



CN4020

Version 5.5.1, 2026-08-14

Table of Contents

1. Introduction	1
1.1. Introduction	1
1.1.1. About This Guide	2
1.1.2. Intended Audience	2
1.1.3. Compatibility	3
1.1.4. Conventions Used in This Guide	3
1.1.5. Related Documentation	3
1.1.6. Safety Notices	3
2. Product Overview & Theory of Operation	5
2.1. Product Overview	5
2.1.1. Architecture Overview	5
2.1.2. Operation Modes	6
2.1.3. Encryption Modes	6
2.1.4. Connection Modes	8
2.1.5. Cryptographic Modes	11
2.1.6. Key Management Overview	12
2.1.7. Performance Characteristics	13
2.1.8. Supported Protocols and Frame Formats	14
2.1.9. Security Certifications	14
2.1.10. Management Interfaces	14
2.1.11. Algorithm Support	15
3. Installation	16
3.1. Package Contents	16
3.2. Physical Installation	16
3.2.1. Placement	16
3.2.2. Rack Mounting (Optional)	16
3.2.3. Environmental Requirements	16
3.2.4. Encryptor Interfaces	17
3.3. Power On	17
4. Getting Started	18
4.1. Getting Started	18
4.1.1. Before You Begin	18
4.1.2. Power-Up and Boot Sequence	18
4.1.3. Connecting to the Management Interface	21
4.1.4. Commissioning	23
4.1.5. Verifying Initial Setup	27
4.1.6. Next Steps	27
5. Management & Administration	28
5.1. Management Overview	28
5.1.1. Management Interfaces	28

5.1.2. Access Methods	29
5.2. CM7 Setup	29
5.2.1. Launching and Logging In	29
5.2.2. CM7 Settings	30
5.2.3. Initial Configuration Settings	31
5.3. User Account Management	32
5.3.1. Roles and Privilege Levels	32
5.3.2. Default Password Behaviour	33
5.3.3. Creating and Managing User Accounts	34
5.3.4. Password Policy	35
5.3.5. Enhanced Password Mode	35
5.3.6. Administrator Access Controls	36
5.3.7. User Inactivity Lockout	37
5.3.8. Administrator Lockout	38
5.3.9. Console Management	39
5.4. SNMP Configuration	39
5.4.1. SNMPv3 Security	39
5.4.2. Enhanced Algorithm Support	40
5.4.3. SNMPv3Q (Quantum-Resistant SNMP)	40
5.4.4. SNMP Security Level	40
5.4.5. SNMP Trap Configuration	41
5.4.6. SNMPv1 Monitoring	41
5.4.7. SNMP over SSH	42
5.4.8. FIPS 140-3 Mode	42
5.5. Certificate Management	43
5.5.1. Certificate Authorities	43
5.5.2. Creating the PKCS#12 File	44
5.5.3. Certificate Hash Algorithms	46
5.5.4. Advanced CA Functions	47
5.5.5. Importing and Exporting CA Files	51
5.5.6. Installing Certificates	51
5.5.7. Managing Installed Certificates	53
5.5.8. x509 Extensions	54
5.5.9. Certificate Servers (OCSP and CRL)	55
5.5.10. Enhanced Certificate Security	56
5.6. KDK Management	58
5.6.1. KDK Creation	58
5.6.2. KDK Installation	58
5.7. Syslog Configuration	59
5.7.1. Syslog Server Setup	59
5.7.2. CM7 Syslog Service	59

5.7.3. Syslog over SSH	61
5.8. Remote Access	61
5.8.1. Remote SSH CLI Access	61
5.8.2. SSH Key Pair Creation	62
5.8.3. SSH Access of Remote Devices	62
5.9. Additional Management Services	63
5.9.1. NTP Configuration	63
5.9.2. TACACS+ Authentication	63
5.9.3. FTP/FTPS Server Configuration	64
5.9.4. RESTful JSON Interface	65
5.9.5. Third-Party Managers	66
5.9.6. CipherTrust Integration	66
6. Network Configuration	68
6.1. Network Configuration	68
6.1.1. Encryptor Connections	68
6.1.2. Management Network	68
6.1.3. Data Interfaces	70
6.1.4. Management Topologies	73
6.1.5. Network Addressing (CM7)	78
7. Encryption Configuration	80
7.1. Encryption Configuration	80
7.1.1. Selecting an Encryption Mode	80
7.1.2. Connection Mode Selection	80
7.2. Key Management	82
7.2.1. Layer 2 Modes	82
7.2.2. Transport Independent Mode	84
7.3. Cryptographic Mode Configuration	85
7.3.1. Selecting a Cryptographic Mode	85
7.3.2. CTR/GCM Shim Configuration	85
7.4. Replay Protection	86
7.4.1. Replay Protection by Connection Mode	87
7.4.2. Replay Protection Statistics	87
7.5. MTU Handling and Encryption Overhead	88
7.5.1. Encryption Overhead Calculation	88
7.5.2. MTU Management in Layer 2 Modes	89
7.5.3. Path MTU Discovery in TIM Mode	89
7.6. Policy Configuration (CM7)	91
7.6.1. Policy Extensions	92
7.6.2. Protocol Configuration (CM7)	93
7.6.3. Reserved Multicast	93
7.6.4. Ethertype Configuration	93

7.6.5. Control Plane and Management Ethertypes	94
7.7. Connection Tables (CM7)	95
7.7.1. Common Parameters (All Modes)	95
7.7.2. Line Mode Connection Fields	96
7.7.3. VLAN Mode Connection Fields	96
7.7.4. MAC Mode Connection Fields	96
7.7.5. TIM Mode Connection Fields	96
7.7.6. Filtering Connections	96
7.8. Line Mode	97
7.8.1. Line Mode Policy	97
7.8.2. Configuring Line Mode	97
7.8.3. Line Mode Specific Settings	98
7.8.4. TRANSEC Mode Overview	99
7.8.5. Shared Settings and Key Management	102
7.9. VLAN Mode	102
7.9.1. VLAN Mode Policy	102
7.9.2. Configuring VLAN Mode	103
7.9.3. VLAN Mode Specific Settings	104
7.10. MAC Mode	106
7.10.1. MAC Mode Policy	106
7.10.2. Configuring MAC Mode	107
7.10.3. MAC Mode Specific Settings	109
7.11. Transport Independent Mode	111
7.11.1. TIM Mode Policy	111
7.11.2. Configuring TIM Mode	112
7.11.3. TIM Mode Specific Settings	114
8. High Availability	123
8.1. High Availability	123
8.1.1. Overview	123
8.1.2. Spanning Tree Protocol (STP) Monitoring	123
8.1.3. Tunnel Keep Alive Monitoring (TKAM)	125
8.1.4. MAC Migration	126
8.1.5. Link Loss Detection	126
8.1.6. Operational Modes During Failure	129
9. Monitoring & Statistics	131
9.1. Monitoring & Statistics	131
9.1.1. Dashboard and System Status	131
9.1.2. Interface Status	133
9.1.3. Statistics	135
9.1.4. Diagnostics	142
9.1.5. Alarms	143

9.1.6. Event and Audit Logs	146
9.1.7. SNMP Trap Monitoring	147
9.1.8. Syslog Integration	147
9.1.9. REST API Monitoring	147
10. Maintenance	149
10.1. Maintenance	149
10.1.1. Firmware Upgrades	149
10.1.2. Configuration Export and Import	155
10.1.3. Rate Limiting	155
10.1.4. Entropy Management	157
10.1.5. FIPS Mode	157
10.1.6. Emergency Erase and Factory Reset	158
10.1.7. USB Port Management	159
10.1.8. Powering Down	160
11. Troubleshooting	161
11.1. Troubleshooting	161
11.1.1. General Troubleshooting Approach	161
11.2. Management Network troubleshooting	161
11.2.1. Management Network Port Reference	161
11.3. Datapath Troubleshooting	162
11.3.1. ePing	162
11.3.2. Ethertype Diagnostics	163
11.3.3. Traffic Analysis	163
11.4. Physical Troubleshooting	164
11.4.1. LED Indicators	164
11.5. Common Issues	165
11.5.1. Connection Establishment Issues	165
11.5.2. Certificate Issues	168
11.5.3. Multipoint Key Issues (VLAN and MAC Modes)	169
11.5.4. VLAN Connectivity Issues	170
11.5.5. TIM Mode Troubleshooting	170
11.5.6. Cable Problems	170
11.5.7. Secure Halt	170
11.6. Contacting Senetas Support	171
11.6.1. Senetas Customer Support Portal	171
11.6.2. Creating a Support Case	172
11.6.3. Contact Information	172
Appendix A: Technical Specifications	173
Hardware Specifications	173
Network Specifications	173
Appendix B: Compliance & Certifications	174

Appendix A: Compliance and Certifications	174
Security Certifications	174
Regulatory Approvals	174
Supported Cryptographic Algorithms	175
Documentation Notice	178
Appendix C: Crypto-Agility	179
Appendix B: Crypto-Agility	179
Overview	179
S-box Customisation	180
Bring Your Own Entropy (BYOE)	182
Bring Your Own Curves (BYOC)	183
Appendix D: CLI Reference	186
Overview	186
Accessing the CLI	186
CLI Conventions	186
Command Modes	186
Syntax Notation	186
Command History	187
Hexadecimal Values	187
Command Quick Reference	187
Command Reference	190
activate	190
alarm	191
audit	191
autodisco	192
autopop	193
banner	194
certificate	195
community	196
con	196
controlplaneif	197
crl	197
crypto	198
date	199
entropy	199
eping	200
eqkd	201
erase	202
ethertypes	202
event	204
fips	205

framegap	205
ftpcfg	206
global	206
help	207
helpall	208
history	208
hostname	209
inband_vlan	209
initcfg	210
inventory	211
ip	212
iprules	213
kdf	214
kem	215
keyprovider	215
kscfg	216
kstier	217
line	218
linkspeed	219
locmacs	220
logout	221
mpls	221
netmacs	222
ntpcfg	223
ocsp	224
overview	225
password	225
policy	227
profile	229
prompt	229
protocol	230
reboot	230
rest	231
sbox	231
sfp	232
shim	233
snap	234
snmpcfg	234
snmptraps	235
sshaux	236
sshcli	237

stats	238
syslog	239
tacacs	240
timezone	240
transec	241
tunnels	242
upgrade	245
usb	245
users	246
version	247
vlan	247

Chapter 1. Introduction

Company and Partner Support Contact Information

Support Contacts

If you encounter a problem while installing, registering or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or Senetas Customer Support. Senetas Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Senetas and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Office	Phone
Australia	1-800-270-923
United Kingdom	0-808-189-1247
USA and Canada	1-800-470-3520
Customer Support Portal	https://support.senetas.com
Email	support@senetas.com

Senetas Corporation Limited.

312 Kings Way
South Melbourne, Victoria, 3205, Australia.
(T) +61 (03) 9868 4555 (F) +61 (03) 9821 4899

Senetas Europe Ltd.

Worting House, Church Lane
Basingstoke, Hants, RG23 8PX, UK.
(T) +44 (0) 1256 345599 (F) +44 (0) 1256 811876

© 2026 Senetas Corporation Limited
Web site: www.senetas.com

1.1. Introduction

Welcome to the CN4020 User Guide.

The CN4020 is a high-performance network encryptor designed to secure data in transit across wide area networks. It provides certified encryption for sensitive traffic while maintaining near line-rate throughput and low latency.

Senetas CypherNET encryptors support both Layer 2 (Ethernet) and Layer 2–4 (Transport

Independent Mode) encryption, providing flexible protection for enterprise, government, and service provider networks.

1.1.1. About This Guide

This guide covers the installation, configuration, operation, and maintenance of the CN4020.

It is organised into the following chapters:

1. **Introduction** — this chapter
2. **Product Overview & Theory of Operation** — architecture, encryption modes, and key concepts (see [Product Overview & Theory of Operation](#))
3. **Installation** — physical installation and initial cabling (see [Installation](#))
4. **Getting Started** — first-time setup, commissioning, and activation (see [Getting Started](#))
5. **Network Configuration** — management and data interface setup (see [Network Configuration](#))
6. **Management & Administration** — user accounts, certificates, SNMP, and syslog (see [Management & Administration](#))
7. **Encryption Configuration** — TIM and Ethernet mode encryption setup (see [Encryption Configuration](#))
8. **High Availability** — redundancy and failover configuration (see [High Availability](#))
9. **Monitoring & Statistics** — status dashboards, event logs, and performance counters (see [Monitoring & Statistics](#))
10. **Maintenance** — firmware upgrades, backup and restore, licensing (see [Maintenance](#))
11. **Troubleshooting** — diagnostics and common issue resolution (see [Troubleshooting](#))



This guide describes features common to all CypherNET encryptor models. Model-specific details — including physical installation, port layouts, and hardware specifications — are provided in the model-specific installation section and specifications appendix for each product.

1.1.2. Intended Audience

This guide is intended for network administrators and security operators responsible for deploying and managing CN4020 encryptors.

It is assumed that the reader is familiar with:

- The topology of the network in which the encryptor is to be deployed
- Basic principles of computer networking, protocols, and interfaces
- The administration and operation of a computer network

1.1.3. Compatibility

This guide applies to the following firmware and management software versions:

Component	Version
CN4020 firmware	5.5.1
CM7 Management System	7.11

1.1.4. Conventions Used in This Guide

The following typographic conventions are used throughout this guide:

Convention	Meaning
<code>monospace</code>	Commands, CLI syntax, file names, and configuration values
bold	UI elements (buttons, menu items, screen names) and important terms
<i>italic</i>	New terms and emphasis

Admonitions

Three types of highlighted paragraphs are used to draw attention to important information:



Provides additional information, reminders, or tips that may assist with a task.



Highlights that extra care should be taken when performing a task, or that an action may have security implications.



Indicates that performing an action incorrectly may cause operational errors, data loss, or system failure.

1.1.5. Related Documentation

In addition to this user guide, the following documentation may be available for your product:

- **CM7 Fleet Management Guide** — CM7 installation, architecture, fleet monitoring, and policy management
- [CLI Reference](#) — complete command reference for all CLI commands (Appendix D)
- **Release Notes** — new features, known issues, and upgrade instructions for each firmware release

1.1.6. Safety Notices

Observe all safety markings and instructions provided on the CN4020 enclosure and in [Chapter 3, Installation](#) of this guide. Follow your organisation's safety policies when installing and servicing

equipment.

Chapter 2. Product Overview & Theory of Operation

2.1. Product Overview

The CN4020 is a hardware-based network encryptor that secures data in transit using the Advanced Encryption Standard (AES). Operating at Layers 2-4 of the OSI model, the encryptor provides tunnel-free point-to-point and multipoint wire-speed encryption with low latency and minimal packet expansion.

Tunnel-free encryption is commonly described as "bump in the wire" technology: the encryptor sits inline between the local (protected) network and the network (unprotected) side, encrypting network packets transparently at the specified layer:

- Layer 2: Ethernet frames
- Layer 3: IP packets
- Layer 4: Transport protocols (TCP/UDP)

The packet header is left unencrypted to allow routing/switching across the network without modifying IP addressing, routing, or upper-layer protocols. This allows the full available bandwidth to be used for encrypted traffic.

2.1.1. Architecture Overview

The CN4020 is deployed inline on the network between two or more sites. Traffic entering the Local port from the protected network is encrypted and forwarded out the Network port toward the unprotected network. Traffic arriving on the Network port is decrypted and forwarded to the Local port.

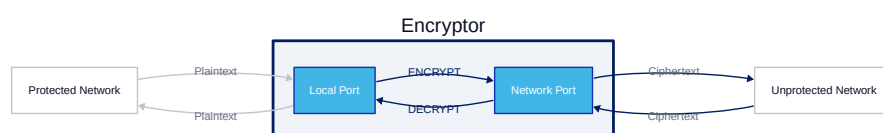


Figure 1. Encryption data flow

Each encryptor is paired with one or more remote encryptors to form encrypted connections. The encryptor is transparent to the network infrastructure — switches, routers, and other devices operate as if the encryptor were not present.

Network traffic can be selectively encrypted, bypassed or discarded by configuring appropriate security policies.

The CN4020 provides three physical interface categories:

Local and Network ports

Carry data plane traffic (encrypted and unencrypted network traffic). The encryptor processes packets at line rate between these ports.

Management port

An RJ45 Ethernet port used for SNMPv3-based management via CM7 or third-party managers and for SSH access to the CLI.

Serial console port

An RJ45 RS-232 connector for local CLI access.

Additional interfaces include USB connectors for firmware upgrades, LED indicators, and a serial console port for local CLI access.

2.1.2. Operation Modes

The CN4020 has three categories of operational settings that determine how it processes traffic:

Operation Mode

The global policy that controls overall traffic handling. The encryptor can be set to one of three states:

- **Discard** — prevents the flow of all traffic (factory default)
- **Bypass** — transmits all frames unencrypted (used during initial setup or troubleshooting)
- **Secure** (Encrypt All) — encrypts traffic according to the configured policy

The Secure mode cannot be selected until a valid certificate (Ethernet modes) or Key Derivation Key (Transport Independent Mode) has been loaded.

Cryptographic Mode

Specifies which AES submode is used for encryption: CFB, CTR, or GCM. See [Cryptographic Modes](#).

Connection Mode

Specifies how the encryptor interprets and applies encryption policy:

- **Ethernet modes** - Point-to-Point (Line), TRANSEC, MAC multipoint, VLAN multipoint
- **Transport Independent mode** - TIM

See [Connection Modes](#).

2.1.3. Encryption Modes

The CN4020 supports two fundamental encryption modes that determine the layer at which encryption is applied.

Ethernet Mode (Layer 2)

In Ethernet mode, the encryptor provides Layer 2 security services by encrypting the payload of Ethernet frames travelling across the network. The encryptor accepts frames on its ingress port, classifies them according to the frame header, and processes each frame according to the configured policy.

Ethernet mode requires an end-end Ethernet network between encryptors, for example:

- Point-point dark fibre
- Metro or Carrier Ethernet service
- Virtual Private LAN Service (VPLS = Layer 2 MPLS)

The available policy actions are:

Encrypt

The payload of the frame is encrypted according to the active connection policy.

Discard

The frame is dropped; no portion is transmitted.

Bypass

The frame is transmitted without alteration.

When a frame is encrypted the encryptor recalculates and appends a new Frame Check Sequence (FCS).

Ethernet mode supports all four Layer 2 connection modes: Point-to-Point (Line), TRANSEC, MAC multipoint, and VLAN multipoint.

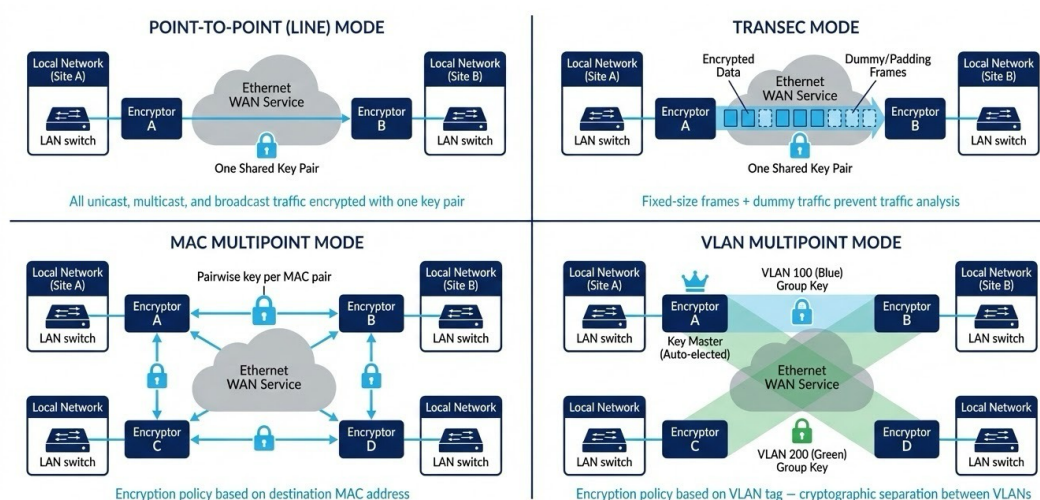


Figure 2. Ethernet connection modes

For detailed encryption configuration, see [Chapter 6: Encryption Configuration](#).

Transport Independent Mode (TIM)

Transport Independent Mode (TIM) allows traffic encryption at layers 2, 3, and 4 of the OSI model. TIM decouples encryption from the underlying transport, enabling encryption across a wide variety of transport networks for example:

- Ethernet network
- Public Internet

- IP routed network
- MPLS
- Satellite links

TIM supports encryption at the following layers:

- **Layer 2** — Ethernet payload encryption
- **Layer 3** — IPv4 payload encryption
- **Layer 4 (UDP)** — UDP payload encryption with NAT pass-through support
- **Layer 4 (TCP)** — TCP payload encryption
- **Layer 4** - Other protocols

Layer 4 (IP + Port) encryption supports NAT pass-through, NetFlow/JFlow, and policy-based routing.

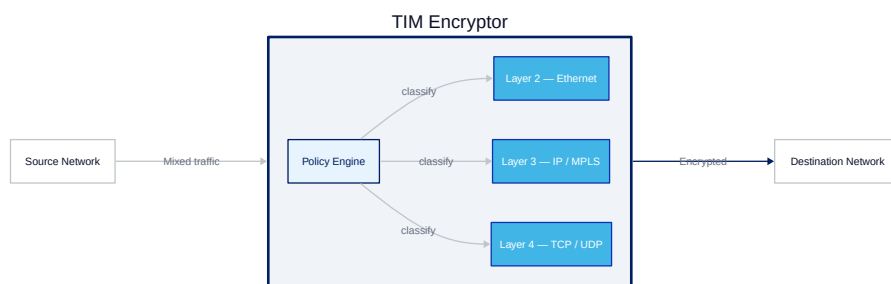


Figure 3. Transport Independent Mode — multi-layer encryption

2.1.4. Connection Modes

The connection mode determines how the encryptor interprets encryption policy and establishes connections with peer encryptors.

Point-to-Point (Line) Mode

Point-to-Point mode provides a dedicated encrypted link between exactly two encryptors over an Ethernet network. A single key pair encrypts all unicast, multicast and broadcast traffic traversing the connection.

Point-to-Point mode is appropriate where:

- Only two sites are connected over an Ethernet or dark fibre link
- A simple, high-performance Layer 2 encryption solution is required



Point-to-Point mode uses a single key pair for all traffic. Cryptographic separation between traffic types is not provided.

TRANSEC Mode

TRANSEC (Traffic Security) mode is a sub-mode of Line mode. It extends Point-to-Point mode by padding frames to a fixed size and inserting dummy frames during idle periods. This disguises traffic patterns and prevents traffic analysis.

TRANSEC mode supports only point-to-point topologies and uses pairwise keys.

MAC Mode

MAC (Media Access Control) mode enables the encryptor to operate within a multipoint or meshed Layer 2 network topology. In this mode, encryption policy is enforced based on the destination MAC address of the Ethernet frame, allowing the device to maintain simultaneous, secure connections with multiple remote encryptors. This configuration provides cryptographic separation of traffic between distinct endpoints, with security associations established either through manual configuration or the encryptor's automatic discovery mechanism.

MAC mode supports:

- Unicast encryption using pairwise keys (one key pair per connection)
- Multicast/broadcast encryption using group key encryption
- Automatic peer discovery based on observed traffic
- Hub-and-spoke and full mesh topologies

The Senetas group key management scheme is decentralised — a group key master is automatically elected among the encryptors within the mesh. The scheme is designed to survive network outages and topology changes without relying on an external key server.

VLAN Multipoint Mode

VLAN mode is a multipoint Ethernet encryption configuration designed to secure traffic between multiple encryptors across switched Ethernet WAN services, such as Metro Ethernet, E-LAN, or VPLS. In this mode, encryption policy is enforced based on the VLAN ID (or stacked QinQ tags) within the Ethernet frame, allowing individual VLANs to be selectively encrypted, bypassed, or discarded.

Unlike unicast-only modes, VLAN mode utilizes a dynamic group key management scheme to secure unicast, multicast, and broadcast traffic. This architecture automatically elects a group key master to distribute shared encryption keys to participating 'peer' encryptors, providing a scalable and fault-tolerant solution that facilitates automatic discovery of new VLAN connections without manual intervention.

VLAN multipoint mode applies encryption policy based on 802.1Q VLAN tags. Each VLAN ID can be assigned an independent encryption policy, providing cryptographic separation between VLANs.

VLAN mode supports:

- Cryptographic separation by VLAN
- Quality of Service (QoS) preservation

- Increased scalability compared to MAC mode
- Frame re-ordering (frames can be delivered in any order)
- Group key encryption using the Senetas group key scheme

Senetas recommends VLAN mode as the default multipoint deployment for Ethernet networks because it allows frame re-ordering and provides per-VLAN cryptographic separation.



VLAN mode can also be used across networks that are not using 802.1Q VLAN tagging. In this case all traffic will be encrypted using a single group key for the native VLAN.

Connection Mode Comparison

The following table summarises key attributes across connection modes.

Table 1. Connection mode attributes

Attribute	Line (Pt-Pt) CFB	Line (Pt-Pt) CTR	MAC CFB	MAC CTR	VLAN CTR
Unicast	y	y	y	y	y
Multicast	y	y	n	n	y
Broadcast	y	y	n	n	y
Point-to-Point topology	y	y	y	y	y
Mesh topology	n	n	y	y	y
Hub/Spoke topology	n	n	y	y	y
Policy basis	ethertype	ethertype	ethertype + DA MAC	ethertype + DA MAC	ethertype + VLAN tag
Cryptographic separation	n/a	n/a	by connection	by connection	by VLAN
Key system	pairwise	pairwise	pairwise	pairwise	groupwise
QoS support	n/a	n/a	n	n	y
Per-frame overhead (octets)	0	8	0	8	8

Key: **y** = supported, **n** = not supported, **n/a** = not applicable.

Table 2. TRANSEC mode attributes

Attribute	TRANSEC (Line, CTR)
Topology	Point-to-Point only

Attribute	TRANSEC (Line, CTR)
Address support	Unicast, Multicast, Broadcast
Key system	Pairwise
QoS support	n/a
Per-frame overhead (octets)	16



The connection modes available depend on the encryptor model and firmware version. Refer to the model-specific documentation for details.

2.1.5. Cryptographic Modes

The cryptographic mode defines which submode of the AES algorithm is used for encryption. All encryptors that communicate with each other must use the same cryptographic mode.

AES-CFB (Cipher Feedback)

In CFB mode, the encryptor operates in a self-synchronising, streaming mode. Encrypted frames are the same size as plaintext frames — there is no packet expansion.

If an encrypted frame is lost in transit, the immediately following frame cannot be decrypted, but the next frame after that will decrypt correctly. This self-correcting mechanism has an error extension of one frame.

CFB mode cannot be used at speeds of 10 Gbps or higher, or for multicast traffic in multipoint (meshed) networks.

AES-CTR (Counter)

In CTR mode, the algorithm is not self-synchronising. Re-synchronisation is achieved by periodically inserting a small shim header (security tag) into encrypted frames containing the current counter value.

If frames are lost, subsequent frames cannot be decrypted until the encryptors re-synchronise on the next shim. The shim insertion rate is configurable in Line and MAC unicast modes (default: every 32 frames; range: 0–32,767). In VLAN and TIM modes, a shim is inserted on every frame.



TIM mode, shim insertion positions vary by encryption layer (Layer 2, Layer 3, Layer 4 UDP, Layer 4 TCP).

The per-frame overhead for CTR mode is 8 octets in Layer 2 Ethernet encryption.

AES-GCM (Galois/Counter)

GCM mode is similar to CTR mode (not self-synchronising; shimming is used) with the added benefits of message authentication.

GCM provides both confidentiality and data integrity verification by adding an Integrity Check Value (ICV) to the end of the frame.

The per-frame overhead for GCM mode depends on the operating mode:

- **Layer 2 Ethernet Encryption (VLAN/Line/MAC):** The overhead is **24 octets** (8-byte + 16-byte ICV).
- **Transport Independent Mode (TIM):** The overhead varies based on the configured encryption layer and key synchronization method. See [TIM frame overhead \(octets\)](#)



AES-GCM is the preferred cryptographic mode for most deployments due to its message authentication capability and efficient processing.

Table 3. Cryptographic mode comparison

Characteristic	CFB	CTR	GCM
Self-synchronising	Yes	No	No
Packet expansion	None	8 octets	24 octets
Message authentication	No	No	Yes
10 Gbps+ support	No	Yes	Yes
Multicast in meshed networks	No	Yes	Yes

For details on default shim rates and configuration ranges by connection mode, see [Cryptographic Mode Configuration](#) in Chapter 6.

When configured in TIM mode, the per-frame overhead depends on the key provider type, the encryption layer, and the cryptographic mode:

Table 4. TIM frame overhead (octets)

	L2	L3	L4 UDP	L4 TCP	UDP tunneling
Time Sync	8	8	8	12	16
CTR Sync	10	10	10	12	18

The overhead is increased by +16 bytes if GCM is enabled

2.1.6. Key Management Overview

The CN4020 uses data encryption keys (DEKs) to encrypt data plane traffic.

In Ethernet modes DEKs are exchanged between peer encryptors during session establishment.

Pairwise keys

Used for unicast traffic in Point-to-Point and MAC modes. Each connection uses a unique key pair

with a separate key for each direction.

Group keys

Used for multicast/broadcast traffic in Multipoint MAC mode and for all traffic in VLAN mode. The Senetas group key management scheme distributes group keys across the mesh without relying on an external key server.

A group key master is automatically elected among the visible encryptors. The scheme supports automatic discovery of multicast groups, secure key distribution, fault tolerance to network outages, and automatic detection of dead peers.

In Transport Independent Mode (TIM), DEK generation is handled by the configured *key provider*, which decouples key management from the transport network.

For encryption configuration and key management procedures, see [Chapter 6: Encryption Configuration](#).

2.1.7. Performance Characteristics

The CN4020 uses a cut-through encryption architecture by default. Encryption and retransmission begin after only partial receipt of the frame, resulting in consistently low latency.



Some configurations require the move to a store-and-forward architecture, increasing latency.

Latency

Latency depends on the network link speed and encryptor model.

The CN4020 operates with a latency of < 10 μ s at 1 Gbps. < 50 μ s at 100 Mbps; < 650 μ s at 10 Mbps.

Jitter

Minimal variation in latency due to efficient hardware-based processing.

Packet expansion

See [Cryptographic Modes](#) for more details.

Control plane overhead

In Ethernet modes the encryptor generates a small amount of inter-peer traffic for key updates and management, using the Senetas registered ethertype (0xFC0F).

In Transport Independent Mode (TIM) there is no control plane between peers.

Frame size

The encryptor supports Ethernet frames in the range 64–10,000 octets. The upper limit is reduced by the size of any inserted shims (for example, in VLAN mode with GCM, the maximum frame size is 9,976 octets).

2.1.8. Supported Protocols and Frame Formats

The CN4020 supports the following Ethernet frame formats:

Ethernet II (DIX)

The standard Ethernet frame format used by TCP/IP, IPX, and most higher-layer protocols. The encryptor encrypts the frame payload while preserving the destination MAC address, source MAC address, and ethertype fields.

IEEE 802.3 SAP

Frames with an 802.2 LLC header, most commonly used for control plane traffic.

IEEE 802.3 SAP SNAP

Extended LLC frames with an OUI and Protocol ID field, supporting vendor-specific protocol sets.

VLAN tagged (802.1Q)

The encryptor is transparent to single VLAN tags with ethertype **0x8100**. The VLAN tag (User Priority, CFI, VLAN ID) is preserved in the clear.

Stacked VLAN (Q-in-Q)

Double-tagged frames are supported when the outer tag uses ethertype **0x8100**. The inner tag (C-VLAN/C-TAG) and outer tag (S-VLAN/S-TAG) are both preserved.

MPLS

The encryptor is transparent to MPLS label stacks with a maximum depth of 5 labels.



Do not confuse VLAN tags (frame header fields that identify traffic) with VLAN encryption mode (an operational mode that uses VLAN tag values to determine encryption policy).

2.1.9. Security Certifications

The CN4020 has been tested and accredited by international security agencies.

FIPS 140 Level 3

Encryptors operate in FIPS mode by default. When FIPS mode is active, startup self-tests are performed and results are logged to the event log. FIPS mode enforces Diffie-Hellman key exchange for authentication and privacy on the management port.

Common Criteria

CC accreditation has been completed.

For the complete list of certifications and compliance standards, see [Appendix B: Compliance](#).

2.1.10. Management Interfaces

The CN4020 supports multiple management interfaces:

CM7 Network Manager

A graphical management application based on SNMPv3. CM7 provides comprehensive configuration, monitoring, and certificate management via the RJ45 Ethernet management port.

Command Line Interface (CLI)

A text-based interface accessible via the serial console port (local) or SSH (remote).

SNMP (Third-Party Managers)

SNMPv3-based integration with third-party network management systems. Senetas provides the required MIBs.

RESTful JSON Interface

An HTTP(S) interface for remote monitoring and issue detection, leveraging the existing SNMP MIB.

For full management configuration details, see [Chapter 5: Management](#).

2.1.11. Algorithm Support

The CN4020 supports a wide range of cryptographic algorithms.

For a comprehensive listing, see the [NIST CMVP public database for Senetas encryptors](#).

Chapter 3. Installation

This chapter describes how to install the CN4020.

3.1. Package Contents

Your CN4020 ships with the following items:

- CN4020 encryptor unit
- 12V DC plug-pack with universal socket adaptors
- Serial console cable
- RJ45 Ethernet cable
- A rack mounting bracket with screws

3.2. Physical Installation

3.2.1. Placement

The CN4020 is a compact desktop unit. Place it on a flat, stable surface with adequate ventilation.

1. Remove the unit from its packaging.
2. Place the unit on a desk or shelf with at least 5 cm clearance on all sides for airflow.
3. Connect the power cable.

3.2.2. Rack Mounting (Optional)

The CN4020 can optionally be rack-mounted using the provided rack-mount kit.

1. Attach the rack-mount brackets to the unit.
2. Slide the unit into a standard 19-inch rack and secure with screws.

3.2.3. Environmental Requirements

Table 5. Environmental Specifications

Parameter	Value
Operating Temperature	0°C to 40°C
Storage Temperature	-20°C to 70°C
Humidity	10% to 90% (non-condensing)
Altitude	Up to 3,000m

3.2.4. Encryptor Interfaces

The CN4020 has 2 SFP data ports and 1 RJ45 management port. Connect the network ports using appropriate SFP transceivers and cables for your deployment.

Datapath Ports

Table 6. Connector LEDs — Local or network ports

Port type	LNK (Left)	SPD (Right)	State
SFP	OFF	OFF	No Link
	AMBER (Solid)	AMBER (Solid)	Port Stopped
	RED (Flash)	RED (Flash)	SFP Fault
	OFF	GREEN (Flash)	LLF Down
	OFF	RED (Solid)	Loss of Signal
	RED (Solid)	RED (Flash)	Loss of Signal & Auto neg. failure
	GREEN (Active)	AMBER (Solid)	Link 100M
	GREEN (Active)	GREEN (Solid)	Link 1000M

Management ports

See [Network Config](#) for more details.

3.3. Power On

The CN4020 encryptor requires a 9-12V DC external plug-pack supplying at least 10 watts of power. A plug pack with universal socket adaptors is supplied with each encryptor. For maximum reliability it is recommended that the encryptor be protected with an uninterruptible power supply (UPS).

1. Connect the plug-pack to the CN4020 and to a mains power outlet.
2. The Power LED on the front panel illuminates green when the unit is powered on.
3. Wait approximately 2 minutes and 30 seconds for the unit to complete its boot sequence.
4. The Status LED turns solid green when the unit is ready.



The supply is designed to withstand normal power fluctuations. However if the mains supply is outside the specified range for the encryptor this may lead to faulty operation and/or damage being sustained.

Chapter 4. Getting Started

4.1. Getting Started

This chapter describes how to perform the initial setup of the CN4020 after physical installation. It covers power-up and self-test, connecting to the management interface, commissioning (IP address, name, date/time), activation, and initial verification.

For product capabilities and encryption mode concepts, see [Chapter 2: Product Overview](#).

4.1.1. Before You Begin

Before starting the commissioning process, ensure the following prerequisites are met:

- The CN4020 is physically installed (see [Installation](#))
- An Ethernet cable for connecting to the management port, and/or a serial cable for CLI access
- A computer with CM7 installed and/or a terminal emulator program.
- The default credentials:
 - **User name:** `admin`
 - **Password:** `$Password1`



The default credentials are well-known and are forceably changed during the activation process. The default credentials are reset whenever the unit is erased or the tamper mechanism is triggered.

4.1.2. Power-Up and Boot Sequence

Following physical installation, connect power to the CN4020 to verify that it operates as expected. Encryptors are shipped in factory default state and require configuration before deployment.

Initial Power-Up

Connect the power cable to the CN4020 and switch on the power supply. The unit enters its boot sequence automatically.

During the boot sequence, the CN4020 performs a series of hardware and software diagnostic tests required for FIPS 140-3 compliance. The results of these tests are recorded in the system event log.

Self-Test Sequence

The CN4020 performs the following self-tests during boot:

Software and firmware integrity tests

A SHA-256 hash is computed for each software and firmware component and compared against a build-time reference value. The SHA-256 integrity test is the first test in the power-up sequence.

In addition to running at start-up, integrity tests run automatically every 24 hours. A start-up sequence can be triggered by a reboot, erase, tamper event, or power cycle.

Data-path tests

The encryptor sends test frames through the bypass and encrypt egress data paths to verify correct operation.

Data-path tests run:

- On policy configuration changes (for example, crypto-mode or IP rule changes)
- Every 24 hours
- At start-up (triggered by reboot, erase, tamper, or power cycle)

Table 7. Software and firmware integrity test results

Result	Action
Success	Normal operation continues. Event log entries are generated for all tests if conducted at start-up. For 24-hour checks, only the software integrity test result is logged.
Fail	The encryptor enters a <i>Secure Halt</i> state (see Secure Halt).

Table 8. Data-path test results

Result	Action
Success	Normal operation continues. Event log entries are generated only if the test was conducted at start-up.
Fail	The following actions occur: • An alarm is raised • A log entry is generated • The encryptor global mode is set to <i>Discard</i> The operator can change the global mode back to <i>Secure</i> without acknowledging the alarm. This triggers another data-path test.

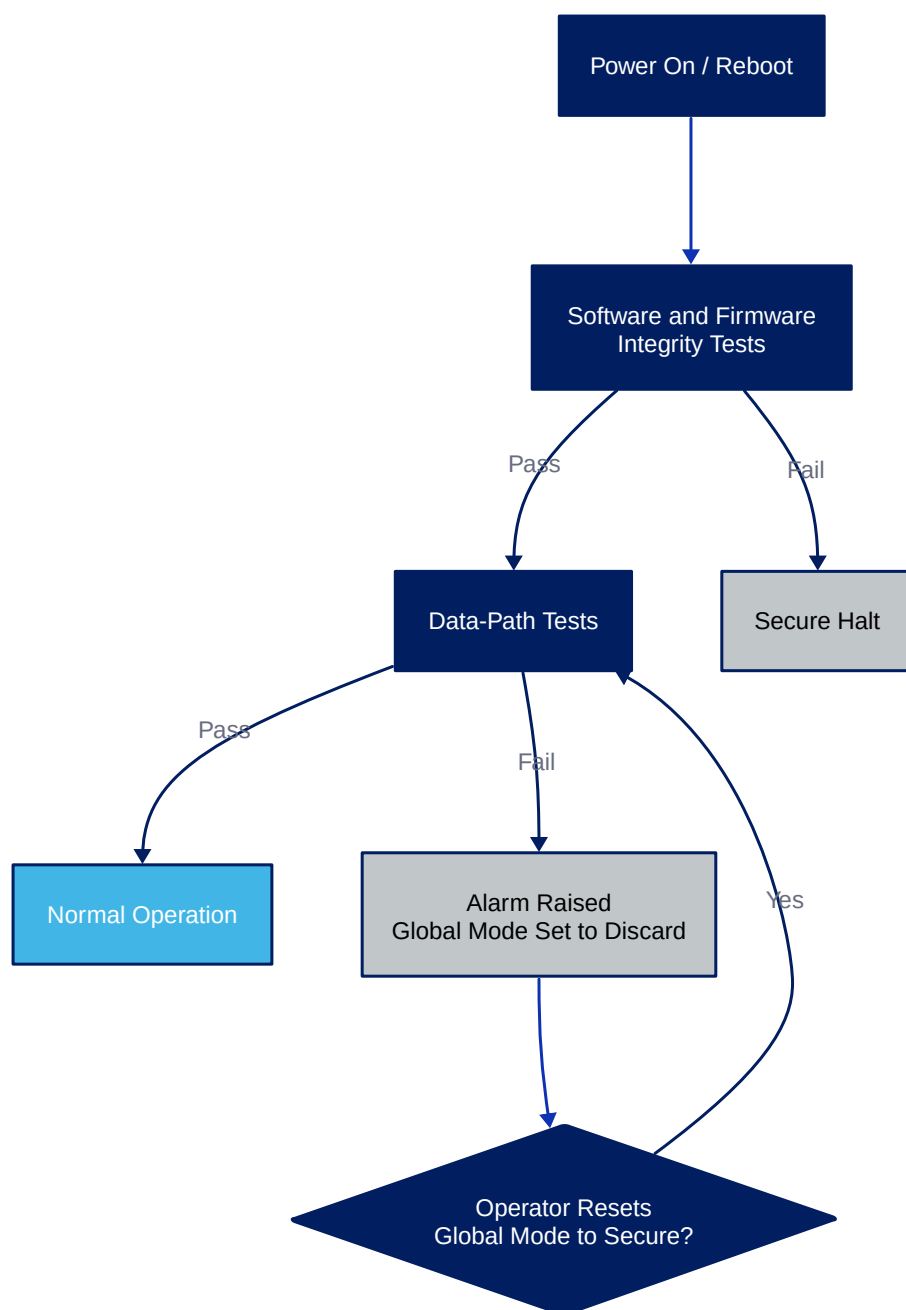


Figure 4. Self-test boot sequence

Secure Halt

If significant errors are detected during the diagnostic phase, the CN4020 enters a *Secure Halt* state instead of completing the boot sequence. In this state:

- All interface ports stop passing traffic

- The unit cannot be managed via the CLI or SNMP
- A diagnostics message is added to the event log
- Temperature protection and tamper services remain active
- The front panel LEDs flash red



A unit in Secure Halt requires recovery before it can return to service. Attempt to clear the condition by power-cycling the CN4020; if the Secure Halt persists, the unit cannot be recovered locally and must be returned to the factory. For the full recovery procedure, see [Chapter 11: Troubleshooting](#).

Tamper Response

If the CN4020 is *tampered*, a log message is generated and the LEDs flash red. The CN4020 is then erased. If the unit has been tampered but is no longer in the tampered state, it boots normally; however, a log message is still generated.



A tamper is an *unauthorized physical event* — such as an attempt to open the enclosure — detected by the internal tamper-protection circuitry, whereas an erase is initiated intentionally by an administrator. Both zeroize all Critical Security Parameters, including the System Master Key and all user passwords. A tamper additionally returns the encryptor to its factory default state, resetting credentials to `admin / $Password1`.

4.1.3. Connecting to the Management Interface

The CN4020 provides multiple management interfaces for initial configuration and ongoing administration. This section describes how to establish a management connection.

Management Interface Options

The CN4020 supports three management access methods:

Ethernet management port (SNMPv3)

An RJ45 Ethernet port for connecting the encryptor to a management network. This is the primary method for commissioning and ongoing management.

Serial console port (CLI)

An RS-232 serial port for direct CLI access. Use the serial console when no IP address has been assigned, or for local troubleshooting.

In-band management (SNMPv3)

Management traffic carried within the encrypted data network. Requires an IP address to be configured first.

For a complete description of management interfaces and access methods, see [Chapter 5: Management](#).

Connecting via the Ethernet Management Port

Each CN4020 has a 10/100/1000Base-T (RJ45) Ethernet port for management.

1. Connect an Ethernet cable from your computer to the management port on the CN4020.
2. Verify the connection:
 - The green link indicator on the RJ45 connector is lit
 - The flashing orange LED indicates Ethernet activity

The management port is auto-sensing and uses auto-negotiation to determine the fastest available speed. The port attempts to connect at 1000 Mbps first, then falls back to 100 Mbps and 10 Mbps until a stable connection is established.

Connecting via the Serial Console Port

The CN4020 provides a CLI accessible through the serial console port. The serial port is a DTE (Data Terminal Equipment) device.

- To connect to another device, use the supplied null-modem cable.

Ensure you have the appropriate serial cable ready at installation time.



Do not connect the serial port to a terminal server that is accessible over an unsecured network without additional protection mechanisms.

Table 9. Serial port settings

Parameter	Setting
Baud rate	9600 bps
Parity	None
Data bits	8
Stop bits	1
Software flow control (XON/XOFF)	Off
Hardware flow control	Off

Table 10. Terminal emulator settings

Parameter	Setting
Local Echo	Off
Line wrap	On
CR/LF translation (inbound)	Off
CR/LF translation (outbound)	Off

Logging In to the CLI

To access the CN4020 command line interface for initial configuration:

1. Open a terminal emulator application (such as PuTTY or Tera Term).
2. Configure the serial connection using the settings in the [serial port settings](#) table above.
3. Press **Enter** to bring up the login prompt.
4. Log in with the default credentials (`admin` / `$Password1`).



The CN4020 does not ship with a preconfigured management IP address. You must assign a management IP address via the CLI before the unit can be managed remotely via CM7 or SSH.

4.1.4. Commissioning

Commissioning is the process of configuring the CN4020 for use in your network and establishing secure key management with peer encryptors, either through a common Certificate Authority (for Line, MAC, and VLAN modes) or a configured Key Provider (for Transport Independent Mode).

Commissioning Overview

The commissioning steps are:

1. Set the management IP address so that CM7 can connect to the unit.
2. Set the encryptor name and date/time.
3. Activate the unit (change the default credentials).
4. Choose the encryption mode and trust model (see [Encryption Mode and Trust Model](#)).
5. Install the initial trust artefact — a certificate or KDK (see [Install the Initial Trust Artefact](#)).
6. Enable encryption (see [Chapter 6: Encryption Configuration](#)).

Setting the IP Address

The CN4020 requires a valid static IP address before CM7 can manage it via the management port or remotely via in-band management. DHCP is not supported because deterministic management addressing is required to ensure reliable discovery, configuration, auditing, and ongoing management of deployed devices.

Both IPv4 and IPv6 addresses are supported on the Ethernet management port.

The management IP address can be set using one of the following methods:

Method 1: CLI

1. Connect to the serial console port using a terminal emulator (see [Connecting via the Serial Console Port](#)).

2. Log in with the default credentials (**admin** / **\$Password1**).
3. Use the **ip** command to set the IP address, subnet mask, and default gateway.

Refer to the [CLI Reference](#) for full **ip** command syntax.



The management IP address is not visible from the networks connected to the Local or Network ports. It is used only for management traffic on the management port.

Method 2: Front Panel

This model does not have a front panel keypad. Use the CLI or CM7 to set the IP address.

Method 3: CM7

If the CN4020 already has an IP address assigned (including a factory-configured address), the address can be changed from CM7:

1. Discover the encryptor in CM7.
2. Navigate to the **Network Addressing** menu item of the selected unit.
3. Enter the new IP address, subnet mask, and gateway.
4. Apply the changes.



Factory-shipped encryptors may already be configured with an IP address. Reconfigure this address with a valid address for your network before deployment.



If you load temporary IP addresses for local testing, ensure the correct production IP addresses are loaded before relocating units to a different subnet. Otherwise, an administrator must visit the site and reconfigure the address via the CLI.



Address changes take effect immediately; there is no need to restart the encryptor. Subsequent IP changes can also be made remotely via SNMP.

Setting the Encryptor Name

Assign a descriptive name to each CN4020 for identification in CM7 and log entries.

The encryptor name can be set using CM7 or the CLI:

- **CM7:** Navigate to the **Overview** menu item of the selected encryptor and enter the name.
- **CLI:** Use the command **hostname**.

Setting Date and Time

The CN4020 requires a valid date and time for correct operation. The encryptor has an internal battery-backed Real Time Clock (RTC) and supports NTP for synchronisation with external time

servers.

The date, time, and timezone can be set using the following methods:

CLI

1. Log in to the CLI with the default credentials (`admin` / `$Password1`).
2. Use the `date` command to set the date and time.
3. Use the `timezone` command to set the timezone.

Refer to the [CLI Reference](#) for full command syntax.

CM7

Use the **Date/Time** option in the CM7 Manage screen to set the date and time.



Each encryptor uses its Real Time Clock to maintain the date and time. Optionally, an NTP server can be configured to synchronise date and time automatically. For NTP configuration, see [Chapter 5: Management](#).

Activation

The activation process changes the credentials of the default administration account from `admin` / `$Password1` to production credentials. Activation requires an administrator logged in to the `admin` account and, for CM7 activation of remote units, an operator at the encryptor.



User accounts cannot be created until the encryptor has been activated.

Activating with CM7

Use CM7 to activate encryptors, particularly units in remote locations. To do this, the encryptor must enter "Activation Mode" as follows:

1. Use the CLI command `activate -e`
2. Use the CLI command `activate -v` to validate the hash values against those reported in CM7.

Refer to the CM7 documentation for the complete activation procedure.

Activating from the CLI

Local encryptors can be activated using the CLI `activate -l` command. This replaces the default administrator password with a new, strong password.

Refer to the [CLI Reference](#) for full `activate -l` command syntax.

Encryption Mode and Trust Model

Before loading any keys or certificates, decide which encryption mode the CN4020 will operate in.

This is a commissioning-time decision: it determines the trust artefact you load in the next step and the configuration path you follow in [Chapter 6: Encryption Configuration](#). This section is a decision aid only — for the underlying concepts, see [Encryption Modes](#) in Chapter 2: Product Overview.

The CN4020 supports two families of encryption mode, distinguished by their root of trust:

Table 11. Encryption mode and trust model

	Layer 2 modes	Transport Independent Mode (TIM)
Root of trust	X.509 certificate	KDK, or external key server (KMIP)
Key management	Inline establishment; control plane between encryptors	Key Derivation Function or external key server; no control plane
Encryption layers	Layer 2 only	Layers 2, 3 and 4 (concurrent)
Policy basis	Ethertype, then VLAN ID / remote MAC	Ethertype, then 5-tuple IP
Networks	Ethernet only	Ethernet, IP WAN, Internet, MPLS, cloud
Trust artefact loaded at commissioning	Certificate	KDK (or key-server configuration)



Your choice here determines the trust artefact you load in the next step and which Chapter 6 configuration path you follow. Switching encryption mode later resets the connection and policy configuration to factory defaults and reboots the unit, so choose deliberately at commissioning.

If you choose a Layer 2 mode, see [Connection Mode Selection](#) in Chapter 6 to choose between Point-to-Point (Line), TRANSEC, MAC, and VLAN multipoint. For Transport Independent Mode, see [Configuring TIM Mode](#) in Chapter 6.

