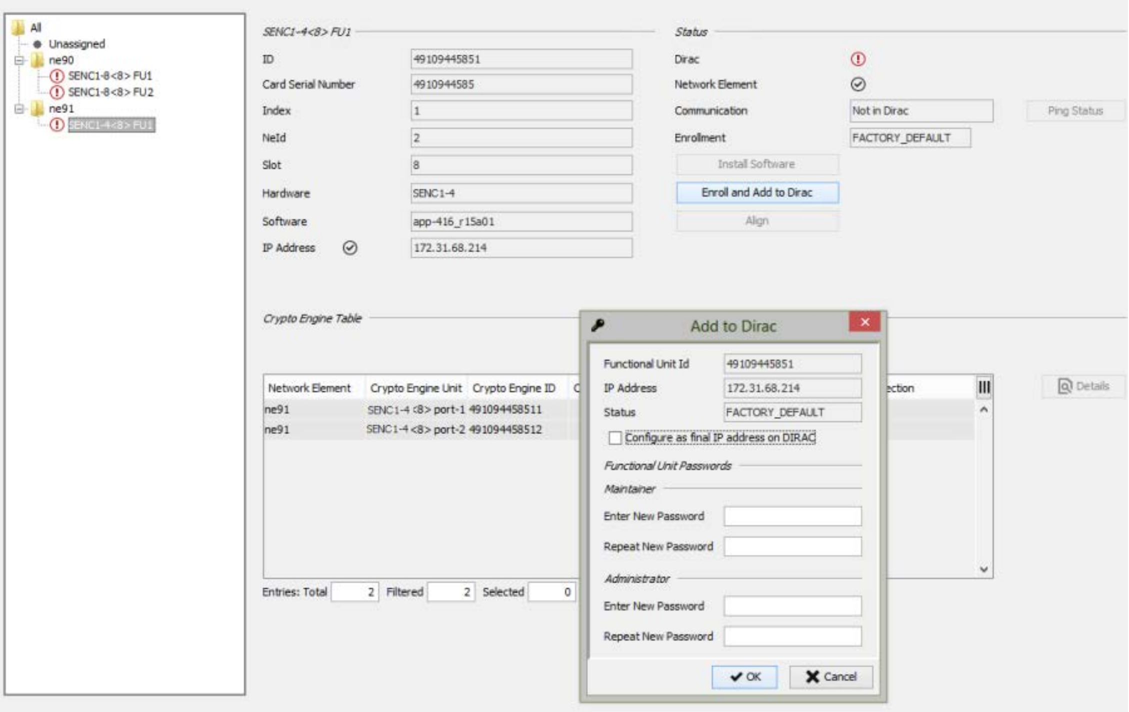
New passwords must be at least 12 characters long and include digits and characters (check this against definition in SENC1 unit)

Also the name of the button may vary slightly depending on the current enrollment status of the unit.



Functional Unit Id 49109445272
IP Address 172.31.68.212
Status READY
☑ Configure as final IP address on DIRAC
Functional Unit Passwords
Maintainer
Enter Password
Administrator
Enter Password

Figure 11: Details of “Add to Dirac”



SENC1-4<8> FU1
ID 49109445851
Card Serial Number 4910944585
Index 1
NeId 2
Slot 8
Hardware SENC1-4
Software app-416_r15a01
IP Address ✓ 172.31.68.214

Status
Dirac !
Network Element ✓
Communication Not in Dirac
Enrollment FACTORY_DEFAULT

Crypto Engine Table

Network Element	Crypto Engine Unit	Crypto Engine ID
ne91	SENC1-4 <8> port-1	491094458511
ne91	SENC1-4 <8> port-2	491094458512

Entries: Total 2 Filtered 2 Selected 0

Add to Dirac
Functional Unit Id 49109445851
IP Address 172.31.68.214
Status FACTORY_DEFAULT
☐ Configure as final IP address on DIRAC
Functional Unit Passwords
Maintainer
Enter New Password
Repeat New Password
Administrator
Enter New Password
Repeat New Password

Figure 12: View with “Add to Dirac” details

The enrollment procedure is basically executing the following operations towards DIRAC and SENC1:

- Set date and time (if in factory default);
- Set passwords (if in factory default);
- Initialize SENC1 (if required);
- Interchange of certificates (SENC1 is provided with DIRAC certificate and DIRAC is provided with SENC1 public certificate);
- Add FU to DIRAC. This also authorizes DIRAC to connect directly to FU SSH and SFTP interfaces with private/&public key authentication.

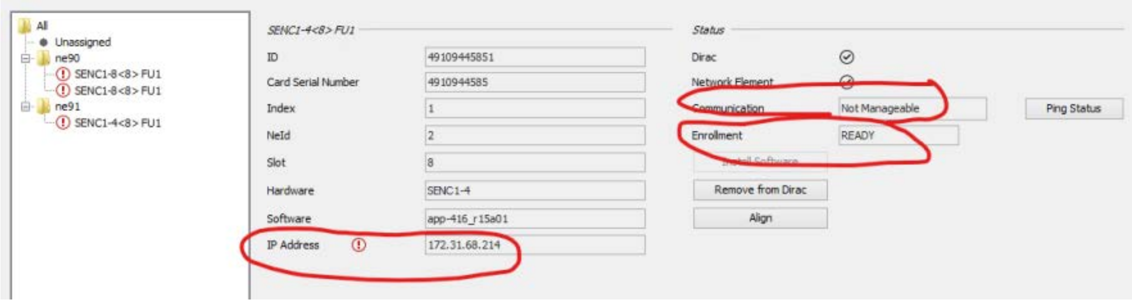
Once the unit is enrolled and known to DIRAC, FOXMAN-UN will be able to work with it.

In the enrollment Dialog (“Add to Dirac”), there is an option named “Configure as final IP address on Dirac”. The IP address is automatically detected from what is configured in the node. During the enrollment procedure, we need to define if this will be the one used as final one for DIRAC or not. The use case behind this option is the initial enrollment of the card in a secure room, where different IP addresses will be used instead of the final one.

If the option is selected, the FU will be created in DIRAC with the already detected IP address; if the option is not selected, the FU will be created in DIRAC without IP address, and later on you will able to propagate the configured IP address to DIRAC.

Once the unit is added to DIRAC, the communication state will change and the unit will be created in DIRAC:

- Communication status will change to real communication status “Manageable” or “Not manageable”;
- Enrollment Status will be set to “Ready”;
- IP Address will show a valid/invalid Status, depending if the option “Configure as final IP” was selected or not.


All
Unassigned
ne90
SENC1-8<8> FU1
SENC1-8<8> FU1
ne91
SENC1-4<8> FU1

SENC1-4<8> FU1
ID: 49109445851
Card Serial Number: 4910944585
Index: 1
NeId: 2
Slot: 8
Hardware: SENC1-4
Software: app-416_r15a01
IP Address: 172.31.68.214

Status
Dirac
Network Element
Communication: Not Manageable
Enrollment: READY

Figure 13: FU View with invalid IP address before alignment

In order to provide the final IP address to DIRAC, you just need to click on the button “Align”.

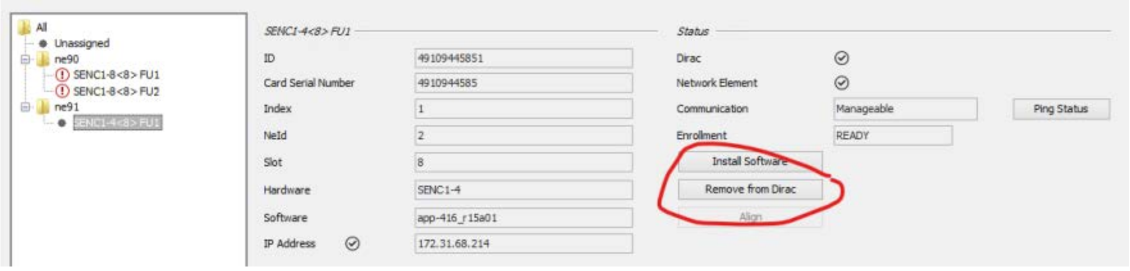
After doing that, all parameters will be configured and the FU status icon should not be red any more.

7.2 SENC1 FU Disenrollment

“Remove from Dirac” is doing exactly what it says: it removes all known information for the selected FU from DIRAC. It will neither move any data from the SENC1 itself or from the Node.

This operation is required to be done always when a FU will not be used any longer in the system in cases such as replacement of a unit, defective unit, old unit, or wrong FU added to DIRAC.

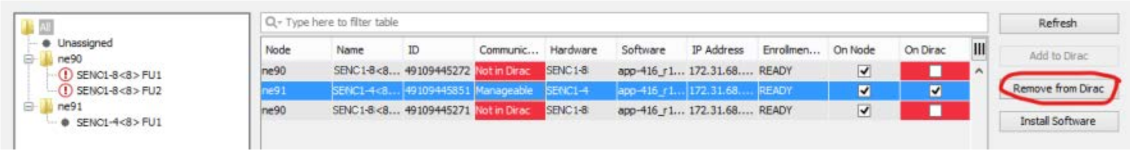
In order to execute the “Remove from Dirac” operation, you can do this via selecting all units in the FU View list and clicking on the “remove from Dirac” button, or selecting one specific FU and doing the same:


All
Unassigned
ne90
SENC1-8<8> FU1
SENC1-8<8> FU2
ne91
SENC1-4<8> FU1

SENC1-4<8> FU1
ID: 49109445851
Card Serial Number: 4910944585
Index: 1
NeId: 2
Slot: 8
Hardware: SENC1-4
Software: app-416_r15a01
IP Address: 172.31.68.214

Status
Dirac
Network Element
Communication: Manageable
Enrollment: READY

Figure 14: ESM - “Remove from Dirac” for single CE



Node	Name	ID	Communic...	Hardware	Software	IP Address	Enrollmen...	On Node	On Dirac
ne90	SENC1-8<8...	49109445272	Not in Dirac	SENC1-8	app-416_r1...	172.31.68....	READY	☑	□
ne91	SENC1-4<8...	49109445851	Manageable	SENC1-4	app-416_r1...	172.31.68....	READY	☑	☑
ne90	SENC1-8<8...	49109445271	Not in Dirac	SENC1-8	app-416_r1...	172.31.68....	READY	☑	□

Figure 15: ESM - “Remove from Dirac” for CE in the list of CEs

i

Please note:

- Remember that DIRAC does not support two FUs with the same IP address. If one FU is already in DIRAC with an IP address, the enrollment of another FU which has the same IP address will fail.

