

Senetas Corporation

CN6140 Encryptor

All Operational Modes

Secure, encrypted data in motion



Senetas CN6140 Encryptor

Document Identifiers

Document: CN6140_ETH_CM7

Document revision: 55-24-010

Revision date: *October 2024*

Compatibility

This manual covers the procedures for setting up, commissioning and operation of the encryptor listed in the table below, using the firmware shown.

Applicability and version support	
CN6140, model A6140B/41B/42B - Dual AC/Dual DC/AC-DC supply	v5.5.0
CM7 Management system (Windows® or MacOS or Linux)	v7.10.0

Copyright © 2024 Senetas Corporation. All rights reserved.

Compliance

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of 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 and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

NOTE: If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- 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.

WARNING: Any changes or modifications not expressly approved by Senetas Corporation could void your authority to operate this equipment.

Senetas documentation is produced in English and may be subject to translation for use in the 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. *(This statement must remain in English.)*



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.



Senetas Security Pty. Ltd.

312 Kings Way

South Melbourne, Victoria 3205

Australia

Customer Support Portal

Email

Office

Australia

United Kingdom

USA and Canada

<https://support.senetas.com>

support@senetas.com

Phone

1-800-270-923

0-808-189-1247

1-800-470-3520

Senetas Corporation Limited.

312 Kings Way

South Melbourne, Victoria, 3205, Australia.

(T) +61 (03) 9868 4555 (F) +61 (03) 9821 4899

© 2024 Senetas Corporation Limited

Web site: www.senetas.com

Senetas Europe Ltd.

Worting House, Church Lane

Basingstoke, Hants, RG23 8PX, UK.

(T) +44 (0) 1256 345599 (F) +44 (0) 1256 811876

User Guide published: Wednesday, 30 October 2024



Introduction

Senetas hardware and software encryption platforms ensure that information is protected as it transits through the network from one location to another. Senetas, based in Melbourne Australia has been designing and manufacturing encryptors for more than a 20 years and has supplied units worldwide to governments, law enforcement agencies, military, financial and other commercial organisations. This manual is intended to provide you with a complete understanding of the Senetas product family and more importantly the role it can play in protecting critical data. This manual includes specific details for the Ethernet Encryptor CN6140 (hereinafter may also be referred to as the "CN6140 Encryptor").

The need for data encryption within the data centre is generally well understood, however the need to secure data-in-transit, that is the data traversing the network, is often overlooked. In reality the security of your data is only as good as that provided by the weakest link and both data-at-rest and data-in-transit must be protected.

NOTE: This document describes the configuration of encryptors at both **Layer 2** and **Layer 2-4**. Where applicable content is annotated with a "(only Layer 2)" or similar identifier so that you can readily determine if the content applies to your needs.

This document is organised into a number of chapters that describe all aspects of the Senetas product and its application. These include; networks, risk, encryption, commissioning, security, certificate and keys, platforms, protocols, installation, management and troubleshooting.

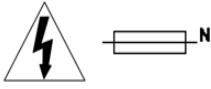
A highlighted section such as this...

..... is used to provide summary information that allows you to gain a high level understanding of the content.

This presentation allows scanning of the content of a chapter to quickly focus on those areas that deliver in-depth coverage of an area of interest.



Safety warnings



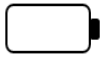
CAUTION: Double pole/neutral fusing

ATTENTION: Fusion pôle double/neutre



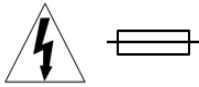
WARNING: Disconnect all power supply cords before servicing.

ATTENTION: Débrancher tous les cordons d'alimentation avant l'entretien.



CAUTION: Risk of explosion if battery is replaced by an incorrect type. Dispose of used batteries in accordance with local laws. Do not charge, heat, open or dispose of in a fire.

ATTENTION: Risqué d'explosion si la batterie est remplacée par un type incorrect. Jetez les piles usagées conformément aux lois locales. Ne pas charger, chauffer, ouvrir ou éliminer dans un incendie.



CAUTION: For continued protection against risk of fire, replace only with the same type and rating of fuse.

ATTENTION: Pour une protection continue contre les risques d'incendie, remplacer uniquement avec le même type et calibre du fusible.

Audience

This document has been written to meet the needs of the broad cross section of readers who have an interest in Senetas encryptors. By including comprehensive information for the complete product range it provides the following:

- An understanding of encryption and products philosophy.
- The requirements of different networks and the way in which the products address these.
- The installation of encryptors
- The configuration of encryptors to meet customer needs.
- The administration of encryptors.
- The diagnosis of any issues that could occur.

It is assumed that the reader is familiar with:

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



Companion documents that contain only a limited number of chapters are also available and these are usually provided for training purposes.

Navigating this document

The 'Table of Content' provides structured access to all of the material that is contained within the document.

Active links are provided throughout to allow navigation within online copies of the manual.

In addition, a comprehensive linked index is provided which is supported by a glossary that explains the many acronyms that are used throughout the communications industry.

Applicability of content

This document describes mutually exclusive features that may not be of interest to the reader. To assist navigation subject matter headings have text appended that describes the applicability. For example if both "Layer 2 VLAN" and "Layer 3 TIM" modes are described, a VLAN related heading might be appended with "(layer 2 VLAN only)".

Senetas documentation includes information that requires particular attention or understanding. The three types of highlighted paragraphs are:

NOTE: This could be a reminder regarding the format of some required information.

WARNING: Highlights that extra care should be taken when performing a task.

CAUTION: Information emphasised because, for example, taking an action incorrectly will cause operational errors or system failure.



Table of Contents

Senetas CN6140 Encryptor	i
Document Identifiers	i
Compatibility	i
Compliance	i
Company and Partner Support Contact Information	ii
Introduction	iii
Safety warnings	iv
Audience	iv
Navigating this document	v
Section 1: Encryption platform	2
CN6140 Encryptors	2
CN6140 Encryptor	3
CN6140 indicators	4
CN6140 LCD backlight	5
CN6140 Network interfaces	5
Encryptor connections	7
Fan tray	7
Battery	7
Pluggable Module Descriptions	8
Optical interface detail	9
Transceiver Vendor codes	11
Forward Error correction	12
Latency	12
Initial power-up	12
Boot up sequence	12
Encryptor Connections	15
Management interfaces	15
Management port statistics	15
Connecting to the Ethernet management port	16
Connecting to the serial management port	16
Personal computer settings	16
Connecting to the local and network ports	17
Local port statistics	17
Network port statistics	19
Environmental requirements	21
Encryptor platform location	22
Commissioning	23
Setting the IP address	23
Setting Name and Date/Time	24
Activation	25
TIM configuration	25
Multi-Slot configuration	26



Certification	27
Firmware Upgrades	27
User defined entropy	29
Preparing the .ent file	30
Monitoring	30
Quantum Origin entropy source integration and support	30
Rate limiting	31
Section 2: Encryption protocols	34
Maximum Transmission Units	34
Introduction	34
MTU considerations	35
Algorithm support	38
Ethernet encryption	39
Basic operation	40
Operation within networks	40
Modes of operation	41
Cryptographic modes	42
Connection modes	43
Connections	43
DEK Pairwise and Group keys (only layer 2)	44
Replay Protection	45
Replay protection settings	45
Replay protection mode statistics	46
Point-to-Point (Layer 2) Line encryption	56
When to use Line mode encryption	56
Operation mode	57
Point-to-point Ethertype policy	57
Configuring Point-to-Point (line) mode	60
Point-to-Point configuration using the CLI	61
TRANSEC	62
Multipoint (Layer 2) MAC encryption	71
Operation mode	72
Ethertype policy	72
MAC address policy and connections	75
MAC address mode of operation	75
MAC Connection Establishment	76
MAC migration	77
Spanning Tree Protocol support	78
Automatic configuration using the CLI	81
Manual configuration using the CLI	84
Multipoint (Layer 2) VLAN encryption	90
Operation mode	91
VLAN Policy settings	91



VLAN Ethertype policy	92
Configuration using the CLI	95
Transport Independent Mode (TIM) (Layer 2, 3 and 4 encryption)	96
Key Identifier (KID)	96
Layer 4 Encryption Mode	97
Key Provider model	97
Traffic encryption	100
TIM policy	101
UDP Tunnelling	103
Key synchronization	105
Encrypted Frame formats	107
Configuration using the CLI	107
Ethernet Protocol(only layer 2)	109
MAC connection mode - Unicast operation	109
Multicast operation	109
Broadcast operation	110
Performance	110
Control plane ethertype	110
Ethernet frame formats	111
Ethernet II (DIX)	111
IEEE 802.3 SAP (with 802.2 LLC header)	111
IEEE 802.3 SAP SNAP	112
VLAN	112
Stacked VLAN	113
MPLS shims	113
TIM frame formats	114
Section 3: Encryptor management overview	115
Encryptor management	115
CM7 network manager	115
Command Line Interface	115
Third-party managers	115
Defining user accounts	116
Administrator access	117
User Inactivity Lockout	118
Administrator Lockout	119
SNMPv1 monitoring	120
User account management	122
RESTful JSON interface	123
RESTful examples	124
SSH Access of Remote Devices	128
CM7 Navigation	129
Sorting discovered encryptors	132
Configuring the discovered encryptor list	133



Installing CM7	133
Windows CM7 installation	134
Linux CM7 installation	136
MacOS CM7 installation	137
Launching and Logging in to CM7	139
Configuring CM7	140
Creating the PKCS#12 file	143
Certificate hash algorithm	144
Certificate Authorities	144
Advanced CA functions	146
Elliptic Curve Parameters screen	149
Importing and exporting CA files	150
QRA-based key generation	152
KDK Key generation	155
Deleting PKCS#12 files	156
Initial configuration settings	157
Moving CM7 to a new PC	159
CM7 Screen selection	160
CM7 Multi-User Mode	160
SNMP security level	160
Discover screen	162
Activate screen	162
Certify screen	164
Internal Certification	165
External certification	167
CM7 Licensing pane	168
KeyVault	170
Key Screen (only layer 3/4)	171
Manage screen	173
Management options	173
Front panel mimic	175
System pane	177
Date/Time pane	178
User	180
Console Management	181
Network addresses	182
SNMP	184
Syslog Server Configuration	184
FTP/FTPS server configuration	187
KeySecure	187
TACACS+	189
Remote Secure Shell CLI access	189
Certificates	192



Certificate Servers	194
Slot	197
License	198
Policy	198
Key Derivation Function	202
Protocol	203
Protocol - Ethertypes	203
IP Rules	205
Connections	208
Quantum Key Distribution (only layer 2)	214
Encryption Interfaces	215
Diagnostics	217
Alarms	220
Audit Log	221
Event Log	221
Upgrade screen	221
External upgrade	222
Internal upgrade	223
Exiting from CM7	224
Section 4: Command Line Interface (CLI)	225
CLI Management	225
CLI connection	225
Customising the CLI	225
Hosts and slots	226
Commands	226
Section 5: SNMP Management	227
SNMP connections	227
Direct connection to front panel	228
SNMP Enhanced Algorithm Support	228
In-band overview	229
Inband connection	229
In-band connection via a local encryptor	229
Inband management concept	230
Enabling Inband management	231
Inband configuration	231
Inband for Multi-slot encryptors	233
Routing considerations	233
Virtual management	234
Out-of-band management	234
In-line management through the encryptors	235
Section 6: Encryptor Troubleshooting	236
Configuration Export	236
Configuration Import	236



Traffic analysis	236
Ethertype diagnostics	237
ePing command	237
Cannot add a connection to the connection table	237
Traffic processing (only layer 3, 4)	240
Safety warnings	241
Section 7: CLI Command Library	242
activate	242
alarm	243
audit	243
autodisco	244
autopop	245
banner	246
certificate	246
community	251
con	251
controlplaneif	251
crl	251
crypto	252
date	253
entropy	253
eping	254
eqkd	255
erase	256
ethertypes	257
event	259
fips	260
ftpcfg	261
global	261
help	262
helpall	262
history	263
hostname	263
inband_vlan	263
initcfg	265
inventory	270
ip	271
iprules	274
kdf	276
kem	277
keypad	277
keyprovider	277
kscfg	278



kstier	279
line	280
linkspeed	281
locmacs	283
logout	284
mode	285
mpls	285
netmacs	286
ntpcfg	287
ocsp	287
overview	288
password	288
policy	292
profile	295
prompt	296
protocol	296
psu	296
qkd	297
qsfp	298
reboot	299
rest	300
sfp	301
shim	302
slot	303
snap	304
snmpcfg	305
snmptraps	305
sshaux	306
sshcli	306
stats	307
syslog	309
tacacs	311
timezone	311
transec	313
tunnels	314
upgrade	317
usb	317
users	317
version	318
vlan	319
Section 8: Open Source Licences	321
Section 9: Alarms, event and audit logs	323
Logs	323



Alarms	323
Event log	324
Audit log	325
SNMP Traps	325
Appendix A-1 Audit log messages	327
Appendix A-2 Event log messages	334
Appendix A-3 Alarm messages	341
Appendix A-4 SNMP trap messages	344
Index	349





Section 1: Encryption platform

This section describes the encryption platform and its related protocols.

CN6140 Encryptors	2
CN6140 Encryptor	3
Forward Error correction	12
Encryptor Connections	15
Commissioning	23
User defined entropy	29
Rate limiting	31

CN6140 Encryptors

Senetas encryptors secure high-speed networks using the proven Advanced Encryption Standard (AES) encryption algorithm. Point-to-point and multi-point, wire-speed encryption with low latency and no packet expansion is made possible by operating at Layer 2 of the OSI model.

Layer 2 encryption is often referred to as a “bump in the wire” technology as it has nearly no overhead and allows the use of the entire bandwidth. Link latency is constant and less than . Furthermore, it ensures protection of all traffic on the network. The frame size can be in the range 64 to 10,000 the upper limit being reduced by the size of any inserted shims, for example in VLAN mode with GCM enabled this would be 9976.

TIM mode encryption at layers 2, 3 and 4 is supported on all CN6000 series encryptors.

The encryptors have received stringent international security accreditations - Common Criteria EAL2+ and FIPS 140-3 Level 3.

The Senetas solution integrates seamlessly into existing network infrastructures. The simple installation procedure and set-and-forget operation ensures rapid deployment and minimal maintenance requirements. Advanced management tools allow easy provisioning and control of security policies for audit and compliance. Group key management and separation of duties underpin best security practices while advanced networking and diagnostic features ensure uncompromising performance.

The CN6140 enclosure is fabricated from steel and designed to fit into 19"-wide (482 mm) communications equipment racks. The units are one rack unit (1U) high (44 mm).

The CN6140 of encryptors have the following interfaces:

- LAN RJ45 auto-negotiating 10BASE-T/100BASE-TX/1000BASE-T Ethernet connector for system management
- CON RJ45 RS232 serial connector for local (CLI) configuration
- USB connectors used for software upgrade capability
- Four line LCD display for user notification
- LED indicators that show the status of the unit.
- Local and network interface ports
- Keypad for user input



Table 1. Key functions

Button	Selection	Configuration
ESC	Return to the first configuration item	Cancel the current choice
Up Arrow	Display the prior configuration item.	Show the previous choice for the highlighted character.
Down Arrow	Display the next configuration item.	Show the next choice for the highlighted character.
ENT	Select the configuration menu for the current item.	Select the current choice for the highlighted character and highlight the next character.

NOTE: If a selection can be configured, the ↵ character will be shown at the bottom right of the display. Configuration requires that the keypad is unlocked.

CN6140 Encryptor

The CN6140 encryptor is a rack mountable unit that is designed for operation in a data centre environment. The unit provides full line rate encryption of Ethernet frames at speeds of up to 10 Gbps.



Figure 1: CN6140 Front view



Figure 2: Rear panel of the CN6000 series encryptors

The CN6140 can be configured to utilize one to four encryption slots with these operating at 1 Gbps or 10 Gbps, that is, all slots must be configured at the same speed. Slot identification is as follows:



Table 2. CN6140 Slot Assignments

Logical Slot	Physical Port	
	Local	Network
0	1	5
1	2	6
2	3	7
3	4	8

Table 3. CN6140 Features and constraints

Feature / utilized ports;	1 Gbps		10 Gbps		
	Single	2 - 4	1	2	3 - 4
Crypto mode	CFB CTR GCM	CFB CTR GCM	CTR GCM	CTR GCM	CTR
Operational mode	Line MAC VLAN TRANSEC TIM	Line MAC VLAN TIM	Line MAC VLAN TRANSEC TIM	Line MAC VLAN TIM	Line
Connections per encryptor	255	255	511	511	1
Ethertype diagnostics	Y	Y	Y	Y	N
Bypass IP Multicast Header	Y	Y	Y	Y	N
Bypass IGMP MLD	Y	Y	Y	Y	N
Transceivers	Optical, Copper	Optical, Copper	Optical, Copper	Optical, Copper	Optical, Copper
Linkspeed	1 Gbps	1 Gbps	10 Gbps	10 Gbps	10 Gbps

CN6140 indicators

The CN6140 has a number of LEDs that indicate the current state of the encryptor.



Table 4. CN6140 front panel indicators

System LEDs	State	Description
Secure	Solid Red	Unit is not activated and traffic is being discarded
	Flashing Red	Unit is not activated and traffic is being bypassed
	Solid Amber	Unit is activated and traffic is being discarded
	Flashing Amber	Unit is activated and traffic is being bypassed
	Solid Green	One or more certificates have been loaded and the unit is operating securely
	Flashing Green	Operating securely but with no certificates loaded, for example, when in Transport Independent Mode (TIM)
System	Solid Red	Secure Halt
	Solid Green	System operating correctly
Alarm	Flashing Red	Alarms exist
	Flashing Amber	Unacknowledged Alarms
	Solid Red	Acknowledged Alarms
	Solid Green	No active alarms
Power	Green	Indicates that power is on

CN6140 LCD backlight

The LCD backlight colour can vary depending on operational status:

- White indicates normal operation
- Red indicates persistent secure halt or power-up self test failure

CN6140 Network interfaces

The CN6140 is factory configured with interfaces as shown in the following table, these supporting a specific combination of protocol, transmission speed and media connection. The interface can be identified from its physical label or via CM7. Additional interface detail is provided on page 9

Table 5. CN6140 interfaces

Model	Protocol	Line Rate	Connections
CN6140	Ethernet	1/10 Gbps	LC-SFP+



Ethernet connector indicator LEDs

Table 6. Connector LEDs

LOCAL or NETWORK PORTS			
Port type	LNK	SPD	LED status/activity indicates:
	(Left)	(Right)	
SFP Ethernet	OFF	OFF	No SFP or SFP socket power off
	AMB (SOL)	AMB (SOL)	Port Stopped
	RED (alt FLSH)	RED (alt FLSH)	SFP Bad
	OFF	GRN (FLSH)	LLF Down
	OFF	RED (SOL)	SFP Good & LOS
	RED (SOL)	RED (SOL)	SFP Good & LOS & Auto Neg. Fail
	GRN (ACT)	AMB (FLSH)	Link 10M
	GRN (ACT)	AMB (SOL)	Link 100M
	GRN (ACT)	GRN (SOL)	Link 1000M
	GRN (ACT)	GRN (SOL)	Link 10G

Legend:

LNK	Link
SPD	Speed
ACT	Activity, flashing at 8.33Hz when frames are processed
FLSH	Flashing at 1.25Hz
Alt-FLSH	Alternate flashing between LNK and SPD LEDs at 1.25Hz
RED	Red
AMB	Amber
GRN	Green
SOL	Solid

Emergency erase

All encryptors have a 'emergency erase' facility which has the same effect as 'tampering' the unit. When erased, all key and user account material is erased.

The CN6140 can be reset to the erased state by any of three methods:

1. The first method is to press and hold down the ESC and ENT buttons for about 10 seconds to display the 'Erase and reboot?' message after which you can press the 'Up' key to display the confirmation request and then the ENT key. Pressing any other key will cancel the operation.
2. The second 'emergency' method, which can be used even when the unit is powered down, requires you to press a reset button that is behind a hole next to the UP/DOWN arrows. A paper clip or similar device is required to do this.



3. The third method is to use the CLI erase command. Note that unless the **-f** switch is included to reset the encryptor to the original 'factory' state, the front panel IP addresses and the operational mode (point to point, MAC, VLAN, TIM etc.) are retained.

Encryptor connections

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

Power supplies and Connectors

The CN6140 encryptors have a pair of dual redundant universal mains power supplies that can accept input in the range 90-250 VAC at 50-60Hz. Supplies will auto-range to the supplied input voltage without user intervention. For safety reasons it is important that the mains plug provides an effective earth for the unit.

For maximum reliability it is recommended that the encryptor be protected with an uninterruptible power supply (UPS).

The CN6000 Series have an IEC13 rear panel mounted sockets that allows connection to the AC supply with an IEC13 cable. Loss of electrical power results in the loss of all connections and their associated encryption keys (but not the configuration settings, certificates or passwords).

As an option, CN6140 encryptors can be equipped with 48 VDC dual-redundant, hot-swappable power supplies. When both supplies are operational, each delivers power to the chassis and the load is shared. When one supply fails an alarm will be indicated (front panel alarm LED flashes red and an event message is logged) and the remaining supply handles the load until the faulty supply is replaced.

Although the supply is hot-swappable, it is not user-serviceable and it must be returned to your supplier for repair.

In the event of power loss an encryptor will automatically re-establish its trusted connections when power returns and traffic is seen. No user action is required.

NOTE: The power supply power LED may stay active for some tens of seconds after power is removed from the module. This is expected behaviour.

Management connections

Encryptors can be locally managed using via an SNMPv3 session that connects using the supplied Ethernet cable and RJ45 socket on the encryptors panel. Command Line Interface (CLI) management is provided via a RJ45 craft connector on the front panel.

Fan tray

CN6140 encryptors are equipped with a fan tray that houses both fans and the lithium backup battery. The tray can be exchanged to facilitate the replacement of the battery without disrupting the encryption of network traffic.

Battery

Senetas encryptors use an internal lithium battery to both power their real-time clock (RTC) and provide essential backup for volatile configuration information. The battery has a typical shelf life of twenty years and its status can be viewed via the CM7 Manage>Diagnostics screen.

Batteries are continuously monitored for low-voltage conditions and the status indicated on a front panel LED. If a low-voltage is detected then an alarm condition will be logged and the front panel battery indicator will be set to red. The battery is located in the replaceable fan tray (the user cannot replace the battery in the fan tray).



Pluggable Module Descriptions

The following sections describe each of the modules that can be replaced in the field.

The Fan Module

The Fan Module is common to all CN6000 series models. It has two fans and a Poly-carbonmonofluoride Lithium Battery.

The fans and the battery are monitored and a faulty fan or a faulty battery will trigger an alarm indicated by the Alarm LED and the LCD on the front panel. These can also be viewed using CM7 or a CLI command.

The Fan Module is hot pluggable and user replaceable. It is fastened to the chassis with two M4x12 screws.

The AC Power Supply Module

The CN6000 AC models employ two AC Power Supply Modules that provide dual redundancy to the internal 12VDC Rail. A fault in the power supply in only one of the modules will not affect the unit's normal operation.

The green LED on the fascia of the AC Power Supply Module indicates the status of the power supply. When the power supply is on and normal, the LED is on; when the power supply input is disconnected or the power supply is faulty, the LED is off.

The AC Power Supply Module has an IEC C14 power inlet to accept a detachable Power Supply Cords with IEC C13 sockets. The AC power input is rated at 100 to 240 VAC, 1.5A, 50 to 60 Hz.

The case of the AC Power Supply Module is made of steel and is connected to the safety earth terminal.

The AC Power Supply Module also has a fan that is being monitored and reported on in the same way as those for the Fan Module.

The AC Power Supply Module is hot pluggable and user replaceable. It is fastened to the chassis with two M4x12 screws.

The DC Power Supply Module

The CN6000 DC models employ two DC Power Supply Modules that provide dual redundancy to the internal 12 VDC Rail. A fault in the power supply in only one of the modules will not affect the unit's normal operation.

The green LED on the fascia of the DC Power Supply Module indicates the status of the power supply. When the power supply is on and normal, the LED is on; when the power supply input is disconnected or the power supply is faulty, the LED is off.

The DC Power Supply Module has a DC Power Input rated at 40.5 to 60 VDC, 2.5A.

The case of the DC Power Supply Module is made of steel and is connected to the safety earth terminal.

The DC Power Supply Module also has a fan that is monitored and reported on in the same way as those for the Fan Module.

The DC Power Supply Module is hot pluggable and user replaceable. It is fastened to the chassis with two M4x12 screws.

DC Power Supply Connector Specifications

In some installations there may be a requirement to provide custom DC Power Supply cables. The information required to do this is contained in the sections that follow.

The input connector in the DC Power Supply Module mates with Molex HCS-125 Connector Housing and Crimp Socket Terminals. The DC Power Supply Wires and the Safety Earth Wire are to be terminated with the Crimp Socket Terminals before being inserted to the Connector Housing. The Molex part numbers are shown below.



Table 7. DC supply connections

Quantity	Wire Size	Molex part number	Description
3	16-18AWG	18-12-1222	3.18mm (.125") Diameter HCS-125 Pin and Socket Crimp Terminal, Series 2047, Female. with Tin (Sn) Plated Brass Contact, Wire Size 16-18AWG, Wire Insulator Diameter 3.05 (.120") max.
	10-14AWG	18-12-1602	3.18mm (.125") Diameter HCS-125 Pin and Socket Crimp Terminal, Series 1901, Female, with Tin (Sn) Plated Brass Contact, Wire Size 10-14AWG, Wire Insulator Diameter 4.57 (.180") max.
1		03-12-1036	3.18mm (.125") Diameter, HCS125, Pin and Socket Plug Housing, Single Row, without Panel Mount Ears, 3 Circuits, Natural, Nylon 94V-2

The following illustration shows the pin-out of the DC Power Supply connector.

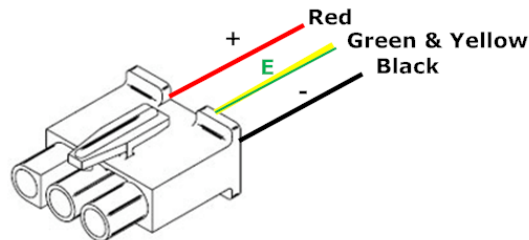


Figure 3: Molex pin connections

Optical interface detail

The following table provides details of all of the optical interfaces that are available for the platforms included in this document.

NOTE: The specified 'reach' of each interface assumes a 'standard' installation using OM2 and/or OM3 fibre. Your network provider should be consulted.

Table 8. SFP (Mbps) optical interfaces

Protocol	Speed	Reach	Fibre Mode	Wavelength	Cage	Part Number
Ethernet	100Mbps	300 m	MM 62.5µm	850	SFP	38-029-6
		550 m	MM 50µm	850	SFP	38-029-6
		2 km	MM	1310	SFP	38-012-6
		10 km	SM	1310	SFP	38-020-6
		30 km	SM	1310	SFP	38-021-6
		30 km	SM	1310	SFP	38-030-6

Table 9. SFP (Gbps) optical interfaces

Protocol	Speed	Reach	Fibre Mode	Wavelength	Cage	Part Number
Ethernet	1 Gbps	300 m	MM 62.5µm	850	SFP	38-029-6
		550 m	MM 50µm	850	SFP	38-029-6
		10 km	SM	1310	SFP	38-020-6
		10 km	SM	1310	SFP	38-075-6
		30 km	SM	1310	SFP	38-021-6
		30 km	SM	1310	SFP	38-030-6
		55 km	SM	1310	SFP	38-036-6
		88 km	SM	1550	SFP	38-038-6
		88 km	SM	1550	SFP	38-062-6

Table 10. SFP+ optical interfaces

Protocol	Speed	Reach	Fibre Mode	Wavelength	Cage	Part Number
Ethernet	1 Gbps	300 m	MM	850	SFP+	38-058-6
		10 km	SM	1310	SFP+	38-059-6
Ethernet	10 Gbps	30 m	RJ45	Copper	SFP+	38-081-6
		100 m	MM	850	SFP+	38-058-6
		10 km	SM	1310	SFP+	38-059-6
		10 km	SM	1310	SFP+	38-066-6
		10-30 km	SM	1310	SFP+	38-070-6
		40 km	SM	1550	SFP+	38-060-6
		80 km	SM	1550	SFP+	38-061-6

NOTE: The CN6140 supports passive Direct Attach Copper (DAC) cables or copper RJ45 SFP+ modules. Customers are advised not to operate unlisted models as this diverges from the safety standard, UL and EMC testing configurations and invalidates conformity to these standards.

The CN6140 can be configured using CM7 or the CLI **protocol** command to support the speeds listed in the following table. If copper SFP+ units are used then it is the responsibility of the installer to ensure that the total power dissipated does not result in overheating of the unit. Each SFP+ cage can dissipate a maximum of 2.5 watts.

Table 11. Heat generated by optical interfaces

Configured Speed	Part Number	Dissipation per Local or Network port
1 Gbps	38-026-6	1.0 watts
10 Gbps	38-081-6	2.5 watts

For example, an encryptor with three 10 Gbps interfaces installed on both the Local and Network ports will dissipate 15 watts.



Transceiver Vendor codes

The following table provides vendor part numbers for each of the optical transceivers supported by Senetas encryptors.

Table 12. Vendor part numbers for SFP+ optical transceivers

Part Number	Cage	Vendor	Vendor Part number	Max Op Temp. °C	Standard
38-081-6	SFP+	Methode	DM7052/3	70	Copper ¹
38-070-6	SFP+	Finisar	FTLX1772M3BCL	75	
38-066-6	SFP+	Finisar	FTLX1472M3BNL	85	1000BASE-LX, 10GBASE-LR/LW
38-065-6	SFP+	Finisar	FTLF8528P3BNV	85	
38-061-6	SFP+	Finisar	FTLX1871D3BCL	70	10GBASE-ZR
38-060-6	SFP+	Finisar	FTLX1672D3BCL	70	10GBASE-ER/EW
38-059-6	SFP+	Finisar	FTLX1475D3BCV FTLX1471D3BCV (EOL)	70	1000BASE-LX 10GBASE-LR/LW
38-058-6	SFP+	Finisar	FTLX8574D3BCV	70	1000BASE-SX 10GBASE-SR/SW

Table 13. Vendor part numbers for SFP (Gbps) optical transceivers

Part Number	Cage	Vendor	Vendor Part number	Max Op Temp. °C	Standard
38-051-6	SFP	Finisar	FTLF8524P2BNV	85	
38-047-6	SFP	Finisar	FTLF1424P2BCR	70	
38-040-6	SFP	Finisar	FTLF1522P1BTL	85	
38-035-6	SFP	Finisar	FTLF1424P2BCL	70	
38-034-6	SFP	Finisar	FTLF1324P2BTL	85	
38-033-6	SFP	Finisar	FTLF8524P2BNL	85	
38-030-6	SFP	Finisar	FTLF1421P1BTL	85	
38-028-6	SFP	Finisar	FTLF1422P1BTL	85	
38-021-6	SFP	Finisar	FTLF1421P1BCL	70	
38-016-6	SFP	Finisar	FTLF1322P1BTR	85	

Table 14. Vendor part numbers for SFP (Mbps) optical transceivers

Part Number	Cage	Vendor	Vendor Part number	Max Op Temp. °C	Standard
38-075-6	SFP	Finisar	FTLF1318P3BTL	85	1000BASE-LX
38-063-6	SFP	Finisar	FTLF1217P2BTL	85	100BASE-FX
38-062-6	SFP	Finisar	FTLF1519P1BNL	85	1000BASE-Z



Table 14. Vendor part numbers for SFP (Mbps) optical transceivers(continued)

Part Number	Cage	Vendor	Vendor Part number	Max Op Temp. °C	Standard
38-038-6	SFP	Finisar	FTLF1519P1BCL	70	1000BASE-ZX
38-036-6	SFP	Finisar	FTLF1419P1BCL	70	1000BASE-LX
38-029-6	SFP	Finisar	FTLF8519P3BNL	85	1000BASE-SX
38-020-6	SFP	Finisar	FTLF1321P1BTL	85	1000BASE-LX

NOTE: Any vendor part number marked EOL are end-of-life and the alternative part number should be used.

¹ To comply with EMC requirements, shielded CAT6 cable must be used

Forward Error correction

Forward Error Correction (FEC) provides for the removal of errors that can occur when data is transmitted over high speed optical links. The introduction of newer, faster, optical links requires the development of new interfaces that are usually expensive, push the limits of the technology, and require the use of FEC to ensure reliable operations.

FEC requires the addition of redundant information to a signal so that the errors can be identified at the receiving end of a link. The Senetas implementation follows IEEE 802.3 chapter 91 [2], which is also known as "IEEE 802.3bj" or "RS-FEC". Ethernet frame transmission is transparent to FEC and no change in bit-rate is required.

The QSFP28 and the longer range CFP4 modules used with the CN9000 series encryptors have non-zero error rates and in some customer installations FEC will be required to achieve low packet loss rates.

FEC can be independently enabled or disabled on both the Local and Network ports and independent status monitoring and statistics are available for both.

Latency

The implementation of FEC does introduce additional latency of the order of 0.25 microseconds.

Initial power-up

Following physical installation it is usual to connect power to the unit to ensure that it operates as expected. Encryptors are shipped in factory default state which means that they will need to be configured according to the requirements of the network.

Boot up sequence

The boot up sequence is entered after a hardware or software restart. For FIPS 140-3 compliance, the software must perform hardware and software diagnostic tests as part of the initialization process. The results of these tests are added to the system event log.

Self-test enhancements

As per FIPS 140-3 compliance, the following are in place:

- The SHA256 cryptographic algorithm used for software Integrity tests is now the first test performed in the set of power-up tests
- In addition to being run at start-up, software and firmware integrity tests are run every 24 hours. A start-up sequence can be triggered by a reboot, erase, tamper or power cycle.

The following actions are performed for software and firmware integrity tests:



- A SHA-256 hash is performed on each software and firmware component and is compared with a build time value

Result	Action
Success	Normal operation continues
	Event log entries generated for all tests if test conducted as part of start-up
	Event Log entry only generated for Software Integrity test if integrity tests conducted as part of 24 hour check
Fail	Encryptor enters 'Secure Halt' state

Self-test frequency

Bypass and Encrypt egress data-path tests are run:

- on policy configuration changes (for example, crypto-mode change, IP rule configuration updates, etc.)
- every 24 hours
- tests also run when there is a start-up triggered by a reboot, erase, tamper or power cycle

The following actions are performed for Bypass and Encrypt egress data-path tests:

- Send a test frame that tests the bypass egress data-path action
- Send a test frame that tests the encrypt egress data-path action using the current crypto policy settings

Result	Action
Success	Normal operation continues
	No log entries are generated if test conducted as part of 24 hour check or configuration change
	Event log entries generated if test conducted as part of start-up
Fail	Alarm raised
	Log entry generated
	Encryptor global mode set to 'Discard'
	The user can change the global mode back to secure without needing to acknowledge the alarm, which will trigger another Bypass and Encrypt Policy test

"Secure halt" actions

Where significant errors are detected during the diagnostic phase, the software will not complete the power up sequence but will instead enter a 'secure halt' state. In this situation:

- The interface ports will not pass any 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 are turned off



Tampering response

Following power up, if the encryptor is in the tampered state, a log message will be generated and the LEDs will flash red. If a unit has been tampered but is no longer in the tampered state it will boot normally however a log message will be generated.



Encryptor Connections

The following sections describe each of the connections that are used to connect and/or manage encryptors within networks.

Management interfaces

Encryptors can be managed via the RJ45 management port (using SNMPv3), the serial console port (using CLI commands) or inband (using SNMPv3). The SNMPv3 sessions use the UDP protocol to ensure operation in noisy environments.

Management port statistics

The following table shows the management port statistics that are available using either SNMPv3 or the CLI.

Table 15. Management Port statistics

Ethernet	Meaning
MAC Address	MAC address of the encryptors management port
Operating Mode	The current mode the encryptor is operating in
Current Link Rate	Encryptor link rate
Configured Link Rate	User specified speed negotiation
Partner Link Rate	Management link rate
IP	Meaning
Packets In	Number of IP packets received by the encryptor
Packets Out	Number of IP packets sent by the encryptor
Header Errors	Number of Header errors in IP packets
Address Errors	Number of address errors in IP packets
Discards	Number of IP packets discarded
ICMP	Meaning
Messages In	Internet Control messages received on the management port
Messages Out	Internet Control messages sent by the management port
Errors	Count of errors detected in ICMP messages
UDP	Actions
Datagrams In	Number of UDP datagrams received by the encryptor
Datagrams Out	Number of UDP datagrams sent by the encryptor
Errors	Number of errors in UDP datagrams



NOTE: Encryptors can be managed via the RJ45 management port (using SNMPv3), the RS232 serial port (using CLI commands) or inband (using SNMPv3). The SNMPv3 sessions use the UDP protocol to ensure operation in noise-prone environments.

Connecting to the Ethernet management port

Each encryptor has a 10/100/1000Base-T (RJ45) Ethernet port which can be connected to a PC or the local trusted network. This port is used to manage the unit.

NOTE: The auxiliary port can be used to provide a second management connection..

When successfully connected, the green link indicator on the RJ45 connector will be lit and the flashing orange LED will indicate Ethernet activity.

The management port is auto-sensing and will use auto-negotiation to determine the fastest speed at which it can run. The port will initially attempt to operate at 1000 Mbps. If this fails, the unit will automatically attempt to connect at the alternative Ethernet speeds of 100 Mbps and then 10 Mbps until a stable connection is established.

Connecting to the serial management port

Encryptors provide a command line interface (CLI) accessible through a serial console port. The encryptor serial console port is a DTE (Data Terminal Equipment) device and can connect to other DTE devices (for example, terminals or end stations) using the supplied null-modem cable. The encryptor can connect to a DCE (Data Communications Equipment) device, for example a modem, using a straight through RS232-C cable (not supplied). Depending on the type of hardware that you are connecting to the serial console port, make sure that you have the appropriate serial cable ready at installation time.

It is not recommended that the serial port be connected to a terminal server and accessed over an unsecured network such as the Internet without additional protection mechanisms.

Both the port and terminal settings are those that will normally exist by default and it is seldom necessary to make any changes.