Install the Initial Trust Artefact

Based on the encryption mode chosen above, load the artefact that establishes trust with peer encryptors. The trust artefact is loaded during or immediately after activation.

For Layer 2 modes — Certificate

Each CN4020 must be signed by a common Certificate Authority to establish trust with its peers. Certificates can be loaded using:

- **CM7** — using the internal (CM7-based) Certificate Authority or an external CA
- **External CA** — import certificates signed by a third-party Certificate Authority

For the complete certificate-installation and management procedures, see [Installing Certificates](#) and [Certificate Management](#) in Chapter 5: Management.

For Transport Independent Mode — KDK or key server

When operating in TIM, each CN4020 establishes trust through its configured key provider rather than a certificate:

- **KDK (Key Derivation Function)** — load a shared Key Derivation Key, generated and distributed using the internal (CM7-based) KDK generator. The same KDK must be set on every device in the network.
- **External key server (KMIP)** — configure the encryptor to obtain keys from a third-party KMIP key server reachable by all encryptors.

For the complete KDK management procedure, see [KDK Management](#) in Chapter 5: Management & Administration. To bring a unit fully into TIM service after loading the KDK, follow the [TIM Commissioning Checklist](#) in Chapter 6: Encryption Configuration.

4.1.5. Verifying Initial Setup

After completing the commissioning process, verify that the CN4020 is operational:

1. Connect to the CN4020 using CM7 or SSH:
 - **CM7:** Open CM7, connect to the encryptor via its management IP address, and check **Front Panel Mimic** and **Alarms** for unit status and active alarms.
 - **CLI:** Open a connection to the console port and use the `alarms` command to verify the unit is operational.
2. Check the front panel indicators:
 - A steady green **Status** LED indicates normal operation
 - Flashing red LEDs indicate a tamper or fault condition
3. Verify network connectivity by pinging the management IP address from your network.
4. Confirm the activation state — the unit should no longer accept the default credentials.
5. Check the **Event Log** for any errors or warnings generated during the boot and commissioning process.

For LED indicator reference and diagnostic procedures, see [Chapter 10: Troubleshooting](#).

4.1.6. Next Steps

After initial setup is complete, proceed to:

- [Chapter 4: Network Configuration](#) — configure data port connections, VLANs, and management network topology
- [Chapter 5: Management](#) — configure user accounts, certificates, SNMP, syslog, and remote access
- [Chapter 6: Encryption Configuration](#) — configure encryption policies, connection modes, and key management

Chapter 5. Management & Administration

5.1. Management Overview

The CN4020 provides multiple management interfaces for configuration, monitoring, and ongoing administration. This chapter covers the management tools, user account administration, SNMP configuration, certificate management, syslog setup, remote access, and integration with external management services.

5.1.1. Management Interfaces

The CN4020 supports the following management interfaces:

CM7 Network Manager

A graphical management application based on SNMPv3. CM7 connects to encryptors via the RJ45 Ethernet management port and provides full configuration, monitoring, and certificate management capabilities.

Command Line Interface (CLI)

A text-based interface accessible via the physical serial port (local) or SSH (remote). The CLI provides configuration and monitoring functions equivalent to CM7. A terminal emulator such as PuTTY or TeraTerm is required for serial access.

SNMP (Third-Party Managers)

Encryptors are managed via SNMPv3 and can therefore be integrated with third-party management systems. Senetas provides the required MIBs. SNMPv1 read-only monitoring is also available as an option.

RESTful JSON Interface

An HTTP(s) interface for remote monitoring and issue detection. The RESTful interface leverages the existing SNMP MIB, allowing OID-based queries via URL parameters.

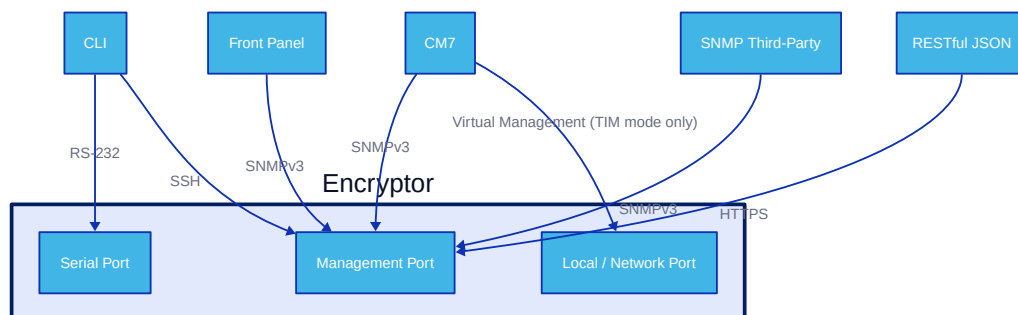


Figure 5. Management interfaces and access methods

5.1.2. Access Methods

Encryptors have two physical management ports: a serial port for CLI access and an RJ45 Ethernet port for SNMPv3-based management. In addition, encryptors operating in TIM mode support virtual management via their Local or Network port.

The available access methods are:

- **Front panel** — direct Ethernet connection to the management port
- **Out-of-band** — management traffic carried on a dedicated management network
- **In-band** — management traffic carried within the encrypted data network
- **Virtual** — management via the Local or Network port (TIM mode only)



When virtual management is enabled, front panel management is disabled and vice versa.

For detailed configuration of management network addresses, IP settings, and gateway configuration, see [Chapter 4: Network Configuration](#).

5.2. CM7 Setup

CM7 is the primary graphical management tool for the CN4020. It communicates with encryptors over SNMPv3 and provides a comprehensive interface for configuration, monitoring, and certificate management.

5.2.1. Launching and Logging In

User credentials are stored securely within each encryptor and are used to authenticate access whenever you log on.

To log in to CM7:

1. Launch the CM7 application. The login dialog is displayed.
2. Enter your **User Name** and **Password**.

User names may contain alphanumeric characters, underscores, dots, and dashes only. All other characters are discarded.

3. Select the target encryptor from the **Encryptor** selector.
4. Click **OK** to connect.



The **Skip** option allows login using the default credentials (**admin** / **\$Password1**). This is convenient when initially activating units.

By default, privacy is enabled and CM7 uses a Diffie-Hellman key exchange to authenticate the user and encrypt each SNMPv3 request.

CM7 stores the names and IP addresses of all discovered encryptors in its database, populating the Encryptor selector for convenient access.



Using the same account names and passwords on all encryptors allows them to be managed from a single CM7 login session without logging out between units.

5.2.2. CM7 Settings

The CM7 user interface can be customised via the Settings screen, accessed by clicking the **cog** icon at the bottom right of the primary CM7 screen. Settings are saved in a CM.ini file or, if selected, in a Configuration server database.

The configurable settings include:

Table 12. CM7 Settings

Setting	Description
Explicit Login	When enabled, only the entered credentials are used to log in to encryptors. If unsuccessful, the next attempt requires credentials to be re-entered via the Login dialog.
Non Activated Password	The password used to access encryptors that have not yet been activated. Defaults to \$Password1 .
Station ID	Identifies the CM7 workstation for concurrent management, allowing multiple managers to work with the same encryptors without their sessions interfering with one another. The default of 0 selects dynamic station IDs, where CM7 is assigned a management slot automatically as needed. This suits almost all deployments and is the recommended setting. A static Station ID from 1 to 5 can be set instead to reserve a fixed slot.
Discovery Polling Timeout (sec)	Timeout for encryptor discovery. Default: 2 seconds. Increase for noisy or large networks.
Discovery Polling Retries	Number of retry attempts during discovery. Default: 1. Increase for noisy environments.
Font	CM7 interface font size, configurable from 9 to 18 point. Default: 11 point.
Hide Not Applicable Settings	When enabled (default), settings that do not apply to the current encryptor model or context are hidden.
Number of Tiled Manage Windows Across	Number of side-by-side encryptor management windows. Default: 2.
Session Timeout (min)	CM7 session inactivity timeout. Default: 5 minutes. Maximum: 60 minutes.
Manage Windows Refresh Rate (sec)	Refresh interval for the currently displayed Manage Window. Default: 15 seconds.

Setting	Description
Encryptor List Refresh Rate (sec)	Refresh interval for the encryptor list. Default: 20 seconds.
Network View Refresh Rate (sec)	Refresh interval for the network view. Default: 60 seconds.
Enable Trap Listener	Enables CM7 to receive SNMP traps sent to its configured trap address.
Trap Listener Port	The port on which CM7 listens for SNMP traps.
Display Reports / Warnings / Errors	Controls which message types are shown in the CM7 log window.
CM Settings Location	Path to the CM settings file (INI file) or Configuration server database selection.

The **CA/Key Management** button opens the Create CA screen for configuring CM7 as a Certificate Authority and defining KDK keys for TIM mode.

5.2.3. Initial Configuration Settings

The first time CM7 runs after installation, it prompts for the settings storage location. Settings can be stored in either a local INI file or a Configuration server database.

INI File Storage

If an INI file is selected, the default location can be changed using the **Browse** button. The path can be set to the **Current User Path** or the **Public Path** as selected during installation.

Redis Server Database

Redis server databases provide a convenient way to share encryptor lists and PKCS#12 files across teams, geographies, or departments. The Redis server can be on a central server or on the local system.

To configure a database:

1. Enter the **Server IP** address and **Port**.
2. Press **Enter** or click the refresh icon.

If the connection is successful, a green tick is displayed. If the connection fails, the indicator is red. Hover over the indicator to display the server status.

3. Select or create a **Database Name**.

Creating a database with the same name as an existing database will overwrite the existing settings.



The Redis server must be configured to use "legacy authentication".



IP address **127.0.0.1** can be used for a server located on the CM7 system.

To delete a database, select it and click the **delete** icon to the right of the Database Name field.



The delete function is hidden if the selected database is currently open.

5.3. User Account Management

The CN4020 uses a role-based access model. User accounts are stored locally on each encryptor — they are not kept in a central repository or in the CM7 database. Up to 30 user accounts can be created per encryptor.

5.3.1. Roles and Privilege Levels

Each user account is assigned one of four privilege levels:

Table 13. User privilege levels

User Level	Privileges Granted
Administrator	Unlimited ability to configure and manage the encryptor. Can initiate firmware upgrades via SNMP, CLI, or keypad.
Supervisor	Can configure with the following exceptions: cannot load certificates, cannot create or edit user accounts, cannot clear audit or event logs, cannot initiate firmware upgrades.
Operator	Monitoring only. Cannot make configuration changes or initiate firmware updates.
Upgrader/Maintainer	Can initiate firmware upgrades remotely via SNMP (not CLI). Cannot make any other configuration changes.

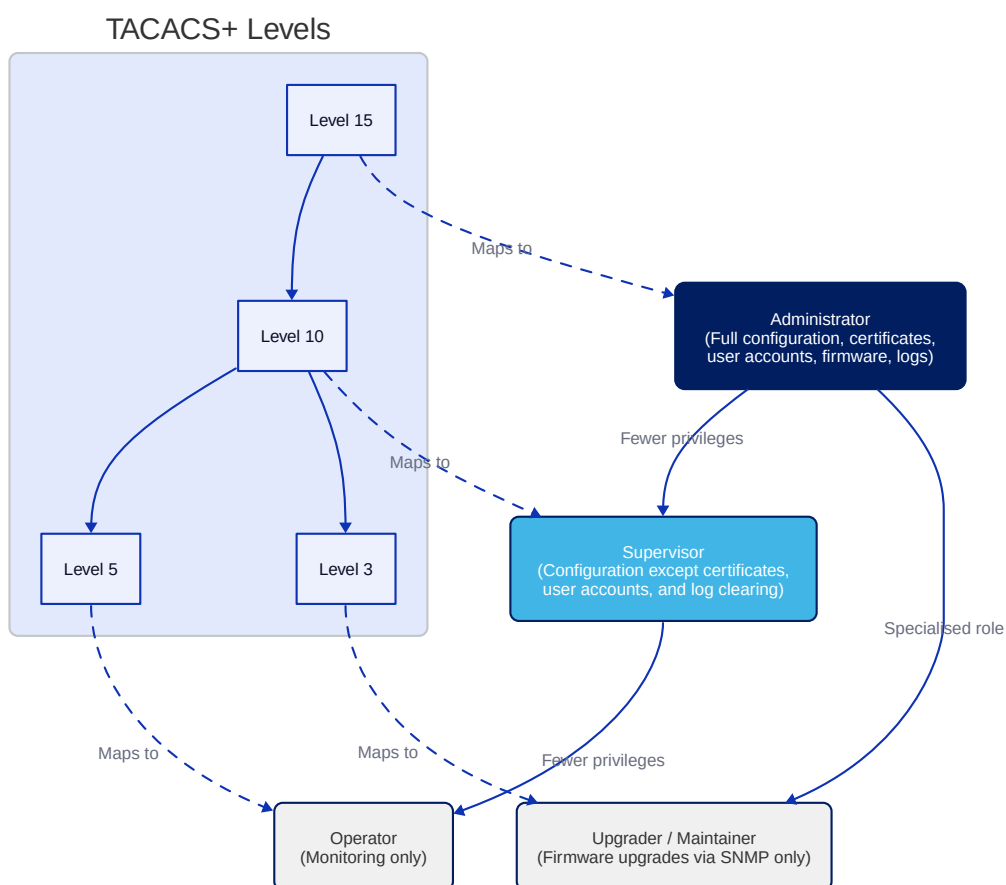


Figure 6. User privilege levels and capabilities

5.3.2. Default Password Behaviour

An unconfigured or freshly erased encryptor contains a single default administrator account:

- **User Name:** `admin`
- **Password:** `$Password1`

In this unactivated state, the default administrator can:

- Activate the encryptor by setting a new password
- Enable Enhanced Password Mode features
- Modify the password policy parameters
- Modify the user inactivity lockout period

For the activation procedure, see [Activation](#) in Chapter 4: Getting Started.



A warning is displayed if the credentials of the new account are set to `admin` /

\$Password1, as this presents a security risk.

5.3.3. Creating and Managing User Accounts

User accounts are managed via the **User** menu in CM7 or via the CLI `users` command.

Each user account is defined by:

- **User Name** — short-form name used as the login ID
- **Description** — long-form name used for reporting purposes
- **Privilege Level** — Administrator, Supervisor, Operator, or Upgrader/Maintainer
- **User Account** — active or disabled
- **Console Access** — enabled or disabled (controls CLI access)
- **SNMP Access** — enabled or disabled (controls SNMP management access)

To create a user account via CM7:

1. Log in to the encryptor with administrator credentials.
2. Navigate to the **User** configuration screen.
3. Click **Add** to create a new account.
4. Enter the user name, description, and password.
5. Select the privilege level.
6. Enable or disable Console Access and SNMP Access as required.
7. Apply the changes to the encryptor.

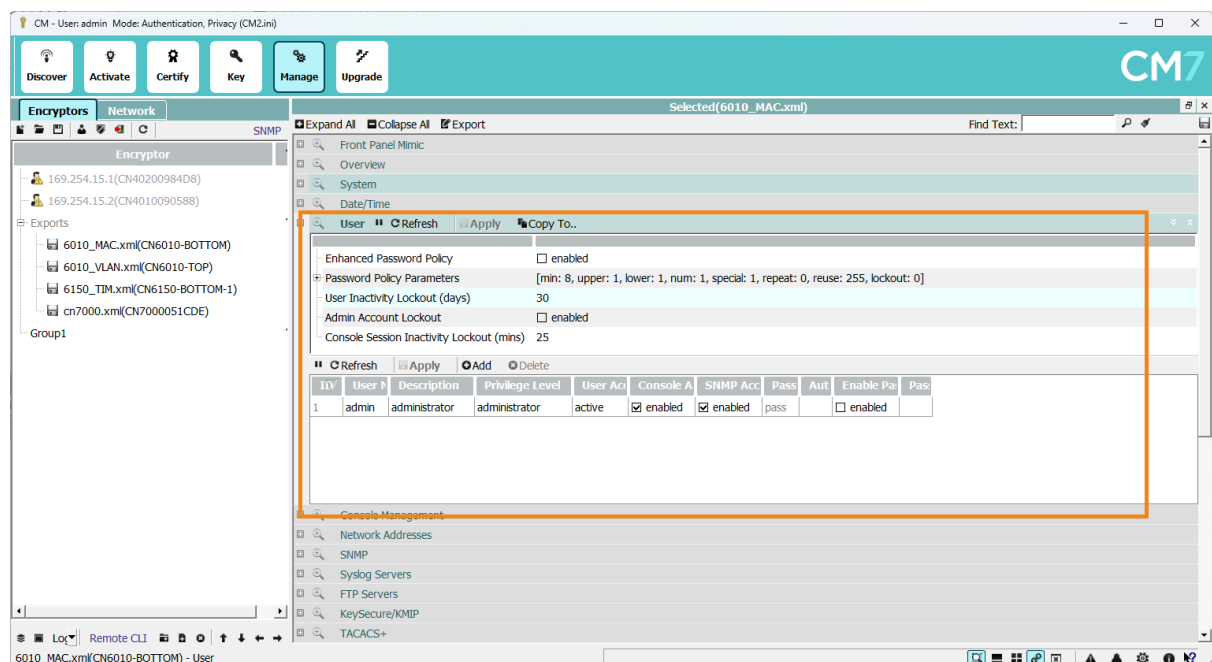


Figure 7. User management

There must always be at least one administrator account on the encryptor. The system does not allow

deletion of the last administrator account. If the encryptor is erased, the default administrator account (`admin` / `$Password1`) is re-established.



User accounts cannot be created until the unit has been activated.

The Encryptor list in CM7 allows multiple encryptors to be selected and updated simultaneously, provided the current user has the same login credentials on each unit.

5.3.4. Password Policy

User passwords are subject to configurable lexical diversity requirements.

Table 14. Default password policy parameters

Requirement	Default Value
Minimum Password Length	8
Minimum Uppercase Characters	1
Minimum Lowercase Characters	1
Minimum Numeric Characters	1
Minimum Special Characters	1
Minimum Consecutive Repeat Characters	0
Reuse History	255
Change Lockout Period	0

When lexical checking is enabled (the default), passwords are validated against these requirements at account creation.

Within each character group, there are no restrictions on which specific characters can be used.

5.3.5. Enhanced Password Mode

Enhanced Password Mode strengthens the default password policy with additional security controls. It is disabled by default.

When enabled, the following functionality applies:

- User lockout after 2 unsuccessful login attempts within an hour (applies to Operator, Upgrader, and Supervisor accounts; administrator accounts are exempt unless Administrator Lockout is enabled — see [Administrator Lockout](#))
- Password lexical checking at logon (not just at account creation)
- Logging of failed logon attempts
- Disallowing passwords that match the User ID

- Password expiry for users on CLI and SNMP/RESTful interfaces (see [Password Expiry](#))

Enhanced mode supports conformance to the AR-25 standard.



Enhanced Password Mode can only be enabled or disabled by an administrator account, regardless of the encryptor's activated state.

Enhanced mode is enabled via the **Management Access** tab in CM7 or the CLI **password** command.

Enhanced lexical checking allows the following additional parameters to be configured:

- Minimum password length: 15–29 characters
- Minimum uppercase characters: 1 or 2
- Minimum lowercase characters: 1 or 2
- Minimum numeric characters: 1 or 2
- Minimum special characters: 1 or 2

Password Expiry

An administrator can set a password expiry period (in days) on each user account individually. The default is 0 (no expiry).

The conditions under which password expiry takes effect depend on the user's privilege level:

Table 15. Password expiry conditions by role

User Role	Conditions Required
Operator, Upgrader, Supervisor	The user's password expiry must be set to a non-zero value, and Enhanced Password Mode must be enabled.
Administrator (console access only)	The user's password expiry must be set to a non-zero value, and Enhanced Password Mode must be enabled, and Administrator Lockout must be disabled (see Administrator Lockout).
Administrator (console, SNMP, and RESTful access)	The user's password expiry must be set to a non-zero value, and Enhanced Password Mode must be enabled, and Administrator Lockout must be enabled (see Administrator Lockout).



There are no alarms or warnings that a password expiry date is about to be reached. The onus is upon the user to track password expiry dates as necessary.

5.3.6. Administrator Access Controls

Administrator-level access controls allow configuration of how users interact with the encryptor.

Table 16. Administrator access controls

Feature	Description
Enable Serial Console Port	Enable or disable access via the serial craft port.
Enable Front Panel Keypad	Enable or disable the keypad to control physical access.
Enable Front Panel USB	Enable or disable firmware upgrades via the USB port.
Enable Password Lexical Check	Enable or disable lexical checking of user passwords. Units with Common Criteria certification do not allow lexical checking to be disabled.
Password Reuse Count	Number of unique passwords that must be entered before a password can be reused for an account.
User Inactivity Lockout	Number of days before an inactive account is disabled. See User Inactivity Lockout .
Session Inactivity Logout	Period of inactivity on the console after which the user is logged out.
Enable Enhanced Password Policy	Enable or disable enforcement of enhanced lexical checking. See Enhanced Password Mode .

5.3.7. User Inactivity Lockout

The User Inactivity Lockout feature enables administrator accounts to block any account from logging in after a specified period of inactivity.

- **Range:** 0–1825 days
- **Default:** 30 days
- **Disabled:** Set to 0



User Inactivity Lockout can only be modified by a user with administrator privileges.



The Enhanced Password Policy must be activated for this feature to take effect.

When the inactivity period elapses, the affected account is blocked. An administrator must re-enable the account via CM7; a password change is not required.

The inactivity period applies differently depending on user role:

- **Operator, Upgrader, and Supervisor accounts** — locked out from CLI and remote management systems (CM7/SNMP) when the inactivity period elapses
- **Administrator accounts** — affected only when **Administrator Lockout** is enabled (see [Administrator Lockout](#))

An Event log entry is created when a user account becomes inactive.

CLI: `users-u<days>`

5.3.8. Administrator Lockout

The Administrator Lockout control determines whether administrator accounts can be locked out due to inactivity or password expiry.

- Disabled by default
- Requires administrator privileges to enable or disable
- Persistent across power cycles, reboots, and `initcfg` (all options)
- All erase triggers (factory erase, erase, tamper) reset the control to the default disabled state



Enabling this control could require an emergency erase of the encryptor if all administrator accounts become locked.

When Administrator Lockout is enabled:

- Administrator accounts are subject to inactivity lockout via CLI and CM7/SNMP
- Administrator accounts are subject to password expiry via CM7/SNMP
- If an administrator's password has expired, the password cannot be updated at the CLI prompt

If all administrator accounts are locked out, management access at the administrator privilege level is lost. If all user accounts are locked out across all interfaces, management access to the device is completely lost.

Recovery procedures depend on the encryptor type:

Table 17. Recovery from full lockout

Encryptor Type	Recovery Method
Encryptors with front panel keypad	Perform an emergency erase (hold ESC and ENT simultaneously for 10 seconds), or tamper the device (pin hole).
Encryptors without front panel keypad	Tamper the device (pin hole).
Virtual encryptors	Spin the Eth0 MAC address.



An emergency erase via the front panel keypad is equivalent to issuing `erase` at the CLI — it returns the device to defaults but retains IP settings. Both an erase and a tamper destroy all keys, including the System Master Key; a tamper additionally clears the retained IP settings, returning the device to a full factory default state.

5.3.9. Console Management

The Console Management settings control the information displayed when the CLI is used.

Pre-Login Banner

The message displayed on the terminal screen before the user logs in. Typically used to advise the user of security requirements.

Post-Login Banner

The message displayed after the user logs in. Typically used to reinforce security requirements, such as advising the user not to leave the terminal unattended.

Prompt

The text displayed before the > symbol as the CLI prompt. Typically set to the encryptor model and/or location.



The pre-login and post-login banners can also be set using the CLI **banner** command.

5.4. SNMP Configuration

Management via SNMP is based on SNMPv3, which provides user authentication and connection privacy using Diffie-Hellman based encryption. SNMPv3 uses the UDP connectionless protocol, which can be routed over any layer 3 network.

5.4.1. SNMPv3 Security

SNMPv3 addresses the security deficiencies of earlier SNMP versions by supporting authentication and encryption. The security model uses the concept of a user for which security parameters — levels of security, authentication, privacy protocols, and keys — are configured for both the agent (encryptor) and the manager.

The security model protects against message delays and message replay using time indicators and request IDs.

Management packets can be sent at two security levels:

authNoPriv (Authentication only)

User credentials are authenticated before access to the encryptor is granted.

authPriv (Authentication and Privacy)

SNMP traffic between the manager and the encryptor is both authenticated and encrypted.



FIPS Mode must be disabled in order to manage the device with authNoPriv.



UDP is connectionless — the management system issues commands that are not acknowledged by the encryptor. CM7 provides configurable retry and timeout

parameters to accommodate noise and network delays.

5.4.2. Enhanced Algorithm Support

The CN4020 supports SHA-512 for authentication and AES-256 for privacy in SNMPv3.

Enhanced algorithm support can be enabled in two ways:

- **CLI:** `snmpcfg -e on|off`
- **CM7:** SNMP pane → select the **Enhanced SNMPv3** tick box in the Manage screen



When Enhanced SNMPv3 is disabled (the default), SNMPv3 uses SHA-1 for authentication and AES-128 for privacy for backward compatibility.

When an encryptor is first upgraded to v5.5.x, the default setting for Enhanced SNMPv3 is **disabled**. However, all subsequent triggers — such as a factory erase or re-upgrade — retain whatever setting had been selected for Enhanced SNMPv3 prior to the trigger.

CM7 can manage a mixture of SHA-1/AES-128 or SHA-512/AES-256 encryptors configurations simultaneously.

5.4.3. SNMPv3Q (Quantum-Resistant SNMP)

To defend against the quantum threat, the SNMPv3 Diffie-Hellman kick-start mechanism supports parallel (hybrid) DH and PQC (Post-Quantum Cryptography) KEM mechanisms. The encryptor (SNMP agent) and CM7 (SNMP browser) derive both a DH key and a KEM shared secret, which are then XORed together to provide quantum-resistant operations.

SNMPv3Q uses standardised post-quantum cryptography KEM (Key Encapsulation Mechanism) algorithms.

To enable SNMPv3Q:

- **CLI:** `snmpcfg -q on|off`
- **CM7:** SNMP pane → select the **SNMPv3Q** tick box in the Manage screen



Enhanced SNMPv3 must be enabled for SNMPv3Q to function.



Other third-party SNMP browsers may not support the hybrid SNMP DH kick-start mechanism. CM7 7.10.0 or later is required to use this feature.

CM7 can manage a mixture of SNMPv3Q-enabled and SNMPv3Q-disabled encryptors simultaneously.

5.4.4. SNMP Security Level

The default security level for CM7 is **SNMPv3: Authentication, Privacy**, which provides a Diffie-

Hellman authenticated and encrypted connection.

The available security levels in CM7 are:

- **SNMPv3: Authentication, Privacy** (default) — full Diffie-Hellman authentication and encryption
- **SNMPv3: Authentication, No Privacy** — provided for compatibility with encryptors running legacy firmware and other SNMP network management tools that do not support Diffie-Hellman
- **SNMPv1: No Authentication, No Privacy** — read-only access only

5.4.5. SNMP Trap Configuration

The SNMP configuration screen allows you to define the addresses to which the encryptor sends SNMP trap messages. Up to 8 trap receivers can be configured, each individually enabled or disabled.

The SNMP management parameters include:

SNMP Privacy

Enables encryption of traffic between CM7 and the encryptor. Enabled by default.

Auth Failures Time Window

The time in minutes during which a user is locked out after consecutive authentication failures. Applicable to SNMPv3 authPriv only.

Auth Failures Before Lockout

The number of consecutive SNMPv3 authPriv failures that trigger a lockout for the Auth Failures Time Window.

Alarm Trap Period

The period in seconds between traps sent for active unacknowledged alarms. A value of 0 sends a trap only when the alarm becomes active — not periodically.

Each trap receiver is defined by:

- **Address** — the IP address of the SNMP receiver
- **Status** — enabled or disabled



CM7 can itself be configured as a trap receiver. For CM7 to receive traps, the trap listener must be enabled in CM7 Settings (see [CM7 Settings](#)).

5.4.6. SNMPv1 Monitoring

SNMPv1 provides read-only monitoring access to the encryptor. It is disabled by default.



SNMPv1 read-only monitoring is configured independently of FIPS mode and can be enabled whether or not FIPS mode is active. Enabling it does not take the encryptor outside its FIPS-validated configuration. The FIPS requirements

described in [FIPS 140-3 Mode](#) apply to the SNMPv3 management connection, not to this read-only monitoring channel.

Table 18. SNMPv1 settings

Feature	Description
Enable SNMPv1 (Monitor Only)	Enable or disable SNMPv1 monitoring. Requires a restart to take effect.
Community String	The community string used to authenticate SNMPv1 clients and identify trap messages. Changing the string logs an audit message. Requires a reboot to take effect.



If SNMPv1 access is used, change the community string from **Public** to a site-specific value to maximise security.

5.4.7. SNMP over SSH

SNMP traffic can be tunnelled through an SSH tunnel to provide benefits such as:

- TCP Packet Retry behaviour
- Limits management hosts to with appropriate SSH keys

It can be configured on the CN4020 as follows:

1. Configure SSHCLI and record the port number in use
2. Load any required SNMP host's ECDSA SSH public key onto the Encryptor
3. Enable SNMP over SSH

SNMP over SSH CM7 Configuration

In order to use SNMP over SSH with CM7, the following steps should be followed:



CM7.11 or later is required.

1. When opening CM7, click "Enable TCP Transport Over SSH" in the login window.
2. Ensure the SSH Credentials Key File has had it's public key loaded onto the CN4020.
3. In addition to entering the Encryptor credentials, enter the password for the SSH Private Key, and the SSHCLI port.
4. Click "Apply" to login to CM7.

5.4.8. FIPS 140-3 Mode

FIPS 140-3 mode is enabled by default. Disabling or re-enabling FIPS mode forces a restart of the encryptor and triggers any applicable startup diagnostic processes.

When FIPS mode is enabled, the following requirements apply to the SNMPv3 management connection:

- SNMP privacy is enforced
- Authentication uses a Diffie-Hellman key exchange

SNMPv1 read-only monitoring (see [SNMPv1 Monitoring](#)) is configured separately and can be enabled regardless of whether FIPS mode is active.

Table 19. FIPS 140-3 settings

Feature	Description
Disable FIPS PUB 140-3 mode	Enable or disable FIPS mode.
Disable SNMP Privacy	Enable or disable privacy on the SNMP management connection.

For full compliance details, see [Chapter 11: Compliance](#).

5.5. Certificate Management

Each encryptor within a security domain must have at least one certificate signed by the same Certificate Authority (CA). CM7 includes a built-in CA that can sign certificates for all target encryptors. Alternatively, any third-party PKI-compatible CA can be used.

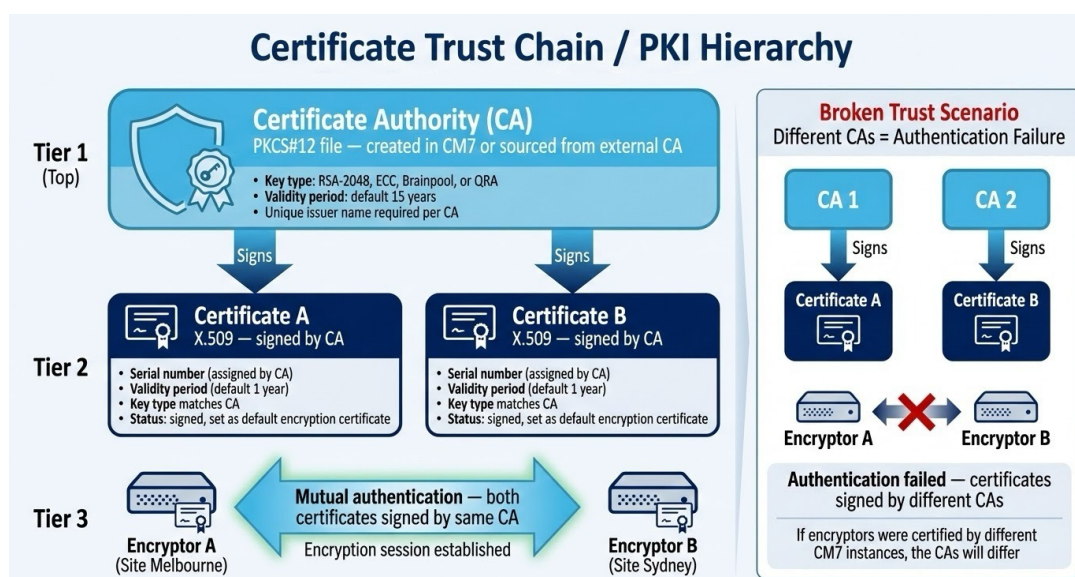


Figure 8. Certificate trust chain and PKI hierarchy

5.5.1. Certificate Authorities

CM7 supports signing certificates using the following key types:

RSA

Rivest-Shamir-Adleman with 2048-bit keys (optionally 4096-bit). This is the default and is considered secure by NIST.

ECC (Elliptic Curve Cryptography)

Faster and more secure than RSA. Preferred by many cryptographic professionals.

Brainpool

An ECC variant that does not use NIST parameters. Preferred by some users for this reason.

PQC (Post-Quantum Cryptography)

Hybrid implementations using quantum-resistant algorithms based on NIST standards. Provides extended security to defend against quantum computing threats.



For most applications, RSA is considered adequate. Your security policy will determine which key type to use.

Certificate Chain Validation

CM7 validates any CA file that is opened by confirming that the entire certificate chain is present and valid. If no valid certificate chain can be established, an error is displayed on the **Internal CA** tab.

CA Serial Number Size

CAs may have a serial number longer than the default 8 bytes. The serial number can be extended by adding bytes in **:XX** format, where **X** is a hex character (0–F).

5.5.2. Creating the PKCS#12 File

The Certificate Authority functionality of CM7 is provided via a PKCS#12 file. This file must be created before CM7 can be used to sign encryptor certificates.

The PKCS#12 file can be created by CM7 itself or sourced from an external CA.

To create an internal CA:

1. Open CM7 Settings and click **CA/Key Management**.
2. Configure the following fields:

Key Type

The key type used when signing certificates. Options include RSA-2048 and supported elliptic curves, including custom curves. The **Add Custom** button allows selection of user-defined elliptic curve types with predefined parameters. For details on defining custom elliptic curve parameters, see [Appendix C: Crypto-Agility — BYOC](#).

Serial Number

The initial serial number used on signed certificates.

CA Issuer Name

The distinguishing name fields that identify the CA. The validity indicator is green when all sub-fields are valid.



A different issuer name must be used for each CA that signs encryptors. Using the same name may cause the PKI process to locate the wrong certificate, resulting in authentication errors.

Validity Period

The date range over which the CA will be valid. Default: 15 years.

CA Password

The password required to sign certificates using this PKCS#12 file. Re-entry is required for confirmation.

3. Select the storage location:

- **CA File** — if using an INI file, specify the file location and name
- **CA** — if using a Configuration server database, select the server and database

4. Click **Create CA File** to generate and save the PKCS#12 file.

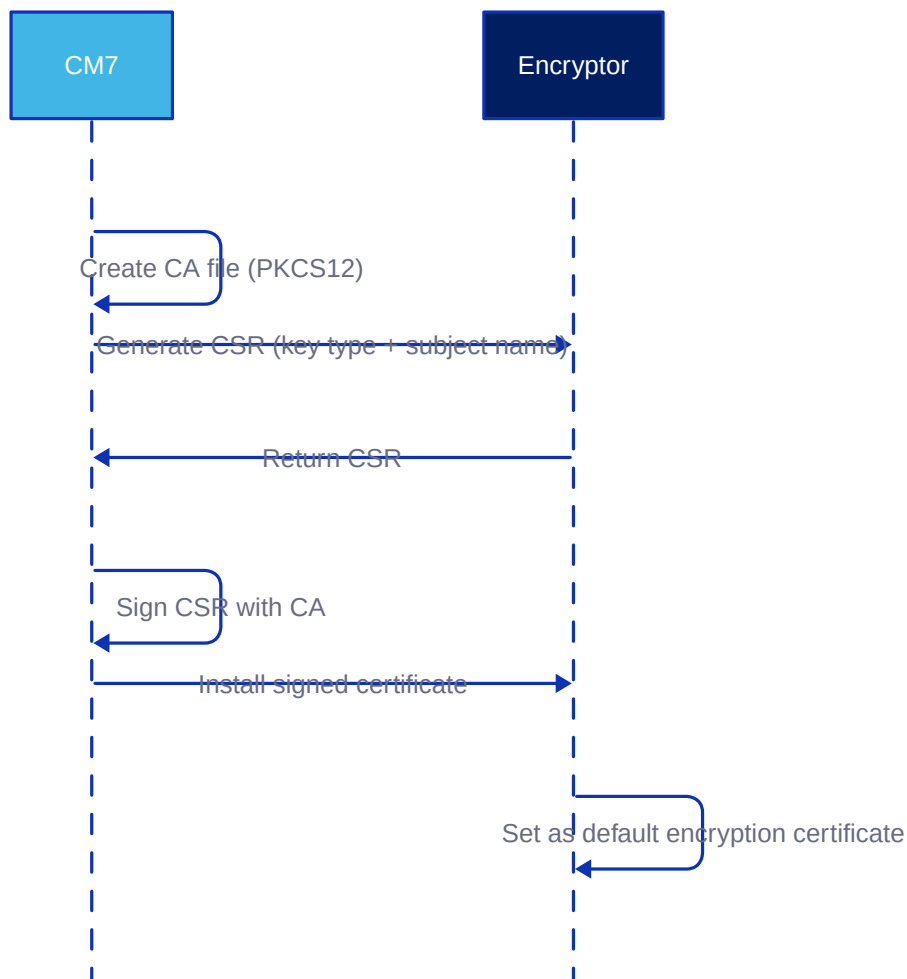


Figure 9. Certificate lifecycle

5.5.3. Certificate Hash Algorithms

The certificate signing algorithm determines the signature hash algorithm used.

Table 20. Certificate hash algorithms

X.509 Certificate Algorithm	Signature Hash Algorithm
RSA-2048	SHA-256
ECDSA-P256	SHA-256
ECDSA-P384	SHA-384
ECDSA-P521	SHA-512

5.5.4. Advanced CA Functions

The Advanced tab of the Certificate Authority screen provides functions for generating Certificate Signing Requests (CSRs), signing them, and saving the results.

CA/Key Management

Create New CA

Advanced

EC Parameters

Export CA Certs

KDK

Certificate Signing Request

☐ Import CSR:

☒ Generate From Key Type: RSA2048, RSA 2048bit

Add Custom

Distinguished Name

Attribute Name: C = country

Attribute Value: AU

Separator: .

Distinguished Name: C=AU,O=Organisation,CN=CommonName

Signing

☒ None

☐ Self-Signed

☐ Sign With:

Serial Number: c5:f0:55:73:00:00:00:00

Validity Period

Not Before: 2019-09-03 09:58

Not After: 2034-09-04 09:58

Save As

File: C:/Users/alan.williamson/Documents/cert1.pem

☒ Include Private Key

Create Certificate Signing Request

Close

Figure 10. Advanced CA functions

Certificate Signing Requests

A CSR can be imported from an existing file or generated using one of the predefined key types or a custom elliptic curve.

The predefined key types include:

- RSA2048 — RSA 2048-bit
- secp256k1 — SECG curve over a 256-bit prime field
- secp384r1 — NIST/SECG curve over a 384-bit prime field
- secp521r1 — NIST/SECG curve over a 521-bit prime field
- prime256v1 — X9.62/SECG curve over a 256-bit prime field
- sect283k1, sect283r1 — NIST/SECG curves over a 283-bit binary field
- sect409k1, sect409r1 — NIST/SECG curves over a 409-bit binary field
- sect571k1, sect571r1 — NIST/SECG curves over a 571-bit binary field
- c2pnb272w1 — X9.62 curve over a 272-bit binary field
- c2pnb304w1 — X9.62 curve over a 304-bit binary field
- c2tnb359v1 — X9.62 curve over a 359-bit binary field
- c2pnb368w1 — X9.62 curve over a 368-bit binary field
- c2tnb431r1 — X9.62 curve over a 431-bit binary field

Previously defined custom EC parameters can be added to the key type list using the **Add Custom** button.

Each CSR requires a **Distinguishing Name** with attributes that identify the certificate. For CSRs that define custom EC parameters, the Distinguishing Name must include:

- **Title** — must be **ECPARAM**
- **Name** — free-form identifier for the curve (e.g., "EC192 curve")
- **Description** — free-form description of the curve

Signing the CSR

The Signing panel allows the CSR to be:

- **Self-signed** — the CSR is signed by its own key
- **Signed using a PKCS#12 file** — the CSR is signed by a CA

If the PKCS#12 file is stored in an INI file, it is selected using the file browser dialog. If stored in a Configuration server database, the dialog allows selection from the available databases on the current server.

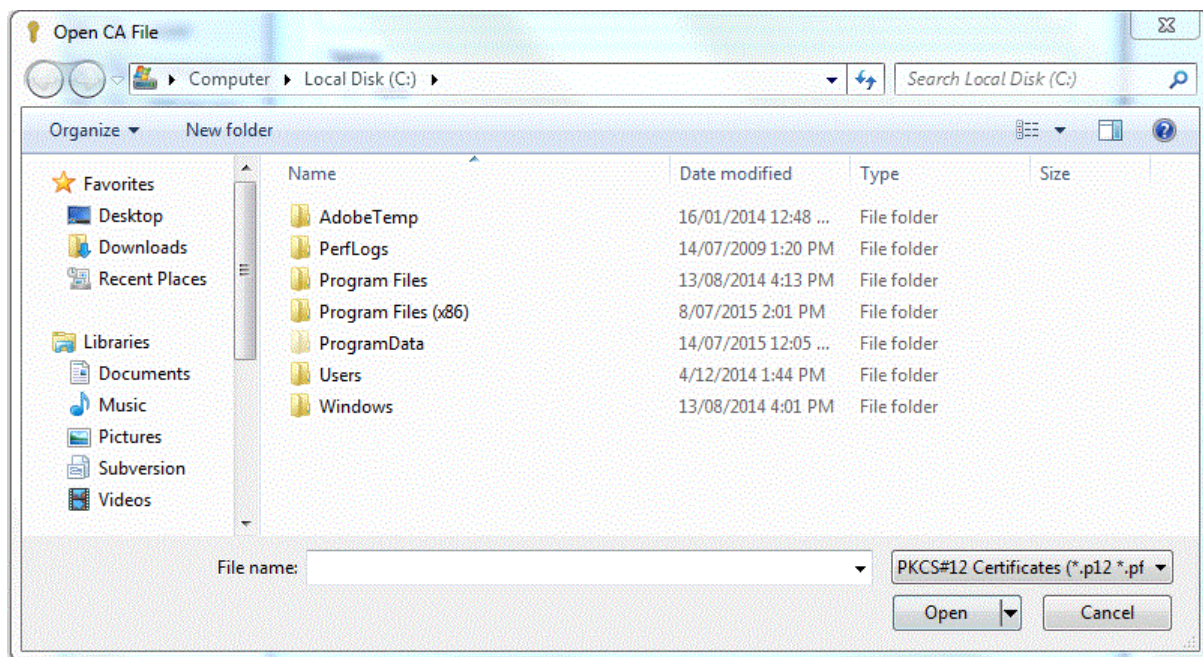


Figure 11. Selecting the PKCS#12 file

Saving the CSR

The **Save As** selector allows the CSR to be saved as either a PKCS#12 file or, for elliptic curve parameters, a **.PEM** file. For parameter files, saving the private key is not required.



Elliptic Curve Diffie-Hellman (ECDH) certificates can only be used when encrypting Ethernet traffic.

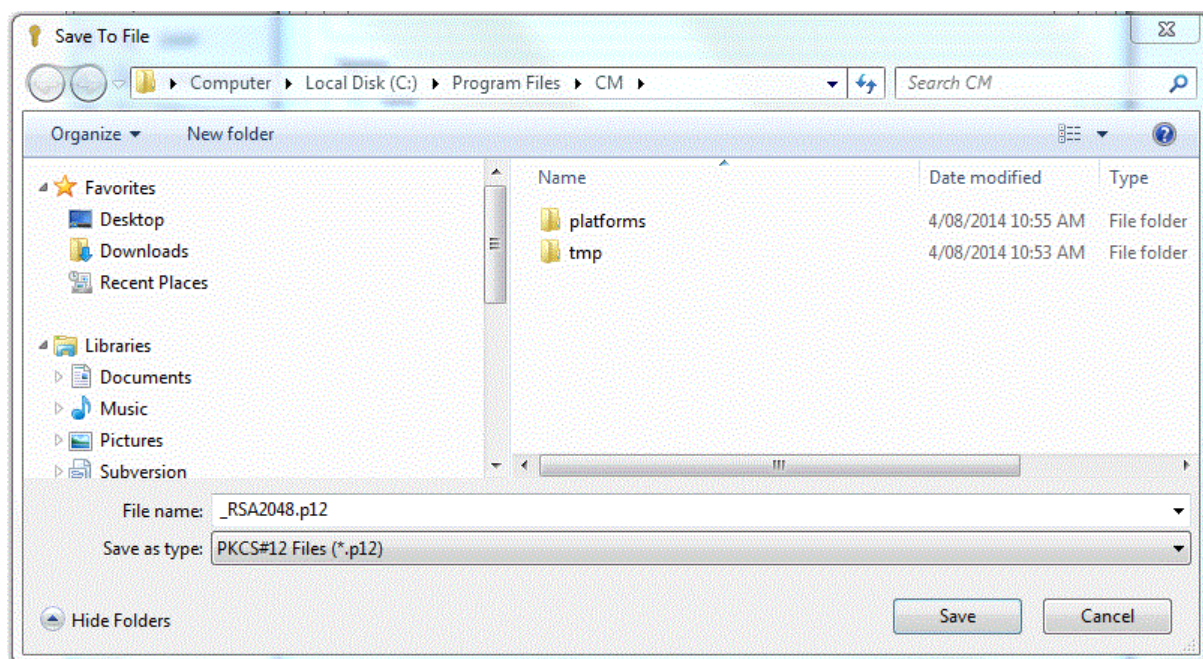


Figure 12. Save CSR dialog

Elliptic Curve Parameters

For encryptors to generate certificates using custom elliptic curves, curve parameters must be defined.

For the full EC Parameters workflow including curve data entry, validation, and PEM file generation, see [Appendix C: Crypto-Agility — BYOC](#).

5.5.5. Importing and Exporting CA Files

PKCS#12 files can be imported into or exported from Configuration server databases.

Import:

1. Select **Import CA File** and use the **Browse** button to locate the PKCS#12 file on the CM7 host file system.
2. Specify the **Import To CA Name** for the database entry.

Export:

1. Select **Export CA** and choose a database on the current server.
2. Specify the **Export To CA File** name and use **Browse** to select the target directory.

5.5.6. Installing Certificates

To establish trust between peer encryptors operating in Layer 2 modes (Line, TRANSEC, MAC, or VLAN), each encryptor must have an X.509 certificate signed by a common Certificate Authority (CA).

The encryptor must be activated before certificates can be loaded. Additionally, certificate management functions require a user account with **Administrator** privileges (the **Supervisor** role cannot load certificates).

Certificates can be signed and installed using the CM7 built-in (Internal) CA, or obtained from an External CA and installed via CM7 or the CLI.

Via CM7 Internal CA

This is the standard and most automated certificate installation method. It utilizes the PKCS#12 Certificate Authority file created or imported within CM7 (see [Creating the PKCS#12 File](#)).

To install a certificate using the CM7 Internal CA:

1. In the CM7 encryptor list, select the activated target encryptor.
2. Click the **Certify** button in the screen selector.
3. Select the **Internal CA** tab.
4. Enter the **CA Password** to unlock the PKCS#12 CA file.
5. Select the desired **Key Type** and **Key Size** (or elliptic curve) from the dropdown list.
6. Configure the **Distinguishing Name** (DN) fields to identify the encryptor (such as Country, Organization, Org Unit, and Common Name).
7. Click **Certify** to initiate the process.

CM7 automatically commands the encryptor to generate a key pair and a Certificate Signing

Request (CSR). CM7 then intercepts the CSR, signs it using the loaded Internal CA, and installs the resulting signed certificate back onto the encryptor.

8. In the Encryptor Tree, confirm that the encryptor's state transitions to **Certified**.

Via CM7 with an External CA

When your security policy requires certificates to be signed by an enterprise or third-party Certificate Authority, you can generate a CSR via CM7 and install the signed certificate returned by the CA.

To install a certificate via CM7 using an External CA:

1. In the CM7 encryptor list, select the activated target encryptor.
2. Click the **Certify** button in the screen selector.
3. Select the **External CA** tab.
4. Select the desired **Key Type** and specify the **Distinguishing Name** (DN) fields for the encryptor.
5. Click **Generate CSR**.

The encryptor generates its key pair and returns the CSR, which is displayed in the CM7 window.

6. Save the generated CSR to a file on your workstation.
7. Submit the CSR file to your external CA to be signed.
8. Once the signed X.509 certificate is returned by the CA (in PEM format):
 - a. Return to the CM7 **Certify** screen (or navigate to **Manage > Certificates**).
 - b. Click **Browse** or **Import PEM** and select the signed certificate file.
 - c. Click **Apply** or **Install** to load the signed certificate onto the encryptor.
9. Ensure the CA root (and any intermediate) certificates are also imported to the encryptor as **X509 CA** certificates to complete the trust chain.

Via CLI with an External CA

For headless or serial-only configurations, you can use the Command Line Interface (CLI) to configure the certificate parameters, generate the CSR, and install the signed certificate.

To install a certificate via the CLI using an External CA:

1. Establish a CLI session (serial console or SSH) and log in with an Administrator-level account.
2. (Optional) Set the desired CSR key algorithm and type:

```
encryptor> certificate -e <algorithm>
```

For example, to use SECG prime 256-bit elliptic curve: **certificate -e prime256v1**.

3. Set the Distinguished Name (DN) subject details for the CSR:


```
encryptor> certificate -s
```

This command starts an interactive prompt. Enter the country, organization, organizational unit, and common name when prompted.

4. Generate and print the CSR:

```
encryptor> certificate -r
```

The PEM-encoded CSR is printed to the terminal. Copy the entire block, including the **-----BEGIN CERTIFICATE REQUEST-----** and **-----END CERTIFICATE REQUEST-----** delimiters.

5. Submit the copied CSR block to your External CA to be signed.
6. Once the signed PEM-encoded certificate is returned by the CA, initiate installation:

```
encryptor> certificate -i
```

7. When prompted, paste the entire PEM-encoded signed certificate block into the CLI terminal.
8. Press **Enter**, and then press **Ctrl+D** on a new line to complete the installation and apply the changes.
9. Verify that the certificate has been successfully installed:

```
encryptor> certificate -p 3
```

Where **3** is the standard index for newly installed X.509 certificates.

5.5.7. Managing Installed Certificates

The CM7 Certificates screen displays the certificates currently installed on the encryptor.