→ Please first remove the old unit.

- Operations on multiple FUs can only be performed as long as the passwords are the same for all units!

7.3 FU Software Upgrade

7.3.1 Via ESW Management - Distribution Wizard

To upgrade the SW of SENC1 FUs in the network, the FOXMAN-UN ESW Distribution Wizard is the preferred tool, supporting SENC1 SW distribution from system release R17A onwards.

To open the ESW Distribution Wizard, select “Network - ESW Management - Distribution Wizard...” from the NEM Desktop menu or click on the “ESW Distribution Wizard” tile of the FOXMAN-UN Homepage (Web UI).

Figure 16: ESW Distribution Wizard tile on FOXMAN-UN Web UI Homepage

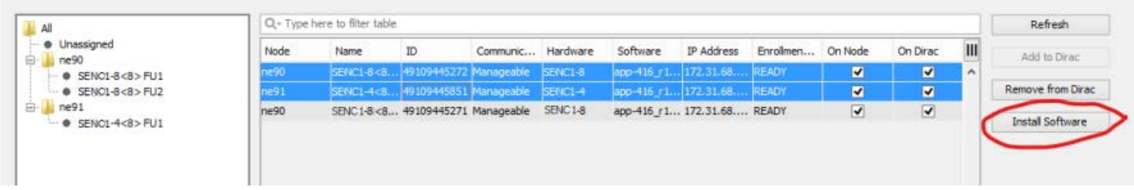
General details of the steps to be executed in the wizard and available options are described in section “Distribution Wizard” of [1KHW002412] FOXMAN-UN ‘NEM GUI Help System’ User Manual. A more detailed procedure is described in [1KHW029028] FOX61x User Manual “SENC1-4, SENC1F4, SENC1-8, SENC1F8”.

7.3.2 Via FOXMAN-UN ESM

As an alternative, FU SW can be upgraded via the FOXMAN-UN ESM. To upgrade the SW of a SENC1, make sure the SW to be installed is available in the “ESW” folder of DIRAC (/opt/dirac/addon/ESW).

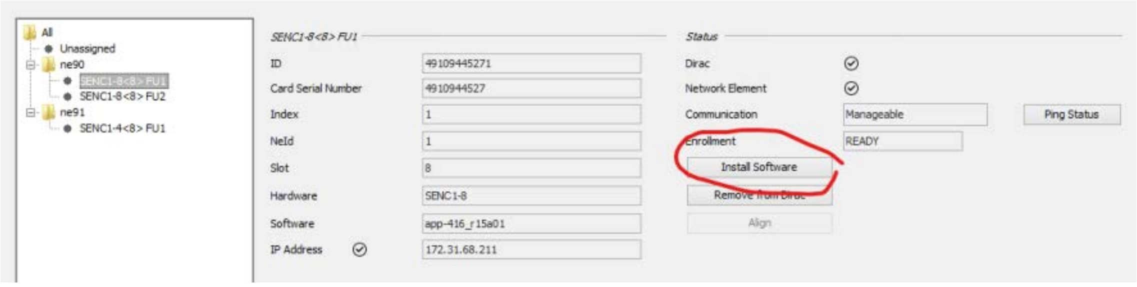
This operation needs to be done on FU level, and therefore can be performed in the FU View, either in the list view or in the FU detailed view.

Once unit has a valid IP address (configured on the unit in the node via FOXCST), the operation can be performed.



Node	Name	ID	Communic...	Hardware	Software	IP Address	Enrollmen...	On Node	On Dirac
ne90	SENC1-8<8...	49109445272	Manageable	SENC1-8	app-416_r1...	172.31.68....	READY	☑	☑
ne91	SENC1-4<8...	49109445851	Manageable	SENC1-4	app-416_r1...	172.31.68....	READY	☑	☑
ne90	SENC1-8<8...	49109445271	Manageable	SENC1-8	app-416_r1...	172.31.68....	READY	☑	☑

Figure 17: FU View - location of the “Install Software” button for several FUs



All
- Unassigned
- ne90
  - SENC1-8<8> FU1
  - SENC1-8<8> FU2
- ne91
  - SENC1-4<8> FU1

SENC1-8<8> FU1

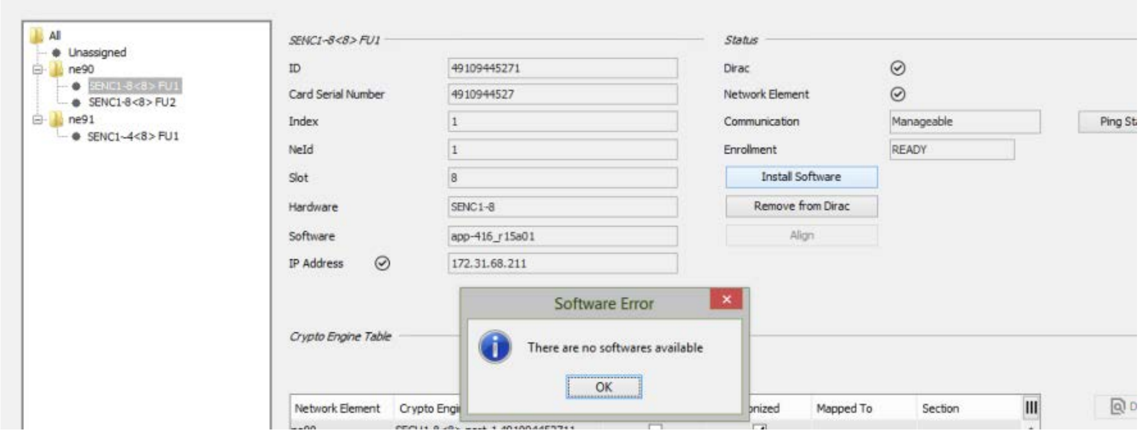
ID: 49109445271
Card Serial Number: 4910944527
Index: 1
NeId: 1
Slot: 8
Hardware: SENC1-8
Software: app-416_r15a01
IP Address ✓: 172.31.68.211

Status

Dirac: ✓
Network Element: ✓
Communication: Manageable
Enrollment: READY

Figure 18: FU Details View - location of the “Install Software” button for one FU

The first time you click on the button, you will see you have no softwares available:



SENC1-8<8> FU1

ID: 49109445271
Card Serial Number: 4910944527
Index: 1
NeId: 1
Slot: 8
Hardware: SENC1-8
Software: app-416_r15a01
IP Address ✓: 172.31.68.211

Status

Dirac: ✓
Network Element: ✓
Communication: Manageable
Enrollment: READY

Crypto Engine Table

Software Error

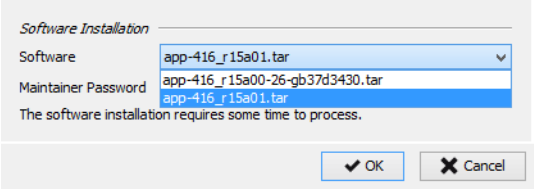
There are no softwares available

Figure 19: FU View message of missing SW

In order to upgrade SENC1 SW, you need to provide released SW to the DIRAC system.
This is done by means of

- importing SENC1 software to the FOXMAN-UN database via the ESW Distribution Wizard or
- copying selected SW to the DIRAC server, inside the folder /opt/dirac/addon/ESW as dirac user; please copy the provided SW, i.e., the application tar file “app-416_xxxx.tar” to the specified folder.

Once done, the application software tars will be available for the upgrade procedure of any FU in the system:



Software Installation

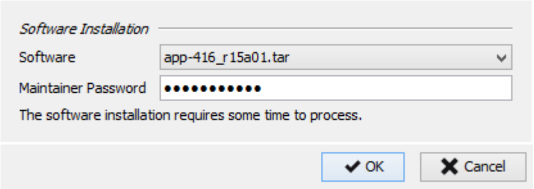
Software: app-416_r15a01.tar
- app-416_r15a00-26-gb37d3430.tar
- app-416_r15a01.tar

Maintainer Password:

The software installation requires some time to process.

Figure 20: Selection of SW to be installed

Please select required SW and provide maintainer password of the related FU.



Software Installation

Software: app-416_r15a01.tar
Maintainer Password: ●●●●●●●●●●●

The software installation requires some time to process.

Figure 21: Enter Password for Maintainer

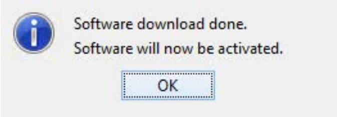
Click on the OK button.

The operation is composed mainly of 2 steps:

- Copying SW upgrade tar file to FU,
- Installing SW.

The overall procedure can take between 1 and 5 minutes, depending on the network speed.

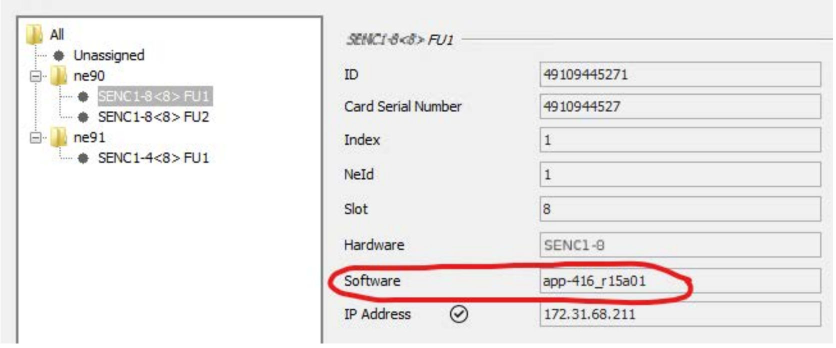
Once the SW is downloaded and the SW upgrade starts, you will see a message window: The SW upgrade will start and eventually the FU will be restarted.



Software download done.
Software will now be activated.

Figure 22: SW Download Confirmation

The FU will appear as “not manageable” in the FU View (“Communication” field) for some time. After the unit is restarted, new SW will be automatically detected and updated on the FU shown data.