Personal computer settings

The required RS232 serial port settings for connecting a PC as the CLI management station are:

Table 16. 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

The recommended terminal settings for connecting to the RS232 port of the encryptor are:



Table 17. Terminal emulator settings

Parameter	Setting
Local Echo	Off - to ensure that commands are visible
Line wrap	On - to prevent loss of data at end of line
Carriage Return/Carriage Return left translation	
Inbound	Off
Outbound	Off

Connecting to the local and network ports

Encryptors are inserted into the network as a 'bump in the wire' such that traffic in both directions is encrypted according to the defined encryption policy. The 'local' port is connected to the trusted network and the 'network' port is connected to the untrusted network.

The local side of the encryptor usually connects equipment that is located nearby and a number of choices are usually available. The network side of the encryptor may need to support longer distances.

For optical networks the network link is likely to be either via 'dark fibre' in which case connections will be point to point, or a fibre to a 'cloud' which can support multipoint.

Table 18. Interface connections

Protocol	Connector	Speed	Media
Ethernet	SFP+	10Gbps	Single/Multi mode optical fibre

It is important that both the fibre and the interfaces be cleaned if they have been exposed to the environment.

Local port statistics

The statistics listed below are accessed using CM7 or the CLI.

Table 19. Local interface Rx statistics

Received Data	Meaning
Buffer Overflow Count	Count of Frames received on the local port and discarded due to internal buffer overflow
Interframe Gap Errors	Count of frames received after an minimum interframe gap violation.
Octet Count	Count of characters received
Frame Count	Count of frames received
FCS Errored frames	The number of received frames that had an FCS error
PCS Errored Frames	The number of received frames that had data errors
Undersized Frames	Count of received frames that were less than 64 characters



Received Data	Meaning
Oversized Frames	Count of received frames that were over 1536 characters
Discarded Frames	Count of received frames discarded due to Policy settings
Bypassed Frames	Count of received frames that are bypassed
PCS Sync State	Current state of local port communications

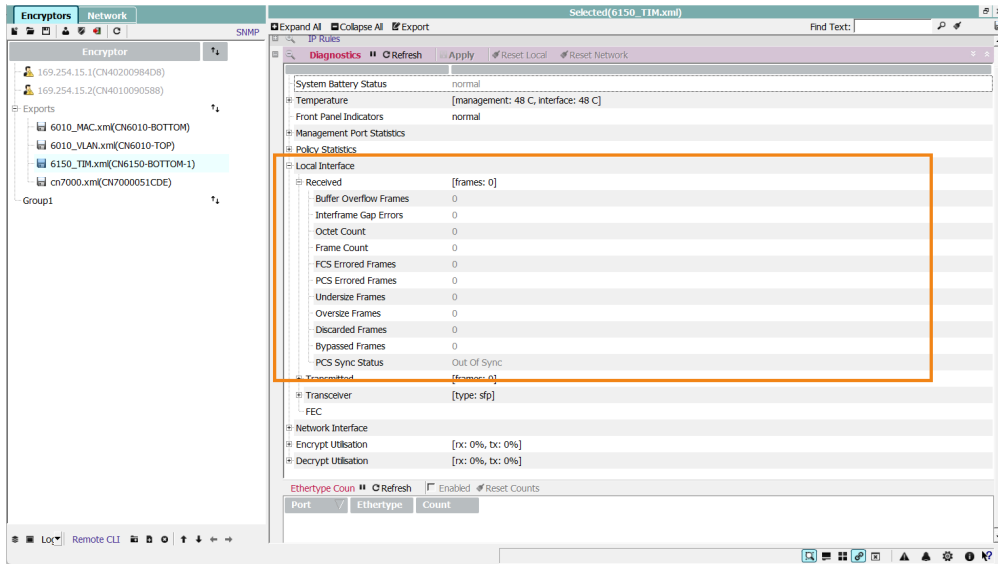


Figure 4: CM7 Local Interface diagnostics screen - Rx stats

Table 20. Local interface Tx statistics

Transmitted Data	Meaning
Octet Count	Count of characters sent
Frame Count	Count of frames sent
FCS Errored Frames	Number of sent frames with FCS errors

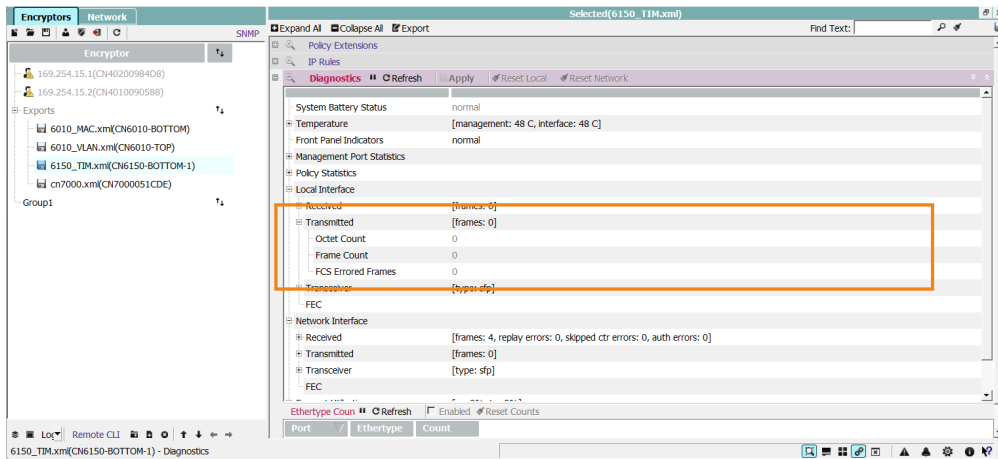


Figure 5: CM7 Local Interface diagnostics screen - Tx stats

Network port statistics

The statistics listed below are accessed using CM7 or the CLI.

Table 21. Network interface Rx statistics

Received Data	Meaning
Buffer Overflow Count	Count of Frames received on the local port and discarded due to internal buffer overflow
Interframe Gap Errors	Count of frames received after an minimum interframe gap violation IFG
Octet Count	Count of received characters
Frame Count	Count of received frames
FCS Errored frames	The number of received frames that had an FCS error
PCS Errored Frames	The number of received frames that had data errors
Undersized Frames	Count of received frames that were less then 64 characters
Oversized Frames	Count of received frames that were over 1536 characters
Discarded Frames	Count of received frames discarded due to Policy settings
PCS Sync State	Current state of network communications
Manage Octet Count	Count of management characters received
Manage Frame Count	Count of management frames received
Manage Drop Frames	Count of management frames dropped due to internal processes
Shim Octet Count	Increments by the crypto excess octets (shim and authentication trailer if present) for each frame that is encrypted/decrypted
Replay Errors	Increments when the counter received in the shim has been observed before or is a value that is less than 256 from the previous greatest received value
Skipped CTR Errors	Increments when the counter received in the shim is greater than what is expected at the receiver
Auth Failed Errors	Number of access attempts that were incorrect.
Reordered Frames	Count increments when the counter received in the shim has a value less than the previous greatest received value
Out of Reorder Window Frames	Increments when the counter received in the shim has a value that is less than 256 from the previous greatest received value
Encrypted Octets	Count of encrypted octets sent
Encrypted Frames	Count of encrypted frames sent



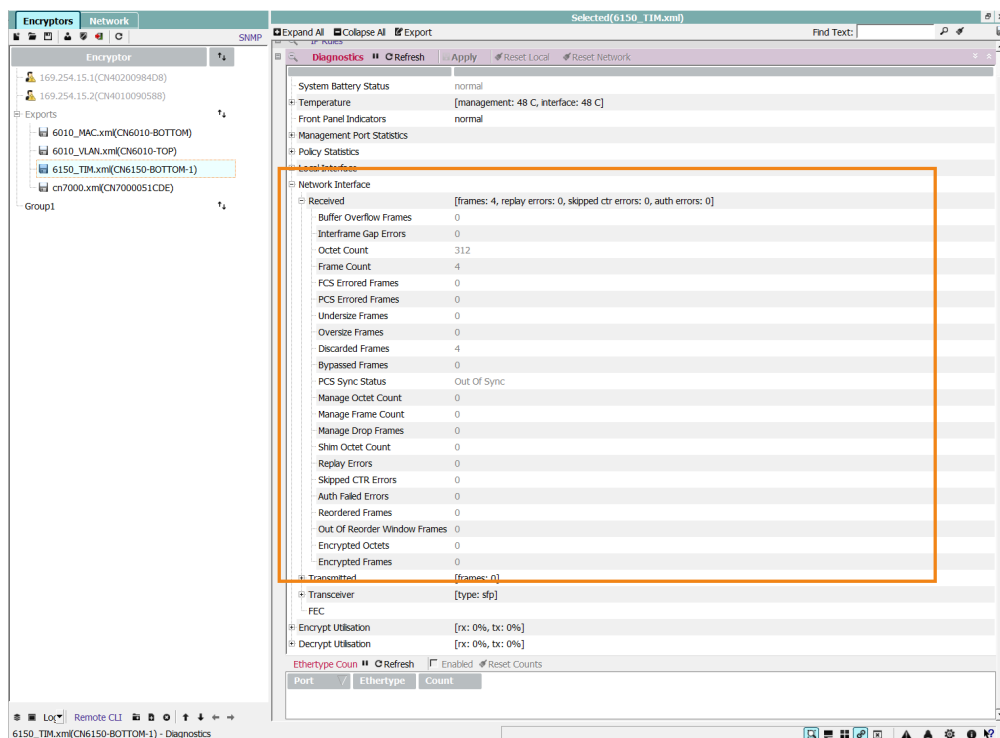


Figure 6: CM7 Network Interface diagnostics screen - Rx stats

Table 22. Network interface Tx statistics

Received Data	Meaning
Octet Count	Count of characters sent
Frame Count	Count of frames sent
FCS Errored Frames	Number of sent frames with FCS errors
Manage Octet Count	Number of management characters sent
Manage Frame Count	Number of management frames sent



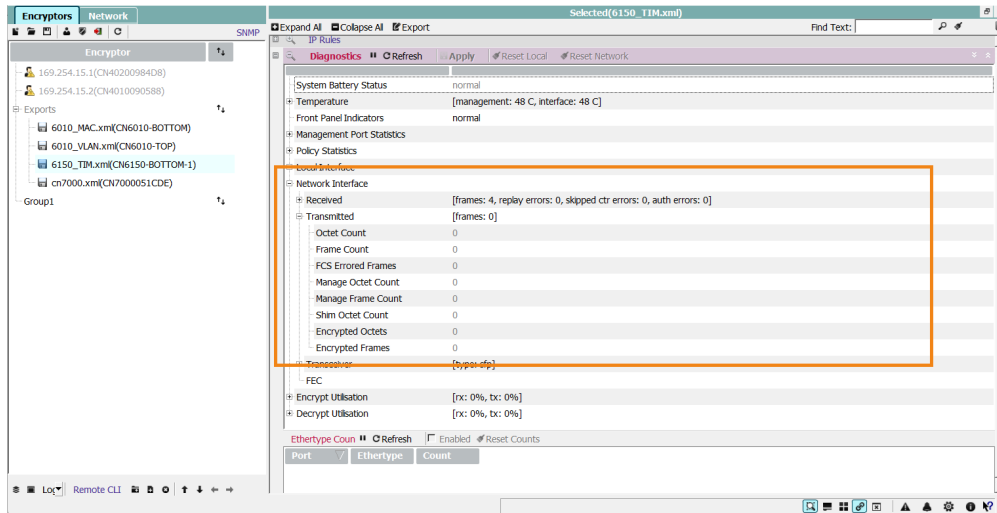


Figure 7: CM7 Network Interface diagnostics screen - Tx stats

Unpacking encryptions

Following delivery the units should be carefully unpacked and the contents checked for completeness. The contents of the shipping box will depend on the encryptor platform model:

CN6140

- CN6140 encryptor platform with Power lead
- RJ45 serial console cable
- RJ45 Ethernet cable
- Two rack mounting brackets with screws
- SFP+ transceivers (as ordered)

Any missing or damaged items should be reported to your supplier immediately.

Environmental requirements

Senetas encryptions operate within a defined environment as follows:

Parameter	Value
Minimum Operating Temperature	0 °C
Maximum Operating Ambient Temperature	50 °C
Minimum Storage Temperature	-40 °C
Maximum Storage Temperature	70 °C
Maximum Operating Altitude	2000 metres above sea level
Operating humidity range	0% to 80% non condensing at 40 °C
Non-operating humidity	95% non condensing

CAUTION: Senetas encryptors with electrical interfaces should not be connected to physical networks that are subject to lightning strikes. One of the major effects of lightning strike on electrical and electronic equipment is a high voltage surge. A surge is caused by the lightning discharge when the associated current tries to find a path to ground. Circuits enclosed in metal conduits are particularly susceptible to strikes on nearby structures.

Encryptor platform location

The encryptor platform must be installed in a secure location to ensure that it cannot be physically bypassed or tampered with. Ultimately the security of the network is only as good as the physical security provided to the encryptor.

Ideally the encryptor will be installed in a climate-controlled environment along with other communications grade electronic equipment, for example a telecommunications room, computer room or dedicated wiring closet.

Choose a location that is as dry and clean.

The encryptors are designed to be located between a trusted (protected) and an un-trusted (unprotected) network. The local interface of the encryptor should be connected to appropriate equipment on the trusted network and the network interface of the encryptor should be connected to the un-trusted (often public) network.

Depending on the topology of your network, the local interface will often connect directly to a router, switch or add-drop multiplexor and the network interface usually connects to the network terminating unit (NTU) provided by the network supplier or carrier.

NOTE: In some cases the network interface may connect to an optical multiplexor ahead of the NTU and dark fibre.

1. Attach the mounting brackets to both sides of the front of the encryptor using the supplied screws.
2. Position the encryptor in the rack aligning the holes in the mounting brackets with the holes in the rack (screws are provided by the rack vendor).
3. Insert and tighten the rack screws, ensuring that the unit is correctly centred and that it will not obstruct other equipment.
4. Attach the front mounting brackets to both sides of the front of the encryptor using the screws that are pre-fitted in the mounting holes.
5. Position the encryptor in the rack aligning the front holes in the mounting brackets with the holes in the rack.
6. Insert and tighten the rack screws (screws are provided by the rack vendor), ensuring that the unit is correctly centred and that it will not obstruct other equipment.
7. Slide the left and right rear extension brackets into the mounting slots in each sides of the encryptor, ensuring that the arrows on the brackets are pointing upwards.
8. Fasten the rear extension brackets to the rack (screws are provided by the rack vendor).



Commissioning

In order to establish trust with its peer(s), each encryptor must be signed by a common Certificate Authority.

The commissioning steps, described in more detail on the following pages, include:

1. Setting the IP address of the encryptor so that CM7 can be used to perform the following steps.
2. setting the Name and Date/Time for the encryptor
3. activation using CM7, which supports all of the current encryptor models.

NOTE: This allows the use of either an internal (CM7 based) or external CA

Default credentials

The encryptor is shipped from manufacturing with a single administration account that has an account name of 'admin' and a password of '\$Password1'.

The 'activation' process during commissioning ensures these credentials are changed.

The default credentials are reset whenever the unit is erased or the tamper mechanism is triggered.

Setting the IP address

An encryptor requires a valid static IP address before CM7 can manage it via the management port or remotely via inband management. DHCP is not supported as it poses a potential security risk. The IP address can be set via the CLI or if an address has already been assigned, the encryptor can be 'discovered' and the IP address changed as described below.

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

The management IP address can be set and changed from:

- The Command Line Interface (CLI)
- The front panel keypad/LCD (CN Series, IPv4 only)
- From CM7 (once an initial address has been assigned).

Only IPv4 addresses can be set from the CN Series front panel. IPv6 addresses must be set from CM7 or the CLI.

If the encryptor already has an IP address assigned you can use CM7 to change the address as described in the sections that follow.

Set the IP address through the CLI

to the CLI using the default account (user name: admin, password: \$Password1)

Use the **ip** command to set the address as described on page 271.

NOTE: The management IP address is not visible from the networks connected to an encryptors Local or Network ports. The IP address is only used for local management via the management port on the encryptor.

Section 1: Encryption platform

Set the IP address from CM7

The IP address of the encryptor can be changed from the Network Addressing menu item of the selected unit. See "Network addresses" on page 182

NOTE: Factory shipped encryptors may already be configured with an IP address. If so, this needs to be reconfigured with a valid IP address for your network. CM7 can be used to do this.

CAUTION: If you load IP addresses into encryptors to facilitate local testing, then prior to relocating the units to a different subnet make sure that the appropriate units have their correct IP addresses loaded. If this is not done then a user with the required 'admin' authority will need to go on site to do this via the CLI.

NOTE: Address changes take effect immediately; there is no need to restart the encryptor. Assuming SNMP access is available, subsequent IP changes can also be made remotely.

Setting Name and Date/Time

Operation of an encryptor requires a valid date and time. The encryptor has an internal battery-backed Real Time Clock (RTC) and also supports NTP for connection to external time servers.

The date and time can be set using the CLI, or with CM7.

The timezone for each encryptor can be set with the CLI **timezone** command as described on page 311, or using CM7.

Setting the encryptor name from CM7

The name of the encryptor can be changed from the Overview menu item of the selected encryptor. See on page 175

Setting Date and time via the CLI

Login to the CLI using the default account (user name: admin, password: \$Password1)

Use the DATE command to set the date and time. See 'date' on page 253 for details.

Setting Date and time via the front panel

After power up the LCD shows the current time, for example:

```
2000-01-01 21:17:35
```

```
Up 0 days 21:20
```

(if the LCD does not show the time then you can cycle back to the time by pressing the Up or Down key repeatedly)

Press the enter key (ENTER) to enable editing

Enter the correct date/time

```
2010-01-21 21:17:50
```

(use the Up or Down keys to change the value)

Press (ENTER) again to accept and set the current digit and move to the next digit

Setting Date and time from CM7

The date and time can be set using the **Date/Time** option as described on page 178

Source of Date/time

Each encryptor uses its real time clock to maintain an accurate date and time.

The date/time value can be set from CM7.

Optionally an external time (NTP) server can be configured so that date and time are automatically established.

NOTE: In multi-slot mode, the date and time can only be set on the host, and any slot is always synchronized. When using CM7, the date/time field is greyed out in the Management view of the slot so cannot be changed by a user. Similarly, the CLI does not allow changes to the date/time of the slot.

Activation

The activation process is used to change the credentials of the default administration account from admin/\$Password1 to those used to secure the unit. The process requires a user who is logged on to the 'admin' account and an operator at the encryptor.

Activating encryptors with CM7

Use CM7 to activate encryptors if they are in a remote location.

The CM7 activation steps are described on page 162

Activating encryptors from the CLI

If the encryptors are local devices, they can be activated using CLI commands. Where supported by the firmware, encryptors can be activated from the CLI using the **activate -I** command as described on page 242

TIM configuration

If an encryptor is to be operated in Transport Independent Mode, after discovering and activating the device, configure TIM parameters using the following steps:

1. Set the connection mode to Transport Independent Mode (TIM) via the CM7 Policy pane or the CLI **con** command
2. Set crypto mode to AES-256-GCM128
3. Set encryption to **Encrypt Global** via the CM7 Policy pane or the CLI **global** command
4. Configure the Ethertypes table for network to be secured using the CM7 Ethertypes pane or the CLI **ethertypes** command
5. Ensure KID is set uniquely across the network and set a limited KID on software/DPDK encryptors (CV1000 & CS1000) if connecting to hardware/FPGA encryptors
6. Configure the key provider - if using KDF, ensure the KDK is set to the same value on ALL devices
7. Configure the key synchronisation method to be the same on all devices (Counter-based synchronisation is recommended to avoid the need for NTP.)
8. Ensure the date and time-zone have been set correctly for all devices. Enable one or more NTP servers via the CM7Date/Time pane or using the CLI **ntpcfg** command
9. Configure the appropriate IPRules for the required/existing L2 / L3 / L4 networks if encrypting at L3 or above. This is done using the CM7 IP Rules pane or the CLI **iprules** command.

Section 1: Encryption platform

- Configure ONE rule at a time, starting at L2, followed by L3, L4 UDP and finally L4 TCP.
 - For each rule perform an end-to-end network check to ensure that the IP Rule is successful and that the network is allowing the encrypted traffic to pass.
 - (Firewalls can block the TCP timestamps required by NTP based encryption)
10. Enable auto-discovery at the correct layer to discover encrypted connections once traffic is being sent. (It is recommended that this is disabled after the network converges and all connections have been discovered.)
 11. Consider MTU implications for the network. If necessary, enable PMTU Max or adjust the MTU in your network to allow for the small additional shim overhead
 12. Check network Firewall configuration to allow the following:
 - ip protocol = 0x63 | 99 (private encryption protocol)
 - TCP timestamps (used for L4 TCP encryption)

NOTE: If a KDK key is to be activated at a given date and time and NTP causes the time to shift more than an hour, the KDK key will be removed and a new KDK key must be generated.

Multi-Slot configuration

The following steps are used to configure the slots of a CN6140 Encryptor:

1. Set Date and Time of Host:

```
CN6140_A>date yyyy-mm-dd hh:mm:ss
```

2. Set IP Address of host either using the front panel or the CLI **ip** command.

```
CN6140_A>ip -s <idx> <addr>/<prefix> <gw>
```

where idx is 1 for IPv4 management, 2 for IPv6.

3. Set the encryption speed:

```
protocol -s <n>
```

n = 1 for 1 x 1 Gbps, = 2 for 1 x 10 Gbps, = 3 for 4 x 1 Gbps, or = 4 for 4 x 10 Gbps.

4. Activate the host following the command prompts:

```
CN6140_A>activate -l
```

NOTE: The host does not require a certificate, these are applied for each slot.

5. Apply required licence to the slot(s):

```
CN6140_A>slot -l <license> <idx> | <idx> ...]
```

Example **slot -l 1.25G 0** assigns 1.25 Gbps license to slot 0

6. Start the slot using idx 0 to 3:

```
CN6140_A>slot -r <idx>
```

7. Login to slot using idx 0 to 3:

```
CN6140_A>slot -c <idx>
```

The selected slot can now be configured using standard single encryptor commands.

To log out from a slot, use the CTRL+q command followed by a q.

After the IP address has been set you can verify the setup by discovering the using CM7. To do this select 'Discover', enter the IP address and then start discovery

When this process completes, add the encryptor to the discovered list. The slots will be discovered and grouped below their host encryptor.

Certification

The steps required to load the initial certificate and change the credentials of the default admin account are described in this section.

Certification with CM7

The steps required to load certificates using CM7 and/or an external Certificate Authority are described on page 164.

Firmware Upgrades

Senetas encryptor firmware upgrades are installed to provide additional functionality or address known limitations of the unit. They are provided either under a maintenance agreement or to fulfil a customer order.

NOTE: Upgrading an encryptor does NOT change the configuration, that is, all certificates, connections, user accounts and configuration information are retained from the old to the new firmware version.

Depending upon the encryptor model, there are a number of installation methods:

- via the front panel using a USB key, or
- via the **upgrade** CLI command (all models), or
- via a local or remote FTP/HTTP server (all models)

Irrespective of the method used, an authorized upgrade image provided by Senetas is loaded into the encryptor.

WARNING: All firmware images provided by Senetas have a .IMG extension. Encryptors with earlier releases must be upgraded using a current release that has the deprecated .CTAM or .SFNT extension after which the unit will be able to recognise the .IMG images.

NOTE: Senetas encryptors support only USB drives that are configured with the FAT or FAT32 format.

All upgrade images are generated and supplied by Senetas (or Senetas' trusted representatives). You should 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.

An example of an upgrade image file name is:

```
CN6140_A-5.5.0.D003-20230210-054031.tar.gz.img
```

In this case, the firmware version is 5.5.0 Delta 003 and the .img suffix identifies the file as a Senetas upgrade image.

Section 1: Encryption platform

During the upgrade process the new firmware image is decrypted, uncompressed and stored internally in non-volatile memory. The new image will not be used, however, until the encryptor is restarted, thus providing a way of synchronising the upgrading of a number of encryptors to the new version. To do this the encryptors are all upgraded to the new image and when convenient, a network wide restart is performed to use the new firmware.

Quantum-ready upgrade images

Upgrade images for Senetas encryptors are also supplied signed by a private key generated from the QRA-based algorithm Falcon-1024.

Quantum-ready images have the naming convention of <Platform-Version.Delta_Date-Time>.tar.gz.qimg. For example:

- CN6140-5.4.0.D11602-20230210-054031.tar.gz.qimg
- CV1000-5.4.0.D12345-20230115-054031.tar.gz.qimg

Both formats of the upgrade images (*.img, *.qimg) will be generated and you will be able to choose the specific format (*.img or *.qimg) for your required upgrade.

NOTE: Encryptors will support both formats for the next few releases, after which support for the older format (*.img) will be deprecated.

WARNING: Firmware versions prior to v5.5.0 will not be able to use *.qimg images to upgrade. Thus, v5.5.0 .qimg upgrade images can not be used to upgrade from v5.2.1(or earlier) to this release.

Once the encryptor is running v5.5.0, *.qimg upgrade images shall be recognised and can be used to upgrade to itself and newer versions.

Firmware downgrades

While it is not recommended, there are situations where a Senetas encryptor needs to be loaded with an earlier version of the encryptor firmware.

Downgrades from version 5.5.0 onwards will automatically perform a full erase when the encryptor is next rebooted using CM7 or detects any other type of trigger that causes the device to perform a reboot or an erase.

However, this only applies from one major release to another and is determined by comparing the first two digits of the firmware number. For example:

- 5.5.1 → 5.5.0 **will not** auto erase
- 5.5.x → 5.2.x **will** auto erase

NOTE: Firmware version 5.5.1 does not currently exist; it is used for illustrative purposes only.

Firmware upgrade using CM7

The steps required to upgrade the firmware using CM7 are described on page 221.

Protocol support

The CM7 management tool currently supports only Ethernet encryptors that have X.509 certificate support. The approach referenced in this section can only be used with these units.

Upgrade progress indication

The progress or status of an encryptor upgrade is now indicated on all CM7 screens by displaying a coloured background for the encryptors:

- green when an upgrade is in progress or has been successfully completed
- red if the upgrade failed

Firmware upgrade using a USB 'memory stick' or drive

An upgrade image stored on a standard USB memory stick can be loaded into a Senetas encryptor via the front panel USB port using the following procedure:

1. Obtain a valid upgrade image from Senetas.
2. Copy the image file onto a USB memory stick in the root directory - ensure that there is only one upgrade image file in this directory or the wrong image may be used.
3. Use the front panel ENT key to select the Upgrade mode
4. Insert the USB memory stick into the encryptor USB port. The encryptor will automatically detect the memory stick and search for a file with the .img extension.

NOTE: Senetas encryptors support only USB drives that are configured with the FAT or FAT32 format.

The encryptor will start transferring the image.

Once the image has been transferred, the encryptor will report the upgrade version number:

```
CN6140.1.3.7.D003
```

The USB memory stick may be unplugged as the image has been loaded into internal memory.

The unit will check the image and commence the upgrade process.

The authenticated image is decrypted, decompressed and stored in non-volatile memory after which the LCD will indicate:

```
Upgrade successful
```

```
Reboot when ready
```

The upgraded firmware image will not be used until the unit is restarted. This can be done immediately or at a later time.

User defined entropy

Senetas encryptors utilise one or more noise/entropy sources to provide robust, FIPS-approved entropy for the purposes of generating all key material within the device. The NIST800-90A/B/C standards have been implemented and the solution certified to FIPS140-2 Level 3.

You may also choose to replace the entropy source with a user-defined entropy pool. To utilize this facility, FIPS mode must be disabled and then entropy enabled either via CM7 or the CLI.

When entropy is enabled an entropy (.ent) file can be loaded using the same procedure as a firmware update; however, a reboot is not required. The entropy file is consumed verbatim for key use, with no other mixing and no qualitative testing applied. This has a twofold benefit for customers:

- Firstly, the entropy pool is not polluted in any fashion with internal processing which provides an assurance that the key material is based solely on the entropy pool data.

Section 1: Encryption platform

- Secondly, for the purposes of AES assurance testing, “known” entropy can be used to facilitate black box testing by the end user. The test entropy pool can be readily erased or overwritten on the 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 be exhausted, the encryptor will revert to the standard internal hardware-based entropy sources without operational impact.

NOTE: Reloading the entropy pool removes any existing data and restarts consumption.

Preparing the .ent file

The following Linux example gives the required steps to construct an entropy file for the purposes of uploading to an encryption device. 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
```

*Illustrative only - select a source as required by the customer.

Monitoring

Once the update is complete, the user should check the event log and verify the SHA256 checksum matches that which was loaded.

With entropy pool enabled, pool statistics are available via CM7 or the CLI. These statistics are provided in the following table.

Table 23. Entropy statistics

Parameter	Description
Entropy pool	Enabled
Size (bytes)	Total size of entropy file
Bytes remaining	Remaining bytes before exhaustion
Bytes used	Bytes consumed to date
Percent used	Percent exhausted
Estimated days remaining	Based on current consumption rate over previous days (7 day rolling window) - allow 24 hours for initial calculation

Alarms are generated when consumption reaches 80, 85, 90, 95 and 100% of the entropy pool.

Quantum Origin entropy source integration and support

The Senetas suite of encryptors now integrates with Quantum Origin, developed by Quantinuum, providing the encryptors with a continual supply of quantum-derived entropy.

Quantinuum has developed the first quantum-computing-hardened cryptographic keys, which the company describes as a near-perfect source of Key Derivation Keys (KDK), known as Quantum Origin. Quantum Origin derived entropy can now be installed on an encryptor using Senetas' existing Bring Your Own Entropy (BYOE) mechanism and new Quantum Origin configuration capabilities.

Senetas encryptors can download a Quantum Origin KDK from the server at regular time intervals. This KDK, along with other data, will be input into a NIST SP800-108 KDF to perform a key expansion operation to generate Quantum Origin derived entropy. The encryptor will detect the presence of new entropy and move it to the active or off line entropy pool (bank) without any disruption to any service and provide continuous Quantum Origin derived entropy to the encryptor.

The encryptor shall monitor entropy usage and user notifications will indicate when the active entropy pool (bank) is nearing exhaustion. If the Quantum Origin entropy is exhausted before the next Quantum Origin KDK can be retrieved, the encryptor will revert to default sources of entropy. Once the next Quantum Origin KDK is downloaded and used to generate entropy, the encryptor will resume the use of Quantum Origin entropy.

To access Quantum Origin entropy, the Senetas encryptor must be:

- in FIPS disabled mode
- activated
- BYOE enabled, via entropy -e CLI command or the 'Manage' screen in CM7 'System' pane, 'Entropy Pool' tick box.

Quantum Origin specific configuration is performed through the quantum_origin CLI commands or the 'Manage' screen in CM7 'System' pane, 'Entropy Pool/Quantum Origin' section. Once all the prerequisite certificates are installed on the encryptor and the Quantum Origin information is configured, Quantum Origin may be enabled. An enable will always trigger an immediate download of a Quantum Origin KDK and generation of Quantum Origin entropy.

NOTE: Both BYOE and Quantum Origin entropy are disabled by default. An erase will delete all BYOE entropy files and disable the feature.

Quantinum server access

To access the Quantum Origin server, you must follow the onboarding process as required by Quantinum. Items you are required to do, include:

- provide IP address/range that their encryptor(s) will present as clients to the Quantum Origin server and have these addresses authorised by Quantinum
- request from Quantinum a Quantum Origin server provided server certificate and CA signing certificate chain and install both on to the encryptor
- generate an EC encryptor certificate (ensuring the subject DN of the CSR uniquely identifies the encryptor), have it signed by a CA certificate chain (either different to or the same as the CA that issued the Quantum Origin server certificate), install the signed encryptor certificate (and CA if different to the Quantum CA) and have these certificates registered with the Quantum Origin server
- receive from Quantinum a shared-secret AES-256 (32 byte) key that will be used to encrypt any key generated for the encryptor, convert the secret key to a 64 character hex string and configure this on the encryptor
- determine the best Quantum Origin server to use and configure on the encryptor the hostname and IP address of the selected server

Rate limiting

Rate limiting is a licensing feature available on the Senetas encryptors that limits the throughput capacity of an encryptor. It can be set at manufacturing time or upgraded via a device specific license upgrade file.

Rate limiting is achieved via Traffic policing which is the process of monitoring ingress traffic to an encryptor and ensuring that the configured license bandwidth is not exceeded. Traffic exceeding the rate limit value is discarded. All traffic, irrespective of policy setting, is included in the bandwidth measurement.

The Rate limiting feature defines a Committed Access Rate (CAR) which is defined as Ethernet Octets in Mbps.

Section 1: Encryption platform

Ethernet Octets per second is defined as; (Ethernet octets + (Number of Ethernet frames x (Minimum IFG + Preamble length))
Minimum IFG = 12 Preamble length = 8

The encryptor guarantees passing traffic at the CAR and in addition can handle temporary bursts above the CAR. Bursts are propagated to the network port. The bucket depth used in the leaky bucket algorithm to measure the local port traffic bandwidth is approximately 67Mb. As such the maximum burst length above the CAR is approximately 67Mb. Large sustained bursts (> 67Mb) above the CAR may lead to packet drops and throttling of the overall output rate.

The user is notified of policing taking affect via the following alarm and event log entry:

```
ALARM_FPGA_BW_CLIPPING - "WARNING - Bandwidth is being clipped
```

The corrective action is to increase the size of the encryptors licence.

Note; no traffic smoothing, shaping or buffering is performed and therefore the latency profile of the traffic is unaltered. If rate limiting is enabled on an encryptor then the network devices connected to the encryptor must perform traffic shaping or policing at or below the CAR (rate limit) specified on the encryptor and be configured to not exceed the maximum burst length defined above.

Additional considerations when configuring peer device traffic shaping-policing:

Connection	Mode	Shim size	Max throughput
Point-Point (Line)	CTR	32	100%
		1	92%
	GCM	32	84%
		1	78%
Multipoint (MAC, VLAN)	CTR	1	92%
	GCM	1	78%
TIM	GCM	1	78%

When TRANSEC is enabled, the 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, please refer to transec section of the document. Additional information is contained in the release notes.

NOTE: When rate limiting is applied by an encryptor burst traffic in excess of the specified limit will result in frames being discarded and SNMP traps being generated. If the application(s) using the link will be impacted by loss of frames then traffic shaping should be applied ahead of the encryptors.



Section 2: Encryption protocols

This section describes the configuration and processing for each encryption protocol.

Maximum Transmission Units	34
Algorithm support	38
Ethernet encryption	39
Modes of operation	41
DEK Pairwise and Group keys (only layer 2)	44
Replay Protection	45
Point-to-Point (Layer 2) Line encryption	56
Multipoint (Layer 2) MAC encryption	71
Multipoint (Layer 2) VLAN encryption	90
Transport Independent Mode (TIM) (Layer 2, 3 and 4 encryption)	96
Ethernet Protocol(only layer 2)	109
Ethernet frame formats	111

Maximum Transmission Units

Introduction

The term Maximum Transmission Unit (MTU) typically refers to the largest possible frame size of a communications Protocol Data Unit (PDU) on the OSI Model Layer 2 data model.

The layer 2 payload MTU is typically 1500 bytes. Encryption adds necessary additional overhead to network packets due to the inclusion of cryptographic headers and trailers.

This additional data increases the size of packets, potentially causing them to exceed the network MTU. When packets surpass the MTU, they can be fragmented or dropped which can introduce latency and reduce overall transmission efficiency. It's important to account for encryption overhead when configuring or assessing MTU values to ensure optimal network performance.

The following table shows the size of the cryptographic header (security tag) added by the encryptor in different modes of operation:

Table 24. Encryption frame overheads

	Security tag size (bytes)					
	Encryption Layer	Layer 2	Layer 3	Layer 4 UDP	Layer 4 TCP	UDP Tun-nelling
Operational Mode	Layer 2 Modes (LINE, VLAN)	8	N/A	N/A	N/A	N/A
	TIM time-based sync	8	8	8	12	16
	TIM counter-based sync	10	10	10	12	18



If GCM mode is enabled then an additional 16 bytes is also added to the end of the frame as a frame integrity check value (ICV).

NOTE: Senetas encryptors are capable of handling jumbo frames up to 10,000 bytes long and do not perform packet fragmentation or reassembly.

To compensate for the additional encryption overhead it may be necessary to adjust the MTU settings across the network.

NOTE: In layer 2 networks there is no dynamic network mechanism to adjust the end-to-end MTU but in IP networks Path MTU Discovery (PMTUD) is typically used to allow devices to automatically discover the MTU of the path being used. PMTUD can help in situations where the MTU may vary.

MTU considerations

Compensating for encryption overhead in Layer 2 encryption modes

NOTE: This section is applicable when the encryptor is running in LINE, MAC or VLAN mode.

1. Determine the maximum encryption overhead in use from the above table and GCM setting
 - a. For example, in VLAN mode with GCM enabled the max overhead = 8 byte security tag + 16 byte ICV = 24 bytes total
2. The default MTU on Ethernet networks is 1500 bytes. To compensate for the encryption overhead it may be necessary to either increase the increase the MTU between encryptors or reduce the MTU on devices behind the encryptors.
 - a. Increasing the MTU between encryptors

If you have control over the MTU settings of the network equipment between the encryptors you can increase the MTU to account for the encryption overhead.

For example, if the encryption overhead is 24 bytes and the standard MTU is 1500 bytes, you might set the MTU to 1524 bytes between the encryptors.

This approach is beneficial when:

- You have control over the intermediate network infrastructure.
- The network infrastructure supports jumbo frames or MTUs larger than standard
- It is more feasible to modify a few devices rather than many endpoints

- b. Reducing the MTU on devices behind the encryptors

By reducing the MTU on devices behind the encryptors, you ensure that even after the encryption overhead is added, the packet size remains within the allowable MTU on the transmission path.

For instance, if the encryption overhead is 24 bytes and the standard MTU is 1500 bytes, you might set the MTU to 1476 bytes on the devices behind the encryptors.

This approach is beneficial when:

- You don't have control over the intermediate network infrastructure.
- The network doesn't support MTU sizes larger than standard.
- You can centrally manage and configure the required number of endpoints.



The choice between the two methods often depends on the specific network topology, the devices involved, administrative preferences, and the scale of deployment.

Compensating for encryption overhead in Layer 3 (IP) networks

This section is applicable when the encryptor is running in Transport Independent Mode (TIM).

The network MTU can be adjusted as described above but in TIM the Encryptor also allows the native PMTUD mechanism of the network to function and has specific policy controls for this.

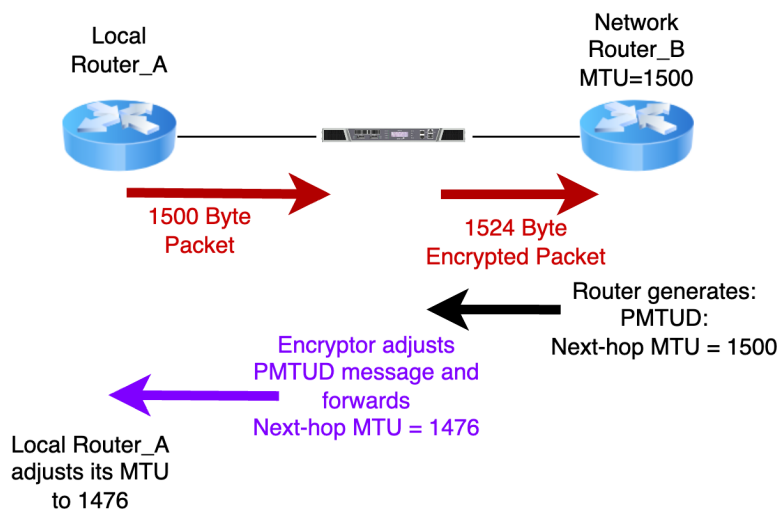
Path MTU Adjustment (PMTUA)

PMTUA is an additional encryptor policy setting that when enabled/ allows the encryptor to automatically adjust the next hop MTU size in PMTUD messages that are received on the network port from a downstream router before being forwarded to the originating host on the local port.

NOTE: Forwarding of PMTUD messages also requires an applicable bypass rule to be configured.

This can be any rule that matches the ICMP (3,4) packet type (e.g. unlisted action = BYPASS) but it is recommended to add an explicit ICMP (3,4) Bypass IPRule associated with this flow to make the behaviour transparent.

The next-hop MTU value is adjusted to allow for the encryption overhead, thus taking care of the end-to-end MTU adjustment without the need for user intervention on the end devices.

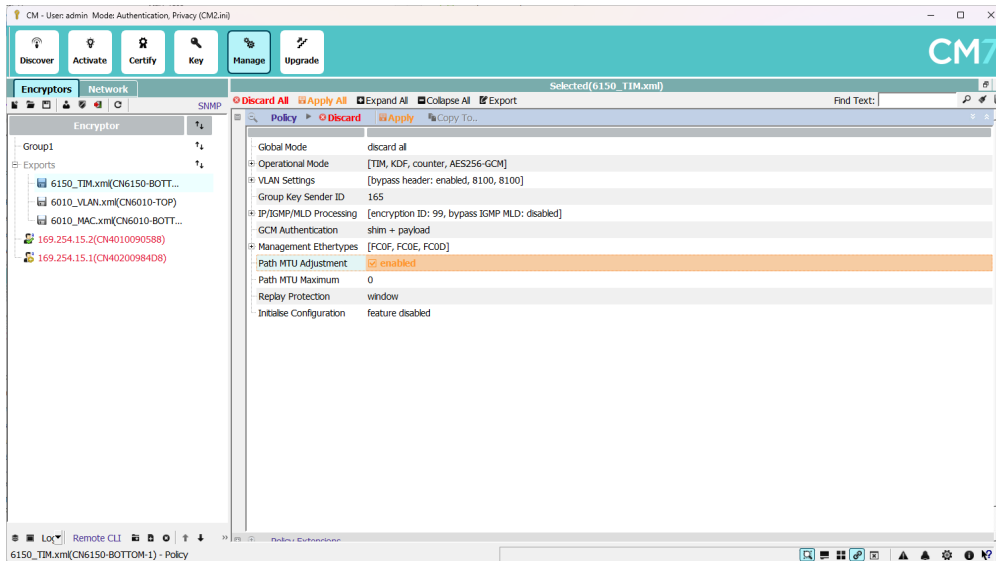


WARNING: PMTUA should only be enabled for traffic that is encrypted with a layer 4 encryption policy. This is because the PMTUD packet received from the network router includes part of the triggering packet's payload (the first 8 bytes) which will be encrypted for all encryption policies other than L4 and therefore unreadable at the originating host.

For this reason PMTU Max is the recommended mechanism to handle MTU issues.

PMTUA is disabled by default, to configure the PMTUA mechanism on a Senetas encryptor, the following methods can be used:

- The CLI command **policy -A <-e | -d>** where the **-e** option enables the feature and the **-d** option disables it
- Via the CM7 'Policy' pane ('Path MTU Adjustment' checkbox), in the 'Manage' screen



To function correctly, the PMTUA feature requires all of the following:

1. PMTUA enabled
2. Encryption policy set to Layer 4
3. L4 checksum calculation feature enabled
4. A policy rule that will bypass PMTUD messages received from the network
5. Global action = Secure

If all the criteria are met, the statistics 'ICMP PMTU Adjusted Frames' (in Local Policy statistics) and 'ICMP PMTU Range Exceeded Frames' (in Network Policy statistics) will be incremented.

If the next-hop MTU size in a validly received ICMP but the above criteria is not met, PMTUA will not occur and only the 'ICMP PMTU Range Exceeded Frames' (in Network Policy statistics) shall be incremented).

If the next-hop MTU size in the corresponding ICMP message is outside the range stated above, then the packet is processed as per the policy and adjustment is not done.

Path MTU Maximum (PMTUM)

PMTUM is an encryptor policy setting that enables you to set a pre-defined maximum MTU size for the network.

When enabled, IPv4 frames received on the local port of the encryptor - that would exceed the configured MTU size when encrypted - will cause the encryptor to generate an ICMP type 3, code 4 (PMTUD) packet which is sent back on the local port to the originator of the packet (with the goal of reducing the originator's MTU).

This packet includes the original IP header and eight bytes of payload (as per the standard) with the next-hop MTU set to: the user configured maximum MTU setting, minus the encryption overhead (for example, 24 bytes) as shown below.



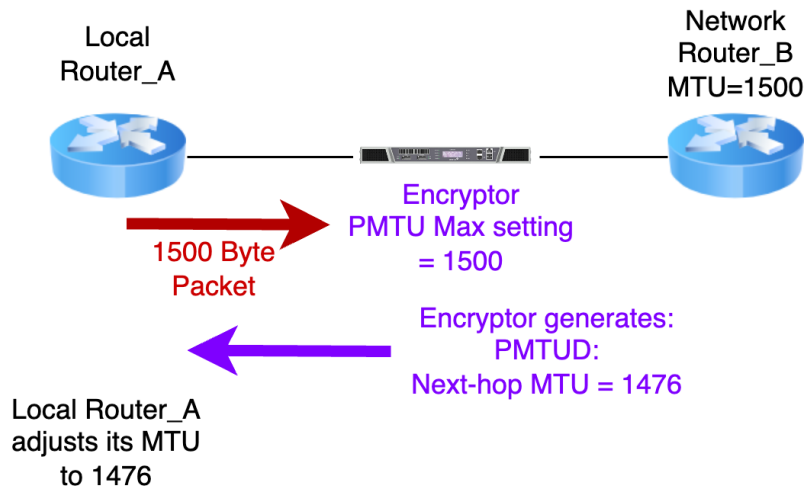
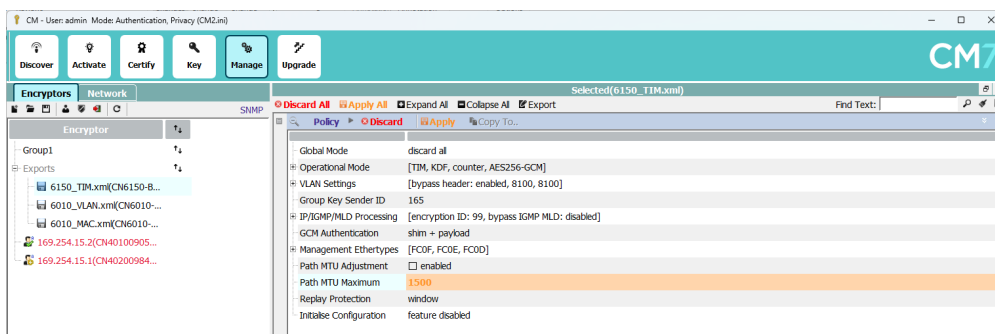


Figure 8: PMTU Max operation

To configure the PMTUM on a Senetas encryptor, the following methods can be used:

- CLI command ***policy -M <mtu size>***
- Via CM7 'Policy' pane ('Path MTU Maximum' field), in the 'Manage' screen.



The configured MTU size can be between 128 - 10,000 bytes. A value of 0 disables the feature.

NOTE: The PMTUM feature is disabled by default.

The statistic 'PMTU Max Tx Frames' (in Local Policy Statistics) is a count of valid ICMPv4 PMTU Max frames sent from the encryptor out the local port.

The new statistic 'IP MTU Exceeded Frames' (in Local Policy Statistics) increments when an IP frame is received on the local port with a length greater than the configured PMTUM value.

The 'IP MTU Exceeded Frames' statistic will increment even if the PMTUM feature is disabled on FPGA-based encryptors.

Algorithm support

The section provides detail of the algorithms that are supported for the functions required to implement the encryptors supplied by Senetas.

The information is provided to assist security professionals who may require it as a supplement to associated documentation.

NOTE: Not all of these are available in all models or when operating in specific modes. Details are available in the relevant section of the documentation.

Secure Message Exchange Algorithms and key sizes

Depends on the certificates assigned to the connection (RSA or ECDSA) and the crypto configuration (AES modes and key size) and connection type (point to point or multipoint/ group key).

TLS Algorithms and key sizes

Only used for services (FTPS, RESTful, KeySecure, etc.); not used for secure connection establishment. Note the availability of certified libraries requires that v1.2 of TLS be used.

Table 25. Mode and Key size per algorithm

Application	Algorithm	Mode / Key size
Secure Message Exchange		
Authentication	RSA	modulus 2048
	ECDSA	NIST curves: P-256, P-384, P-521
Key exchange	RSA-OAEP	modulus 2048
	ECDH	NIST curves: P-256, P-384, P-521
	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 (version 2.0)		
Authentication	ECDSA	NIST curves: P-256, P-384, P-521
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 (restricted to v1.2)		
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

Ethernet encryption

This document provides detail of the manner in which Ethernet traffic can be encrypted using Senetas encryptors. This document describes the basic operation of the Ethernet encryptors and the normal or preferred mode of operation.

The options and features available are determined by the encryptor model, the firmware version and the type of accreditation and these constraints are highlighted where appropriate.

Basic operation

The Ethernet encryptor provides Layer 2 security services by encrypting the contents of data frames travelling across Ethernet networks. The encryptor encrypts data between a local (protected) network and a remote (protected) network across the public (unprotected) network. An encryptor is paired with one or more remote Ethernet encryptors to provide secure data transfer over encrypted connections as shown in Figure 9 below.

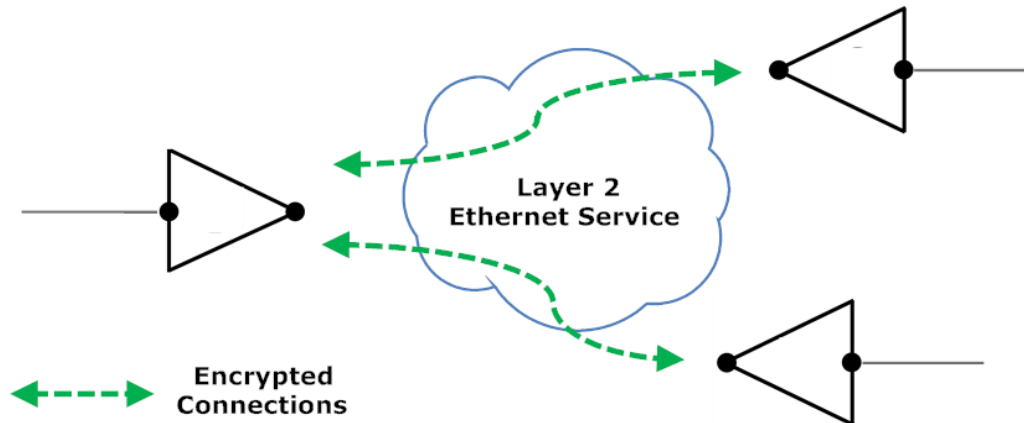


Figure 9: Ethernet network topology

An encryptor's Ethernet receiver accepts frames on its ingress port; valid frames are classified according to the frames header then processed according to the configured policy of the encryptor.

The available policy actions are:

- Encrypt – payload of frame is encrypted according to policy
- Discard – drop the frame, no portion is transmitted
- Bypass – transmit the frame without alteration

When an encryptor is in Encrypt or Bypass it recalculates and appends a Frame Check Sequence (FCS) to each frame that is transmitted.

Policy

Ethernet encryption policy provides fine control over how Ethernet frames are processed as they pass through the encryptor.

Operation within networks

The Senetas Ethernet encryptor requires very little re-configuration prior to being installed within the network that is to be secured.

Senetas recommends that the encryptor be deployed in the default multipoint mode using the appropriate VLAN policy settings. The primary advantage of this is that it allows frame re-ordering; however, in some cases this mode of operation is not appropriate.

Ethernet encryptors can be managed by the Senetas CM7 management system or via the Command Line Interface (CLI).

The encryption algorithm for the Ethernet encryptor is AES using cipher feedback mode (CFB) or counter mode (CTR) or Galois counter mode (GCM). Accreditation for FIPS-140-2 or Common Criteria EAL4 utilises a key size of 256 bits. Encryptors configured to operate in TIM mode or at 10Gbps or higher must use CTR or GCM mode; and to ensure synchronization, CTR (or GCM) mode must also be used to encrypt multicast traffic in meshed networks. Each connection between encryptors uses a unique key pair with a separate key for each direction.

The frame overhead for Layer 2 encryptors configured in CTR mode is 8 octets, and in GCM mode, 24 octets.

When configured in TIM mode the overhead for each frame is as shown below and depends on the key provider, the layer at which encryption is applied, and the encryption mode.

NOTE: Senetas encryptors from hardware version 5.2.x support counter based key providers.

Table 26. Ethernet frame overheads

Encryption mode	Time-based key provider				Counter-based key provider			
	Layer 2	Layer 3	Layer 4		Layer 2	Layer 3	Layer 4	
			UDP	TCP			UDP	TCP
CTR	8	8	8	12	10	10	10	12
GCM	24	24	24	28	26	26	26	28

The Operation mode of the encryptor can be configured to place it in one of three states:

1. **Discard** to prevent the flow of traffic
2. **Bypass** so that all traffic flows unencrypted
3. **Secure** (Encrypt All) so that traffic is encrypted subject to policy settings.

When the encryptor is shipped, it is in **Discard** mode. **Bypass** mode is usually only used during initial setup or for troubleshooting.

The **Secure** mode cannot be selected until the encryptor has a valid certificate loaded.

In normal operation (with the Secure mode selected) traffic will be encrypted and statistics are available from the CLI or CM7. The following should be noted:

- The discarded frame count shown on the encryptors indicates a count of frames that do not pass through the encryptor (that is frames that are deliberately discarded due to policy settings)
- The LOCAL discard count will increment for received frames if there is no matching policy in the connection table (for example if frames on VLAN 100 are received on the local interface but there is no policy in the connection table for VLAN 100)
- The NETWORK discard count will increment for the same reason as above but also indicates normal heartbeat messages sent between the encryptors for key management purposes. As these are not passed through the device they will also increment the network port discard count.

In a well-designed and configured network, you would expect to see the network discard count continuously increment without implying loss of user data.

Modes of operation

Ethernet encryptors have a number of global settings that specify how they operate.



- The **Operation Mode** specifies the global or overall policy
- The **Cryptographic Mode** specifies the encryption algorithm submode
- The **Connection Mode** specifies how encryptors interpret policy

Cryptographic modes

The cryptographic mode is a setting that defines whether the encryption algorithm uses the Cipher Feedback (CFB) or Counter (CTR) or the Galois/Counter (GCM) submode of the AES algorithm. All encryptors that communicate with each other must be configured to use the same cryptographic mode. If you switch between submodes the connection policy must be changed; a warning is displayed.

NOTE: The submodes that are supported depends upon the firmware revision of the encryptor.

Both encryption at 10Gbps or higher, or the encryption of multicast traffic within a meshed (multipoint) network, require the use of one of the counter submodes, that is, CFB cannot be used.

In CFB mode the encryptor operates in a self-synchronising, streaming mode of operation. Encrypted frames are not expanded and the encryptor will automatically self-synchronise in the event of frame loss. If an encrypted frame is lost then the following frame cannot be decrypted but the next frame will be correct (that is, there is a self-correcting mechanism with error extension of one frame).

In CTR mode the algorithm is not self-synchronising; re-synchronisation is facilitated by periodically adding a small shim header to the encrypted frames that contains the current counter.

In MAC mode if frames are lost, subsequent frames will not be correctly decrypted until the encryptors re-synchronise to the same counter value which occurs when the next shim is received. The shim header can be inserted at a user selectable rate as specified in the following table.

Operational mode	Shim rate	User settable
Line (Point-point)	default = 32 [^]	Yes, 0 to 32,767
TRANSEC	default = 32 [^]	Yes, 0 to 32,767
MAC - Unicast	default = 32 [^]	Yes, 0 to 32,767
MAC - Multicast	1	No
VLAN	1	No
TIM	1	No

* LLC_SAP, LLC_SAP_SNAP frames are always shimmed when encrypted

[^] If MTU overflow protection is enabled then depending upon the speed of the link, frames exceeding the following lengths will not be shimmed.

Linkspeed	Frame length
100 Mbps	> 256
1 Gbps	> 256
10 Gbps	> 1510

The shim is inserted on each frame when operating in VLAN or SPB mode.



The shim insertion rate can be set from the CM7 Policy tab or using the CLI **shim** command 302Shim.htm. A facility is also provided to disable shim insertion on frames which if shimmed would violate the maximum MTU setting (1518 for Ethernet).

NOTE: When the policy is based on VLAN tags each frame is shimmed and frames can be delivered in any order.

The GCM mode is similar to CTR in that it is not self-synchronising; and shimming is used. It has the added advantages of low processing overhead and the provision of message authentication which make it a preferred mode.

NOTE: When establishing connections, in most instances the factory default settings are appropriate and few configuration changes are required.

NOTE: When in Multipoint mode, a change from CTR or GCM to CFB mode is prevented by either of the following conditions:

- The ethertype table contains 'FollowCI' actions for multicast or broadcast traffic. These would need to be changed to 'Bypass' or 'Discard' to allow for CFB operation in meshed mode
- Multicast connections remain in the CI/Tunnels table. Removing these may require disabling multicast auto-discovery

Connection modes

The Ethernet encryptor can be configured to operate in TIM (Transport Independent Mode) or one of the following layer 2 modes; Point-to-Point (line) mode, MAC multipoint (mesh) mode, VLAN multipoint mode. The mode is selected using the CM7 policy tab or the CLI **line** and **con** commands. See "Replay Protection" on page 45 for additional information.

When configured in Point-to-point (Line) mode encryptors can have TRANSEC framing enabled to disguise patterns in traffic thus preventing traffic analysis.

NOTE: To clarify configuration and operation of a Senetas encryptor, the sections that follow may reference modes other than the one that is the focus of this document.

Connections

The table that follows shows the maximum number of connections and lookups that are supported in each of the operational modes.

Encryptor	Mode	# Connections	# Lookups	Notes
CN6140 (1 Gbps)	MAC	252	256	255 Shared between locmacs and netmacs table
	VLAN	255	256	256 shared between vlan IDs and customer reserved MAC addresses for bypass
	TIM	255	64	64 IP Rules Max
CN6140 (10 Gbps)	MAC	508	512	511 Shared between locmacs and netmacs table
	VLAN	511	512	512 shared between vlan IDs and customer reserved MAC addresses for bypass
	TIM	255	64	64 IP Rules Max



DEK Pairwise and Group keys (only layer 2)

Data encryption keys (DEK) are used to encrypt data plane traffic. DEK are exchanged between peer encryptors during session establishment.

Pairwise keys are used when encrypting unicast traffic and the units are operating in Point-to-point or MAC mode.

The Senetas Group key system is used for encryption of Multicast traffic or when the units are operating in VLAN mode.

Connection Mode selection

Prior to configuring the connection mode of the encryptors all of the network and security requirements should be reviewed, including the following:

- Where there are only two sites or a dark fibre connection exists, Point-to-Point provides a simple secure layer 2 solution
- Point-point mode uses the same key for all Unicast and Multicast traffic; cryptographic separation is not provided
- If expansion beyond two sites is expected then a multipoint mode may be a better choice as this would allow the addition of further units without re-configuration of the existing units
- The MAC-based multipoint configuration is appropriate where cryptographic separation of layer 2 traffic between different sites is desirable
- MAC-based policies allow inclusion/exclusion of specific network endpoints. This can be based on manual specification of addresses
- The VLAN-based layer 2 multipoint mode allows QoS services and offers increased scalability
- VLAN-based policies allow inclusion/exclusion of specific VLANs
- Multipoint modes allow security to be based on Certificates
- The VLAN mode and multicast MAC mode traffic use the Senetas group key scheme which is resilient to traffic disruption. (Refer to "DEK Pairwise and Group keys (only layer 2)" on page 44 for details.)
- Transport Independent Mode (TIM) allows encryption of L2, L3 and L4 Ethernet traffic

Mode availability

The connection modes that can be selected will be determined by the encryptor model and possibly the firmware release. Refer to the model specification for more details.

The CM7 Operational mode selectors as shown in Figure 10 on the facing page are used to select the desired mode. The 'Line Mode' selector is not visible if the unit is in VLAN mode; in that case the unit must be changed to MAC mode (as shown below) after which a restart will occur and the Line Mode selector will be available. In a similar manner, if the unit is in Line mode, the Connection Mode selector is not visible and then line mode must be cleared before the connection mode can be changed.



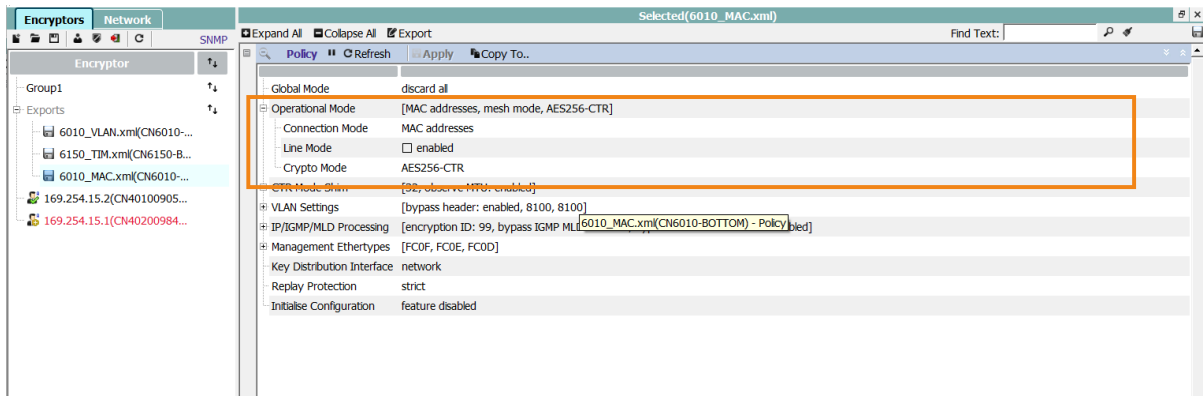


Figure 10: CM7 Operational mode selection

Switching between modes may request a restart which if initiated results in re-initialization of the encryptor as follows:

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

During normal power cycling and encryptor is not re-initialized and previously established connections will be retained.

Replay Protection

Replay protection allows for encryptors to mitigate against replay attacks. Protection is provided by using the frame counter to ensure that frames are not seen to be repeated at any point.

The behaviour of the encryptor upon seeing a repeated frame is dependent on the replay protection setting.

Three options for controlling replay/reordering of packets may be selected:

- Strict
- Disabled
- Window

These options are hardcoded and dependent on the settings of the following features:

- Operational mode
- MTU overflow setting
- Crypto mode
- Shim rate

Replay protection settings

Strict

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

A calculated packet count is the packet count value calculated by the decrypt datapath and is only used for when the shim rate is not equal to 1. For example, not every frame has a synchronisation shim.

Disabled

When the disabled option is selected, no replay protection is provided. This means that:

- Packets can be re-ordered.
- Packets can be replayed.

WARNING: There may be regulatory requirements prohibiting disabling replay protection so seek guidance before selecting this setting.

Window

Reordering can sometimes occur within a network for reasons of which a customer may have no knowledge or control.

Reordering may occur due to:

- different routing paths in the network
- different queue paths within routers/switches
- quality of service (QOS) within the network

Therefore, when using the Window setting, there is a proscribed range of values (256 bits previous to the highest received frame counter number). A packet number must be within the range to be accepted as valid and decrypted; any other value results in the packet being discarded.

Up to 16 VLANs and 32 encryptors are supported, connections after this will operate with replay protection disabled. Example connection mappings are:

- For Line mode this is a 1:1 mapping between sending and receiving encryptors.
- For TIM mode this is a N:1 mapping between sending and receiving encryptors. i.e. a receiver needs N windows, one per sending encryptor.
- For VLAN mode this is a N*M:1 mapping between sending and receiving encryptors. i.e. a receiver needs N*M windows, where N is the number of senders and M is the number of connections/VLAN-ids.

Replay protection mode statistics

Replay protection detects replayed packets and discards the packet instead of decrypting it.

'Replay Error Frames' have been enhanced and 'Reordered Frames' and 'Out Of Reorder Window Frames' statistics have been introduced to assist with replay and reordering diagnostics.

These statistics can all be found under the CLI command **stats** or **stats -n** or via the CM7 'Diagnostics' pane under the 'Network Received' section in the 'Manage' screen.

NOTE: The three statistics are only valid on the *decrypt* data path.

Network Port Replay Errors

This statistic only increments when the counter in the received shim has been observed before. The Replay Error counter only increments for replayed packets.

NOTE: If a frame fails authentication and is deemed to be replayed, only the authentication error statistic will increment



Network Port Reordered Frames

The 'Reordered Frames' statistic will increment when the counter received in the shim has a value that is:

- less than the greatest previously received value
- within the replay acceptance window (256 wide)

These frames are not discarded but the counter indicates to the user that reordering has occurred.

NOTE: Reordered frame statistics are not available on CN6140 4x10G.

Network Port Out of Reorder Window Frames

'Out Of Reorder Window Frames' statistic increments when the counter received in the shim has a value that is less than 256 from the greatest previously received value. These frames are discarded if the replay protection setting is set to 'window'.

If a frame fails authentication and is deemed to be out of the reorder window, only the authentication error statistics will increment.

NOTE: Out of reorder window frame statistics are not available on CN6140 4x10G

Table 27. Replay/Reordering versus Operational mode and Configuration settings

Configuration						Replay protection mode supported		
Operational mode	Connection type	Sender ID	MTU over-flow protection	Shim rate	Crypto mode	Strict	Window	Disabled
Line	NA	Fixed to Off	NA	NA	CFB	N	N	Y (default)
Line OR Transec1.	NA	Fixed to Off	Don't care	!= 1	CTR or GCM	Y (default)	N	Y
Line OR Transec	NA	Fixed to Off	Off	1	CTR or GCM	Y	Y (default)	Y
Line	NA	Fixed to Off	ON	1	CTR or GCM	Y (default)	N	Y
MAC	Unicast	Fixed to Off	Don't care	Don't care	CTR or GCM	Y (default)	N	Y
MAC2.	Group key	Fixed to Off	Off	Fixed to 1 (in FPGA)	CTR or GCM	N	N	Y (default)
VLAN	Group key	Off	Fixed to Off	Fixed to 1 (in FPGA)	CTR or GCM	N	N	Y (default)
VLAN	Group key	On	Fixed to Off	Fixed to 1 (in FPGA)	CTR or GCM	N	Y (default)	Y
TIM	NA	Fixed to On	Fixed to Off	Fixed to 1 (in FPGA)	CTR or GCM	N	Y (default)	Y



Switching configuration

You are able to change the replay protection mechanism. The replay protection setting can vary depending on mode and the configuration settings. Switching between any of the above configuration resets the replay protection mode to the default setting.

NOTE: To make changes, you must have Supervisor or Administrator privileges.

Changes can be made via the CLI using the policy command

policy -w <strict|window|disabled>

where *-s*: strict, *-d*: disabled and *-w*: window are defined above.

The following table shows attributes in each of the connection modes can be used to select the configuration that meets the needs of a network.



Table 28. Connection mode attributes

Attribute / Connection mode		Line (Pt-Pt)		Multipoint			
				MAC			VLAN
Accreditation	FIPS / CC AES-256	CFB	CTR	CFB	CTR		CTR
Address Support	Unicast	y	y	y	y		y
	Multicast	y	y			y	y
	Broadcast	y	y			y	y
Topology Supported	Point-to-Point	y	y	y	y	y	y
	Mesh			y	y	y	y
	Hub / Spoke			y	y	y	y
Encryption Policy	Policy basis	ethertype (e)		e+da MAC address			e+VLAN tag
	Policy edits by authorised user			y	y	y	y
	MAC addresses observed or learnt	na	na	y	y	y	na
	Ageing of learnt MAC addresses	na	na			y	na
	VLAN ID observed or learnt	na	na	na	na	na	y
	Payload encryption offset	y	y	y	y	y	y
	Ethertype mutation	y*	y*	y	y*	na	na
Security	Cryptographic separation by VLAN	na	na				y
	Cryptographic separation	na	na	y1	y1	y1	
	MTU overflow protection	s	y	na	y		
	Message authentication						
	Replay protection	y	y		y		y



Table 28. Connection mode attributes (continued)

Attribute / Connection mode		Line (Pt-Pt)		Multipoint			
				MAC		VLAN	
	Key System	pairwise				groupwise	
Network considerations	Quality of Service support	na	na			y	y
	Per frame overhead (octets)	none	8	none	8	8	8

y - supported na - not applicable s - selectable <blank> - unsupported y1 - by connection y* - non-shimmed frames

The following table shows attributes in each of the connection modes can be used to select the configuration that meets the needs of a network.

Table 29. Connection mode attributes (10 Gbps, V2.1.2 on)

Attribute / Connection mode		Line (Pt-Pt)		Multipoint			
				MAC		VLAN	
Accreditation	FIPS / CC AES-256	CTR	GCM	CTR	GCM	CTR	GCM
Address Support	Unicast	y	y	y		y	y
	Multicast	y	y		y	y	y
	Broadcast	y	y		y	y	y
Topology Supported	Point-to-Point	y	y	y	y	y	y
	Mesh			y	y	y	y
	Hub / Spoke			y	y	y	y
Encryption Policy	Policy basis	ethertype (e)		e+da MAC address		e+VLAN tag	
	Policy edits by authorised user			y	y	y	y
	MAC addresses observed or learnt	na	na	y	y	na	na
	Ageing of learnt MAC addresses	na	na		y	na	na
	VLAN ID observed or learnt	na	na	na	na	y	y
	Payload encryption offset	y	y	y	y	y	y
	Ethertype mutation	y*	y*	y*	na	na	na



Table 29. Connection mode attributes (10 Gbps, V2.1.2 on)(continued)

Attribute / Connection mode		Line (Pt-Pt)		Multipoint				
				MAC		VLAN		
Security	Cryptographic separation by VLAN	na	na			y	y	y
	Cryptographic separation	na	na	y1	y1			
	MTU overflow protection	y	y	y				
	Message authentication		y			y		y
	Replay protection	y	y	y		y	y	y
	Key System	pairwise			groupwise			
Network considerations	Quality of Service support	na	y		y	y	y	y
	Per frame overhead (octets)	8	8	8	8	8	8	8

y - supported na - not applicable s - selectable <blank> - unsupported y1 - by connection y* - non-shimmed frames

The following table shows attributes in each of the connection modes can be used to select the configuration that meets the needs of a network.

Table 30. TRANSEC Connection mode attributes (<= 1 Gbps, V2.4.0 on)

Attribute / Connection mode		Line (Pt-Pt)
Accreditation	FIPS / CC AES-256	CTR
Address Support	Unicast	y
	Multicast	y
	Broadcast	y
Topology Supported	Point-to-Point	y
	Mesh	na
	Hub / Spoke	na



Table 30. TRANSEC Connection mode attributes (<= 1 Gbps, V2.4.0 on)(continued)

Attribute / Connection mode		Line (Pt-Pt)
Encryption Policy	Policy basis	ethertype(e)
	Policy edits by authorised user	
	MAC addresses observed or learnt	na
	Ageing of learnt MAC addresses	na
	VLAN ID observed or learnt	na
	Payload encryption offset	y
	Ethertype mutation	y*
Security	Cryptographic separation by VLAN	na
	Cryptographic separation	na
	MTU overflow protection	y
	Message authentication	na
	Replay protection	y
	Key System	pairwise
Network considerations	Quality of Service support	na
	Per frame overhead (octets)	16

y - supported na - not applicable s - selectable <blank> - unsupported y1 - by connection y* - non-shimmed frames

The following table shows attributes in each of the connection modes can be used to select the configuration that meets the needs of a network.

Table 31. TRANSEC Connection mode attributes (10 Gbps, V2.4.0 on)

Attribute / Connection mode		Line (Pt-Pt)
Accreditation	FIPS / CC AES-256	CTR
Address Support	Unicast	y
	Multicast	y
	Broadcast	y



Table 31. TRANSEC Connection mode attributes (10 Gbps, V2.4.0 on)(continued)

Attribute / Connection mode		Line (Pt-Pt)
Topology Supported	Point-to-Point	y
	Mesh	na
	Hub / Spoke	na
Encryption Policy	Policy basis	ethertype (e)
	Policy edits by authorised user	
	MAC addresses observed or learnt	na
	Ageing of learnt MAC addresses	na
	VLAN ID observed or learnt	na
	Payload encryption offset	y
	Ethertype mutation	y*
Security	Cryptographic separation by VLAN	na
	Cryptographic separation	na
	MTU overflow protection	y
	Message authentication	na
	Replay protection	y
	Key System	pairwise
Network considerations	Quality of Service support	na
	Per frame overhead (octets)	16

y - supported na - not applicable s - selectable <blank> - unsupported y1 - by connection y* - non-shimmed frames

Table 32. CN6140 Connection mode attributes

Feature	1 Gbps	4 x 1 Gbps	10 Gbps	4 x 10 Gbps
Crypto mode	CFB, CTR, GCM		CTR, GCM	CTR
Operational mode	Line TRANSEC MAC VLAN TIM	Line MAC VLAN TIM	Line TRANSEC MAC VLAN TIM	Line
No. of Connections per Encryptor (slot) instance	256		512	1



Table 32. CN6140 Connection mode attributes(continued)

Feature	1 Gbps	4 x 1 Gbps	10 Gbps	4 x 10 Gbps
Ethertype Diagnostics	Yes			No
Bypass IP Multicast header	Yes			No
Bypass IGMP MLD	Yes			No
Transceivers	Optical Copper		Optical	
Linkspeed (clocking)	1 Gbps		10 Gbps	





Point-to-Point (Layer 2) Line encryption

Point-to-point or Line mode is used to secure a single point-to-point connection as shown below. The mode is well suited to bulk traffic processing using a simple encryption policy.

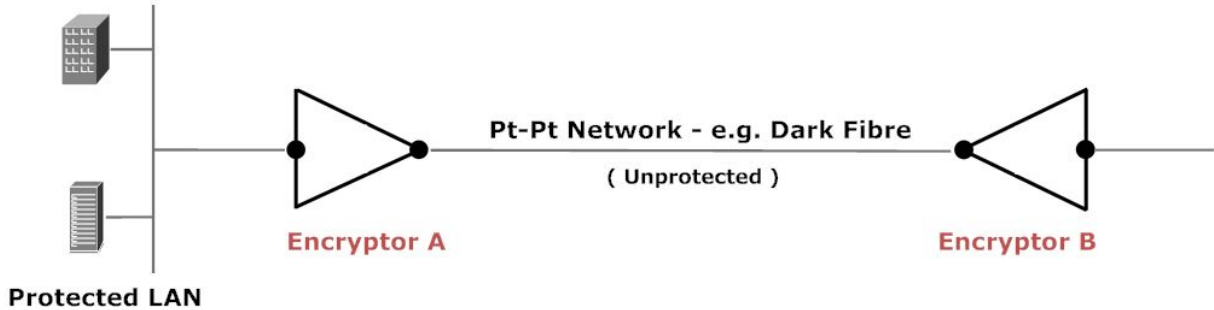


Figure 11: Point to Point network topology

NOTE: Line mode encryption is designed to operate over point-point links and requires that frame order is preserved. In some networks, for example service provider networks, frame order may not be guaranteed and instances of this will be indicated by "shim sync rewind" event log entries. In such cases both encryptors should have their 'shim rate' set to 1, and have 'mtu overflow protection' disabled.

When TRANSEC operation is enabled the only topology settings that are applicable are the Global ones.

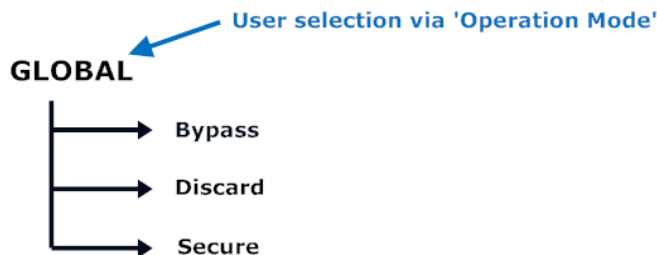


Figure 12: Point to point Policy

When to use Line mode encryption

Line mode encryption is best suited for encryption across end-to-end Ethernet networks or dark fibre links where a secure connection between two endpoints is required and ideal for situations where simplicity and high performance are critical.

It is ideal for point-to-point encryption of data.

Line mode encryption:

- Ensures secure communication over a direct, point-to-point link
- Simplifies the encryption process with minimal configuration
- Provides highest throughput and lowest latency at full line speed



Operation mode

Operation mode is a global selector that provides a quick way of bypassing or discarding all traffic through the encryptor regardless of the ethertype of a frame. Depending on factory settings, the initial mode is either 'Bypass' or 'Discard'.

The required mode is set to via the global Mode setting on the CM7 Policy tab. Setting the mode to 'Secure' (Encrypt All) specifies that frames will be processed as defined by policy. The mode can also be set using the CLI **global** command.

When the operator changes the mode of a layer 2 encryptor to 'Secure' the following transitions occurs:

1. Connection/tunnel discovery commences
2. Ethertype policy is then applied

Point-to-point Ethertype policy

The point-to-point ethertype table provides control over processing based on the ethertype of the frame. This table shown in Figure 13 below, specifies the default actions for common ethertypes.

Ethertypes that are not included in the ethertype table are processed according to the "Unlisted Ethertype Action" processing policy and this entry can be edited as required.

ID	Type	Observe ..	Offs...	Broadcast .	Multicast A.	Unicast Actio	Mutation En.	Muta..	Injected T..
1	05FF (LENGTH)	<input type="checkbox"/> ignore	0	bypass	bypass	follow CI	<input type="checkbox"/> disabled	0000	bypass
2	0800 (IPV4)	<input type="checkbox"/> ignore	20	bypass	discard	follow CI	<input checked="" type="checkbox"/> enabled	F800	discard
3	0806 (ARP)	<input type="checkbox"/> ignore	0	bypass	discard	bypass	<input type="checkbox"/> disabled	F806	bypass
4	86DD (IPV6)	<input type="checkbox"/> ignore	40	bypass	discard	follow CI	<input checked="" type="checkbox"/> enabled	F6DD	discard
5	8808 (MAC-C)	<input type="checkbox"/> ignore	0	bypass	bypass	bypass	<input type="checkbox"/> disabled	F808	bypass
6	8809 (SPMA)	<input type="checkbox"/> ignore	0	bypass	bypass	bypass	<input type="checkbox"/> disabled	F809	bypass
7	88CC (LLDP)	<input type="checkbox"/> ignore	0	bypass	bypass	bypass	<input type="checkbox"/> disabled	F8CC	bypass
8	9000 (LOOPBACK)	<input type="checkbox"/> ignore	0	bypass	bypass	bypass	<input type="checkbox"/> disabled	F000	bypass

Figure 13: Default Point-to-Point ethertype values

Additional ethertypes (up to a total of 15) can be added by clicking on the 'Add' button on the Policy tab, specifying each of the new column values as listed below, and then clicking the 'Apply' button. The policy for an existing ethertype can be changed by changing the displayed value and clicking 'Apply'.

Table 33. Ethertype attributes

Field Name	Content
ID	Sequential ID - system assigned index
Type	Hex value and Ethertype name
Observe Offset	Observe if active, Ignore to ignore value
Offset Bytes	Octets to be left in clear if Observe is active
Broadcast Action	Discard, Bypass or FollowCI
Multicast Action	Discard, Bypass or FollowCI
Unicast Action	Discard, Bypass or FollowCI
Mutation	Disabled, Enabled - to mutate ethertype
Mutation Value	Value to mutate type to
Injected Type	Discard, Bypass - action on observed mutated type

Observe Offset can be enabled to allow a selected number of octets at the start of the payload to be left in the clear. Default is to encrypt the entire payload. See " Point-to-point Ethertype policy " on page 57.

The action can be set to 'Bypass', 'Discard' or 'FollowCI' for each of the Ethernet addressing modes - Unicast, Multicast and Broadcast. If the 'FollowCI' policy is selected then the configured 'Offset' and/or 'Mutation' policy will be applied.

Mutation can be set active to mutate the frames ethertype to an different ethertype prior to transmission and restore it to the original ethertype when processing received frames. Note that offset and mutation need to be set identically in all peer encryptors and in CM7 the 'Copy To ..' button can be used to do this.

Where mutation is enabled, the injected traffic action will be either 'Bypass' or 'Discard', the latter being used to prevent traffic from within the network reaching the secure network(s).

NOTE: Prior to version 2.1.1 of the firmware, only Unicast address types could be specified to follow the connection identifier/tunnel action. The addition of multicast encryption in version 2.1.1 allowed all address types to be specified.

Ethertype mutation

Mutation allows the ethertype of the frame to be changed to a specified value when encrypting and reinstated to the original value when decrypting. See the ethertypes CLI command on page 1.

NOTE: Ethertype mutation or an Encryption offset may be required if intermediate equipment between a pair of encryptors makes decisions based on visibility of the payload that follows the Ethernet header.

Examples of this are layer 2 services that require certain data to be present; although strictly speaking, this should not be the case in a true layer 2 network.

Mutation (rather than Encryption offset) is the preferred method of addressing this type of problem as it does not leave any portion of the payload as plaintext.



Encryption offset (only L2 modes)

The ethernet configuration allows an optional encryption offset to be specified. The offset moves the encryption start point in the frame by the specified number of bytes, allowing a portion of the frame to be sent in the clear.

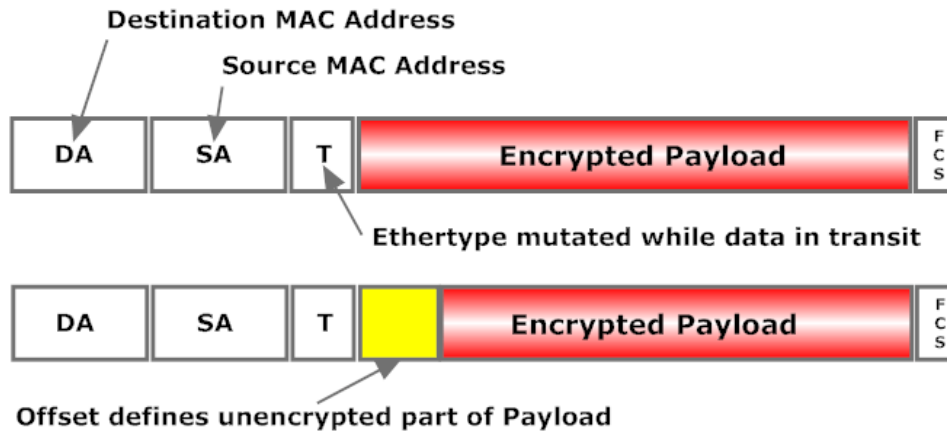


Figure 14: Point-to-point Mutated and Offset frames

NOTE: When passing VLAN traffic on a link configured in point-to-point (line) mode the VLAN identifier must be manually configured in the connection table. This can also be configured via the CLI `inband_vlan` command as described on page 1.

This is not required in Multipoint mode as the ID is automatically learnt.

Bypass Reserved Multicast

In networks with switches or other configurable devices between encryptors it may be necessary to enable the bypassing of groups of MAC addresses that are used for this purpose. The following figure shows the CM7 screen used to do this.

The screenshot shows the 'Bypass Reserved Multicast' configuration page. The 'Bypass Reserved Multicast' checkbox is checked (enabled). Below, a table lists reserved MAC addresses with their corresponding protocols and bypass options.

ID	MAC Address	Bypass ...
1	01:80:C2:00:00:0* - Link Constrained Protocol	<input type="checkbox"/> enab...
2	01:80:C2:00:00:00 - STP Spanning Tree Protocol	<input type="checkbox"/> enab...
3	01:80:C2:00:00:01 - MAC Pause Frame	<input type="checkbox"/> enab...
4	01:80:C2:00:00:02 - LACP Link Aggregation Control Protocol	<input type="checkbox"/> enab...
5	01:80:C2:00:00:03 - Port Access Protocol	<input type="checkbox"/> enab...
6	01:80:C2:00:00:0E - LLDP IEEE Link Layer Discovery Protocol	<input type="checkbox"/> enab...
7	01:00:5E:00:00:** - Routing Protocol (e.g. OSPF)	<input type="checkbox"/> enab...
8	01:00:0C:CC:CC:CC - Cisco VTP/DTP/CDP	<input type="checkbox"/> enab...
9	01:00:0C:CD:CD:D0 - Cisco LZTP	<input type="checkbox"/> enab...
10	01:00:0C:DD:DD:DD - Cisco CGMP	<input type="checkbox"/> enab...
11	01:00:0C:CC:CC:CD - Cisco SSTP	<input type="checkbox"/> enab...



Figure 15: Bypass Reserved Multicast selection

Configuring Point-to-Point (line) mode

For the purposes of discussion we will assume that the network example shown on page 60 will be secured in Point-to-Point mode.

The mode can be selected via the global Mode setting on the CM7 Policy tab or via the CLI **line** command as described on page 1.

When operating over a service provider link (ISP), and the provider has configured a VLAN, then the VLAN ID must be configured in the connection table to allow the encryptors management traffic to traverse the network. Note that this is required on both units and it can be tested using the CLI **eping -v** command.

Reconfiguring the encryptor requires changes to the internal state that are best made by setting the parameters and restarting the unit. Because this is a significant event you are asked to confirm the operation, after which the restart is initiated and CM7 will not be responsive until rebooting completes which can take up to 30 seconds.



Point-to-Point configuration using the CLI

When configuring via the CLI a number of commands are used as detailed in the steps that follow. For brevity, where the same command is used on each encryptor, they are shown one after the other, without reference to the requirement to log on to each in turn or the fact that some commands will restart the unit.

1. Ensure that the configuration of the encryptor is in the default condition.