The certificate list includes the following fields:

Table 21. Certificate list fields

Field	Description
ID	Index identifying the certificate. Index 1 is reserved for a (deprecated) V1 certificate, index 2 for a V2 certificate, and index 3 and above for X.509 certificates and EC parameter files. The default encryption certificate is flagged and highlighted green.
Type	Certificate type: X509 EN (Encryption), X509 CA (Certificate Authority), X509 OT (Other), or ECParm (custom elliptic curve parameters).
Identifier	A unique hash code derived from the certificate content.
PK Type	Key type used to sign the certificate: RSA, ECDH, or PQC.

Field	Description
PK Size	Length of the signing key.
Days Remaining	Number of days before the certificate expires.
Status	Current status: signed, unsigned, or expired.
Usage	Current utilisation: "in use" or "not in use". Not applicable when operating in TIM mode.
Signed By	The ID and hash of the CA certificate that signed this certificate. May show "self-signed" for CA certificates.

The certificate detail view shows:

- **Version** — 1, 2, or 3 (V1 and V2 are deprecated)
- **Serial Number** — assigned by the CA when the certificate was signed
- **Validity** — the date/time range within which the certificate is valid
- **Distinguishing Names** — issuer and subject details loaded by the CA

Setting Default Certificates

To set an encryption certificate as the default, select it and click **Set As Default**.



When hybrid certificates are used, **Set As Default** is replaced with two selectors: **Set Primary Default** and **Set Ancillary Default**. A default must be manually selected.

For details on how the default encryption certificate is used in encryption sessions, see [Chapter 6: Encryption Configuration](#).

Importing PEM Certificates

PEM certificates can be imported using the **Import PEM** button on the Certificates screen.

Deleting Certificates

Select a certificate and click **Delete** to remove it from the encryptor.



KeyVault and eQKD are unable to be used on host encryptors.

5.5.8. x509 Extensions

The CN4020 is aware of the following x509 extensions that streamline management of a fleet of devices or apply restrictions to meet the expectations of external services.

These can be selected ahead of certificate install when using CM7 Internal CA, or attached to a certificate when signing a CSR with an External CA.

Subject Alternative Name

When installed, it should have the value "IP:EncryptorIP".



This must be set for a certificate to be permitted to be used on the RESTful interface.

5.5.9. Certificate Servers (OCSP and CRL)

The Certificate Server configuration allows you to define the Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP) servers used to validate X.509 certificates. Up to 10 servers can be configured.



Certificate servers are only applicable to encryptors operating in LINE, MAC, or VLAN modes. Encryptors in Transport Independent Mode (TIM) use Sender IDs for key identification and do not use X.509 certificates. See [Encryption Configuration](#) for TIM key management details.

Check Period (in minutes)

The period between certificate validity checks. A value of 0 disables checking.

To configure servers:

1. Navigate to the **Certificate Servers** tab in CM7.
2. Add a server by specifying its URL, which must use an IP address (name resolution is not supported).

Example server entries

- OCSP: <https://192.168.0.1:443/ocsp/>
- CRL: <http://192.168.0.2/localFTP/crls/cert.crl>

Each entry has an **ID** (index used for CLI editing) and a **URL** (the server address).



To retrieve CRL updates over an HTTPS connection, the IP address and certificate to supply must be configured in the FTP Servers table.

The CRL is a list of revoked certificates. As the list grows, it can become large and inefficient to process. Each CRL entry specifies the server address and the path to the CRL file. The encryptor periodically downloads the CRL file at the configured check period interval.

Table 22. CRL server entry fields

Field	Description
ID	Index of the server entry, used when editing via the CLI.
URL	Full path to the CRL file, e.g. http://192.168.0.2/localFTP/crls/cert.crl .

OCSP provides a more efficient real-time validation mechanism and is the recommended method.



Neither CA certificates nor PQC certificates can be revoked via OCSP.

Configuration can also be performed via the CLI `ocsp` and `crl` commands.



It is recommended to use an FTP server for certificate revocation data, which must be entered in the FTP servers list on the encryptor with a matching certificate.

The OCSP server (responder) validates a certificate using its serial number and returns one of the following statuses:

- **good** — certificate is valid
- **revoked** — certificate has been revoked
- **unknown** — certificate status cannot be determined
- **unreachable** — the OCSP server cannot be contacted

5.5.10. Enhanced Certificate Security

OCSP Nonce

A nonce (number used once) can be included in OCSP requests to mitigate replay attacks. The nonce is a random or pseudo-random number that ensures each request is unique.

- **CLI:** `ocsp -n <y|n>`
- **Default:** disabled



A nonce can be applied in both Strict OCSP enabled and disabled modes.

Strict OCSP

Strict OCSP tightens the certificate validation mechanism. Under the standard OCSP model, **unknown** and **unreachable** responses can be treated as acceptable, which may allow potentially invalid certificates to pass validation undetected. Strict OCSP addresses this by requiring a **good** response — any other result, including **revoked**, **unknown**, or **unreachable**, causes a validation failure.

- **CLI:** `ocsp-s`
- **Default:** disabled

Prerequisites for enabling Strict OCSP:

- Only one OCSP server may be configured
- "Treat certificates with an unknown OCSP status as valid" must be disabled
- All OCSP settings must be configured prior to enabling Strict OCSP

To maintain a connection, you must always receive a **good** response from the OCSP server.

Recommended settings for maximum security:

- "Treat certificates with an unknown OCSP status as valid" disabled
- OCSP nonce enabled
- HTTPS configured for OCSP access
- Strict OCSP handling with retries enabled

OCSP Response Behaviour

The encryptor contacts OCSP servers periodically at the configured update interval. The behaviour for each possible response is:

Table 23. OCSP response behaviour

OCSP Response	Qualifier	Standard Action	Strict OCSP Enabled
GOOD	Previous response "GOOD"	No action	Same
GOOD	Certificate previously not "GOOD"	Relevant connections set to "UP" state	Same
REVOKED	Certificate previously "REVOKED"	No action	Same
REVOKED	Certificate not previously "REVOKED"	Relevant connections set to "FAULT" state	Same
UNKNOWN	"Treat unknown as valid" enabled	Treat as "GOOD"	Not applicable
UNKNOWN	"Treat unknown as valid" disabled	Treat as "REVOKED"	Same
UNKNOWN	Retry Limit = 0 (Strict OCSP)	Not applicable	Treat as "UNKNOWN"
UNKNOWN	Retry Limit > 0 (Strict OCSP)	Not applicable	Retry until limit reached or response received; if limit reached, treat as "UNKNOWN"

OCSP Response	Qualifier	Standard Action	Strict OCSP Enabled
UNREACHABLE	"Treat unknown as valid" enabled	Treat as "GOOD"	Not applicable
UNREACHABLE	"Treat unknown as valid" disabled	Treat as "REVOKED"	Same
UNREACHABLE	Retry Limit = 0 (Strict OCSP)	Not applicable	Treat as "UNREACHABLE"; connection set to "FAULT" state
UNREACHABLE	Retry Limit > 0 (Strict OCSP)	Not applicable	Retry until limit reached or response received; if limit reached, treat as "UNREACHABLE" and set to "FAULT" state

5.6. KDK Management



KDKs are only applicable when operating in Transport Independent Mode (TIM)

Each encryptor within a TIM network must share the same KDK. CM7 includes a build in KDK management system that can generate KDKs both from entropy sourced from the host running CM7 or an encryptor within the network.

5.6.1. KDK Creation

Method 1: CM7

The KDK functionality of CM7 is provided via the "CA/Key Management" window (accessed via "Settings"). Within this screen:

1. Navigate to the "KDK" tab.
2. Select either "Generate in CM7" or "Generate On An Encryptor".
3. Confirm the KDK File save location is appropriate.
4. Click "Create KDK File", and define a password to protect the file.

The KDK has now been created, and will auto-populate in the KDK field in the "Key" Screen in CM7.

5.6.2. KDK Installation

Method 1: CM7

1. Navigate to the "KDK" screen

2. Select the appropriate "KDK file", and enter the password.
3. If required, specify an "Install UTC Time"
4. Click "Add KDK"
5. Refresh the Encryptor Tree and confirm the KDK has been updated.

Method 2: CLI



Loading KDK via the console port is not permitted when an encryptor has FIPS mode enabled.

Use the `kdf` command to manage the installed KDK.

5.7. Syslog Configuration

The CN4020 supports forwarding audit and event logs to external syslog servers for centralised logging and correlation with other network devices.

5.7.1. Syslog Server Setup

An administrator can configure up to 10 syslog servers by specifying their IPv4 or IPv6 addresses.

Syslog messages use the standard non-secure RFC 5424 format with the following facility assignments:

- **LOCAL4** — audit log messages
- **LOCAL5** — event log messages

To configure syslog servers:

1. Navigate to the **Syslog Server Configuration** screen in CM7.
2. Add syslog server entries by specifying the **ID** and **IP Address**.

IP addresses are validated. DNS lookup is not supported.

Syslog servers can also be configured via the CLI.



When syslog is enabled, the use of NTP servers is recommended to ensure accurate timestamps on log entries. Both syslog and NTP are disabled by default and must be configured by an administrator.

If NTP is configured, it is assumed that both syslog and NTP servers exist within the same secure protected network and no additional security is required.

5.7.2. CM7 Syslog Service

CM7 includes a built-in syslog service that can receive syslog messages from encryptors.

Platform behaviour:

- **Windows:** The syslog service starts automatically on port 514 after CM7 installation and runs in the background regardless of whether CM7 is open.
- **Linux and macOS:** The syslog service must be started manually via the **CM Settings** dialog.

To receive syslog messages, add the IP address of the CM7 host to the syslog server table on each encryptor.

The syslog service can be started or stopped via:

- The operating system's Services management interface
- CM7 directly



If the service is started or stopped via CM7, CM7 must be run with administrative privileges.

Syslog Log Files

When syslog is enabled and the encryptor is logging to the CM7 syslog service, a text file is created with the prefix **CM7_Syslog**.

Log file locations:

- Windows: **C:\ProgramData\Senetas**
- macOS: **/home/<username>/.config/Senetas/**

Filename format:

- Current file: **CM7_Syslog<StartDateTime>.txt**
- Previous files: **CM7_Syslog<StartDateTime>--<EndDateTime>.txt**
- DateTime format: **yyyy-mm-dd_hhmmss**

A syslog file is not created until the first syslog message is received from the encryptor.

Logging Interval

CM7 writes syslog messages to a new file at a configurable interval.

- **Default:** 7 days
- **Range:** 1–24 days

When logged in as an administrator, modifying the syslog file interval restarts the CM7 syslog service and applies the new interval immediately.

When logged in as a non-administrator, the updated interval does not take effect until the current period concludes.

Export and Delete Syslog

Export Syslog: Use the **Export Syslog** button in CM7 Settings to export the current syslog file. If no file exists, the message "Syslog is empty - nothing to export." is displayed.

Delete Syslog: Use the **Delete Syslog** button to delete the current syslog file. If no file exists, the message "Syslog is empty - nothing to delete." is displayed.



The Export/Delete Syslog buttons apply only to the currently active syslog file, not files from previous periods.

If the syslog file is deleted mid-period, CM7 continues writing to the pre-existing period endpoint. For example, if 6 days have elapsed during a 7-day interval and the file is deleted, the newly created file will only be active for 1 day.

5.7.3. Syslog over SSH

Syslog messages can be tunnelled via an SSH tunnel if required. This can be done as follows:



Whilst the port numbers can be changed, matching port numbers must be maintained.

- **Encryptor Configuration**

1. Enable SSH CLI and record the configured port number (i.e 2222)
2. Copy the Syslog Server's ECDSA SSH key onto the CN4020's SSH CLI table
3. Enable "Syslog over SSH"
4. Add an entry into the Syslog Server's table of **127.0.0.1:9100**

- **Syslog Server configuration**

1. Configure a .conf file including the following:

```
module(load="imtcp")
input(type="imtcp" port="9123")
```

2. Restart the syslog service
3. Create a reverse SSH tunnel using the following command (Linux) **ssh -fN -p 2222 -R 9100:<ServerIP>:9123 cli@<EncryptorIP>**

5.8. Remote Access

The CN4020 supports remote management via SSH in addition to the local serial CLI and CM7.

5.8.1. Remote SSH CLI Access

The CLI is accessible via a remote Secure Shell (SSH) connection, providing management functions equivalent to those available via CM7.

- **Default state:** SSH is disabled
- **Maximum concurrent sessions:** 10
- **Key type:** Only ECDSA keypairs are valid for SSH use

SSH must be enabled using the CM7 interface or the local (physical) CLI before remote connections can be established.

Remote SSH access facilitates:

- Remote scripting for device configuration and certification
- Verification of current configuration status
- General health monitoring

5.8.2. SSH Key Pair Creation

An SSH public/private key pair is required for authentication. The key pair is generated using the Remote CLI pane in CM7.

To create an SSH key pair and enable remote CLI access:

1. Open CM7, connect to the encryptor, and navigate to the **Remote CLI** pane.
2. Enable **Remote CLI Access** and verify the port is set to 22.
3. Click the **Remote CLI** button at the bottom of the interface. A Remote CLI Key Generation dialog is displayed.
4. Click **Generate Key**.
5. Enter and confirm a password for the key.
6. Click **OK**. A public key is generated and saved.
7. Click **OK** again. A terminal session window is displayed, from which you can log in to the encryptor.



The Remote CLI in CM7 includes a full terminal emulator with enhanced capabilities.

5.8.3. SSH Access of Remote Devices

Encryptors with an Auxiliary LAN port (a second physical RJ45 management port) support tertiary SSH access to remote devices via the local CLI, SSH CLI, or CM7 Remote CLI.

To enable SSH access of remote devices:

1. Enable Auxiliary Management mode:

CLI: `ip-aenabled`

2. Configure the AUX IP management port:

CLI: `ip-s<index><ipaddress/mask><gateway>`

3. Enable the AUX port:

CLI: `ip-e<index>`



The auxiliary management IP interface must be on the same subnet as the third-party device.

The `sshaux` CLI command displays the default user, default IP address, and the public SSH key of the encryptor. This key can be pasted into the `authorized_keys` file on the remote device for public key authentication without PAM access.

Connection options:

- `sshaux-c` — connect using public key authentication
- `sshaux-p` — enforce PAM (username/password) login
- `sshaux-suser@<IPv4addr|IPv6addr>[:port]` — modify the default user and address

If no user and address is provided with the `-c` or `-p` options, the default values are used.



Due to FIPS certification requirements, only EC key exchange algorithms are supported.

5.9. Additional Management Services

5.9.1. NTP Configuration

NTP allows for time synchronisation across a network, ensuring that all logging and events report based on a shared reference.

The CN4020 can have up to 10 NTP servers listed.

NTP servers are added via the "Date/Time" panel in CM7, or via the `ntpcfg` CLI command. The current status of the ntp connections is only reported via CLI.

5.9.2. TACACS+ Authentication

TACACS+ is an open standard for remote Authentication, Authorisation, and Accounting (AAA) services. It provides centralised management of encryptors with password change available from CM7 and the CLI.



The TACACS+ implementation uses the MD5 hashing algorithm. When TACACS+ is enabled, the encryptor is no longer FIPS 140-3 compliant. Enabling the protocol provides clear guidance that an unsupported FIPS 140-3 feature is in use.

The TACACS+ configuration fields are:

TACACS+ Operations

Enable or disable global TACACS+ operation.

Auditing Message Broadcast

Enable or disable broadcasting of auditing messages to all TACACS+ servers. When disabled (default), messages are sent only to the active server that provided authentication/authorisation.

Ticket Request User

The predefined user name used by CM7 to send ticket requests to the TACACS+ server.

Ticket Request Password

The password used to verify the TACACS+ connection based on the CM7-supplied ticket request password.

The lower section of the configuration screen allows adding, editing, and deleting TACACS+ servers by IP address.

TACACS+ User Level Mapping

Table 24. TACACS+ user level mapping

TACACS+ User Level	CN4020 User Identifier
15	Administrator
10	Supervisor
5	Operator
3	Upgrader

5.9.3. FTP/FTPS Server Configuration

CM7 includes a built-in FTP server for encryptor firmware upgrades. Both FTP and FTPS protocols are supported.



Where remote encryptors need to be upgraded, the FTPS protocol should be used to provide a secure connection.

The configuration fields include:

- **Restrict to FTP Servers** — when enabled, FTP requests to IP addresses not defined in the encryptor's FTP server table are rejected
- **ID** — numeric index of the configured server
- **IP Address** — the IP address of the FTP/FTPS server
- **Certificate** — the certificate used for FTPS authentication

To configure an FTPS server, an FTP server key and certificate must be created and stored in a password-protected **.p12** file. Click the **New** button next to the **Private Key** field to create the key and

certificate. When upgrades are initiated, the FTP server certificate is extracted from the .p12 file and added to the FTP server table on the target encryptors.

Caveats:

- Certificates cannot be installed prior to activation — FTP connections must be used for unactivated encryptors
- A user with Upgrader privilege may only use FTP (not FTPS) connections
- For an Upgrader to use FTPS, an administrator must have previously installed the required certificate
- Multi-slot encryptors do not support certificate installation and therefore cannot use FTP over TLS
- Firmware version 5.x.x and higher require EC FTP certificates

For firmware upgrade procedures, see [Chapter 9: Maintenance](#).

5.9.4. RESTful JSON Interface

A RESTful HTTP(s) interface is provided for remote monitoring and issue detection. The interface leverages the existing SNMP MIB, allowing queries using OID textual representations within URL parameters.

Access is controlled via user console access rights — the user must be authorised.

Configuration

The RESTful interface can be configured using:

- **CLI:** `rest` command
- **CM7:** Right-click a control and save OIDs to the clipboard for use in RESTful queries

Monitoring Examples

The RESTful interface supports the following monitoring use cases:

- **Alarm monitoring** — query the AlarmGroup OID to show the status of encryptor alarms
- **Certificate monitoring** — monitor CertificateState and CertificateDaysLeft
- **Audit and event log monitoring** — query audit and event log entries (centralised syslog is the preferred option; the RESTful interface is an alternative)
- **Connection status** — query connection tables specific to the operational mode (e.g., VLAN mode connections)
- **Interface status** — examine the status of network links

For interpretation of monitoring data, see [Chapter 8: Monitoring](#).

5.9.5. Third-Party Managers

An existing SNMPv3 manager can be used to manage and monitor encryptors. Senetas provides copies of the MIBs that define the SNMPv3 traffic used by encryptors.

Integration of MIBs allows both monitoring and control of units via the secure SNMPv3 management port.

SNMPv1 can also be used for read-only monitoring where SNMPv1 access has been granted to individual user accounts.

5.9.6. CipherTrust Integration

The SafeNet CipherTrust platform provides centralized key management and cryptographic protection for CN4020 devices. CM7 can configure CipherTrust servers to support two distinct integration methods: Key Provisioning (via KMIP) and System Masterkey Splitting (KeySecure).

Up to 10 servers (tied to tiers) can be configured.

The configuration fields are:

CipherTrust

Enable or disable key provision.

Owner Name

The name of the client account within the CipherTrust system.

Password

The password for the account.

Key Provisioning (KMIP)

CM7 can configure the encryptor to obtain data plane encryption keys (DEKs) directly from a CipherTrust key server using the Key Management Interoperability Protocol (KMIP).



When the CipherTrust server is used for KMIP key provisioning, the encryptor is dependent on the server to establish encrypted tunnels. If the CipherTrust server becomes unreachable, data plane encryption keys cannot be retrieved, and secure connections cannot be established or rotated.

System Masterkey Splitting (KeySecure)

To enhance physical security, the encryptor's System Masterkey can be split between the local encryptor hardware and the CipherTrust server. When enabled, a portion of the masterkey resides on the CipherTrust server, requiring a secure connection to the server to reconstruct the masterkey on startup.



Enabling System Masterkey Splitting creates an absolute startup dependency on the CipherTrust infrastructure. If the CipherTrust server cannot be contacted during

startup (for example, due to network outages, routing failures, or server downtime), the encryptor will be completely unable to complete its boot process or initialize its encryption engines. Use this feature only when a highly resilient, redundant path to the CipherTrust server is guaranteed.

CipherTrust Tiers

The CipherTrust platform provides a multi-tier load balancing feature with up to three levels of load balancing groups (tiers). When one tier is unreachable, the system fails over to the next tier.



Tiers must be configured in order — tier 3 cannot exist without tier 1 and tier 2, unless a global tier without a suffix is provided.

Table 25. CipherTrust tier fields

Field	Description
ID	Server identifier.
Tier	The tier number used to access the configuration.
Port	The port number.
Protocol	The connection protocol: ssl (authenticated, recommended) or tcp (unauthenticated).
Pool	The communications pool size.
Read Timeout	Read timeout value.
Idle Timeout	Idle timeout value.
Retry Interval	Retry interval value.
Certificate	The identifier of the certificate used to authenticate the connection.

Chapter 6. Network Configuration

6.1. Network Configuration

This chapter describes how to configure the network interfaces and management connectivity of the CN4020. It covers management interface addressing, data port connections, pluggable hardware modules, and management network topologies.

For initial setup and commissioning, see [Chapter 3: Getting Started](#). For encryption policy and connection mode configuration, see [Chapter 6: Encryption Configuration](#).

6.1.1. Encryptor Connections

The CN4020 has connectors that source power, connect to CM7 or another management system, and connect to the local (protected) and the remote (unprotected) networks.

6.1.2. Management Network

The management interface provides out-of-band access to the CN4020 for configuration and monitoring. The CN4020 can be managed via the RJ45 management port (using SNMPv3), the serial console port (using CLI commands), or in-band (using SNMPv3). When enabled, the auxiliary port allows management by an additional management system.

SNMPv3 sessions use the UDP protocol to ensure reliable operation in noise-prone environments.

For a description of management tools and access methods, see [Chapter 5: Management](#).

Management Interface Configuration

The management port supports IPv4 and IPv6 addressing. Configure the following settings via CM7 or the CLI `ip` command:

Table 26. Management interface settings

Setting	Description
IP Address	Management interface IP address in CIDR notation.
Prefix / Subnet Mask	Network mask that applies to the management IP address.
Gateway	Default gateway for management traffic.
Status	Set to <i>Enabled</i> or <i>Disabled</i> to control access via this address.

In CM7, navigate to the **Network Addresses** section of the Manage screen to configure these settings. Select the required field, enter the new value, and click **Apply**.

The Network Addresses display shows the following sections:

- **Inband Management Gateway** — when enabled, the encryptor operates as an inband gateway for managing remote encryptors

- **Front Panel Main Port** — the physical (MAC) address of the primary management port



Address changes take effect immediately; there is no need to restart the CN4020.

Management Port Statistics

The following statistics are available for the management port via CM7 or the CLI.

Table 27. Management port — Ethernet statistics

Statistic	Description
MAC Address	MAC address of the management port.
Operating Mode	Current operating mode of the CN4020.
Current Link Rate	Actual negotiated link speed.
Configured Link Rate	User-specified speed negotiation setting.
Partner Link Rate	Link rate of the connected management device.

Table 28. Management port — IP statistics

Statistic	Description
Packets In	Number of IP packets received.
Packets Out	Number of IP packets sent.
Header Errors	Number of IP packets with header errors.
Address Errors	Number of IP packets with address errors.
Discards	Number of IP packets discarded.

Table 29. Management port — ICMP statistics

Statistic	Description
Messages In	ICMP messages received on the management port.
Messages Out	ICMP messages sent by the management port.
Errors	Errors detected in ICMP messages.

Table 30. Management port — UDP statistics

Statistic	Description
Datagrams In	Number of UDP datagrams received.
Datagrams Out	Number of UDP datagrams sent.
Errors	Number of errors in UDP datagrams.

For additional monitoring and diagnostics, see [Chapter 8: Monitoring](#).

6.1.3. Data Interfaces

The CN4020 is inserted into the network as a "bump in the wire." Traffic in both directions is encrypted according to the defined encryption policy.

Local port

Connected to the trusted (protected) network. The local side of the CN4020 typically connects to equipment in close proximity.

Network port

Connected to the untrusted (unprotected) network. The network side may need to support longer distances, depending on the physical media.

Transceiver Compatibility

The physical media at each port determines the required transceiver type. The CN4020 supports copper and optical transceivers in the following categories:

- **Copper (RJ45)** — for distances up to approximately 100 metres
- **Multi-mode fibre** — for short to medium distances
- **Single-mode fibre** — for longer distances

The supported reach depends on the fibre mode, wavelength, and installation environment.



The specified reach of each transceiver assumes a standard installation using OM2 and/or OM3 fibre. Consult your network provider for site-specific guidance.

For the list of supported transceivers and vendor part numbers, refer to the model-specific specification page.

The data ports accept SFP or SFP+ transceivers.



Clean both the fibre connectors and the transceiver interfaces before insertion if they have been exposed to the environment.

Interface Settings

The management port is auto-sensing and uses auto-negotiation to determine the fastest available link speed. The port attempts to connect at 1000 Mbps first, then falls back to 100 Mbps and 10 Mbps until a stable connection is established.

The following interface settings can be configured:

- **Speed/Duplex** — auto-negotiate (default) or set manually
- **MTU** — maximum transmission unit (default: 1500; increase for jumbo frames if required)

- **Link monitoring** — monitor interface link state for operational status

Local Port Statistics

The following statistics are available for the local port via CM7 or the CLI.

Table 31. Local port — Rx statistics

Statistic	Description
Buffer Overflow Count	Frames received on the local port and discarded due to internal buffer overflow.
Interframe Gap Errors	Frames received after a minimum interframe gap violation.
Octet Count	Total characters received.
Frame Count	Total frames received.
FCS Errored Frames	Received frames with Frame Check Sequence errors.
PCS Errored Frames	Received frames with Physical Coding Sublayer data errors.
Undersized Frames	Received frames shorter than 64 bytes.
Oversized Frames	Received frames longer than 1536 bytes.
Discarded Frames	Received frames discarded due to policy settings.
Bypassed Frames	Received frames that were bypassed (not encrypted).
PCS Sync State	Current state of local port communications.

Table 32. Local port — Tx statistics

Statistic	Description
Octet Count	Total characters sent.
Frame Count	Total frames sent.
FCS Errored Frames	Sent frames with Frame Check Sequence errors.

Network Port Statistics

The following statistics are available for the network port via CM7 or the CLI.

Table 33. Network port — Rx statistics

Statistic	Description
Buffer Overflow Count	Frames received on the network port and discarded due to internal buffer overflow.
Interframe Gap Errors	Frames received after a minimum interframe gap violation.
Octet Count	Total characters received.

Statistic	Description
Frame Count	Total frames received.
FCS Errored Frames	Received frames with Frame Check Sequence errors.
PCS Errored Frames	Received frames with Physical Coding Sublayer data errors.
Undersized Frames	Received frames shorter than 64 bytes.
Oversized Frames	Received frames longer than 1536 bytes.
Discarded Frames	Received frames discarded due to policy settings.
PCS Sync State	Current state of network communications.
Manage Octet Count	Management characters received.
Manage Frame Count	Management frames received.
Manage Drop Frames	Management frames dropped due to internal processing.
Shim Octet Count	Crypto excess octets (shim and authentication trailer) for each encrypted or decrypted frame.
Replay Errors	Frames where the counter in the shim has been observed before.
Skipped CTR Errors	Frames where the counter in the shim is greater than the expected value at the receiver.
Auth Failed Errors	Authentication failures.
Reordered Frames	Frames where the counter in the shim is less than the previous greatest received value.
Out of Reorder Window Frames	Frames where the counter value falls outside the reorder window (more than 256 behind the previous greatest value).
Encrypted Octets	Total encrypted octets.
Encrypted Frames	Total encrypted frames.

Table 34. Network port — Tx statistics

Statistic	Description
Octet Count	Total characters sent.
Frame Count	Total frames sent.
FCS Errored Frames	Sent frames with Frame Check Sequence errors.
Manage Octet Count	Management characters sent.
Manage Frame Count	Management frames sent.

For guidance on interpreting port statistics, see [Chapter 8: Monitoring](#).

6.1.4. Management Topologies

The CN4020 supports several management connectivity models. The appropriate topology depends on whether the encryptors are co-located, remotely accessible via a dedicated management network, or reachable only through the encrypted data network.

Direct Connection (Front Panel)

A direct connection from the CM7 host to the RJ45 management port on the front panel is the simplest method of managing an encryptor. This requires a common subnet between the CM7 host and the management port.

Switches are commonly used to connect to and manage multiple units from a single CM7 instance.

This method is suitable for:

- Local connections in data centres
- Test setups used to configure units prior to deployment

The CM7 host must be able to reach the front panel IP address of each CN4020.

Out-of-Band Management

If the CN4020 is in a different location, SNMPv3 management traffic can be routed via a Layer 3 network to the management port. Because SNMPv3 traffic is encrypted, the connection is secure without additional protection.

Out-of-band management is the recommended method for managing remote encryptors when a dedicated management network is available.

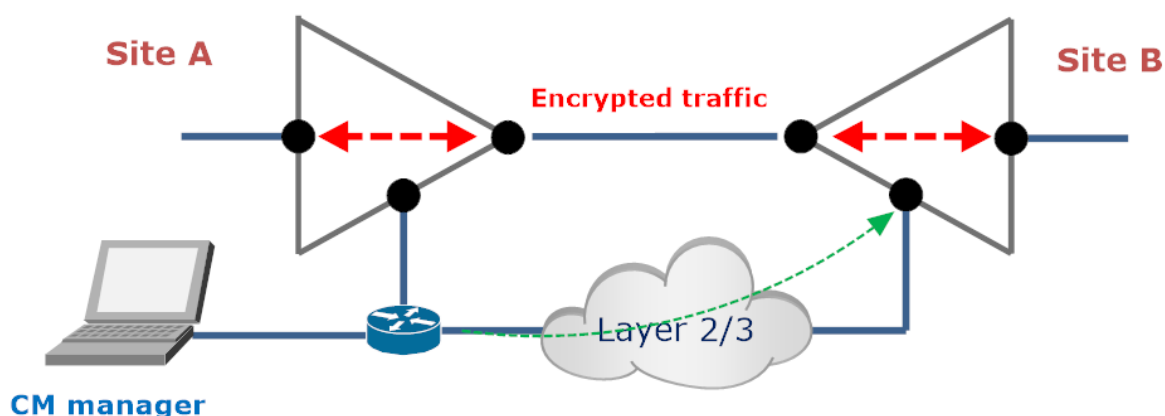


Figure 13. Out-of-band management

In-Band Management

In-band management allows remote encryptors to be managed over the same network that the encryptors secure. One local encryptor is configured as a management gateway that forwards management traffic to remote peer encryptors.



In-band management does not apply to encryptors operating in Transport

Independent Mode (TIM). For TIM mode management, see [Virtual Management \(TIM Mode\)](#).

Concept

The gateway encryptor connects between the CM7 host and the remote encryptors. Management IP packets are sent from the CM7 host to the front panel of the gateway encryptor, which forwards them over the network to the remote device(s).

Each remote encryptor is assigned a virtual IP address so that CM7 can discover and manage it. The virtual IP addresses are used only by the gateway encryptor and do not exist on any physical network.



Only one encryptor can act as the gateway encryptor.

When acting as a gateway on non-Ethernet configurations, the encryptor resolves IP destination addresses to network connections. For unknown destinations, the gateway encryptor performs a broadcast to other encryptors in the network to resolve the address (similar to ARP on an Ethernet network).

In-band management is protocol-independent and can be used with both Ethernet and non-Ethernet encryptors.

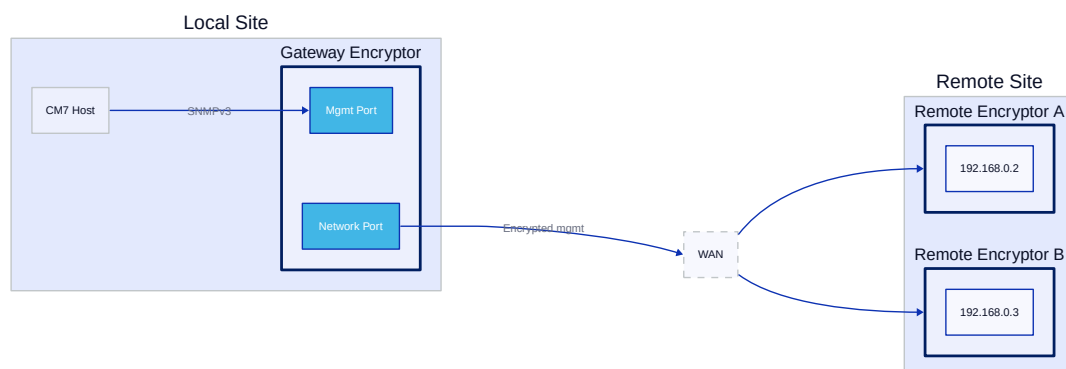


Figure 14. In-band management architecture

Inband Addressing

Where in-band management is used, the gateway encryptor routes traffic addressed to a remote encryptor via its network port. Each remote encryptor routes the SNMPv3 response back via the network to the gateway encryptor and then to CM7.



The protocol of the encrypted link may not be Ethernet, but from a management perspective it is treated as if it is.

Inband Configuration

In-band management is enabled and configured from the CLI `ip` command or from CM7.

The following settings are configurable via the CLI **ip** command:

- Management IPv4 address, mask, and gateway
- Management IPv6 address, mask, and gateway
- Inband management IPv4 and IPv6 addresses
- Inband gateway function (enable or disable)
- Management port settings (auto-negotiate, speed, duplex)
- Inband VLAN tag (Ethernet line mode only)

To configure in-band management via CM7, navigate to the **Network Addresses** section of the Manage screen and enable the **Inband Management Gateway** option.

The following rules must be observed when configuring in-band management for remote encryptors:

1. All inband management virtual IP addresses must be on the same subnet as the inband IP address of the gateway encryptor. Only IP packets belonging to this subnet are forwarded from the front panel to the network encryption port.
2. The CM7 host must have a static route added to ensure that inband packets are routed to the front panel of the gateway encryptor.

For example, on a Windows host:

```
ROUTE ADD 192.168.0.0 MASK 255.255.255.0 10.0.0.1
```



The **ROUTE ADD** command may require elevated privileges. Use the **-p** switch to make the route persistent across reboots.

3. On each remote encryptor, ensure that the default gateway and inband gateway both point to the inband IP address of the gateway encryptor.
4. Ensure that network masks are set correctly for both the management Ethernet port and inband addresses.
5. Ensure that the **Management Gateway** function is enabled on the gateway encryptor via the CM7 **Network Addresses** pane.
6. If a remote (non-gateway) encryptor has firmware earlier than v5.0, disable its front panel to prevent routing loops.



When upgrading an encryptor over inband management, the file transfer may take longer than five minutes.

The following tables show example address configurations for gateway and managed encryptors.

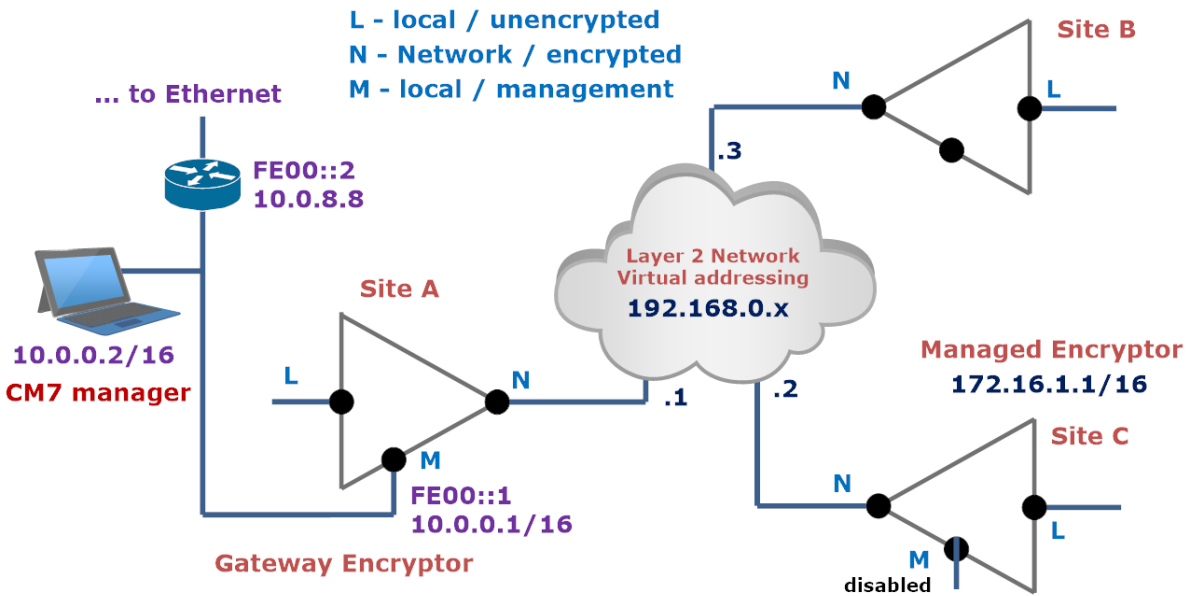


Figure 15. Inband management configuration example

Table 35. Example — Gateway encryptor settings

Index	Connect via	Enabled	IP Address	Gateway
1	IPv4 Front Panel	Yes	10.0.0.1/16	10.0.0.8
2	IPv6 Front Panel	Yes	FE00::1	FE00::2
3	IPv4 Inband	Yes	192.168.0.1/24	0.0.0.0
4	IPv6 Inband	Yes	FE01::1	00::0

Table 36. Example — Managed (remote) encryptor settings

Index	Connect via	Enabled	IP Address	Gateway
1	IPv4 Front Panel	No	172.16.1.1/16	172.16.1.254
2	IPv6 Front Panel	No		
3	IPv4 Inband	Yes	192.168.0.2/24	192.168.0.1
4	IPv6 Inband	Yes	FE01::2	FE01::1

The gateway encryptor does not respond to ARP requests for its inband IP address or any known remote encryptor inband IP addresses. It responds only to ARP requests for its local (front panel) IP address.

Routing Considerations

All management traffic uses SNMPv3 over UDP port 161.

Each CN4020 has a configurable front panel Ethernet address that can be defined using IPv4 and/or IPv6. Management traffic is routable; as a general rule, the accessibility of an encryptor can be determined by pinging its management address.

If the management traffic is routed to the front panel of the gateway encryptor, the intermediate router may also require a static route.

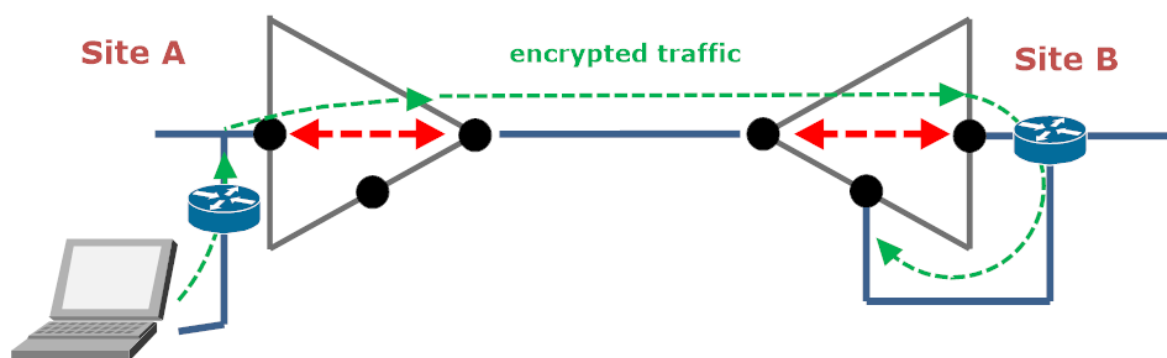
In-Line Management

In-line management inserts management traffic into the encrypted data stream and connects it back to the front panel of the remote encryptor(s).



In-line management is **not recommended** because the operational state of the encryptors can impact management connectivity.

The alternative "in-line bypass" mode can be used for encryptors located within Shortest Path Bridging (SPB) networks.



CM manager

Figure 16. In-line management

Virtual Management (TIM Mode)

Virtual management allows encryptors operating in TIM mode to be managed via the local or network interface.

The encryptor captures incoming management packets before they reach the encryption engine; this applies to packets arriving at both the local and network ports. No IP rules on the encryptor being managed are required for virtual management.



Virtual management traffic must be bypassed through local encryptors with IP Rules if being used to manage remote encryptors from the local LAN.

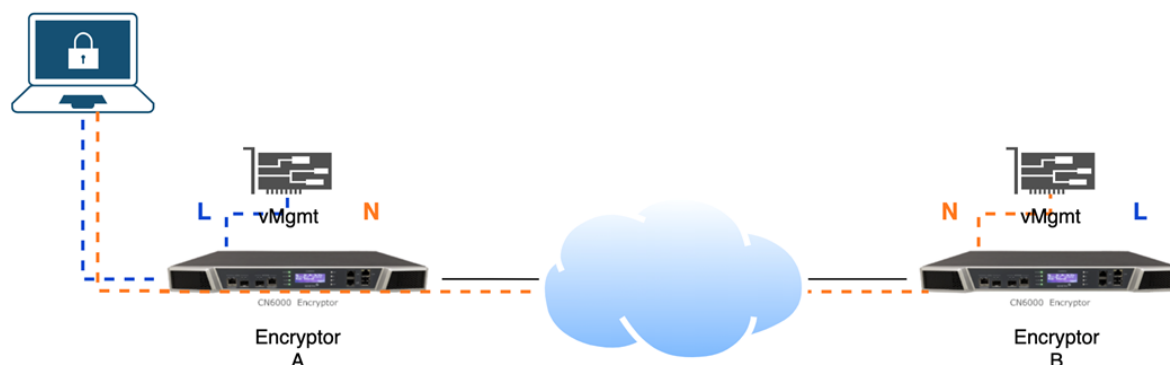


Figure 17. Virtual management

Caveats:

- Enabling or disabling virtual management reboots the CN4020.
- Virtual management configuration is persistent across all reboots and erases, except for a factory erase (**erase-f**).
- Virtual management does not support IPv6 addresses.

Virtual management can be enabled using:

- CM7 — via the **Network Addresses** section of the Manage screen
- CLI — using the **ip-v** command
- SNMP — using the equivalent OID



Virtual management is visible and configurable in all connection modes, but it is only functional in TIM mode.



When virtual management is enabled, front panel management is disabled.

6.1.5. Network Addressing (CM7)

The CM7 **Network Addresses** screen provides a consolidated view of all management addresses configured on the CN4020.

Front Panel Addresses

The front panel can be assigned both IPv4 and IPv6 addresses for the primary and auxiliary management ports.

Table 37. Network address fields

Field	Description
Address	The IP address of the CN4020 in CIDR notation.
Prefix	The network mask that applies to the IP address.

Field	Description
Gateway	The gateway address for management traffic.
Status	Set to <i>Enabled</i> or <i>Disabled</i> to allow access via this address.

Inband Addresses

When in-band management is configured, IPv4 and IPv6 inband addresses are displayed alongside the front panel addresses. Each address can be edited by selecting the required field, entering the new value, and clicking **Apply**.

For in-band configuration procedures, see [Inband Configuration](#).

Inband VLAN Configuration

The inband VLAN section allows a VLAN ID to be specified for inband management. This is required where encryptors are remotely managed within a VLAN environment.



Inband management within VLAN (VPLS) networks requires at least one VLAN entry. An untagged entry exists by default; additional entries may be required depending on the network topology.

Refer to the CLI `inband_vlan` command for configuration details.

Chapter 7. Encryption Configuration

7.1. Encryption Configuration

This chapter describes how to configure encryption on the CN4020. It covers encryption mode selection, and configuration points that are shared across all encryption modes.

For conceptual descriptions of encryption modes, connection modes, and cryptographic modes, see [Chapter 2: Product Overview](#).

7.1.1. Selecting an Encryption Mode

The CN4020 supports the following encryption modes:

Ethernet Mode (Layer 2)

Encrypts Ethernet frame payloads at Layer 2. Supports four connection modes: Point-to-Point (Line), TRANSEC, MAC multipoint, and VLAN multipoint. Suitable for dedicated links, dark fibre, and switched Ethernet networks.

Transport Independent Mode (TIM)

Encrypts traffic at layers 2, 3, and 4 of the OSI model. Decouples encryption from the underlying transport, enabling encryption across MPLS, Carrier Ethernet, and dark fibre networks. Uses an extensible key provider model (KDF or KMIP) for key generation.

The encryption mode is configured using the CM7 Policy tab or the CLI `con` command.



The connection modes available depend on the encryptor model and firmware version. Refer to the model-specific documentation for details.

7.1.2. Connection Mode Selection

Prior to configuring the connection mode, review the network and security requirements:

- Where only two sites are connected or a dark fibre link exists, **Point-to-Point** provides a simple Layer 2 encryption solution.
- Point-to-Point mode uses a single key for all unicast and multicast traffic; cryptographic separation is not provided.
- If expansion beyond two sites is expected, a multipoint mode avoids reconfiguration of existing encryptors when adding new sites.
- **VLAN multipoint** supports QoS services and offers increased scalability. VLAN-based policies support inclusion and exclusion of specific VLANs. Senetas recommends VLAN mode as the default multipoint deployment.
- **MAC multipoint** is appropriate where cryptographic separation of Layer 2 traffic between sites is required. MAC-based policies support inclusion and exclusion of specific network endpoints.
- **TIM** allows encryption of Layer 2, 3, and 4 Ethernet traffic.

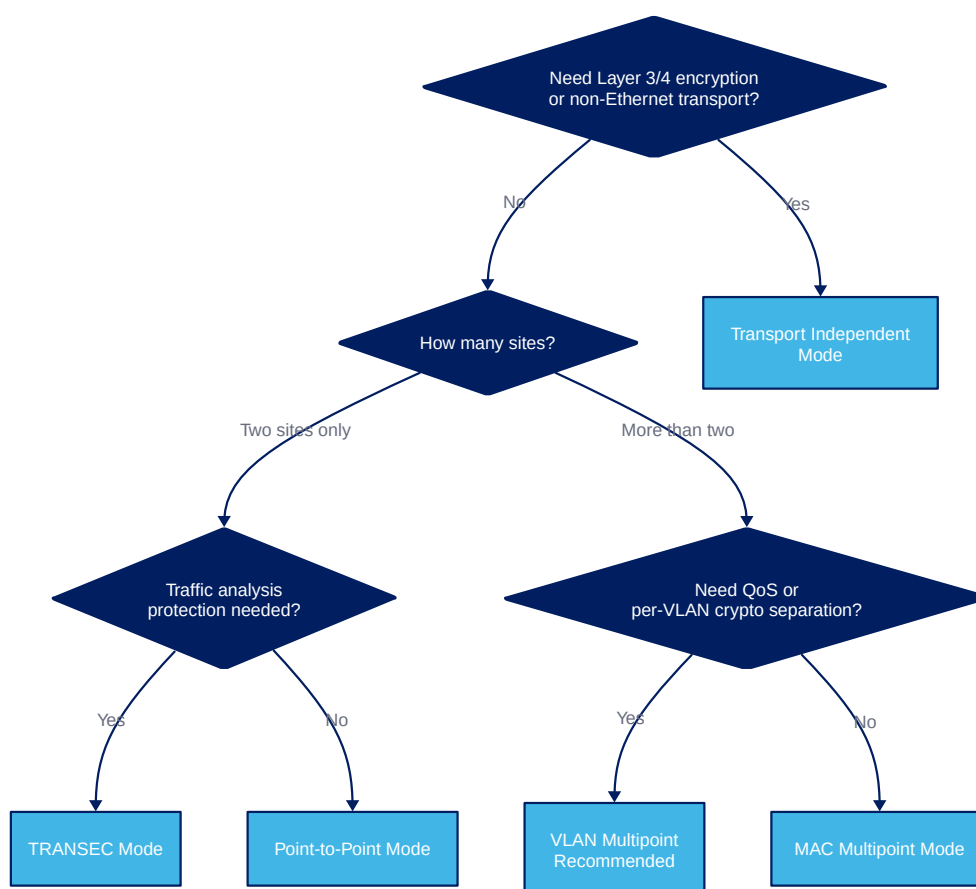


Figure 18. Connection mode selection guide

Switching Connection Modes

The connection mode is selected using the CM7 Policy tab or the CLI `line` and `con` commands.

When switching between modes, the encryptor requests a restart. On restart:

- Address (locmacs/netmacs) or VLAN tables are cleared
- The connections table is reinitialised
- The ethertypes table is reinitialised to the applicable default

During normal power cycling the encryptor is not reinitialised and previously established connections are retained.



In CM7, the Line Mode selector is not visible when the unit is in VLAN mode. The unit must first be changed to MAC mode (which triggers a restart), after which the Line Mode selector becomes available. Similarly, if the unit is in Line mode, the Connection Mode selector is not visible until Line mode is cleared.

7.2. Key Management

The CN4020 uses Data Encryption Keys (DEKs) to encrypt data plane traffic.

For a conceptual overview of pairwise and group key systems, see [Key Management Overview](#) in Chapter 2.

7.2.1. Layer 2 Modes

For detailed procedures on creating, signing, and installing certificates, see [Installing Certificates](#) and [Certificate Management](#) in Chapter 5.

Classical Algorithms

Classical Algorithms (and their associated certificates) are used as Primary Certificates.

The available Classical Algorithms when FIPS mode is enabled are:

- RSA2048
- prime256v1
- secp384r1
- secp521r1

When FIPS mode is disabled, the following are also available:

- Brainpool
- C2TNB
- C2PNB
- SM2

Post-Quantum Cryptography (PQC)

Post-Quantum Cryptography (PQC) uses quantum-resistant algorithms to provide protection against brute-force attacks using quantum computing. PQC techniques are used in conjunction with classical algorithms in a hybrid approach.



Encryptors configured with a PQC ancillary certificate cannot establish connections with devices running firmware v5.1.x or earlier. All devices in the network must use the same version of firmware.



To sign and install PQC certificates with v5.5.x firmware, CM7 must be upgraded to version 7.10.0.

The supported quantum-resistant KEM algorithms are:

- Kyber512, Kyber768, Kyber1024

- Kyber512-90s, Kyber768-90s, Kyber1024-90s

The available PQC certificate signing algorithms are:

- Dilithium2, Dilithium3, Dilithium5
- Dilithium2-AES, Dilithium3-AES, Dilithium5-AES
- Falcon-512, Falcon-1024
- SPHINCS+ variants (Haraka and SHAKE256, 128f/192f/256f, robust/simple)



SPHINCS+ certificates are not recommended. Due to their size, some SPHINCS+ certificates may not install, and if installed, they may degrade encryptor manageability.



Senetas recommends the use of Dilithium certificates.

Quantum Key Distribution (QKD)

QKD integrates external quantum key distribution devices for key exchange.



QKD or eQKD can only be enabled in VLAN, Line, and TRANSEC operational modes.

Enabling or disabling QKD requires an encryptor reboot.

QKD Configuration

At each endpoint, configure the following parameters:

Local KME IP

IP address of the local Key Management Entity (QKD device), accessible from the front panel management port.



As the CN4020 does not use DNS, the 'Local SAE ID' is the Encryptor's front panel IP Address.

Remote SAE IP

Front panel IP address of the remote encryptor.

Certificate

Certificate for the secure HTTPS connection to the KME device. Supports EC certificates.



QKD tunnels use both the retrieved QKD keys and the standard keys exchanged between the encryptors using the certificates assigned to the connection.