SENC1-8<8> FU1

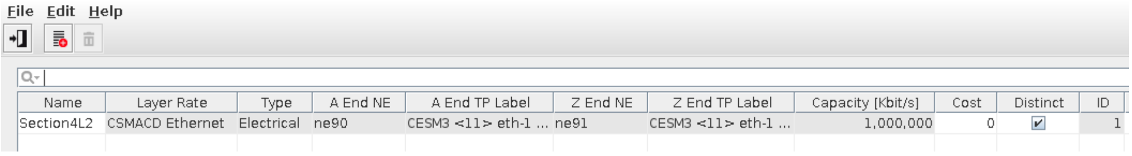
ID	49109445271
Card Serial Number	4910944527
Index	1
NeId	1
Slot	8
Hardware	SENC1-8
Software	app-416_r15a01
IP Address ✓	172.31.68.211

Figure 23: FU Status after successful SW installation

Please note:
The “Install Software” process will just download the file and rename it in order to start the upgrade. If the upgrade was successful you will see the new SW in the ESM FU View. If it was not successful you will still see the old SW. No error message will be issued.

7.4 L2 Encryption

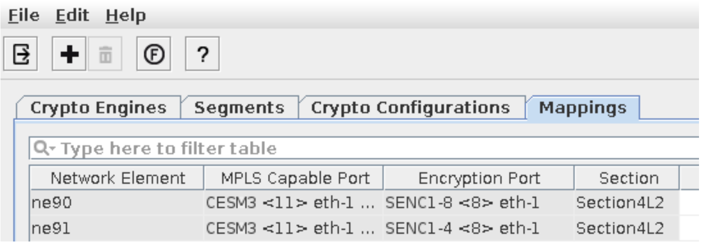
For setting up L2 encryption, a section must be present between the MPLS capable ports:



Name	Layer Rate	Type	A End NE	A End TP Label	Z End NE	Z End TP Label	Capacity [Kbit/s]	Cost	Distinct	ID
Section4L2	CSMACD Ethernet	Electrical	ne90	CESM3 <11> eth-1 ...	ne91	CESM3 <11> eth-1 ...	1,000,000	0	☑	1

Figure 24: Section between two MPLS Capable Ports, view in Section Manager

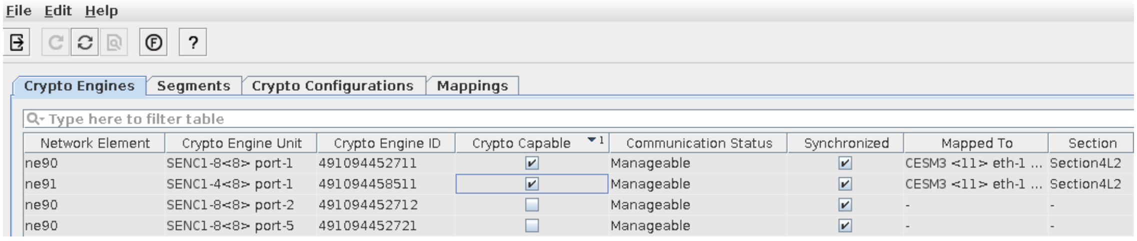
CEs must be mapped to the MPLS capable ports (two ports per section are therefore required):



Network Element	MPLS Capable Port	Encryption Port	Section
ne90	CESM3 <11> eth-1 ...	SENC1-8 <8> eth-1	Section4L2
ne91	CESM3 <11> eth-1 ...	SENC1-4 <8> eth-1	Section4L2

Figure 25: Section with two Ports in the ESM

CEs must be properly configured (Crypto Capable):

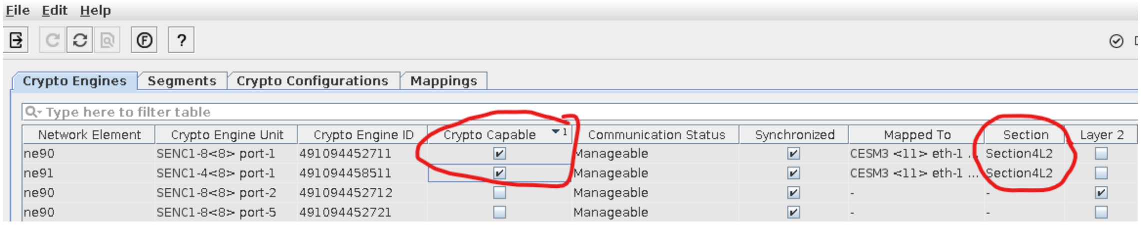


Network Element	Crypto Engine Unit	Crypto Engine ID	Crypto Capable	Communication Status	Synchronized	Mapped To	Section
ne90	SENC1-8<8> port-1	491094452711	☑	Manageable	☑	CESM3 <11> eth-1 ...	Section4L2
ne91	SENC1-4<8> port-1	491094458511	☑	Manageable	☑	CESM3 <11> eth-1 ...	Section4L2
ne90	SENC1-8<8> port-2	491094452712	☐	Manageable	☑	-	-
ne90	SENC1-8<8> port-5	491094452721	☐	Manageable	☑	-	-

Figure 26: Crypto Engines in the ESM must be Crypto Capable

7.4.1 Enabling L2 Encryption

As stated before, this operation can only be performed if 2 “Crypto Capable” Crypto Engines are connected to the same section:

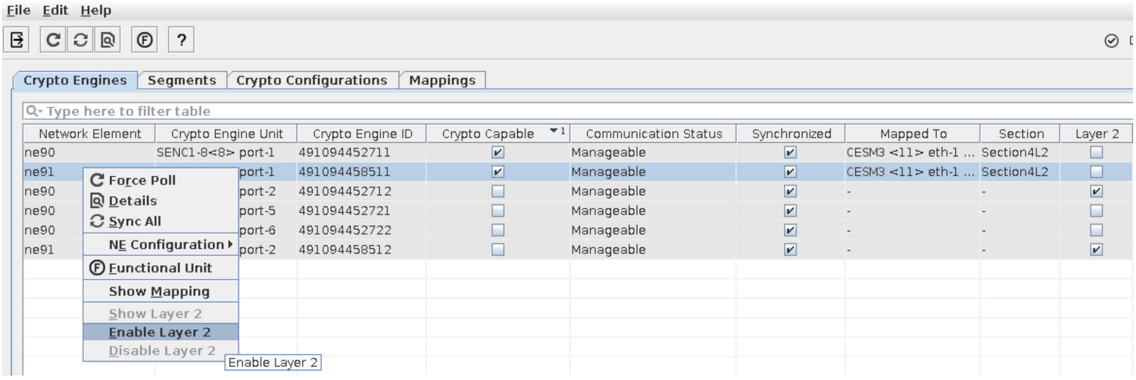


Network Element	Crypto Engine Unit	Crypto Engine ID	Crypto Capable	Communication Status	Synchronized	Mapped To	Section	Layer 2
ne90	SENC1-8<8> port-1	491094452711	☑	Manageable	☑	CESM3 <11> eth-1 ..	Section4L2	☐
ne91	SENC1-4<8> port-1	491094458511	☑	Manageable	☑	CESM3 <11> eth-1 ...	Section4L2	☐
ne90	SENC1-8<8> port-2	491094452712	☐	Manageable	☑	-	-	☑
ne90	SENC1-8<8> port-5	491094452721	☐	Manageable	☑	-	-	☐

Figure 27: Two Crypto Capable CEs as Section End Points

In such a case the easiest way to configure L2 is to open the context menu on the CE tab, and click on “Enable L2”. The menu will be enabled only if the conditions are fulfilled.

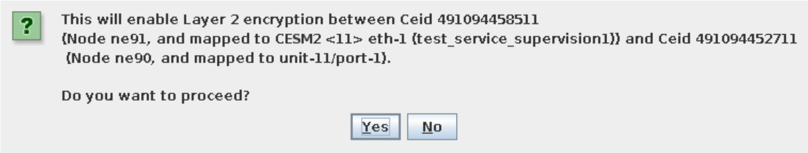
To open the context menu, right-click on any of the 2 CEs connected to the required section where you would like to encrypt L2 protocol data.



Network Element	Crypto Engine Unit	Crypto Engine ID	Crypto Capable	Communication Status	Synchronized	Mapped To	Section	Layer 2
ne90	SENC1-8<8> port-1	491094452711	☑	Manageable	☑	CESM3 <11> eth-1 ...	Section4L2	☐
ne91	port-1	491094458511	☑	Manageable	☑	CESM3 <11> eth-1 ...	Section4L2	☐
ne90	port-2	491094452712	☐	Manageable	☑	-	-	☑
ne90	port-5	491094452721	☐	Manageable	☑	-	-	☐
ne90	port-6	491094452722	☐	Manageable	☑	-	-	☐
ne91	port-2	491094458512	☐	Manageable	☑	-	-	☑

Figure 28: Context Menu on CE to Enable L2 Encryption

This will pop up a message window which will point out all relevant information and which will require a user confirmation.

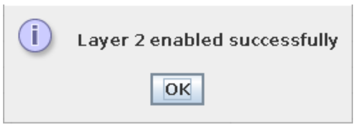


This will enable Layer 2 encryption between Ceid 491094458511 (Node ne91, and mapped to CESM2 <11> eth-1 (test_service_supervision1)) and Ceid 491094452711 (Node ne90, and mapped to unit-11/port-1).

Do you want to proceed?

Figure 29: Confirmation dialog for Enabling L2 Encryption

Once confirmed, the operation will create the required configuration on both involved CEs.