```
CN6140_A>initcfg -a
CN6140_B>initcfg -a
```

2. Enable point-to-point (line) mode on the peer and then local encryptor.

```
CN6140_A>line -e
CN6140_B>line -e
```

3. View the tunnels/connections. [Optional]

```
CN6140_A>tunnels
Interface (tunnel/CI) MAC address : 00:d0:1f:aa:aa:aa
Front Panel Management MAC address : 00:d0:1f:00:aa:aa

CI   Origin   Action   State   Peer Name           Remote Encryptor MAC MAC Header
----
0001 System   Secure   Start   TBD                 00:00:00:00:00:00
```

```
CN6140_B>tunnels
Interface (tunnel/CI) MAC address : 00:d0:1f:bb:bb:bb
Front Panel Management MAC address : 00:d0:1f:00:bb:bb

CI   Origin   Action   State   Peer Name           Remote Encryptor MAC MAC Header
----
0001 System   Secure   Start   TBD                 00:00:00:00:00:00
```

4. Set the global policy to enable security.

```
CN6140_A>global -e
CN6140_B>global -e
```

5. Confirm that the tunnels/connections are in the Up state. [Optional]

```
CN6140_A>tunnels
Interface (tunnel/CI) MAC address : 00:d0:1f:aa:aa:aaFront Panel Management MAC address :
00:d0:1f:00:aa:aa
CI   Origin   Action   State   Peer Name           Remote Encryptor MAC MAC Header
----
0001 System   Secure   Up      CN6140_B           00:d0:1f:bb:bb:bb