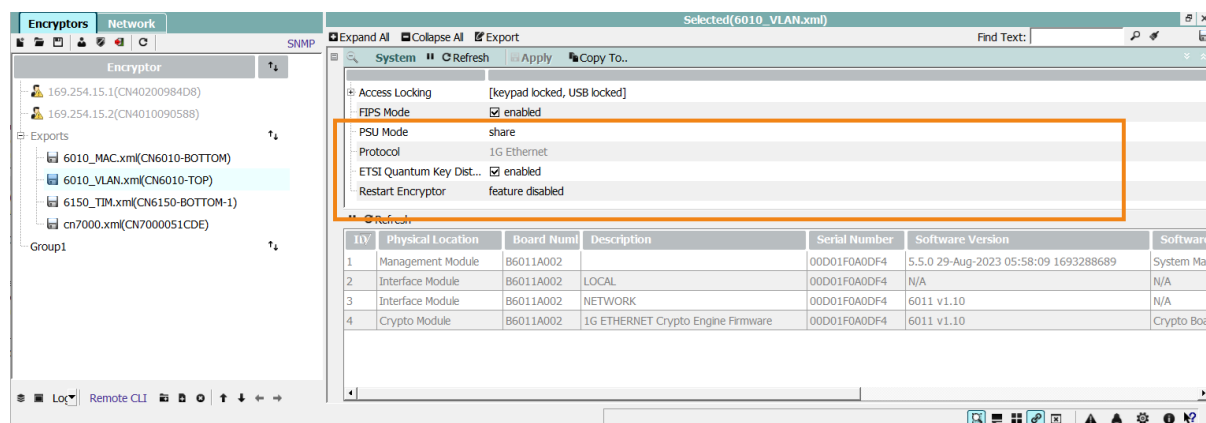


Figure 19. QKD mode selection

If QKD key retrieval fails from the KME device at either end, the encryptor reverts to internal classical CNET keys.

QKD Statistics

The CM7 QKD pane displays:

- **Successful QKD Requests** — keys successfully received from the QKD device
- **Failed QKD Requests** — keys requested but not received
- **Peer Failed QKD Key Requests** — peer-reported failed requests
- **Key Update Failures** — failed key updates due to QKD failure
- **Egress Key Status** — type of keys currently in use for key exchanges

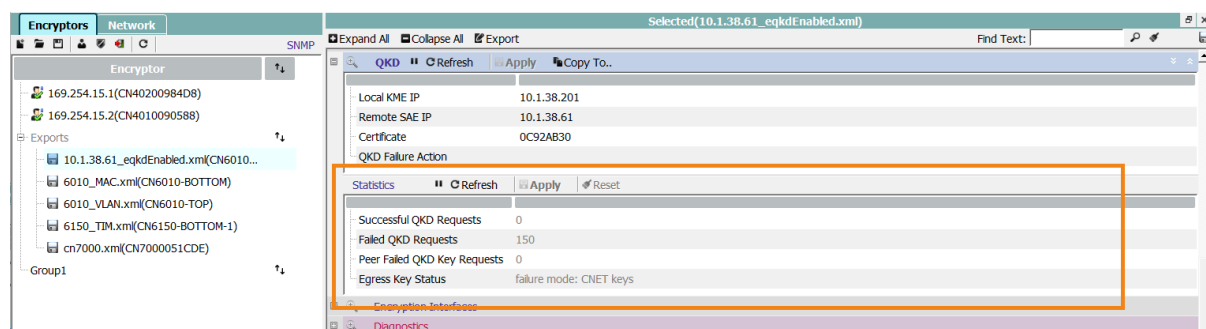


Figure 20. QKD statistics

7.2.2. Transport Independent Mode

For detailed procedures on KDK generation, installation, and distribution, see [KDK Management](#) and [KDK Installation](#) in Chapter 5.

KDF

A Key Derivation Function is a NIST-approved method of generating a sequence of encryption keys from an initial Key Derivation Key (KDK).

Once seeded with the KDK, encryptors algorithmically generate consecutive AES keys that are independent and exhibit forward and backward secrecy.

The KDF greatly simplifies key management in large-scale environments and removes the need to exchange keys across the underlying network.

KMIP

The Key Management Interoperability Protocol (KMIP) key provider delegates key generation and distribution to an external Key Management Service. For detailed setup and integration procedures using the SafeNet CipherTrust platform, see [CipherTrust Integration](#) in Chapter 5.

7.3. Cryptographic Mode Configuration

The cryptographic mode defines which AES submode is used for encryption. All encryptors that communicate with each other must use the same cryptographic mode.

For a comparison of cryptographic modes, see [Cryptographic Modes](#) in Chapter 2.



The CN4020 supports crypto-agility features that allow customisation of cryptographic operations, including cipher modification, custom entropy, and custom elliptic curves. These features require non-FIPS mode. See [Appendix C: Crypto-Agility](#) for details.

7.3.1. Selecting a Cryptographic Mode

The cryptographic mode is set from the CM7 Policy tab (Crypto Mode selector) or the CLI. If the mode is changed, the connection policy must also be updated; a warning is displayed.

The following constraints apply:

- CFB mode cannot be used at speeds of 10 Gbps or higher.
- CFB mode cannot be used for multicast traffic in meshed (multipoint) networks.
- When in multipoint mode, a change from CTR or GCM to CFB is prevented if:
 - The ethertype table contains **FollowCI** actions for multicast or broadcast traffic (change these to **Bypass** or **Discard** first)
 - Multicast connections remain in the connections table (remove these, which may require disabling multicast auto-discovery)

7.3.2. CTR/GCM Shim Configuration

In CTR and GCM modes, the encryptor periodically inserts a shim header containing the current counter value for synchronisation. The shim insertion rate varies by connection mode:

Table 38. Shim insertion rates by connection mode

Connection Mode	Default Shim Rate	User Settable
Line (Point-to-Point)	32	Yes (0–32,767)
TRANSEC	32	Yes (0–32,767)

Connection Mode	Default Shim Rate	User Settable
MAC — Unicast	32	Yes (0–32,767)
MAC — Multicast	1	No
VLAN	1	No
TIM	1	No

The shim rate can be set from the CM7 Policy tab or using the CLI `shim` command.



LLC_SAP and LLC_SAP_SNAP frames are always shimmed when encrypted.

An MTU overflow protection feature prevents shim insertion on frames that would exceed the maximum MTU (1518 octets for standard Ethernet). This can be enabled from the CM7 Policy tab (**Prevent MTU Overflow**) or the CLI. For comprehensive MTU management guidance, including overhead calculation and Path MTU Discovery, see [MTU Handling and Encryption Overhead](#).

7.4. Replay Protection

Replay protection mitigates replay attacks by using the frame counter to detect repeated frames.

Three replay protection modes are available:

Strict

Any frame counter value less than or equal to the previously seen or calculated counter value causes a tunnel restart.

Disabled

No replay protection is provided. Frames can be reordered and replayed.

Window

Frames with a counter value within a 256-bit window of the highest received value are accepted. Frames outside this window are discarded.

Supported capacity:

- Up to 16 VLANs and 32 encryptors
- Connections exceeding these limits operate with replay protection disabled

Window mapping examples:

- Line mode: 1:1 mapping between sender and receiver
- TIM mode: N:1 mapping (one window per sending encryptor)
- VLAN mode: N×M:1 mapping (N senders × M VLANs)

Replay Protection: 256-Frame Sliding Acceptance Window

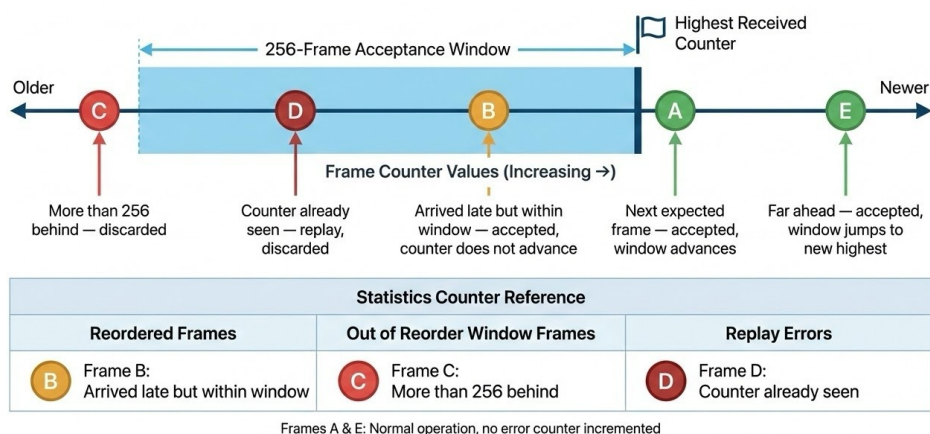


Figure 21. Replay protection: 256-frame sliding acceptance window

7.4.1. Replay Protection by Connection Mode

The available replay protection modes depend on the operational mode, crypto mode, and shim rate:

Table 39. Replay protection mode availability

Operational Mode	Crypto Mode	Shim Rate	Strict	Window	Disabled
Line (CFB)	CFB	n/a			Default
Line or TRANSEC	CTR or GCM	!= 1	Default		Yes
Line or TRANSEC	CTR or GCM	1 (MTU overflow off)	Yes	Default	Yes
Line	CTR or GCM	1 (MTU overflow on)	Default		Yes
MAC — Unicast	CTR or GCM	any	Default		Yes
MAC — Group key	CTR or GCM	1			Default
VLAN (SID off)	CTR or GCM	1			Default
VLAN (SID on)	CTR or GCM	1		Default	Yes
TIM	CTR or GCM	1		Default	Yes

7.4.2. Replay Protection Statistics

The following statistics are available via the CLI `stats` command or the CM7 Diagnostics pane under Network Received:

Network Port Replay Errors

Increments when a received shim counter has been seen before.

Network Port Reordered Frames

Increments when a received counter is less than the highest previously received value but within the 256-bit acceptance window. These frames are not discarded but indicate that reordering has occurred.

Network Port Out of Reorder Window Frames

Increments when a received counter is more than 256 below the highest received value. These frames are discarded when replay protection is set to Window.



All three statistics are valid only on the decrypt data path. If a frame fails authentication and is also replayed or out of window, only the authentication error statistic increments.

When Strict mode detects a frame counter violation, the encryptor logs a **shim sync rewind** event and restarts the tunnel.

7.5. MTU Handling and Encryption Overhead

The encryption process introduces additional overhead to every packet through the insertion of a security tag (shim) and, when AES-GCM is enabled, an Integrity Check Value (ICV) trailer. If the resulting packet size exceeds the Maximum Transmission Unit (MTU) of the network path, packets may be dropped or require fragmentation by upstream devices.

It is a critical design characteristic of the CN4020 that it **does not perform packet fragmentation or reassembly**. Proper MTU management is therefore essential to prevent packet loss.

7.5.1. Encryption Overhead Calculation

To manage MTU effectively, administrators must account for the overhead introduced by the encryption mode. The following table summarises the maximum overhead for each mode when AES-GCM is enabled.

For detailed overhead values by connection mode, see [Cryptographic Modes](#) in Chapter 2. For TIM-specific overhead by encryption layer, see [TIM Frame Overhead](#).

Table 40. Maximum encryption overhead by mode (AES-GCM)

Mode	Shim (bytes)	ICV (bytes)	Total (bytes)
Layer 2 (Line/VLAN/MAC)	8	16	24
TIM Time-sync (L2/L3/UDP)	8	16	24
TIM Time-sync (TCP)	12	16	28
TIM Time-sync (UDP Tunnel)	16	16	32

Mode	Shim (bytes)	ICV (bytes)	Total (bytes)
TIM Counter-sync (L2/L3/UDP)	10	16	26
TIM Counter-sync (TCP)	12	16	28
TIM Counter-sync (UDP Tunnel)	18	16	34



The ICV is only present when AES-GCM is enabled. In CTR mode, the overhead is the shim size only (the ICV column becomes 0).

7.5.2. MTU Management in Layer 2 Modes

Layer 2 networks (Line, MAC, VLAN modes) do not support dynamic Path MTU Discovery (PMTUD). The encryptor cannot dynamically signal hosts to reduce their packet size. Accommodating the encryption overhead requires manual configuration of the network environment using one of two approaches.

Approach A: Increase Network MTU (Jumbo Frames)

If the intermediate network infrastructure is under the administrator's control, the MTU on the links between encryptors should be increased to absorb the encryption overhead.

Example: To support a standard 1500-byte payload with 24 bytes of encryption overhead (VLAN mode, AES-GCM), the network MTU should be set to **1524 bytes**.



The CN4020 supports jumbo frames up to 10,000 bytes.

Approach B: Reduce Endpoint MTU

If the intermediate network is limited to a standard 1500-byte MTU (for example, a service provider network), the MTU on the devices *behind* the encryptors (routers, servers, workstations) must be reduced to allow room for the encryption overhead.

Example: With 24 bytes of overhead (VLAN mode, AES-GCM), the endpoint MTU should be set to **1476 bytes**.

7.5.3. Path MTU Discovery in TIM Mode

When operating in Transport Independent Mode (TIM), the CN4020 supports Path MTU Discovery (PMTUD) via the **Path MTU Maximum (PMTUM)** or **Path MTU Adjust (PMTUA)** features. PMTUM allows the administrator to define a maximum MTU threshold on the encryptor, which then generates PMTUD packets when the max is exceeded.

PMTUA allows the encryptor to modify PMTUD frames passing through the encryptor.

PMTUM Operation

The PMTUM feature operates as follows:

1. **Detection:** When an IPv4 packet arrives at the Local port, the encryptor calculates whether the packet plus the required encryption overhead will exceed the configured PMTUM threshold.
2. **Response:** If the threshold would be exceeded, the encryptor generates an ICMP Type 3, Code 4 (Fragmentation Needed) message.
3. **Next-Hop Calculation:** The ICMP message is sent back to the source host. The encryptor calculates and includes a Next-Hop MTU value:

$$\text{Next-Hop MTU} = \text{Configured PMTUM} - \text{Encryption Overhead}$$

4. **Adjustment:** The transmitting host receives the ICMP message and automatically lowers its MTU for that session to the specified value, ensuring subsequent packets pass through without fragmentation.



When a received packet triggers the PMTUM behaviour, the packet is still encrypted and transmitted by the CN4020.

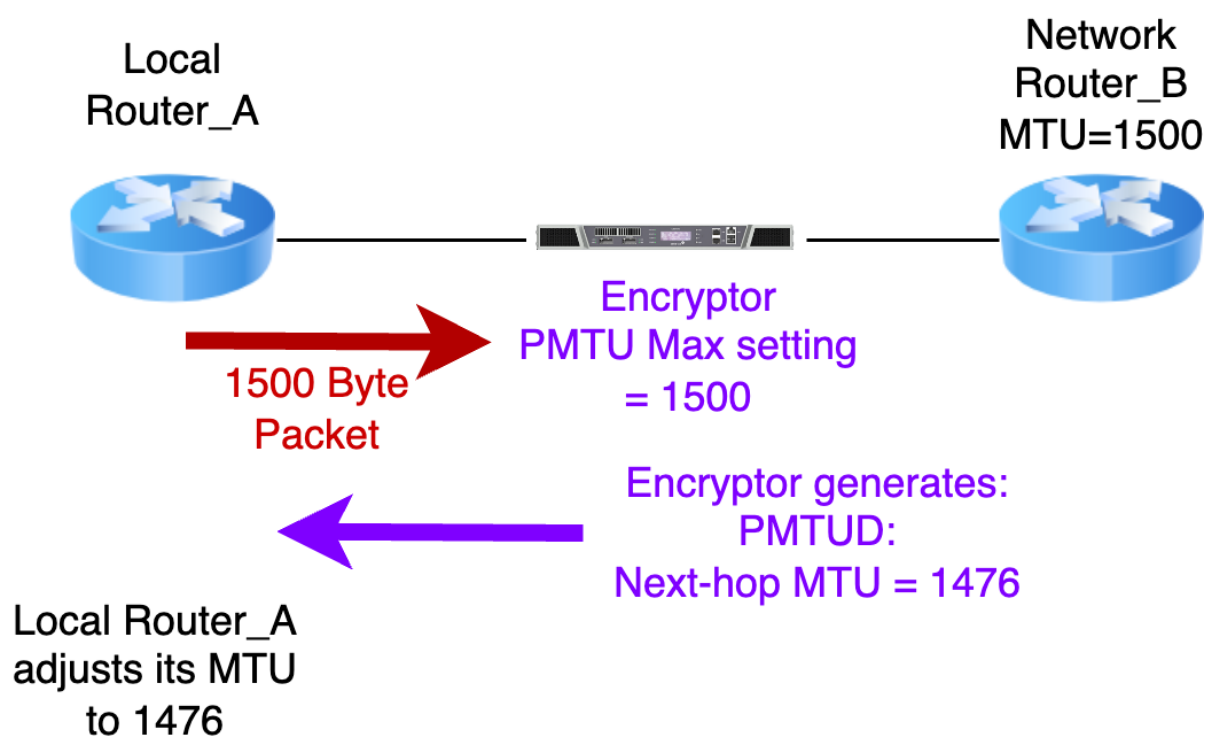


Figure 22. PMTU Max operation

Configuring PMTUM

The PMTUM value can be configured between 128 and 10,000 bytes. A value of 0 disables the feature.

CLI

```
policy -M <mtu size>
```

CM7

Navigate to the **Manage** screen, select the **Policy** pane, and edit the **Path MTU Maximum** field.

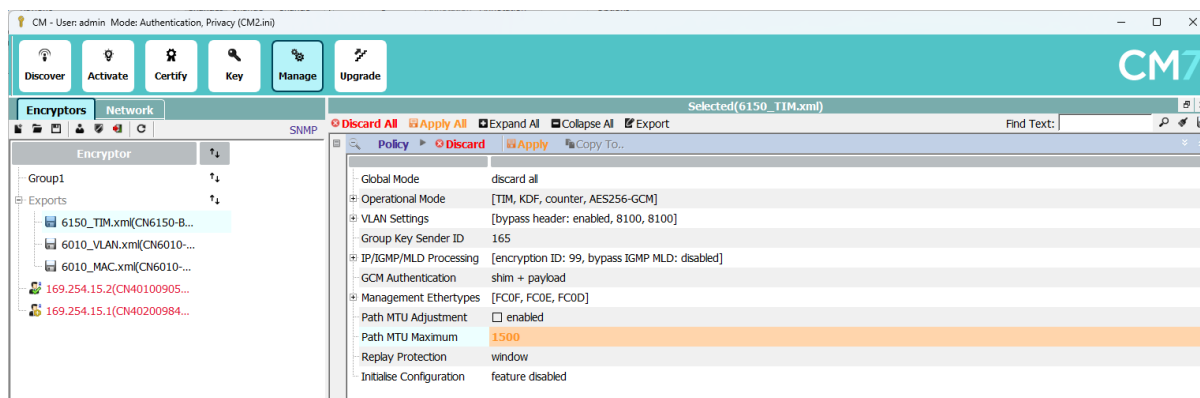


Figure 23. PMTUM configuration

Monitoring PMTUM Statistics

The CN4020 tracks MTU-related events to assist with diagnostics:

PMTU Max Tx Frames

Number of valid ICMPv4 PMTUD packets sent to source hosts.

IP MTU Exceeded Frames

Number of IPv4 packets received that exceeded the configured threshold.



On FPGA-based models, the IP MTU Exceeded Frames statistic increments even when the PMTUM feature is disabled, serving as a passive warning of potential packet loss due to encryption overhead.

For full statistics details, see [Path MTU Discovery Statistics](#) in Chapter 9.

PMTUA Operation

When enabled, PMTUA modifies PMTU frames that are received by the network port, reducing the advertised PMTU by the encryption overhead.



PMTUA cannot be enabled unless Layer 4 Checksum Recalculation is enabled.



PMTUA can only respond to PMTUD frames that are generated by other nodes in the network.

7.6. Policy Configuration (CM7)

The CM7 **Policy** tab provides comprehensive control over encryption policy. The available fields depend on the connection mode of the encryptor being managed.

Table 41. Policy parameters

Parameter	Description
Global Mode	Top-level mode: Discard, Bypass, or Encrypt.

Parameter	Description
Operational Mode	Shows the current operating mode (summarises connection and cryptographic modes).
Line Mode	Enable for Point-to-Point mode. Must be disabled to allow multipoint mode selection.
Connection Mode	Select MAC, VLAN, or TIM. Also configurable via CLI <code>con</code> command.
Key Provider	TIM mode only. Select KDF (Key Derivation Function) or KMIP (external key server).
TRANSEC	Displayed when Line mode is enabled. Controls transport frame header, frame length, frames per second, bandwidth, and MAC addresses.
Crypto Mode	Specifies the AES submode (CFB, CTR, or GCM).
CTR Mode Shim / Shim Rate	Shim insertion configuration for CTR and GCM modes.
Prevent MTU Overflow	Prevents shim insertion on frames that would exceed the MTU.
VLAN Settings	Bypass VLAN Headers, default/alternate ethertype, Q-in-Q policy.
IGMP/MLD Processing	IGMP/MLD bypass and IP multicast header bypass settings.
Management Ethertypes	Ethertypes reserved for management frames, Sender ID frames, and control plane traffic. See Control Plane and Management Ethertypes for more details.
Key Distribution Interface	Network (default) or Local (management port). VLAN Mode only.
Path MTU Adjustment	Enables encryptor based adjustment of recieved PMTU frames to allow for encrypted overhead.
Path MTU Maximum	When set, causes encryptor to generate a PMTU frame in response to packets being transmitted over the defined maximum.
Replay Protection	See Replay Protection for more information.
Initialise Configuration	Reset options (all, CI and MAC addresses, or global operation mode).

7.6.1. Policy Extensions

Table 42. Policy extension parameters

Parameter	Description
STP Monitoring	Monitors BPDU messages for topology change detection and MAC table reload.
Connection Keep Alive Monitoring	Monitors connection activity and advises if inactive.

Parameter	Description
Bypass MPLS Shim(s)	Leaves MPLS tags unencrypted. Default: enabled.
MPLS Alternate	Specifies an alternate MPLS ethertype.

7.6.2. Protocol Configuration (CM7)

The CM7 **Protocol** tab refines Ethernet policy and manages reserved multicast addresses.

7.6.3. Reserved Multicast

Bypass Reserved Multicast

When enabled, traffic to listed multicast MAC addresses is left unencrypted. Default: disabled (for security and certification compliance).



Before enabling, verify that none of the listed MAC addresses also map to IP multicast traffic that should be encrypted. Due to IP-to-MAC multicast address mapping, 32 IP multicast addresses map to one MAC address.

Unknown Network Traffic Adopts Pending Action

In MAC mode, applies the Pending connection action to frames with unknown destination MAC addresses.

Unknown VLAN Action

Action for traffic with unknown VLAN tags (VLAN mode only).



This is set to discard by default. It can only be changed to bypass if FIPS mode is disabled.

7.6.4. Ethertype Configuration

Up to 15 ethertypes can be configured with per-address-class actions.

In non-TIM modes, actions per ethertype are:

- **Discard**, **Bypass**, or **FollowCI** for Broadcast, Multicast, and Unicast

In TIM mode, additional actions are available:

- **L2** (Layer 2 encryption) or **L3/L4** (Layer 3/4 encryption)

Commonly pre-configured ethertypes:

Table 43. Pre-configured ethertypes

Ethertype	Name	Default Rationale
0x05FF	Length	Length-encoded frames

Ethertype	Name	Default Rationale
0x0800	IPv4	Standard user traffic. Encrypted and typically mutated to prevent core network interference.
0x0806	ARP	Usually bypassed to allow core network interrogation.
0x86DD	IPv6	Standard user traffic. Encrypted and mutated.
0x8847	MPLS-u	MPLS label assignment for routing.

7.6.5. Control Plane and Management Ethertypes

In Layer 2 modes of operation (Line, MAC, and VLAN), the encryptor uses dedicated Ethertypes to mark encrypted frames, manage synchronisation, and coordinate peer-to-peer key exchange. These are referred to as **Control Plane and Management Ethertypes**.

By default, these control plane frames use standard, pre-registered Senetas Ethertypes. However, all three are user-configurable to prevent conflicts with other protocols in use on the local network.

Table 44. Control plane and management ethertypes

Frame Type	Default Value	Operational Role and Usage
Management Frames	0xFC0F	Used to mark standard encrypted data frames in Line, MAC, and VLAN modes. It is also used to carry key exchange and group discovery traffic when the Key Distribution Interface is set to network (the default).
Sender ID Frames	0xFC0E	Used to identify and mark encrypted frames in VLAN mode when a unique Group Key Sender ID (SID) is configured and enabled on the encryptor.
Type 3 Management Frames	0xFC0D	Used exclusively for key exchange and group discovery frames when out-of-band key distribution is enabled by setting the Key Distribution Interface to management (VLAN only).



When modifying control plane and management ethertypes, observe the following constraints:

- **Uniqueness:** Each of the three control plane ethertypes must be assigned a unique value within an individual encryptor. Do not assign the same ethertype value to multiple control plane roles.
- **Peer Consistency:** Configured control plane ethertype values must match exactly across all peer encryptors in the network. A mismatch will prevent key distribution and disrupt encryption synchronization.
- **Collision Avoidance:** The user must ensure that none of the control plane ethertypes conflict with standard payload traffic or other active network protocols (such as LACP, STP, or ARP) traversing the encryptor.

7.7. Connection Tables (CM7)

The CM7 **Connections** tab displays active connections and their parameters. The available columns depend on the connection mode.

7.7.1. Common Parameters (All Modes)

Local Encryptor MAC Address

Displays the MAC address of this encryptor.

Key Update Interval (min)

Time between key updates. Default: 60 minutes. Range: 1–60 minutes.



Depending on the connection type (unicast vs. group) and certificate type in use, key updates may or may not trigger certificate re-authentication. See the **Authentication Interval (hours)** field below for details.

Close Connection on Expiry

When enabled, certificate expiry closes associated connections. Applicable to Line and MAC modes.

KEM

The Key Encapsulation Mechanism used to encrypt the DEK (when a PQC certificate is in use).

Authentication Interval (hours)

The time between certificate-based re-authentication requests (applicable to L2 Modes).

By default, this setting is disabled (0). Peer re-authentication and key updates behave differently depending on the connection type and certificate in use:

- **Unicast Connections using ECDSA (or Hybrid ECDSA + PQC) Certificates:** Certificate re-authentication occurs automatically on every key update (driven by the **Key Update Interval**), regardless of the **Authentication Interval** configuration. For hybrid connections, both the ECDSA and PQC components are automatically re-authenticated during this process.
- **Unicast Connections using RSA (or Hybrid RSA + PQC):** Certificate re-authentication is **not** performed on key updates unless the **Authentication Interval** is configured (value greater than 0). If configured, a certificate-based re-authentication handshake is triggered during the key update once the configured time interval has been exceeded.
- **Group Connections (All Certificate Types):** Certificate re-authentication is **not** automatically performed on key updates regardless of the certificate type. Re-authentication only occurs if the **Authentication Interval** is configured (value greater than 0). When configured, it causes group members to check the validity status of both their own certificates and the certificates being used by other members of the group once the interval is exceeded.

7.7.2. Line Mode Connection Fields

In addition to common parameters:

- **Remote MAC** — MAC address of the remote peer
- **Rx Frames / Tx Frames** — per-connection frame counters
- **Key Update / Time Remaining** — key rotation status

7.7.3. VLAN Mode Connection Fields

In addition to common parameters:

- **Group Auto Discovery** — enables automatic VLAN connection establishment
- **Dead Peer Detection Interval (sec)** — period after which an unresponsive peer causes traffic discard
- **Prohibit Master** — prevents the encryptor from becoming the group key master
- **VLAN ID** — the VLAN identifier for the connection
- **VLAN Header** — the VLAN header content

7.7.4. MAC Mode Connection Fields

In addition to common parameters:

- **Unicast Auto Discovery** — enables automatic connection creation from traffic
- **Group Auto Discovery** — enables multicast and VLAN connection establishment
- **Delete Multicast Connections** — inactivity period before multicast connections are removed
- **Authentication Interval (hours)** — time between certificate authentication requests
- **VLAN ID Override** — enables a specific VLAN ID for management traffic
- **Prohibit Master** — prevents the encryptor from becoming the group key master

7.7.5. TIM Mode Connection Fields

- **Auto-Discovery** — enables automatic KID connection creation per layer (L2, L3, L4)
- **Key ID** — the unique network-wide KID value
- **Encryptor** — IP address and name of the peer
- **Key Number** — count of assigned keys
- **Auth Errors / Replay Errors** — error counters

7.7.6. Filtering Connections

When the connection table contains many entries, use the Filter function:

- In VLAN mode: filter by VLAN IDs and VLAN ID ranges

- In MAC mode: filter by Remote MACs and Remote MAC ranges
- In TIM mode: filter by Key ID

7.8. Line Mode

7.8.1. Line Mode Policy

Point-to-Point (Line) mode secures a single connection between exactly two encryptors. A single key pair encrypts all traffic traversing the link.



Line mode is designed for point-to-point links and requires that frame order is preserved. On service provider networks where frame order may not be guaranteed (indicated by **shim sync rewind** event log entries), set the shim rate to 1 on both encryptors and disable MTU overflow protection.

7.8.2. Configuring Line Mode

This section describes the minimal steps required to configure point-to-point (Line) and TRANSEC connections on the encryptor.

Prerequisites

- The unit must be activated (see [Activation](#)).
- Administrator-level access is required to load certificates and apply global policies.

Configuration Steps

Using CM7

1. **Set Connection Mode to Line:** In the CM7 Policy tab, ensure the Line Mode selector is checked (this will trigger a reboot if switching modes).



The Line mode selector only appears when the device is operating in MAC mode.

1. **Install a Primary Certificate:** Ensure the default X.509 certificate is loaded and validated (see [Installing Certificates](#)).
2. **Install an Ancillary Certificate (Optional):** Ensure the ancillary X.509 certificate (PQC only) is loaded and validated.
3. **Configure QKD (Optional):** If using QKD, configure QKD settings as required.
4. **Configure Ethertype Policy:** Define ethertype handling rules (see [Protocol Configuration](#) in Chapter 6).
5. **Enable TRANSEC (Optional):** If traffic analysis protection is required, enable TRANSEC Mode and configure frame settings (see [Configuring TRANSEC](#)).
6. **Set the Global Mode to Secure:** Set the Global Mode field to **Secure** (Encrypt All).

7. **Verify Connection:** Confirm the connection displays as **Up** on the CM7 Connections tab.

Using the CLI

1. **Set Connection Mode to Line (Standard):**

```
encryptor> line -e
```

This command reinitialises connection tables and restarts the unit.

2. **Install a Primary Certificate:**

```
encryptor> certificate -i
```

Paste the PEM certificate when prompted (see [Installing Certificates via CLI](#)).

3. **Enable TRANSEC (Optional):**

```
encryptor> transec -e
```

Configure specific transport frame settings if required (see [Configuring TRANSEC](#)).

4. **Set the Global Policy to Secure:**

```
encryptor> global -e
```

5. **Verify Connection:**

```
encryptor> tunnels
```

7.8.3. Line Mode Specific Settings

This section details the individual parameters and settings referenced during the configuration of Line and TRANSEC modes.

Policy Extensions

The Policy Extensions tab provides additional configuration options.

Table 45. Point-to-Point policy extension settings

Setting	Description
Observe SNAP PID	When enabled, the SNAP header PID field in 802.3 SAP SNAP frames is matched to the ethertype policy table. Default: enabled.
Bypass MPLS Shim(s)	When enabled, MPLS shims are left unencrypted and encryption starts after the labels. Maximum MPLS stack depth: 5. Default: enabled.

Setting	Description
MPLS Alternate	Specifies an additional MPLS ethertype in addition to the standard 0x8847 . Default: 0x8848 .

Connection Options

Table 46. Connection options

Setting	Description
Key Update Interval	Time in minutes between key updates. Range: 1–60 minutes. Default: 60.
Key via Management Network	Routes key distribution through the management port instead of the network port. Required when the encrypted network prevents multicast key distribution.

7.8.4. TRANSEC Mode Overview

TRANSEC (Transmission Security) disguises traffic patterns to prevent traffic analysis. A TRANSEC-enabled encryptor generates and transmits fixed-size encrypted frames at a constant rate, regardless of the actual traffic load.

In the absence of user data, the encryptor fills transmitted frames with pseudo-random data that is indistinguishable from encrypted traffic. TRANSEC supports only point-to-point topologies and uses pairwise keys.

TRANSEC Characteristics

- Encrypts entire Ethernet frames, including MAC addresses and all header fields
- Fixed-size, fixed-rate encrypted frames on the network port
- Frame rate, frame length, destination MAC, source MAC, and header bytes are all user-configurable
- Minimises both latency and jitter of user data
- Control plane OAM frames can optionally bypass encryption via the Bypass Reserved Multicast setting

Frame Format

TRANSEC transport frames contain:

- A fixed, configurable header (12–82 octets: destination MAC, source MAC, optional VLAN tags, optional MPLS labels)
- An 8-octet shim for encryption synchronisation (ethertype **0xFC0F** by default)
- AES-256 CTR mode encrypted payload using a modified GFP (Generic Framing Protocol) mechanism

- Frame Check Sequence (FCS)

Client frames are encapsulated into transport frames using GFP. GFP frames are not split across transport frames; unused payload is filled with 4-octet GFP idle frames.

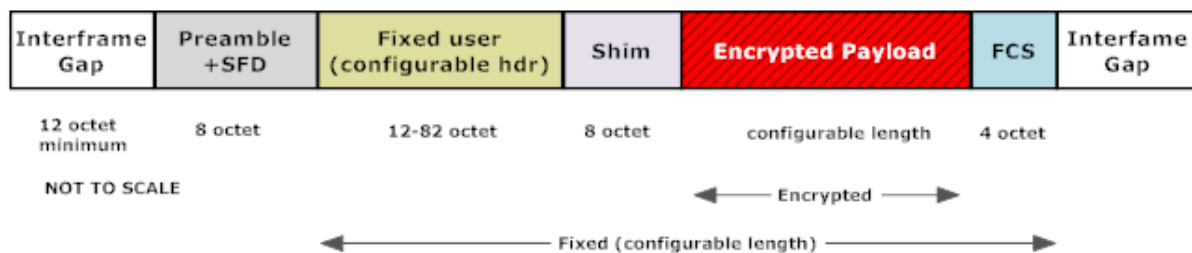


Figure 24. TRANSEC frame

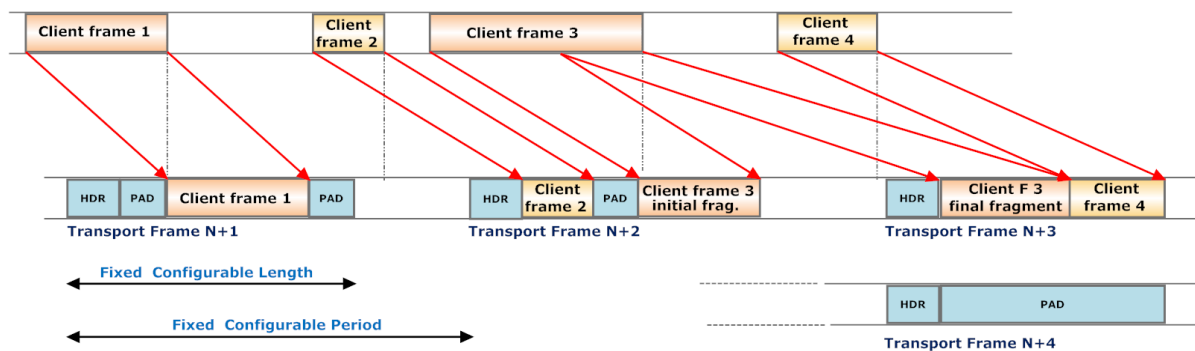


Figure 25. TRANSEC frame assembly

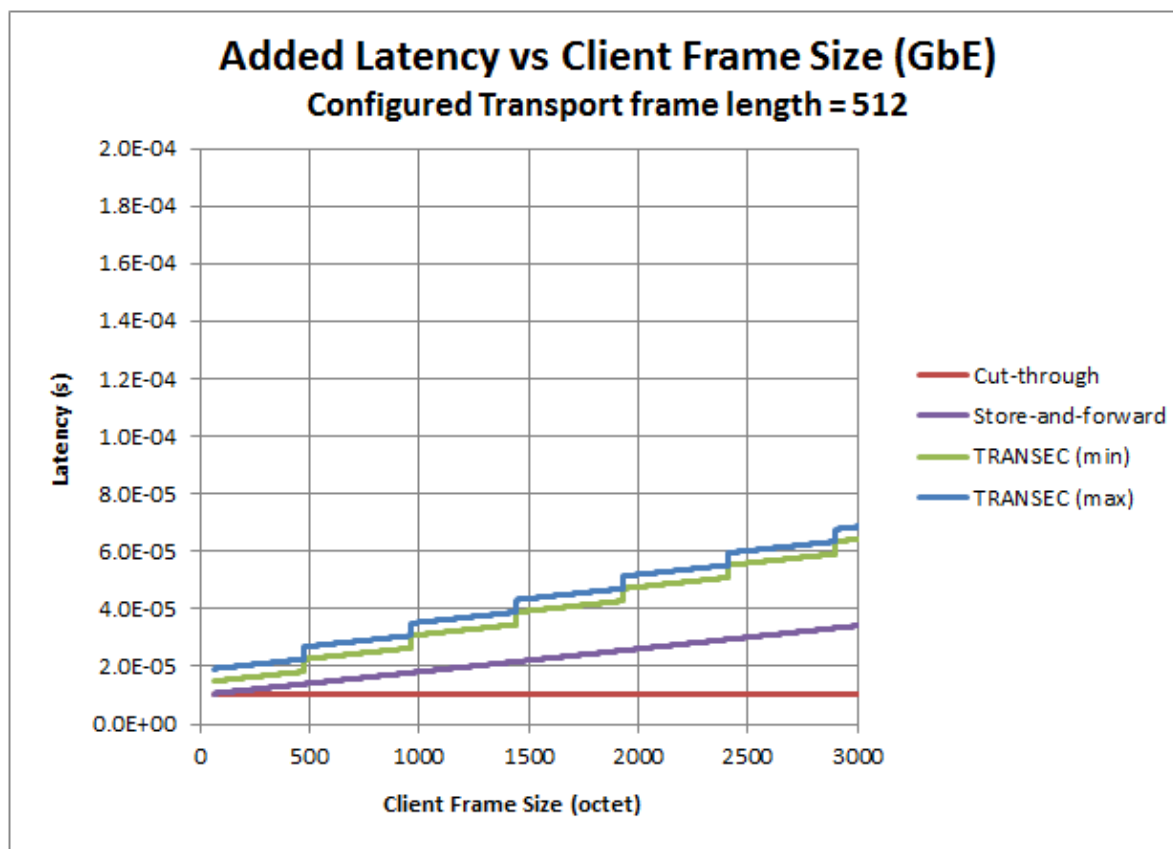


Figure 26. Latency variation with transport length of 512 octets

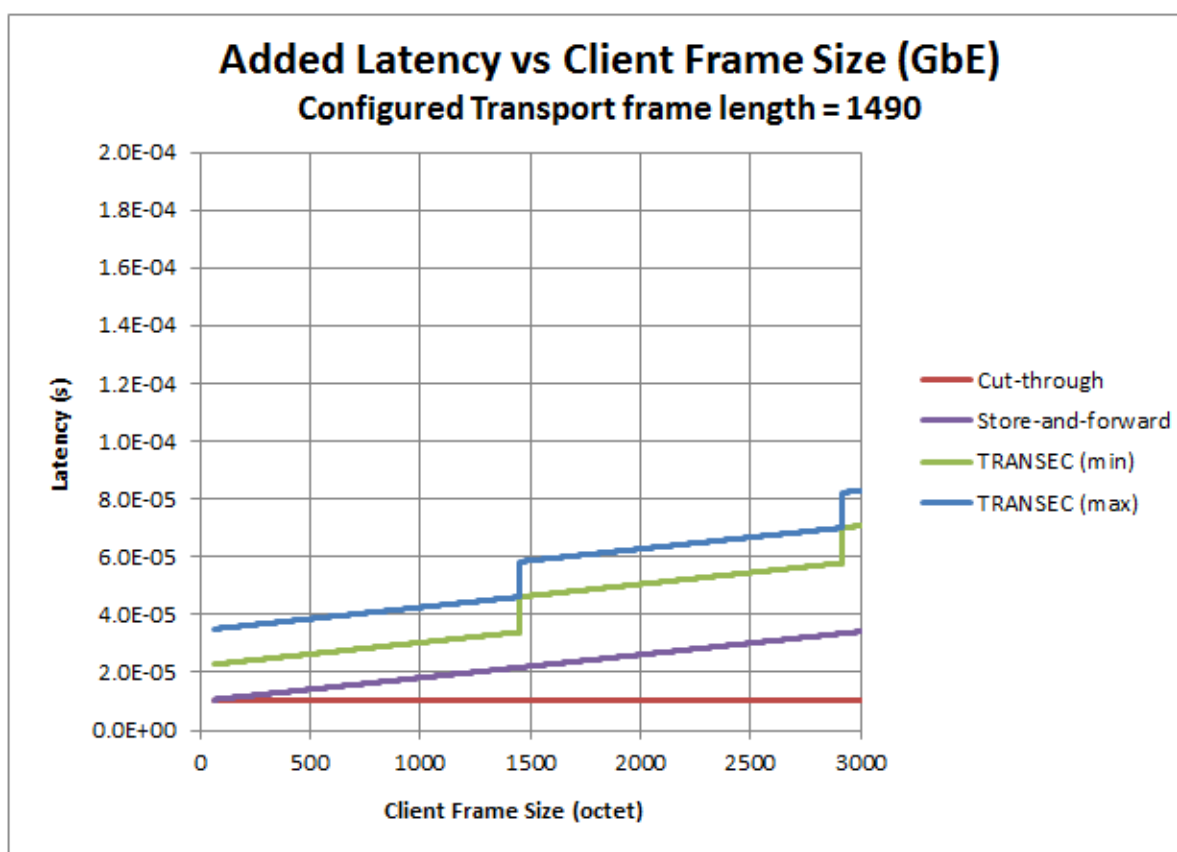


Figure 27. Latency variation with transport length of 1490 octets

TRANSEC Frame Rate Configuration

Three interdependent values control TRANSEC transmission:

Frame Rate

Frames per second (fps) transmitted on the network port.

Frame Length

Length of each transport frame in octets.

Bandwidth

The resulting line rate in bits per second.

The relationship between these values:

$$\text{Percentage} = 100\% \times \text{Frame_Rate} \times ((\text{Frame_Length} + 20) \times 8) / \text{Line_Rate}$$

where 20 octets represents the interframe gap (12 octets) plus preamble and start-of-frame delimiter (8 octets).



Set utilisation to less than 100%. Allow headroom for encryptor key management traffic and (if enabled) in-band management traffic. Both encryptors must operate at the same speed.

Configuring TRANSEC

Configure the following parameters from the CM7 Policy tab (TRANSEC section) or via CLI `transec` commands:

- **TRANSEC Mode** — enable or disable
- **Frame Length** — transport frame length in octets
- **Frames Per Second** — transmission rate
- **Bandwidth (%)** — link utilisation percentage
- **Destination MAC** — MAC address of the remote peer
- **Source MAC** — MAC address of the local encryptor
- **Header Bytes** — additional header content (VLAN tags, MPLS labels)

When TRANSEC is enabled, only global policy settings apply; per-ethertype policy settings are not used for the encrypted data.

If TRANSEC is enabled on a rate-limited encryptor, the TRANSEC transmit bandwidth limit must not exceed the rate-limiting bandwidth minus the encryption overhead.

7.8.5. Shared Settings and Key Management

For general details on shared encryption parameters such as key management, cryptographic mode configuration, replay protection, MTU handling, and common policy or connection settings, see [Encryption Configuration](#).

7.9. VLAN Mode

7.9.1. VLAN Mode Policy

VLAN multipoint mode applies encryption policy based on 802.1Q VLAN tags. Each VLAN ID can be assigned an independent encryption policy.

Encryption policy is applied hierarchically:

1. **Global mode** — highest priority
2. **Ethertype policy** — frame-level classification
3. **VLAN ID** — determines the connection and encryption action

VLAN Ethertype Policy

The VLAN mode ethertype table functions identically to the Point-to-Point ethertype table. When the ethertype action is set to `FollowCI`, the connection identifier action applies.

Up to 15 etherypes can be configured. Mutation and encryption offset are available as in other Layer 2 modes.

7.9.2. Configuring VLAN Mode

This section describes the minimal steps required to configure VLAN Multipoint connections on the encryptor.

Prerequisites

- The unit must be activated (see [Activation](#)).
- Administrator-level access is required to load certificates and apply VLAN connection rules.

Configuration Steps

Using CM7

1. **Set Connection Mode to VLAN:** In the CM7 Policy tab, set the Connection Mode selector to **VLAN** (this will trigger a reboot).
2. **Install a Primary Certificate:** Ensure the default X.509 certificate (RSA, ECDSA) is loaded and validated (see [Installing Certificates](#)).
3. **Install an Ancillary Certificate (Optional):** Ensure the ancillary X.509 certificate (PQC only) is loaded and validated.
4. **Configure the Sender ID (SID) (Optional for CN4xxx, CN6000):** Assign a unique SID value (1–511) to each encryptor across the network (see [VLAN Settings](#)).
5. **Configure Connections:**
 - For automatic setup: enable **Group Auto Discovery** (see [Auto-Discovery](#)).
 - For manual setup: add VLAN tags to the connections table (see [Configuring VLAN Connections](#)).
6. **Configure VLAN & Q-in-Q Settings:** Specify VLAN ethertypes, bypass behavior, and tag matching policies (see [VLAN Settings](#)).
7. **Configure IGMP/MLD Snooping (Optional):** Enable multicast header bypass and control frame bypass if required (see [IGMP/MLD Settings](#)).
8. **Set Global Mode to Secure:** Set the Global Mode field to **Secure** (Encrypt All).
9. **Verify Connection:** Confirm connection states in the CM7 Connections tab.

Using the CLI

1. **Set Connection Mode to VLAN:**

```
Encryptor> con -V
```

This command reinitialises tables and reboots the encryptor.

2. **Install a Primary Certificate:**

```
encryptor> certificate -i
```


Paste the PEM certificate when prompted (see [Installing Certificates via CLI](#)).

3. Install an Ancillary Certificate (Optional):

```
encryptor> certificate -i
```

Paste the PEM certificate when prompted (see [Installing Certificates via CLI](#)).

4. Configure the Sender ID (SID):

```
Encryptor> policy -i <SID_value>
```

(Triggers a reboot).

5. Configure Connections:

- For automatic setup: enable **Group Auto Discovery**:

```
Encryptor> autodisco -e
```

- For manual setup: Add secure or bypass connection rules for specific VLAN tags (see [Configuring VLAN Connections](#)):

```
Encryptor> tunnels -a -sec <vlan_id>
```

6. Set Global Mode to Secure:

```
Encryptor> global -e
```

7. Verify Connections: Check active tunnels:

```
Encryptor> tunnels
```

7.9.3. VLAN Mode Specific Settings

This section details the individual parameters and settings referenced during the configuration of VLAN Multipoint Mode.

VLAN Settings

Configure the following settings from the CM7 Policy tab:

- **Operational mode** — set to VLAN
- **VLAN ethertype** — must match the network (default: **0x8100**)
- **Alternate ethertype** — for Q-in-Q deployments where inner and outer tags use different ethertypes

- **Sender ID (SID)** — a unique value (1–511) for each encryptor in the network



Changing the Sender ID stops all connections. Connections must be restarted manually.



Setting a Sender ID modifies the Key Update Interval to 30 minutes. This value is not modified when Sender ID mode is disabled.



Sender IDs must either be set on all or no encryptors in the network.

The Control Plane Interface can also be modified in VLAN mode (default: **network**). When set to **management**, key exchanges are sent out the Front Management Port instead of the network port using **Control Plane Ethertype Type 3**. This should only be used when the encryptors are located within an MPLS network.

Bypass VLAN Headers

When enabled (the default), VLAN headers with ethertype **0x8100** are left unencrypted and encryption begins after the VLAN tags. A maximum VLAN stack depth of 2 is supported.

When enabled, the encryptor automatically learns the VLAN tag required to communicate with each peer.

Q-in-Q Policy

Q-in-Q policy controls how many VLAN tags define a unique connection:

- **1 tag** — only the outer tag is used, regardless of how many tags are present
- **2 tags** — the number of tags present (1 or 2) defines the connection

Configuring VLAN Connections (CLI)

Tagged or untagged connections can be added from the CLI:

```
Encryptor> tunnels -a -byp ①
Encryptor> tunnels -a -dis 101 ②
Encryptor> tunnels -a -sec 101 102 ③
```

- ① Add an untagged bypass connection
- ② Add a single-tagged discard connection for VLAN 101
- ③ Add a double-tagged secure connection for VLANs 101 and 102

For hex-format tags (4-character ethertype identifier followed by 4-character VLAN tag):

```
Encryptor> tunnels -a -sec 8100F010
```

IGMP/MLD Settings

When operating in VLAN mode with an active Sender ID, IGMP snooping can be supported within the encrypted network through a combination of bypassing IGMP/MLD control frames and encrypting after the IP multicast header.

Configure the following from the CM7 Policy tab (IGMP/MLD Processing section):

IP Protocol Encryption ID

The IPv4/IPv6 next header protocol identifier used for encrypted IP multicast traffic.

Bypass IGMP/MLD

Bypasses IPv4 IGMP and IPv6 MLD control plane frames.

Bypass IP Multicast Header

Leaves IPv4 and IPv6 multicast IP headers unencrypted to support IGMP snooping within the encrypted segment.

Policy Extensions (VLAN Mode)

Table 47. VLAN mode policy extension settings

Setting	Description
Observe SNAP PID	Matches SNAP header PID to the ethertype policy table. Default: enabled.
Bypass MPLS Shim(s)	Leaves MPLS shims unencrypted. Default: enabled.
MPLS Alternate	Specifies an additional MPLS ethertype. Default: 0x8848.
IGMP/MLD Settings	Enables IGMP/MLD snooping support.

Shared Settings and Key Management

For general details on shared encryption parameters such as key management, cryptographic mode configuration, replay protection, MTU handling, and common policy or connection settings, see [Encryption Configuration](#).

7.10. MAC Mode

7.10.1. MAC Mode Policy

MAC multipoint mode encrypts traffic based on Ethernet destination MAC addresses, enabling encrypted mesh networks between multiple encryptors.

Encryption policy is applied hierarchically:

1. **Global mode** — highest priority
2. **Ethertype policy** — frame-level classification
3. **MAC address policy** — destination MAC determines the connection

MAC Address Policy and Connections

Frames with an ethertype policy of **FollowCI** have their final action determined by their MAC address:

- Destination MAC for frames received on the Local port
- Source MAC for frames received on the Network port

The connection table contains:

- A single **Pending** connection (default policy for unknown MAC addresses)
- A single **Bypass** connection
- A single **Discard** connection
- Zero or more connections to remote encryptors (created by auto-discovery or manual entry)

7.10.2. Configuring MAC Mode

This section describes the minimal steps required to configure MAC Multipoint connections on the encryptor using either automatic or manual configuration.