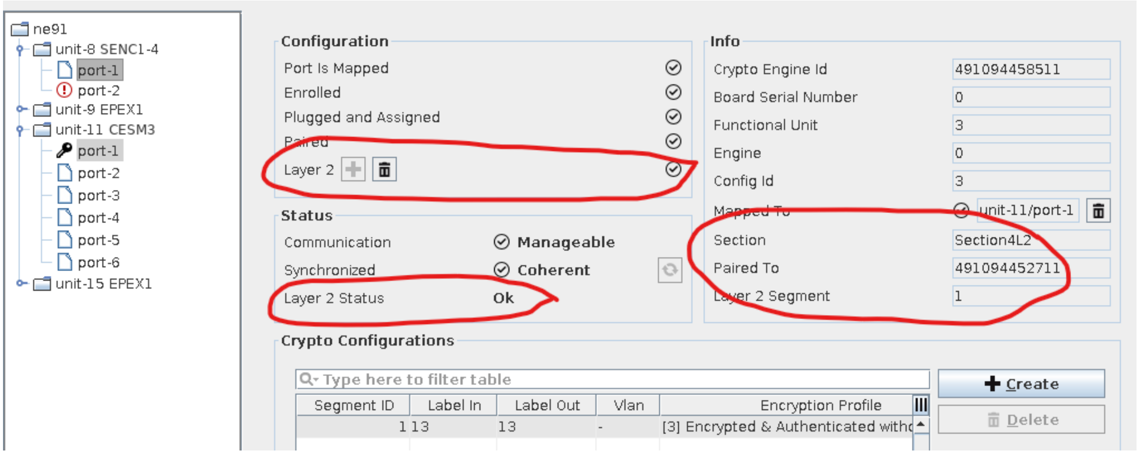
Layer 2 enabled successfully

Figure 30: L2 Encryption is Confirmed

7.4.2 Checking L2 Status

Layer 2 is a property that can be enabled/disabled/wrongly configured/properly configured per CE.

To check the status you need to go to the CE details and see the status of the L2 configuration for that specific CE:



Configuration

- Port Is Mapped ✓
- Enrolled ✓
- Plugged and Assigned ✓
- Paired ✓
- Layer 2 ✓

Status

- Communication: Manageable
- Synchronized: Coherent
- Layer 2 Status: Ok

Info

Crypto Engine Id	491094458511
Board Serial Number	0
Functional Unit	3
Engine	0
Config Id	3
Mapped To	unit-11/port-1
Section	Section4L2
Paired To	491094452711
Layer 2 Segment	1

Crypto Configurations

Segment ID	Label In	Label Out	Vlan	Encryption Profile
1	13	13	-	[3] Encrypted & Authenticated withc

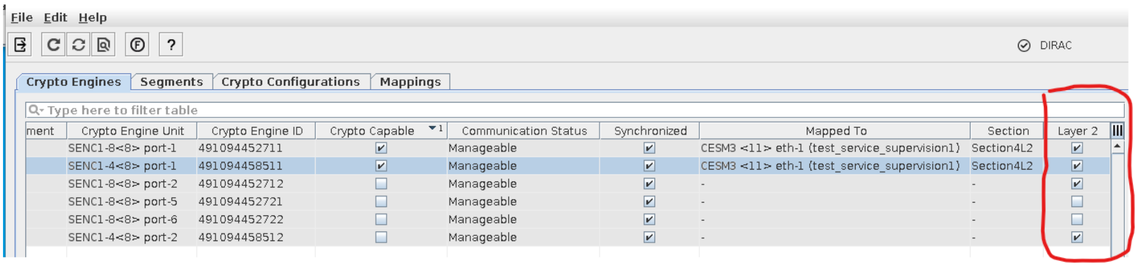
Figure 31: View L2 Status of Specific CE

At this point you can see all L2 related information for that specific CE:

- Configuration: Layer2: is there a L2 configuration for the selected CE?
- Status: Is the configuration in proper status?
- Has the CE a valid related section?
- To which CE is the current one paired? (via mappings and sections)
- Which one is the Crypto Segment describing the current L2 configuration?

There are other places in the system where you can check the L2 status:

- CE tab: Here you can see whether a specific CE has a L2 configuration (we don't know at this point the status of the L2 configuration).

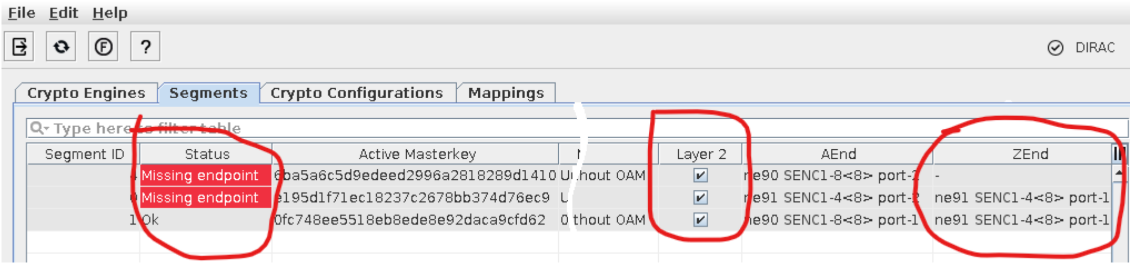


ment	Crypto Engine Unit	Crypto Engine ID	Crypto Capable	Communication Status	Synchronized	Mapped To	Section	Layer 2
	SENC1-8<8> port-1	491094452711	☑	Manageable	☑	CESM3 <11> eth-1 (test_service_supervision1)	Section4L2	☑
	SENC1-4<8> port-1	491094458511	☑	Manageable	☑	CESM3 <11> eth-1 (test_service_supervision1)	Section4L2	☑
	SENC1-8<8> port-2	491094452712	□	Manageable	☑	-	-	☑
	SENC1-8<8> port-5	491094452721	□	Manageable	☑	-	-	□
	SENC1-8<8> port-6	491094452722	□	Manageable	☑	-	-	□
	SENC1-4<8> port-2	491094458512	□	Manageable	☑	-	-	☑

Figure 32: Check Status of L2 Encryption in ESM - CE Tab

- Segment tab: If you sort rows based on the L2 column, you will see all Crypto Segments which are defining the L2 configuration. You can check the required CE by filtering A-End or Z-End points.

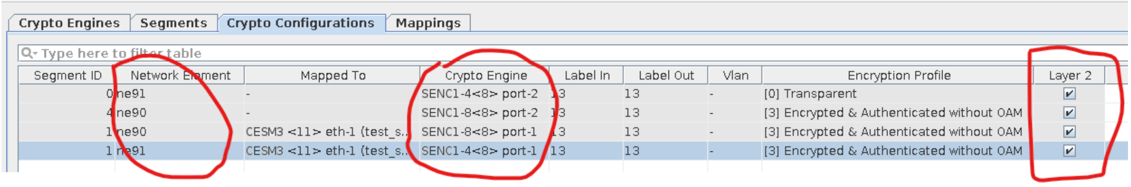
The status of the segments is also specifying the status of the L2 Crypto Configuration.



Segment ID	Status	Active Masterkey	I	Layer 2	AEnd	ZEnd
4	Missing endpoint	6ba5a6c5d9edeed2996a2818289d1410	Ui.hout OAM	☑	ne90 SENC1-8<8> port-2	-
0	Missing endpoint	e195d1f71ec18237c2678bb374d76ec9	U	☑	ne91 SENC1-4<8> port-2	ne91 SENC1-4<8> port-1
1	Ok	0fc748ee5518eb8ede8e92daca9cfd62	0 thout OAM	☑	ne90 SENC1-8<8> port-1	ne91 SENC1-4<8> port-1

Figure 33: L2 Encryption Status in ESM - Segments

- Crypto Configuration: This refers to the defined L2 configuration on each of the CEs; here you are not able to see any information of the status or of the link information between 2 CEs; nevertheless you can filter to see L2 information of specific CEs:



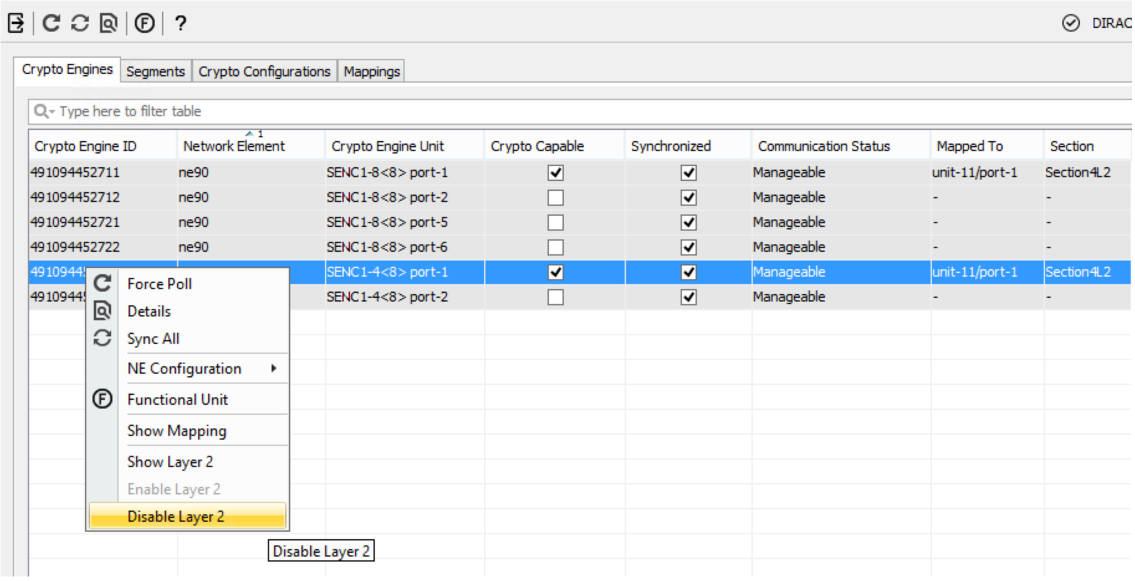
Segment ID	Network Element	Mapped To	Crypto Engine	Label In	Label Out	Vlan	Encryption Profile	Layer 2
0	ne91	-	SENC1-4<8> port-2	13	13	-	[0] Transparent	☑
4	ne90	-	SENC1-8<8> port-2	13	13	-	[3] Encrypted & Authenticated without OAM	☑
1	ne90	CESM3 <11> eth-1 (test_s...	SENC1-8<8> port-1	13	13	-	[3] Encrypted & Authenticated without OAM	☑
1	ne91	CESM3 <11> eth-1 (test_s...	SENC1-4<8> port-1	13	13	-	[3] Encrypted & Authenticated without OAM	☑

Figure 34: L2 Information in Crypto Configuration Tab (Filtered)

7.4.3 Removing L2 Configuration

This can be done in the CE tab or in the CE Detailed View.