CN6140_B>tunnels
Interface (tunnel/CI) MAC address : 00:d0:1f:bb:bb:bb
Front Panel Management MAC address : 00:d0:1f:00:bb:bb
```

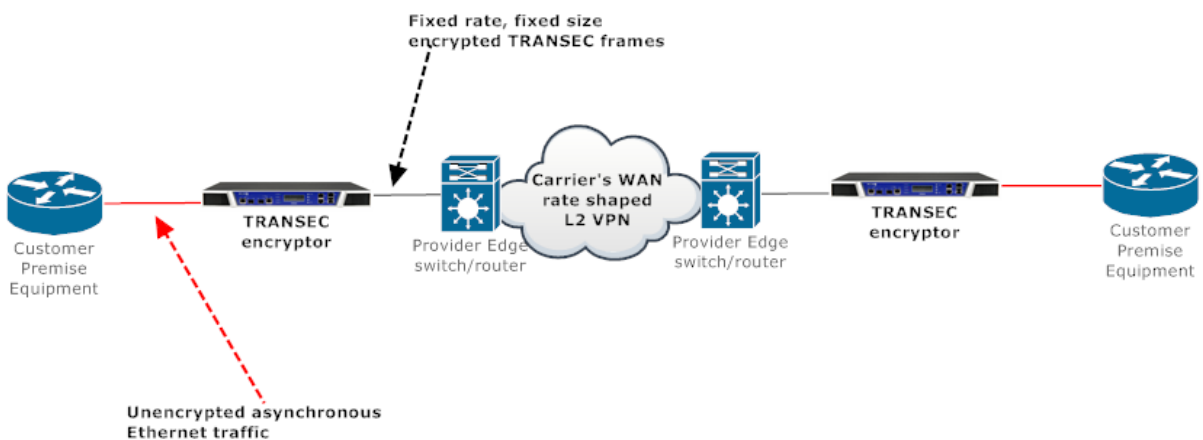


CI	Origin	Action	State	Peer Name	Remote Encrytor MAC	MAC Header
0001	System	Secure	Up	CN6140_A	00:d0:1f:aa:aa:aa	

TRANSEC

Traffic Analysis is the process of intercepting and examining messages in order to deduce information from patterns in communication. It can be performed even when the messages are encrypted and cannot be decrypted. TRANSEC is transmission security and is used to disguise patterns in network traffic to prevent Traffic Analysis.

Additional information can be obtained from Wikipedia, see: http://en.wikipedia.org/wiki/Traffic_analysis.



NOTE: TRANSEC can only be enabled on the CN4010, CN4020, CN6010, CN6040 and CN6100 models and only supports point-to-point connections. TRANSEC can only be used between encryptors operating at the same speed, that is, 1 Gbps to 1 Gbps and 10 Gbps to 10Gbps. If TRANSEC is enabled on a rate limited encryptor then the TRANSEC transmit bandwidth limit should not exceed the rate limiting bandwidth (minus the encryption overhead).

Encryption characteristics

TRANSEC enabled encryptors provide transmission security across a point-to-point rate-limited layer 2 VPN service provider network.

A TRANSEC enabled encryptor generates and transmits fixed-size encrypted Ethernet frames at a constant frame rate out the WAN facing network port.

The TRANSEC encryptor encrypts the entire Ethernet frame received on the local port so that no MAC addresses, other header information or payload data is exposed.

The rate of the transmitted Ethernet frame is constant and independent of the received plaintext traffic rate from the local port.

In the absence of user data from the local port the TRANSEC encryptor fills the transmitted frames with pseudo-random or encrypted data such that it cannot be distinguished from encrypted user data.

TRANSEC encryptors default to decrypting traffic received on their network interface and discard all introduced traffic that is not 'real' user data.

TRANSEC encryptors default to only transmitting decrypted 'real' user data out of the local interface port.

TRANSEC encryptors may (under policy) bypass certain control plane Ethernet Operations, Administration and Management (OAM) frames that are necessary for correct operation of the network.

The transmitted encrypted Ethernet frame rate and size are both configurable.

Ethernet headers of encrypted traffic (including both the source and destination MAC addresses and other optional header fields (VLAN tag, MPLS shim, etc.) are also user configurable.

TRANSEC encryptors are designed to minimise both the latency and jitter (variation in latency) of user data.

Data Plane traffic

On the RED interface the customer network generates asynchronous Ethernet traffic (known here as client traffic) of variable frame length and frequency.

On the BLACK port the TRANSEC encryptor generates fixed-size, fixed-rate encrypted frames (known here as transport traffic) containing a user defined fixed Ethernet frame header. Note that when rate limiting is applied to an encryptor, the limit applies to the transport traffic and this should be taken into account when establishing the parameters.

The contents of all client frames, including frame payload and frame header, is encrypted and encapsulated in the transmitted transport frames to ensure no leakage of sensitive data across the WAN.

To defeat traffic analysis across the layer 2 VPN, transport frames are of a constant size and transmitted at a constant frequency even in the absence of client frames.

Control Plane traffic

By default all client frames entering a TRANSEC-enabled encryptor are either encrypted or discarded and absolutely no traffic is bypassed. Practical experience on many service provider networks, however, has shown that it is sometimes necessary for customer premise equipment (e.g. a router or switch) to be able to communicate with the provider edge router or switch in order for end-end communications to work.

This is typically required when service providers use Ethernet OAM (Operations Administration & Management) to administer, manage and maintain network connectivity for purposes such as fault management, performance monitoring and link-layer discovery.

To allow for this the TRANSEC encryptor retains the capability to optionally bypass certain well-known protocols used for Operations and Maintenance (i.e. control plane) purposes. Mostly these protocols are identified by a reserved MAC address which we refer to as 'Reserved Multicast'.

If the 'Bypass Reserved Multicast' policy is enabled, each control plane protocol can be independently configured to bypass these frames through the encryptor without modification.

This facility, which is available in all connection modes, is disabled by default such that none of these traffic types are bypassed.



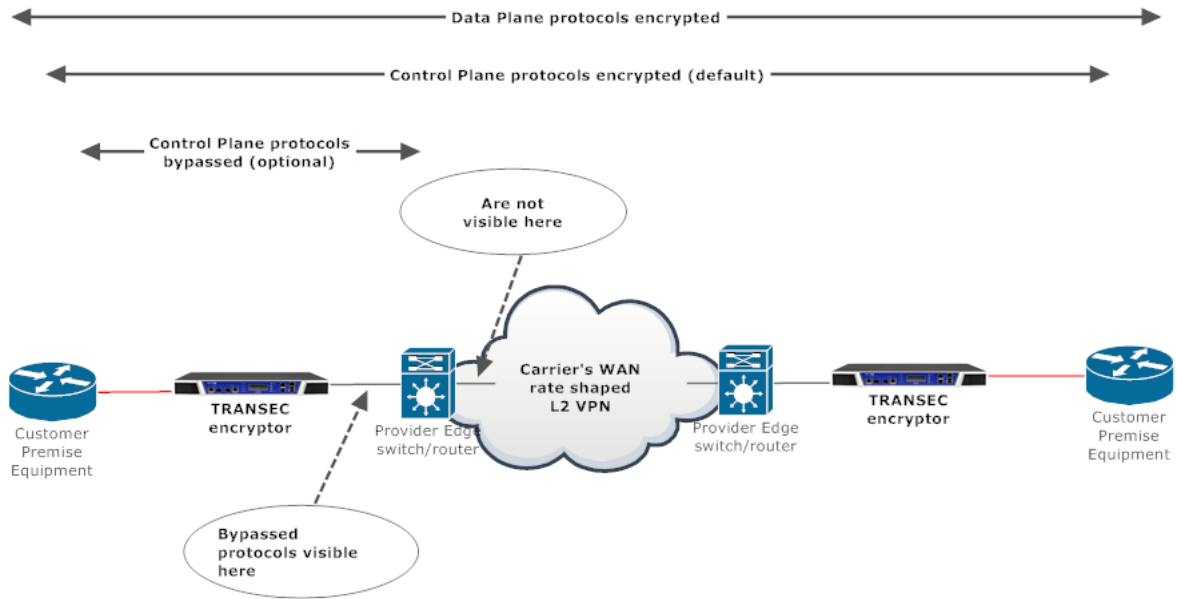


Figure 16: Re-assembly of Client Frames

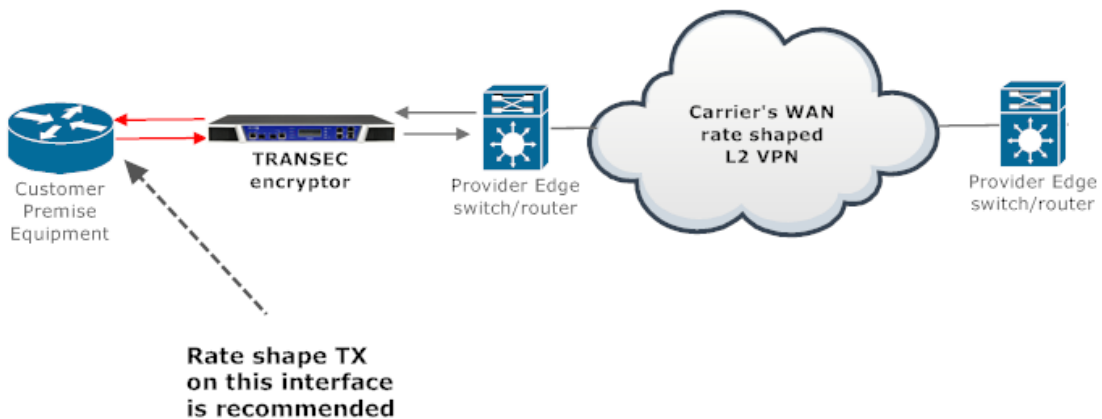
Flow Control

The encryptor does not participate in Ethernet flow control mechanisms, i.e. it does not generate or act on received PAUSE frames.

As discussed in the previous section, PAUSE frames may be optionally bypassed through the encryptor if required. However the end-to-end propagation delay on that link may prevent flow control operating correctly across the encryptors.

Because the TRANSEC encryptor necessarily causes bandwidth expansion (i.e. bandwidth transmitted on the BLACK interface is higher than that received on the RED interface) it is important not to overload the encryptors RED interface as this may cause buffer overflow and traffic to be discarded.

To prevent this it is recommended that the Customer Premise Equipment should rate-limit its transmissions using normal traffic shaping mechanisms (e.g. Cisco GTS).



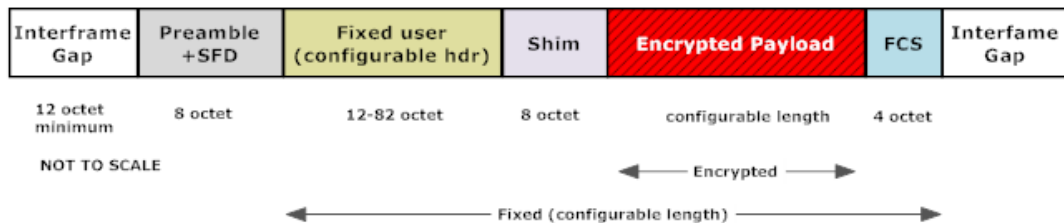
If TRANSEC is enabled on a rate limited encryptor then the TRANSEC transmit bandwidth limit should not exceed the rate limiting bandwidth (minus the encryption overhead).



Frame formats

TRANSEC-enabled encryptors expect the **client frames** received on the local port to be in the standard Ethernet format. See "Ethernet frame formats" on page 111.

The transport frame format as shown below contains a fixed (configurable) user header, an 8 octet shim used for encryption synchronization, an AES 256-bit CTR mode encrypted payload and a final frame check sequence.



Transport frames have a **header** that is between 12-82 octets long and is fully user configurable. In the simplest case this header comprises only Destination and Source MAC addresses. However the encryptor allows for more complicated headers that may include VLAN tags and multiple MPLS labels.

Configuration parameters allow the FPGA hardware to read data from memory and generate the required header combinations with minimal hardware complexity or overhead.

This feature allows TRANSEC enabled encryptors to be configured so that user traffic can negotiate 'challenging' networks that may be encountered when the units are deployed.

The transport frame header contains an 8 octet **shim** which is required for encryption synchronization. The Senetas encryptor formats this shim using an ethertype (0xFC0F) that is reserved for this purpose; however, this can be configured if required.

Common Ethertypes such as IPv4 (0x0800) should be avoided as experience shows that many switches inside service provider networks will 'look inside' well known frame types even if the provider has sold a 'transparent' service. Use of these can cause problems which include:

- Modifying user traffic (e.g. updating IP header checksums)
- Discarding user traffic
- Reordering user traffic

The encrypted **payload** uses a modified GFP (Generic Framing Protocol) mechanism to encrypt client frames. GFP is used because it is a well defined mature standard that it is widely used to efficiently transport Ethernet or Fibre Channel over SDH or OTN networks.

The modified GFP mechanism has been designed for quick recovery after a lost transport frame and has the following characteristics:

- GFP frames are not split across transport frames. The start of the first GFP frame is aligned with the start of the payload area.
- Unused payload area is filled with 4 octet long GFP idle frames, so there may be up to 3 octets of padding at the end containing all zeros.

Instructions for configuring the TRANSEC frame header are included in the CM7 policy section on page 198 and the CLI transec command described on page 313.



Transport Frame generation

Transport frames are generated at a fixed (configurable) rate; they all have the same (configurable) length. In the example shown in Figure 17 below:

- Client frame 1 is fully carried by Transport frame N+1
- Client frame 2 is fully carried by Transport frame N+2
- Client frame 3 is split across Transport frames N+2 and N+3

When client frames are available they are encapsulated into one or more transport frames. When client frames are not available the transport frames are padded.

- Transport frame N+1 carries the configurable frame header, client frame 1 and some padding.
- Transport frame N+2 carries the configurable frame header, client frame 2 and part of client frame 3.
- Transport frame N+3 carries the configurable frame header, the remainder of client frame 3 and some padding.
- Transport frame N+4 carries the configurable frame header and padding (no client frame available).

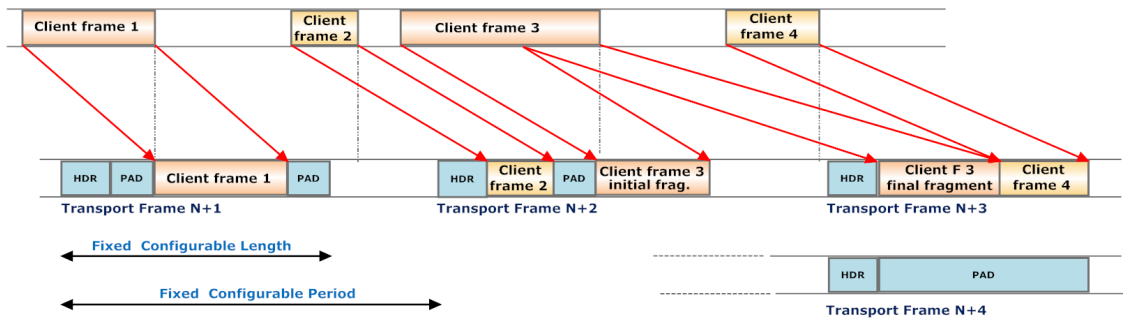


Figure 17: Transport Frame Assembly

Client Frame reassembly

Figure 18 below shows how a client frame is reassembled from received transport frames after transmission.

All transport frames containing fragments of a client frame must completely arrive before the decryptor will start to send the client frame to the remote LAN.

This is necessary because:

- The decryptor must wait until the last frame to know that all the fragments have been collected
- The decryptor must wait to receive a valid FCS at the end of the transport frame

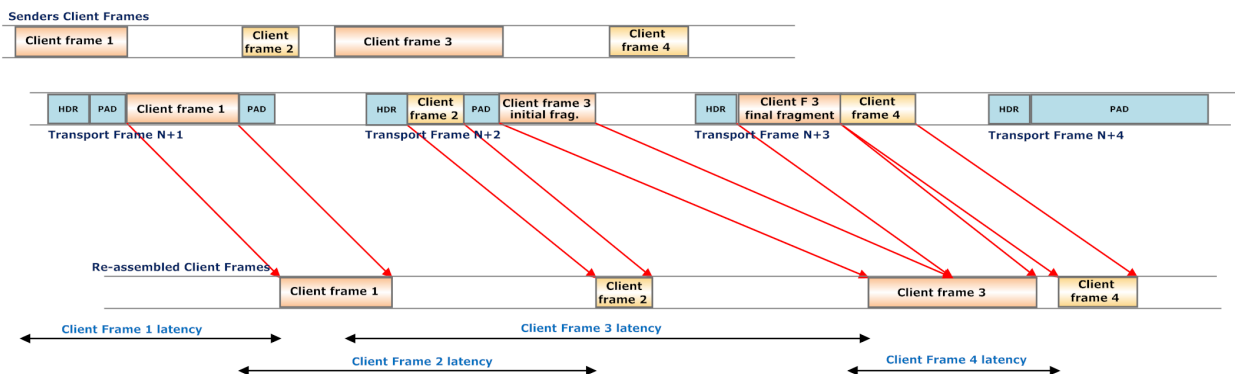


Figure 18: Re-assembly of Client Frames



Frame Rates

Three interdependent values relate to the transmission between two encryptors operating in TRANSEC mode. These are:

Frame Rate - the frames per second (fps) being transferred, for example 10,000.

Frame Length - the length of each frame in octets, for example 1,500.

Line Rate - the actual line rate of the connection in bits per second (bps), for example: 1×10^9 .

Given that the line rate is fixed, we can specify either of the remaining two or the percentage link utilization to establish the characteristics of the link. The applicable calculations are:

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

where 20 is the number of octets of unavoidable overhead per Ethernet frame, consisting of 12 octets (average) of interframe gap (IFG) plus 8 octets of preamble and start-of-frame delimiter.

$$\text{bps} = \text{Frame_Rate} \times \text{Frame_length} \times 8$$

CAUTION: The maximum bandwidth available is determined by the frame-rate settings and in real-world scenarios an allowance needs to be made for encryptor key management traffic and (if enabled) in-band management traffic. It is recommended that the utilization be set to less than 100%. Note also that both encryptors MUST be operating at the same speed.



Performance

The transport frame length and transmission rate are both user configurable and will affect the efficiency and latency of the encrypted connection. Note that on 10Gbps models the transport frame must be a multiple of 8 octets and if the set length is not a multiple it will be rounded down, for example, 159 would become 152.

Short transport frames are less efficient than long transport frames as the ratio of header to client data is higher. However, short transport frames have lower latency as on average less data needs to be buffered before reassembly.

Figure 19 below shows the available client bandwidth as a function of client frame size for three different configured transport frame lengths. The graph shows that efficiencies above 90% can easily be achieved by choosing the appropriate transport frame length. Refer also to the note on page 65.

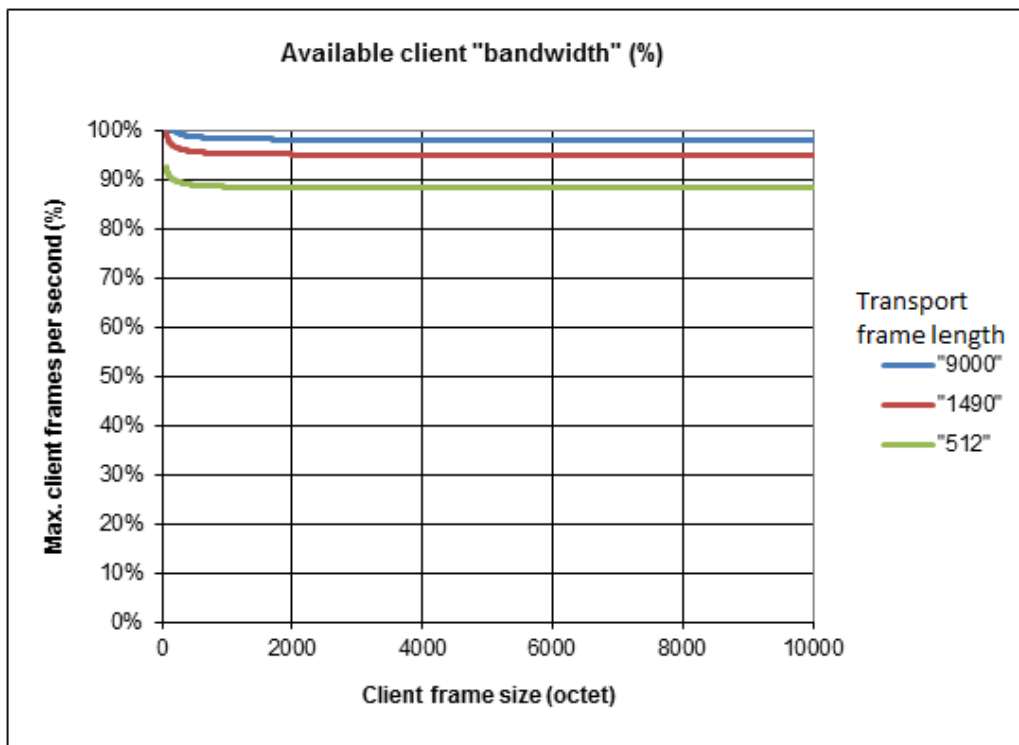


Figure 19: Transport efficiency

The figures that follow show how end-end latency varies with different client frame lengths dependent on the configured transport frame length.

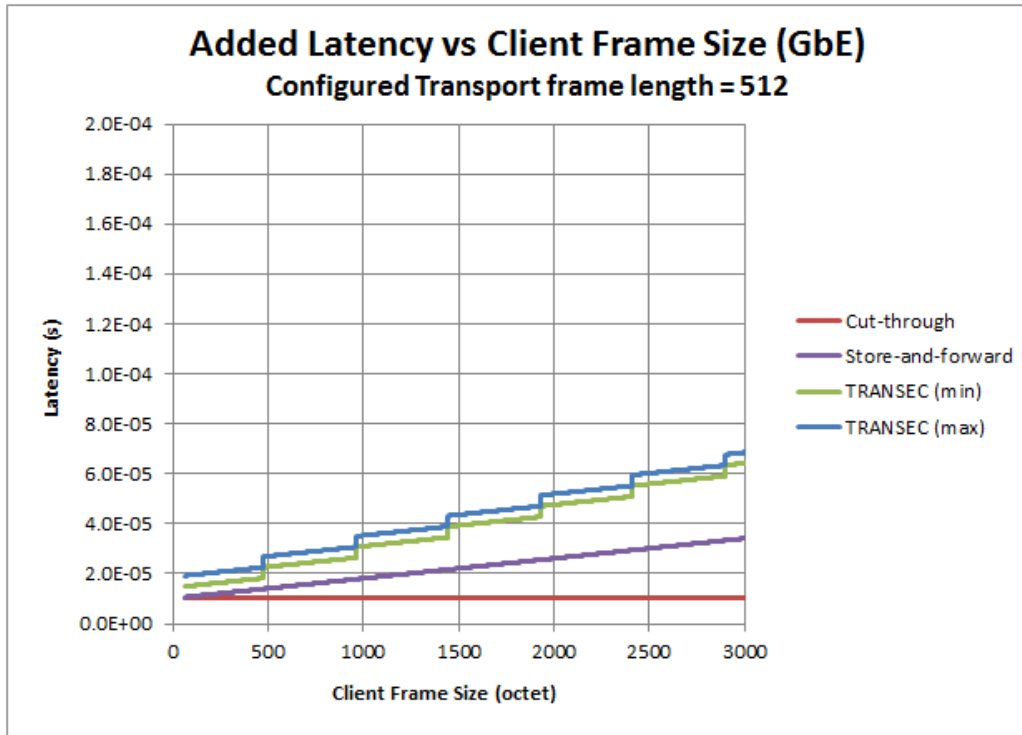


Figure 20: Latency variation with transport length of 512 octets

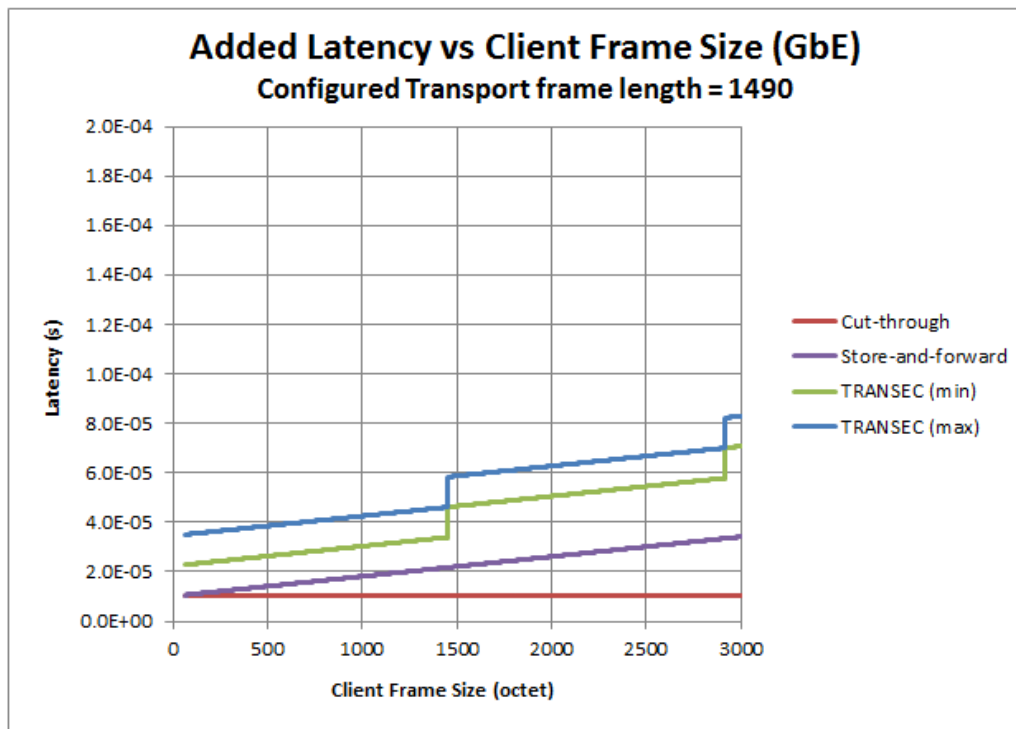


Figure 21: Latency variation with transport length of 1490 octets



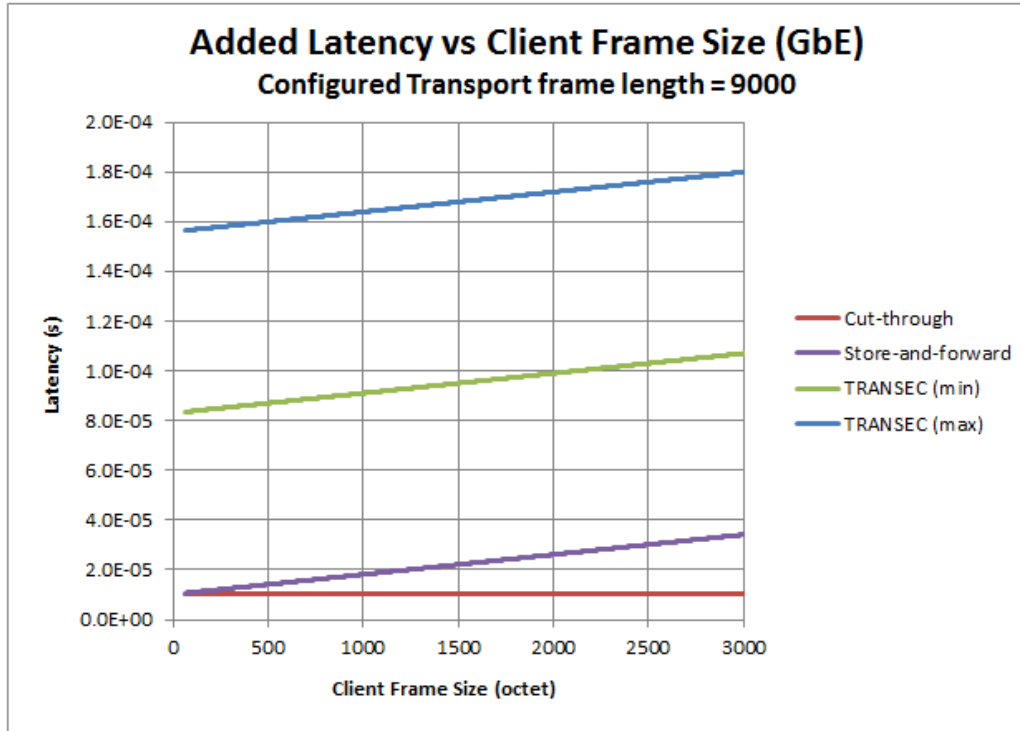


Figure 22: Latency variation with transport length of 9000 octets



Multipoint (Layer 2) MAC encryption

In general VLAN mode is recommended for multipoint Ethernet networks.

However, MAC mode can be used as an alternative to VLAN mode when policy needs to be applied to specific endpoint devices. For example, it may be necessary to discard traffic from a specific MAC address.

Encryptors can be configured in meshed networks as shown below so that traffic between end points can be encrypted based on the MAC address of the connected equipment..

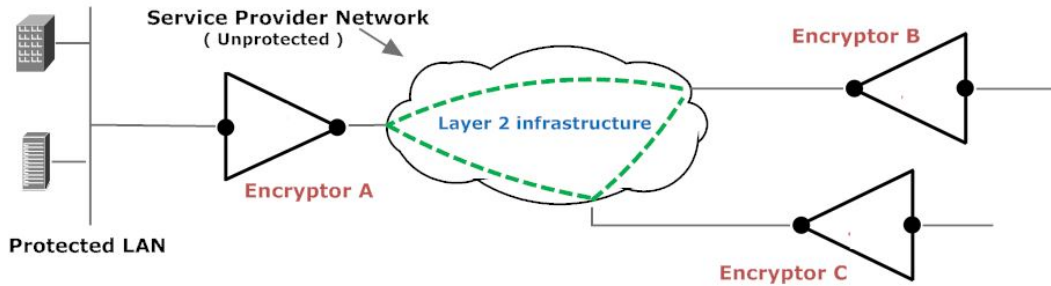


Figure 23: Multipoint MAC topology

Encryption policy is applied in a hierarchical manner as shown in Figure 24 below with the GLOBAL setting having the highest priority. Policy based on the ethertype of the frame is applied next, followed by policy based on the MAC address of the frame.

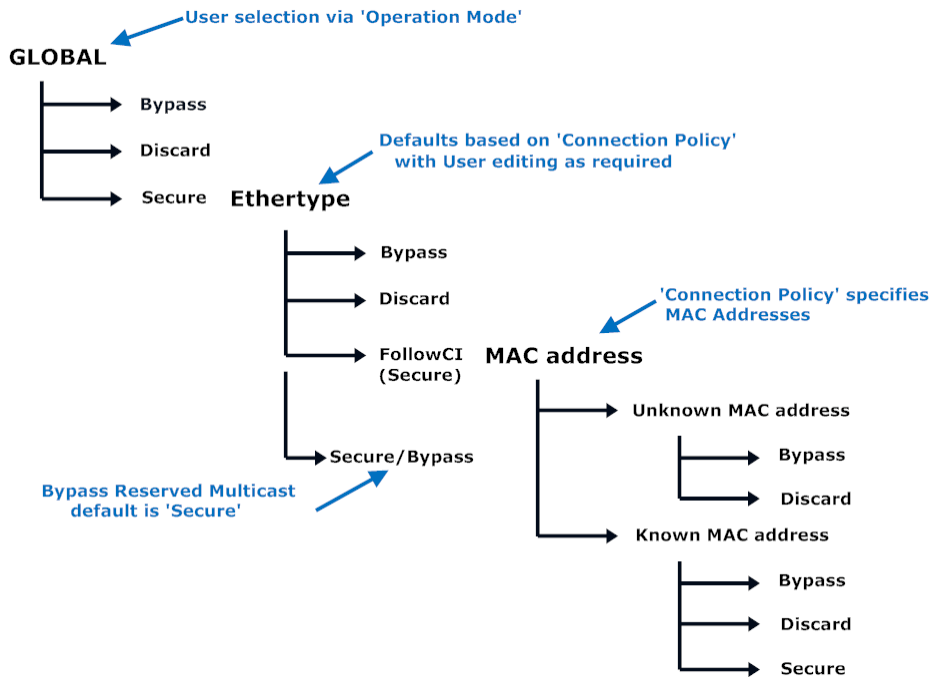


Figure 24: Multipoint MAC policy



Operation mode

Operation mode is a global selector that provides a quick way of bypassing or discarding all traffic through the encryptor regardless of the ethertype of a frame. Depending on factory settings, the initial mode is either 'Bypass' or 'Discard'.

The required mode is set to via the global Mode setting on the CM7 Policy tab. Setting the mode to 'Secure' (Encrypt All) specifies that frames will be processed as defined by policy. The mode can also be set using the CLI **global** command.

When the operator changes the mode of a layer 2 encryptor to 'Secure' the following transitions occurs:

1. Connection/tunnel discovery commences
2. Ethertype policy is then applied

Ethertype policy

The MAC mode ethertype table provides control over processing based on the ethertype of the frame. The table shown in Figure 25 below by default specifies actions for common ethertypes.

Ethertypes that are not included in the ethertype table are processed according to the "Unlisted Ethertype Action" processing policy and this entry can be edited as required.

ID	Type	Observe ..	Offs...	Broadcast .	Multicast A.	Unicast Actio	Mutation En.	Muta..	Injected T..
1	05FF (LENGTH)	<input type="checkbox"/> ignore	0	bypass	bypass	follow CI	<input type="checkbox"/> disabled	0000	bypass
2	0800 (IPV4)	<input type="checkbox"/> ignore	20	bypass	discard	follow CI	<input checked="" type="checkbox"/> enabled	F800	discard
3	0806 (ARP)	<input type="checkbox"/> ignore	0	bypass	discard	bypass	<input type="checkbox"/> disabled	F806	bypass
4	86DD (IPV6)	<input type="checkbox"/> ignore	40	bypass	discard	follow CI	<input checked="" type="checkbox"/> enabled	F6DD	discard
5	8808 (MAC-C)	<input type="checkbox"/> ignore	0	bypass	bypass	bypass	<input type="checkbox"/> disabled	F808	bypass
6	8809 (SPMA)	<input type="checkbox"/> ignore	0	bypass	bypass	bypass	<input type="checkbox"/> disabled	F809	bypass
7	88CC (LLDP)	<input type="checkbox"/> ignore	0	bypass	bypass	bypass	<input type="checkbox"/> disabled	F8CC	bypass
8	9000 (LOOPBACK)	<input type="checkbox"/> ignore	0	bypass	bypass	bypass	<input type="checkbox"/> disabled	F000	bypass

Figure 25: Default MAC mode Ethertype Policy

NOTE: When encrypting multicast traffic in multipoint mode the shim insertion rate is set to once per frame to facilitate automatic group key updates where there are multiple senders. In this mode the Shim Rate cannot be changed.

Additional ethertypes (up to a total of 15) can be added by clicking on the 'Add' button on the Policy tab, specifying each of the new column values as listed below and then clicking the 'Apply' button. The policy for an existing ethertype can be changed by changing the displayed value and clicking 'Apply'.



Table 34. Ethertype attributes

Field Name	Content
ID	Sequential ID - system assigned index
Type	Hex value and Ethertype name
Observe Offset	Observe if active, Ignore to ignore value
Offset Bytes	Octets to be left in clear if observed
Broadcast Action	Discard, Bypass or FollowCI
Multicast Action	Discard, Bypass or FollowCI
Unicast Action	Discard, Bypass or FollowCI
Mutation	Disabled, Enabled - to mutate ethertype
Mutation Value	Value to mutate type to
Injected Type	Discard, Bypass - action on observed mutated type

The action can be set to 'Bypass', 'Discard' or 'FollowCI' for each of the Ethernet addressing modes - Unicast, Multicast and Broadcast. If the 'FollowCI' policy is selected then the configured 'Offset' and/or 'Mutation' policy will be applied.

Observe Offset can be set active to allow a selected number of octets at the start of the payload to be left in the clear. Default is to encrypt the entire payload. See " Ethertype policy " on page 72.

Mutation can be enabled to mutate the ethertype to an alternate ethertype prior to transmission and restore it to the original ethertype when processing received frames. Note that offset and mutation need to be set identically in all peer encryptors and in CM7 the 'Copy To ..' button can be used to do this.

Where mutation is enabled, the injected traffic action will be either 'Bypass' or 'Discard', the latter being used to prevent traffic from within the network reaching the secure network(s).

NOTE: Prior to version 2.1.1 of the firmware, only Unicast address types could be specified to follow the connection identifier/tunnel action. The addition of multicast encryption in version 2.1.1 allowed all address types to be specified.

Ethertype mutation

Mutation allows the ethertype of the frame to be changed to a specified value when encrypting and reinstated to the original value when decrypting. See the ethertypes CLI command on page 1.

NOTE: Ethertype mutation or an Encryption offset may be required if intermediate equipment between a pair of encryptors makes decisions based on visibility of the payload that follows the Ethernet header. Examples of this are layer 2 services that require certain data to be present; although strictly speaking, this should not be the case in a true layer 2 network. Mutation (rather than Encryption offset) is the preferred method of addressing this type of problem as it does not leave any portion of the payload as plaintext.



Encryption offset (only L2 modes)

The ethertype configuration allows an optional encryption offset to be specified. The offset moves the encryption start point in the frame by the specified number of bytes, allowing a portion of the frame to be sent in the clear.

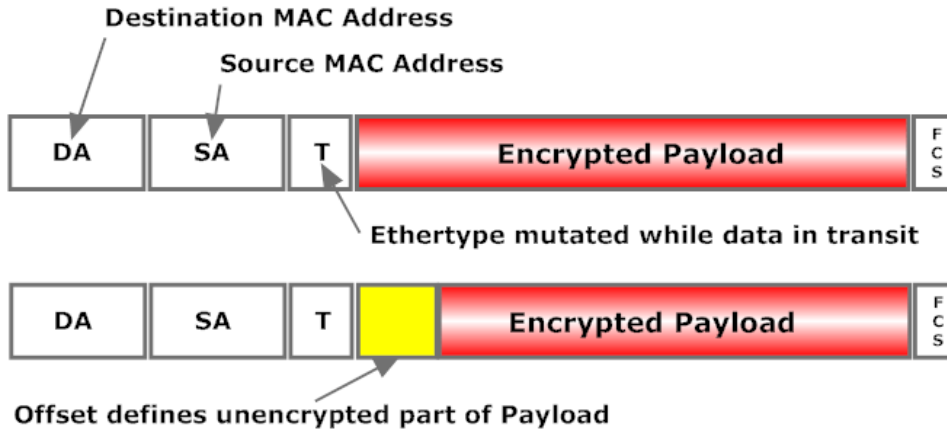


Figure 26: Point-to-point Mutated and Offset frames

NOTE: When passing VLAN traffic on a link configured in point-to-point (line) mode the VLAN identifier must be manually configured in the connection table. This can also be configured via the CLI `inband_vlan` command as described on page 1. This is not required in Multipoint mode as the ID is automatically learnt.

Bypass Reserved Multicast

In networks with switches or other configurable devices between encryptors it may be necessary to enable the bypassing of groups of MAC addresses that are used for this purpose. The following figure shows the CM7 screen used to do this.

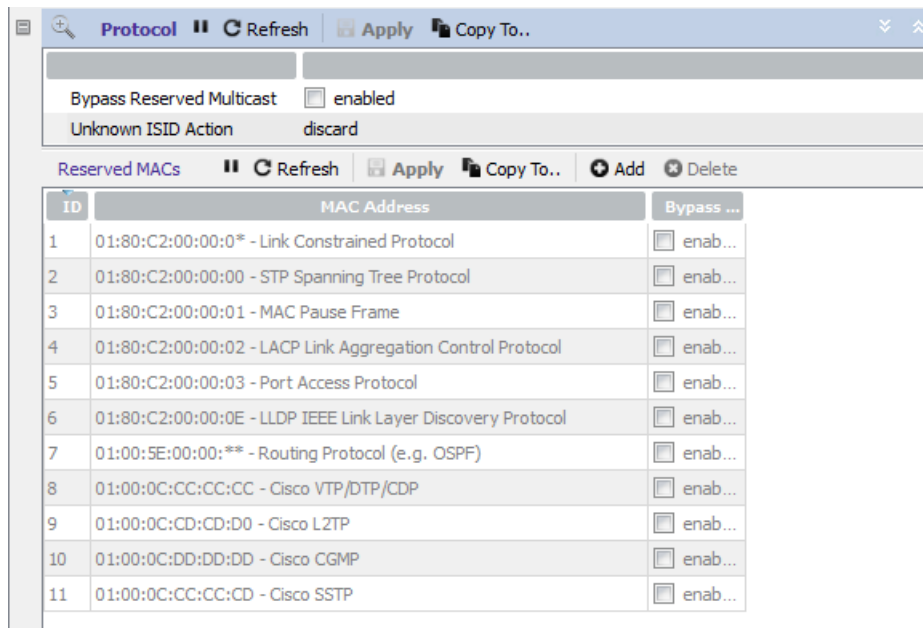


Figure 27: Bypass Reserved Multicast selection



MAC address policy and connections

Frames whose ethertype policy is set to 'FollowCI' have their final policy determined by their MAC address.

The MAC address used is:

The Destination MAC address for frames received on the Local port

AND

The Source MAC address for frames received on the Network port

When operating in MAC mode the connection table contains the following entries:

- A single Pending connection
- A single Bypass connection
- A single Discard connection
- Zero or more connections to remote encryptors

The first three entries are created automatically and the remaining ones are created through automatic discovery or manual entry by a user.

MAC address mode of operation

In MAC mode the encryptor can be used in a meshed topology and supports encrypted connections to multiple remote encryptors as was shown in above.

In this mode the security policy is extended to the remote MAC addresses transmitted frames.

Policy is established/defined by associating the destination MAC address of the frame with a unique connection between two physical locations. This association can occur in one of two ways:

- Automatic discovery of MAC addresses
- Manual entry of MAC addresses

The auto-discovery configuration option allows the encryptor to learn the MAC addresses from the network traffic and automatically establish secure connections with peer encryptors. See "MAC address mode of operation" on page 75).

Auto-discovery checkboxes are provided for both unicast and multicast traffic. Broadcast traffic is not auto-discovered.

When multicast auto-discovery is enabled you can also set the inactivity time (in minutes) after which multicast connections will be deleted. This setting should only be left at the default value of 0 where multicast traffic is predictable; otherwise the continued addition of new multicast groups is likely to fill the netmacs table after which new connections will not establish.

If auto-discovery is disabled then the required remote identifiers must be manually configured in the encryptor.

When encrypting unicast traffic, entries in the connection table represent the MAC addresses protected by the connection.

When a Unicast frame is received with an unknown MAC address and Unicast Auto-discovery is enabled the MAC address is initially associated with the 'System Pending' connection.

If manual addition or entry is required then these can be made using the 'Add' and/or 'Apply' buttons on the MAC Addresses tab.



MAC Connection Establishment

When configured in multipoint MAC mode the encryptor maintains internal tables of local and network MAC addresses for all frames that pass through it. Addresses listed in the local MAC (locmac) table are those of devices protected behind the encryptor's local port.

Addresses in the network MAC (netmac) table are those of devices that exist somewhere on the network side of the encryptor. Each address in the network MAC table is associated with a connection table entry.

If the Auto Discovery option is enabled the tables can be automatically populated by the encryptor as frames are received. The encryptor parses all frames received on both local and network interfaces and adds the frame's MAC addresses to the internal MAC tables.

When a newly discovered remote MAC address is assigned to the system pending Tunnel/CI table entry, the local encryptor will try to establish whether there is a remote peer encryptor protecting the new address. If a remote peer is found and an existing connection exists between the two encryptors, the new MAC address will be assigned to this connection. If there is no existing connection the local encryptor will then attempt to establish a secure connection with the remote peer. Once this has been established, a new Tunnel/CI entry will be created in the Connection Table (CAT) with the Origin field set to automatic. The remote MAC address will then be assigned to the new connection. If a peer encryptor cannot be found the remote MAC address will be left in the system pending entry and the process will be repeated.

Management Frames are transmitted using Ethernet II with a proprietary Senetas ethertype of FC0F.

NOTE: While the FC0F ethertype has been formally registered and it is unlikely that other vendors will use it, Senetas encryptors also use several other unregistered high range ethertypes. These include FC0E and FC0D and in the unlikely event that these clash with other vendor equipment you should reconfigure to avoid them.

Automatic discovery

Automatic configuration begins when the encryptors are set to 'Line mode' and their 'Operation Mode' is set to 'Encrypt All'. The transition from Point-to-point (Line) mode to Multipoint mode will force an encryptor restart and this requires user confirmation.

NOTE: Only one connection is established between a given pair of Ethernet encryptors. All Unicast frames passing through the encryptor are processed according to the specified action for that connection.

The figures that follow show the process that is followed as the encryptors use the proprietary ERP message to configure the units:



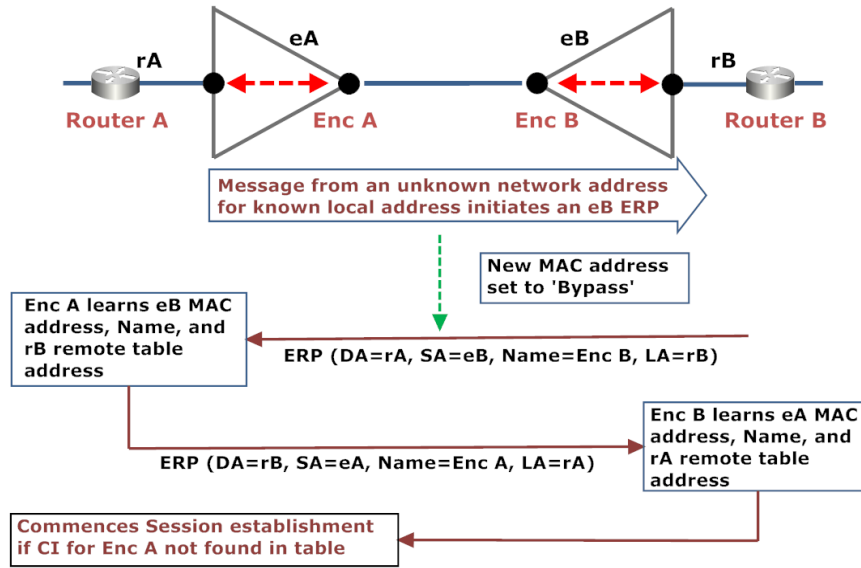


Figure 28: Network invocation ERP message flows

Unidentified traffic on the local port results in use of the Encryption Resolution Protocol (ERP) to determine and learn the name and address of the remote unit that protects the remote device. A new connection is established if a CI does not already exist.

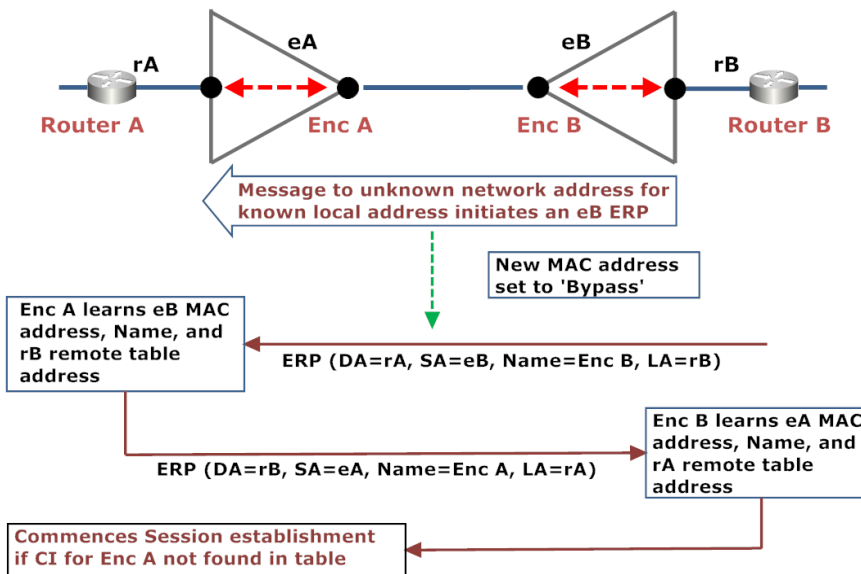


Figure 29: Local invocation ERP message flows

MAC migration

The figure that follows shows the process that is followed when a device such as a PC is moved from one geographic location to another.



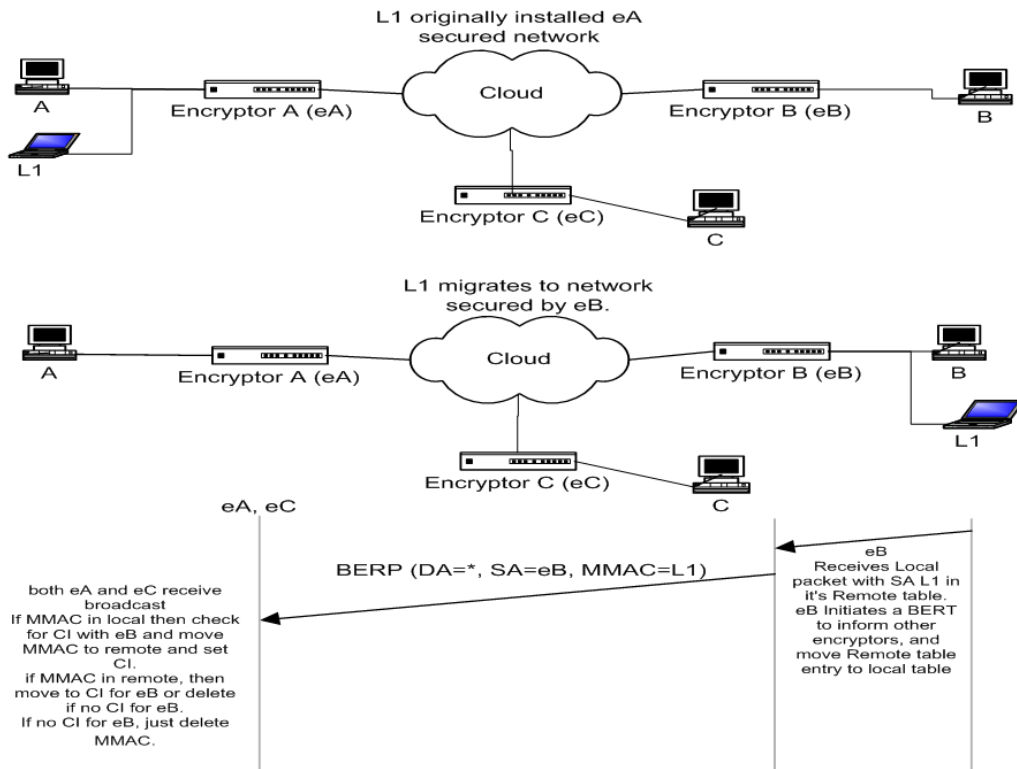


Figure 30: Automatic MAC migration

Spanning Tree Protocol support

The CN Series supports operation in networks that use the Per-VLAN Spanning Tree Protocol (PVST or STP) to provide redundant communication paths (see CLI reference **policy** command).

STP is used to prevent active loops in a switched network and can provide high availability and automatic failover to redundant links.

To maintain an STP topology all switches advertise their STP knowledge via configuration messages. These configuration messages are transmitted periodically (once every hello time). Absence of these messages can cause inactive ports to become active and cause a topology change.

When a topology change occurs, a topology change message is sent on the affected links. This informs the switches of the change and a new path is selected.

Refer to Wikipedia for additional detail - http://en.wikipedia.org/wiki/Spanning_tree_protocol.

STP monitoring

The STP Monitoring feature makes use of the above information to enable failover between encryptors. The encryptor can be connected to any switch or port within a Spanning Tree Topology. There are no limitations on the type of the spanning tree port type connected, that is, the encryptor can be connected to a root, designated, alternate or backup port.

The encryptor monitors STP Configuration and Topology Change messages to identify when a topology change occurs. When a topology change is detected, the local MAC address table is purged. The absence of local MAC address in the encryptor means that when the Spanning Tree Topology reconverges and starts forwarding data, new address are identified on the local



(Protected) side of the encryptor. When new MAC address are identified on the local side of the encryptor the Auto-Discovery feature causes the encryptor to notify all other encryptors that it is now protecting these MAC address; completing the failover process.

Encryptors detect a topology change on the following conditions:

- BPDU Topology Change message
- BPDU Configuration message with Topology Change flag set
- BPDU Configuration message with Topology Change Acknowledge flag set
- BPDU Configuration message absence at least 3 hello time periods followed by BPDU configuration message reception

NOTE: STP monitoring requires auto-discovery to be enabled.

Local MAC address purging

Typical operation of the encryptor is to preserve MAC addresses, that is, No ageing. When STP monitoring is enabled and an STP topology change is identified, the Local MAC address table is “aged” (purged).

NOTE: STP Monitoring does not have any adverse effects on the encryptor’s throughput or latency.

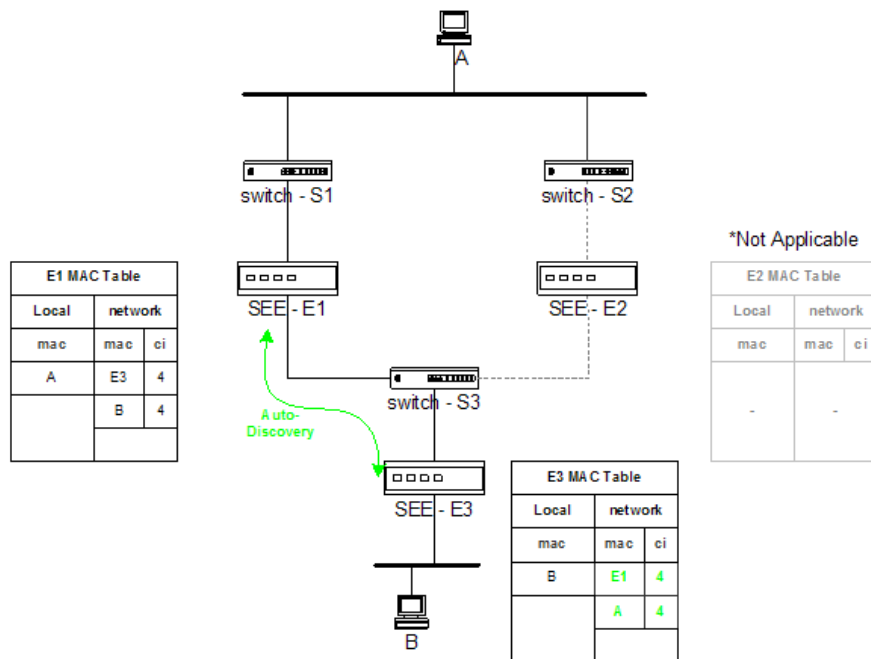


Figure 31: STP initial State

In this example, encryptor SEE-E1 is on the active path within the spanning tree. The SEE-E2 encryptor is on a blocked/alternate segment and is not visible to the other encryptors. SEE-E1 and SEE-E3 identify each other and establish a connection via the auto-discovery mechanism.

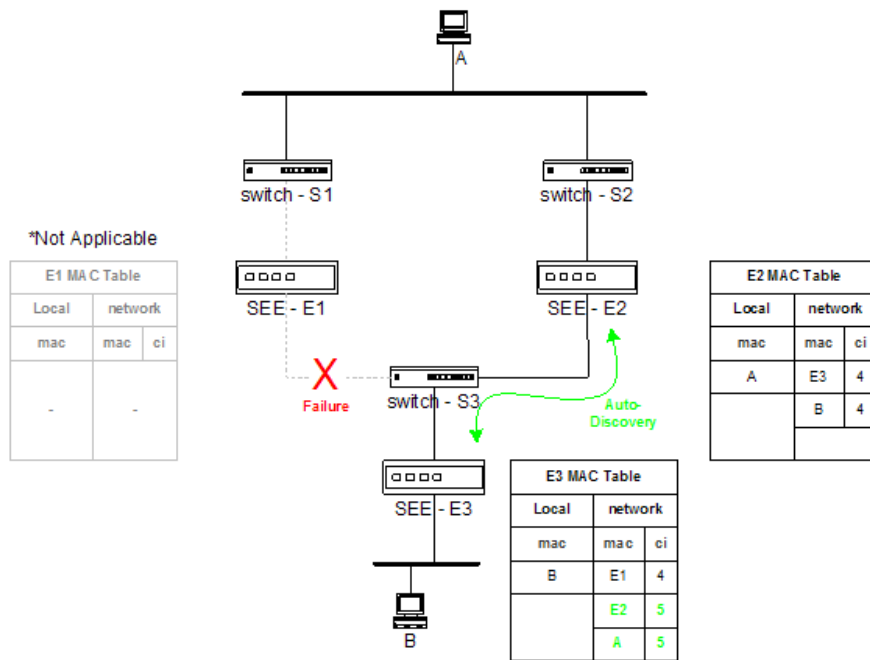


Figure 32: STP failover state

If a failure occurs on the active path the Spanning Tree detects the failure and performs a topology change to use the inactive/alternate path.

SEE-E2 and SEE-E3 identify each other and establish a connection via the auto-discovery mechanism if they have not previously communicated. Note that the SEE-E3 encryptor is notified of the change and the remote MAC address A is moved from connection 4 to connection 5.

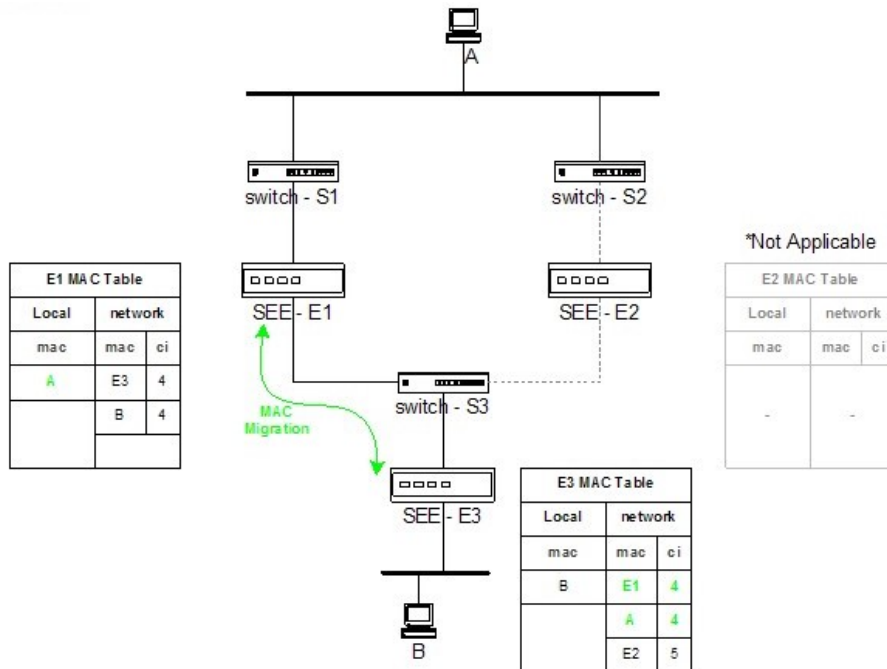


Figure 33: STP restored state



Once the failure is removed the root path is restored. The Spanning Tree generates a topology change and the local MAC table in SEE-E1 is purged. Then, as traffic is forwarded, the MAC discovery mechanism SEE-E1 learns MAC address A and notifies SEE-E3. SEE-E3 adjusts its network MAC table accordingly to map MAC address A back to connection 4.

Configuring STP monitoring

STP monitoring can be configured from the CLI using the following steps.

1. Enable Auto-Discovery

```
Encryptor>autodisco -e
Automatic session discovery enabled
```

2. Set ether type table policy for H05FF multicast addressed frames to Bypass AND / OR

Set Reserved Multicast Address Bypass Enabled.

```
Encryptor>ethertypes -e
Enter Ether type [(O)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 ether type
SafeEnterprise Encryptor>
```

AND / OR

```
Encryptor>policy -b -e
Reserved Multicast bypass enabled
```

3. Enable STP Monitoring

```
Encryptor>policy -s -e
STP monitoring enabled
```

Automatic configuration using the CLI

1. Ensure that the configuration of the encryptor is in the default condition by using the **initcfg** CLI command on each unit. This command will restart the encryptor.

```
CN6140_A>initcfg -a
CN6140_B>initcfg -a
CN6140 (slot 0)>initcfg -a
```



2. Ensure that Auto-Discovery is enabled.

```
CN6140_A>autodisco -e
```

```
CN6140_B>autodisco -e
```

```
CN6140 (slot 0)>autodisco -e
```

3. Put the encryptors into 'Secure' mode.

```
CN6140_A>global -e
```

```
CN6140_B>global -e
```

```
CN6140 (slot 0)>global -e
```

4. Confirm that the tunnels/connections are in the 'Up' state and that the addresses were learnt correctly. [Optional]

The connections will not be 'Up' until a connection (based on traffic) is initiated between encryptors. Use only non-production traffic to initiate a connection between encryptors.

```
CN6140_A>tunnels
```

```
Interface (tunnel/CI) MAC address : 00:d0:1f:aa:aa:aa
```

```
Front Panel Management MAC address : 00:d0:1f:00:aa:aa
```

```
CI   Origin   Action   State   Peer Name           Remote Encryptor MAC MAC Header
```

```
----
```

```
0001 PENDING   Bypass   Up      N/A
```

```
0002 System    Discard   Up      N/A
```

```
0003 System    Bypass   Up      N/A
```

```
0004 Automatic Secure    Up      CN6140_B           00:d0:1f:bb:bb:bb
```

```
0005 Automatic Secure    Up      CN6140 (slot 0)    00:d0:1f:cc:cc:cc
```

```
CN6140_B>tunnels
```

```
Interface (tunnel/CI) MAC address : 00:d0:1f:bb:bb:bb
```

```
Front Panel Management MAC address : 00:d0:1f:00:bb:bb
```

```
CI   Origin   Action   State   Peer Name           Remote Encryptor MAC MAC Header
```

```
----
```

```
0001 PENDING   Bypass   Up      N/A
```

```
0002 System    Discard   Up      N/A
```

```
0003 System    Bypass   Up      N/A
```

```
0004 Automatic Secure    Up      CN6140_A           00:d0:1f:aa:aa:aa
```

```
0005 Automatic Secure    Up      CN6140 (slot 0)    00:d0:1f:cc:cc:cc
```

```
CN6140 (slot 0)>tunnels
```

```
Interface (tunnel/CI) MAC address : 00:d0:1f:cc:cc:cc
```

```
Front Panel Management MAC address : 00:d0:1f:00:cc:cc
```

```
CI   Origin   Action   State   Peer Name           Remote Encryptor MAC MAC Header
```

```
----
```

```
0001 PENDING   Bypass   Up      N/A
```

```
0002 System    Discard   Up      N/A
```

```
0003 System    Bypass   Up      N/A
```



0004	Automatic	Secure	Up	CN6140_A	00:d0:1f:aa:aa:aa
0005	Automatic	Secure	Up	CN6140_B	00:d0:1f:bb:bb:bb

```

CN6140 (slot 0)>netmacs
-----
Network Mac      CI
-----
00:d0:1f:aa:aa:aa 0004
00:11:11:11:11:11 0004
00:d0:1f:bb:bb:bb 0005
00:22:22:22:22:22 0005
4 Valid records

CN6140 (slot 0)>locmacs
-----
Local Mac
-----
00:33:33:33:33:33
1 Valid record

```

5 Change Pending tunnel/connection to discard. [Post commissioning step]

The pending connection (CI 0001) is used to define policy (Bypass/Discard) on all packets with unknown remote identifiers. The action of this tunnel should be changed to 'Discard' in order to prevent against ARP spoofing/man in the middle attacks.

```

CN6140_A>tunnels -e 1
-----
CI   Origin   Action   State   Peer Name   Remote Encryptor MAC MAC Header
-----
0001 PENDING   Bypass   Up      N/A
-----
Remote Encryptor MAC :: N/A
Remote Encryptor Name : [] N/A
Tunnel Action: <(D)iscard | (B)ypass>: [Bypass] D
Extra header length (0,4,8) : N/A
Updated existing tunnel

CN6140_A>

```

```

CN6140_B>tunnels -e 1
-----
CI   Origin   Action   State   Peer Name   Remote Encryptor MAC MAC Header
-----
0001 PENDING   Bypass   Up      N/A
-----

```



```

Remote Encryptor MAC :: N/A
Remote Encryptor Name : [] N/A
Tunnel Action: <(D)iscard | (B)ypass>: [Bypass] D
Extra header length (0,4,8) : N/A
Updated existing tunnel
CN6140_B>

```

```

CN6140 (slot 0)>tunnels -e 1

```

CI	Origin	Action	State	Peer Name	Remote Encryptor MAC	MAC Header
0001	PENDING	Bypass	Up	N/A		

```

Remote Encryptor MAC :: N/A
Remote Encryptor Name : [] N/A
Tunnel Action: <(D)iscard | (B)ypass>: [Bypass] D
Extra header length (0,4,8) : N/A
Updated existing tunnel
CN6140 (slot 0)>

```

6 Ensure that auto-discovery is disabled by selecting and disabling it in each encryptor.

[Post commissioning step to lock down configuration]

```

CN6140_A>autodisco -d
CN6140_B>autodisco -d
CN6140 (slot 0)>autodisco -d

```

Manual configuration using the CLI

The following configuration example refers to the network topology described in Figure 23 on page 71.

The following commissioning steps should only use non-production traffic as it may not be encrypted until commissioning is complete.

1 Use the 'initcfg' command to ensure that the encryptors configuration is in default condition This command causes an intentional restart.