Prerequisites

- The unit must be activated (see [Activation](#)).
- Administrator-level access is required to load certificates and modify MAC tables.

Configuration Steps

Using CM7

1. **Set Connection Mode to MAC:** In the CM7 Policy tab, set the Connection Mode selector to **MAC** (this will trigger a reboot).
2. **Install a Primary Certificate:** Ensure the default X.509 certificate (RSA, ECDSA) is loaded and validated (see [Installing Certificates](#)).
3. **Install an Ancillary Certificate (Optional):** Ensure the ancillary X.509 certificate (PQC only) is loaded and validated.
4. **Configure Connections:**
 - For automatic setup: enable **Unicast Auto Discovery** (see [Auto-Discovery](#)).
 - For manual setup: manually add target remote MAC addresses in the connections list (see [MAC Connection Establishment](#)).
5. **Configure STP Support (Optional):** If your network utilizes Spanning Tree, enable STP Monitoring (see [Spanning Tree Protocol Support](#)).
6. **Set Global Mode to Secure:** Set the Global Mode field to **Secure** (Encrypt All).
7. **Verify Connection:** Confirm the connection displays as **Up** on the CM7 Connections tab.
8. **Secure the Connection (Post-Commissioning):** Change the action of the **Pending** connection to **Discard** (under the Connections tab) and disable auto-discovery to lock down the mesh

network (see [Auto-Discovery](#)).

Using the CLI

1. Set Connection Mode to MAC:

```
Encryptor> con -M
```

This command reinitialises tables and reboots the encryptor.

```
. **Install a Primary Certificate:**
+
[source,cli]
```

```
encryptor> certificate -i
```

```
+
Paste the PEM certificate when prompted (see xref:management.adoc#install-via-cli-external-
ca[Installing Certificates via CLI]).
```

```
. **Install an Ancillary Certificate (Optional):**
+
[source,cli]
```

```
encryptor> certificate -i
```

```
+
Paste the PEM certificate when prompted (see xref:management.adoc#install-via-cli-external-
ca[Installing Certificates via CLI]).
```

```
. **Configure Tunnels and MAC Tables:**
* **Automatic Setup (ERP):** Enable auto-discovery:
Encryptor> autodisco -e
```

- **Manual Setup:** Manually configure connections, local MACs, and net MACs (see [MAC Connection Establishment](#)):

```
Encryptor> tunnels -a <remote_MAC>
Encryptor> locmacs -a <MAC>
Encryptor> netmacs -a <MAC> <connection_index>
```

1. Set Global Mode to Secure:

```
Encryptor> global -e
```

2. **Lock Down Configuration (Post-Commissioning):** Secure the pending connection and disable auto-discovery:

```
Encryptor> tunnels -e 1
Tunnel Action: <(D)iscard | (B)ypass>: [Bypass] D
```

```
Encryptor> autodisco -d
```

3. **Verify Setup:** Check tunnel states:

```
Encryptor> tunnels
```

7.10.3. MAC Mode Specific Settings

This section details the individual parameters and settings referenced during the configuration of MAC Multipoint Mode.

Auto-Discovery

When unicast auto-discovery is enabled, the encryptor learns MAC addresses from network traffic and automatically establishes secure connections with peer encryptors.

Auto-discovery checkboxes are provided for both unicast and multicast traffic. Broadcast traffic is not auto-discovered.

When multicast auto-discovery is enabled, set the inactivity timeout (in minutes) after which multicast connections are deleted. Leave the default of 0 only where multicast traffic is predictable; otherwise the netmacs table may fill, preventing new connections.

MAC Connection Establishment

The encryptor maintains internal tables:

Local MAC (locmac) table

MAC addresses of devices behind the encryptor's Local port.

Network MAC (netmac) table

MAC addresses of devices on the network side. Each address is associated with a connection table entry.

When auto-discovery identifies a new remote MAC address:

1. The address is assigned to the system Pending connection
2. The encryptor attempts to find a peer encryptor protecting the address using the Encryption Resolution Protocol (ERP)
3. If found and a connection exists, the MAC is assigned to the existing connection
4. If found and no connection exists, a new secure connection is established
5. If no peer is found, the address remains in the Pending entry and the process repeats

Management frames use Ethernet II with the Senetas registered ethertype **0xFC0F**.

MAC Migration

When a device moves from one location to another, the encryptor auto-discovery mechanism detects the change and reassigns the MAC address to the appropriate connection.

Spanning Tree Protocol Support

The CN4020 supports operation in networks using Per-VLAN Spanning Tree Protocol (PVST/STP) to provide redundant communication paths.

When STP monitoring is enabled:

- The encryptor monitors STP Configuration and Topology Change messages
- On topology change, the local MAC address table is purged
- As traffic resumes after reconvergence, auto-discovery reassigns MAC addresses to the correct connections

The encryptor can be connected to any port within a Spanning Tree topology (root, designated, alternate, or backup).

STP monitoring detects topology changes based on:

- BPDU Topology Change messages
- BPDU Configuration messages with Topology Change or Topology Change Acknowledge flags set
- BPDU Configuration message absence for at least 3 hello time periods followed by reception



STP monitoring requires auto-discovery to be enabled.



STP monitoring does not affect the encryptor's throughput or latency.

Configuring STP Monitoring (CLI)

1. Enable auto-discovery:

```
Encryptor> autodisco -e
```

2. Set ether type policy for **H05FF** multicast addressed frames to **Bypass**, and/or enable Reserved Multicast Address Bypass:

```
Encryptor> ethertypes -e  
Enter Ether type [(0)ther, Value (Hex)]: 05ff
```

Or:

```
Encryptor> policy -b -e
```

3. Enable STP monitoring:

```
Encryptor> policy -s -e
```

Policy Extensions (MAC Mode)

Table 48. MAC mode policy extension settings

Setting	Description
Observe SNAP PID	Matches SNAP header PID to the ethertype policy table. Default: enabled.
STP Monitoring	Monitors BPDU messages for topology change detection.
Tunnel Keep Alive Monitoring	Protocol-independent mechanism for detecting network failover.
Observe Pending Ingress Action	When enabled, applies the Pending connection action to frames received on the network port with unknown local MAC addresses.
Bypass MPLS Shim(s)	Leaves MPLS shims unencrypted. Default: enabled.
MPLS Alternate	Specifies an additional MPLS ethertype. Default: 0x8848 .

Shared Settings and Key Management

For general details on shared encryption parameters such as key management, cryptographic mode configuration, replay protection, MTU handling, and common policy or connection settings, see [Encryption Configuration](#).

7.11. Transport Independent Mode

7.11.1. TIM Mode Policy

Transport Independent Mode (TIM) allows encryption at layers 2, 3, and 4 of the OSI model. An extensible key provider model decouples key generation from the underlying network.

TIM Policy Overview

TIM policy has similarities to VLAN policy with extensions for Layer 3 and 4 traffic.

Ethertype Table

The default in TIM mode is to bypass all traffic except IPv4 unicast. IPv4 traffic is further classified using the IP Rules table.

The Bypass MPLS Shim(s) feature must remain enabled in TIM mode to allow L3/L4 header inspection.

IP Rules Table

Defines IPv4/IPv6 policy based on IP address, protocol, and TCP/UDP port numbers using Longest Prefix Match (LPM).

See [IP Rules](#) for configuration details.

Encrypted Frame Formats (TIM)

The encryption policy determines where in the frame the shim is located and which portion is encrypted. [TIM encrypted frame formats by encryption layer](#) shows the frame structure at each encryption layer, including the position of the security shim and the encrypted region.

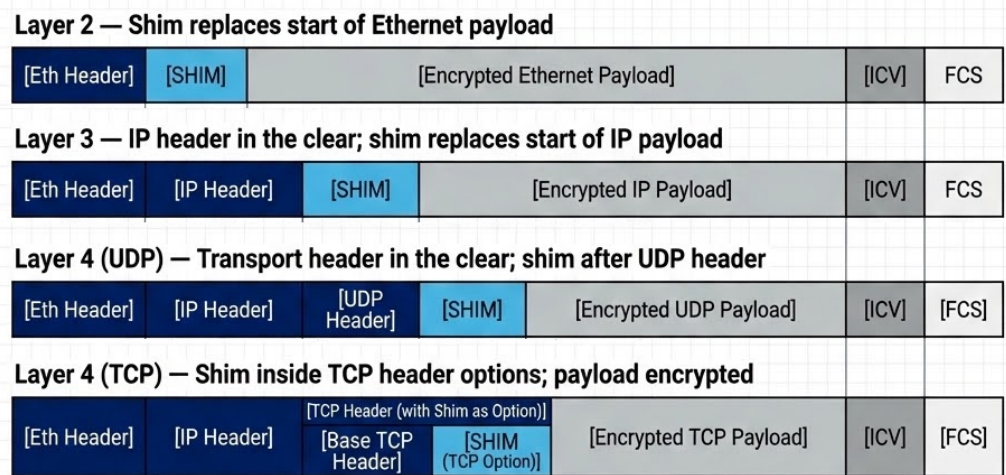


Figure 28. TIM encrypted frame formats by encryption layer

The supported encryption layers are:

- **Layer 2** — shim and encryption applied to the Ethernet payload
- **Layer 3** — shim and encryption applied to the IP payload
- **Layer 4 (TCP)** — shim inserted as a TCP Timestamp option; payload encrypted
- **Layer 4 (UDP)** — shim inserted after the L4 header; payload encrypted



For TCP frames, the shim is inserted as a TCP Timestamp option. For UDP frames, the shim is inserted immediately following the L4 header.

The maximum MTU for CN series encryptors is 10,000 bytes minus 28 bytes of overhead (12-byte shim + 16-byte authentication tag) when using the default GCM mode.

7.11.2. Configuring TIM Mode

This section describes the minimal steps required to bring a unit into Transport Independent Mode (TIM) service during commissioning.

Prerequisites

- The unit must be activated (see [Activation](#)).
- Ensure the date, timezone, and NTP configuration are correct on all devices (NTP is required for time-based key synchronisation).

Configuration Steps

Using CM7

1. **Set the Connection Mode to TIM:** In the CM7 Policy tab, set the Connection Mode selector to **TIM** (this will trigger a reboot).
2. **Load Key Material (KDK):** If using KDF, generate and distribute the Key Derivation Key (KDK) to all devices in the network (see [KDK Management](#)).
3. **Select the Key Synchronisation Method:** Choose time-based or counter-based synchronisation (see [Key Synchronisation](#)).
4. **Configure the Key Identifier (KID):** Set a unique KID on each encryptor in the network (see [Key Identifier \(KID\)](#)).
5. **Configure IP Rules:** Define encryption rules (see [IP Rules](#)).
 - Configure the "Unlisted IP Action" (Discard by default)
6. **Configure Connections:**
 - For automatic setup: enable **Auto Discovery** at the appropriate layer (see [Auto-Discovery](#)).
 - For semi-automatic setup: On the 'Key' screen, select all encryptors in the network and click "Auto-add Peer Tunnels"
 - For Manual setup: Add all encryptor KIDs to each other via the Connections table.
7. **Configure Global Mode:** Set the global mode to **encrypt**.
8. **Verify Setup:** Check connection states on the CM7 Connections tab.

Using the CLI

1. **Set the Connection Mode to TIM:**

```
Encryptor> con -T
```

This command resets all tunnel/CI and MAC data to factory defaults and reboots the encryptor.

2. **Load Key Material (KDK):** If using KDF, configure the Key Derivation Key (KDK):

```
Encryptor> kdf -k
```



Loading a KDK via the console interface can only be completed if FIPS mode is disabled.

3. **Select the Key Synchronisation Method:** Set to time-based or counter-based (see [Key Synchronisation](#)):

```
Encryptor> keyprovider -k <time|counter>
```

4. **Configure the Key Identifier (KID):** Set the unique KID:

```
Encryptor> policy -d <KID_value>
```

(Triggers a reboot).

5. **Configure IP Rules:** Define unlisted action and 5-tuple IP rules. (see [IP Rules](#)):

```
Encryptor> iprules -a <ip_address> <action>
```

6. **Configure Connections:**

- Automatic Setup

```
Encryptor> autodisco -e
```

- Manual Setup

```
Encryptor> tunnels -a <sec|dis|byp> [<key_id>]
```

7. **Set the Global Mode to Encrypt:**

```
Encryptor> global -e
```

8. **Verify Tunnels:** Check connection states:

```
Encryptor> tunnels
```

7.11.3. TIM Mode Specific Settings

This section details the individual parameters and settings referenced during the configuration of Transport Independent Mode.

Key Identifier (KID)

The KID is a unique network-wide value that identifies a pool of keys used for encryption by one transmitting encryptor and decryption by all receiving encryptors.

Requirements:

- Valid only when the operational mode is set to TIM
- A unique value must be set on each encryptor

The key pool is sourced from the configured key provider (KDF or KMIP).

If an encryptor detects a duplicate KID, the alarm **ALARM_DUPLICATE_KID_DETECTED** is raised and all frames with that KID are discarded. To resolve:

1. Set the global mode to Discard

2. Change the KID value (triggers a reboot)
3. Acknowledge the alarm
4. Set the global mode to Encrypt

On power-up in TIM mode, the KID is set to a random value. It can be manually set using the CLI `policy -d` command (triggers a reboot).

Layer 4 Encryption Mode

To enable Layer 4 IP rules:

- CLI: `iprules -l4 -e`
- CM7: enable the **Layer 4 Encryption Mode** checkbox in the IP Rules pane

Once enabled, Layer 4 IP rules policies can be entered and Layer 4 auto-discovery enabled.



It is recommended that all Layer 4 IP rule policies specify the same action (for example, all encrypt or all bypass). Mixing encryption and bypass actions is not recommended.

Key Provider Model

The key provider model is an abstracted service interface for secure key generation, synchronisation, and update between encryptors.

Available key providers:

Key Derivation Function (KDF)

A NIST-approved method (SP 800-108) for deriving multiple encryption keys from an initial Key Derivation Key (KDK) using HMAC in counter mode.

The KDF:

- Produces AES-256 keys that are used directly as Data Encryption Keys
- Provides key separation — compromise of one derived key does not affect the security of prior or future keys
- Does not require a centralised key server

The KDK must be derived from a cryptographically secure PRNG and kept secret. Each encryptor in the network must use the same KDK, which can be generated on one encryptor and distributed to others via the CLI `kdf` command or via CM7.

External KMIP Key Server

Relies on a third-party Key Management Service (for example, Thales CipherTrust) for key generation and distribution. The key server must be reachable by all encryptors. Key management messaging occurs only between individual encryptors and the key server.

Encryptors communicate with the key server over an authenticated TLS v1.2 session using KMIP. Keys are uniquely named using the requesting encryptor's SID (for example, `SID_DEK_0`).

Configure the key provider using the CLI `keyprovider` command or the CM7 Policy tab (Key Provider selector).



Changing the key provider does not restart the egress tunnel. It can take up to two key updates to take effect. It is recommended to manually restart the tunnel after changing the key provider.

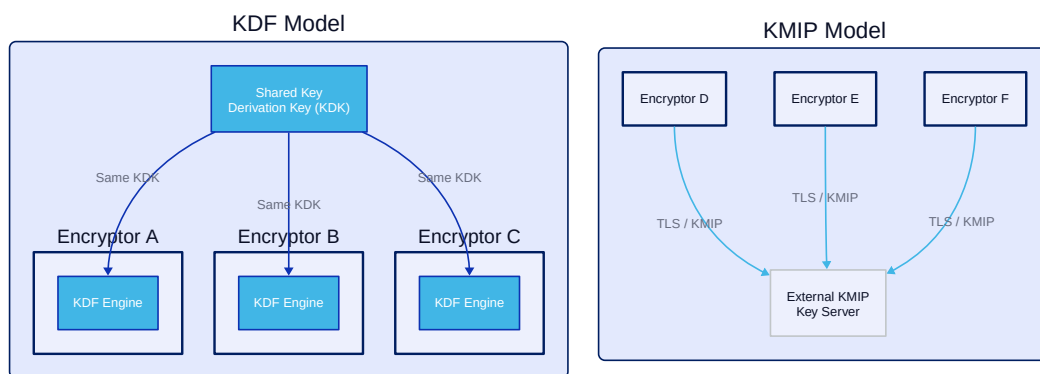


Figure 29. TIM key provider architectures: KDF vs KMIP

Key Synchronisation

Key synchronisation ensures that peer encryptors use the same DEK. Two methods are available, selected using the CLI `keyprovider -k` command:

Time-based

DEKs are updated automatically every hour (non-configurable period). Synchronisation is guaranteed through a common NTP time reference. Keys are numbered based on hours elapsed since the Unix epoch (00:00:00, 1 January 1970).

All keys change synchronously across the network on hour boundaries. After a key update, transmitters generate a replacement DEK within a fixed time window. Receivers update their keys within a similar window.



NTP must be configured and operational for time-based synchronisation.

Counter-based (default)

Key updates are synchronised based on the frame counter. When the counter is exhausted, the key number is incremented.



When both the key number and frame counter are exhausted, the encryptor discards all traffic until a new KDK is installed.

Encryptors maintain two DEKs at all times (for example, **SID_DEK_1a** and **SID_DEK_1b**) to allow atomic key rollover without traffic loss. The shim in each encrypted frame contains a Key Bank field indicating which DEK to use.



Switching between time-based and counter-based synchronisation clears all existing IP rules. Switching from time to counter reinitialises key numbers to 1 even if the same KDK is used.

UDP Tunnelling

UDP tunnelling encapsulates any IP protocol inside a UDP header, inserting an 8-byte UDP header after the IP header, followed by the security shim and encrypted payload.

The default UDP source and destination port is 64527 (configurable).

UDP tunnelling is recommended when:

- TCP cannot be natively encrypted at Layer 4 due to firewall interference with the TCP timestamp field
- Layer 4 protocols not based on UDP or TCP require encryption
- NAT/PAT environments require operation without exposing the inner Layer 4 header
- Multiple encryptors at one site require distinguishable traffic via configurable ports
- Port blocking by carriers or firewalls must be avoided

Enable UDP tunnelling using the CM7 Manage pane or the CLI:

```
Encryptor> iprules -ltu -e
```

Configure UDP tunnel policies via the IP Rules table:

```
Encryptor> iprules -a <ip_address> [tcp|udp] [port] ltu
```

Change tunnel ports:

```
Encryptor> iprules -h -s <src|dst> <port_number>
```



Choose port numbers from the IANA dynamic/private range (49152–65535) to avoid collisions with well-known service ports.



Port number 0 is not an acceptable value.

Auto-Population

Auto-population automatically creates tunnels by retrieving keys from the key provider. It is an alternative to auto-discovery or manual tunnel creation.

Auto-population must only be enabled when auto-discovery is disabled. When enabled, the encryptor deletes existing tunnels and IP rules, reboots, and populates all tunnels on start-up.

Enable/disable via CLI:

```
Encryptor> autopop -e
Encryptor> autopop -d
```



The auto-population feature is not supported with counter-based key synchronisation.

KDK Management

The CN4020 uses Data Encryption Keys (DEKs) to encrypt data plane traffic.

For a conceptual overview of pairwise and group key systems, see [Key Management Overview](#) in Chapter 2.

Generating KDK Keys in CM7

To generate KDK keys for distribution to TIM-mode encryptors:

1. In CM7, open **Settings** → **CA/Key Management** and select the **KDK** tab.
2. Keys can be manually entered (unless in FIPS mode) or generated using the **Autofill KDK** selector, which allows CM7 or any listed encryptor to be used as the key source.
3. Click **Create KDK File**. Enter a password to protect the file.
4. The key file is saved to the AppData path for the logged-in user. The filename suffix is based on the hash of the KDK.

 CA/Key Management ✕

Create New CA Advanced EC Parameters Export CA Certs **KDK**

This screen creates **Key Derivation Key (KDK)**, encrypts it and stores it in a file. The **KDK** can be created from DRBG of a selected encryptor, generated in CM7 or entered manually.

1. Enter **KDK** manually or select an option from **Autofill KDK** combo box.
2. Select a name and location for the file to store the encrypted **KDK** in.
3. Click '**Create KDK File**' button.
4. To encrypt the **KDK** enter and confirm a password. **This password will be required when distributing the KDK to encryptors!**

KDK: 

Hash:

Autofill KDK:

Generate in CM7 



KDK File: 

Create KDK File

Close

Figure 30. KDK generation

Distributing KDK Keys

1. Select the **Key** button in the CM7 Manage screen.
2. Browse to the KDK key file and enter the assigned password.
3. To apply the key immediately, leave the **Install UTC Time** selector blank. To schedule installation, set the required date and time.
4. Select the target encryptors in the encryptor list.
5. Click **Add KDK**.

Following distribution, CM7 displays a hash of the current key and (if scheduled) the pending key.



If the UTC Time field was left blank, connections restart immediately using the new key.

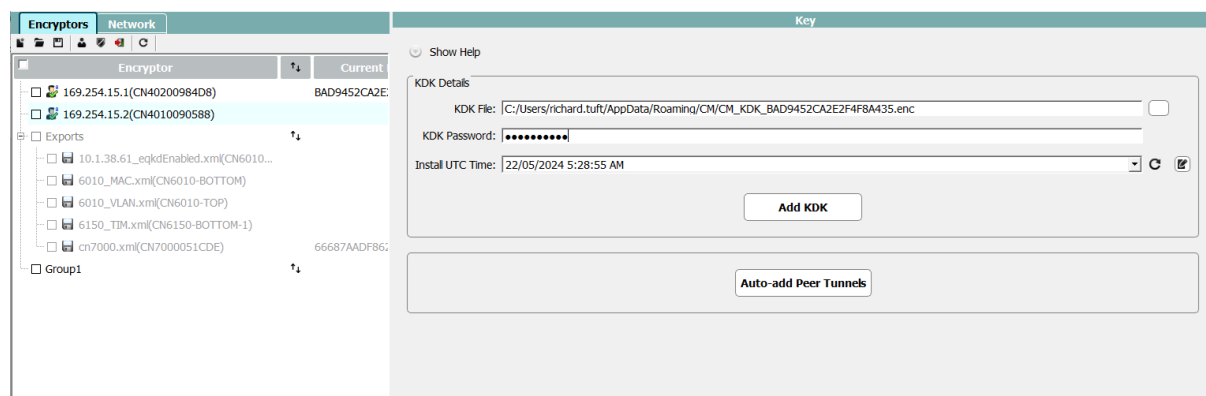


Figure 31. KDK installation

Auto-Add Peers

Click **Auto-add Peer Tunnels** in the CM7 Key screen to automatically create tunnels between available encryptor pairs.

KDF and FIPS Mode

When FIPS mode is enabled, the CLI **kdf -g** and **kdf -k** commands cannot be used locally. KDF keys can still be entered via CM7, SNMPv3, or the remote CLI.

When FIPS mode is disabled, all methods are available: local CLI, CM7, SNMPv3, and remote CLI.

Post-Quantum Cryptography (PQC)

As TIM does not use public key cryptography, it is not vulnerable to quantum-based attacks.

IP Rules

The IP Rules table determines the encryption policy for traffic in TIM mode. Rules are matched using Longest Prefix Match (LPM) on IP addresses.

IP Rules Parameters

Action for Unlisted IPs

Action for addresses not in the table: **Discard**, **Bypass**, **Encrypt L2**, **Encrypt L3**, or **Encrypt L4**. When set to Encrypt L4, UDP and TCP packets are encrypted at L4; all other packets are encrypted at L3.

Layer 4 Checksum Calculation

When enabled, the encryptor operates in Store-and-Forward mode, performing L3 and L4 checksum updates and checks. When disabled, the encryptor operates in cut-through mode (no checksum checks).

DPDK-based encryptors (CN7000 series and CV1000) always operate in Store-and-Forward mode.

Each rule entry specifies:

- **Destination IP Address** and **Destination Prefix** — for LPM matching
- **Source IP Address** and **Source Prefix** — for LPM matching
- **Protocol** — for Layer 4 matching (TCP: 6, UDP: 17)
- **Destination Port** and **Source Port** — for Layer 4 matching
- **Action** — **Discard**, **Bypass**, **Encrypt L2**, **Encrypt L3**, or **Encrypt L4**



Since the TCP checksum is based on the IP header, Layer 3 encryption for TCP traffic on NAT-based networks does not work as expected. Use Layer 4 encryption policy in such cases.

Layer 4 Checksum Calculation

When enabled, the encryptor operates in Store-and-Forward mode, performing L4 checksum updates and checks. When disabled, the encryptor operates in cut-through mode (no checksum checks).

Enable Layer 4 checksum calculation when the encrypted data traverses a network that performs:

- Network Address Translation (NAT)
- Port Address Translation (PAT)
- Deep packet inspection to Layer 4



Enabling Layer 4 checksum calculation makes the encryptor a store-and-forward device, which increases latency.

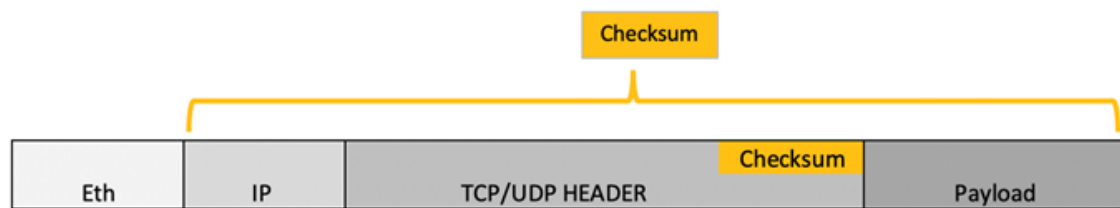


Figure 32. Layer 4 checksum calculation

Specifying IP Rules

Wildcards (*) are accepted for the protocol and port fields only (not for IP address and subnet mask).

- Source IP address can be 0.0.0.0/0 (wildcard) or a valid IPv4 address with mask 1–32
- Source port can be * (wildcard) or a value between 1–65,535
- If a port number is specified, the protocol must also be specified (UDP: 17 or TCP: 6)
- Up to 8 distinct source address/mask pairs can be specified per destination address/mask
- Layer 4 encryption (c14) is only applicable for TCP and UDP; specifying c14 with any other protocol causes an audit log entry



IPv6 addresses are not supported in IP rules.

IP Rules for Virtual Management

The location of the managing host determines whether IP rules are required for virtual management:



These requirements differ between FPGA and DPDK units.

- Virtual management traffic is captured before the encryption engine; no IP rules are required at the device being managed
- If the managing host is on the LAN side of the network, IP rules are required to bypass management traffic intended for remote devices

Shared Settings and Key Management

For general details on shared encryption parameters such as key management, cryptographic mode configuration, replay protection, MTU handling, and common policy or connection settings, see [Encryption Configuration](#).

Chapter 8. High Availability

8.1. High Availability

This chapter describes the high availability features of the CN4020. It covers network-level failover mechanisms, link-level resilience features, and power supply redundancy.

For encryption mode and connection mode configuration, see [Chapter 6: Encryption Configuration](#).

8.1.1. Overview

The CN4020 provides high availability through several complementary mechanisms:

Network-level failover

Spanning Tree Protocol (STP) monitoring detects topology changes in the switching infrastructure and triggers automatic failover to redundant paths. Tunnel Keep Alive Monitoring (TKAM) provides protocol-independent detection of connection loss between encryptor peers.

Link-level resilience

Local Link Monitoring (LLM) detects loss of the local port link and transitions the encryptor to discard mode. Link Loss Forwarding (LLF) propagates optical signal loss across ports so that upstream and downstream equipment can detect the failure.

MAC migration

Automatic relearning of MAC addresses when protected devices relocate between sites.

8.1.2. Spanning Tree Protocol (STP) Monitoring

The CN4020 supports operation in networks that use the Per-VLAN Spanning Tree Protocol (PVST or STP) to provide redundant communication paths.

STP prevents active loops in a switched network and provides automatic failover to redundant links. The STP monitoring feature enables the CN4020 to detect topology changes and trigger failover between encryptors.

How STP Monitoring Works

All switches in an STP topology advertise their STP knowledge via configuration messages (BPDUs), transmitted periodically at the hello time interval. Absence of these messages can cause inactive ports to become active, triggering a topology change.

When a topology change occurs, the affected switches send topology change messages and select a new forwarding path.

The CN4020 monitors STP configuration and topology change messages to identify when a topology change occurs. The encryptor can be connected to any switch or port within an STP topology — there are no limitations on the spanning tree port type (root, designated, alternate, or backup).

The encryptor detects a topology change on the following conditions:

- BPDU Topology Change message received
- BPDU Configuration message with Topology Change flag set
- BPDU Configuration message with Topology Change Acknowledge flag set
- BPDU Configuration message absence for at least 3 hello time periods, followed by BPDU configuration message reception



STP monitoring requires auto-discovery to be enabled.



STP monitoring does not have any adverse effects on the encryptor's throughput or latency.

Failover Process

When a topology change is detected, the CN4020 purges its local MAC address table. Under normal operation the encryptor preserves MAC addresses (no ageing). With STP monitoring enabled, a topology change triggers the local MAC address table to be aged (purged).

Once the spanning tree reconverges and begins forwarding data, new addresses are identified on the local (protected) side of the encryptor. The auto-discovery mechanism then notifies all peer encryptors that this encryptor now protects these MAC addresses, completing the failover.

The following sequence describes a typical STP failover:

1. **Initial state** — Encryptor E1 is on the active path within the spanning tree. Encryptor E2 is on a blocked/alternate segment and is not visible to other encryptors. E1 and E3 identify each other and establish a connection via auto-discovery.
2. **Failover** — A failure occurs on the active path. The spanning tree detects the failure and performs a topology change to use the inactive/alternate path. E2 and E3 identify each other and establish a connection via auto-discovery (if they have not previously communicated). E3 is notified of the change and the remote MAC address is moved from the original connection to the new connection.
3. **Restoration** — The failed path is restored. The spanning tree generates a topology change and the local MAC table in E1 is purged. As traffic is forwarded, E1 relearns the MAC addresses via auto-discovery and notifies E3. E3 adjusts its network MAC table to map addresses back to the original connection.

Configuring STP Monitoring

STP monitoring is configured from the CLI using the following steps.

Prerequisites

- The encryptor must be in multipoint MAC mode.
- Auto-discovery must be enabled.

Procedure

1. Enable auto-discovery:

```
Encryptor>autodisco -e
Automatic session discovery enabled
```

2. Set the ethertype table policy for 05FF multicast-addressed frames to bypass:

```
Encryptor>ethertypes -e
Enter Ethertype [(0)ther, Value (Hex)]: 05ff
Type exists
Offset Enable: <(Y)es | (N)o>: [No]
Unicast Action: <(F)ollow CI | (D)iscard | (B)ypass>: [Follow CI]
Multicast Action: <(D)iscard | (B)ypass>: [Bypass]
Broadcast Action: <(D)iscard | (B)ypass>: [Bypass]
Updated existing ethertype
```

Alternatively, enable reserved multicast address bypass:

```
Encryptor>policy -b -e
Reserved Multicast bypass enabled
```

3. Enable STP monitoring:

```
Encryptor>policy -s -e
STP monitoring enabled
```

STP Monitoring Requirements and Constraints

- Requires auto-discovery to be enabled.
- Operates in Layer 2 multipoint (MAC) mode only.
- The encryptor can be connected to any spanning tree port type (root, designated, alternate, or backup).
- No adverse effect on throughput or latency.

8.1.3. Tunnel Keep Alive Monitoring (TKAM)

Tunnel Keep Alive Monitoring (TKAM) is a protocol-independent mechanism for detecting network failover at the connection level.

How TKAM Works

When TKAM is enabled, encryptors send and receive keep-alive messages every 30 seconds to the peer encryptor on each encrypted connection.

If 10 consecutive keep-alive messages are not received on a connection, the encryptor automatically purges the network MAC addresses associated with that connection. This allows new MAC addresses to be learnt via auto-discovery, enabling failover to an alternative path.

Configuring TKAM

Enable TKAM from the CLI using the `policy` command:

Prerequisites

- The encryptor must be in multipoint mode.
- Auto-discovery must be enabled.

TKAM Requirements and Constraints

- Operates in multipoint mode only.
- Requires auto-discovery to be enabled.
- Keep-alive interval: 30 seconds (not user-configurable).
- Detection threshold: 10 consecutive missed keep-alive messages.

8.1.4. MAC Migration

When a device (such as a workstation) is physically moved from one geographic location to another, the CN4020 automatically detects the change and relearns the MAC address at the new location.

The auto-discovery mechanism updates the MAC tables on all affected encryptors so that traffic continues to flow securely to the device at its new location. No manual reconfiguration is required.

8.1.5. Link Loss Detection

The CN4020 provides two link-level detection mechanisms that enable upstream and downstream network equipment to respond to failures.

Local Link Monitoring (LLM)

Local Link Monitoring detects loss of the local port link and transitions the encryptor to global discard mode, preventing traffic from being forwarded without encryption.

When LLM is enabled:

- If the local link goes down, LLM moves the global mode from secure or bypass to discard.
- If the local link is already down at the time LLM is enabled, the global mode is not updated.
- Once in discard mode, the encryptor does not pass traffic until an administrator or supervisor logs in and changes the global mode back to secure.



An administrator can change the global mode from discard to secure or bypass even while LLM is enabled and the local link is down.

LLM is configured using the CLI `linkspeed` command with the `-m` flag.

Link Loss Forwarding (LLF)

Link Loss Forwarding is used on optical Ethernet links to propagate a loss of received signal on one port to the transmitter on the opposite port. This enables upstream and downstream network equipment to detect the failure and take appropriate action, such as switching to alternative network paths.

For example, a loss of Rx signal on the network port is forwarded to the local port by turning off the Tx laser on the local port.

Link loss can be propagated in a single direction or in both directions. The following options are available via the CLI `linkspeed -f` command:

Table 49. LLF direction options

Option	Description
Disabled	LLF is not active.
Propagate Net→Loc	Network port signal loss is forwarded to the local port.
Propagate Loc→Net	Local port signal loss is forwarded to the network port.
Propagate Loc↔Net	Signal loss is propagated in both directions.



LLF is available on optical links only. It is not supported on copper interfaces.

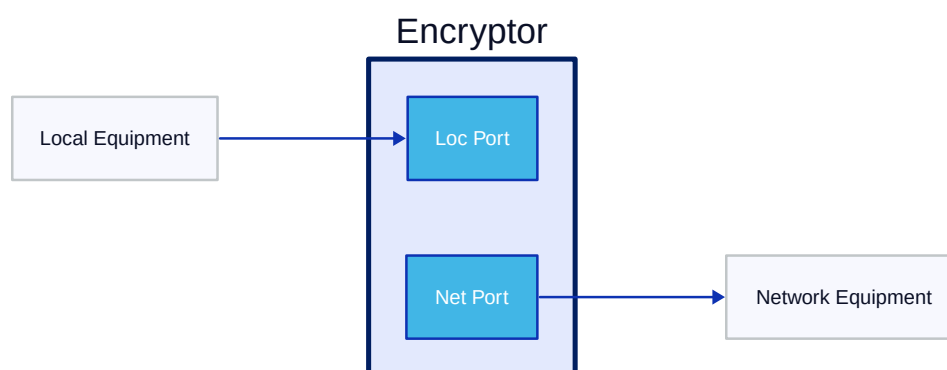


Figure 33. LLF disabled — no signal propagation

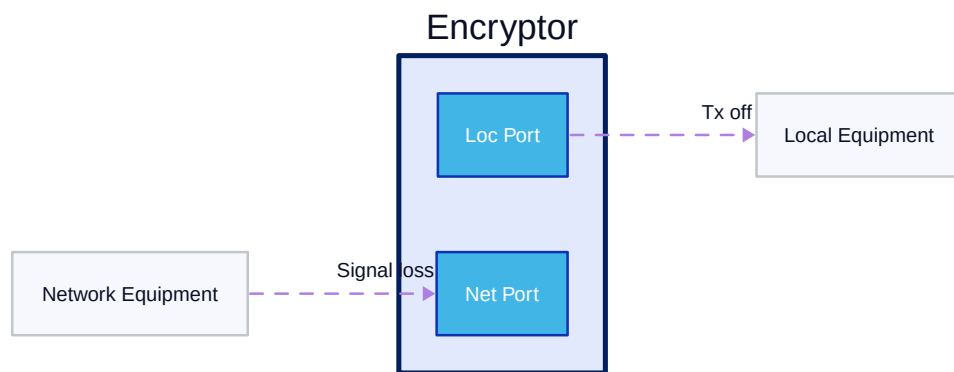


Figure 34. LLF Net to Loc — network signal loss forwarded to local port

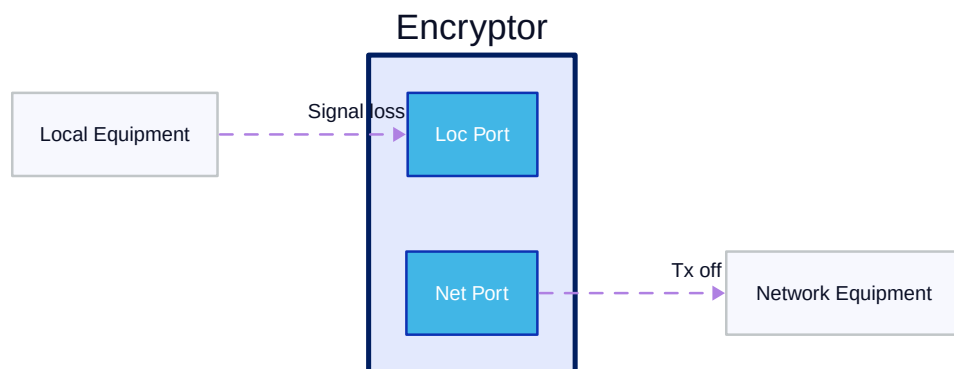


Figure 35. LLF Loc to Net — local signal loss forwarded to network port

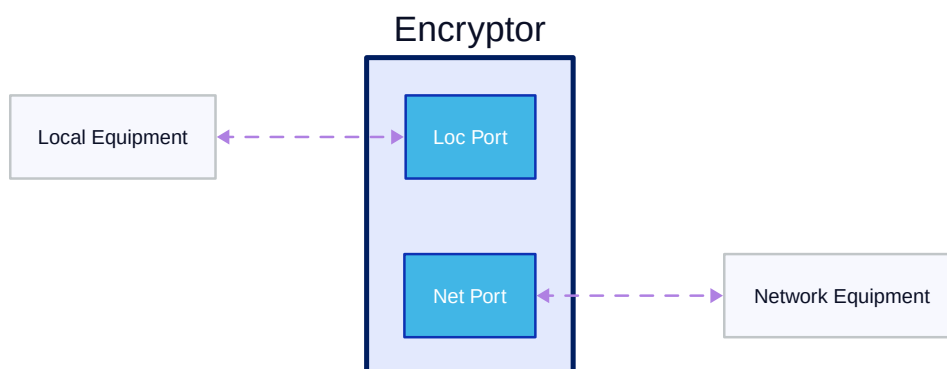


Figure 36. LLF bidirectional — signal loss propagated in both directions

Connection-Status-Tied LLF

In point-to-point (line) mode, LLF can be tied to connection status. When enabled, the local port Tx laser is not turned on (indicating link up) until the encryptor has successfully completed key negotiation and is ready to pass traffic securely.

This prevents upstream equipment from forwarding traffic before the encrypted connection is established.

Configure this option using the CLI `linkspeed -c` command.

8.1.6. Operational Modes During Failure

The CN4020 operation mode is a global selector that controls traffic handling. The mode determines how the encryptor responds when a failure or state change occurs.

The following modes are available:

Bypass

All traffic passes through the encryptor without encryption. The Secure LED flashes red (not activated) or amber (activated).

Discard

All traffic is dropped. The Secure LED is solid red (not activated) or solid amber (activated).

Secure (Encrypt All)

Frames are processed according to the configured encryption policy. The Secure LED is solid green (certificates loaded) or flashing green (no certificates loaded, for example in TIM mode).

The operation mode can be set via the CM7 Policy tab or the CLI `global` command. The initial mode depends on factory settings and is either bypass or discard.

When the mode is changed to secure, the following transitions occur:

1. Connection and tunnel discovery commences.
2. Ethertype policy is applied.

The following HA mechanisms interact with the global operation mode:

- **LLM** — forces the mode to discard when the local link is lost (see [Local Link Monitoring \(LLM\)](#)).
- **STP monitoring** — purges local MAC addresses on topology change, triggering re-discovery (see [Spanning Tree Protocol \(STP\) Monitoring](#)). The global mode is not changed.
- **Power loss recovery** — connections are re-established automatically when power returns; the mode is preserved from prior configuration.

Table 50. Secure LED states

LED State	Condition	Description
Solid Red	Not activated	Traffic is being discarded.
Flashing Red	Not activated	Traffic is being bypassed.
Solid Amber	Activated	Traffic is being discarded.
Flashing Amber	Activated	Traffic is being bypassed.
Solid Green	Activated, certificates loaded	Operating securely.
Flashing Green	Activated, no certificates	Operating securely (for example, in TIM mode).

Chapter 9. Monitoring & Statistics

9.1. Monitoring & Statistics

This chapter describes how to monitor the CN4020, view operational statistics, and interpret alarms and log data. Monitoring is available through CM7, the CLI, SNMP, and the RESTful JSON interface.

For SNMP and syslog server configuration, see [Management & Administration](#). For encryption mode and replay protection configuration, see [Encryption Configuration](#). For network interface configuration, see [Network Configuration](#).

9.1.1. Dashboard and System Status

The CM7 Manage screen provides a real-time view of the CN4020 status. The following displays are available from the Manage screen selectors.

Front Panel Mimic

The Front Panel Mimic displays a virtual representation of the front panel of the selected encryptor. The display includes the state of all LEDs and the content of the LCD, providing a remote view of the unit's operational status.



The appearance of the front panel mimic varies by encryptor model and type.

Overview Display

The Overview selector displays encryptor identification and descriptive information.

Description

The encryptor model and protocol.

Contact

Contact information such as a responsible person, department, and telephone number. This field is editable.

Name

The name that identifies the encryptor. From firmware version 2.6.0/4.6.0 onward, the name conforms to RFC 1035 section 2.3.1: only alphanumeric characters, hyphens (-), and dots (.) are permitted, and these must not appear in the first or last positions.



This name is distinct from the CLI prompt name, which is set using the CLI `prompt` command.

Comment

A free-text comment stored in the encryptor and included in configuration detail exports.

Vendor

A manufacturer-generated identification string.

Firmware

The firmware version, hardware version, and serial number of the unit.

System Status

The System display provides system-level information and shows the status of hardware modules.

Local Time

The current date and time. This can be set manually or updated automatically via NTP.

Access Locking

- **Front Panel Keypad** — locks the front panel to prevent configuration changes.
- **Front Panel USB** — locks the USB socket so that inserted USB drives are ignored. The USB socket must be unlocked before loading firmware upgrades.



Only USB drives formatted with FAT or FAT32 are supported.

FIPS PUB 140-3 Mode

Enables or disables FIPS mode. FIPS mode is enabled by default.

Entropy Pool

Displays the status of a user-provided entropy pool when enabled. See [Entropy Pool Statistics](#) for the available pool statistics.

Restart Encryptor

Restarts the encryptor with an option to erase the unit first. A confirmation dialog is displayed before the restart proceeds. Following a non-erase restart, the unit re-establishes connections based on current mode and policy settings.

Hardware Modules

The System display shows details for each hardware module installed in the encryptor:

- **Management Module** — management processor details
- **Interface Module (Network)** — network-side interface module details
- **Interface Module (Local)** — local-side interface module details

Each module entry includes the following fields:

Field	Description
ID	Unit identifier within the encryptor
Physical Location	Module location within the chassis

Field	Description
Board Number	Manufacturing code identifying the module type
Description	Functional description of the module
Serial Number	Unique serial number of the module
Software Version	Version of software loaded on the module
Build ID	Build identifier of the software
Build Number	Build sequence number
Build Date and Time	Date and time the software build was performed

Utilization

The Utilization pane displays real-time traffic metrics for both ingress and egress ports in both directions.

Long-Term Logging

The Utilization display includes a long-term logging facility that records utilization statistics over extended periods. This feature uses the CM7 OID Logger service (*CM0idLoggerService*), which runs independently of CM7 and writes utilization values to a CSV file.



SNMPv1 must be enabled for long-term logging to function.

To use long-term logging:

1. Click **Logging: Start** to begin logging for the selected encryptor.
2. Click **Logging: Stop** to end logging.
3. Click **Logging: View** to open the CM7 OID Logger window, which displays logged values in both numeric and graphical format.

The OID Logger supports the following additional capabilities:

- Add any OID for long-term logging
- Right-click any panel on the Manage window to add or remove OIDs from the OID Logger
- Enable or disable logging per IP address

9.1.2. Interface Status

The Encryption Interfaces display provides status and monitoring information for the local and network data interfaces.

Navigate to the Encryption Interfaces option in the CM7 Manage screen to view the following status information:

Maximum Link Capability

The maximum speed the link can operate at.

Current Link Status

The current status of the link, including local and network port states.

Link Status

The current speed and mode of the link.

Network Interface Status

The speed and operational status of the network port.

Local Interface Status

The speed and operational status of the local port.

Configured Link Speed

The configured link speed setting.

Auto-Negotiate Port Speed

When enabled, the unit communicates with the connected device to determine the correct operating speed.

Local Link Monitoring

Local Link Monitoring (LLM), when enabled, sets the unit into global discard mode if a link loss is detected on the local port. Once in discard mode, the unit does not pass traffic until an administrator or supervisor user resets the unit to encrypt.



If the local link is already down when LLM is enabled, the global mode is not updated. LLM only triggers on a link transition from up to down.



An administrator can change the global mode from discard to secure or bypass even if LLM is enabled and the local link is down.

Link Loss Forwarding

Link Loss Forwarding (LLF) propagates link state across the local and network ports of the encryptor. Separate settings are available for optical and electrical interfaces.

Optical LLF

Controls optical Link Loss Forwarding. Loss of an optical signal on one port results in the signal being turned off at the other port. Available settings:

- **Local** — loss at the local port turns off the network port laser
- **Network** — loss at the network port turns off the local port laser
- **Bi-directional** — loss at either port turns off the other port's laser

Optical LLF Tied to Session

When enabled, the output laser does not turn on until a secure connection is re-established.

Electrical LLF

For units with RJ45 interfaces. Loss of the input connection on either port drops the output on the opposite port.

Electrical LLF Tied to Session

When enabled, the link remains down until a secure connection is re-established.



LLF only operates if the local and network ports use the same media type (both copper or both optical).

For interface configuration procedures, see [Network Configuration](#).

9.1.3. Statistics

The CN4020 provides detailed traffic and operational statistics accessible through CM7 and the CLI. Statistics are organized by interface: management port, local (trusted) interface, and network (untrusted) interface.

Management Port Statistics

The management port statistics are available via SNMPv3 or the CLI.

Table 51. Management port — Ethernet statistics

Statistic	Description
MAC Address	MAC address of the management port
Operating Mode	Current operating mode of the encryptor
Current Link Rate	Current link rate
Configured Link Rate	User-specified speed negotiation setting
Partner Link Rate	Link rate of the management link partner

Table 52. Management port — IP statistics

Statistic	Description
Packets In	IP packets received
Packets Out	IP packets sent
Header Errors	IP packets with header errors
Address Errors	IP packets with address errors
Discards	IP packets discarded

Table 53. Management port — ICMP statistics

Statistic	Description
Messages In	ICMP messages received
Messages Out	ICMP messages sent
Errors	Errors detected in ICMP messages

Table 54. Management port — UDP statistics

Statistic	Description
Datagrams In	UDP datagrams received
Datagrams Out	UDP datagrams sent
Errors	Errors in UDP datagrams

Local Interface Statistics

The local (trusted) interface statistics are accessed using CM7 or the CLI.

Table 55. Local interface — Rx statistics

Statistic	Description
Buffer Overflow Count	Frames received and discarded due to internal buffer overflow
Interframe Gap Errors	Frames received after a minimum interframe gap violation
Octet Count	Total octets received
Frame Count	Total frames received
FCS Errored Frames	Frames received with FCS errors
PCS Errored Frames	Frames received with PCS (data) errors
Undersized Frames	Frames received with fewer than 64 octets
Oversized Frames	Frames received with more than 1536 octets
Discarded Frames	Frames discarded due to policy settings
Bypassed Frames	Frames that bypassed encryption processing
PCS Sync State	Current synchronization state of local port communications

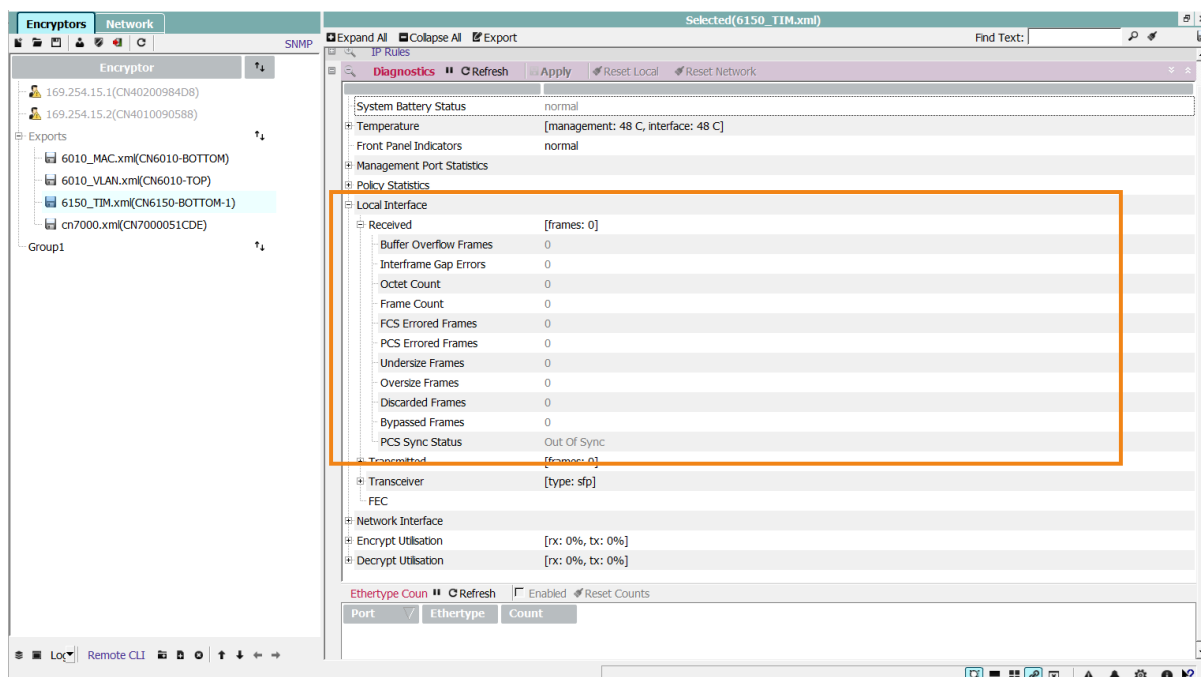


Figure 37. Local interface diagnostics — Rx statistics

Table 56. Local interface — Tx statistics

Statistic	Description
Octet Count	Total octets transmitted
Frame Count	Total frames transmitted
FCS Errored Frames	Frames transmitted with FCS errors

Network Interface Statistics

The network (untrusted) interface statistics are accessed using CM7 or the CLI. The network interface includes additional counters for management frames, encryption overhead, and replay protection.