On CE tab, just open the context menu, and click on “Disable L2”:



Crypto Engine ID	Network Element	Crypto Engine Unit	Crypto Capable	Synchronized	Communication Status	Mapped To	Section
491094452711	ne90	SENC1-8<8> port-1	☑	☑	Manageable	unit-11/port-1	Section4L2
491094452712	ne90	SENC1-8<8> port-2	□	☑	Manageable	-	-
491094452721	ne90	SENC1-8<8> port-5	□	☑	Manageable	-	-
491094452722	ne90	SENC1-8<8> port-6	□	☑	Manageable	-	-
491094		SENC1-4<8> port-1	☑	☑	Manageable	unit-11/port-1	Section4L2
491094		SENC1-4<8> port-2	□	☑	Manageable	-	-

Figure 35: Context Menu on CE to Disable L2 Encryption

You will get a warning window to which you need to agree:

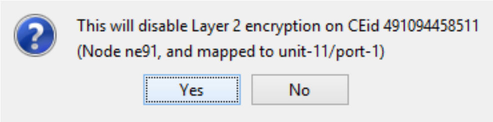
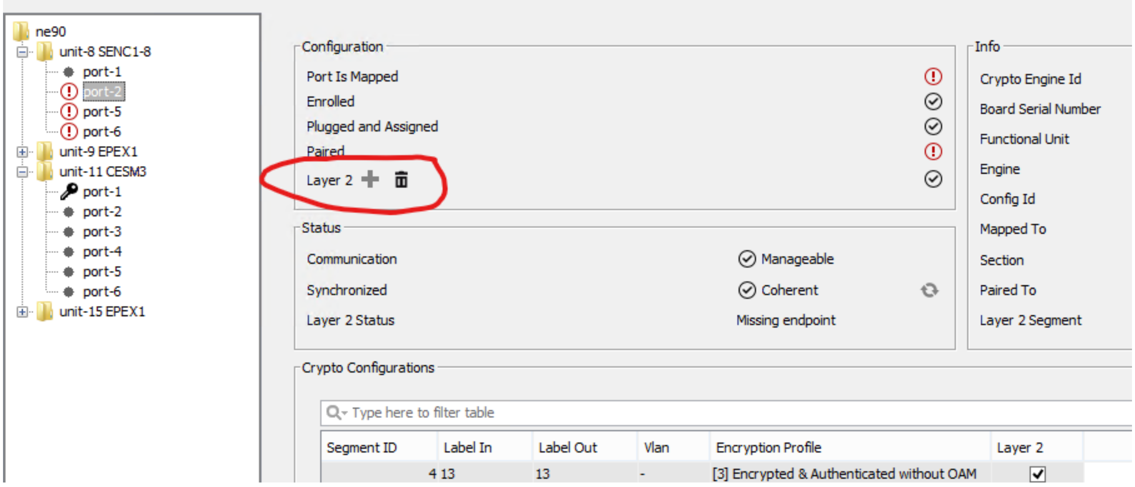

This will disable Layer 2 encryption on CEid 491094458511
(Node ne91, and mapped to unit-11/port-1)

Figure 36: Confirm Disabling of L2 Encryption

The procedure is similar if you disable L2 encryption from CE Details window, but in this case you need to click on the trash can button near the Layer 2 configuration.



Configuration

- Port Is Mapped !
- Enrolled ✓
- Plugged and Assigned ✓
- Paired !
- Layer 2 ✓

Status

- Communication: Manageable
- Synchronized: Coherent
- Layer 2 Status: Missing endpoint

Segment ID	Label In	Label Out	Vlan	Encryption Profile	Layer 2
4	13	13	-	[3] Encrypted & Authenticated without OAM	☑

Figure 37: Disabling L2 Encryption from CE Details Dialog

All L2 information on the ESM windows / tabs will be updated accordingly.

Please note:

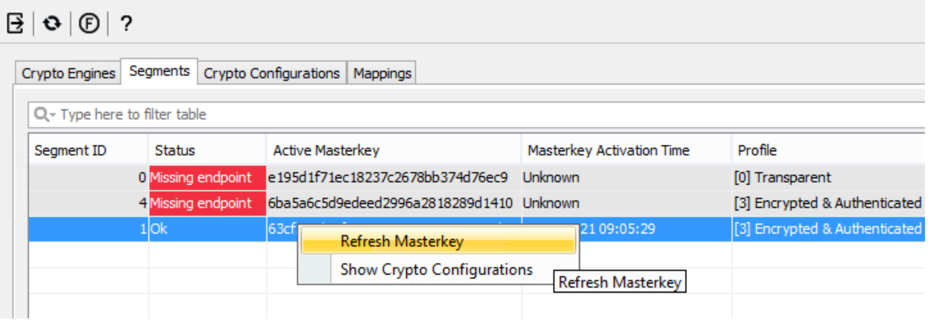
- L2 encryption refers only to the encryption of some L2 protocols (not all L2 data).
- When Enabling L2 encryption, you need to select the CE of one side, and when executing, the configuration will be created on both sides. When disabling L2 encryption, this must be done on all CEs involved one by one.
- When using a new FU, L2 protocol is enabled and in transparent mode by default. Recommended way to proceed is to delete default L2 configuration and reconfigure proper one.

7.5 Master Key Refresh

A master key (MK) refresh needs to be done on the ESM - Segments tab.

The only requirement associated with the operation is that a Crypto Segment must have 2 and only 2 Crypto Configurations associated.

For a MK refresh, you open the context menu of the selected CS and select “Refresh Masterkey”.



Segment ID	Status	Active Masterkey	Masterkey Activation Time	Profile
0	Missing endpoint	e195d1f71ec18237c2678bb374d76ec9	Unknown	[0] Transparent
4	Missing endpoint	6ba5a6c5d9edeed2996a2818289d1410	Unknown	[3] Encrypted & Authenticated
1	Ok	63cf	21 09:05:29	[3] Encrypted & Authenticated

Figure 38: Context Menu for Master Key Refresh

If everything goes smoothly you will see a short message box saying that the refreshing operation was successful.

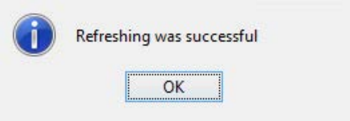

Refreshing was successful

Figure 39: Confirmation: Master Key Refresh Success

8 Operation

8.1 DIRAC Server Use Cases

i **Please note:**
It is assumed that the DIRAC application is installed on the same server as the FOXMAN-UN.

8.1.1 CLI Login on the DIRAC Server

To do a CLI login,

Proceed as follows:

1. Login as dirac user on the Linux machine the DIRAC server is running and open a terminal.
   - If not physically present at the server machine, as SSH login for the dirac user is prevented for security reasons, the recommendation is to create a separate local user on the DIRAC server to be able to log in via SSH.
   - Then, from a terminal on your remote machine start an SSH session as the newly created separate local user to the machine running the DIRAC server. Once logged in, change to user dirac via the “su dirac” command.
2. In the terminal start the DIRAC server CLI:
   ```
   $ Cli.sh
   ```
   or
   ```
   $ /opt/dirac/bin/Cli.sh
   ```
3. Check the available commands:
   ```
   dirac> help
   ```

Result: You have successfully logged in to the DIRAC server and started its CLI.

End of instruction

8.1.2 CLI Logout from the DIRAC Server

To do a CLI logout,

Proceed as follows:

1. Exit from the DIRAC CLI:
   ```
   dirac> exit
       $
   ```
2. Terminate the SSH session or exit from the terminal:
   ```
   $ exit
   ```

Result: You have successfully logged out from the DIRAC CLI and terminated the SSH session.

End of instruction

8.1.3 Shutdown and Restart of the DIRAC Server from DIRAC CLI

To shut down the DIRAC server,

Proceed as follows:

1. Shut down the DIRAC server from the DIRAC CLI. All DIRAC processes are stopped:

```
dirac> dirac-shutdown
OK
dirac>
```

2. Check the DIRAC server status:

```
dirac> status
 Process name:     diracserverd
 Process Id:       0
 Process state:    inactive
 Process substate: dead
 Running since:    Fri 2021-05-28 14:08:01 CEST
 Server status:    inactive
 QRNG source:      unknown
 QRNG status:      unknown
```

Result: You have successfully shut down the DIRAC server.

End of instruction

To restart the DIRAC server,

Proceed as follows:

1. Restart the DIRAC server from the DIRAC CLI. All DIRAC processes are stopped (if running) and restarted:

```
dirac> dirac-restart
Restarting the Dirac server will take a few moments.
............
OK
dirac>
```

2. Check the DIRAC server status:

```
dirac> status
 Process name:     diracserverd
 Process Id:       552325
 Process state:    active
 Process substate: running
 Running since:    Wed 2022-08-03 11:55:37 CEST
 Server status:    active
 QRNG source:      Quantis (S/N not available)
 QRNG status:      OK
```

Result: You have successfully restarted the DIRAC server.

End of instruction

8.1.4 Start and Stop DIRAC Processes from a Terminal

The commands to start or stop the DIRAC processes are available in the directory “/opt/dirac/bin”.

To start the DIRAC processes,

Proceed as follows:

1. As dirac user open a terminal and enter the command “diracstart”:

```
[dirac@myserver]$ diracstart
 Starting DIRAC target services

Done.
```

```
[dirac@myserver]$
```

Result: You have successfully started the DIRAC processes.

End of instruction

To stop the DIRAC processes,

Proceed as follows:

1. As dirac user open a terminal and enter the command “diracstop”:

```
[dirac@myserver]$ diracstop
 Stopping DIRAC target services

Done.

[dirac@myserver]$
```

Result: You have successfully stopped the DIRAC processes.

End of instruction

8.1.5 DIRAC Server has Booted without QRNG

In case the DIRAC server has booted without operational Quantis device the DiracServer and the QuantisWatcher services are not active. To recover from this situation perform the following steps:

Recover from booting without QRNG

→ Restart the DIRAC server with a QRNG. Proceed as follows:

1. Plug and configure a valid QRNG, e.g. a Quantis device.
   - Please refer to [1KHW029081] User Manual “DIRAC - DIRAC Server Installation”.
2. Login to the DIRAC server.
   - See section 8.1.1 CLI Login on the DIRAC Server (on page 32).
3. Reboot the DIRAC server.
   - See section 8.1.3 Shutdown and Restart of the DIRAC Server from DIRAC CLI (on page 32).
4. Check the DIRAC server status. All services must be active

```
dirac> status
 Process name:     diracserverd
 Process Id:       3493530
 Process state:    active
 Process substate: running
 Running since:    Wed 2024-04-03 13:20:39 CEST
 Server status:    active
 QRNG source:      Quantis (S/N not available)
 QRNG status:      OK
```

Result: You have successfully rebooted the DIRAC server with an active QRNG.