```

CN6140_A>initcfg -a
CN6140_B>initcfg -a

```



```
CN6140 (slot 0)>initcfg -a
```

2 Ensure that unicast auto-discovery is disabled.

```
CN6140_A>autodisco -d
```

```
CN6140_B>autodisco -d
```

```
CN6140 (slot 0)>autodisco -d
```

3 Put the encryptors into 'Secure' mode to allow connections based on traffic.

```
CN6140_A>global -e
```

```
CN6140_B>global -e
```

```
CN6140 (slot 0)>global -e
```

4 Add the required connections/(tunnels) manually.

```
CN6140_A>tunnels -a 00:d0:1f:bb:bb:bb
```

```
Remote Encryptor Name : [] CN6140_B
```

```
Tunnel Action: <(D)iscard | (B)ypass | (S)ecure>: [Discard] S
```

```
Extra header length (0,4,8) : [0] 0
```

```
Added new tunnel ci 4
```

```
CN6140_A>tunnels -a 00:d0:1f:cc:cc:cc
```

```
Remote Encryptor Name : [] CN6140 (slot 0)
```

```
Tunnel Action: <(D)iscard | (B)ypass | (S)ecure>: [Discard] S
```

```
Extra header length (0,4,8) : [0] 0
```

```
Added new tunnel ci 5
```

```
CN6140_B>tunnels -a 00:d0:1f:aa:aa:aa
```

```
Remote Encryptor Name : [] CN6140_A
```

```
Tunnel Action: <(D)iscard | (B)ypass | (S)ecure>: [Discard] S
```

```
Extra header length (0,4,8) : [0] 0
```

```
Added new tunnel ci 4
```

```
CN6140_B>tunnels -a 00:d0:1f:cc:cc:cc
```

```
Remote Encryptor Name : [] CN6140 (slot 0)
```

```
Tunnel Action: <(D)iscard | (B)ypass | (S)ecure>: [Discard] S
```

```
Extra header length (0,4,8) : [0] 0
```

```
Added new tunnel ci 5
```

```
CN6140 (slot 0)>tunnels -a 00:d0:1f:aa:aa:aa
```

```
Remote Encryptor Name : [] CN6140_A
```

```
Tunnel Action: <(D)iscard | (B)ypass | (S)ecure>: [Discard] S
```

```
Extra header length (0,4,8) : [0] 0
```



```
Added new tunnel ci 4
```

```
CN6140 (slot 0)>tunnels -a 00:d0:1f:bb:bb:bb
```

```
Remote Encryptor Name : [] CN6140_B
```

```
Tunnel Action: <(D)iscard | (B)ypass | (S)ecure>: [Discard] S
```

```
Extra header length (0,4,8) : [0] 0
```

```
Added new tunnel ci 5
```

5 Add the local MAC addresses.

```
CN6140_A>locmacs -a 00:11:11:11:11:11
```

```
Added new local mac address
```

```
CN6140_B>locmacs -a 00:22:22:22:22:22
```

```
Added new local mac address
```

```
CN6140 (slot 0)>locmacs -a 00:33:33:33:33:33
```

```
Added new local mac address
```

6 Add the network MAC addresses.

```
CN6140_A>netmacs -a 00:22:22:22:22:22
```

```
Enter CI to associate mac address with : 4
```

```
Added new remote mac address
```

```
CN6140_A>netmacs -a 00:33:33:33:33:33
```

```
Enter CI to associate mac address with : 5
```

```
Added new remote mac address
```

```
CN6140_B>netmacs -a 00:11:11:11:11:11
```

```
Enter CI to associate mac address with : 4
```

```
Added new remote mac address
```

```
CN6140_B>netmacs -a 00:33:33:33:33:33
```

```
Enter CI to associate mac address with : 5
```

```
Added new remote mac address
```

```
CN6140 (slot 0)>netmacs -a 00:11:11:11:11:11
```

```
Enter CI to associate mac address with : 4
```

```
Added new remote mac address
```

```
CN6140 (slot 0)>netmacs -a 00:22:22:22:22:22
```

```
Enter CI to associate mac address with : 5
```



Added new remote mac address

7 Confirm that the tunnels are in the 'Up' state. [optional]

Note that the tunnels will not be 'Up' until a connection is initiated between encryptors. Use only non-Production traffic to initiate a connection between encryptors.

```
CN6140_A>tunnels -e 1
```

CI	Origin	Action	State	Peer Name	Remote Encryptor MAC	MAC Header
0001	PENDING	Bypass	Up	N/A		

```
Remote Encryptor MAC :: N/A
```

```
Remote Encryptor Name : [] N/A
```

```
Tunnel Action: <(D)iscard | (B)ypass>: [Bypass] D
```

```
Extra header length (0,4,8) : N/A
```

```
Updated existing tunnel
```

```
CN6140_A>
```

```
CN6140_B>tunnels -e 1
```

CI	Origin	Action	State	Peer Name	Remote Encryptor MAC	MAC Header
0001	PENDING	Bypass	Up	N/A		

```
Remote Encryptor MAC :: N/A
```

```
Remote Encryptor Name : [] N/A
```

```
Tunnel Action: <(D)iscard | (B)ypass>: [Bypass] D
```

```
Extra header length (0,4,8) : N/A
```

```
Updated existing tunnel
```

```
CN6140_B>
```

```
CN6140 (slot 0)>tunnels -e 1
```

CI	Origin	Action	State	Peer Name	Remote Encryptor MAC	MAC Header
0001	PENDING	Bypass	Up	N/A		

```
Remote Encryptor MAC :: N/A
```

```
Remote Encryptor Name : [] N/A
```

```
Tunnel Action: <(D)iscard | (B)ypass>: [Bypass] D
```

```
Extra header length (0,4,8) : N/A
```

```
Updated existing tunnel
```

```
CN6140 (slot 0)>
```



```

CN6140_A>tunnels
Interface (tunnel/CI) MAC address : 00:d0:1f:aa:aa:aa
Front Panel Management MAC address : 00:d0:1f:00:aa:aa

CI   Origin   Action   State   Peer Name   Remote Encryptor MAC   MAC Header
----  -
0001 PENDING   Bypass   Up      N/A
0002 System   Discard  Up      N/A
0003 System   Bypass   Up      N/A
0004 Automatic Secure   Up      CN6140_B   00:d0:1f:bb:bb:bb
0005 Automatic Secure   Up      CN6140 (slot 0)  00:d0:1f:cc:cc:cc
CN6140_A>netmacs
Network Mac      CI
-----
00:d0:1f:bb:bb:bb 0004
00:22:22:22:22:22 0004
00:d0:1f:cc:cc:cc 0005
00:33:33:33:33:33 0005
4 Valid records
    
```

```

CN6140_A>locmacs
Local Mac
-----
00:11:11:11:11:11
1 Valid record
    
```

```

CN6140_B>tunnels
Interface (tunnel/CI) MAC address : 00:d0:1f:bb:bb:bb
Front Panel Management MAC address : 00:d0:1f:00:bb:bb

CI   Origin   Action   State   Peer Name   Remote Encryptor MAC   MAC Header
----  -
0001 PENDING   Bypass   Up      N/A
0002 System   Discard  Up      N/A
0003 System   Bypass   Up      N/A
0004 Automatic Secure   Up      CN6140_A   00:d0:1f:aa:aa:aa
0005 Automatic Secure   Up      CN6140 (slot 0)  00:d0:1f:cc:cc:cc
CN6140_B>netmacs
Network Mac      CI
-----
00:d0:1f:aa:aa:aa 0004
00:11:11:11:11:11 0004
    
```



```
00:d0:1f:cc:cc:cc 0005
```

```
00:33:33:33:33:33 0005
```

```
4 Valid records
```

```
CN6140_B>locmacs
```

```
Local Mac
```

```
-----
```

```
00:22:22:22:22:22
```

```
1 Valid record
```

8 Change Pending tunnel to Discard. [Post commissioning step]

The pending tunnel (CI 0001) is used to determine policy (Bypass/Discard) on all packets with unknown remote MAC addresses. You should ensure that the action of this tunnel is set to 'Discard' (the default state) in order to prevent ARP spoofing/man-in-the-middle attacks.



Multipoint (Layer 2) VLAN encryption

VLAN encryption mode is best used across end-to-end Ethernet multipoint or 'hub and spoke' networks.

This mode seamlessly encrypts all unicast, broadcast and multicast traffic and can be used whether VLAN tags are present or not in the traffic.

Each VLAN is encrypted with a unique key and the mode supports complex network topologies with group key encryption.

VLAN helps prevent unauthorized access and data breaches within segmented network zones and is fault-tolerant, self-healing, and highly resilient to network outages.

Ethernet encryption policy provides fine control over how Ethernet frames are processed as they pass through the encryptor.

Encryption policy is applied in a hierarchical manner as shown in Figure 34 below with the GLOBAL setting having the highest priority. Policy based on the ethertype of the frame is applied next, followed by policy based on the VLAN IDs.

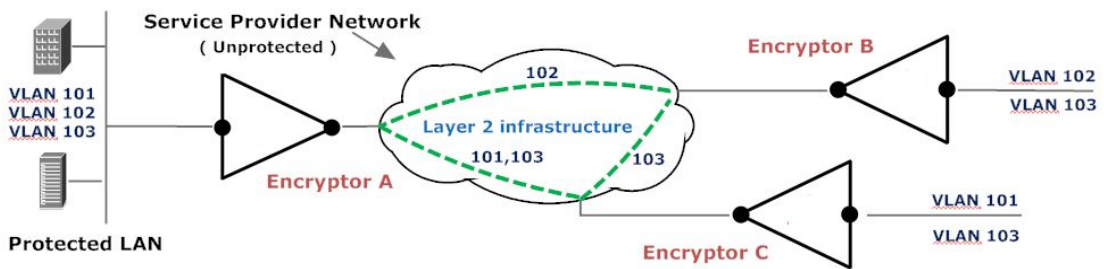


Figure 34: Multipoint VLAN network topology

Encryption policy is applied in a hierarchical manner as shown in Figure 35 below with the GLOBAL (operation mode) setting having the highest priority followed by the ethertype and then the VLAN ID(s) of the frame.

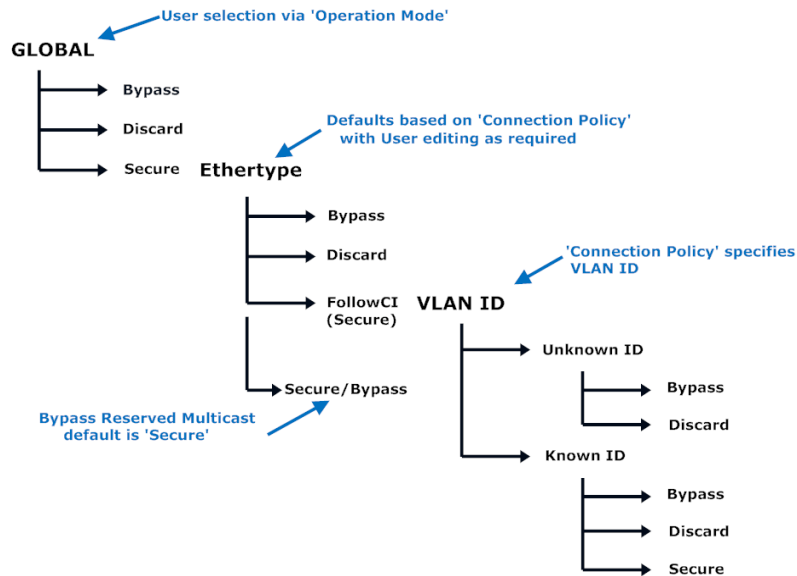


Figure 35: Multipoint VLAN Policy

The 'Secure' selection on the 'Ethernet Summary' tab specifies that frames will be secured as specified by the 'ethertype' policy and then the tunnel/connection (CI) policy. 'Secure' can also be set using the CLI **global** command as described on page .



Operation mode

Operation mode is a global selector that provides a quick way of bypassing or discarding all traffic through the encryptor regardless of the ethertype of a frame. Depending on factory settings, the initial mode is either 'Bypass' or 'Discard'.

The required mode is set to via the global Mode setting on the CM7 Policy tab. Setting the mode to 'Secure' (Encrypt All) specifies that frames will be processed as defined by policy. The mode can also be set using the CLI **global** command.

When the operator changes the mode of a layer 2 encryptor to 'Secure' the following transitions occurs:

1. Connection/tunnel discovery commences
2. Ethertype policy is then applied

VLAN Policy settings

VLAN settings are configured using the CM7 screens that follow.

Figure 36: CM7 VLAN settings

The required settings are:

- Operational mode should be set to VLAN
- The VLAN and alternate ethertypes should match the network
- The user must ensure that within a network a unique sender ID (SID) is configured in each encryptor, valid values for the SID are 1-511. Note that changing the Sender ID will stop all connections and they must be restarted manually.

Bypass VLAN Headers

When enabled (the default), VLAN headers are automatically bypassed and encryption begins after the VLAN tags. This is only for VLAN tags with the 0x8100 ethertype. A maximum VLAN stack depth of 2 is supported.

The ethertype policy for VLAN tagged frames depends on the policy switched over the VLAN, that is, it depends on the 'ultimate ethertype' following the tag.

When enabled, the connection with the peer encryptor learns the VLAN tag required to communicate with the peer encryptor. When disabled, the VLAN tags are encrypted and the default ethertype policy is the same as is set for (O)ther ethertypes.

VLAN Primary and Alternate Ethertypes

The VLAN primary ethertype is the value that will be parsed on the tags to identify tagged frames. It has a default value of 0x8100. However, if required, this may be changed to match the value used in the network. Some network vendors use a different value, for example 0x9100.

In the Q-in-Q case where the ethertypes may differ, there is an ability to specify an 'Alternate ethertype'. This may be enabled on a 'per connection' basis, specifying that the alternate be used on the 'inner tag' of frames that have 2 tags.

Refer to See "VLAN tagged frame" on page 113 and "Stacked VLAN frame" on page 113 for VLAN frame formats.



Q-in-Q Policy

Q-in-Q policy allows you to select the number of VLAN tags that will be used to define a unique connection. If the value is selected as '1 tag' then irrespective of the number of VLAN tags present, only the 'Outer tag' will be used. If '2 tags' is specified, then the number that exist (either 1 or 2) will be used.

VLAN Ethertype policy

The VLAN mode ethertype table provides control over processing based on the ethertype of the frame. The table shown in Figure 37 below by default specifies actions for common ethertypes.

Ethertypes that are not included in the ethertype table are processed according to the "Unlisted Ethertype Action" processing policy and this entry can be edited as required.

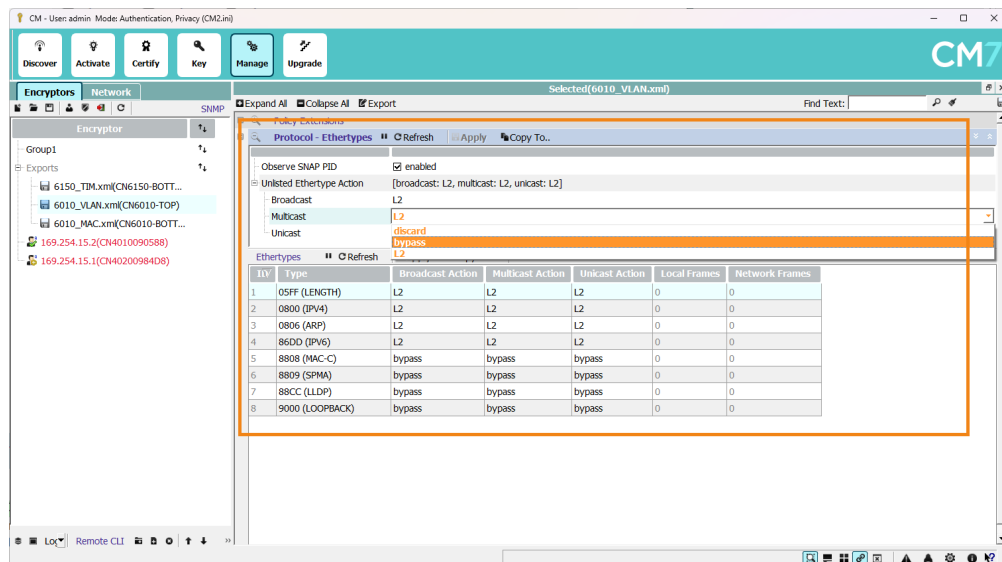


Figure 37: Default VLAN Ethertype values

An action can be specified for each Ethernet address class (unicast, multicast and broadcast). When the ethertype action is set to FollowCI, the connection identifier/tunnel action (as shown in the Tunnel/CI settings) is followed.

Additional ethertypes (up to a total of 15) can be added by clicking on the 'Add' button on the Policy tab, specifying each of the new column values as listed below, and then clicking the 'Apply' button. The policy for an existing ethertype can be changed by editing the displayed value and clicking 'Apply'.

Table 35. Ethertype attributes

Field Name	Content
ID	Sequential ID - system assigned index
Type	Hex value and Ethertype name
Broadcast Action	Discard, Bypass or FollowCI
Multicast Action	Discard, Bypass or FollowCI
Unicast Action	Discard, Bypass or FollowCI

The action can be set to 'Bypass', 'Discard' or 'FollowCI' for each of the Ethernet addressing modes - Unicast, Multicast and Broadcast. If the 'FollowCI' policy is selected then the 'Offset' and/or 'Mutation' settings will be applied.

The Add/Edit function either displays an additional line or highlights the selected ethertype so that policy can be entered or changed. The Apply or Discard selector is then used to save or discard the entry.

Ethertype mutation

Mutation allows the ethertype of the frame to be changed to a specified value when encrypting and reinstated to the original value when decrypting. See the ethertypes CLI command on page 1.

NOTE: Ethertype mutation or an Encryption offset may be required if intermediate equipment between a pair of encryptors makes decisions based on visibility of the payload that follows the Ethernet header. Examples of this are layer 2 services that require certain data to be present; although strictly speaking, this should not be the case in a true layer 2 network. Mutation (rather than Encryption offset) is the preferred method of addressing this type of problem as it does not leave any portion of the payload as plaintext.

Encryption offset (only L2 modes)

The ethertype configuration allows an optional encryption offset to be specified. The offset moves the encryption start point in the frame by the specified number of bytes, allowing a portion of the frame to be sent in the clear.



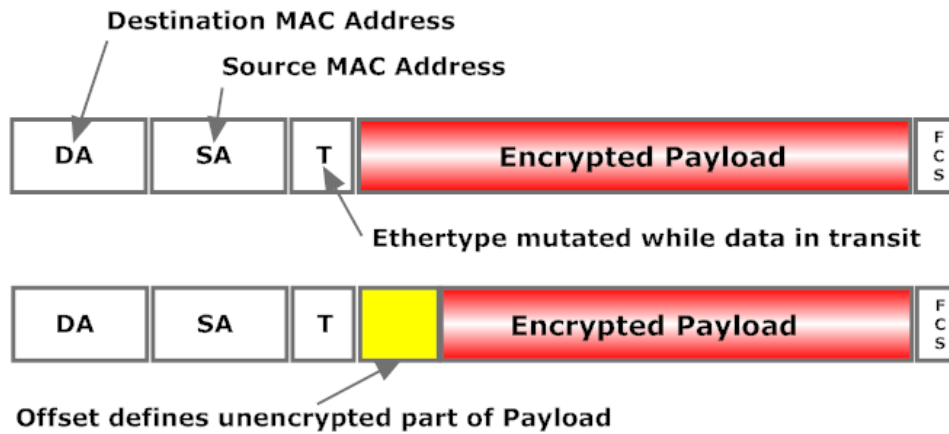


Figure 38: Point-to-point Mutated and Offset frames

NOTE: When passing VLAN traffic on a link configured in point-to-point (line) mode the VLAN identifier must be manually configured in the connection table. This can also be configured via the CLI `inband_vlan` command as described on page 1. This is not required in Multipoint mode as the ID is automatically learnt.

Bypass Reserved Multicast

In networks with switches or other configurable devices between encryptors it may be necessary to enable the bypassing of groups of MAC addresses that are used for this purpose. The following figure shows the CM7 screen used to do this.

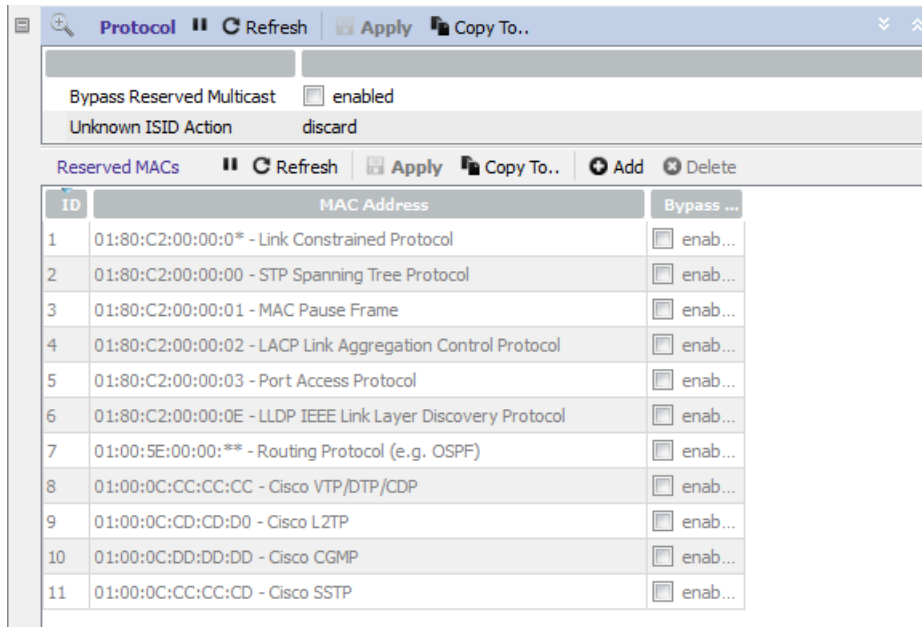


Figure 39: Bypass Reserved Multicast selection



Configuration using the CLI

Assuming that the encryptor is in VLAN mode then tagged or untagged connections can be added. Connections can be set to bypass, discard or secure.

The following commands add connections in each of these modes for untagged, single tagged and double tagged traffic using decimal VLAN IDs.

```
CN6140_A>tunnels -a -byp
CN6140_B>tunnels -a -dis 101
CN6140 (slot 0)>tunnels -a -sec 101 102
```

If the tags need to be specified in hex then the format is as follows. Note that the first four characters are the VLAN ethertype identifier and the last four are the VLAN tag in hex.

```
CN6140_B>tunnels -a -sec 8100F010
CN6140 (slot 0)>tunnels -a -sec 91000A03
```



Transport Independent Mode (TIM) (Layer 2, 3 and 4 encryption)

TIM should be employed when encrypting across non-Ethernet networks as it is ideal for securing data across diverse and complex network infrastructures, especially when it is desirable to encrypt concurrent traffic flows at different layers of the OSI network model, without modifying existing network setups.

TIM provides a great deal of versatility because it:

- works across any network transport infrastructures, such as IP, MPLS, and public Internet
- provides flexible and scalable encryption that adapts to different network layers and protocols
- utilizes group key encryption for efficient and secure communication, reducing operational complexity
- is highly scalable, even to hundreds of endpoints
- has no 'across the wire' key exchange, which eliminates the quantum attack surface

In TIM operations, an extensible 'key provider' model is used to define how the data encryption keys (DEKs) are generated. This model decouples key distribution from the underlying network and allows the selection of a generation method that meets the needs of the network topology.

NOTE: When in modes other than TIM, encryptors securely distribute keys between themselves across a Layer 2 network using certificate-based authentication.

Key Identifier (KID)

The KID is a unique network wide value that identifies a pool of keys to be used for encryption (by one and only one transmitting encryptor) and decryption (by all receiving encryptors). The conditions for its use are:

- valid when the operational mode is set to TIM
- A unique value must be set on each encryptor

The pool of keys is sourced from the key provider (**keyprovider -s**), which can be set to an internal FIPs approved key derivation function (KDF) or an external key management server via the KMIP protocol (e.g. Thales KeySecure).

If an encryptor detects a KID value equal to its own value, then an alarm is generated ALARM_DUPLICATE_KID_DETECTED to warn the user of this misconfiguration. The alarm MV_TRAP_DUPLICATE_KID_DETECTED is raised and cleared automatically, but not acknowledged. All packets containing that particular KID are then discarded.

If this occurs the user is then required to;

- switch to global discard
- manually change the KID value (which forces a reboot)
- acknowledge the alarm
- switch to global encrypt

Upon power up in TIM operational mode the encryptor sets the KID to a random value. This value can be manually set via the **policy -d** command however this will trigger an encryptor reboot sequence.

The KID range for the CN4000, CN6000 and CN9000 range platforms has a limited KID range of 1-256.

The KID range for the CN7000 and CV1000 platform can be set to an extended KID range of 1-131072 which can be enabled by the **policy -r** CLI command.

If interoperability with other platforms is required, all KIDs should remain in the default 1-256 range."



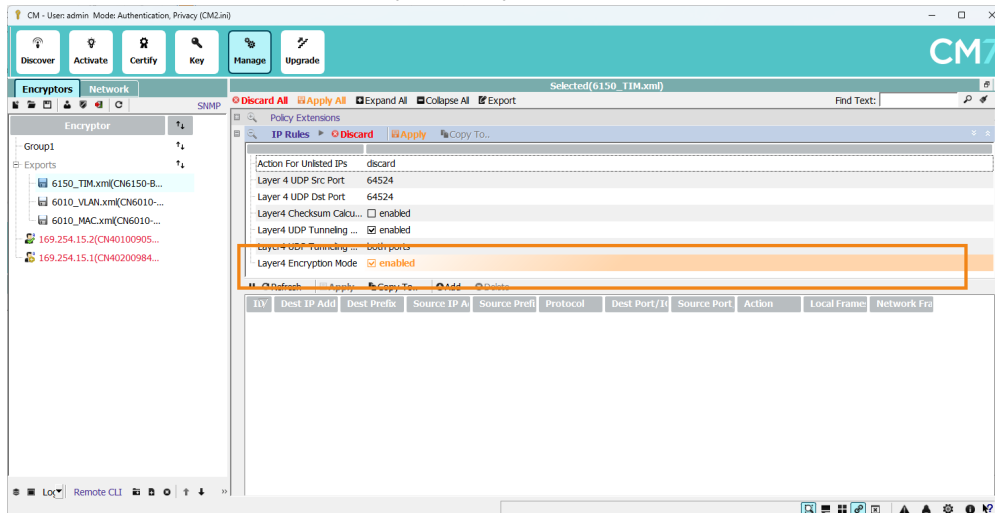
Layer 4 Encryption Mode

To enable encryption policies at Layer 4, it is necessary to firstly enable Layer 4 IPRules using either of the following methods:

- using the CLI command: ***iprules -l4 <-e|-d>***

or

- from the CM7 **IP Rules** pane: enable the 'Layer 4 Encryption Mode' checkbox



Once enabled, Layer 4 IPRules policies can be entered and Layer 4 auto-discovery enabled.

NOTE: It is recommended that Layer 4 IPRule policies all specify the same action, for example all encrypt or all bypass. It is not recommended to mix encryption and bypass actions.

Key Provider model

The 'key provider' model is an abstracted service interface whose purpose is to ensure that encryption keys are securely generated, synchronised and updated between encryptors independently of the underlying WAN.

The model is extensible and the functionality depends upon the version number. Available plugin key providers are:

- Key Derivation Function
- External KMIP key server

The Key Provider model can be configured using the CLI ***keyprovider*** command.

```
CN6140_A>keyprovider
Key Provider mode is : Key Derivation Function
CN6140_A>
```

Each key provider generates and manages keys in a different way, for example:

- Key Derivation Function - the next iteration of the KDF returns the key
- Key Server - issuing a GET command to an external Key Server returns the key



CAUTION: 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.

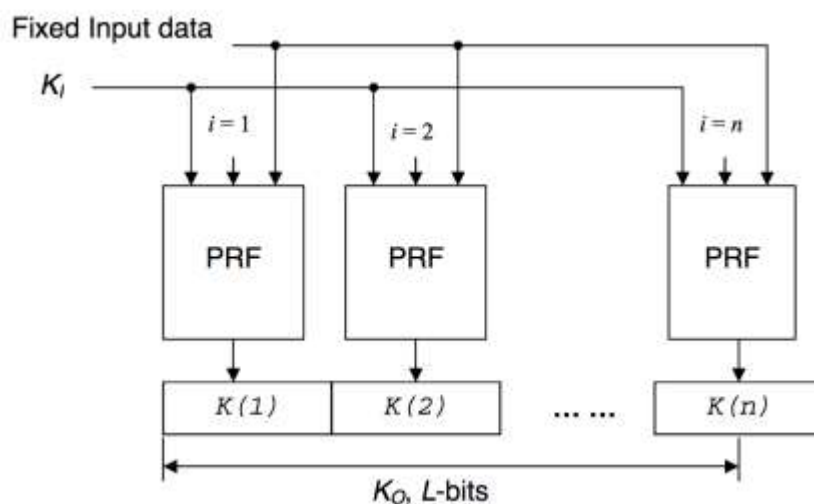
Key Derivation Function

A key derivation function (KDF) is a method of deriving multiple encryption keys from an initial secret key using a pseudo-random function.

When operating in TIM mode, the KDF option provides NIST approved encryption keys as specified in Special Publication 800-108:

<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-108.pdf>

The KDF operates in counter mode using a Keyed-Hash Message Authentication Code (HMAC):



The KDF takes as input a Key Derivation Key, an incrementing counter and fixed input data. The output from the KDF is called the derived keying material and it can be used directly as symmetric encryption keys.

A KDF is considered secure because:

- The output from any one iteration is indistinguishable from truly random data
- The KDF provides key separation meaning that the compromise of any one derived key does not degrade the security strength of any prior or future derived keys

The KDF provider serves as the default mode, implementing a FIPS approved key derivation function based on a manual or automatic key distribution model (MKD/AKD). There is no requirement for a centralised key server in this mode of operation.

The Key Derivation Key (KDK) must be derived from a Cryptographically Secure PRNG (for example the PRNG used in a CN series hardware appliance) and kept secret. The overall security of a KDF depends on the securely generating and sharing the KDK.

Each encryptor in a network must use the same KDK which can be generated on one encryptor and manually loaded into others via the CLI (using the **kdf** command) or over SNMP using, for example, CM7 KMIP Key server.

```
CN6140_A>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  
CN6140_A
```

Each iteration of the KDF produces a 256 bit output key that is used directly as a Data Encryption Key.

Incrementing counter: The encryptors use a counter input to the KDF that is equal to the number of hours that have elapsed since the Unix datum: 00:00:00 1 January 1970.

Encryptors must therefore be synchronised to a common time reference to ensure that they are using the same counter value (i.e. key) at all times.

It is recommended that the encryptors are configured to use a common NTP server to achieve this (see instructions on NTP configuration).

Fixed Input Data: The fixed input data to the KDF is required by the NIST standard and uses a unique per entity (encryptor) context string to ensure that each encryptor is generating unique encryption keys to encrypt their egress data.

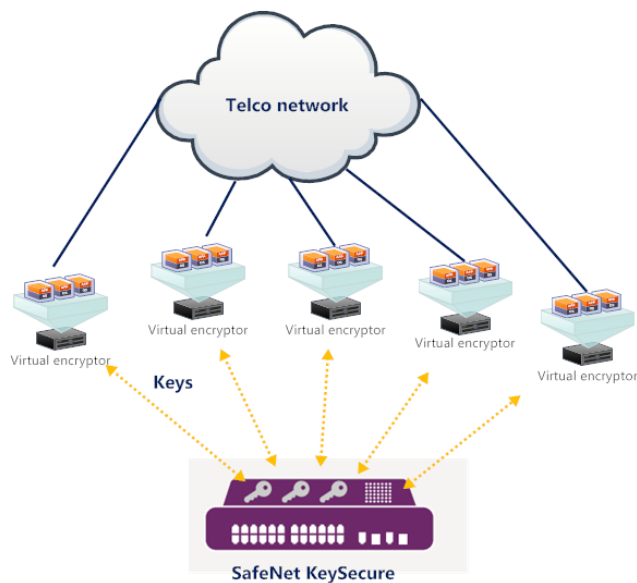
KMIP key servers

The Key Server provider option relies on an external 3rd party Key Management Service (KMS) as shown below.

A KMS is a service where encryption keys are created and managed for example SafeNet KeySecure: <https://safenet.Thales.com/data-encryption/enterprise-key-management/key-secure/>.

KeySecure is available as a FIPS certified hardware appliance with tamper protection or as a virtual machine.





Encryption keys are generated, stored and distributed from the centralised key server and therefore must be reachable by all encryptors in the network.

Key management messaging occurs **ONLY** between individual encryptors and the central key server.

NOTE: This model provides isolation of the control plane from the data plane and allows for transport independent encryption.

Key server mode relies on an authoritative time source to ensure key synchronisation between encryptors. Therefore as for the KDF provider, NTP support required in the network.

Encryptors communicate with the key server over an authenticated TLS session using the standards based Key Management Interoperability Protocol (KMIP) or a similar protocol (e.g. Thales's NAE). TLS v1.2 is required.

Data encryption keys are generated in the key server on request by each encryptor using KMIP commands.

- Generated keys are uniquely named using the requesting encryptors SID to identify them e.g. SID_DEK_0
- The keys are retained in the key server and can be read on demand at any time by any encryptor when required to decrypt traffic

Traffic encryption

In TIM mode data can be encrypted with confidentiality only (using CTR mode) or with confidentiality and authentication using, GCM mode.

All Data Encryption Keys (DEK) are AES-256 keys and encrypted frames are shimmed.

Each encryptor must be configured with a unique Sender ID which is sent in the encrypted frames and used to identify the originating encryptor.

- The encryptor SID is configurable via the CLI **snmp** command or via another configuration method if supported (e.g. cloud-init)

Egress Flow (Encryption Local -> Network port)

In TIM mode each encryptor has a single transmitter key and all secure traffic is encrypted using that key. The Data Encryption Key (DEK) is unique per encryptor and used to encrypt data in the egress direction, this key is called the egress DEK.

NOTE: Future implementations may support multiple egress DEKs per transmitter e.g. a separate DEK per VLAN or IP subnet for example.

Ingress Flow (Decryption Network -> Local port)

When an encryptor receives an encrypted frame it must identify the key required to decrypt it.

The receiver uses the SID and Key Bank in the encrypted frame's shim to identify the decryption key to use.

If the receiver doesn't yet have keys for the received SID it will request them from the key provider which will retrieve the keys using a provider specific mechanism (e.g. using KDF internally or requesting them from the external key server).

A receiver must store two keys plus a salt for every peer encryptor with which it communicates.

NOTE: The number of peers supported under TIM depends on the encryptor model.

WARNING: When operating under TIM, frames greater than 2048 bytes will not trigger auto-discovery.

TIM policy

The encryption policy used when operating in TIM mode has similarities to those applicable in VLAN mode, with the extensions required for layer 3 and 4 traffic.

In TIM mode the default is to bypass all traffic except IPv4 Unicast, with further lookups based on the IPv4/6 addresses and ports.

NOTE: If the combination of the L3 header and L4 header exceeds 128 bytes, then the frame is discarded.

Ethertype Table

Based on the topology of the network, review the ethertypes policy table and the 'bypass reserved multicast' setting. The default in TIM mode is to bypass all traffic except IPv4 unicast which is then further defined using the `lprules` table.

NB: When placed into TIM mode, the sender ID is randomly set and should be unique within the network. The sender ID is also used as the Key ID (KID) when running in TIM mode, and these terms may be used interchangeably.

lprules Table

The IP Rules table further defines IPv4/IPv6 policy lookups based on IP address, IP next protocol fields and TCP/UDP port numbers. These rules are established using the `lprules` CLI command.

The IP address search is based on a longest prefix match (LPM), and several sub-netted entries may be required to fully prescribe policy.

IP Rules encrypt datapath

The IP Rules command matches destination IP address and destination TCP/UDP port.

Actions encrypt L2, L3, L4 and L4 udp tunnelling instruct the policy where to insert the shim and directs the policy to follow the CI action.



- When the action equals **Bypass** the frame is bypassed irrespective of the CI Action.
- When the action is **Discard** the frame is discarded irrespective of the CI Action.
- If no IP Rule is matched then the default IP Rule action is followed (Discard/Bypass).

A maximum of 64 IP rules entries can exist on FPGA based (CN series) encryptors and up to 256 on DPDK based (CS/CV series) encryptors.

IP Rules decrypt datapath

The decryption is based on the shim location in the incoming packet. Once a shim is located in the packet then the packet is decrypted based on whether the packet is shimmed at Layer 2, 3 or 4.

If there is no shim in a packet:

- The IP Rules command tries to match both the source and destination IP addresses and TCP/UDP ports.
 - If no matching IP rule is found then the default IP rule action is followed (discard/bypass).
 - If the matching IP rule action is Discard or Bypass then that action applies to the unshimmed frame.
 - If the matching IP rule action is Encrypt (cl2, cl3 or cl4) then the unshimmed frame is discarded*.
- * The exception is TCP control frames (SYN, ACK, FIN, RST or a combination of these) with zero payload lengths which are bypassed if they match a rule to Encrypt at layer 4 (action = cl4)

To configure IP Rules use the ***iprules -a*** and ***iprules -d <idx>*** CLI command or the CM7 IP Rules pane in the 'Manage' screen.

NOTE: IPv6 addresses are not supported in IP rules.

Specifying IP rules

Wildcards (*) are only accepted for the protocol and port fields (not IP address and subnet mask). The source IP address/mask can have a wildcard value of 0.0.0.0/0 or contain a valid IPv4 address with a mask value between 1 - 32. The Source port number can have a wildcard value of '*' or a value between 1 - 65535. If no mask is specified via the CLI it defaults to 32. Up to 8 distinct source address/masks can be specified for each destination address/mask.

If the port number is specified then the protocol field must also be specified as UDP (17) or TCP (6), that is a wildcard cannot be used for the protocol field in this scenario. Effectively, the port number is only valid for TCP and UDP protocols. If they are specified for any other protocol, IP Rule addition will fail and an audit log will be generated.