Table 57. Network interface — Rx statistics

Statistic	Description
Buffer Overflow Count	Frames received and discarded due to internal buffer overflow
Interframe Gap Errors	Frames received after a minimum interframe gap violation
Octet Count	Total octets received
Frame Count	Total frames received
FCS Errored Frames	Frames received with FCS errors
PCS Errored Frames	Frames received with PCS (data) errors
Undersized Frames	Frames received with fewer than 64 octets
Oversized Frames	Frames received with more than 1536 octets

Statistic	Description
Discarded Frames	Frames discarded due to policy settings
PCS Sync State	Current synchronization state of network communications
Manage Octet Count	Management octets received (in-band management traffic)
Manage Frame Count	Management frames received
Manage Drop Frames	Management frames dropped due to internal processes
Shim Octet Count	Crypto overhead octets (shim and authentication trailer) per encrypted/decrypted frame
Replay Errors	Frames where the shim counter has been observed before (replayed packets)
Skipped CTR Errors	Frames where the shim counter is greater than expected at the receiver
Auth Failed Errors	Frames that failed authentication
Reordered Frames	Frames where the shim counter is less than the previous greatest received value but within the replay acceptance window
Out of Reorder Window Frames	Frames where the shim counter is more than 256 behind the previous greatest received value
Encrypted Octets	Total encrypted octets
Encrypted Frames	Total encrypted frames

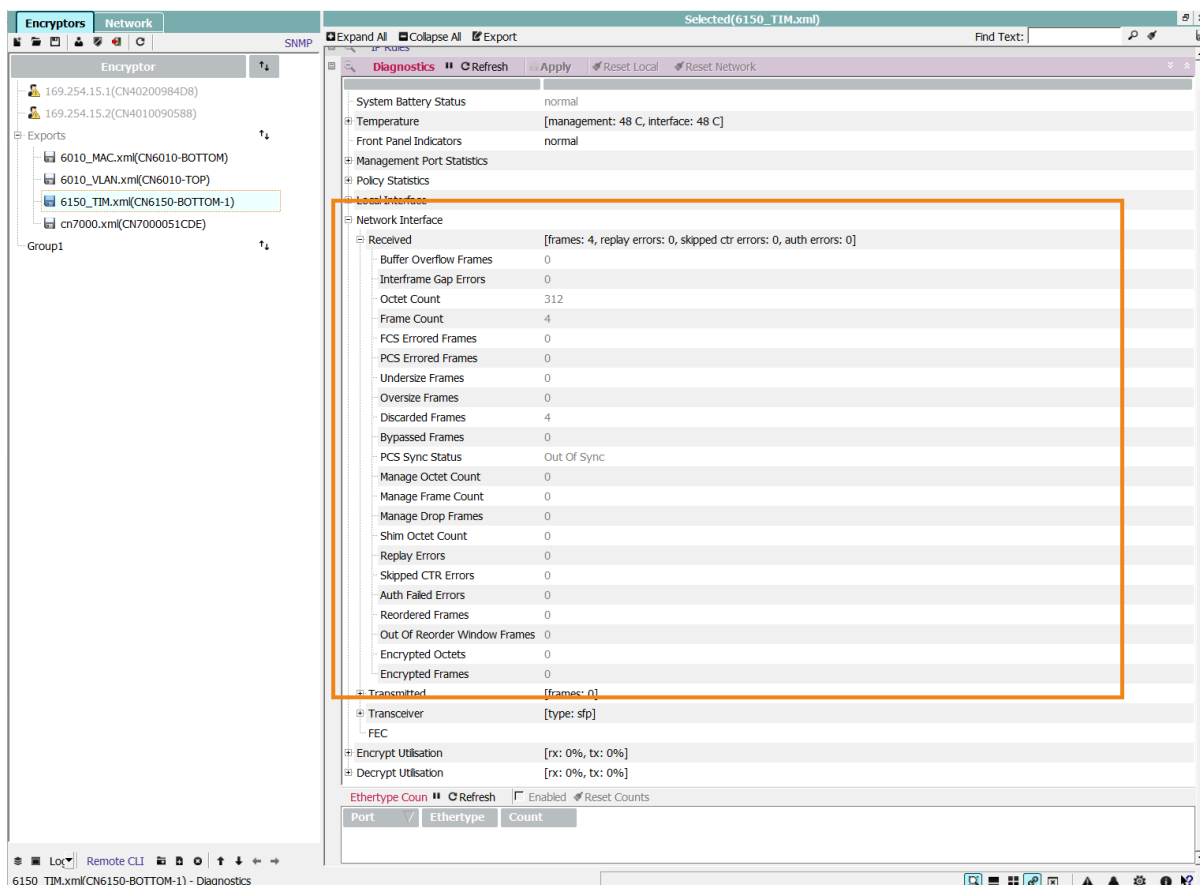


Figure 38. Network interface diagnostics — Rx statistics

Table 58. Network interface — Tx statistics

Statistic	Description
Octet Count	Total octets transmitted
Frame Count	Total frames transmitted
FCS Errored Frames	Frames transmitted with FCS errors
Manage Octet Count	Management octets transmitted
Manage Frame Count	Management frames transmitted

Path MTU Discovery Statistics

When Path MTU Maximum (PMTUM) is enabled in TIM mode, the CN4020 tracks MTU-related events. These statistics are available via the CLI `stats` command or through the CM7 Diagnostics pane.

PMTU Max Tx Frames

Number of valid ICMPv4 PMTUD packets sent by the CN4020 to source hosts. Increments each time the encryptor generates an ICMP Type 3, Code 4 (Fragmentation Needed) message in response to an oversized packet.

IP MTU Exceeded Frames

Number of IPv4 packets received that exceeded the configured Path MTU Maximum threshold.



On FPGA-based models, this statistic increments even when the PMTUM feature is disabled, serving as a passive warning of potential packet loss due to encryption overhead.

For configuration details, see [MTU Handling and Encryption Overhead](#) in Chapter 7.

Replay Protection Statistics

Replay protection detects replayed packets and discards them instead of decrypting. Three statistics assist with replay and reordering diagnostics. These statistics are available via the CLI `stats` or `stats-n` command or through the CM7 Diagnostics pane under the Network Received section.



These three statistics are only valid on the decrypt data path.

Replay Errors

Increments when the counter in the received shim has been observed before. This counter increments only for replayed packets.



If a frame fails authentication and is deemed to be replayed, only the Auth Failed Errors statistic increments.

Reordered Frames

Increments when the received shim counter value is:

- less than the greatest previously received value, and
- within the replay acceptance window (256 frames wide)

Reordered frames are not discarded. This counter indicates that frame reordering has occurred in the network.

Out of Reorder Window Frames

Increments when the received shim counter value is more than 256 behind the greatest previously received value. These frames are discarded when replay protection is set to `window` mode.



If a frame fails authentication and is deemed out of the reorder window, only the Auth Failed Errors statistic increments.

The following table shows which replay protection modes are supported for each combination of operational mode and configuration settings.

Table 59. Replay protection mode support by operational mode

Operational Mode	Connection Type	Sender ID	MTU Overflow Protection	Shim Rate	Crypto Mode	Strict	Window	Disabled
Line	NA	Off	NA	NA	CFB	N	N	Y (default)
Line or TRANSEC	NA	Off	Don't care	!= 1	CTR or GCM	Y (default)	N	Y
Line or TRANSEC	NA	Off	Off	1	CTR or GCM	Y	Y (default)	Y
Line	NA	Off	On	1	CTR or GCM	Y (default)	N	Y
MAC (unicast)	Unicast	Off	Don't care	Don't care	CTR or GCM	Y (default)	N	Y
MAC (group key)	Group key	Off	Off	1 (FPGA)	CTR or GCM	N	N	Y (default)
VLAN (Sender ID off)	Group key	Off	Off	1 (FPGA)	CTR or GCM	N	N	Y (default)
VLAN (Sender ID on)	Group key	On	Off	1 (FPGA)	CTR or GCM	N	Y (default)	Y
TIM	NA	On	Off	1 (FPGA)	CTR or GCM	N	Y (default)	Y

For replay protection configuration, see [Encryption Configuration](#).

Entropy Pool Statistics

When a user-provided entropy pool is enabled, pool consumption statistics are available via CM7 or the CLI.

Table 60. Entropy pool statistics

Parameter	Description
Entropy Pool	Enabled or disabled
Size (bytes)	Total size of the entropy file
Bytes Remaining	Remaining bytes before pool exhaustion

Parameter	Description
Bytes Used	Bytes consumed to date
Percent Used	Percentage of pool exhausted
Estimated Days Remaining	Based on the current consumption rate over a 7-day rolling window (allow 24 hours for initial calculation)

Alarms are generated when entropy pool consumption reaches 80%, 85%, 90%, 95%, and 100%.

For entropy pool configuration, see [Maintenance](#).

Resetting Statistics

Statistics counters can be reset from the CM7 Diagnostics pane.

The **Reset Local** button clears:

- Local port statistics
- Local ethertype statistics (TIM operational mode only)
- Local IP Rules table statistics

The **Reset Network** button clears:

- Network port statistics
- Network ethertype statistics (TIM operational mode only)
- Network IP Rules table statistics
- Tx and Rx tunnel/connection statistics

9.1.4. Diagnostics

The Diagnostics display in CM7 provides hardware health information and detailed interface statistics in a consolidated view. The display is organized into three areas: system health (battery, temperatures, front panel indicators, and management port), local interface, and network interface.

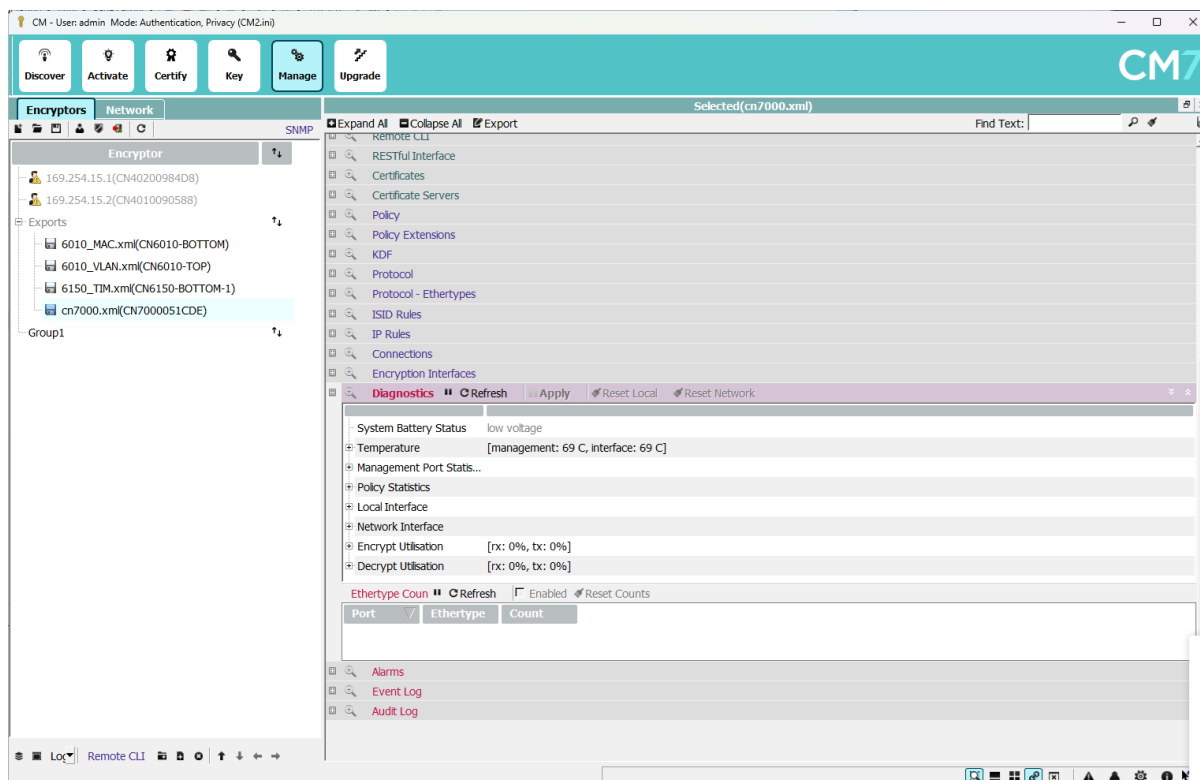


Figure 39. Diagnostics overview

System Health

System Battery Status

Indicates whether the battery is normal or requires replacement.

Temperature

Displays the internal temperatures of the encryptor:

- **Management Module** — temperature of the management module
- **Interface Module** — temperature of the interface module

Front Panel Indicators

The Diagnostics display shows the current state of all front panel indicators. This provides a consolidated view of LED states for remote monitoring without physical access to the unit.

Ethertype Counts

The lower portion of the Diagnostics display shows ethertype counts, which can be enabled to display the ethertypes of all traffic passing through the encryptor.



Ethertype counts are not available on 100 Gbps encryptors.

9.1.5. Alarms

The CN4020 generates alarms to indicate conditions that require operator attention. Alarms are stored in the encryptor and are accessible via CM7, the CLI, SNMP, and the REST API.



Only a user with administrator or supervisor privileges can acknowledge alarms.

Alarm States and Lifecycle

Each alarm exists in one of the following states:

Table 61. Alarm states

State	Meaning
Active unacknowledged	Alarm condition is currently active and has not been acknowledged by a user
Active acknowledged	Alarm condition is currently active and has been acknowledged by a user
Inactive unacknowledged	Alarm condition has cleared but was not acknowledged before it became inactive
Inactive	Alarm condition has cleared and all previous alarms have been acknowledged

When an alarm becomes active:

1. The alarm is listed in the alarm table.
2. The alarm LED on the front panel updates (see [Alarm LED Behaviour](#)).
3. A record is added to the event log indicating that the alarm was set.
4. When the alarm condition clears, an event is logged indicating that the alarm was cleared.

An active alarm remains in the alarm table until acknowledged by a user, even if the alarm condition itself has cleared.

Alarm LED Behaviour

The alarm LED on the front panel indicates the aggregate alarm status with the following precedence:

LED State	Meaning
Flashing red	At least one active unacknowledged alarm exists
Solid red	At least one active acknowledged alarm exists
Flashing orange	At least one inactive unacknowledged alarm exists
Green	No alarms present

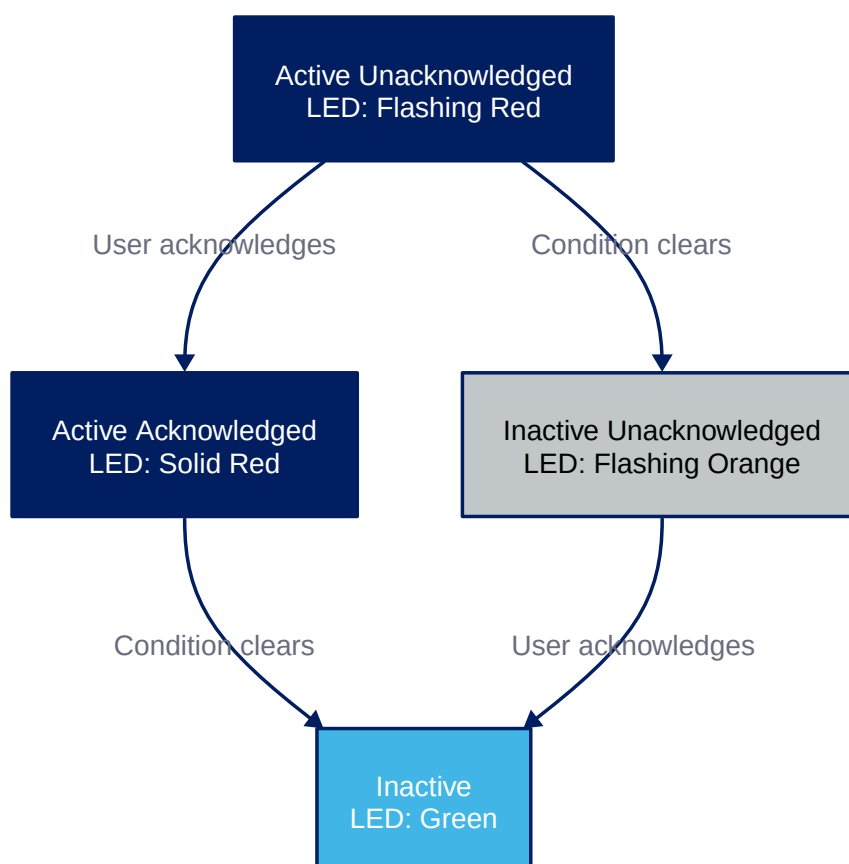


Figure 40. Alarm state lifecycle and LED indicators

Viewing and Acknowledging Alarms

To view and acknowledge alarms in CM7:

1. Navigate to the **Alarms** option in the Manage screen.
2. The alarm table displays the following fields:
 - **ID** — sequential index of the alarm entry
 - **Time** — date and time the alarm was raised
 - **Description** — description of the alarm condition
 - **State** — current state (active/inactive, ACK/NAK)
3. To acknowledge alarms, select individual alarms or use **Acknowledge All**.
4. Click **Refresh** to update the alarm display.

9.1.6. Event and Audit Logs

The CN4020 maintains two separate logs in non-volatile memory: an event log and an audit log. Both logs are preserved across power cycles.

Each log can contain a maximum of 4000 records. When a log becomes full, it can be configured to either overwrite the oldest records (wrap enabled) or stop logging new records (wrap disabled). This setting is configured through CM7 or the CLI.

Every log record is time-stamped. Both logs can be viewed from CM7, the CLI, or remotely via SNMP.



The logs should be maintained and regularly examined to ensure undesired events are detected.

Event Log

The event log records significant system events such as power-up, self-test results, and alarm conditions being set or cleared.

Each entry includes:

- **ID** — sequential number identifying the order in which the event was logged
- **Time** — date and time the event occurred
- **Description** — description of the event

Example event log entry:

```
2004-09-14 11:48:40 Alarm cleared: Network interface path RDI
```

Audit Log

The audit log records all configuration changes made to the encryptor. Each entry includes the name of the user who made the change and a description of the change.

Each entry includes:

- **ID** — sequential number identifying the order in which the operation was logged
- **Time** — date and time the operation was performed
- **Description** — the user identifier and the operation performed

Example audit log entry:

```
2004-09-08 09:40:19 admin: E3/T3 configuration on network port changed:  
Tx clock source: internal, Loopback: none, Payload scrambling: enabled,  
HCS coset addition: enabled, framing: E3 6832 ADM
```

Viewing, Filtering, and Exporting Logs

To view logs in CM7:

1. Navigate to the **Event Log** or **Audit Log** option in the Manage screen.
2. Use the **Description Filter** field to search for entries matching a specific term. Matching entries are highlighted.
3. Click **Save** to export the log to a text file.
4. Click **Clear** to remove all entries from the selected log.



Only a user with administrator privileges can clear the event and audit logs.

9.1.7. SNMP Trap Monitoring

The CN4020 sends SNMP traps as asynchronous notifications when alarm conditions are set or cleared.

Encryptors send SNMPv2 enterprise-specific trap messages to all defined trap handlers. Each trap message contains the text of the alarm description. Up to eight trap handler IP addresses can be defined and enabled.

CM7 can operate as a trap handler, displaying the alarm status of multiple encryptors. Third-party network management systems (such as IBM Tivoli or NetView) can also receive and process these traps.



In a Linux environment, CM7 trap listening requires root privileges.



When changing the trap port number, disable traps before changing the port and re-enable them afterward.

For SNMP trap handler configuration, see [Management & Administration](#).

9.1.8. Syslog Integration

The CN4020 can forward events to an external syslog server for centralised log management and long-term retention. Syslog integration enables security information and event management (SIEM) platforms to collect and correlate encryptor events with other network infrastructure events.

For syslog server configuration, see [Management & Administration](#).

9.1.9. REST API Monitoring

The RESTful HTTP(s) interface provides programmatic access to encryptor monitoring data. The interface leverages the existing SNMP MIB, enabling OID-based queries via URL parameters using textual OID representations.

Access to the RESTful interface requires user authentication via console access credentials.

For REST API configuration, see [Management & Administration](#).

The following monitoring functions are available through the REST API:

Alarm Monitoring

The **AlarmGroup** OID provides the status of all encryptor alarms. Most alarm tables include a count scalar variable for monitoring.

Certificate Monitoring

Certificates can be monitored via the REST API with particular focus on:

- **CertificateState** — current state of each certificate
- **CertificateDaysLeft** — days remaining before certificate expiry

Audit and Event Log Monitoring

The audit and event logs can be queried via the REST API. While centralised syslog server configuration is the preferred approach for log aggregation, the REST API provides an alternative for programmatic log access.

Connection Status

Connection status tables are specific to the protocol and operational mode selected. The connection status field (for example, **gEthVLANConnCiStatus** in VLAN mode) indicates whether each connection is active.

Interface Status

The REST API provides access to the link status of both the local and network interfaces.

Chapter 10. Maintenance

10.1. Maintenance

This chapter describes maintenance procedures for the CN4020, including firmware upgrades, configuration export and import, licensing, entropy management, FIPS mode configuration, emergency erase, and powering down.

For monitoring entropy pool statistics, see also [Monitoring & Statistics](#). For certificate management, see [Management & Administration](#).

10.1.1. Firmware Upgrades

Firmware upgrades are installed to provide additional functionality or address known limitations. They are provided either under a maintenance agreement or to fulfil a customer order.



Upgrading an encryptor does not change the configuration. All certificates, connections, user accounts, and configuration information are retained from the old to the new firmware version.

Upgrade Image Formats

All upgrade images are generated and supplied by Senetas or Senetas' trusted representatives. Never attempt to load an upgrade image obtained from any other source into an encryptor.

Upgrade images are supplied encrypted with a Senetas key (using Triple DES) to ensure confidentiality during transit. During the upgrade process, the new firmware image is decrypted, decompressed, and stored internally in non-volatile memory.

Senetas provides two upgrade image formats:

Standard images (.img)

The original format. Naming convention: `<Platform>_<Variant>-<Version>.<Delta>-<Date>-<Time>.tar.gz.img`

Example: `CN6010_A-5.5.1.D003-20230210-054031.tar.gz.img`

Quantum-ready images (.qimg)

Signed by a private key generated from the quantum-resistant algorithm Falcon-1024. Naming convention: `<Platform>-<Version>.<Delta>-<Date>-<Time>.tar.gz.qimg`

Example: `CN6010-5.4.0.D11602-20230210-054031.tar.gz.qimg`



Encryptors will support both formats for the next few releases, after which support for the older format (.img) will be deprecated.



Firmware versions prior to v5.5.x cannot use .qimg images. You must first upgrade

to v5.5.x using a **.img** image before **.qimg** images will be recognised.



All firmware images provided by Senetas have a **.IMG** extension. Encryptors running earlier releases that use the deprecated **.CTAM** or **.SFNT** extension must first be upgraded to a release that recognises **.IMG** images.

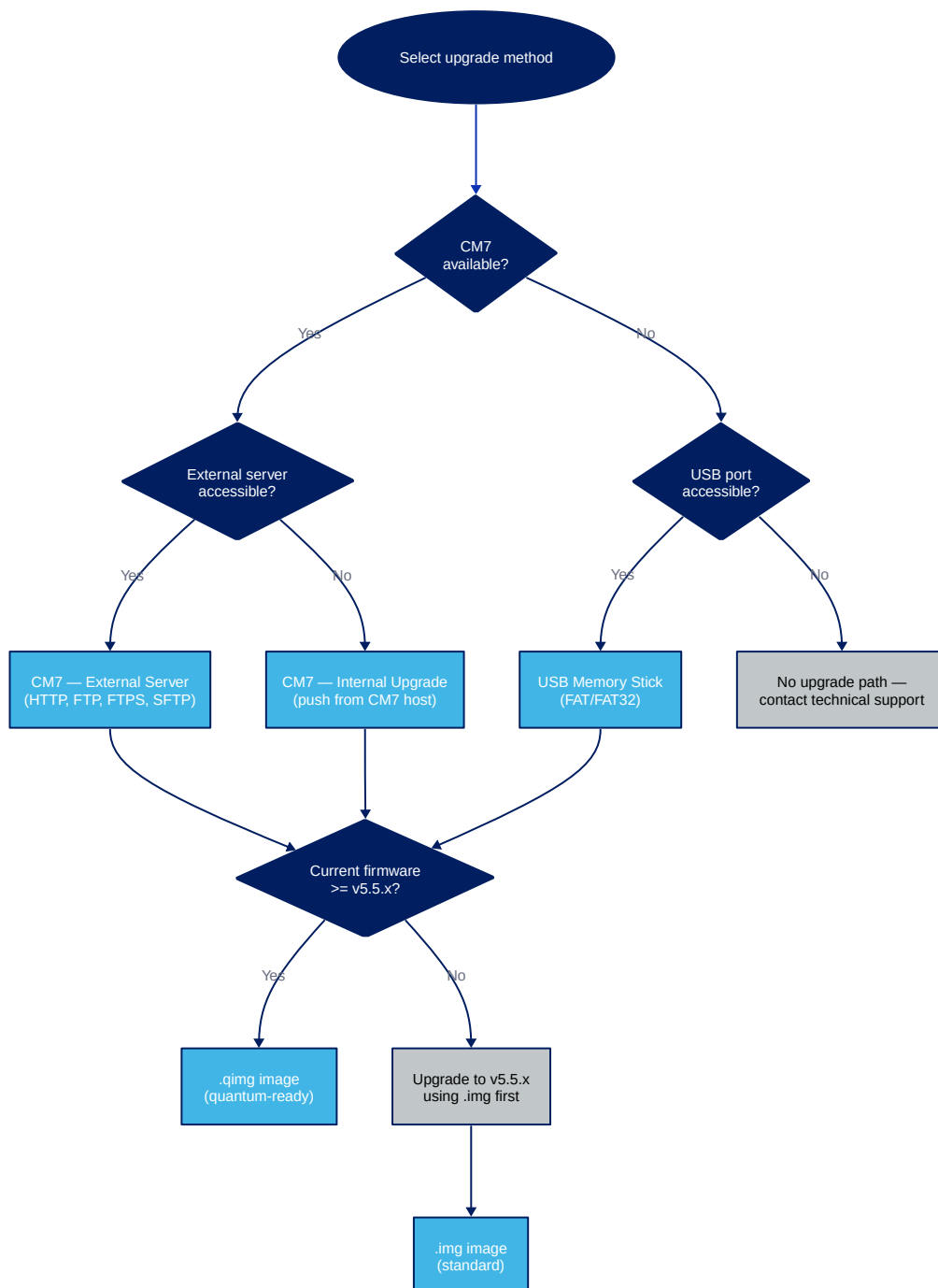


Figure 41. Firmware upgrade method selection

Pre-Upgrade Checklist

Before performing a firmware upgrade:

- Verify that the default certificate on the encryptor has not expired. An upgrade requires a reboot, and the encryptor will check the validity of the default certificate on restart. If the certificate has expired, traffic will not restart after the reboot.
- Schedule the upgrade during a maintenance window. The new firmware image is not used until the encryptor is restarted, allowing you to stage upgrades across multiple encryptors and perform a coordinated restart.
- Confirm that the upgrade image file was obtained from Senetas or an authorised representative.

Upgrading via CM7 — External Server

An upgrade image hosted on an external server can be loaded into the encryptor using the CM7 Upgrade screen.

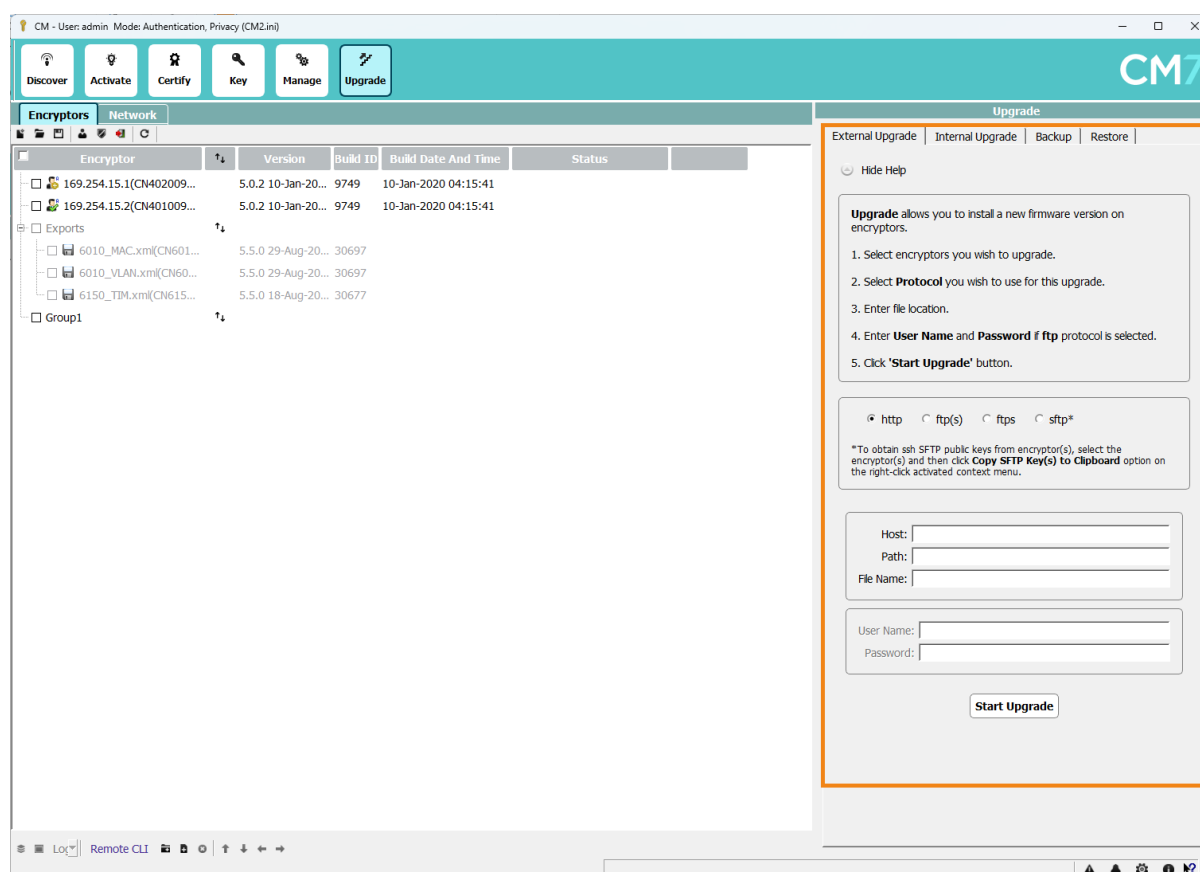


Figure 42. External upgrade dialog



CM7 currently supports only Ethernet encryptors with X.509 certificate support for this procedure.

1. In CM7, navigate to the **Upgrade** screen.
2. Select the protocol for the file transfer:

HTTP

Standard HTTP download.

FTP(S)

Uses unencrypted FTP if no certificate is configured in the FTP server table. If a certificate is configured, encrypted FTPS (explicit, port 21) is used.

FTPS

Always uses encrypted FTPS (implicit, port 990). A certificate must be configured in the encryptor's FTP server table.

SFTP

Secure FTP.

3. Enter the **Host** (IP address of the server hosting the image).
4. Enter the **Path** (location of the file on the server).
5. Enter the **File Name** (name of the upgrade image).
6. Enter the **User Name** and **Password** for server access.
7. Initiate the upgrade.



When upgrading an encryptor over in-band management, the file transfer may take longer than five minutes.

CM7 indicates upgrade progress on all screens by displaying a coloured background for the encryptor:

- **Green** — upgrade in progress or successfully completed
- **Red** — upgrade failed

Upgrading via CM7 — Internal Upgrade

The internal upgrade method allows the upgrade image to be pushed from the CM7 host to the encryptor.

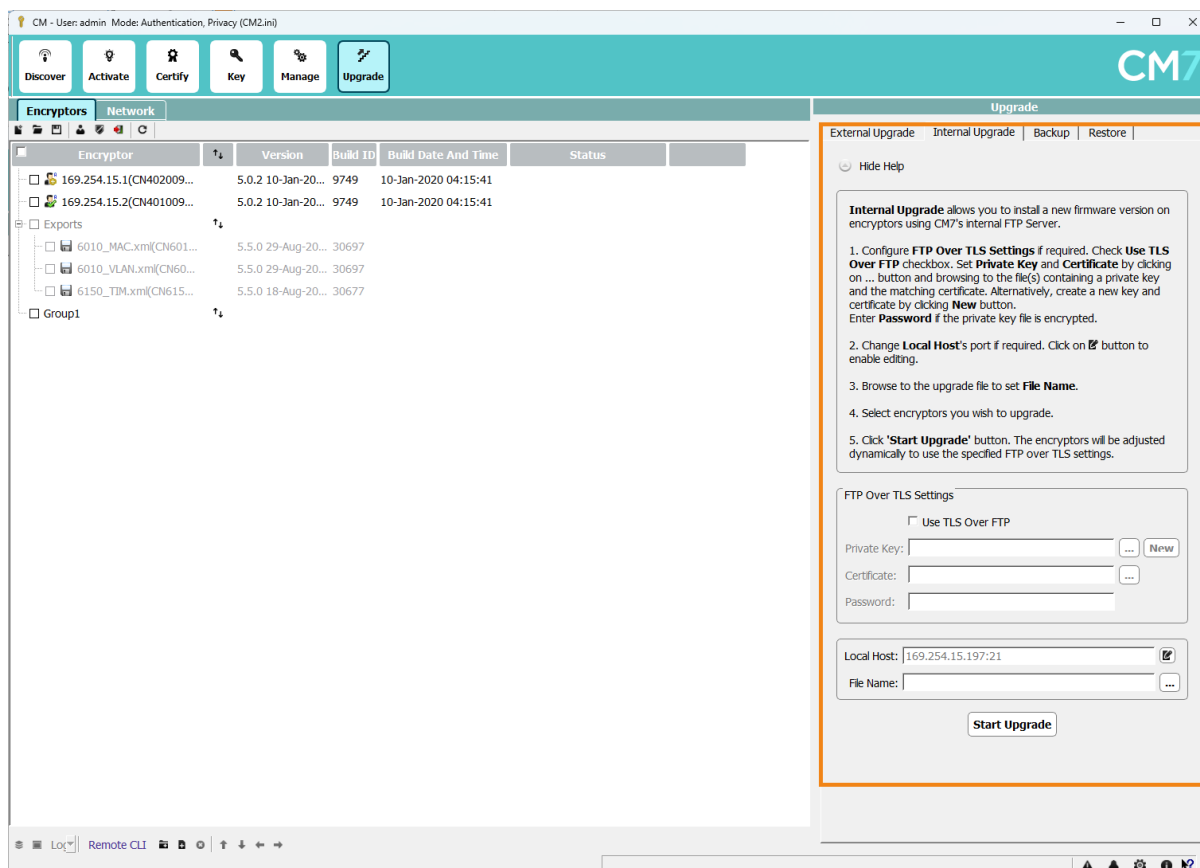


Figure 43. Internal upgrade dialog

1. In CM7, navigate to the **Upgrade** screen and select **Internal Upgrade**.
2. Configure the required fields:

Private Key

The private key for the transfer.

Certificate

The certificate for the transfer.

Password

The password that allows access to the server.

Local Host

The local host address.

File Name

The name of the upgrade image.

3. Initiate the upgrade.

Upgrading via USB

An upgrade image stored on a USB memory stick can be loaded into the encryptor via the device's USB port.



Senetas encryptors support only USB drives formatted with FAT or FAT32.

1. Obtain a valid upgrade image from Senetas.
2. Copy the image file to the root directory of a USB memory stick. Ensure that there is only one upgrade image file in the root directory, or the wrong image may be used.
3. Insert the USB memory stick into the encryptor USB port.
4. Use the CLI **upgrade** command to initiate the upgrade (see [Upgrading via CLI](#)).

The upgraded firmware image is not used until the encryptor is restarted. This can be done immediately or at a later time.

Upgrading via CLI

The **upgrade** command initiates a firmware upgrade using an image supplied via a USB memory stick. This provides an alternative means of installing firmware on encryptors that do not have a front panel keypad.

Precondition: You must be logged in with an **admin** account.

```
upgrade
```

The encryptor searches the USB memory stick for a valid upgrade image and begins the transfer process.

Post-Upgrade Verification

After upgrading:

1. Reboot the encryptor to activate the new firmware.

To coordinate upgrades across multiple units, stage the image on all encryptors first, then perform a network-wide restart.

2. Verify the running firmware version:
 - **CM7:** Check the firmware version displayed on the **Overview** or **System** screen.
 - **CLI:** Run the **version** command.
3. Check the event log for any upgrade-related errors.
4. Verify that encrypted traffic is flowing by checking encryption interface statistics.

Firmware Downgrades

While not recommended, there are situations where an encryptor may need to be loaded with an earlier firmware version.



Downgrades from version 5.5.x onwards automatically perform a full erase when the encryptor is next rebooted. This applies only when crossing a major release

boundary, determined by comparing the first two digits of the firmware version number.

Table 62. Downgrade auto-erase rules

From	To	Auto-Erase
5.5.x	5.4.x	No — same major release (5.x)
5.5.x	5.2.x	Yes — different major release

After a downgrade with auto-erase, the encryptor requires full reconfiguration.

10.1.2. Configuration Export and Import

The CN4020 supports exporting and importing configuration data through CM7. These operations use non-secure XML files that capture the encryptor's configuration parameters.



Configuration export files do not contain security information (keys, certificates, or credentials). They are intended for diagnostics and support purposes.

Exporting Configuration

1. In CM7, click the **Export Config** button at the top of the management pane.
2. Save the resulting XML file.

The exported file can be provided to support staff for diagnostic purposes or uploaded to the Customer Support Portal.

Importing Configuration

1. In CM7, select and open the XML file containing the configuration settings.
2. The imported encryptor configuration appears in the left-hand panel of the CM7 interface.
3. Select the specific pane you need to modify.
4. A group of settings (in a pane) can be imported back into one or more encryptors.

10.1.3. Rate Limiting

Rate limiting is a licensing feature that limits the throughput capacity of an encryptor. It can be set at manufacturing time or upgraded via a device-specific licence upgrade file.

Rate limiting uses traffic policing to monitor ingress traffic and ensure the configured licence bandwidth is not exceeded. Traffic exceeding the rate limit is discarded. All traffic, irrespective of policy setting, is included in the bandwidth measurement.

Committed Access Rate (CAR)

Defined as Ethernet Octets in Mbps.

Ethernet Octets per second = Ethernet octets + (Number of Ethernet frames × (Minimum IFG + Preamble length))

Where Minimum IFG = 12, Preamble length = 8.

Burst handling

The encryptor guarantees passing traffic at the CAR and can handle temporary bursts above the CAR. The bucket depth used in the leaky bucket algorithm is approximately 67 Mb. Large sustained bursts (> 67 Mb) above the CAR may lead to packet drops and throttling of the overall output rate.

No traffic smoothing, shaping, or buffering is performed — the latency profile of the traffic is unaltered. If rate limiting is enabled, the network devices connected to the encryptor must perform traffic shaping or policing at or below the CAR.

When policing takes effect, the encryptor generates the following alarm:

ALARM_FPGA_BW_CLIPPING - "WARNING - Bandwidth is being clipped"

The corrective action is to increase the encryptor's licence capacity.

Table 63. Maximum effective throughput by connection mode and encryption mode

Connection Mode	Encryption Mode	Shim Size	Max Throughput (% of CAR)
Point-to-Point (Line)	AES-CTR	32	100%
Point-to-Point (Line)	AES-CTR	1	92%
Point-to-Point (Line)	AES-GCM	32	84%
Point-to-Point (Line)	AES-GCM	1	78%
Multipoint (MAC, VLAN)	AES-CTR	1	92%
Multipoint (MAC, VLAN)	AES-GCM	1	78%
TIM	AES-GCM	1	78%



When rate limiting is applied, burst traffic in excess of the specified limit results in frames being discarded and SNMP traps being generated. If the applications using the link will be impacted by frame loss, apply traffic shaping ahead of the encryptors.

When TRANSEC is enabled, the rate limit applies to the speed at which transport frames are sent, not the speed at which client frames arrive. TRANSEC mode requires substantial traffic bandwidth engineering — refer to [TRANSEC](#) for details.

10.1.4. Entropy Management

Senetas encryptors utilise one or more noise/entropy sources to provide robust, FIPS-approved entropy for generating all key material within the device. The NIST SP 800-90A/B/C standards are implemented and the solution is certified to FIPS 140-3 Level 3.

By default, the encryptor uses internal hardware-based entropy sources. Two alternative entropy mechanisms are available for environments that require external entropy:

- **Bring Your Own Entropy (BYOE)** — load a user-supplied entropy file

BYOE entropy is disabled by default. An erase operation deletes all BYOE entropy files and disables BYOE

Bring Your Own Entropy (BYOE)

BYOE allows you to completely replace the internal entropy source with a user-defined entropy pool.

For full BYOE configuration procedures including file preparation, loading, and verification, see [Appendix C: Crypto-Agility — BYOE](#).

Entropy Monitoring

When the entropy pool is enabled, pool statistics are available via CM7 or the CLI.

Table 64. Entropy pool statistics

Parameter	Description
Entropy pool	Enabled or disabled
Size (bytes)	Total size of the loaded entropy file
Bytes remaining	Remaining bytes before exhaustion
Bytes used	Bytes consumed to date
Percent used	Percentage of the pool exhausted
Estimated days remaining	Based on the current consumption rate over a 7-day rolling window. Allow 24 hours for the initial calculation.

Alarms are generated when consumption reaches the following thresholds: 80%, 85%, 90%, 95%, and 100%.

10.1.5. FIPS Mode

The CN4020 operates in FIPS or non-FIPS mode. When FIPS mode is enabled (the default), the encryptor is in compliance with all security requirements of the FIPS 140 standard.



Changing FIPS mode reboots the encryptor and removes all certificates and user credentials. This is required to ensure the FIPS security requirements are

maintained.

Non-FIPS mode enables the following features:

- Management of encryptors with SNMP privacy options disabled (legacy compatibility)
- Bring Your Own Entropy (BYOE) and Quantum Origin entropy (see [Entropy Management](#))
- Crypto-agility features: S-box Customisation, CSDK, Bring Your Own Curves (see [Appendix C: Crypto-Agility](#))

To view the current FIPS mode:

```
fips
```

To enable FIPS mode:

```
fips on
```

To disable FIPS mode:

```
fips off
```

In normal use, FIPS mode should be enabled.

10.1.6. Emergency Erase and Factory Reset

The CN4020 provides an emergency erase facility that has the same effect as a tamper event. When erased, all key material and user account data are destroyed.



An erase operation destroys all certificates, connections, user accounts, and encryption keys. No traffic will flow through the encryptor after an erase, and the unit requires full reconfiguration.

CLI Erase

The **erase** command erases the encryptor's configuration and reboots to factory default state.

```
erase
```

By default, the configured IP address, connection mode, and any virtual management configuration are preserved.

To perform a full factory reset including front panel IP addresses:

```
erase -f
```

Example

```
CN6010_A>erase
Warning this command will erase the configuration to factory defaults do you wish to proceed ?
(y/n) y
Are you sure ? (y/n) y
Erasing unit and rebooting . . .
```

Front Panel Erase**Front Panel Keypad**

On models with a front panel keypad:

1. Press and hold the **ESC** and **ENT** buttons simultaneously for approximately 10 seconds.
2. The display shows **Erase and reboot?**.
3. Press the **Up** key to display the confirmation prompt.
4. Press **ENT** to confirm the erase. Pressing any other key cancels the operation.

Front Panel Pinhole

All FPGA-based encryptors include a recessed erase button located behind a pinhole on the front panel. This method can be used even when the unit is powered down.

1. Insert a paperclip or similar tool into the erase pinhole.
2. Press and hold the button.
3. The encryptor performs an emergency erase.

10.1.7. USB Port Management

The USB port on the CN4020 can be locked to prevent access to the front panel USB interface. When locked, the encryptor does not respond to any USB device, including memory sticks containing valid firmware upgrades or entropy files.

To view the current USB port status:

```
usb
```

To lock the USB port:

```
usb lock
```

To unlock the USB port:

```
usb unlock
```



If the USB port is locked, you must unlock it before performing a USB-based

firmware upgrade or entropy file load.

10.1.8. Powering Down

The CN4020 requires no special shutdown procedure before removing power. Unlike many networking devices, there is no graceful-shutdown command to issue and no risk of configuration loss or storage corruption from an abrupt power-off: configuration and keys are committed to persistent storage as they are changed.

To power down the CN4020, simply disconnect the power source.



Removing power is not the same as an erase. Powering the CN4020 off and on again preserves its configuration and keys; the encryptor resumes its previous state at the next start-up. To clear configuration and keys, use the erase procedures described in [Emergency Erase and Factory Reset](#).

Chapter 11. Troubleshooting

11.1. Troubleshooting

This chapter provides guidance for diagnosing and resolving common issues with the CN4020.

For event log, alarm, and audit log interpretation, see [Monitoring & Statistics](#). For certificate management procedures, see [Management & Administration](#).

11.1.1. General Troubleshooting Approach

When diagnosing an issue with the CN4020, follow this general approach:

1. Check the **Dashboard** or **Overview** screen in CM7 for system status and active alarms.
2. Review the **Event Log** for error messages (see [Monitoring & Statistics](#)).
3. Verify physical connections — power cables, network cables, SFP/transceiver modules, and front panel LED indicators.
4. Compare the current configuration against the expected configuration.
5. Use the diagnostic tools described in this chapter (ePing, ethertype diagnostics, traffic analysis).
6. If the issue persists, contact Senetas technical support (see [Contacting Senetas Support](#)).

11.2. Management Network troubleshooting

11.2.1. Management Network Port Reference

To allow the CN4020 to communicate with external management and authentication services, ensure that any firewalls within the management network are configured to allow the following default ports and protocols:

Table 65. Default management network ports

Service / Function	Default Port	Protocol	Direction
SNMPv3 Management (CM7 / Third-party)	161	UDP	Inbound
SNMP Traps	162 ^[1]	UDP	Outbound
Secure Shell (SSH) Remote CLI	22 ^[1]	TCP	Inbound
Network Time Protocol (NTP)	123	UDP	Outbound
Syslog Service	514 ^[1]	UDP	Outbound
TACACS+ Authentication	49 ^[1]	TCP	Outbound
RESTful API Server	7437	TCP	Inbound
HTTP CRL Retrieval	80 ^[1]	TCP	Outbound

Service / Function	Default Port	Protocol	Direction
HTTPS OCSP / CRL Retrieval	443 ^[1]	TCP	Outbound
Quantum Key Distribution (QKD) HTTPS	443	TCP	Outbound
File Transfer (FTP / SFTP / FTPS)	21 ^[1] / 22 ^[1] / 990 ^[1]	TCP	Inbound/Outbound
CipherTrust / KeySecure (KMIP)	5696 ^[1]	TCP	Outbound



SNMP, SNMPTraps and syslog messages can optionally be tunnelled securely via SSH, which routes traffic over the configured SSH port (default: 22) instead of their default UDP ports.

11.3. Datapath Troubleshooting

11.3.1. ePing

The **eping** command constructs a proprietary Senetas Ethernet frame and transmits it out of the network port. It tests connectivity to remote encryptors and verifies that they are operational and able to respond to management traffic.

A response verifies that there is a network-level connection from the local encryptor to the remote encryptor(s).

Table 66. ePing command syntax

Command	Description
eping	Display help message
eping -m <mac>	Ping the specified MAC address (unicast)
eping -b	Broadcast to all encryptors
eping -l <size>	Set buffer size (64–1530 bytes)
eping -c <count>	Repeat the specified number of times (1–10)
eping -v <id>	Specify VLAN ID(s) in decimal (e.g., 110 or 120 110 for outer/inner)
eping -v <tag>	Specify VLAN tag(s) in hex (e.g., :81000003 or 8100000a8100000b)
eping -d <vlan>	VLAN double-tagged frame (e.g., 9100XXXX8100XXXX)

The request frame uses the network port MAC address of the local encryptor as the source address and ethertype **0xFC0F** with subtype **eping**. The default payload length is 64 bytes.

The **-v** or **-d** options tag the frame with VLAN tags so it can traverse VLAN-tagged provider networks. This is used to test reachability in service provider networks.

The **-c** option introduces a nominal 5-second delay between requests.

Use **eping** when:

- Connections do not come up
- Connections come up, but no end-to-end traffic is seen
- Connections come up, but traffic is intermittent

11.3.2. Ethertype Diagnostics

The CN4020 contains a diagnostic facility that displays a count by ethertype of all received Ethernet frames.



This facility introduces additional processing. Disable it when not required.

Ethertype counts can be used to determine whether unexpected traffic within the network may be causing problems. If unexpected traffic is identified, use CM7 or the CLI **ethertypes** command to modify the policy.

To view ethertype statistics via the CLI:

```
ethertypes -s
```

11.3.3. Traffic Analysis

Wireshark or similar network analysis tools can be used to capture and analyse traffic. PCAP files captured with Wireshark can be shared with Senetas support to assist in diagnosing issues.

CM7 Diagnostics Screen

The CM7 Diagnostics screen provides real-time information about the encryptor's operational health:

System

- **Battery status** — normal or requires replacement
- **Management module temperature**
- **Interface module temperature**
- **Front panel indicator states**

Management port statistics

- Ethernet IP — packets in, packets out, header errors, address errors, discards
- Ethernet ICMP — messages in, messages out, errors
- Ethernet UDP — datagrams in, datagrams out, errors

Local and network interface statistics

- **Received** — buffer overflow count, interframe gap errors, octet count, frame count, FCS errored frames, PCS errored frames, undersize frames, oversize frames, discarded frames, PCS sync status

- **Transmitted** — octet count, frame count, FCS errored frames

Use the **Reset Local** and **Reset Network** buttons to clear statistics counters. Resetting clears port statistics, ethertype statistics (TIM mode only), and IP rules table statistics.

For ongoing monitoring of these statistics, see [Monitoring & Statistics](#).

11.4. Physical Troubleshooting

11.4.1. LED Indicators

The CN4020 has front panel LEDs that indicate the current operational state.

System LEDs

Table 67. Front panel system LED indicators

LED	State	Description
Secure	Solid Red	Unit is not activated and traffic is being discarded
Secure	Flashing Red	Unit is not activated and traffic is being bypassed
Secure	Solid Amber	Unit is activated and traffic is being discarded
Secure	Flashing Amber	Unit is activated and traffic is being bypassed
Secure	Solid Green	One or more certificates loaded; unit is operating securely
Secure	Flashing Green	Operating securely but with no certificates loaded (e.g., Transport Independent Mode)
System	Flashing Red	Secure halt — immediate attention required
System	Solid Green	System operating correctly
Alarm	Flashing Red	Active alarms exist
Alarm	Flashing Amber	Unacknowledged alarms
Alarm	Solid Red	Acknowledged alarms
Alarm	Solid Green	No active alarms
Power	Green	Power is on

LCD Backlight

Ethernet Connector LEDs

Each local and network port has two LEDs: LNK (link, left) and SPD (speed, right).