End of instruction

8.1.6 Backup and Restore of DIRAC Server Persistent Data

The DIRAC server maintains a database with the following persistent data:

- DIRAC Device Management Channel private key

- DIRAC private and public keys for SSH and SFTP authentication against FU
- SENC1 Functional Units public keys
- DIRAC-FOXMAN-UN HTTPS certificate
- Topology database (SENC1 Crypto Engines and MPLS tunnels endpoints)
- Local log files

8.1.6.1 Backup and Restore with Scripts

The backup and restore procedures for the DIRAC server can be done with scripts available at /opt/dirac/bin:

```
Syntax:   nemdiracbackup [backup filename]
Syntax:   nemdiracrestore [backup filename]
```

i **Please note:**
The “backup filename” parameter is optional.

→ Without a backup filename the scripts create and use per default a backup file named “nemdiracbackup.tar” stored in the /opt/dirac/bin directory.

The scripts restore and backup the following persistent data:

- DIRAC Device Management Channel key pairs
- SENC1 Crypto Engine public keys
- Topology database (SENC1 Crypto Engines and MPLS tunnels endpoints)

Backup and restore of DIRAC server

The persistent data of the DIRAC server shall be restored.

→ Backup. Proceed as follows:

1. Login as dirac user on the Linux machine.
2. Open a terminal.
3. Move to the directory /opt/dirac/bin:
   ```
   $ cd /opt/dirac/bin
   ```
4. Create a backup of the DIRAC server:
   ```
   $ ./nemdiracbackup
   ```
   - The script creates or updates the backup file nemdiracbackup.tar in the folder “/opt/dirac/bin”.

Result: The backup of the DIRAC server persistent data is done.

→ Restore. Proceed as follows:

1. Login as dirac user on the Linux machine.
2. Open a terminal.
3. Move to the directory /opt/dirac/bin:
   ```
   $ cd /opt/dirac/bin
   ```
4. Restore the DIRAC server:
   ```
   $ ./nemdiracrestore
   ```
   - The script restores the data from the backup file “/opt/dirac/bin/nemdiracbackup.tar”.
   - The script reboots the DIRAC server to load the backup.

Result: The DIRAC server is restored.

End of instruction

i

Please note:
If the topology database has been modified between the backup and restore events the modifications must be done again.

8.1.6.2 Virtual Machine Snapshot

In case the DIRAC server is installed on a Linux Virtual Machine, running on an Oracle VirtualBox, a snapshot of the virtual machine provides the DIRAC server configuration with all persistent data.

The virtual machine snapshot restore operation restores the persistent data to the DIRAC server.

Backup and restore of DIRAC server

The persistent data of the DIRAC server shall be restored. It is assumed that after the backup process the SENC1 Functional Units and MPLS tunnel endpoints have been modified.

→ Backup. Proceed as follows:

1. Create a snapshot of the DIRAC server virtual machine at time T1.

Result: The backup of the DIRAC server persistent data is done.

→ Modify the SENC1 network setup. Proceed as follows:

1. Create SENC1 Crypto Engines on the DIRAC server at time T2.
2. Delete SENC1 Crypto Engines on the DIRAC server at time T3.
3. FOXMAN-UN creates and pushes new MPLS tunnels to the DIRAC server T4.

Result: Crypto Engines and tunnels have been modified in the DIRAC server.

→ Restore. Proceed as follows:

1. At time T5 restore the DIRAC server virtual machine snapshot of time T1.
2. Reboot the DIRAC server.
3. Setup date and time of the DIRAC server.
   - The DIRAC server checks the communication with all SENC1 Functional Units and performs a realignment of the DNMS tables if necessary:
   - Crypto Engines created: The Crypto Engines created at T2 are not checked.
   - Crypto Engines deleted: Communication with the Crypto Engines deleted at time T3 is not possible.
4. In the DIRAC server add the Functional Units from time T2.
   - The DIRAC server synchronizes the DNMS tables with the SENC1 units.
5. In the DIRAC server delete the Functional Units from time T3.
6. In FOXMAN-UN align the new MPLS tunnels created at T4 with the DIRAC server.

Result: The DIRAC server is restored and realigned with all SENC1 modifications.

End of instruction

8.2 Master Key Generation and Distribution

Master Keys are only generated and distributed …

- on request of the FOXMAN-UN when deploying an encrypted tunnel, or
- on request from the FOXMAN-UN ESM.

Master Keys are generated for a particular LSP and distributed to all MPLS tunnel endpoints terminating this LSP.

In the SENC1 Crypto Engine the new Master Key is stored in the Master Key bank which is currently not used. The switching of the active Master Key to the newly deployed Master Key is done according to the procedure described in section 4.4 DIRAC Key Management (on page 14).

Please note:
The example below uses the following parameters
→ SENC1 Crypto Engine A identifier = 491091199911
→ SENC1 Crypto Engine B identifier = 491091199912
→ Label switched path identifier = 100

Master Key generation and distribution

→ Generate a new Master Key. Proceed as follows:

1. Login as dirac user on the Linux machine.
2. Open a terminal.
3. Connect to the DIRAC server:
   ```
   $ /opt/dirac/bin/Cli.sh
   ```
4. Check the available Crypto Engines in the DIRAC server:

```
dirac> crypto-engine --list
 Ce Id        |Engine|Dci|Sci |Status
 491092685711 1       15  42   OK
 491092685712 2       7   22   OK
 491092685721 1       9   33   OK
 491092685722 2       2   2    OK
 491092685811 1       711 1780 OK
 491092685812 2       701 1752 OK
 491092685821 1       8   17   OK
 491092685822 2       2   2    OK
```

5. Check the configured crypto segments:

```
dirac> crypto-segment --list
 Segment|Status|Profile               |Layer |Active Master Key               |Activated At
 2       Ok     Encrypt & Authenticate LAYER2 6ba5a6c5d9edeed2994b4422448c1730 23-05-2021 07:42:11
```

6. Generate a new Master Key for one of the listed segments:

```
dirac> master-key --renew --segment_id 2
            Result:                 true
            Description:            "Master key of all crypto engines refreshed:
                                    491092685711"
```

7. Check the Master Key usage for the specific segment:

```
dirac> crypto-segment --list
 Segment|Status|Profile               |Layer |Active Master Key               |Activated At
 2       Ok     Encrypt & Authenticate LAYER2 0fe638ee4427eb3ede3e81cdac8ffd53 24-05-2021 07:19:14
```

Result: The Master Key for a specific segment is renewed.

End of instruction

8.3 SENC1 Unit Handling

For the procedures to add, remove and replace a SENC1 unit in a FOX61x network element refer to [1KHW029028] FOX61x User Manual “SENC1-4, SENC1F4, SENC1-8, SENC1F8”.

8.4 DIRAC Server Troubleshooting Logs

Several log files are accessible by the dirac user in the /var/log/dirac directory.

All log files are available in up to 10 revisions with a size of 2 MB each. The revisions are numbered *.log.1 to *.log.10, and the log file used for the actual information storage is named *.log. The log file storage is handled as shown in Figure 40. All log files are persistent across a reboot.

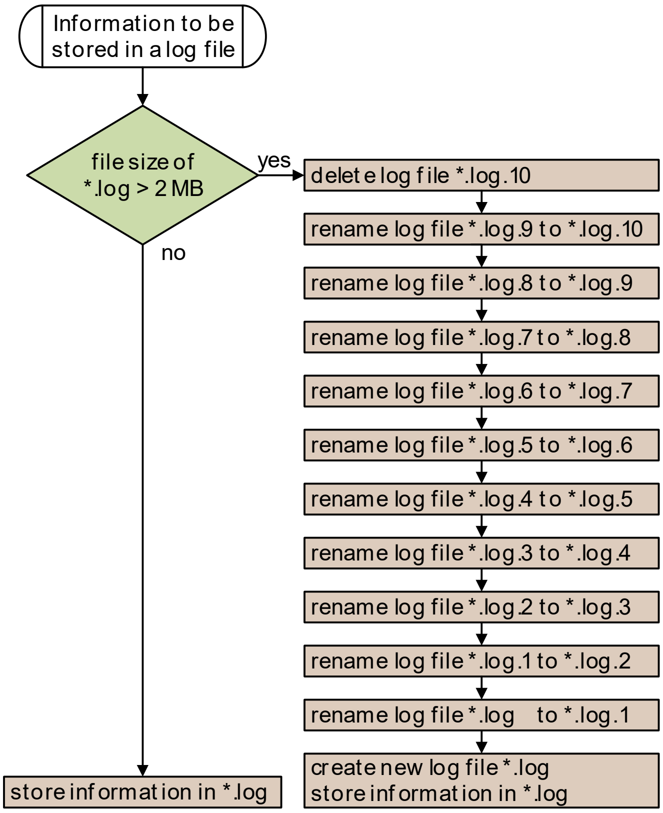

Information to be stored in a log file
file size of *.log > 2 MB
yes
no
delete log file *.log.10
rename log file *.log.9 to *.log.10
rename log file *.log.8 to *.log.9
rename log file *.log.7 to *.log.8
rename log file *.log.6 to *.log.7
rename log file *.log.5 to *.log.6
rename log file *.log.4 to *.log.5
rename log file *.log.3 to *.log.4
rename log file *.log.2 to *.log.3
rename log file *.log.1 to *.log.2
rename log file *.log to *.log.1
create new log file *.log
store information in *.log
store information in *.log

Figure 40: Log file handling in the DIRAC server

Log files accessible in the /var/log/dirac directory are:

- server_errorWarning.log

  The log file gathers WARN, ERROR and FATAL logs from the DIRAC CLI, the DNMS Portal, the DNMS Router and the NMS Application Server.

- server.log

  The log file gathers INFO, WARN, ERROR and FATAL logs from the DIRAC Server.

8.5 FOXMAN-UN Use Cases

8.5.1 Add the FOX61x Network Elements to the FOXMAN-UN FOX61x Agent

Please note:
For a description of how to create a FOXMAN-UN FOX61x agent and how to add the FOX61x network elements to the FOX61x agent please refer to [1KHW002412] FOXMAN-UN 'NEM GUI Help System' User Manual.

8.5.2 Deploy an Encrypted MPLS-TP Tunnel in FOX61x Network Elements

Please note:
For a description of how to configure encrypted MPLS tunnels in FOXMAN-UN refer to [1KHW002412] FOXMAN-UN 'NEM GUI Help System' User Manual.

To deploy an encrypted MPLS-TP tunnel in a FOX61x network element the following main steps have to be performed

- Add the FOX61x network elements to the FOXMAN-UN FOX61x agent. See section 8.5.1 Add the FOX61x Network Elements to the FOXMAN-UN FOX61x Agent (on page 39).
- Create the mapping between the core unit and SENC1 unit front ports.
- Add a MPLS tunnel between two FOX61x network elements:
  - Create a service profile
  - Add network elements
  - Create the link between the two network elements
  - Create the tunnel
  - Save and deploy the tunnel

The example below shows how a FOXMAN-UN operator adds a new MPLS tunnel endpoint.

8.5.2.1 Prerequisites

The following prerequisites must be met:

- The DIRAC server is up and running.
- The target SENC1 Functional Units must be enrolled and deployed in the FOX61x network element, including the cabling between the front ports of the core unit and the SENC1 unit.
- The layer 2 packet encryption must be configured on the SENC1 Crypto Engines.
- The encryption parameters (inter-frame gap and SCC generation) must be configured on the MPLS-TP ports of the core unit. For details refer to the section “Encryption Parameters on the Core Unit” in the SENC1 unit user manual ([1KHW029028] FOX61x User Manual “SENC1-4, SENC1F4, SENC1-8, SENC1F8”).
- FOXMAN-UN and the DIRAC server should both be synchronized via NTP.

8.5.2.2 Add a MPLS Tunnel between two FOX61x Network Elements

Create and deploy an MPLS tunnel

→ Create the mapping between the core unit and the SENC1 unit ports. Proceed as follows:

1. In FOXMAN-UN start the Ethernet Security Manager:
   - NEM Desktop - Application - Ethernet Security Manager….
2. In the “Mappings” tab open the “Edit” menu and click “Create”.
   - The “Create Mapping” dialog opens.
3. Select the first network element.

4. In the “Central Unit Port” table select the core unit (central unit) port that has been connected to the unencrypted SENC1 unit port.
5. In the “Encryption Unit Port” table select the SENC1 unit port that has been connected to the core unit MPLS-TP port.
6. Click OK.
7. Repeat the above steps for the second network element.

Result: The port mapping is defined.

→ Create a service profile. Proceed as follows:

Please note:
All profile parameters are configured as “Variable” so they can be modified later on when creating the MPLS tunnel using this profile.

1. In FOXMAN-UN start the Ethernet Networking Package:
   - NEM Desktop - Application - Ethernet Networking Package….
2. In the “Service Profile” tab open the “Edit” menu and click “Create Service Profile…”.
   - The “Create Service Profile” dialog opens.
3. Enter the profile parameters as required
4. Click Next.
5. Enter the class type and UNI port parameters as required
6. Click Next.
7. Enter the tunnel parameters as required
8. Click Next.
9. Enter the routing parameters as required
10. Click Finish.

Result: The service profile is created.

→ Add the network elements. Proceed as follows:

Please note:
The FOX61x network elements must have been added to the FOX61x agent before executing these steps.

1. In the “NE” tab open the “Edit” menu and click “Add NEs…”.
   - The “Add NEs to ENP-Nodes Domain” dialog opens.
2. Select the first NE and click “Add to ENP Domain”.
3. Select the second NE and click “Add to ENP Domain”.
4. Click Close.

Result: The FOX61x network elements are added to the ENP domain.

→ Create the link between the two network elements. Proceed as follows:

1. In the “Link” tab open the “Edit” menu and click “Create Link…”.
   - The “Create Link” dialog opens.
2. Enter the link parameters
   - Name = <any name>
   - A End NE = <first added NE>.
   - A End TP = <MPLS-TP port on the core unit>
   - Z End NE = <second added NE>.
   - Z End TP = <MPLS-TP port on the core unit>

3. Click OK.

Result: The link between the two FOX61x network elements is created.

→ Create the tunnel between the two network elements. Proceed as follows:

1. In the “Tunnel” tab of the Ethernet Networking Package open the “Edit” menu and click “Create Tunnel…”.
   - The “Create Tunnel” dialog opens.
2. Enter the tunnel parameters
   - Name = <any name>
   - Initiator = <first added NE>.
   - Terminator = <second added NE>.
   - Service Profile = <previously created service profile>
3. In the “Working LSP” tab click “Automatic Routing”.
4. In the “BFD” tab enter the BFD parameters as required
5. In the “Encryption” tab enter the Encryption parameters as required:
   - Profile = <select an encryption profile>.
   - Click “Create End-to-End Encryption”.
6. Click “Save”.
7. Click “Deploy”.

Result: The encrypted tunnel between the two FOX61x network elements is created and deployed.
On the SENC1 Crypto Engines the MPLS tunnel endpoints are created with the “TunnelId” parameter set to the “Required Segment Id” of the “Encryption” tab.

End of instruction

8.5.2.3 Check the Encryption Parameters of the MPLS Tunnel

Check the Encryption parameters

→ Check the encryption parameters. Proceed as follows:

1. In FOXMAN-UN start the Ethernet Security Manager:
   - NEM Desktop - Application - Ethernet Security Manager….
2. In the “Crypto Engines” tab check that all involved SENC1 Crypto Engines are synchronized and have the “Communication Status” set to “Ok”. The Crypto Engines connected to a core unit MPLS-TP port have the “Crypto Capable” parameter enabled.
3. In the “Crypto Termination Points” tab check that mapped core unit ports are listed and are synchronized.
4. In the “Crypto Configurations” tab check that the involved SENC1 Crypto Engines are listed with the correct incoming and outgoing LSP labels, and that they are mapped to the correct core unit MPLS-TP port.

Result: The encryption parameters are checked.

End of instruction

8.5.3 Remove an Encrypted MPLS-TP Tunnel from the FOX61x Network Elements

i **Please note:**
For a detailed description of how to remove encrypted MPLS tunnels from FOXMAN-UN please refer to the FOXMAN-UN documentation.

8.5.3.1 Prerequisites

The following prerequisites must be met:

- The DIRAC server is up and running.
- The target SENC1 Functional Units must be enrolled and deployed in the FOX61x network element, including the cabling between the front ports of the core unit and the SENC1 unit.
- The encrypted tunnel to be removed is deployed.
- FOXMAN-UN and the DIRAC server should be synchronized.

8.5.3.2 Remove the Encryption Parameters from a MPLS Tunnel

Remove the Encryption parameters

→ Remove the MPLS tunnel endpoint encryption parameters. Proceed as follows:

1. In FOXMAN-UN start the Ethernet Networking Package:
   - NEM Desktop - Application - Ethernet Networking Package….
2. Open the “Tunnel” tab:
   - Select the tunnel to be deleted
   - Open the “Edit” menu and click “Delete Tunnel”
   - Confirm the warning message with “Yes”
3. The FOXMAN-UN performs the following tasks:
   - FOXMAN-UN sends a tunnel deletion request to the DIRAC server.
   - The DIRAC server checks the synchronization between FOXMAN-UN and the DIRAC server database.
   - The DIRAC server checks the deletion feasibility.
   - The DIRAC server sends the tunnel deletion command to the targeted Crypto Engines.
   - The DIRAC server checks the result of the operation in the SENC1 Crypto Engines and, in case of success, deletes the tunnel from its database and updates the configuration identifier.
   - The DIRAC server sends back the response to the FOXMAN-UN.

Result: The tunnel is removed from the FOXMAN-UN and DIRAC server database, and the encrypted tunnel endpoints have been removed from the involved SENC1 Crypto Engines via the DIRAC server.

→ Check the encryption parameters. Proceed as follows:

1. In FOXMAN-UN start the Ethernet Security Manager:
   - NEM Desktop - Application - Ethernet Security Manager….
2. In the “Crypto Configurations” tab check that the involved MPLS tunnel endpoints have been removed from the SENC1 Crypto Engines.

Result: The encryption parameters are checked.

End of instruction

9 User Interface Reference

For a description of the ESM GUI refer to [1KHW002412] FOXMAN-UN ‘NEM GUI Help System’ User Manual, section “Ethernet Security Manager”.

9.1 DIRAC Server CLI

The DIRAC server CLI is running on the DIRAC server. Via the DIRAC server CLI interface an administrator can manage and operate the DIRAC server.

For a description of the DIRAC server please refer to section 4 DIRAC Functional Description (on page 13).

The DIRAC server CLI commands support the

- command history (up/down arrow buttons),
- command editing, and
- auto-completion (tab button).

Square brackets indicate optional parameters.

i

Please note:
Every command is supported as parameter of the “help” command, describing features and arguments, for example

```
→ help version
→ help -C version
```

The commands are grouped as follows:

- Built-in Commands,
- Crypto Commands,
- Functional Unit Commands,
- Layer 2 Commands,
- Management Commands,
- Master Key Commands,
- Software Management Commands.

9.1.1 Built-in Commands

CLI syntax for the built-in commands:

```
Syntax:   clear
Syntax:   exit
Syntax:   quit
Syntax:   help [[-C] string]
Syntax:   history [[--file] file]
Syntax:   version
Syntax:   script [--file] file
```

Table 6: DIRAC built-in commands

Operation Name	Parameter Name	Range	Description
`clear`			Clear the shell screen.
`exit`			Exit from the DIRAC server CLI. Terminate the current session.
`quit`			Exit from the DIRAC server CLI. Terminate the current session.

Table 6: DIRAC built-in commands (continued)

Operation Name	Parameter Name	Range	Description

`help`	`[-C]`
	`--command`
		`<command>`
		`<command>`
			Without parameter: List all available CLI commands with a short description.
			With the -C or --command option: shows a short description of the specific command (string), including all command options and parameters.

`help`	`<command>`		Show a short description of a specific command, including all command options and parameters.
`history`	`[--file]`	`<file>`	Display or save the history of previously entered commands. Without parameter the command displays the history on the screen. With the file option the history is saved to the specified file (path/filename). [Optional, default = <none>]
`script`	`--file`	`<file>`	Read and execute commands from a file. A file name (path/filename) must be provided.