Table 68. RJ45 Ethernet connector LEDs

LNK (Left)	SPD (Right)	Indicates
OFF	OFF	No link
Amber (solid)	Amber (solid)	Port stopped
OFF	Green (flashing)	LLF down
Green (activity)	Amber (flashing)	Link 10 Mbps
Green (activity)	Amber (solid)	Link 100 Mbps
Green (activity)	Green (solid)	Link 1000 Mbps

Table 69. SFP Ethernet connector LEDs

LNK (Left)	SPD (Right)	Indicates
OFF	OFF	No SFP or SFP socket power off
Amber (solid)	Amber (solid)	Port stopped
Red (alternate flash)	Red (alternate flash)	SFP bad
OFF	Green (flashing)	LLF down
OFF	Red (solid)	SFP good, loss of signal (LOS)
Red (solid)	Red (solid)	SFP good, LOS, auto-negotiation failure
Green (activity)	Amber (flashing)	Link 10 Mbps
Green (activity)	Amber (solid)	Link 100 Mbps
Green (activity)	Green (solid)	Link 1000 Mbps / 10 Gbps

Table 70. LED legend

Abbreviation	Meaning
LNK	Link
SPD	Speed
ACT	Activity — flashing at 8.33 Hz when frames are processed
FLSH	Flashing at 1.25 Hz
Alt-FLSH	Alternate flashing between LNK and SPD LEDs at 1.25 Hz
SOL	Solid

11.5. Common Issues

11.5.1. Connection Establishment Issues

If an encrypted connection between two encryptors fails to establish, follow this diagnostic method:

1. Ensure the network is working correctly without the encryptors installed.
2. Configure the encryptors into bypass mode, insert one or both into the network, and verify end-to-end connectivity.
3. Switch to secure mode and test again.
4. Use the `eping` command to test connectivity between encryptors. On some provider networks, VLAN tagging may be required.

The connection status (UP, DOWN, FLOW1, etc.) together with event log messages are the most effective diagnostic indicators.

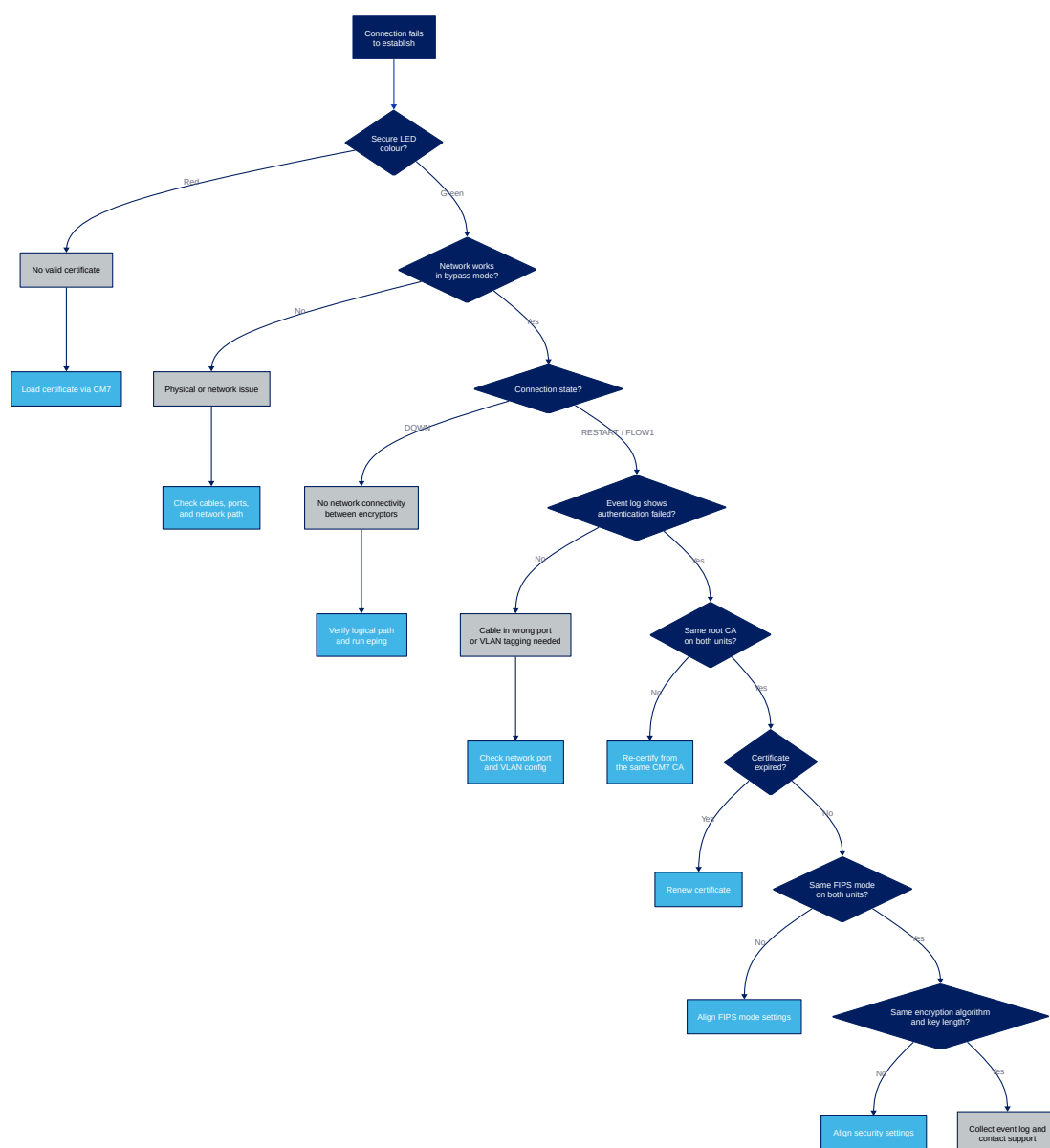


Figure 44. Connection establishment diagnostic flowchart

No Valid Certificate

An encryptor requires a valid certificate before any connections or user accounts can be created.

Symptom: The Secure LED is red. Connections cannot be added to the connection table.

Resolution: Load a valid certificate. The Secure LED turns green once a certificate has been loaded. See [Management & Administration](#) for certificate management procedures.

Certificates Signed by Different CAs

Each encryptor in a network must have a certificate signed by the same root CA. Encryptor authentication is based on signed X.509 certificates.

Symptom: An **authentication failed** message is logged in the event log. The connection is rejected.

Resolution: Verify that both encryptors have certificates signed by the same root CA. If they were certified by different copies of CM7, the CAs will differ.

Certificate Expired

Certificates have a validity period (default: one year, configurable). The validity period is checked as part of peer-to-peer authentication.

Symptom: The connection is rejected. An event log message is logged.

Resolution: Renew the expired certificate on the affected encryptor.

Incompatible Security Settings

The security settings for each connection (encryption algorithm, mode, and key length) are exchanged during the key exchange process.

Symptom: The connection cannot be established. An event log message is logged.

Resolution: Verify that both encryptors are configured with the same encryption algorithm, mode, and key length.

FIPS Mode Incompatibility

Both encryptors must be set to the same FIPS mode (on or off), as this determines the message digest algorithm used during authentication.

Symptom: An **authentication failed** message is logged.

Resolution: Verify that both encryptors have the same FIPS mode setting. See [FIPS Mode](#) for details.

Cable Plugged into Wrong Port

Secure connections are established between the **network** interfaces of peer encryptors.

Symptom: The encryptors never progress beyond the RESTART or FLOW1 states. No event log message is logged.

Resolution: Verify that the network cable is connected to the network port, not the local port.

No Logical Network Connection

The network ports of the encryptors must be logically connected across the network.

Symptom: The encryptors are unable to communicate and the session does not establish.

Resolution: Verify network connectivity between the two encryptors. Check for firewall rules, routing issues, or physical link failures between them.

11.5.2. Certificate Issues

Certificates Cannot Be Installed

Internal key generation not completed

Before a certificate can be loaded, the encryptor must complete generating its internal RSA key pair. A new key pair is generated each time a new certificate is loaded.

Symptom: The Secure LED flashes orange while key generation is in progress.

Resolution: Wait for key generation to complete. The Secure LED turns red (no certificate loaded) or green (certificate already exists) when ready.

Certificate validity period

Encryptors only accept a certificate that is currently valid — the **Not Before** and **Not After** times on the certificate must encompass the current time on the encryptor.

Symptom: The certificate is rejected during loading.

Resolution: If the time on the PC loading the certificate is ahead of the encryptor's time, either set the PC time slightly before the encryptor or manually adjust the certificate **Not Before** time backwards (e.g., one hour) when loading it.

Password lexical checking

Password lexical checking enforces strict requirements on user password syntax.

Symptom: The administrator password loaded as part of the certification process does not meet lexical requirements; the new account and the certificate are rejected.

Resolution: Ensure the password meets the lexical requirements described in [Management & Administration](#).

Certificate Details Will Not Display

Symptom: Selecting a certificate in CM7 does not display its details.

Resolution: This is most likely caused by a management network issue. Verify connectivity between CM7 and the encryptor.

Certificates and Users Disappear After Reboot

Time not set

Encryptors rely on the internal real-time clock being set to a valid time during initial configuration. In factory default state, the clock does not have a valid time. Many security functions use time as part of the authentication process.

Resolution: Set the encryptor's date and time during initial commissioning. See [Getting Started](#).

Encryptor tampered

The CN4020 has a tamper detection mechanism that detects attempts to access the enclosure. If a tamper event is detected, the encryptor returns to factory default state and loses all previously configured settings.

Resolution: Reconfigure the encryptor. Investigate the cause of the tamper event.

11.5.3. Multipoint Key Issues (VLAN and MAC Modes)

When operating in VLAN mode or MAC mode with multicast traffic, the encryptor uses the Senetas group key scheme.

When connections are established and the status is UP, the connection name starts with **M** (Key Master) or **S** (Key Slave) to indicate the encryptor's role for each connection.

On any VLAN or multicast connection, there should be exactly one Master and one or more Slaves. The Key Master distributes encryption keys to all Slave encryptors in the group and sends a keep-alive message to all group members every 3 seconds.

The protocol is fault-tolerant. If the Master is lost due to a device or network failure, the remaining Slaves negotiate and one automatically assumes the Master role.

All Encryptors Report as Master

Symptom: All encryptors show UP status with connection names starting with **M**. No data flows.

Cause: Each encryptor assumes the Master role if it stops receiving keep-alive messages and cannot find any other peer encryptors to negotiate with. If the entire network is down and encryptors cannot communicate, they all assume Master role. When this condition is detected, the units enter dead-peer mode and discard traffic.

Resolution:

1. Verify network connectivity between all encryptors in the group.
2. Restoration of connectivity allows the units to exit dead-peer mode and resume normal operation.
3. Confirm that one encryptor reports **M** (Master) and all others report **S** (Slave) — this proves successful key agreement and correct network operation.

11.5.4. VLAN Connectivity Issues

Auto-Discovery Not Enabled

Setting VLAN mode does not automatically enable auto-discovery.

Best practice: Enable auto-discovery to allow the encryptors to learn available VLAN associations, then disable auto-discovery to inhibit further learning.

VLAN Connections Do Not Restart After Mode Change

Symptom: VLAN connections are stopped after changing the global mode from Secure to Discard or Bypass.

Cause: Discovered VLAN connections are stopped whenever the global mode changes.

Resolution: Restart each connection individually after changing the global mode back to Secure.

11.5.5. TIM Mode Troubleshooting

When diagnosing TIM mode (layer 3/4) traffic issues, test protocols separately to isolate the source of the problem. For example, a firewall may be dropping TCP timestamped packets while UDP encrypted data traverses the network.

Key diagnostic steps:

- A remote encryptor is identified by its KID (Key ID) value.
- KID can be auto-discovered from an encrypted packet at any layer (L2, L3, L4-TCP, L4-UDP), provided the corresponding auto-discovery is enabled.
- Configure **iprules** for specific protocols one at a time and verify whether the remote encryptor is discovered. Delete the remote encryptor's CI and test with the next protocol.

11.5.6. Cable Problems

A damaged or faulty cable can cause intermittent or complete connectivity failures. If all other possible causes have been eliminated, check copper and fibre optic cables.



Test cables in a controlled environment before connecting them to production networks.

11.5.7. Secure Halt

If significant errors are detected during the power-up self-tests or runtime integrity checks, the CN4020 enters a *Secure Halt* state (see [Secure Halt](#)). In this state the module enters a secure shutdown that prevents all configuration and blocks every network data interface, so it cannot be managed via the CLI or SNMP.

The Secure Halt state is indicated by the front panel LEDs flashing red.

Follow this recovery protocol:

1. **Power-cycle the unit.** Attempt to clear the error by restarting (power-cycling) the CN4020. A transient fault is cleared by the restart and the unit completes its boot sequence normally.
2. **Return persistent failures to the factory.** If the Secure Halt condition persists after the power-cycle, a persistent (hard) error has occurred. The module **cannot be recovered locally** and **must be returned to the factory** for inspection and repair. Contact Senetas support to arrange return of the unit (see [Contacting Senetas Support](#)).



A diagnostics message describing the failure is written to the event log. Because the module blocks management access while halted, this message is normally retrieved through CM7 or from the logs after a successful restart, rather than directly from the affected unit.

11.6. Contacting Senetas Support

If you are unable to resolve an issue, contact Senetas technical support with the following information:

- CN4020 model and serial number
- Firmware version (found under **System** in CM7 or via the **version** CLI command)
- Description of the issue and steps to reproduce
- Event log export (see [Monitoring & Statistics](#))
- Configuration export (see [Configuration Export](#))
- Screenshots of any error messages
- PCAP captures if relevant (see [Traffic Analysis](#))

11.6.1. Senetas Customer Support Portal

The Senetas Customer Support Portal provides registered users with:

- Software and firmware updates
- Documentation, white papers, and data sheets
- Case management — create, track, and resolve support cases
- Equipment & Support Contract information

Portal access: <https://support.senetas.com/>

To request portal access, email support@senetas.com. The required setup link will be sent to you.



Portal credentials are case-sensitive. After three incorrect login attempts, the account is locked and you must contact Senetas support to re-enable access.

11.6.2. Creating a Support Case

Customers with a current Support and Maintenance Agreement can create support cases through the portal.

1. Log in to the Customer Support Portal.
2. Select **Create Call**.
3. Select **Service Call**.
4. Select the relevant contract
5. Fill in the form. The fields marked with '*' are required.
 - Contract
 - Fault Code
 - Description
 - Fault Notes
6. Please ensure a detailed and accurate description is supplied.
7. Optionally attach relevant documents (configuration exports, PCAP files, screenshots).
8. Select **Create Call**.



The **Required Date & Time** field must be set to a time in the future. This is by default set one hour from when **Create Call** was initiated.

The case is posted to the Senetas CRM system and actioned by support staff. You can view and update existing cases via the **My Cases** section of the portal.

11.6.3. Contact Information

Telephone

- Australia: 1300 783 300
- International: +61 3 9868 4539

Email

support@senetas.com

[1] Port can be modified

Appendix A: Technical Specifications

This appendix provides the detailed technical specifications for the CN4020.

Hardware Specifications

Table 71. CN4020 Hardware Specifications

Parameter	Value
Model	CN4020
Form Factor	Desktop
Dimensions (H x W x D)	33 x 180 x 125 mm
Weight	475 g
Power Supply	External AC adapter, 100-240VAC, 50/60Hz, 0.7A
Power Consumption	18W (typical)
Operating Temperature	0°C to 40°C
Storage Temperature	-20°C to 70°C
Humidity	10% to 90% (non-condensing)

Network Specifications

Table 72. CN4020 Network Specifications

Parameter	Value
Data Ports	2 x SFP
Management Port	1 x RJ45 10/100/1000BASE-T
Console Port	1 x RJ45 Serial
Maximum Throughput	1 Gbps
Latency	< 50 μ s
Supported Transceivers	SFP (1G), per compatibility list

Appendix B: Compliance & Certifications

Appendix A: Compliance and Certifications

This appendix lists the security certifications, regulatory approvals, and supported cryptographic algorithms for CypherNET network encryptors.



Certification status may vary by model and firmware version. Consult the product datasheet or contact Senetas for the current certification status of a specific model.

Security Certifications

FIPS 140

CypherNET encryptors are validated to FIPS 140-2 Level 3 requirements.

When operating with FIPS mode enabled (the default), the encryptor is in compliance with all security requirements of the FIPS 140 standard, including:

- NIST SP 800-90A/B/C entropy generation standards
- Power-up self-tests performed at every boot
- Continuous integrity monitoring (SHA-256 hash verification every 24 hours)
- Diffie-Hellman key exchange enforced on the management port for authentication and privacy

For details on enabling and disabling FIPS mode, see [FIPS Mode](#).

Common Criteria

CypherNET encryptors have been evaluated under Common Criteria for all models within the CN Series.

NATO Approval

The Senetas CN4020 is approved to NATO RESTRICTED.

Regulatory Approvals

FCC Part 15

CypherNET encryptors have been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the US Federal Communication Commission (FCC) Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses, and can radiate radio frequency energy. If not installed and used in accordance with the instructions, it may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment causes harmful interference to radio or television reception (determined by turning

the equipment off and on), try one or more of the following:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.



Any changes or modifications not expressly approved by Senetas Corporation could void your authority to operate this equipment.

Supported Cryptographic Algorithms

The following tables list the cryptographic algorithms supported by CypherNET encryptors.



Not all algorithms are available on all models or when operating in specific modes. Refer to the relevant section of this guide for mode-specific availability.

Secure Message Exchange Algorithms

These algorithms are used for encrypted connection establishment between encryptors.

Table 73. Secure message exchange algorithms

Function	Algorithm	Mode / Key Size
Authentication	RSA	Modulus 2048
Authentication	ECDSA	NIST curves: P-256, P-384, P-521
Key exchange	RSA-OAEP	Modulus 2048
Key exchange	ECDH	NIST curves: P-256, P-384, P-521
Key exchange	AES	CFB / 256
Symmetric encryption	AES	CFB, CTR, GCM / 128, 256
Signatures	SHA-2	SHA-256, SHA-384, SHA-512
Hash for HMAC	SHA-2	SHA-256

SSH Algorithms

SSH version 2.0 is used for remote CLI management.

Table 74. SSH algorithms

Function	Algorithm	Mode / Key Size
Authentication	ECDSA	NIST curves: P-256, P-384, P-521

Function	Algorithm	Mode / Key Size
Key exchange	ECDH	NIST curves: P-256, P-384, P-521
Symmetric encryption	AES	CTR, GCM / 128, 256
Hash for HMAC	SHA-2	SHA-256, SHA-512

TLS Algorithms

TLS version 1.2 is used for service connections (FTPS, RESTful API, CipherTrust integration). TLS is not used for encrypted tunnel establishment.



The availability of certified libraries requires the use of TLS v1.2.

Table 75. TLS algorithms

Function	Algorithm	Mode / Key Size
Authentication	ECDSA	NIST curves: P-256, P-384, P-521
Key exchange	ECDH	NIST curves: P-256, P-384, P-521
Symmetric encryption	AES	CBC, GCM / 128, 256
Hash for HMAC	SHA-2	SHA-256, SHA-384, SHA-512

Post-Quantum Cryptography (PQC)

Support for quantum-resistant algorithms was introduced in firmware v5.2.0. Encryptors offer a build-dependent selection of algorithms.



All encryption devices that are required to interoperate must be configured with the same PQC settings and matching KEM selection.

Key Encapsulation Mechanism (KEM) Algorithms

The following KEM algorithms are supported for quantum-resistant key exchange:

- Kyber512
- Kyber768
- Kyber1024
- Kyber512-90s
- Kyber768-90s
- Kyber1024-90s

PQC Signing Algorithms

The following signing algorithms are available for PQC certificates:

Dilithium (recommended)

- DILITHIUM2
- DILITHIUM3
- DILITHIUM5
- DILITHIUM2-AES
- DILITHIUM3-AES
- DILITHIUM5-AES

Falcon (recommended)

- Falcon-512
- Falcon-1024

SPHINCS+

- SPHINCS+-Haraka-128f-robust
- SPHINCS+-Haraka-128f-simple
- SPHINCS+-Haraka-192f-robust
- SPHINCS+-Haraka-192f-simple
- SPHINCS+-Haraka-256f-simple
- SPHINCS+-Haraka-256f-robust
- SPHINCS+-SHAKE256-128f-simple



The use of SPHINCS+ certificates is not recommended. Due to their size, some SPHINCS+ certificates may not install, and if installed, they could degrade the manageability of the encryptor.



Senetas recommends the use of Dilithium or Falcon certificates.

Algorithm Usage Flags

When selecting algorithms via the CLI `certificate -e` command, usage flags indicate each algorithm's capabilities:

Table 76. Algorithm usage flags

Flag	Description
+FIPS	Algorithm is FIPS-approved
-FIPS	Algorithm is not FIPS-approved
+TUN	Algorithm may be used for tunnel encryption
-TUN	Algorithm is not available for tunnel encryption
+TLS	Algorithm may be used for TLS connections (HTTPS/FTPS)

Flag	Description
-TLS	Algorithm is not available for TLS connections
+PRI	May be selected as Primary (Default) tunnel certificate (currently RSA/ECDSA only)
-PRI	Not usable as Primary tunnel certificate
+ANC	May be selected as Ancillary (Default) tunnel certificate (currently PQC only)
-ANC	Not usable as Ancillary tunnel certificate

When certifying a unit for the first time, the Primary Default certificate is automatically set only if the certificate is suitable as the primary certificate. The Ancillary Default certificate is not set automatically. Clearing it (setting to 0) disables all PQC functionality.

Documentation Notice

Senetas documentation is produced in English and may be subject to translation for use in other geographies where Senetas products are installed. Senetas does not accept responsibility for any translation errors. All documentation remains the intellectual property of Senetas Corporation and must not be copied without permission. The documentation — or any translation of it — must not be used to reverse-engineer Senetas products.

Appendix C: Crypto-Agility

Appendix B: Crypto-Agility

This appendix describes the crypto-agility features of the CN4020. Crypto-agility allows organisations to customise cryptographic operations to meet sovereign, proprietary, or evolving security requirements.



All crypto-agility features require **non-FIPS mode**. When FIPS mode is disabled, the encryptor no longer operates in compliance with FIPS 140 requirements. See [FIPS Mode](#) for details on enabling and disabling FIPS mode.

When FIPS mode is re-enabled (via the `fips on` command), the encryptor performs a secure reboot and reset of all cryptographic configurations. This process permanently deletes all custom S-box definitions, unloads custom CSDK libraries, erases any custom BYOE entropy pool (reverting the device to its standard FIPS-approved internal hardware noise source), and clears all custom elliptic curve (BYOC) parameters. This ensures that the encryptor returns to a fully certified and validated FIPS-compliant state.

Overview

Crypto-agility features enable organisations to:

- Implement sovereign or proprietary cryptographic standards
- Modify cryptographic operations privately, without disclosing parameters to the vendor or third parties
- Adapt to evolving threats by replacing or augmenting standard algorithms

The following crypto-agility features are available:

Table 77. Crypto-agility features

Feature	Description	Applicable Models	Interface
S-box Customisation	Modify AES substitution values to alter cipher behaviour	FPGA-based models (CN4xxx, CN6xxx, CN9xxx)	CLI (<code>sbox</code> command)
CSDK (Cipher Software Development Kit)	Write and compile custom symmetric ciphers in C or assembly	Software-based models (CN7xxx, CV1000)	Development environment
BYOE (Bring Your Own Entropy)	Load external entropy for key generation	All models	CM7
BYOC (Bring Your Own Curves)	Define custom elliptic curve parameters for asymmetric operations	All models	CM7

All four features are independent and can be used in combination.

S-box Customisation



S-Boxes are not functional in 5.5.1. If this functionality is required, contact your support provider for an updated build.

Customised S-boxes (Substitution-boxes) allow modification of the standard AES (Advanced Encryption Standard) symmetric cipher by altering its substitution values.

Purpose

S-box customisation supports sovereign or proprietary cryptographic standards on FPGA-based encryptors. On these hardware-based platforms, crypto-agility is delivered through modifications to the AES cipher rather than through complete cipher replacement.

Privacy

Users can implement their own unique cryptographic parameters securely.

Anonymity

Modifications are performed by the customer directly on the encryptor without disclosing the specific S-box values to the vendor (Senetas/Thales) or any third parties.

Configuration

Users modify the S-box values directly on the encryptor using the CLI **sbox** command in Configuration mode.

Example: Inserting a Custom S-box

```
encryptor> sbox -i
Warning: Installing an S-Box will reboot the encryptor.
Paste Custom S-Box and Test Vectors (Ctrl-D to end):
SBOX =
637c777bf26b6fc53001672bfed7ab76ca82c97dfa5947f0add4a2af9ca472c0b7fd9326363ff7cc34a5e5f171d8311
504c723c31896059a071280e2eb27b27509832c1a1b6e5aa0523bd6b329e32f8453d100ed20fcb15b6acbbe394a4c58
cfd0efaafb434d338545f9027f503c9fa851a3408f929d38f5bcb6da2110fff3d2cd0c13ec5f974417c4a77e3d645d1
97360814fdc222a908846eeb814de5e0bdbe0323a0a4906245cc2d3ac629195e479e7c8376d8dd54ea96c56f4ea657a
ae08ba78252e1ca6b4c6e8dd741f4bbd8b8a703eb5664803f60e613557b986c11d9ee1f8981169d98e949b1e87e9ce5
528df8ca1890dbfe6426841992d0fb054bb16

#ENCRYPT

[CTR128]

COUNT = 0
ACTION = ENCRYPT
KEY = 2b7e151628aed2a6abf7158809cf4f3c
IV = f0f1f2f3f4f5f6f7f8f9fafbfcfdfeff
PLAINTEXT =
6bc1bee22e409f96e93d7e117393172aae2d8a571e03ac9c9eb76fac45af8e5130c81c46a35ce411e5fbc1191a0a52e
ff69f2445df4f9b17ad2b417be66c3710874d6191b620e3261bef6864990db6ce9806f66b7970fdff8617187bb9fffd
ff5ae4df3edbd5d35e5b4f09020db03eab1e031dda2fbe03d1792170a0f3009cee
```

```

CIPHERTEXT =
874d6191b620e3261bef6864990db6ce9806f66b7970fdff8617187bb9fffdff5ae4df3edbd5d35e5b4f09020db03ea
b1e031dda2fbe03d1792170a0f3009cee37402669a2aa7228eb8758f3094613ccc09fb2313491fc0a95ddc9e3c47614
e4613d7347920bf8a73e26a53a4e484ce96399d35a687d50d86c7bc80803850b5f

...

Validating custom S-box...
Validation passed. The encryptor will now reboot to apply the custom S-box.
Rebooting...

```

Example: Reverting to Default AES S-box

```

encryptor> sbbox -d
Warning: Deleting a Custom S-Box will reboot the encryptor.
Do you wish to proceed (y/n) y
Custom S-Box has been deleted.
Rebooting...

```

Assurance Testing

To ensure that the customised cipher functions correctly and maintains integrity, the system includes a testing framework:

Trigger Conditions: Both KATs and UKATs are executed automatically at every device boot sequence, and immediately during S-box insertion when using the `sbbox -i` command.

Known Answer Tests (KATs)

The encryptor performs KATs to verify the custom S-box against expected cryptographic outputs.

Failure Behaviour: If any KAT fails during boot, the startup sequence is halted, data-plane encryption is disabled, a critical alarm is raised, and the front-panel Alarm LED illuminates solid red.

Recovery Procedure: Access the local console CLI and execute the `sbbox -d` command to delete the custom S-box and restore the default AES configuration, or perform a manual Emergency Erase / Factory Reset to wipe the system parameters and reboot into a safe default state.

Unknown Answer Tests (UATs)

UATs output the result of a test cryptographic operation using the custom S-box to the system event log. This allows security administrators to manually verify that the hardware-level cipher transformation is executing exactly as intended.

Failure Behaviour: As the CN4020 does not contain expected results, behaviour must be validated by the user. The custom s-box should be deleted and verified independently before re-install.

Event Log Entries: A successful UAT generates an informational event log record containing the input plaintext, the custom S-box ciphertext output, and a verification status (e.g., `Custom S-Box UAT executed - Output: 8ea2b7ca...`).

Bring Your Own Entropy (BYOE)

BYOE allows you to completely replace the internal entropy source with a user-defined entropy pool.

Prerequisites:

- FIPS mode must be disabled (see [FIPS Mode](#))
- The encryptor must be activated

Benefits:

- The entropy pool is not mixed with internal processing, providing assurance that key material is based solely on the entropy pool data.
- For AES assurance testing, known entropy can be used to facilitate black-box testing. The test entropy pool can be erased or overwritten on completion of any test cycle.

The entropy file includes a SHA-256 signature which is verified during file loading and process start-up. If verification fails or the entropy pool is exhausted, the encryptor reverts to the standard internal hardware-based entropy sources without operational impact.



Reloading the entropy pool removes any existing data and restarts consumption.

Enabling BYOE

Enable the entropy pool using one of the following methods:

CM7

Navigate to the **Manage** screen, **System** pane, and enable the **Entropy Pool** tick box.

CLI

```
entropy -e
```

To disable BYOE:

```
entropy -d
```

To view entropy pool status:

```
entropy
```

If the entropy pool is not enabled, the status command displays: **External entropy pool loading is disabled!**

Preparing the .ent File

Construct an entropy file using the following procedure. Maximum file size is 10 MB.

```
head -c 10M /dev/random > ent.bin
sha256sum ent.bin > ent.sha2
tar -zcvf <filename>.ent ent.bin ent.sha2
```

①

① Replace `/dev/random` with the entropy source required by your organisation.



Separate entropy files must be used on each encryptor to ensure cryptographic integrity is maintained.

Loading Entropy

Load the `.ent` file using the same procedure as a firmware update:

- **Via USB:** Copy the `.ent` file to a USB memory stick and load it through the front panel or CLI.
- **Via CM7:** Use the upgrade mechanism to transfer the file.

A reboot is not required after loading an entropy file.

After loading, check the event log and verify that the SHA-256 checksum matches the value computed when the file was prepared.

For Quantum Origin integration (automated quantum-derived entropy), see [Quantum Origin Integration](#).

For entropy pool monitoring and exhaustion alarms, see [Entropy Monitoring](#).

Bring Your Own Curves (BYOC)

BYOC allows customers to define and use bespoke Elliptic Curve (EC) parameters instead of relying on the standard named curves.

Purpose

In standard configurations, the encryptor uses approved curves such as NIST P-256, P-384, and P-521 for key agreement and digital signatures. BYOC enables organisations to implement sovereign or proprietary elliptic curve parameters for asymmetric cryptographic operations, without disclosing the specific parameters to the vendor or third parties.

Defining Custom EC Parameters

Custom elliptic curve parameters are configured through the CM7 **EC Parameters** screen:

1. Enter the curve data into the parameter fields.



The X/Y parameters and G parameters are mutually exclusive — only one set is required.

CM7 accepts the complete set of elliptic curve domain parameters, which includes:

- **Field Size (bits):** The size of the finite field (typically between 160 and 521 bits).
 - **Field Type:** The finite field representation—either Prime ($\mathbb{F}_p$) or Binary ($\mathbb{F}_{2^m}$).
 - **Prime (p) / Irreducible Polynomial ($f(t)$):** The modulo prime number or irreducible polynomial defining the field.
 - **Coefficient a :** The first coefficient of the elliptic curve equation.
 - **Coefficient b :** The second coefficient of the elliptic curve equation.
 - **Generator Point (G):** The coordinates (G_x and G_y) of the base generator point on the curve.
 - **Order (n):** The prime order of the generator point G .
 - **Cofactor (h):** The integer cofactor of the elliptic curve group.
2. Click **From Curve Data** to create the parameters. The parameters and a validity indicator are displayed.
 3. Save the parameters to the clipboard or to a PEM-formatted file for use as custom key types when generating certificates.

The image shows a software window titled "CA/Key Management" with a close button (X) in the top right corner. The window has five tabs: "Create New CA", "Advanced", "EC Parameters" (which is selected), "Export CA Certs", and "KDK". The "EC Parameters" tab contains a section titled "Curve Data" with several input fields, each followed by a "hex" label. The fields are: "Prime(p):", "A Coefficient:", "B Coefficient:", "X:", "Y:", "G(uncompressed):", "Order:", and "Cofactor:". Below these fields are three buttons: "From Curve Data" (with a lightning bolt icon), "Load From Clipboard" (with a clipboard icon), and "Clear" (with a trash can icon). At the bottom of the window are three more buttons: "Save To File..." (with a floppy disk icon), "Copy To Clipboard" (with a clipboard icon), and "Close". A scrollbar is visible on the right side of the "Curve Data" section.

CA/Key Management

Create New CA Advanced **EC Parameters** Export CA Certs KDK

Curve Data

Prime(p): hex

A Coefficient: hex

B Coefficient: hex

X: hex

Y: hex

G(uncompressed): hex

Order: hex

Cofactor: hex

⚡ From Curve Data 📋 Load From Clipboard 🗑 Clear

💾 Save To File... 📋 Copy To Clipboard Close

Figure 45. Elliptic curve parameters

For certificate generation using custom curves, see [Advanced CA Functions](#).

Appendix D: CLI Reference

Overview

The CN4020 provides a Command Line Interface (CLI) that can be accessed using a terminal emulator connected to the serial craft interface. The CLI provides a comprehensive management capability including the ability to configure encrypted connections, manage user accounts, and view log records and alarms. The functionality provided by the CLI is similar to that provided by CM7, however CM7 is required for the activation and/or certification of units.

The CLI supports a configurable prompt, as well as configurable pre-login and post-login banner messages. The prompt text is displayed ahead of the **>** symbol to identify the encryptor to which you are connected. It can be set to show the logical name of the unit within the network or the physical location.

Accessing the CLI

The CLI operates through an RS-232 serial connection to the encryptor's RJ45 craft port. Configure your terminal emulator with the following settings:

- **Baud rate:** 9600
- **Data bits:** 8
- **Parity:** None
- **Stop bits:** 1
- **Flow control:** None

The CLI requires a user account on the encryptor and the user must log in with the same authentication password as used with CM7. The CLI enforces a three-try, three-minute lockout process to prevent automated attacks. A session timeout logs the user out after ten minutes of inactivity.

SSH access to the CLI can also be enabled using the **sshcli** command.

CLI Conventions

Command Modes

Commands are available depending on the user's role (Administrator, Supervisor, Operator, or Upgrader). A list of available commands can be obtained by typing **help**. Additional help can be obtained on each command by appending **-h** to any command.

Syntax Notation

The following conventions are used in command descriptions:

Notation	Meaning
<value>	Required argument — replace with an actual value
[option]	Optional argument
a b	Choose one of the alternatives
<CR>	Press Enter (carriage return)
-flag	A command option flag

Command History

The console supports a command history buffer that is 25 commands deep. Use the up and down arrow keys to cycle through the buffer. The history buffer is cleared each time a user logs in or out.

Hexadecimal Values

Where a command requires a hexadecimal argument, the value is usually entered in the four-character (hhhh) form. CLI output will usually display hex values in the Hhhh form; however, this document specifies them using the 0xhhhh form.



The encryptor will not be damaged by anything you type into the CLI.

Command Quick Reference

Command	Description	Mode
activate	Change default credentials prior to loading certificates	Config
alarm	Display and acknowledge alarms	User
audit	Display and manage the audit log	User
autodisco	Enable or disable automatic session discovery	Config
autopop	Enable or disable auto-population of connections	Config
banner	View and modify pre-login and post-login banners	Config
certificate	View and manage X.509 certificates	Config
community	View and modify the SNMPv1 community string	Config
con	View and modify the multipoint connection policy	Config
controlplaneif	Set the port used for key distribution	Config
crl	View and modify CRL server entries	Config
crypto	Change the encryption algorithm, mode, and key size	Config
date	View and change the internal date and time	Config

Command	Description	Mode
entropy	Enable or disable the entropy pool	Config
eping	Send a proprietary diagnostic Ethernet ping	User
eqkd	Manage standards-based quantum key distribution (QKD)	Config
erase	Erase configuration and reboot to factory defaults	Config
ethertypes	Set frame processing policy by ethertype	Config
event	Display and manage the event log	User
fips	Set and display FIPS operational mode	Config
ftpcfg	Configure and manage remote FTP server access	Config
global	Set the top-level processing policy for Ethernet frames	Config
help	Display available console commands	User
helpall	Display help for all available commands	User
history	Show command history for the current session	User
hostname	Set the hostname of the encryptor	Config
inband_vlan	Specify VLAN tags for in-band management frames	Config
initcfg	Reset security policy to known starting conditions	Config
inventory	Display control and interface module details	User
ip	Configure management and in-band IP addresses	Config
iprules	Establish IP policy rules for TIM mode L3/L4 traffic	Config
kdf	Generate and manage key derivation keys	Config
kem	Display quantum resistant key encapsulation algorithms	Config
keyprovider	Specify the key provider for TIM mode	Config
kscfg	Configure KeySecure remote server settings	Config
kstier	Manage KeySecure tier configurations	Config
line	Enable or disable point-to-point (line) mode	Config
linkspeed	Set physical interface connection parameters	Config
locmacs	List and manage local MAC addresses (multipoint MAC mode)	Config
logout	Log out of the CLI session	User
mpls	Set MPLS frame processing policy	Config

Command	Description	Mode
netmacs	List and manage network MAC addresses (multipoint MAC mode)	Config
ntpcfg	Configure NTP server addresses	Config
ocsp	View and manage OCSP server entries	Config
overview	View and modify contact, location, and comments	Config
password	View and modify user password policy	Config
policy	Configure miscellaneous Ethernet policy settings	Config
profile	Set administrative mode (standard or simplified)	Config
prompt	Customise the CLI prompt	Config
protocol	Configure protocol and link speed	Config
reboot	Reboot the encryptor	Config
rest	Enable or disable the RESTful server	Config
sbox	Insert, update, or delete a custom S-Box	Config
sfp	SFP transceiver diagnostics	User
shim	Set shim insertion rate for CTR/GCM modes	Config
snap	Set policy for IEEE 802.3 LLC SNAP frames	Config
snmpcfg	Configure SNMPv3 privacy settings	Config
snmptraps	Add or delete SNMPv3 trap server entries	Config
sshaux	Configure tertiary SSH access for remote devices	Config
sshcli	Enable or disable SSH CLI access	Config
stats	Display port statistics	User
syslog	Configure syslog server entries	Config
tacacs	Define and manage TACACS+ server connections	Config
timezone	Set the timezone of the encryptor	Config
transec	Enable or disable TRANSEC framing	Config
tunnels	View and control encrypted connections (tunnels)	Config
upgrade	Initiate firmware upgrade from USB	Config
usb	Lock or unlock the front panel USB interface	Config
users	View and edit authorised system users	Config
version	Display software version information	User

Command	Description	Mode
<code>vlan</code>	Set policy for IEEE 802.1Q tagged frames	Config

Command Reference

activate

Synopsis

```
activate [-e | -d | -l | -v]
```

Description

Change the default credentials of the `admin` account prior to loading certificates. The encryptor must be activated before certificates can be loaded. Activation requires the encryptor to be placed in activate mode (`-e`), after which CM7 displays the activation digest and allows entry of new credentials. The `-l` option allows activation to be performed locally using only the CLI.

Arguments

`-e`

Enable encryptor for activation

`-d`

Disable activation

`-l`

Perform local activation

`-v`

Verify hash code

Mode

Configuration mode

Example

```
encryptor> activate -e
Activate mode enabled. Awaiting Hash!

encryptor> activate -v
EF3233252A3B57A127E7812EAB274363EA4562FB3213BA68231EF3a
Confirm (y/n)?y
Encryptor is activated

encryptor> activate -l
Account[admin]
Password>newPassword
Password>newPassword
Confirm[y/n]y
Encryptor is activated
```

alarm

Synopsis

```
alarm [-a <x> <y> | -a * | -n]
```

Description

Display the current state of the alarm table and acknowledge individual alarms. Alarm conditions appear with a state of **ACTIVE_NAK** (not acknowledged). Once acknowledged, the state becomes **ACTIVE_ACK**; the alarm remains in the table until the condition clears.

Arguments

-a <x> <y>

Acknowledge alarms x, y, etc. (where x > y)

-a *

Acknowledge all alarms

-n

Print the number of active alarms

Mode

User mode

Example

```
encryptor> alarm
Alarm count = 4 Unacknowledged count = 4
(001): id=004 02/12/2003 15:13:16 ACTIVE_NAK Local port link down indication
(002): id=005 02/12/2003 15:13:16 ACTIVE_NAK Network port link down indication
(003): id=010 02/12/2003 15:13:10 ACTIVE_NAK Local interface loss of signal
(004): id=024 02/12/2003 15:13:09 ACTIVE_NAK Network interface loss of signal
```

audit

Synopsis

```
audit [-l <n> | -s <n> | -n | -c | -w <on|off>]
```

Description

Display records in the audit log. The audit log is a non-volatile record of changes made to the system configuration, with each record time-stamped and containing the user ID and a description of the change. The log has a maximum of 4000 records.

Arguments

-l <n>

List the last *n* records in the log

-s <n>

List records starting from record *n*

-n

Print the number of records in the log

-c

Clear the audit log

-w <on|off>

Turn log wrapping on or off

Mode

User mode

Example

```
encryptor> audit
Number of audit records is 1
Log wrapping enable
(1): 24/11/2003 16:24:48 User account added as follows Id: admin, Name:
administrator, Status: yes, Level: administrator, Console: yes, Snmp: yes
```

autodisco

Synopsis

autodisco [-e[u|m] | -d[u|m] | -a <minutes> | -e L2 | -d L2 | -e L3 | -d L3 | -e L4T | -d L4T | -e L4U | -d L4U]

Description

Turn MAC address auto-discovery on or off for layer 2 encryptors, and control auto-discovery at Layer 2, 3, or 4 for TIM mode encryptors. In multipoint MAC mode, auto-discovery allows automatic creation of connections from observed traffic. In TIM mode, auto-discovery can be enabled or disabled in a hierarchical manner.

Arguments

-e[u|m]

Enable auto-discovery (optionally limited to unicast or multicast)

-d[u|m]

Disable auto-discovery (optionally limited to unicast or multicast)

-a <minutes>

Set the multicast session timeout period in minutes

-e L2

Enable auto-discovery at Layer 2

-d L2

Disable auto-discovery at Layer 2

-e L3

Enable auto-discovery at Layer 3

-d L3

Disable auto-discovery at Layer 3

-e L4T

Enable auto-discovery at Layer 4 TCP

-d L4T

Disable auto-discovery at Layer 4 TCP

-e L4U

Enable auto-discovery at Layer 4 UDP

-d L4U

Disable auto-discovery at Layer 4 UDP

Mode

Configuration mode

Example

```
encryptor> autodisco
Automatic session discovery: enabled
Layer2 Autodiscover : disabled
Layer3 Autodiscover : disabled
Layer4 TCP Autodiscover : disabled
Layer4 UDP Autodiscover : disabled

encryptor> autodisco -e
Automatic session discovery enabled
```

autopop**Synopsis**

autopop [-e | -d]

Description

Enable or disable auto-population of connections. When auto-population is enabled, the connection table is cleared and the encryptor reboots, also clearing the IP Rules table.

Arguments

-e

Enable auto-population of CIs

-d

Disable auto-population of CIs

Mode

Configuration mode

Example

```
encryptor> autopop -e
Warning this command will delete existing connections and reboot the encryptor

Do you wish to proceed (y/n) Y
Automatic Populate enabled
```

banner

Synopsis

banner [-r <string> | -o <string>]

Description

View and modify the pre-login and post-login banner strings displayed on the CLI console. During entry of banner text, each line is prefixed with the count of characters already entered. Pressing Ctrl+D on the first line and accepting the entry clears the banner text.

Arguments

-r <string>

Update the pre-login banner

-o <string>

Update the post-login banner

Mode

Configuration mode

Example

```
encryptor> banner
Pre-login Banner:
Post-login Banner:

encryptor> banner -r
Enter pre-login banner text, max 2559 characters.
Press <CTRL>D on a new line to finish

0000 :Access is restricted to IT staff
```

0033 :

Press a to accept, d to discard

Changes applied

certificate

Synopsis

```
certificate [-p <idx> | -i | -r | -e | -s | -d | -c | -C | -b <idx> | -R | -k <options> | -q <options>]
```

Description

View and manage X.509 certificates on the encryptor. Multiple certificates are supported and these can be signed by different Certificate Authorities. The **-e** option sets the CSR algorithm type, the **-k** option creates a CA signing certificate, and the **-q** option creates an encryptor certificate.

Arguments

-p <idx>

Print certificate details for the specified index

-i

Install a PEM-encoded X.509 certificate from the CLI

-r

Print the X.509 certificate signing request

-e

Set the X.509 CSR algorithm type

-s

Display and set the certificate signing request subject

-d

Delete a certificate

-c

Set the default certificate (Primary)

-C

Set the default certificate (Ancillary)

-b <idx>

Backup the CA signing certificate

-R

Restore the CA signing certificate

-k -d <DN> [-a <validity>] [-s <serial>]

Create a CA signing certificate with the specified distinguished name

-q -d <DN> [-a <validity>] [-s <serial>]

Create an encryptor certificate with the specified distinguished name

Mode

Configuration mode

Example

```
encryptor> certificate
Certificate found
Version: 1
SerialNumber: 0
Signature algorithm SHA
CA Name: Australia:Senetas:Support
My Name: Australia:Senetas:Sales:000000
Not Before: 2003-10-21 15:49:50
Not After: 2005-10-21 15:49:50
```

community

Synopsis**community [-s <name>]****Description**

View and modify the community string used in SNMPv1 messages. The encryptor must be rebooted for the new value to take effect.

Arguments**-s <name>**

Set the SNMP community string

Mode

Configuration mode

con

Synopsis**con [-m | -v | -T]****Description**

View and modify the multipoint connection policy of an Ethernet encryptor. The connection policy defines the remote ID on which the connection policy is based when the encryptor is in multipoint

mode. This command is not available if the encryptor is in point-to-point (line) mode.

Arguments

-m

Enable MAC connection mode

-v

Enable VLAN connection mode

-T

Enable TIM connection mode

Mode

Configuration mode

controlplaneif

Synopsis

```
controlplaneif [net | man]
```

Description

Set the port over which key distribution will occur. The default is the network port. When VLAN is used as the connection policy and certain topologies (such as Link Aggregation) limit multicast management frame distribution, keys can be distributed via the front panel management port.

Arguments

net

Set key distribution to the network port

man

Set key distribution to the management port

Mode

Configuration mode

crl

Synopsis

```
crl [-a <url> | -c | -d <idx> | -e <idx> | -p [idx] | -u [interval]]
```

Description

View and modify CRL (Certificate Revocation List) server entries for the encryptor. It is recommended to use an FTP server, which must be entered in the FTP servers list with a matching certificate.

Arguments

-a <url>

Add a CRL server entry

-c

Clear all stored CRLs

-d <idx>

Delete a CRL server entry

-e <idx>

Edit a CRL server entry

-p [idx]

Print CRL server entry details

-u [interval]

Display or update the CRL update interval

Mode

Configuration mode

Example

```
encryptor> crl -a http://10.0.1.34/crlfile.crl
CRL entry added

encryptor> crl
CRL update interval is 1 minutes
Index URL
1      http://10.0.1.34/crlfile.crl
```

crypto

Synopsis

crypto [-s]

Description

View or change the encryption algorithm, mode, and key size. In order for the cryptographic mode to be changed, the encryptor must have its global processing policy set to Bypass or Discard.

Arguments

-s

Set the crypto mode (presents a selection list)

Mode

Configuration mode

Example

```
encryptor> crypto -s
Global Crypto Mode Configuration options:
- ->(1) Algorithm = AES      Mode = CFB      Key Length = 256
      (2) Algorithm = AES      Mode = CFB      Key Length = 128
      (3) Algorithm = CAMELLIA Mode = CFB      Key Length = 256
      (4) Algorithm = SEED     Mode = CFB      Key Length = 128
      (5) Algorithm = AES      Mode = Counter Key Length = 256
Enter new Global Crypto Mode >: [1]
```

date

Synopsis

date [**<yyyy-mm-dd>**] [**<hh:mm:ss>**]

Description

View and change the internal date and time of the encryptor using ISO 8601 format. Without arguments, the command displays the current date, time, and uptime. The date and time can be set independently or together.

Arguments

<yyyy-mm-dd>

Set the date

<hh:mm:ss>

Set the time

Mode

Configuration mode

Example

```
encryptor> date
2004-11-01 16:27:41 up 3 days 00:05

encryptor> date 2004-10-28
Setting to Thu Oct 28 16:28:27 2004

encryptor> date 13:11:20
Setting to Thu Oct 28 13:11:20 2004
```



It is very important to set the time in a factory default unit. Failing to do so will cause the encryptor to believe it has been tampered with, resulting in all certificate, user, and connection information being erased when the unit next reboots.

entropy

Synopsis

```
entropy [-e | -d]
```

Description

Enable or disable the entropy pool of the encryptor. The entropy pool can only be enabled if FIPS mode is turned off. When enabled, an entropy (.ent) file can be loaded from a USB memory stick. When disabled, the encryptor uses internal noise sources for entropy.

Arguments

-e

Enable entropy pool loading

-d

Disable entropy pool loading

Mode

Configuration mode



Senetas encryptors support only USB drives configured with the FAT or FAT32 format.

eping

Synopsis

```
eping [-m <mac> | -b] [-l <size>] [-c <count>] [-v <id>] [-d <vlan>]
```

Description

Construct and transmit a proprietary Senetas Ethernet frame out of the network port for diagnostic purposes. A response verifies connectivity from the local encryptor to the remote encryptor(s) and that the responding units are operational.

Arguments

-m <mac>

Ping the specified MAC address

-b

Broadcast destination

-l <size>

Send the specified buffer size (64—1530)

-c <count>

Repeat the specified number of times (1—10)

-v [<id>[<id>]]

Specify VLAN ID(s) in decimal or VLAN tag(s) in hex

-d <vlan>

VLAN double-tagged frame

Mode

User mode

eqkd

Synopsis

eqkd [-e | -d | -k <addr> | -r <SAE_ID> | -c | -s | -q <SAE_ID> | -S]

Description

Enable and configure standards-based (ETSI) quantum key distribution (QKD) management. This command is only applicable to layer 2 encryptors and is available in VLAN, Line, and TRANSEC operational modes. With no arguments, **eqkd** displays the current ETSI QKD configuration settings and status.