9.1.2 Crypto Commands

CLI syntax for the crypto commands:

```
Syntax:  crypto-configuration --audit [[--endpoints] string]
Syntax:  crypto-configuration --list [[--ce_id] long] [[--segment_id]
         long] [[--label] long]
Syntax:  crypto-engine --forcepoll [--id] long
Syntax:  crypto-engine --list [[--fu_id] long] [[--fu_name] string] [[-
         -fu_ip] string]
Syntax:  crypto-engine --show [--id] long
Syntax:  crypto-segment --list
Syntax:  crypto-segment --show
```

Table 7: DIRAC crypto commands

Operation Name	Parameter Name	Range	Description
`crypto-configuration`	`--list`		Get a list of the crypto configurations. The list/ table output includes the following parameters: - Ce Id - Segment - Label In - Label Out - Vlan - Profile - Active Master Key - Activation Time - Fallback Master Key
	`--list --ce_id`	`<CE_ID>`	Get a list of the crypto configuration of a specific crypto engine ID, which is an integer of usually 12 digits.
	`--list --segment_id`	`<segID>`	Get a list of the crypto configuration of the crypto engine with a specific segment ID, which is an integer (e.g. 2101).
	`--list --label`	3000 … `1048575`	Get a list of the crypto configuration of the crypto engine with a specific label.

Table 7: DIRAC crypto commands (continued)

Operation Name	Parameter Name	Range	Description
`crypto-engine`	`--forcepoll --id`	`<CE_ID>`	Reload data from one crypto engine into DIRAC. The crypto engine ID is an integer of usually 12 digits.
	`--list`		Get a list of crypto engines. The list/table output includes the following parameters: - Ce Id (crypto engine ID) - Engine - dci (DIRAC configuration index) - sci (SENC1 CE configuration index) - Status
	`--list --fu_id`	`long`	Get a list of a crypto engine with functional unit ID “long”. The functional unit ID “long” is usually the card’s serial number complemented with the digit 1 or 2.
	`--list --fu_name`	`long`	Get a list of a crypto engine with functional unit name “long”. The functional unit name “long” is the human readable identifier of the functional unit.
	`--list --fu_ip`	`long`	Get a list of a crypto engine with functional unit IP address “long”. The functional unit IP address “long” is the IP address string with a length of min 3, max 50 digits/characters.
	`--show --id`	`long`	Show detailed information of one specific crypto engine. “long” is the ID of the crypto engine (mandatory).
`crypto-segment`	`--list`		Get a list of crypto segments. The list/table output includes the following parameters: - Segment - Status - Labels - Profile (configured encryption profile) - Active Master Key - Activated At (date & time)
	`--list --tunnel_id`	`long`	Get a list of crypto segments with Tunnel ID “long”.
	`--list --label`	`long`	Get a list of crypto segments with Label “long”.
	`--show --id`	`long`	Show information about one crypto segment with Segment ID “long”.

9.1.3 Functional Unit Commands

CLI syntax for the functional unit commands:

```
Syntax:  functional-unit --add [--id] string [[--name] string] [[--
         description] string] [[--ip] string] [[--pk-file] string]
Syntax:  functional-unit --audit [[--endpoints] string]
Syntax:  functional-unit --export [--id] string [[--file] string]
Syntax:  functional-unit --info [--id] string
Syntax:  functional-unit --list
Syntax:  functional-unit --modify [--id] string [[--name] string] [[--
         description] string] [[--pk-file] string] [[--ip] string]
Syntax:  functional-unit --ping [[--id] string]
Syntax:  functional-unit --remove [--id] string
```

```
Syntax:  functional-unit --show [[--id] string] [[--ip] string] [[--
         name] string]
```

Table 8: DIRAC functional unit commands

Operation Name	Parameter Name	Range	Description
`functional-unit`	`--add --id`	`string`	Add the functional unit with given ID to the system. id of the functional unit. (usually card's serial Number + 1 or 2) [Mandatory] [A Valid FU Id is a number between 11 and 17 digits, ending in 1 or 2.]
	`--name`	`string`	Human readable identifier of the functional unit [Optional, default = <none>] [size must be between 3 and 50]
	`--description`	`string`	Functional Unit's description [Optional, default = <none>] [size must be between 3 and 2147483647]
	`--ip`	`string`	Functional Unit ip address [Optional, default = <none>] [Provide a valid IPv4 Address]
	`--pk-file`	`string`	Path to the public key of the functional unit [Optional, default = <none>]
`functional-unit`	`--audit`		Audit functional unit issues.
	`--audit --endpoints`	`string`	comma-separated IDs or IPs of related functional units [Optional, default = <none>]
`functional-unit`	`--export --id`	`string`	Export a certificate to a file. id of the FU [Mandatory] [A Valid FU Id is a number between 11 and 17 digits, ending in 1 or 2.]
	`--export --id --file`	`string`	File to export the certificate to [Optional, default = <none>]
`functional-unit`	`--info --id`	`string`	Execute GetInfo Operation against one functional unit. id of the FU. (card SN + 1 or 2) [Mandatory] [A Valid FU Id is a number between 11 and 17 digits, ending in 1 or 2.]
`functional-unit`	`--list`		List the functional units configured in the system.

Table 8: DIRAC functional unit commands (continued)

Operation Name	Parameter Name	Range	Description
`functional-unit`	`--modify --id`	`string`	Modify the functional unit's basic configuration. id of the functional unit. (usually card SN + 1 or 2) [Mandatory] [A Valid FU Id is a number between 11 and 17 digits, ending in 1 or 2.]
	`--name`	`string`	Human readable identifier of the functional unit. [Optional, default = <none>] [size must be between 3 and 50]
	`--description`	`string`	Functional Unit's description. [Optional, default = <none>] [size must be between 3 and 2147483647]
	`--pk-file`	`string`	Path to the public key of the functional unit. [Optional, default = <none>]
	`--ip`	`string`	Functional Unit's ip address. [Optional, default = <none>] [Provide a valid IPv4 Address]
`functional-unit`	`--ping --id`	`string`	Ping the functional unit. id of the FU. (usually card SN + 1 or 2) [Optional, default = <none>] [A Valid FU Id is a number between 11 and 17 digits, ending in 1 or 2.]
`functional-unit`	`--remove --id`	`string`	Remove the specified functional unit. id of the FU. (usually card SN + 1 or 2) [Mandatory] [A Valid FU Id is a number between 11 and 17 digits, ending in 1 or 2.]
`functional-unit`	`--show`		Show functional unit detailed information
	`--show --id`		id of the FU. (usually card SN + 1 or 2) [Optional, default = 0] [A Valid FU Id is a number between 11 and 17 digits, ending in 1 or 2.]
	`--show --ip`		ip of the FU [Optional, default = <none>]
	`--show --name`		Name of the FU [Optional, default = <none>]

9.1.4 Layer 2 Commands

CLI syntax for the layer 2 commands:

```
Syntax:  layer2-encryption --audit
Syntax:  layer2-encryption --activate
Syntax:  layer2-encryption --deactivate
Syntax:  layer2-encryption --delete
Syntax:  layer2-encryption --pair
Syntax:  layer2-encryption --show
Syntax:  layer2-encryption --list
```

9.1.5 Management Commands

CLI syntax for the management commands:

```
Syntax:  date
Syntax:  dirac-restart
Syntax:  dirac-shutdown
```

```
Syntax:  mgmt-cert --renew
Syntax:  status
Syntax:  table-mode [[--mode] string]
Syntax:  version
```

Table 9: DIRAC management commands

Operation Name	Parameter Name	Range	Description
`date`			Show the DIRAC system date and time
`dirac-restart`			Restart the DIRAC server. All services composing the DIRAC server subsystems are restarted.
`dirac-shutdown`			Shut down the DIRAC server. All services composing the DIRAC server subsystems are stopped. To restart the DIRAC server use the reboot command.
`mgmt-cert`	`--renew`		Refresh certificates for the management channel.
`status`			Get the status of all DIRAC server and related components: - Process name, - Process ID, - Process state, - Process sub-state, - Running since (date&time), - Dirac server status, - QRNG source, - QRNG status.
`table-mode`			Get the current table mode and table style.
	`--mode`	`on` `off`	Turn table view mode on or off. [Optional, default = <none>]
`version`			Get the version of the DIRAC server and CLI. The command returns the - Dirac CLI version, - Dirac Server version.

9.1.6 Master Key Commands

CLI syntax for the master key commands:

```
Syntax:  master-key --generate
Syntax:  master-key --list [--segment_id] long
Syntax:  master-key --provider
Syntax:  master-key --renew [--segment_id] long
```

Table 10: DIRAC master key commands

Operation Name	Parameter Name	Range	Description
`master-key`	`--generate`		Provide one random master key
`master-key`	`--list --segment_id`	`long`	Get a list of master keys for the segment given in “long”.
`master-key`	`--provider`		Get information regarding Master Key Provider.
`master-key`	`--renew --segment_id`	`long`	Renew the master key for a specific crypto segment given in “long”.

9.1.7 Software Management Commands

CLI syntax for the software management commands:

```
Syntax:  blm --list
Syntax:  blm --authorize
Syntax:  blm --du
Syntax:  blm --activate
Syntax:  blm --rm
Syntax:  blm --apply
Syntax:  blm --upload
```

Table 11: DIRAC software management commands

Operation Name	Parameter Name	Range	Description
blm	--list		List available packages in FU
blm	--authorize		Authorize DIRAC to perform maintainer operations towards SENC1 units, without prompting for password.
blm	--du		Show disk usage FU information.
blm	--activate		Activate a package already copied to FU.
blm	--rm		Delete a package on FU.
blm	--apply		Transfer and try to activate a package in specified IP address.
blm	--upload		Copy a package to specified FU.

10 Annex

10.1 Associated Documents

[1KHW028777]	Release Note “FOX61x”
[1KHW002497]	FOX61x Operating Instruction “Precautions and safety”
[1KHW028522]	FOX61x User Manual “Management Communication”
[1KHW029081]	User Manual “DIRAC - DIRAC Server Installation”
[1KHW029028]	FOX61x User Manual “SENC1-4, SENC1F4, SENC1-8, SENC1F8”
[1KHW002412]	FOXMAN-UN ‘NEM GUI Help System’ User Manual
[1KHW029012]	FOXMAN-UN in Firewalled Environment, Application Note

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