Arguments

-e

Enable ETSI QKD mode

-d

Disable ETSI QKD mode

-k <IPv4|IPv6>

Set the default Key Management Entity (KME) address

-r <SAE_ID>

Set the default remote Secure Application Entity (SAE) ID

-c

Set the HTTPS certificate (server or end-user certificate)

-s

Get status from server (deprecated; supported only on EQKD v0.9.3c and earlier)

-q <SAE_ID>

Get or query key status from server

-S

Clear status counters

Mode

Configuration mode

Example

```
encryptor> eqkd -h
Usage: eqkd          View ETSI QKD configuration settings/status
    -e              Enable ETSI QKD mode
    -d              Disable ETSI QKD mode
    -k              Set default Key Management Entity (KME) IPv4/IPv6 address
    -r              Set default remote Secure Application Entity (SAE) ID
    -c              Set https certificate (server or end user certificate)
    -s              Get status from server (only supported EQKD v0.9.3c and earlier)
    -q              Get/query key status from server
    -S              Clear status counters
    -h              This help message
```

erase

Synopsis

erase [-f]

Description

Erase the current configuration and reboot the unit to factory default state. All user and connection entries are deleted and the unit's certificate is destroyed. The configured IP address, connection mode, and any virtual management configuration are preserved unless the **-f** option is used.

Arguments

-f

Fully erase the unit, including the front panel IP address

Mode

Configuration mode

Example

```
encryptor> erase
Warning this command will erase the configuration to factory defaults
do you wish to proceed ? (y/n) y
Are you sure ? (y/n) y
Erasing unit and rebooting . . .
```

ethertypes

Synopsis

ethertypes [-s | -a | -d <ethertype> | -d * | -e | -1 <ethertype> | -2 <ethertype> | -3 <ethertype> | -c | -r | -l]

Description

Set the policy for frame processing by ethertype. Policy can be set for up to 15 different ethertype values; those not explicitly listed are handled under the **Other** policy. Ethertype **0x05FF** represents length-encoded frames.

Arguments

-s

Show ethertype statistics (count of frames bypassed or discarded)

-a

Add an ethertype

-d <ethertype>

Delete the specified ethertype

-d *

Delete all ethertypes

-e

Edit an ethertype

-1 <ethertype>

Set control plane ethertype 1 (hex)

-2 <ethertype>

Set control plane ethertype 2 (hex)

-3 <ethertype>

Set out-of-band control plane ethertype 3 (hex)

-c

Toggle ethertype diagnostic counting on or off

-r

Reset all diagnostic counts

-l

List ethertype diagnostic counts

Mode

Configuration mode

The CN4020 has a diagnostic capability that, when enabled, counts by ethertype the Ethernet frames received and passed through the encryptor on both the local and network ports. These counts are stored in a table for diagnostic purposes and are controlled using the **-c**, **-r**, and **-l** flags.



The diagnostic counting feature incurs a processing overhead and should be turned off during normal operation. Whenever the encryptor is rebooted, the feature is turned off.

Example

```
encryptor> ethertypes
Offset Encryption Mutate Mutated
Ethertype (Name) Enable Offset Enable Etherbyte Unicast Multicast Broadcast NonMutant
-----
H05ff (Length)      N      H0      NA      UseCI      UseCI      UseCI      NA
H0800 (IPv4)        N      H14     Y       Hf800      UseCI      UseCI      UseCI      Discard
H0806 (ARP)         N      H0      Y       Hf806      UseCI      UseCI      UseCI      Discard
H86dd (IPv6)        N      H28     Y       Hf6dd      UseCI      UseCI      UseCI      Discard
H8808 (MAC-C)       N      H0      N       Hf808      Bypass     Bypass     Bypass     Bypass
H8809 (SPMA)        N      H0      N       Hf809      Bypass     Bypass     Bypass     Bypass
H88cc (LLDP)        N      H0      N       Hf8cc      Bypass     Bypass     Bypass     Bypass
H9000 (Loopback)    N      H0      N       Hf000      Bypass     Bypass     Bypass     Bypass
Other               N      H0      NA      UseCI      UseCI      UseCI      NA
9 Records in Etherbyte table
Control plane etherbyte : fc0f
```

event

Synopsis

```
event [-l <n> | -s <n> | -n | -c | -w <on|off>]
```

Description

Display the event log, clear the log, and control the wrapping mode. The event log is a non-volatile record of significant events, with each record time-stamped. The log has a maximum of 4000 records.

Arguments

-l <n>

List the last *n* records in the log

-s <n>

List records starting from record *n*

-n

Print the number of records in the log

-c

Clear the event log

-w <on|off>

Turn log wrapping on or off

Mode

User mode

Example

```
encryptor> event
Number of event records is 13
Log wrapping enabled
(1): 24/11/2003 16:24:44 System started
(2): 24/11/2003 16:24:47 Alarm set: Network interface loss of signal
(3): 24/11/2003 16:24:48 Alarm set: Local interface loss of signal
(4): 24/11/2003 16:24:52 Alarm set: Network port link down indication
(5): 24/11/2003 16:24:53 Alarm set: Local port link down indication
```

fips

Synopsis

fips [**on** | **off**]

Description

Set and display the FIPS 140 operational mode of the encryptor. If FIPS mode is enabled (the default), the encryptor complies with all FIPS 140 security requirements. Changing FIPS mode reboots the encryptor and removes all certification and user credentials.

Arguments

on

Enable FIPS mode (will erase and reboot)

off

Disable FIPS mode (will erase and reboot)

Mode

Configuration mode

Example

```
encryptor> fips
FIPS mode enabled
```

framegap

Synopsis

framegap [**-r** | **-s**]

Description

View and set the interframe gap (IFG) used on the Ethernet ports.

Arguments

-r

Set the interframe gap to repeater mode (88 bit times)

-s

Set the interframe gap to standard mode (96 bit times)

Mode

Configuration mode

ftpcfg

Synopsis

```
ftpcfg [-a | -d <idx> | -e <idx> | -c | -r <on|off> | -s]
```

Description

Configure and manage access to remote FTP servers.

Arguments

-a

Add a remote FTP server entry

-d <idx>

Delete an FTP remote server entry

-e <idx>

Edit an FTP remote server entry

-c

Clear all remote FTP server settings

-r <on|off>

Restrict FTP access to listed servers only

-s

Show the public key for SFTP upgrades

Mode

Configuration mode

global

Synopsis

```
global [-b | -d | -e]
```

Description

Set the top-level processing policy for received Ethernet frames. The global policy can be set to Bypass (all frames pass through), Discard (all frames are discarded), or Encrypt (ethertype and remote ID policies are applied).

Arguments

-b

Set global mode to Bypass

-d

Set global mode to Discard

-e

Set global mode to Encrypt

Mode

Configuration mode

Example

```
encryptor> global
Global mode: bypass

encryptor> global -e
Global mode set to encrypt
```



All operational modes except TIM must have valid certificates loaded onto the encryptor to enable changing the global mode to Encrypt.

help

Synopsis

help

Description

Display a list of all available console commands with brief descriptions. Use **command -h** for detailed help on any individual command.

Mode

User mode

Example

```
encryptor> help
alarm      - View, clear & acknowledge alarms
audit      - View the audit log
event      - View the event log
reboot     - Reboot the unit
```



```
users      - View/edit system users
certificate - View the current certificate details
ip         - View/edit ip, mask and gateway addresses
date      - View/edit date and time
inband    - View/change inband settings
sessions  - View/edit session details
version   - Display version information.
erase     - Erase unit
fips      - View/change FIPS operation mode
password  - View/change user password policy
help      - List all available commands
history   - Print command history
logout    - Logout from console
prompt    - Change the console prompt
Try 'command -h' for more detailed help
```

helpall

Synopsis

```
helpall
```

Description

Display help information about all available console commands. Individual commands may also be run with the **-h** flag for specific help.

Mode

User mode

history

Synopsis

```
history
```

Description

Show the command history for the current CLI session. Previous commands are stored in a 25-deep command history buffer. The buffer is cleared each time a user logs in or out.

Mode

User mode

Example

```
encryptor> history
01: date
02: users
03: pvc
04: help
05: ip -s
06: pvc
07: sessions
08: fips
09: history
```

hostname

Synopsis

```
hostname [-s <hostname>]
```

Description

View or set the hostname of the encryptor.

Arguments

```
-s <hostname>
```

Set the hostname

Mode

Configuration mode

inband_vlan

Synopsis

```
inband_vlan [-a [<id> [<id>]] | -e <idx> [<id> [<id>]] | -d <idx> | -d *]
```

Description

Specify the VLAN tag(s) used for in-band management frames. When operating in networks that use VLAN tagging, entries for each VLAN in use must be added so that remote encryptors can be managed. There must be at least one entry in the table; by default this is the untagged entry.

Arguments

```
-a
```

Add an untagged entry

```
-a [<id> [<id>]]
```

Add VLAN ID(s) in decimal (single or double tag)

```
-a [<tag> [<tag>]]
```

Add a single or double VLAN tag in hex

```
-e <idx> [<id> [<id>]]
```

Edit the given record

```
-d <idx> [<idx>..]
```

Delete the given record(s)

```
-d *
```

Delete all records

Mode

Configuration mode

Example

```

encryptor> inband_vlan
index : tag(s)
-----
1      : (untagged)
        00:d1:1f:0a:0f:13
2      : 8100 001f
3      : 8100 008f
        00:d1:1f:0a:0f:27
4      : 8100 04bf
        00:d1:1f:0a:0f:20
        02:d1:1f:0a:0f:20
-----
00:d1:1f:0a:0f:13 vlan idx 1
00:d1:1f:0a:0f:20 vlan idx 4
02:d1:1f:0a:0f:20 vlan idx 4
00:d1:1f:0a:0f:27 vlan idx 3

```

initcfg

Synopsis

```
initcfg [-a | -c | -g | -1 | -2 | -3 | -4]
```

Description

Reset the encryptor's security policy to known starting conditions. This command affects the operating mode, ethertype policy, connection identifiers, MAC tables, state, and global policy only; it will not change other configuration settings or erase the X.509 certificate. Executing this command forces a reboot.

Arguments

-a

Reset tunnel/CI, MAC, and global config to defaults and reboot

-c

Reset tunnel/CI and MAC to defaults and reboot

-g

Reset global config to default and reboot

-1

Test level 1 defaults

-2

Test level 2 defaults

-3

Test level 3 defaults (line mode only)

-4

Test level 4 defaults (line mode only)

Mode

Configuration mode

Example

```

encryptor> initcfg -a
Warning this command will reset all tunnel/CI, MAC and global data to their
factory defaults and reboot the unit!

do you wish to proceed ? (y/n) y
Are you sure ? (y/n) y
Resetting config and rebooting

```

inventory**Synopsis****inventory****Description**

Display details of the control and interface modules of the encryptor, including board numbers, serial numbers, software versions, and build information.

Mode

User mode

Example

```

encryptor> inventory
=====
Management Module
-----
Board Number      = B2010A005-51
Description       = System Module
Serial Number     = 00D01F030219
Software Version  = 2.7.1
Build ID          = 5.C245
Build Number      = 1302757132
Build Date & Time = 14-Apr-2017 14:58:52
=====
Interface Module
-----
Board Number      = B2084A001-51
Description       = Gigabit Ethernet Crypto I/F Card
Serial Number     = 00D01F030470
Software Version  = 2084 v2.2.16

```

ip

Synopsis

```
ip [-s <idx> <addr>/<prefix> <gw> | -e <idx> | -d <idx> | -i <e|-d> | -c <value> | -v <e|-d> | -g <e|-d>]
```

Description

Configure the IP addresses of the management port (IPv4 idx=1, IPv6 idx=2) and the in-band addresses (IPv4 idx=3, IPv6 idx=4).

Arguments

-s <idx> <addr>/<prefix> <gw>

Edit IPv4 or IPv6 management settings for the specified index

-e <idx>

Enable interface entry (idx 1—4)

-d <idx>

Disable interface entry (idx 1—4)

-i <e|-d>

Enable or disable this device as an in-band gateway

-c <value>

Set or reset the DSCP value

-v <e|-d>

Enable or disable the virtual management interface (TIM mode only)

-g <e|-d>

Enable or disable the auxiliary interface as an in-band gateway for remote encryptor management

Mode

Configuration mode

Example

```
encryptor> ip
Index Port      Status  AF    Address/Prefix
-----
01  Management    Enabled IPv4   172.16.6.20/16
      172.16.1.1
02  Management    Disabled IPv6   ::1:1:1:2/96
      ::1:1:1:1
03  Inband Mgmt(0) Disabled IPv4   2.1.1.2/16
      2.1.1.1
04  Inband Mgmt(0) Disabled IPv6   ::192:168:53:20/112
      ::192:168:53:1
```

```
encryptor> ip -s 1 10.0.33.80/16 10.0.1.254
```

iprules

Synopsis

```
iprules [-a <dst_addr>/<prefix> <src_addr>/<prefix> <protocol_id> <dst_port> <src_port>
<action> | -d <idx> | -d * | -c | -u <action> | -s <src|dst> <port> | -l <e|-d> | -ltu
<e|-d> | -ltu -m <src|dst|both> | -l4 <e|-d>]
```

Description

Establish IP policy rules for L3/L4 Ethernet traffic when operating in TIM mode. Rules are based on longest prefix match (LPM) and support encryption at Layer 2, 3, or 4, as well as bypass and discard actions.

Arguments

-a <dst_addr>/<prefix> <src_addr>/<prefix> <protocol_id> <dst_port> <src_port> <action>

Add an IP rule (action: **d** = discard, **b** = bypass, **l2** = encrypt L2, **l3** = encrypt L3, **l4** = encrypt L4, **ltu** = L4 UDP tunnel). The source address, protocol, and ports may be wildcarded with *****.

-d <idx>

Delete an IP rule

-d *

Delete all IP rules

-c

Clear all rules and restore all other settings to defaults

-u <action>

Set the action for unlisted (unmatched) IP addresses (**b**, **d**, **l2**, **l3**, **l4**, or **ltu**)

-s <src|dst> <port>

Set the source or destination port used for Layer 4 UDP tunnelling (1—65535)

-l <e|-d>

Enable or disable Layer 4 TCP/UDP checksum calculation

-ltu <e|-d>

Enable or disable Layer 4 UDP tunnel encryption mode

-ltu -m <src|dst|both>

Match Layer 4 UDP-tunnelled packets on the UDP source port, destination port, or both

-l4 <e|-d>

Enable or disable Layer 4 encryption mode (TCP/UDP/ICMP)

Mode

Configuration mode

Example

```

encryptor> iprules
IP policy rules
Index Address          Netmask Protocol Port  Action
-----
1    192.168.1.0          24      *      *    Encrypt L3
2    192.168.1.20        32      6      *    Encrypt L4
3    192.168.1.22        32      1      *    Discard
4    192.168.1.22        32      88     *    Bypass
5    192.168.1.22        32      6      20   Encrypt L3
6    192.168.1.22        32      6      *    Discard
7    192.168.1.22        32      6      22   Encrypt L4
8    192.168.1.20        32      17     *    Bypass

encryptor> iprules -a 200.0.0.10 * l3
Action set to CryptLayer3!

```

kdf

Synopsis

kdf [-g | -k <key> -d <datetime>]

Description

Generate and display a new key derivation key (KDK). The key can be copied and distributed to peer encryptors to enable encryption. When a new KDK is generated, any existing key is automatically erased.

Arguments

-g

Generate and display a new key derivation key

-k <key> -d <datetime>

Install a key derivation key (64 hex characters). The **-d** timestamp (**yyyy-mm-dd hh:mm:ss**, expressed in the encryptor's local time) sets when the key takes effect. If the timestamp is within two key update intervals of the present time, the key is installed with immediate effect and all CIs are restarted.

Mode

Configuration mode

Example

```

encryptor> kdf -g
This will destroy the current Key derivation key.
and install a new one. It will be displayed once for distribution.
Do you wish to continue (y/n) ?y

```

```

Key Derivation Key:
bd6db004257ca63c1b8a0d42a051485fa859c0fbf7f463c07d47c2961ad377dd
HASH:
9a7c80afa55d9d8550a4498961cf3c9b172210bf63897b60e0560fc818acba294

encryptor> kdf -k 8b0bf71ad7a70e434063dccf21c5fbf3fd9608eb324321ed56288bfabec5039e
Key derivation key successfully installed

```



When a KDF is generated, any existing key derivation key within the encryptor is automatically erased.



When FIPS mode is enabled, the **-g** and **-k** commands are not available via the local CLI. The KDF may still be entered using CM7, SNMPv3, or the remote CLI.

kem

Synopsis

```
kem [-e]
```

Description

Display the quantum resistant algorithms used to create key encapsulations. A key encapsulation mechanism (KEM) secures symmetric key material for transmission using asymmetric (public-key) algorithms.

Arguments

-e

Edit the PQC key encapsulation selection

Mode

Configuration mode

keyprovider

Synopsis

```
keyprovider [-s | -k <time|ctr>]
```

Description

Specify the key provider used in TIM mode. Key synchronisation can be based on time (requiring a common NTP source) or a counter (removing the time dependency).

Arguments

-s

Set the key provider (presents a selection list)

-k <time|ctr>

Set the key sync mode to time or counter

Mode

Configuration mode

Example

```
encryptor> keyprovider
Key Provider mode is : Key Derivation Function
Key Sync mode is : TIME

encryptor> keyprovider -s
-->[01] Key Derivation Function
    [02] Key Server [KMIP]

Enter new Key Provider mode >: 02
Please ensure KeySecure is setup and KMIP enabled.
Key Provider Mode set to: Key Server [KMIP]
```



Changing the key provider mode does not restart the egress tunnel and it can take up to two key updates for it to take effect. It is recommended that the tunnel be manually restarted.

kscfg

Synopsis

```
kscfg [-a <addr> <tier> | -k <addr> <tier> | -e | -d | -E | -D | -r <idx> | -c | -C | -s]
```

Description

Enable, disable, and configure KeySecure remote server settings. Entries are maintained separately for the NAE-XML master key and the KMIP session key.

Arguments

-a <IPv4 or IPv6 addr> <tier>

Add a KeySecure server entry for the NAE-XML master key

-k <IPv4 or IPv6 addr> <tier>

Add a KeySecure server entry for the KMIP session key

-e

Enable KeySecure for the NAE-XML master key

-d

Disable KeySecure for the NAE-XML master key

-E

Enable KeySecure for the KMIP session key

-D

Disable KeySecure for the KMIP session key

-r <idx>

Remove a KeySecure server entry

-c

Clear all NAE-XML master-key KeySecure server entries

-C

Clear all KMIP session-key KeySecure server entries

-s

Set or clear the KeySecure key owner for the NAE-XML master key

Mode

Configuration mode

Example

```

encryptor> kscfg -a 192.168.1.10 1
encryptor> kscfg
KeySecure remote server settings
Index  Address      Tier
-----
1      192.168.1.10  1

encryptor> kscfg -e
KeySecure remote server enabled, config written

```

kstier**Synopsis**

```

kstier [-a <port> <proto tcp|ssl> <params> [<cert_idx>] | -k <port> <proto ssl>
<params> [<cert_idx>] | -d <idx> | -e <idx> <params> | -c | -C]

```

Description

Add, delete, and edit KeySecure tier configurations, supporting load balancing groups and multi-tier load balancing. Tier entries are maintained separately for the NAE-XML master key and the KMIP session key. The **<params>** are: connection pool size, timeout (ms), read timeout (ms), idle timeout (ms), and retry interval (ms).

Arguments

```

-a <port> <proto tcp|ssl> <params> [<cert_idx>]

```

Add a KeySecure tier entry for the NAE-XML master key

-k <port> <proto ssl> <params> [<cert_idx>]

Add a KeySecure tier entry for the KMIP session key

-d <idx>

Delete a KeySecure tier entry

-e <idx> <port> <proto tcp|ssl> <params> [<cert_idx>]

Edit a KeySecure tier entry

-c

Clear all NAE-XML master-key KeySecure tier entries

-C

Clear all KMIP session-key KeySecure tier entries

Mode

Configuration mode

Example

```
encryptor> kstier -a 1234 ssl 300 30000 30000 600000 600000
Enter certificate index: 6

encryptor> kstier
KeySecure tier entries
Index Tier Port Proto Pool Timeout Read   Idle   Retry  Certificate
          Size      Timeout Timeout Interval
-----
1      1  1234 ssl   300  30000  30000  600000  600000  98018d83
```

line

Synopsis

line [-e | -d]

Description

Enable or disable point-to-point (line) mode of operation. Changing between point-to-point and multipoint modes will reboot the encryptor.

Arguments

-e

Enable line mode

-d

Disable line mode

Mode

Configuration mode

Example

```
encryptor> line
Line mode: disabled

encryptor> line -e
Warning this command will reset all tunnel/CI, MAC
data to their factory defaults and reboot the unit!
do you wish to proceed ? (y/n) y
Are you sure ? (y/n) y
Line mode enabled
Resetting config and rebooting . . .
```



Changing between point-to-point and multipoint modes will reboot the encryptor.

linkspeed

Synopsis

```
linkspeed [-a <e|d> | -s | -m <e|d> | -f | -c <e|d>]
```

Description

Set the physical interface connection parameters for both local and network ports, including link speed, auto-negotiation, link loss forwarding, and local link monitoring.

Arguments

-a <e|d>

Enable or disable auto-negotiation

-s

Set the link speed (presents a selection list). The available speeds and media depend on the model and its port type; dual-port fixed-speed builds do not offer this option.

-m <e|d>

Enable or disable local link monitoring

-f

Set the Optical Link Loss Forwarding (oLLF) action

-c <e|d>

Enable or disable tying optical LLF to connection status (line mode only)

Mode

Configuration mode

Example

```

encryptor> linkspeed
Link parameter          Status
-----
Maximum link capability  1Gb/s Full Duplex
Configured link speed    100Mb/s Full Duplex
Current link status      100Mb/s Full Duplex
Current link status (Network) 100Mb/s Full Duplex
Current link status (Local)  100Mb/s Full Duplex
Auto Negotiation         enabled
Local link monitoring     disabled
Optical Link Loss Forwarding disabled
LLF tied to connection(line mode) enabled

encryptor> linkspeed -s
Link speed options:
  10Mb/s Full Duplex  (1)
-> 100Mb/s Full Duplex (2)
  1Gb/s Full Duplex   (3)
New link speed >: [2] 3
Link speed set to: 1Gb/s Full Duplex

```

locmacs

Synopsis

```
locmacs [-a <mac> | -d <mac> | -d * | -n]
```

Description

List the MAC addresses learnt from the protected (local) network in multipoint MAC mode. Each learnt MAC address is listed in this table but, unlike the netmacs table, local MAC addresses are not tied to a connection identifier.

Arguments

-a <mac>

Add a local MAC address

-d <mac>

Delete a specified local MAC address

-d *

Delete all local MAC addresses

-n

Display the count of local MAC addresses

Mode

Configuration mode

Example

```
encryptor> locmacs
```

```

Local Mac
-----
00:13:72:28:5e:62
00:12:3f:75:26:05
00:80:2d:6e:ee:20
00:15:f2:71:74:2c
00:0a:e4:3f:4a:71
00:e0:81:34:85:f5
6 Valid records

```



It is recommended to use auto-discovery mode to automatically populate this table to avoid misconfiguration.

logout

Synopsis

logout

Description

Log the current user out of the CLI and return to the login prompt.

Mode

User mode

Example

```

encryptor> logout
Welcome to Encryptor
Version: 4.0.0
Built: 14-Jul-2010 12:56:48
LOGIN:

```

mpls

Synopsis

mpls [-p <e|d> | -a]

Description

Set the policy for processing Ethernet frames tagged with labels on MPLS (Multi-Protocol Label Switched) networks. If protocol shim bypass is enabled, the encryptor will detect and ignore MPLS shim headers and base its policy on the ultimate ethertype.

Arguments

-p <e|d>

Enable or disable shim header bypass

-a

Set the alternate MPLS tag ethertype (0x8847 is built in)

Mode

Configuration mode

Example

```

encryptor> mpls
MPLS parameter                Status
-----
Protocol shim(s) bypass       enabled
Alternate MPLS ethertype      H8848

```

netmacs

Synopsis

```
netmacs [-a <mac> [-m] | -e <mac> | -d <mac> | -d * | -l <CI> [-m] | -n]
```

Description

List the MAC addresses learnt from the unprotected (network) network in multipoint MAC mode. Each learnt MAC address is tied to an encrypted tunnel whose connection identifier (CI) is listed in the table.

Arguments

-a <mac>

Add a network MAC address to the connection specified by CI

-a <mac> -m

Add a network MAC address to the connection specified by remote MAC

-e <mac>

Edit (move) a network MAC address to a different CI

-d <mac>

Delete a specified network MAC address

-d *

Delete all network MAC addresses

-l <CI>

List network MAC addresses for the connection specified by CI

-l <mac> -m

List network MAC addresses for the connection specified by remote MAC

-n

Display the count of network MAC addresses

Mode

Configuration mode

Example

```

encryptor> netmacs
Network Mac      CI
-----
00:d0:1f:01:06:4c 0001
1 Valid record

encryptor> netmacs -e 00:d0:1f:01:06:4c
Enter CI to associate mac address with : 2
Moved mac address

```

ntpcfg**Synopsis**

```
ntpcfg [-a <addr> | -d <idx> | -c | -p]
```

Description

Configure the addresses of NTP servers used by the encryptor to establish its date and time. The presence of at least one valid address enables NTP synchronisation.

Arguments

-a <IPv4|IPv6 addr>

Add an NTP server entry

-d <idx>

Delete an NTP server entry

-c

Clear all NTP server settings

-p

Print current NTP status

Mode

Configuration mode

Example

```

encryptor> ntpcfg
NTP server details
Index Address
-----
1      192.189.54.17
2      1.1.1.1
3      1.1.1.2

```


4 ::2

ocsp

Synopsis

```
ocsp [-a <url> | -c | -d <idx> | -e <idx> <url> | -p [idx] | -n <y|n> | -r [0-255] | -s  
| -u [interval] | -v <y|n>]
```

Description

View and manage Online Certificate Status Protocol (OCSP) server entries for the encryptor.

Arguments

-a <url>

Add an OCSP server entry (maximum of 8)

-c

Set the certificate used for signing OCSP requests

-d <idx>

Delete an OCSP server entry

-e <idx> <url>

Edit an OCSP server entry

-p [idx]

Print OCSP server entry details

-n <y|n>

Enable or disable the OCSP request nonce

-r [0-255]

Display or set the number of retries when an OCSP server is unreachable (default 0; Strict mode only)

-s

Set OCSP response handling to Strict mode

-u [interval]

Display or set the OCSP update interval (minutes)

-v <y|n>

Treat certificates with unknown OCSP status as valid

Mode

Configuration mode

Example

```
encryptor> ocsf -a y http://10.0.33.100
OCSP entry added

encryptor> ocsf -p
OCSP updates are disabled
Certificates with unknown status are treated as valid
OCSP request signing certificate is not set
Index SSL URL
1      Y   http://10.0.33.100
```

overview

Synopsis

```
overview [-c <contact> | -l <location> | -m <comment>]
```

Description

View and modify the encryptor's contact details, location information, and comments field. To clear an entry, specify the required option and an empty string ("").

Arguments

-c <contact>

Set the contact details (quoted string)

-l <location>

Set the location information (quoted string)

-m <comment>

Set the comments (quoted string)

Mode

Configuration mode

Example

```
encryptor> overview
Contact :
Location :
Comment :

encryptor> overview -c "for Support call +1 555 123456"
```

password

Synopsis

```
password [-r <0-255> | -o <0|1-240> | -e [on|off] | -m <8-29> | -u <1-2> | -l <1-2> |
-n <1-2> | -s <1-2> | -c <0-10>]
```

Description

View and modify the user password policy. Enhanced mode can be enabled to enforce additional security requirements including user lockout, password lexical checking at logon, and password expiry.

Arguments

-r <0-255>

Set the password reuse history size

-o <0|1-240>

Set the password change lockout period

-e [on|off]

Enable or disable enhanced password mode

-m <8-29>

Set the minimum password length

-u <1-2>

Set the minimum number of uppercase characters

-l <1-2>

Set the minimum number of lowercase characters

-n <1-2>

Set the minimum number of numerical characters

-s <1-2>

Set the minimum number of special characters

-c <0-10>

Set the maximum number of consecutive repeat characters (0 = disabled)

Mode

Configuration mode

Example

```
encryptor> password
Password enhanced mode: Disabled
Password lexical check: Enabled
Password reuse history: 255
Password requirements:
1. Length of 8-29 characters
2. At least 1 uppercase alpha character
3. At least 1 lowercase alpha character
4. At least 1 numerical character
5. At least 1 special character
```

```
encryptor> password -m 15
Minimum password length: 15
```

policy

Synopsis

```
policy [-s <-e|-d> | -k <-e|-d> | -p <options> | -m <-d|-b> | -a <all|l2> | -b <-e|-d>
| -l <-e|-d> | -f <-e|-d> | -e <idx> | -i <-e|-d> | -r <-e|-d> | -z <-e|-d> <proto> | -A
<-e|-d> | -M <mtu> | -d <sid> | -w <mode>]
```

Description

Configure miscellaneous Ethernet policy settings. The available options depend on the operational mode of the encryptor.

Arguments

-s <-e|-d>

Enable or disable STP monitoring to delete local MAC addresses

-k <-e|-d>

Enable or disable tunnel keep-alive monitoring

-p -a <mac>

Enable bypassing a specified MAC address when in VLAN connection mode

-p -e <idx>

Edit bypassing of a specified MAC address (by index)

-p -d <idx>

Delete bypassing of a specified MAC address (by index)

-m <-d|-b>

Enable or disable bypass/discard of default multicast/VLAN action

-a <all|l2>

In GCM mode, authenticate entire packet or shim + payload

-b <-e|-d>

Enable or disable bypass of reserved multicast addresses

-l <-e|-d>

Enable or disable bypass of IGMP or MLD packets

-f <-e|-d>

Enable or disable bypass of IP multicast header

-e <id>

Set the IP Protocol Encryption Identifier

-i <-e|-d>

Observe pending action for unknown DA on ingress

-r <-e|-d>

Enable or disable limited KID range for TIM mode

-z <-e|-d> tcp

Enable or disable bypass of zero-payload TCP frames

-z <-e|-d> udp

Enable or disable bypass of zero-payload UDP frames

-z <-e|-d> icmp

Enable or disable bypass of zero-payload ICMP frames

-z <-e|-d> ip

Enable or disable bypass of zero-payload IP frames

-A <-e|-d>

Enable or disable Path MTU adjustment

-M <mtu>

Set Path MTU maximum (576—10000 bytes, 0 = disabled)

-d <sid>

Set the Sender ID when in VLAN/ISID connection mode (1—512, 0 = disabled)

-w <strict|window|disabled>

Set replay protection mode

Mode

Configuration mode

Example

```

encryptor> policy
Policy parameter(s)      Status
-----
Bypass Reserved Multicast disabled
STP Monitoring           disabled
Tunnel Keep Alive Monitoring disabled
Observe Pending on unknown (DA) Ingress disabled
Sender ID = 000         Disabled

encryptor> policy -s -e

```

STP monitoring enabled

profile

Synopsis

```
profile [-f | -s]
```

Description

Set the administrative mode to either standard (four roles: Administrator, Supervisor, Operator, Upgrader) or simplified (two roles: Administrator, Operator). Changing this setting requires an erase and reboot.

Arguments

-f

Set full/standard administrative mode

-s

Set simplified administrative mode

Mode

Configuration mode

Example

```
encryptor> profile
Profile: Full/Standard

encryptor> profile -s
WARNING: Changing the profile mode will erase the configuration
and reboot this encryptor
Do you wish to proceed ? (y/n) n
Profile mode unchanged
```



Changing this setting will erase the configuration and reboot the encryptor.

prompt

Synopsis

```
prompt <name>
```

Description

Set the CLI prompt to a custom name (maximum 30 characters), such as encryptor location or asset number. The value is stored in non-volatile memory and preserved across reboots.

Arguments

<name>

The new prompt string (maximum 30 characters)

Mode

Configuration mode

Example

```
encryptor> prompt Adelaide1
Adelaide1>
```

protocol

Synopsis

protocol [-s]

Description

Select the protocol and link-speed configuration for the encryptor. The available options are determined by the model and the loaded license, and may include 1—4 links at 1 Gbps or 10 Gbps. Executing the protocol command deletes any S-Box definition files and forces a reboot.

Arguments

-s

Set the protocol (presents a selection list)

Mode

Configuration mode

Example

```
encryptor> protocol -s

Global Speed Configuration options:
--> (1) Ethernet - 1Gbps
    (2) Ethernet - 10Gbps
    (3) Ethernet - 4x1Gbps
    (4) Ethernet - 4x10Gbps
Enter new Global speed >: [1] 2
Warning this command will erase the configuration to factory defaults
and reboot the encryptor!
Do you wish to proceed? (y/n)
```



Changing the protocol erases the configuration and reboots the encryptor.

reboot

Synopsis

reboot

Description

Perform a complete reboot of the encryptor. During the reboot process, no traffic will pass through

the unit.

Mode

Configuration mode

Example

```
encryptor> reboot
Are you sure you want to reboot the unit ? (y/n)
```

rest

Synopsis

```
rest [-e | -d | -s]
```

Description

Enable or disable the RESTful server, which provides remote monitoring of the encryptor via a web browser. Access is controlled via user console access rights.

Arguments

-e

Enable the RESTful server

-d

Disable the RESTful server

-s

Set the HTTPS server certificate (end-user certificate)

Mode

Configuration mode

Example

```
encryptor> rest
REST server is disabled
REST https server certificate hash: 675af1b2

encryptor> rest -e
Enabled RESTful server.
```

sbox

Synopsis

```
sbox [-e | -i | -d | -v]
```


Description

Insert, update, or delete a custom S-Box. This command is only available if the encryptor is not in FIPS mode. Only users with administrative credentials can manage an S-Box.

Arguments

-e

Echo characters when entering a custom S-Box definition (default is no echo)

-i

Insert a custom S-Box and its corresponding test vectors (will reboot)

-d

Delete the custom S-Box and revert to default AES S-Box (will reboot)

-v

Display a detailed help message showing the expected S-Box format

Mode

Configuration mode



The update process uses the **-i** option to replace an existing S-Box. If insertion fails, the previous S-Box is retained.

sfp

Synopsis

sfp [-l | -n | -d | -v]

Description

Display information reported by the Small Form Pluggable (SFP) transceivers plugged into the local and network ports.

Arguments

-l

Display local port SFP information

-n

Display network port SFP information

-d

Display SFP diagnostics

-v

Display verbose SFP information

Mode

User mode

Example

```
encryptor> sfp -lvd
```

SFP LOCAL PORT SERIAL DIGITAL DIAGNOSTICS

```

Vendor Name       = FINISAR CORP.
Vendor Part Number = FTRJ1421P1BCL
Vendor Serial Number = P8N1KRG
Vendor Revision    = A
Date Code         = 051124
Ethernet Compliance = 1000BASE-LX
Encoding          = SONET Scrambled
Nominal Bit Rate   = 2500 Mbits/s
Link length (9/125) = 20000 m
Laser Wavelength   = 1310 nm

```

=====							
	Warning Limits		Alarm Limits		Flags		
=====							
Parameter	Measured	High	Low	High	Low	Warn	Alarm
Temperature(C)	+39.19	+93	-3	+110	-9	OK	OK
VCC (V)	+3.25	+3.7	+3.05	+4.00	+2.80	OK	OK
TX Bias (uA)	18668	70000	4000	8400	2000	OK	OK
TX Power (dBm)	+0.93	+4.90	-4.10	+6.90	-6.10	OK	OK
RX Power (dBm)	-33.98	+5.49	-13.58	+7.26	-17.67	LOW	LOW

shim

Synopsis

```
shim [-r <0-32767> | -m <e|-d>]
```

Description

Set the shim insertion rate for CTR and GCM encryption modes. A value of 1 shims every frame; a value of 32 shims every 32 frames. Lower shim rates increase throughput but extend error recovery time if loss occurs.

Arguments

-r <0-32767>

Set the shim insertion rate (0 = disable)

-m <e|-d>

Enable or disable MTU overflow prevention on shim insertion

Mode

Configuration mode

Example

```
encryptor> shim
SHIM parameter      Status
-----
SHIM rate           32
MTU overflow prevention on shim enabled
```



It is not recommended to use a shim rate setting of 0 because this completely disables shim insertion.

snap

Synopsis

```
snap [-p <e|-d>]
```

Description

Set the policy for processing Ethernet frames in the IEEE 802.3 LLC SNAP format. If SNAP PID for ethertype processing is enabled, the frame is encrypted based on the SNAP PID. If disabled, the frame is processed according to the length-encoded frame policy (ethertype `0x05FF`).

Arguments

```
-p <e|-d>
```

Enable or disable observing SNAP PID for ethertype processing

Mode

Configuration mode

Example

```
encryptor> snap
SNAP parameter      Status
-----
Observe SNAP PID for ethertype processing enabled

encryptor> snap -p -d
SNAP PID for ethertype processing disabled
```

snmpcfg

Synopsis

```
snmpcfg [-e [on|off] | -q [on|off] | -p [on|off] | -s [on|off] | -v [on|off] | -w <x> | -f <x>]
```

Description

Configure SNMPv3 privacy settings. Privacy can only be disabled if FIPS mode is disabled, as SNMP privacy is mandatory for FIPS compliance.

Arguments

-e [on|off]

Enable or disable SNMP Enhanced AUTHPRIV (SHA512/AES256)

-q [on|off]

Enable or disable SNMPv3Q Quantum Hybrid mode

-p [on|off]

Enable or disable SNMP privacy

-s [on|off]

Enable or disable SNMP TCP transport over SSH

-v [on|off]

Enable or disable SNMPv1

-w <x>

Set the time window (minutes) for USM authentication errors (0 = disabled)

-f <x>

Set the number of USM authentication errors before lockout

Mode

Configuration mode

Example

```
encryptor> snmpcfg
SNMP Privacy mode enabled

encryptor> snmpcfg -p off
Disable SNMP Privacy selected. Validation...succeeded.
SNMP Privacy Disabled
```

snmptraps**Synopsis**

snmptraps [-a <addr> [-v <2|3>] [-s <model>] | -e <idx> | -d <idx> | -r <idx> | -p]

Description

Add, enable, disable, or remove entries in the SNMPv3 trap server list.

Arguments**-a <IPv4|IPv6 addr>**

Add an SNMPv3 trap server entry

-v <2|3>

Set the SNMP trap type (default is v2)

-s <AuthPriv|AuthNoPriv|NoAuthNoPriv>

Set the SNMPv3 trap type server security model

-e <idx>

Enable an SNMPv3 trap server entry

-d <idx>

Disable an SNMPv3 trap server entry

-r <idx>

Remove an SNMPv3 trap server entry

-p

Purge all SNMPv3 trap server entries

Mode

Configuration mode

sshaux

Synopsis

sshaux [-a | -e | -c | -p | -s]

Description

Configure tertiary SSH access for remote devices via the auxiliary management port. Only EC key exchange algorithms are supported when using the auxiliary port.

Arguments

-a

Enable the remote auxiliary management port

-e

Access the AUX port via CLI

-c

Connect using public key authentication

-p

Enforce PAM (username/password) for login

-s

Set the default SSH destination

Mode

Configuration mode

Example

```
encryptor> sshaux -a  
SSHAUX enabled
```

sshcli

Synopsis

```
sshcli [-a <"key string"> | -e | -d | -p | -r <idx> | -c | -l <e|d>]
```

Description

Enable or disable SSH CLI access. SSH public keys can be added to a table and the SSH server port can be specified. Only ECDSA key pairs are valid for SSH use.

Arguments

-a <"key string">

Add an SSH public key entry (double-quote the key)

-e

Enable remote SSH CLI access

-d

Disable remote SSH CLI access

-p

Set the SSH server port number

-r <idx>

Remove an SSH public key entry

-c

Clear all SSH public key entries

-l <e|d>

Enable or disable SSH verbose logging to the event log

Mode

Configuration mode

Example

```
encryptor> sshcli -e  
SSH enabled
```



It is recommended that verbose logging is left disabled unless diagnosing connectivity issues.

stats

Synopsis

```
stats [-l | -n | -r | -u | -p]
```

Description

Display statistics for the local and network ports, including frame counts, error counts, utilisation bandwidth, and policy statistics.

Arguments

-l

Show local port statistics

-n

Show network port statistics

-r

Reset all statistics

-u

Show instantaneous utilisation bandwidth

-p

Show policy statistics

Mode

User mode

Example

```
encryptor> stats
Ethernet Local Port Statistics:
Rx Corrupted Frames    = 0
Rx Interframe Gap Errors = 0
Rx Octet Count         = 0
Rx Frame Count         = 0
Rx FCS Errored Frames  = 0
Rx PCS Errored Frames  = 0
Rx Undersized Frames   = 0
Rx Oversized Frames    = 0
Rx Discarded Frames    = 2
Rx PCS Sync Status     = In Sync
Tx Octet Count         = 0
Tx Frame Count         = 2
Tx FCS Errored Frames  = 0

Ethernet Network Port Statistics:
Rx Corrupted Frames    = 0
Rx Octet Count         = 0
Rx Frame Count         = 0
Tx Octet Count         = 71202
```

```
Tx Frame Count      = 343
Tx FCS Errored Frames = 0
```

syslog

Synopsis

```
syslog [-a <addr>[:port] [A] | -d <idx> | -p | -f <on|off> | -s <on|off> | -S <e|-d>]
```

Description

Configure syslog server entries for the encryptor. Up to 10 distinct servers can be configured using IPv4 or IPv6 address notation. DNS lookup is not supported. Extended timestamps follow the RFC3164 format.

Arguments

-a <IPv4|IPv6 addr>[:port] [A]

Add a syslog server entry (append **A** to direct the entry to the auxiliary port)

-d <idx>

Delete a syslog server entry

-p

Purge all syslog server entries

-f <on|off>

Enable or disable the extended timestamp format (RFC3164)

-s <on|off>

Enable or disable tunnelling of syslog messages via SSH

-S <e|-d>

Enable or disable inclusion of system logs

Mode

Configuration mode

Example

```
encryptor> syslog -a fc0f:1234::1
Restarting system log daemon: syslogd.

encryptor> syslog
NB: Event messages are syslog facility Local5.*
    Audit messages are syslog facility Local4.*
Index Address
-----
1      10.65.65.118
2      fc0f:1234::1
```




SSH CLI must be enabled on the encryptor and the public key of the syslog server must be added to the SSH CLI table before enabling SSH tunnelling of syslog messages.

tacacs

Synopsis

```
tacacs [-a <addr[:port]> <timeout> <key> | -e | -d | -p | -r <idx> | -c | -b <on|off> |  
-s <password>]
```

Description

Define and manage TACACS+ server connections. Entries can be added for IPv4 and/or IPv6 servers.

Arguments

-a <IPv4 or IPv6 addr[:port]> <timeout> <key>

Add a TACACS+ server entry

-e

Enable TACACS+

-d

Disable TACACS+

-p

Change password for TACACS+ account

-r <idx>

Remove a TACACS+ server entry

-c

Clear all TACACS+ server settings

-b <on|off>

Broadcast audit notifications to all servers

-s <password>

Set the SNMPv3 USM TACACS+ user password (this is not the user password)

Mode

Configuration mode

timezone

Synopsis

```
timezone [-s | -c]
```

Description

Set the timezone of the encryptor to that of its physical location. The command presents a hierarchical selection of region, country, and timezone.

Arguments

-s

Set the timezone (interactive selection)

-c

Reset the timezone to its default

Mode

Configuration mode

Example

```
encryptor> timezone -s
Please select region >: 7
Timezone options for Australia:
(1) Lord Howe Island
(2) Tasmania - most locations
(3) Tasmania - King Island
(4) Victoria
(5) New South Wales - most locations
...
Please select timezone >: 4
Selected timezone information:
Country name: Australia
Timezone name: Melbourne
Timezone comments : Victoria
Offset to UTC: +10.00
Do you wish to change to new timezone? (y/n)
```

transec

Synopsis

```
transec [-a <dst> <src> [header] | -r <rate> | -b <rate> | -c <rate> | -e | -d | -p |
-l <length> | -t <ethertype>]
```

Description

Enable or disable TRANSEC framing and configure the parameters used to generate transport frames. When configuring maximum throughput, allow for client traffic and encryptor management traffic.

Arguments

-a <dst> <src> [header]

Set header information (hex)

-r <rate>

Set rate in frames per second

-b <rate>

Set rate in bits per second

-c <rate>

Set rate as a percentage

-e

Enable TRANSEC mode

-d

Disable TRANSEC mode

-p

Display TRANSEC configuration information

-l <length>

Set frame length in bytes

-t <ethertype>

Set frame ethertype (hex)

Mode

Configuration mode

Example

```
encryptor> transec
Transec mode is disabled

encryptor> transec -e
Warning this command will enable TRANSEC mode
and reboot the unit!
do you wish to proceed ? (y/n) y
TRANSEC mode enabled
Rebooting . . .
```

tunnels

Synopsis

```
tunnels [-a <options> | -d <CI> | -d * | -e <CI> | -l <CI> | -l * | -L | -s <CI> | -s *
| -r <CI> | -r * | -k <n> | -i <n> | -c <CI> | -C <CI> | -f <CI> | -x [on|off] | -p <n>
| -P [on|off]]
```

Description

View and control encrypted connections (tunnels). In line mode the encryptor has one connection; in multipoint MAC mode it may have up to 512 connections (three reserved by the system).

Arguments

-a <options>

Add a tunnel (MAC address or VLAN tags with action: **sec**, **dis**, **byp**)

-d <CI>

Delete the tunnel specified by CI

-d *

Delete all tunnels

-e <CI>

Edit the tunnel specified by CI

-l <CI>

List the tunnel specified by CI

-l *

List all tunnels

-L

List all tunnel VLANs in decimal

-s <CI>

Stop the tunnel specified by CI

-s *

Stop all tunnels

-r <CI>

Restart the tunnel specified by CI (renegotiate session keys)

-r *

Restart all tunnels

-k <n>

Set the key update interval (1—60 minutes)

-i <n>

Set the re-authentication update interval (hours, 0 = disabled)

-c <CI>

Set the primary certificate to use for the specified CI

-C <CI>

Set the ancillary certificate to use for the specified CI

-f <CI>

Clear the RX/TX counters for the specified connection

-x [on|off]

Enable or disable X.509v3 certificate expiry checks for established tunnels

-p <n>

Set the peer detection interval (0—10 seconds, 0 = disabled)

-P [on|off]

Prohibit or allow acting as a group key master



The re-authentication update interval (**-i**) and key update interval (**-k**) behave differently depending on the connection type and certificate in use:

- **Unicast Connections (ECDSA & Hybrid ECDSA+PQC):** Certificate re-authentication occurs automatically on every key update (defined by **-k**), regardless of the re-authentication interval setting (**-i**). For hybrid connections, both the ECDSA and PQC components are automatically re-authenticated.
- **Unicast Connections (RSA & Hybrid RSA+PQC):** Re-authentication does not occur on key updates unless the re-authentication interval is configured (**-i <n>** where **n > 0**). By default, **-i** is set to **0** (disabled).
- **Group Connections (All Certificate Types):** Re-authentication does not occur on key updates unless the re-authentication interval is configured (**-i <n>** where **n > 0**). When configured, group members check the validity status of both their own certificates and those used by other members of the group once the interval has been exceeded.

Mode

Configuration mode

Example

```
encryptor> tunnels
Interface (tunnel/CI) MAC address      : 00:d0:1f:02:00:6e
Front Panel Management MAC address    : 00:d0:1f:01:06:4c
CI   Origin Action State Peer Name     Remote Encryptor MAC  MAC Header
-----
0001 System Secure Up   TooterTurtle  00:0d:b9:12:eb:52

encryptor> tunnels -a 00:0d:b9:12:eb:52
```

```
Remote Encryptor Name : [] TooterTurtle  
Tunnel Action: <(D)iscard | (B)ypass | (S)ecure>: [Discard] S  
Extra header length (0,4,8) : [0] 0  
Added new tunnel ci 4
```

upgrade

Synopsis

upgrade

Description

Initiate a firmware upgrade using an image supplied via a USB memory stick. Prior to issuing the command, the user must log in using an **admin** account.

Mode

Configuration mode



Senetas encryptors support only USB drives configured with the FAT or FAT32 format.

usb

Synopsis

usb [lock | unlock]

Description

Prevent or allow access to the encryptor front panel USB interface via a logical locking mechanism. If the port is locked, the encryptor will not respond to any USB device, including memory sticks containing a valid firmware upgrade.

Arguments

lock

Disable the USB port

unlock

Enable the USB port

Mode

Configuration mode

Example

```
encryptor> usb  
USB port is unlocked
```

users

Synopsis

```
users [-a | -e <index> | -n | -d <index> | -v <e|-d> | -u <days> | -s <mins>]
```

Description

View and edit the table of authorised system users. Only an Administrator can add new accounts or make changes to existing accounts.

Arguments

-a

Add a user (interactive prompts for user details)

-e <index>

Edit the user at the specified index

-n

Show the number of users

-d <index>

Delete the user at the specified index

-v <e|-d>

Enable or disable admin account logout

-u <days>

Set the user inactivity account timeout (0—1825 days; 0 = disabled)

-s <mins>

Set the session inactivity timeout (3—60 minutes)

Mode

Configuration mode

Example

```
encryptor> users
Number of users in table is 1
Index UserId  Active Level           Console Snmp
-----
1      admin   Yes   Administrator Yes      Yes

encryptor> users -a
User id: <3-10 characters>: [] glen
User name: <max 30 characters>: [] simmons
Status: <(A)ctive | (I)nactive>: [Active]
Level: <(A)dmin | (S)uper | (O)perator | (U)pgrader >: [Operator]
Console access: <(E)nabled | (D)isabled>: [Enabled]
SNMP access: <(E)nabled | (D)isabled>: [Enabled]
```

```

Auth password: <8-29 characters>: *****
Confirm password: <8-29 characters>: *****
Privacy password: <8-29 characters>: *****
Confirm password: <8-29 characters>: *****
Password expiry: <yyyy-mm-dd | (S)ixty days | (D)isabled>: [0000-00-00]
Is the information correct? (y/n/q) y
New record added - index 3

```

version

Synopsis

version

Description

Display software version information for the encryptor, including version numbers, build date and time, and library build ID.

Mode

User mode

Example

```

encryptor> version
Software:
Version      : 2.7.1
Build Number : 1283747687
Build Date   : 06-Sep-2017
Build Time    : 04:34:47
Library
Build ID: D753

```

vlan

Synopsis

vlan [-p <e|-d> | -1 | -2 | -m <e|-d> | -v <tag(s)> | -s]

Description

Set the policy for Ethernet frames that have IEEE 802.1Q headers. The CN Series supports stacking up to a maximum of two nested VLAN tags.

Arguments

-p <e|-d>

Enable or disable VLAN protocol tag bypass

-1

Set the VLAN primary ethertype (0x8100 is built in)

-2

Set the VLAN alternate ethertype (0x8100 is built in)

-m <e|-d>

Enable or disable multicast management VLAN substitution

-v <tag(s)>

Set VLAN tag(s) for multicast VLAN substitution (e.g. 81000001 or 8100000181000002)

-s

Set the number of stacked VLAN IDs used to establish a VLAN connection

Mode

Configuration mode

Example

```
encryptor> vlan
VLAN parameter          Status
-----
Protocol tag(s) bypass   enabled
Alternate VLAN ethertype H8100
```