```
AUDIT - IP rules configuration : Invalid Iprule specified
```

Layer 4 encryption (cl4) is only applicable for TCP and UDP. So if cl4 is specified in the IP Rule, and protocol is not TCP or UDP then the IP Rule addition will fail generating the same audit log entry.

Defining rules for unspecified addresses

Encrypt datapath: Define the default action if no rules are matched.

Decrypt datapath: Define the default action if no shim is present and no rules are matched.

The action specified by **-u** switch applies to all packets that don't match any of the rules specified in the IP Rules table. So in the encrypt direction, if the destination IP address in a packet doesn't match an IP Rule, then the default action is applied to the corresponding packet.

If the global mode action is **encrypt**, and the Ethertype action outcome is encrypt L3/L4 then the IP Rules feature comes into effect. If there is no match (for example, unlisted) in the IP rules table, then the action defined by this command is followed.

Valid settings are: {Discard, Bypass, Encrypt_L2, Encrypt_L3, Encrypt_L4, Encrypt L4 UDP tunnelling}



WARNING: Encrypt_L2, Encrypt_L3 and Encrypt_L4 require that the CI ACTION is set to secure.

NOTE: If the default action is set to Encrypt_L4 but the user traffic is not UDP or TCP, then the frame is encrypted at L3.

NOTE: If the default action is set to Encrypt_L3 but the user traffic is not IPv4 or IPv6, the frame will follow the Ethertype table action for that Ethertype (i.e. this action does not apply).

Clearing and/or Deleting rules

The **-c** CLI command clears all of the rules and the **-d <idx>** CLI command removes the rule at index position idx.

UDP Tunnelling

UDP (User Datagram Protocol) tunnelling is a TIM capability that allows any IP protocol to be tunnelled inside a UDP header as shown below:

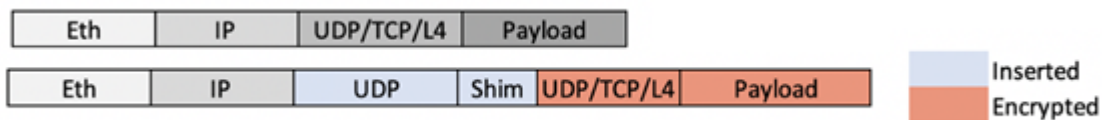


Figure 40: TIM UDP Tunnelling format

When enabled, the encryptor will:

- insert an additional 8-byte UDP header after the IP header
- insert a security tag (shim) after the UDP header
- encrypt the remainder of the packet
- set the IP protocol of the encrypted packet to UDP

Decryption will undo this and restore the original IP protocol type.

The default value for the UDP tunnel header's source and destination ports is 64527 and can be changed via user control. The original IP protocol field is encrypted and transported end to end.

UDP tunnelling is recommended:

- When TCP cannot be natively encrypted at layer 4 due to a firewall blocking or removing the TCP timestamp field that contains the Security Tag (shim) of the encryptor.
- To allow layer 4 protocols not based on UDP or TCP to be encrypted and transported inside a UDP header
- To allow operation in a NAT/PAT environment without exposing the inner layer 4 header information
- To allow operation in a NAT/PAT environment when multiple encryptors are located at a site – by using configurable ports
- To prevent port blocking (for example, by carriers or nation state firewalls) – by using configurable ports

UDP tunnelling mode must be enabled on the encryptor using the CM7 Manage pane or the CLI command:

iprules -ltu -e

UDP tunnels can be configured for specific policies using an 'LTU' action via the IP Rules table in CM7 or CLI.



iprules -a <ip address> [tcp|udp] [port] itu

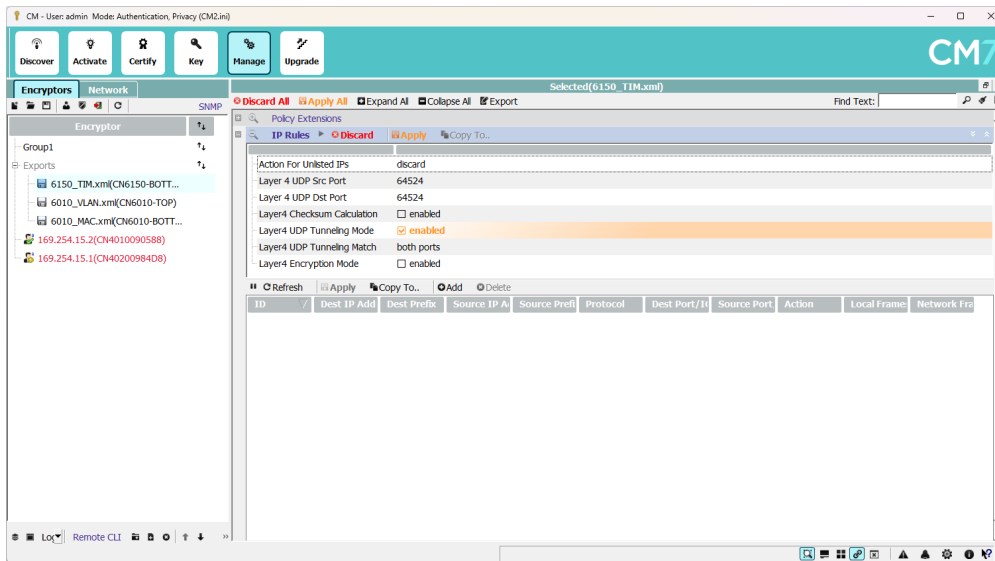


Figure 41: Enable UDP tunnelling

The tunnel source and destination ports can be changed via IP Rules using the CLI command:

iprules -h -s <src/dst> <port_number>

WARNING: Port number 0 (zero) is not an acceptable value.

or via CM7

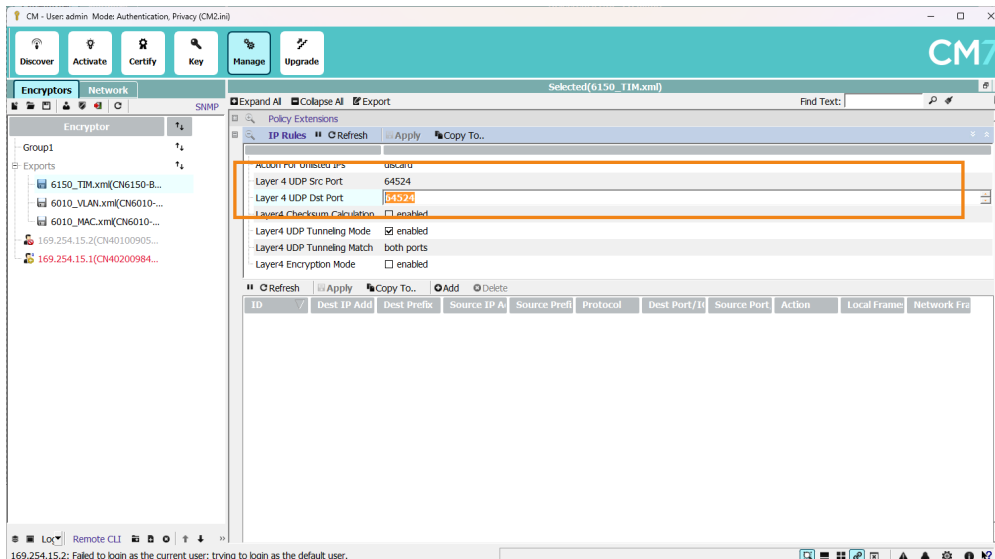


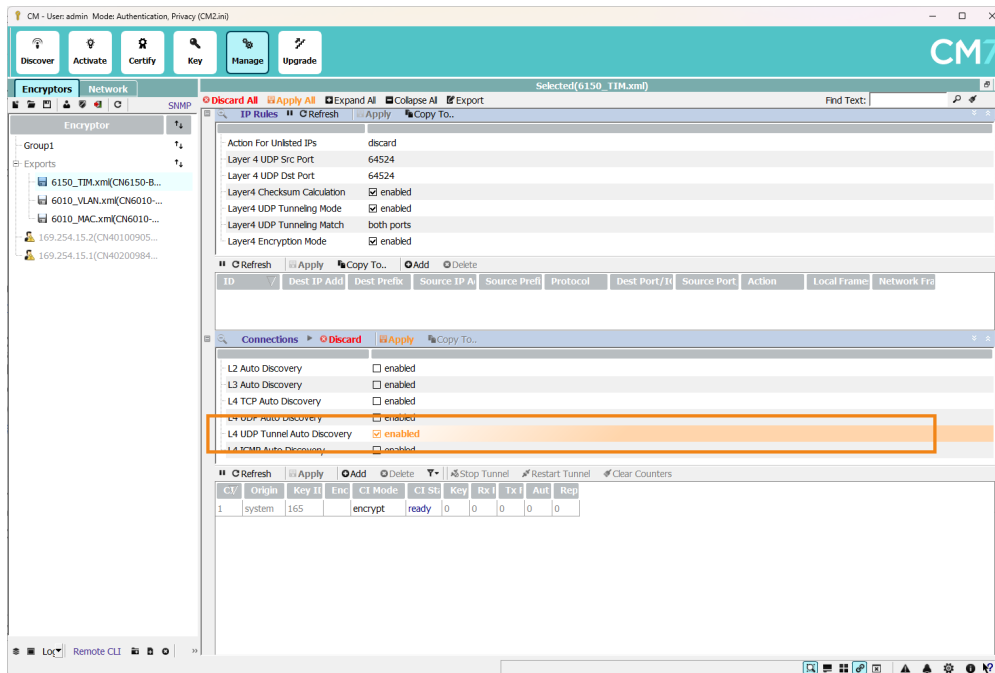
Figure 42: Select port for UDP tunnelling

NOTE: It is recommended that port numbers from the IANA dynamic/private range (49152 to 65535) are chosen to avoid collisions with well-known service ports.

When operating in TIM mode, the auto discovery of L4 UDP tunnels is enabled by using either:



- the CLI command **autodisco -e /d ltu**
- the CM7 Manage screen



WARNING: Frames greater than 2048 bytes in length will not trigger auto-discovery.

NOTE: The existing IP Rule action of 'CL4' should be used when, native L4 UDP or TCP encryption is required.

The following statistics are available to assist with L4 Tunnelling diagnostics:

- Local Rx and Network Rx:
 - IPv4 header checksum errors
 - UDP checksum errors
 - TCP checksum errors
- Network Tx and Rx:
 - L3 IPv4 Tunnelled Frames
 - L4 UDP Tunnelled Frames

Key synchronization

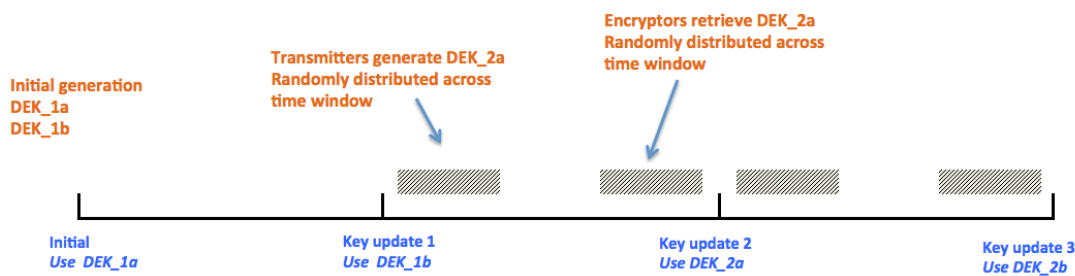
Key synchronization is the process that ensures that the same DEK is used by peer encryptions. Key synchronization is either time or counter based and is used with either a KDF or KMIP server as the key provider. The Key Synchronization method is selected using the **keyprovider -k** CLI command with counter as the default.



Time based key synchronization is where data encryption keys (DEK) are updated every half an hour automatically (the period is non-configurable) and synchronization is guaranteed through the use of a common time reference (NTP should therefore be enabled). Each DEK is assigned a number, keys are numbered with reference to the number of hours since the Linux datum and are shown in the connection table.

CI	Origin	Access	State	KID	Key#	RX Frames	Tx Frames	AuthErr	Replay
1001	System	Secure	Up	24814	421804	0	78	0	0
1002	Auto	Secure	Up	40430	421856	43	0	0	0

DEKs are updated every hour automatically (the period is non-configurable) and synchronisation is guaranteed through the use of a common time reference (NTP should therefore be enabled).



All keys are changed synchronously across the network on hour boundaries (since the datum). After a key update the transmitters generate a replacement DEK and this occurs in a fixed time window after the key update. To minimise load on external key servers (when used as the key provider) transmitters updates occur randomly across the allotted window.

In a similar manner all receivers must update their keys prior to the next key changeover time and this is also done randomly across the allotted window as shown above.

Encryptors always maintain two DEKs e.g. *SID_DEK_1a* and *SID_DEK_1b* to allow atomic roll-over of keys without traffic loss:

- One DEK will be the current DEK used to encrypt traffic
- The other will be the next DEK to be used when the current DEK expires
- The shim in each encrypted frame contains a Key Bank field which indicates the DEK to be used for that frame

Regardless of the key provider, the time since datum can be used to calculate the correct key and this provides a robust synchronisation mechanism that allows encryptors to leave, join or restart at any time during the key update period.

With counter based key synchronization key updates are synchronized based on the frame counter instead of time. The encryptor uses a key number for deriving it's DEK until the frame counter is exhausted at which point the key number is incremented.

WARNING: When both the key number and frame counter are exhausted the device will begin to discard traffic until a new KDF is installed.

Modifying the key synchronization setting from time to counter (or vice versa) clears all existing IP rules settings on the unit. Modifying the Key Sync Mode to time and then back to counter will re-initialise the key numbers back to 1 even if the same KDK is used.

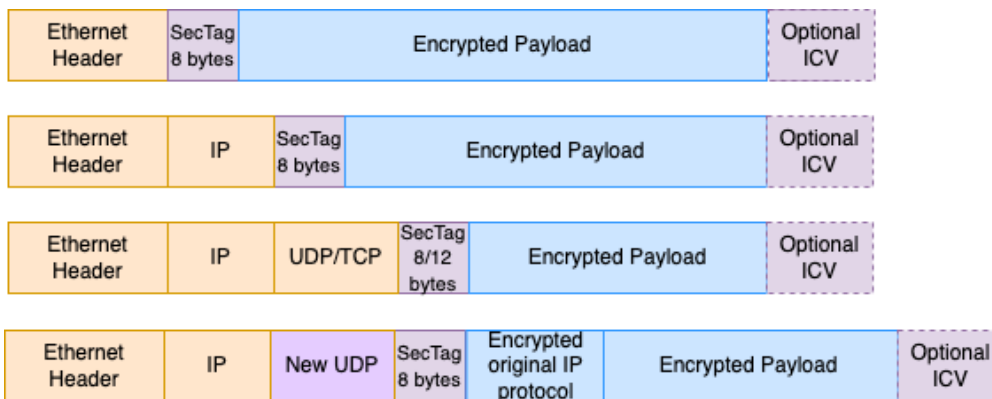


The auto populate feature is not supported when using counter based key synchronization and is disabled when counter is enabled.

Note that if the device is rebooted after ingress tunnels are discovered, then following start-up the egress tunnel key number will be 2 more than prior to reboot. However ingress tunnels will have their key numbers initialised to 0 and traffic discarded until the tunnel is re-learnt.

Encrypted Frame formats

The encryption policy determines where in the frame the shim is located and which portion of the frame is encrypted, i.e. at layer 2, 3 or 4 as shown below. IP Rules are used to establish L3/L4 encryption and L4 encryption can be configured as either IP+port or UDP tunnelled.



NOTE: For TCP frames, the SHIM is inserted as a TCP Timestamp option. UDP frames have shim inserted immediately following the L4 header.

NOTE: MTU adjustments should be made on LOCAL port connections to the devices to ensure the encryption SHIM (typically 8 bytes, or 12 for TCP) are catered for and maximum MTU is not exceeded within the network. For CN series encryptors with default GCM mode enabled the maximum MTU is 10,000-28 (12 byte shim + 16 byte auth tag).

Configuration using the CLI

The following steps are required to configure an encryptor for operation in TIM mode. Encryptors operating in TIM mode do not require certificates to establish trust as this functionality is provided by the key provider mechanism.

NOTE: Other certificates may be used for management related functions, including FTPS, KMIP, and HTTPS. A minimum of TLS v1.2 is required.

Activation

Activate the device using either local CLI activation, or remote activation using the CM7 management tool.

NTP setup

The optimal TIM mode of encryption relies on network time synchronisation across all encryption devices. Ensure at least one NTP server is configured on each encryption platform, and confirm current status.

Auto population



Auto-population is a facility that can be used to automatically create tunnels. It is an alternative to the auto-discovery or manual tunnel creation methods and must only be enabled (transitioned from disabled to enabled) when auto-discovery is disabled.

When the auto population is enabled the encryptor will delete any existing tunnels and IP Rules, reboot, and on start-up automatically populate (create) all tunnels by retrieving the keys from the designated key provider mechanism. Note if a key provider is set to Key Server (KMIP) the tunnel creation time may be sub-optimal depending on the key server availability. Note that for the CN series the range is 1-256.

The encryptor is not effected by disabling auto population..

To remove the auto-populated tunnels the **tunnels -d** command can be used.

The CLI commands to enable/disable the auto-populate option are:

```
CN6140_A>autopop -e
```

and

```
CN6140_A>autopop -d
```

The command will reboot the encryptor.

Connection mode

Use the CLI **con** command to set the mode to TIM.

```
CN6140_A>con -T
```

```
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)
```

As indicated this command will reboot the encryptor.

Policy

Following the above steps the encryptor can be placed directly into global mode "encrypt", however you should check that auto-discovery is enabled.

```
CN6140_A>autodisco -e
```

```
Automatic Unicast discovery is enabled  
Automatic Multicast/VLAN discovery enabled
```

```
CN6140_A>global -e
```

```
Global mode set to encrypt
```

```
CN6140_A>
```

WARNING: When operating under TIM, frames greater than 2048 bytes will not trigger auto-discovery.



Ethernet Protocol(only layer 2)

The Ethernet encryptor has a flexible policy that allows it to operate over transparent layer 2 Ethernet services. The encryptor is transparent to those services that fit within the definition of transparent Ethernet. However, the network to be encrypted must meet the following criteria:

- When the connection policy is multipoint MAC, the MAC address **MUST** be preserved and the network between the encryptors cannot change the Ethernet header.
- When the connection policy is 'Point-to-point' (Line) or 'MAC based' the transmission order of frames **MUST** be preserved. This means that Quality of Service (QoS) must occur outside the encryptors and not between encryptors where it could reorder frames. This does not apply when the policy is based on the VLAN ID.
- The layer 3 data is encrypted and therefore network devices cannot make any decisions based on it. Any attempt to do so may impact network reliability and/or performance.

In practical terms it is not always possible to ensure that the network meets these requirements. Senetas encryptors, however, are designed to address many of the issues that are presented by a network's layer 2 and layer 3 devices.

Ethernet encryption

The acceptance of Ethernet as the basis of most communications networks also means that Ethernet is the most frequently encrypted protocol.

Senetas Ethernet encryptors can be configured to handle all of the protocol variants that exist.

MAC connection mode - Unicast operation

Unicast traffic is encrypted using a key pair for each of the established connections.

When operating in Point-point (line) mode there is just one entry in the connection table. When operating in multipoint mode, there can be many table entries, these being added manually, or if 'Auto discovery' is enabled, automatically added based on the observed traffic. Once added, entries do not age and will remain in the table.

Multicast operation

The encryption of multicast/broadcast Ethernet traffic in firmware versions 2.0.0 and earlier is only provided for units configured in Point-to-point (line) mode. Version 2.1.0 onward also provides encryption for multicast traffic in multipoint (meshed) networks; however, to ensure backwards compatibility this is turned off by default.

Multicast traffic between encryptors connected in Point-to-point mode shares the same single key pair that is used by unicast traffic. The remainder of this section only applies to multicast traffic being encrypted by units that are configured in multipoint mode.

Multicast encryption is used to encrypt traffic sent from a host to all members of a multicast group. Unlike unicast encryption (which encrypts traffic from a single sender to a single receiver and uses a unique pair of keys per encrypted connection), multicast encryption within a multipoint network requires a group key management infrastructure to ensure that each encryptor can share a set of encryption keys per multicast MAC address.

The Senetas group key management scheme which is used for multicast, VLAN based encryption is responsible for ensuring group keys are maintained across the visible network. The scheme is designed to be secure, dynamic and robust, with an ability to survive network outages and topology changes automatically. It does not rely on an external key server to distribute group keys, which could introduce a single point of failure and compromise.



For robustness and security a group key master is automatically elected amongst the visible encryptors within a mesh based on the actual traffic. The 'Bypass Reserved Multicast' flag may need to be enabled so that this traffic is allowed.

When in MAC mode using a selected key master from within the group allows:

- Automatic discovery of multicast encryption groups
- Automatic ageing/deletion of inactive groups
- Secure distribution and updates of keys to all members of multicast groups
- New members to securely join or leave the group at any time
- Fault tolerance to network outages and topology changes
- Automatic detection of dead peers

If communications problems segment the network, the group key management scheme will automatically maintain/establish new group key managers within each segment. Subsequent reconnection of these segments will instigate a transparent re-electing of a single group key manager.

Broadcast operation

The encryption of broadcast traffic must be manually configured.

Performance

The CN Series uses a 'cut-through' encryption architecture requiring only partial receipt of the frame before encryption and re-transmission can begin. This architecture has the benefit of consistently low latency, in the order of 7 uS at 1Gbps

In Cipher Feedback Mode (CFB) encrypted frames are the same size as plaintext frames and no packet expansion is performed.

In Counter mode (CTR) it is necessary to periodically insert an 8-byte shim into frames to ensure counter values are synchronised at both ends. In MAC mode the shim insertion period is configurable.

An encryptor will also generate a very small amount of traffic between it and its peer that is used for key updates and management purposes. This traffic is sent using the Senetas registered ethertype (0xFC0F) to distinguish it from other network frames.

Latency and Jitter

Latency within an encryptor refers to time between when a data frame arrives on an ingress or egress port to when it leaves on the corresponding egress or ingress port.

Jitter refers to the variation in latency due to processing overheads within the encryptor.

NOTE: Encryptor latency is specified on a 'per unit' basis and depends on both the data transmission speed and encryptor processing.

Control plane ethertype

By default all encryptor management traffic uses the reserved 0xFC0F ethertype. Since the ethertype of the encryptor will be ignored on the local port it is not possible to 'nest' encryptors without changing the ethertype of the unit so that it does not conflict with those being used by outer units.



If encryptor nesting is required then the management ethertype of the outer pair needs to be set to a unique value using the -s hhhh command, where hhhh is a hex value. The encryptors must be restarted before the new value will take effect. A suggested value for hhhh is 0xFC0E.

Ethernet frame formats

There are a number of frame formats used in Ethernet communication and each of these is supported by Senetas encryption. These are described in the subsections that follow, after which the formats used for VLANs and MPLS networks are discussed.

Ethernet II (DIX)

The original and most commonly used frame format is Ethernet (version II), also known as DIX (Digital, Intel and Xerox). Many higher level protocols such as TCP/IP and IPX use Ethernet II encapsulation.

The frame is formatted and encrypted as shown in Figure 43 below:

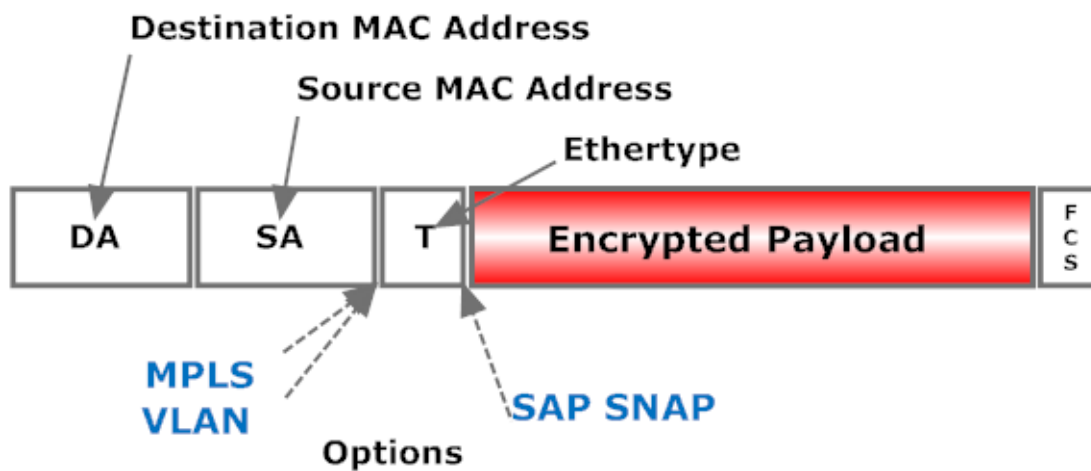


Figure 43: Ethernet II format

DA is the destination MAC address

SA is the source MAC address

T is the Ethertype

Payload is the data to be secured

FCS is the computed Frame checksum

IEEE 802.3 SAP (with 802.2 LLC header)

In an IEEE 802.3 SAP (Service Access Point) frame, the “ethertype” field is replaced by a “length” field which is then followed by an LLC (Logical Link Control) header which carries information about the type of protocol contained in the packet. The length field range of 0x0000-0x05DC indicates the number of valid bytes in the payload. This frame format is most commonly used for control plane traffic.

The 802.3 SAP frame is formatted and encrypted as shown in Figure 44 on the next page:

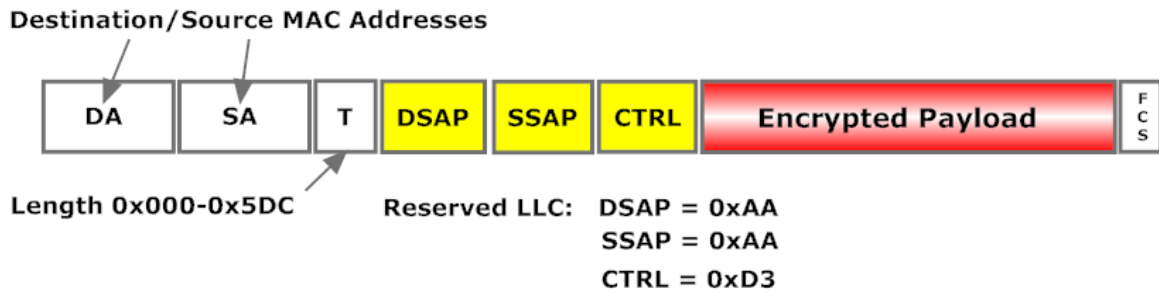


Figure 44: IEEE 802.3 SAP format

IEEE 802.3 SAP SNAP

The IEEE 802.3 LLC SNAP format extends the protocols than can be supported by the IEEE 802.3 SAP format by the addition of an OID and Protocol ID field.

The SNAP OUI is an organisationally unique identifier. This allows different vendors to implement their own Ethernet protocol set. A special reserved OUI value of all zeros 0x000000 indicates that the SNAP Protocol ID (PID) is equivalent to the Ethernet Ethertype Type field values. Refer to RFC1024 for more details.

This format is also used for control plane traffic. The 802.3 SAP SNAP frame is formatted and encrypted as shown in Figure 45 below:

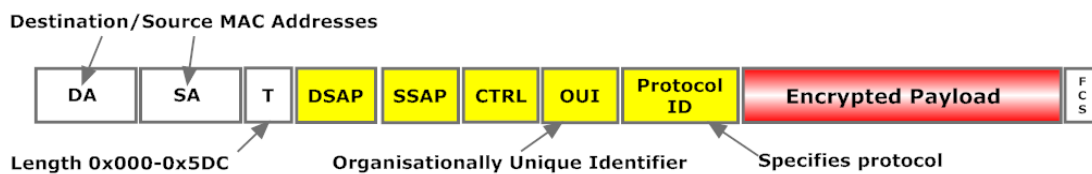


Figure 45: IEEE 802.3 SAP SNAP format

VLAN

A VLAN frame extension or tag can be inserted between the Source Address and the type/length field in any of the Ethernet frame types. The purpose of the tag is to identify the VLAN the frame originates from. The encryptor is transparent to VLAN tags provided the ethertype is 0x8100. The VLAN tag consists of the following fields:

- User Priority
- Canonical Form Indicator (CFI)
- VLAN Identifier.

WARNING: Do not confuse VLAN tags with the VLAN mode of encryption. The former contain the values that differentiate traffic; the latter is a mode of operation that uses the VLAN tag value(s) to determine the encryption policy that will be applied to the frame.

The VLAN tagged frame is formatted and encrypted as shown in Figure 46 on the facing page

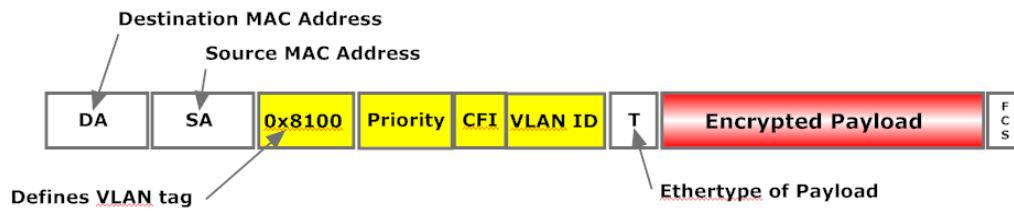


Figure 46: VLAN tagged frame

VLAN ethertypes

A value of 0x8100 is generally used to flag the presence of VLAN tags. However it is not a standard and other vendors may use a different value, for example, 0x9100.

Stacked VLAN

Two VLAN tags can be inserted in an Ethernet frame. This is referred to as VLAN tag stacking. In an Ethernet-based DSL aggregation network, service providers can use two VLAN tags to allow for a larger number of customers to be aggregated. This is known as Q-in-Q, VLAN-in-VLAN, or double-tagging. The stacked VLAN tagged frame is formatted and encrypted as shown in Figure 47 below

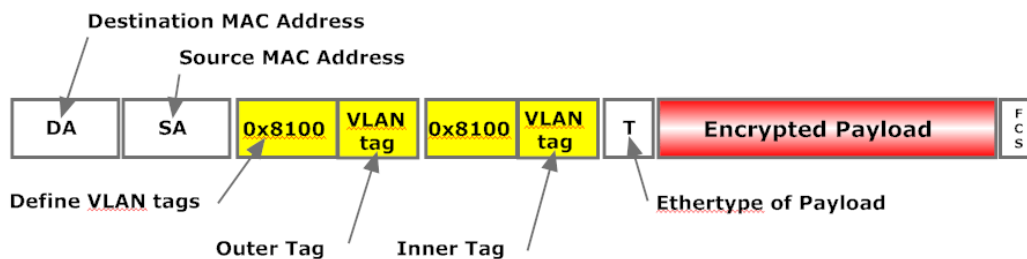


Figure 47: Stacked VLAN frame

The inner VLAN tag is known as the customer or customer equipment VLAN, C-VLAN, CE-VLAN, or C-TAG. The outer VLAN tag is known as the service or service provider VLAN, S-VLAN, SP-VLAN, PE-VLAN, or S-TAG.

The encryptor is also transparent to stacked VLAN tags but only when the outer tag has an etherType of 0x8100.

MPLS shims

Shims/labels are added to an IP packet to route it through a network. The encryptor is transparent to MPLS shims. The maximum MPLS stack depth is 5.

MPLS frames are formatted and encrypted as shown in Figure 48 on the next page:

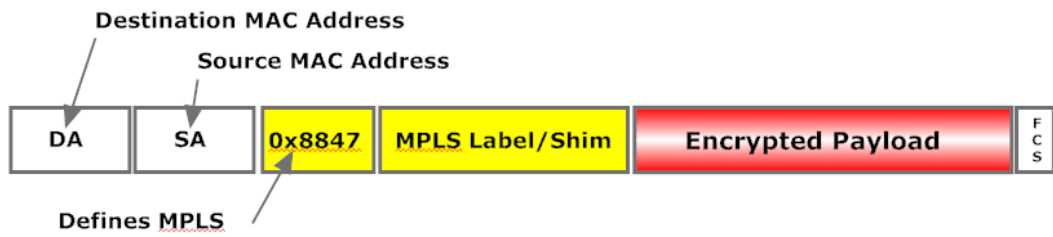


Figure 48: MPLS tagged frame

MPLS labels

Senetas encryptors allow up to 5 MPLS labels.

Pause Frames

Ethernet pause frames are a type of special control frame used to regulate the flow of data within an Ethernet network.

The inability to handle the incoming data rate, leads to packet loss, buffer overflow, or degraded performance. In such cases, the receiving device can send pause frames to the transmitting device, requesting it to temporarily halt the transmission of data.

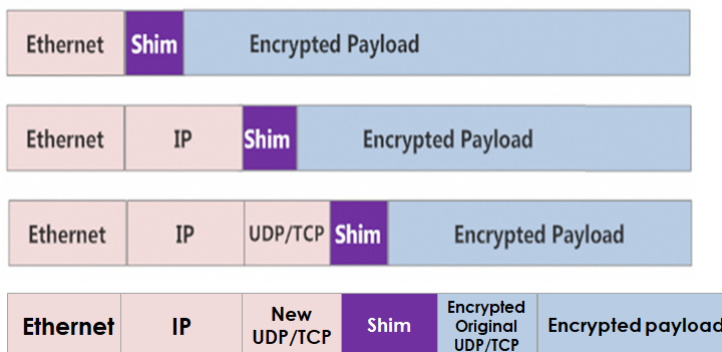
There are two types of pause frames:

- pause frames
- priority-based pause frames.

Pause frames are generally used for conventional Ethernet traffic, while **priority-based pause frames** are employed in networks that support quality of service (QoS) mechanisms.

TIM frame formats

Encryptors operating in Transport Independent Mode (TIM) allow simultaneous encryption at layers 2, 3, and 4. The following diagram shows the shim insertion position for 'Layer 2 Ethernet', 'Layer 3 IPv4/IPv6', 'Layer 4 (IP + port)', and 'Layer 4 UDP tunnelling'.



Layer 4 (IP + Port) encryption supports NAT pass-through, Netflow/Jflow, and Policy based routing.



Section 3: Encryptor management overview

Management connections are used to configure an encryptor and to facilitate the ongoing monitoring of its performance. There are two connection methods for device management:

- a serial port that allows connection via a Command Line Interface (CLI) and a character based approach to control and configuration
- a graphical user interface using the Simple Network Management Protocol version 3 (SNMPv3) via a RJ45 Ethernet port.

Virtual management

When operating in TIM mode, encryptors can also be managed via their Local or Network port using virtual management. When virtual management is enabled, front panel management is disabled and vice versa.

Senetas provides PC-based management systems for the CN series of encryptors that address the needs of a wide range of users. This document describes the methods used to connect to encryptors, thus providing you with the information required to select a solution that best meets your needs.

The management and control methods are summarised in the sections that follow.

Encryptor management

Ethernet encryptors can be managed either:

- via the front panel using SNMPv3
- via the serial port

The management systems supported are as follows:

CM7 network manager

The CM7 network management package can be used with all Ethernet encryptors. Encryptors operating in TIM mode (but not the CN6040 or multi-port CN6140) take the IP address from the management port. The address can be reached at both the local and network ports simultaneously. It is not possible to only allow access via just one port.

When Virtual management is enabled, management via the front panel is disabled.

Command Line Interface

The command line interface provides a means of configuring and monitoring units via a serial link and terminal emulation package.

Details of the required physical connection and its configuration are provided in the installation manual for the encryptor.

The available CLI commands are described in detail in the Command Line Interface section beginning on page 225.

NOTE: To use the CLI the management system must install a terminal emulator such as Hyperterm, TeraTerm or PUTTY.

Third-party managers

Encryptors are managed via SNMPv3 and therefore third-party managers that use this protocol can be configured to manage and monitor units. Senetas provides the required MIBs to support these modes of operation and can assist with implementation.



Monitoring via SNMP:

SNMPv3 is required to manage encryptors; however, SNMPv1 can be used to monitor their status.

SNMPv1 access can be granted to Individual user accounts to facilitate this.

Defining user accounts

Additional user accounts are added via the User menu of the selected encryptor as shown in Figure 49 below. The details of each user can be changed as required and then applied back to the unit.

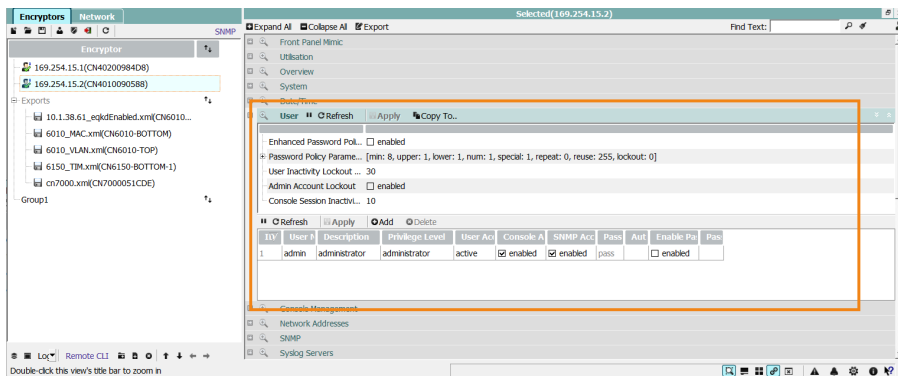


Figure 49: User Management

There must always be at least one administrator account present on the encryptor; the system will not allow you to delete the last account. If you erase the encryptor then the default administrator account will be re-established with the admin/\$Password1 credentials.

All authorised users are assumed to be competent and trusted not to abuse their privileges so as to undermine the security

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

A user account is defined by an access level, a unique User Name and Authentication Password and an optional Full Name that can be used to identify the person or a functional role.

Users can have their Privilege level defined and access via the console (CLI) or SNMP management port can be enabled or disabled.

User accounts can be disabled if they are not required for day-to-day operations. This facility is often used where an external party should only be granted access when their assistance is required.

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

NOTE:

If FIPS mode is enabled (See "FIPS PUB 140" on page 121) then the encryptor enforces both authentication AND privacy. The encryption keys for privacy mode are derived between the encryptor and the SNMP manager using the Diffie-Hellman key agreement protocol.

By default, user passwords are subject to lexical diversity requirements as follows:

- At least one upper-case alphabetic character
- At least one lower-case alphabetic character



- At least one digit
- At least one punctuation character

Within each of these groups there are no restrictions on the character set that can be used.

This requirement can be disabled from the Management Access tab (see on the previous page).

When enhanced mode is turned off (the default) and lexical checking is enabled, testing using the default rules is only performed when accounts are created. Enhanced mode, which is enabled using either the Management Access tab or the CLI **password** command, enforces diversity checking whenever a user logs on and allows these checks to be strengthened. Enhanced mode allows configuration to support AR-25-2.

Authentication / privacy

Authentication requires that each of the messages between CM7 and an encryptor be authenticated.

Privacy requires that the traffic between CM7 and an encryptor be encrypted.

NOTE: Care is required when using later versions of CM6 with earlier versions of firmware as not all of the features are available.

Administrator access

The User Access options described in Table 36 below can be used to configure the manner in which users interact with an encryptor.

The Serial port, the CN Series keypad and the CN/CS Series USB ports can be individually disabled to prevent unauthorized access to the unit.

Password lexical checking can be disabled or extended by setting both the minimum length and optional AR-25 requirements.

Table 36. User access

Feature	Description
Enable Serial Console Port	Specifies whether access is available via the serial craft port
Enable Front Panel Keypad (CN series only)	Enable/disable the keypad to control access
Enable Front Panel USB	Enable/disable firmware upgrades via the USB port
Enable Password Lexical Check	Enable/disable the lexical checking of user passwords. Note that units that are Common Criteria certified do not allow lexical checking to be turned off
Password Reuse Count	Specifies the number of unique passwords that must be entered before a password can be reused for an account
User Inactivity Lockout	Specifies the number of days before an inactive (no logins in this period) account is disabled
Session Inactivity Logout	Specifies the period of inactivity on the console after which the user is logged out
Enable Enhanced Password Policy	Enable/disable the enforcement of enhanced lexical checking. Enhanced checking allows conformance to the AR-25 standard.



Feature	Description
Minimum Password Length	Enforce length of 15-29 characters
Minimum Number of Uppercase Characters	Set minimum to 1 or 2 characters
Minimum Number of Lowercase Characters	Set minimum to 1 or 2 characters
Minimum Number of Numeric Characters	Set minimum to 1 or 2 numerics
Minimum Number of Special Characters	Set minimum to 1 or 2 characters

User Inactivity Lockout

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

The User Inactivity Lockout feature enables admin accounts to block any account from logging in after a specified period of time has elapsed since their previous interaction with the Encryptor. By default, this is set to 30 days. Setting this value to zero disables this check.

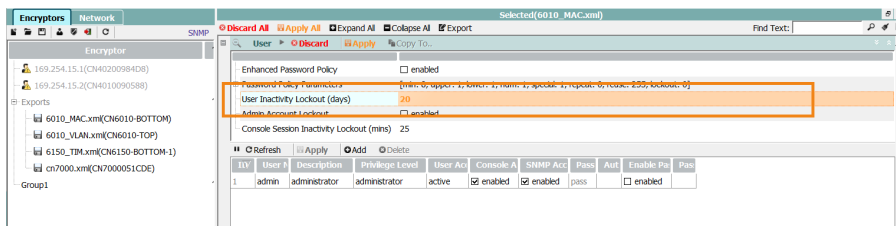


Figure 50: Set user inactivity period via CM7

When used, if the time period elapses, the affected user account is blocked. If this occurs, the account must be set to active again by an administrator account via CM7. This does not require a change of password.

The user inactivity period can also be configured via the CLI command: **users -u <days>**

The inactivity period can be set between 0 to 1825 days. A value of 0 means it is disabled and a user will never be locked out due to inactivity.

NOTE: To enable this lockout feature, the Enhanced Password Policy must also be activated.

This setting applies to operator, upgrader and supervisor user accounts on CLI and CM7/SNMP, Depending on the 'Administrator Lockout' setting, inactivity lockout can also apply to administrator user accounts on CLI and CM7/SNMP

If user inactivity period is non-zero and the period has elapsed with no activity for a user:

- Operator, upgrader and supervisor user accounts are locked out from CLI and remote management systems such as CM7 and SNMP



- If 'admin lockout' is disabled, administrator accounts are not affected and cannot be locked out due to inactivity
 - If 'admin lockout' is enabled, administrator accounts are locked out from CLI and CM7/SNMP, irrespective of the device's activated state
- An Event log entry is created for user accounts that have become inactive

Administrator Lockout

The lockout administrator control, named 'Admin Account Lockout' was added at the CLI and CM7 (SNMP) interfaces and enables or disables whether administrator accounts can be locked out:

- due to inactivity via CLI and SNMP/CM7; and/or
- due to password expiry via SNMP/CM7; and
- if admin password has expired, no ability to update the password at the CLI prompt

'Admin Account Lockout' behaves as follows:

- It requires Administrator privileges to enable or disable it (activated state)
- Can be enabled or disabled while device is inactivated by the default administrator account
- When enabled, applies to the default administrator (inactivated state) or all administrator users (activated state)
- It is disabled by default
- It is persistent across power cycles, reboots and initcfg (all options)
- All erase triggers (e.g. factory erase, erase and tamper) will clear the control to the default disabled state during normal operation
- If all administrator users are locked out (either due to password expiry or inactivity) but one or more other privilege level users are still active at either interface, the device may still be managed (in a limited capacity) but administrator privilege level management access to the device, will have been lost
- If all users are locked out of all interfaces (either due to password expiry or inactivity), management access to the device will have been completely lost
- Only an emergency erase* or tamper clears the 'admin lockout' control to the default disabled state if the device cannot be managed as a result of all users being locked out or to regain administrator privilege level management access to the device

Enabling the 'Admin Lockout' control on either the CLI or CM7 provides a clear warning to the user:

CAUTION: Enabling this control could require an Emergency erase of the encryptor if all administrator accounts become locked!

This control should be used with extreme caution - if all administrator accounts are locked out (activated state) or the default administrator account is locked out (inactivated state) due to inactivity or password expiry, then the encryptor will require an emergency erase or tamper to regain administrator privilege level management access. With the exception of virtual encryptors, this will require physical access to the device.

NOTE: The emergency erase mechanism can only be performed on encryptors with front panel keypads via holding down the 'ESC' and 'ENT' buttons simultaneously for 10 seconds.

As a summary, in order to regain management access after a full lockout or to regain administrator level privilege management, the user will need to:



To regain management access to encryptors with front panel keypads:

- Perform an emergency erase; or
- Tamper device (pin hole or lid removal)

To regain management access to encryptors without front panel keypads:

- Tamper device (pin hole or lid removal)

To regain management access to Virtual Encryptors:

- Spin Eth0 MAC address

NOTE: Performing an emergency erase (via front panel keypad) is identical to issuing 'erase' at the CLI; it shall return the device to defaults but keep IP settings.

Tampering the device is similar to erasing the device with the addition of also deleting the SMK.

SNMPv1 monitoring

SNMPv1 monitoring can be enabled or disabled. SNMPv1 uses a 'Community String' to authorise connection and this string can be configured either via CM7 or the CLI **community** command as shown on page .

If SNMPv1 access is to be used then to maximise security the Community string should be changed from Public to another value.

Table 37. Remote management

Feature	Description
Enable SNMPv1 (Monitor only)	Enable/disable SNMPv1 monitoring (requires restart)
Community String	Specifies the community string of the encryptor (requires reboot)

NOTE: For the setting to take affect, some versions of the firmware require a restart after SNMPv1 is enabled or disabled.

Inband management is available for the Ethernet encryptors.

The inband management gateway is initially disabled to prevent access to the units via the network. The gateway must be enabled to discover and use the configured inband addresses.

The encryptor that is to be used as the gateway for the inband management of remote units must have its 'Management Gateway' enabled so that it can communicate with remote units over the encrypted network.

Table 38. SNMP inband management

Feature	Description
Enable Inband Management	Show Enable/disable status of Inband SNMP Management
Enable Management Gateway	Enable/disable Inband Management Gateway

FIPS 140-3 mode is enabled by default; however, it can be disabled. Switching modes will force a restart of the encryptor and the running of any applicable startup diagnostic processes. FIPS mode enables privacy and enforces authentication using a Diffie-Hellman key exchange.



Table 39. FIPS PUB 140

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



User account management

Encryptor management is based on a user role model. User accounts can be created at one of four predefined privilege levels:

Table 40. User credentials

User level	Privileges granted
Administrator	Unlimited ability to configure and manage an encryptor Can initiate firmware upgrades via SNMP, CLI or Keypad
Supervisor	Ability to configure with the following exceptions: <ul style="list-style-type: none"> • Cannot load certificates • Cannot create/edit user accounts • Cannot clear audit or event logs • Cannot initiate firmware upgrades
Operator	Monitoring only Cannot make configuration changes Cannot initiate firmware updates
Upgrader/Maintainer	Can initiate firmware upgrades remotely via SNMP (not CLI) Cannot make any other configuration changes

User accounts are stored in each encryptor. They are not kept in a central repository or in the CM7 database. As described in the following section, up to 30 separate user accounts can be created.

To manage an encryptor you must have an account registered on the device. Each account has an **id** and **password** that must be entered into the CLI or CM7 to gain access to the encryptor.

An un-configured (or erased) encryptor contains a default administrator account that allows the unit to be configured. This account has the following credentials:

```
Name: admin
Password: $Password1
```

To guard against unauthorised access this account should be replaced with a new administrator account note however that this is done as part of the 'activation' process.

NOTE: A warning dialogue is displayed if the credentials of the new account are entered as admin/\$Password1 as this presents a real security risk.

RESTful JSON interface

A RESTful HTTP(s) interface is provided for the purposes of remote monitoring and issue detection.

The RESTful interface leverages the existing SNMP MIB interface, providing the ability to walk the SNMP MIB from any existing OID using its textual representation within a URL parameter.

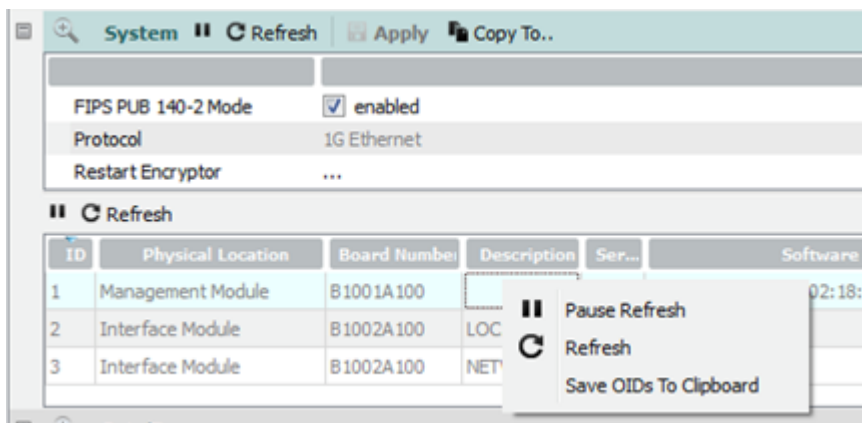
The RESTful interface access is controlled via the user console access rights, that is, the user must be authorized.

Configuration

The RESTful interface can be configured using either the **rest** CLI command or CM7.

Access with CM7

When using CM7, the area of interest can be determined using either OIDs from either the Senetas provided MIB files, or those provided by right clicking a control and saving the OIDs to the clipboard.



In the above example the following inventory table OIDs are saved:

Inventory
Board Number, 1.3.6.1.4.1.3534.3.1.1.2.1.1.2.1.3
Description, 1.3.6.1.4.1.3534.3.1.1.2.1.1.2.1.4
Serial Number, 1.3.6.1.4.1.3534.3.1.1.2.1.1.2.1.5
Software Version, 1.3.6.1.4.1.3534.3.1.1.2.1.1.2.1.6
Software Description, 1.3.6.1.4.1.3534.3.1.1.2.1.1.2.1.7
Build ID, 1.3.6.1.4.1.3534.3.1.1.2.1.1.2.1.8
Build Number, 1.3.6.1.4.1.3534.3.1.1.2.1.1.2.1.9
Build Date And Time, 1.3.6.1.4.1.3534.3.1.1.2.1.1.2.1.10

RESTful examples

The following sections provide examples of how the RESTful interface can be used to perform typical functions.

Alarm monitoring

The OID for the AlarmGroup can be used to show the status of an encryptors alarms. Most tables provide a count scalar variable for monitoring.



```
https://10.65.65.81:7437/fjson/param/AlarmGroup
{
  "sysAlarmCount.0": "1",
  "sysAlarmUnackCount.0": "1",
  "sysAlarmTable": [
    {
      "index": "1",
      "sysAlarmId": "66",
      "sysAlarmTimeStamp": "2017-10-4,6:5:38.0,+0:0",
      "sysAlarmDescr": "Secure tunnel(s) are down",
      "sysAlarmState": "activeNak"
    }
  ],
  "sysAlarmTrapPeriod.0": "0"
}
```

Certificate monitoring

Certificates can be monitored with particular focus on CertificateState and CertificateDaysLeft.



```

https://10.65.65.81:7437/json/param/secCertificateTable
{
  "secCertificateTable": [
    {
      "index": "3",
      "certificateIndex": "3",
      "certificateType": "x509Encryptor",
      "certificateName": "\\15aee9d0\\",
      "certificatePubKeyAlg": "rsa",
      "certificatePubKeySize": "2048",
      "certificateNew": "\\\"",
      "certificateCurrent": "\\-----BEGIN CERTIFICATE----- MIIDQzCCAiuAwI
      bWUxGjAYBgoJkiaJk/IsZAEBDAAoxNDk1MjYxNzg0MCIYDzIwMTcxMTIyMDYwNDUz Wg
      b3JpYTE5MBAK1UEBwwJTWVsYm91cm5lMQwwCgYDVQQKDANPcmcxETAPBgNVBAsM CFB
      A4IBDwAwggEKAoIBAQQDco5z50+8y6gPFpGJmv9i57Rd5jE5/kFE37nDKVLZEJpTP TBH
      ZYqXX21Tm183nN6VV0mHT0qLxh0vXzgpblMu6eDVxaKvw9THGLYhhbpNu5np33a IwP
      2WGvr7UqC/OC4GKTgRs56j+UgToVoeUUG25zHldsFA0f4E7WCNJGbAcVSt9CG27Q tL
      BQADggEBAFGHBYs2pfvUxj7YiE6yNGnEM2xwkcAH2N4Tg/N1NDAUJ5I59FpwcAjM cHJ
      Df5tbKoenFguscYqXkmfGFxFyM3H9zg055ytJZPd3etZnlS10U1Q5ZvoihYh4Mgx Ume
      GZ4Hw9xkwjlnIJJioETZaNs1uFxr5pALR3moyRmQe0tZcnk1D+zrZGLZbHv5gY Ep
      "certificateLastError": "\\\"",
      "certificateDaysLeft": "0",
      "certificateRowStatus": "active",
      "certificateState": "certStateInvalid",
      "certificateInUse": "notInUse"
    },
    {
      "index": "4",
      "certificateIndex": "4",
      "certificateType": "x509Encryptor",
      "certificateName": "\\675af1b2\\",
      "certificatePubKeyAlg": "rsa",
      "certificatePubKeySize": "2048",
      "certificateNew": "\\\"",
      "certificateCurrent": "\\-----BEGIN CERTIFICATE----- MIIDQzCCAiuAwI
      bWUxGjAYBgoJkiaJk/IsZAEBDAAoxNDk1MjYxNzg0MCIYDzIwMTcxMDYwNDUz Wg
      b3JpYTE5MBAK1UEBwwJTWVsYm91cm5lMQwwCgYDVQQKDANPcmcxETAPBgNVBAsM CFB
      A4IBDwAwggEKAoIBAQQDc04P55A2jEWP1LhxV2z1Aii2DE19WuenT5HjY5dDd0WJ S8B
      kgsGWXAD94GokBiorBdizKa20E1PK+lygfu01pHhpmnV1FGet///+X6mhanqG1j1 iL
      /FYxlau0id0Mgbk6swZx8kNrJYfdqYxFjlxTX9UaIwQmWAXT tjRnW0H2WrExvSdhJP5
      05fMYr4kskhyMK+uBdQZnkm3/YQaPY/NfSNQ0YqoTsNfLV6KB0KstHqQ/Wki70LS lDg
      /k78LZY2VhMxVJH YT00529RyuLjghdlL08o7N/Tp2PxA67eXQgp3qEk0UTsof/eBZNP
      "certificateLastError": "\\\"",
      "certificateDaysLeft": "361",
      "certificateRowStatus": "active",
      "certificateState": "certStateSigned",
      "certificateInUse": "notInUse"
    }
  ]
}

```

Audit and Event log monitoring

In addition to monitoring Alarms, it may be beneficial to collate/monitoring changes in the audit and event logs. Centralised remote syslog server configuration is the preferred option to achieve this, however it is also possible to monitor these logs via the RESTful interface.

```
https://10.65.65.81:7437//json/param/sysAuditGroup
{
  "sysAuditDisplayLevel.0": "0",
  "sysAuditCount.0": "27",
  "sysAuditTable": [
    {
      "index": "1",
      "sysAuditId": "0",
      "sysAuditTimeStamp": "2017-10-3,1:54:25.0,+0:0",
      "sysAuditDescr": "admin: Cleared audit log "
    },
    {
      "index": "2",
      "sysAuditId": "0",
      "sysAuditTimeStamp": "2017-10-3,8:13:30.0,+0:0",
      "sysAuditDescr": "New certificate requested "
    }
  ]
}
```

```
https://10.65.65.81:7437//json/param/sysLogGroup
{
  "sysLogDisplayLevel.0": "0",
  "sysLogCaptureLevel.0": "0",
  "sysLogStorage.0": "0",
  "sysLogSize.0": "0",
  "sysLogCount.0": "379",
  "sysLogTable": [
    {
      "index": "1",
      "sysLogId": "0",
      "sysLogTimeStamp": "2017-10-3,1:54:45.0,+0:0",
      "sysLogSeverity": "inform",
      "sysLogDescr": "REST server using CA (944e5b3e), client cert (675af1b2) "
    },
    {
      "index": "2",
      "sysLogId": "0",
      "sysLogTimeStamp": "2017-10-3,1:54:45.0,+0:0"
    }
  ]
}
```

Connection status

Connection tables are specific to the protocol and operational mode selected. The following example relates to VLAN mode. In all cases specific focus should be given to the connection status (in this case gEthVLANConnCiStatus).




```

https://10.65.65.81:7437/json/param/gEthVlanConnCiTable
{
  "gEthVlanConnCiTable": [
    {
      "index": "1",
      "gEthVlanConnCiIndex": "1",
      "gEthVlanConnCiType": "manual",
      "gEthVlanConnCiName": "\ \",
      "gEthVlanConnCiVlanIDTags": "\0100\",
      "gEthVlanConnCiInnerVlanAltEtherType": "disabled",
      "gEthVlanConnCiMode": "discard",
      "gEthVlanConnCieKeyNumber": "0",
      "gEthVlanConnCiiKeyNumber": "0",
      "gEthVlanConnCinNextUpdateTime": "0",
      "gEthVlanConnCiUpTime": "0",
      "gEthVlanConnCiStatus": "up",
      "gEthVlanConnCiStatsRXFramesV2": "?",
      "gEthVlanConnCiStatsTXFramesV2": "?",
      "gEthVlanConnCiControl": "0",
      "gEthVlanConnCiRowStatus": "active",
      "gEthVlanConnCiTxCertificateHash": "\36 37 35 61 66 31 62 32 00 \",
      "gEthVlanConnCiTxCertificateSubject": "\\",
      "gEthVlanConnCiRxCertificateHash": "\30 30 30 30 30 30 30 00 \",
      "gEthVlanConnCiRxCertificateSubject": "\\",
      "gEthVlanConnCiCertificateType": "default",
      "gEthVlanConnCiAuthError": "?"
    }
  ]
}

```

Interface status

This allows the status of the links to be examined.

```

https://10.65.65.81:7437/json/param/gEthVlanConnCiTable
{
  "gEthVlanConnCiTable": [
    {
      "index": "1",
      "gEthVlanConnCiIndex": "1",
      "gEthVlanConnCiType": "manual",
      "gEthVlanConnCiName": "\ \",
      "gEthVlanConnCiVlanIDTags": "\0100\",
      "gEthVlanConnCiInnerVlanAltEtherType": "disabled",
      "gEthVlanConnCiMode": "discard",
      "gEthVlanConnCieKeyNumber": "0",
      "gEthVlanConnCiiKeyNumber": "0",
      "gEthVlanConnCinNextUpdateTime": "0",
      "gEthVlanConnCiUpTime": "0",
      "gEthVlanConnCiStatus": "up",
      "gEthVlanConnCiStatsRXFramesV2": "?",
      "gEthVlanConnCiStatsTXFramesV2": "?",
      "gEthVlanConnCiControl": "0",
      "gEthVlanConnCiRowStatus": "active",
      "gEthVlanConnCiTxCertificateHash": "\36 37 35 61 66 31 62 32 00 \",
      "gEthVlanConnCiTxCertificateSubject": "\\",
      "gEthVlanConnCiRxCertificateHash": "\30 30 30 30 30 30 30 00 \",
      "gEthVlanConnCiRxCertificateSubject": "\\",
      "gEthVlanConnCiCertificateType": "default",
      "gEthVlanConnCiAuthError": "?"
    }
  ]
}

```



SSH Access of Remote Devices

All CN Series encryption devices that have an Auxiliary LAN port (a second physical RJ45 management port) now have the ability to provide tertiary SSH access of remote devices via the local CLI, SSH CLI or CM7 Remote CLI on an encryptor.

To use this method of remote access, the Auxiliary Management mode must be 'enabled'. This can be done using the CLI command ***ip -a enabled***.

The AUX IP management port must also be enabled and configured:

- Configure the port using the CLI command ***ip -s <index> <ip address/mask> <gateway>*** or CM7 Network Addresses field in the Manage interface
- Enable the port using the CLI command ***ip -e <index>*** or CM7 Network Addresses.

WARNING: Ensuring that the auxiliary management IP interface is on the same subnet as the third party device.

At the CLI, the new ***sshaux*** CLI command will display the default user and default IP address and the public SSH key of the encryptor. This key may be pasted into the authorized keys file on the remote device for public key authentication without the need for PAM access.

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

The ***sshaux -c*** and ***sshaux -p*** options allow you to connect using public key authentication or enforce PAM (username/-password) for login respectively. If no user and address is provided with these options, the default values are used.

The default user and address may be modified via the CLI command ***sshaux -s user@<IPv4addr|IPv6addr>[:port]***



CM7 Navigation

The layout and features common to most views within CM7 are highlighted below.

NOTE: Some icons representing specific functionality may not be available on all screens

CypherManager Main Interface

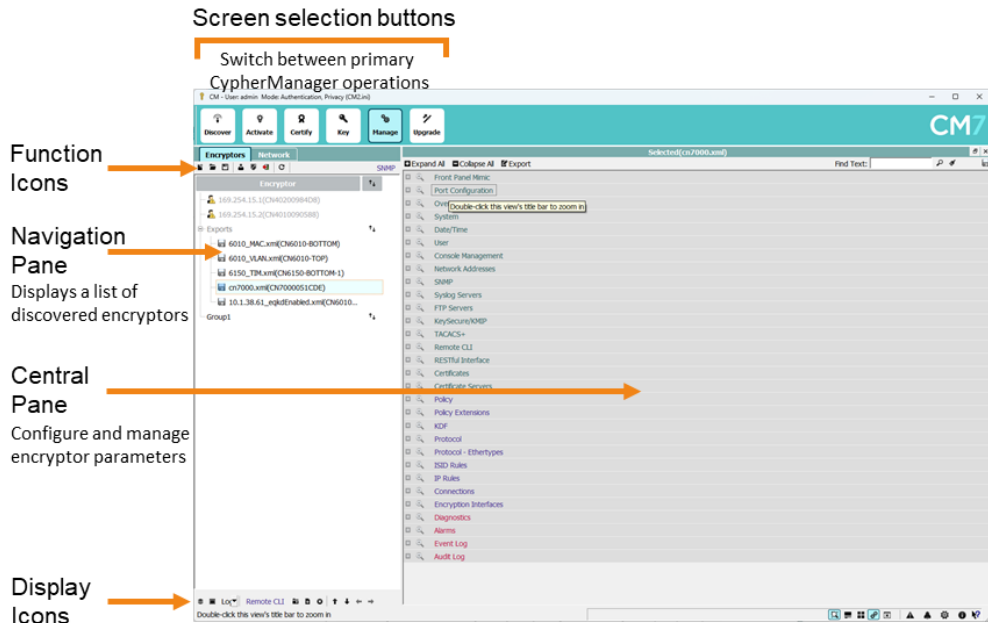


Figure 51: CM7 Main interface

Navigation is performed by clicking, double clicking or right-mouse clicking on the various screen elements, including the function icons, central pane elements, and display icons.

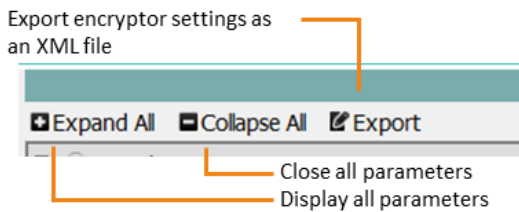


Figure 52: Interface icons - Parameter display

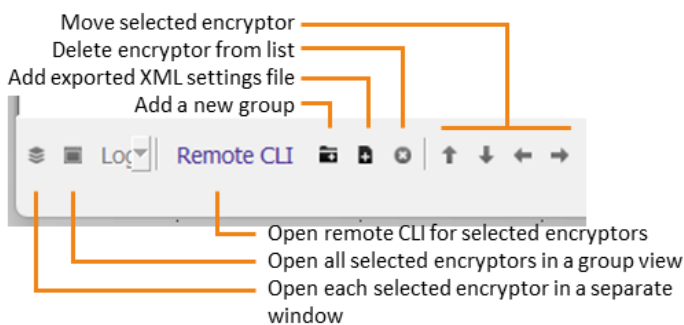
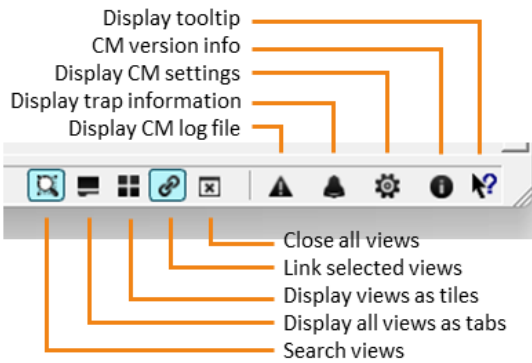
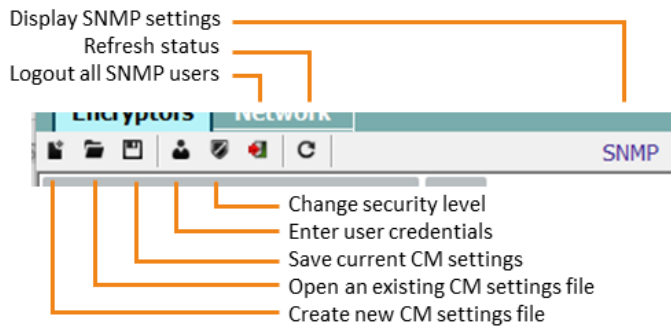
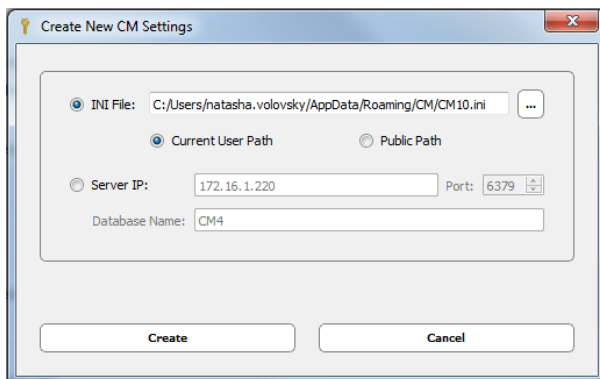


Figure 53: Interface icons - Encryptor list**Figure 54:** Interface icons - CypherManager settings and display**Figure 55:** Interface icons - Settings and security

The 'create new' icon allows you to create a new .INI file or configuration database into which you can save discovered encryptors. The following two screens show the selection for these.

**Figure 56:** Create a new INI file

You can make the .INI file specific to the current user or allow it to be accessed by any CM7 user.

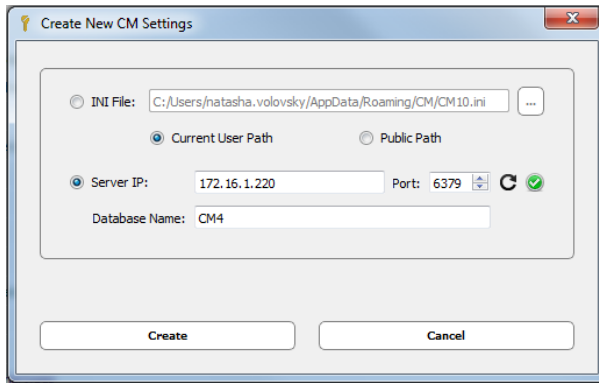


Figure 57: Create a new Configuration database

The named database is created on the specified server. When 'Create' is clicked the database is created and CM7 restarts, allowing the user to specify their Station ID.

The second 'Open' icon allows you to select an existing .INI file or configuration database as the source of the discovered encryptors.

Locating and selecting an existing .INI file loads its encryptors into the discovered list and makes it the current source of discovered units. If a database is required then the following screen is used.

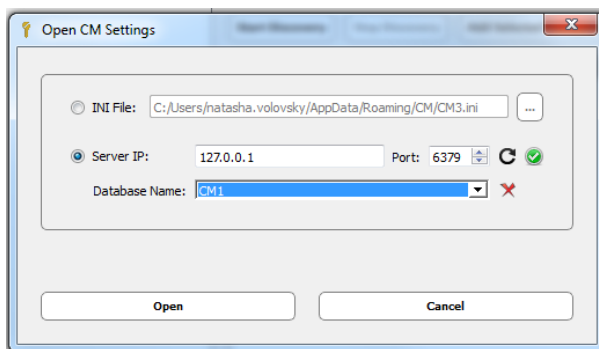


Figure 58: Select an existing database

Note that the red 'delete' icon next to the Database Name selector can be used to delete databases that are no longer required.

Clicking the 'browse' button to the right of the 'INI File' selector displays the existing .INI files so that the desired one can be selected.

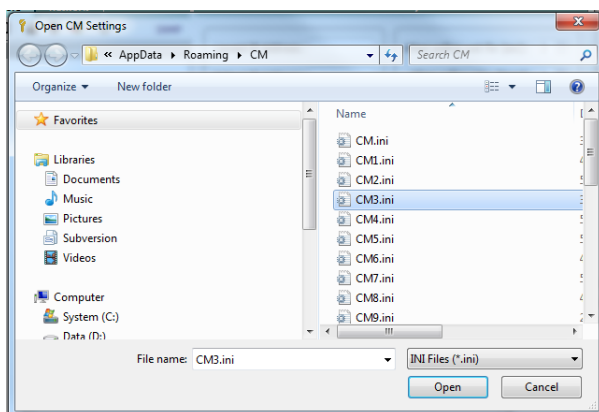


Figure 59: Select an existing .INI file

The third 'SaveAs' icon allows you to save the current list of discovered encryptors into either an .INI file or a configuration database. This function is used to transfer encryptors from the current source to a selected source.

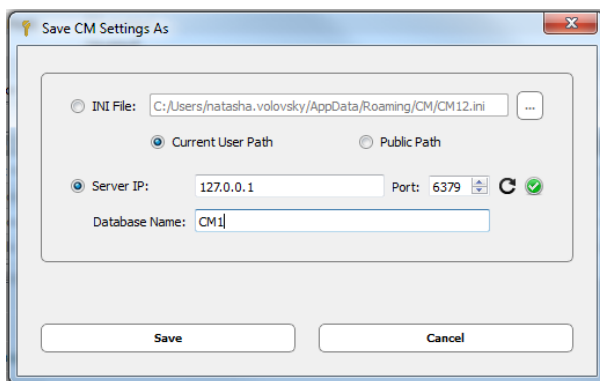


Figure 60: Save current list to a database

If the specified database already exists a warning dialog is displayed so that you can specify whether it should be overwritten or not.

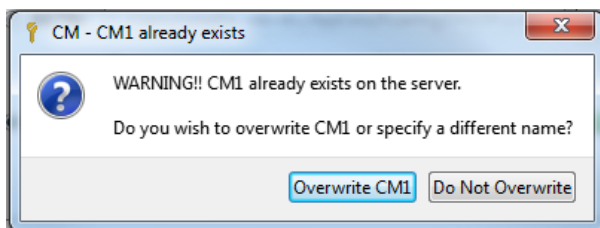


Figure 61: Database exists warning

Sorting discovered encryptors

The 'Sort' icon, displaying up-down arrows to the right of the header row of the Discovered Encryptors list, allows the encryptor tree be sorted alphabetically. Each click on it reverses the order. This icon is also shown next to groups and again repeated clicking will reverse the order.

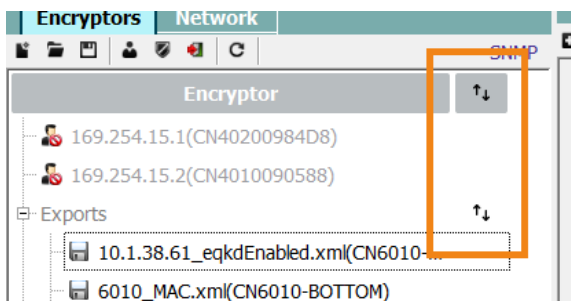


Figure 62: Interface icons - alphabetical list sort

Configuring the discovered encryptor list

Right-clicking on an encryptor listed within the navigation pane opens up a pop-up menu.

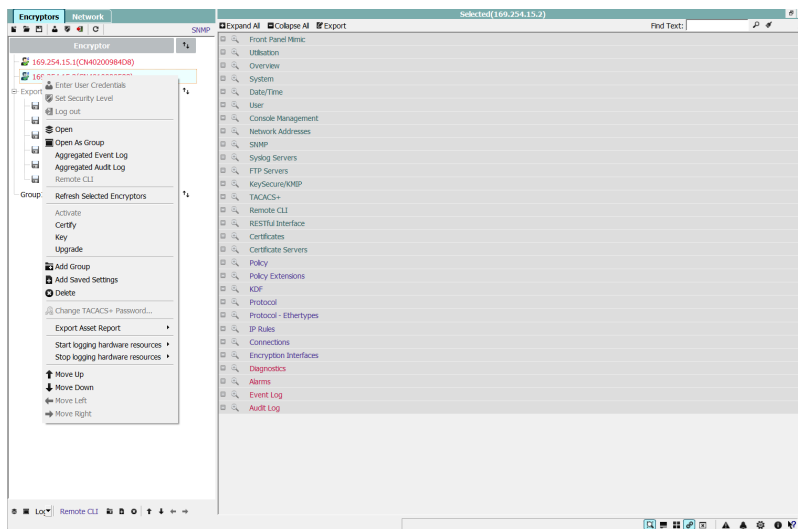


Figure 63: Encryptor list pop-up menu

The pop-up menu contains the same options as the buttons within that configuration group's title bar, these being enabled or disabled depending upon the current state of the encryptor.

Open - displays the Management options so that the selected unit can be managed

Open As Group - opens a window which has combined views of all selected encryptors

Aggregated Event Log - enable/disable the aggregation of Event log entries

Aggregated Audit Log - enable/disable the aggregation of Audit log entries

Activate - selects the Activation screen

Certify - allows the signing of certificates within the selected encryptor (only available if layer 2 modes enabled)

Upgrade - allows the upgrading of the firmware of the selected encryptor

Add Group - add a new group that can be used to logically associate encryptors

Add Saved Setting - adds an encryptor that has been saved as an XML file (See "Manage screen" on page 173)

Delete - delete the selected unit

Change TACACS+ Password - change the TACACS+ password

Move Up - move the selected unit up within the group

Move Down - move the selected unit down within the group

Move Left - move the selected unit left within the group

Move Right - move the selected unit right within the group

Installing CM7

This version is supported by CM7 version 7.9.0.B37.



CM7 is supported on the following operating systems:

Windows:

- Windows 10, Windows 11
- Windows Server 2019, Windows Server 2022

Linux

- Debian (Bullseye)
- CentOS/Redhat 8.0 variant

Recommended system specifications are: 4Gb RAM, 200Mb disk space and Core i5 processor or better.

MacOS

- CM7 can be installed on Apple computers with MacOS running on Intel x64 and ARM M1 processors.

WARNING: Before installing or upgrading your Cypher Manager software you must exit any running instances.

The following sections outline the CM7 installation steps for each of the operating systems.

Windows CM7 installation

1. Download the latest version of Cypher Manager to the computer that will be hosting the software
2. Start Windows
3. From the Windows Start Menu choose 'Run'.
4. Type drive:\setup where 'drive' is the location of the downloaded installation image
5. Press the Enter key.

Setup will copy installation files to the hard disk of the PC and then display the following 'Welcome dialog' box indicating the version of CM7 that you have selected. (The version may differ from that shown in Figure 64 below.)

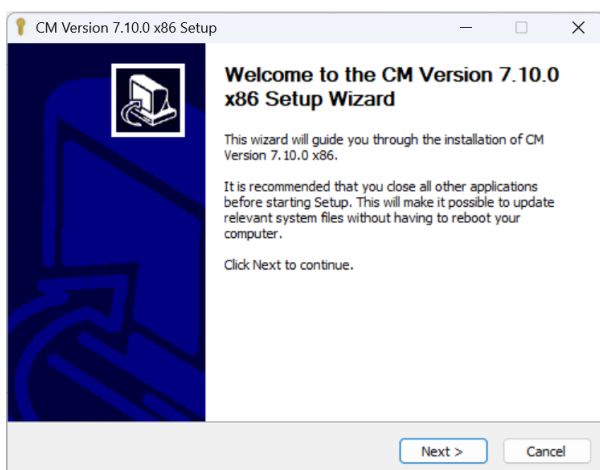


Figure 64: Setup screen

After ensuring that any current instance of CM7 is closed, click on the **Next** button to initiate installation. CM7 will begin to install and you will be asked to accept the License Agreement.

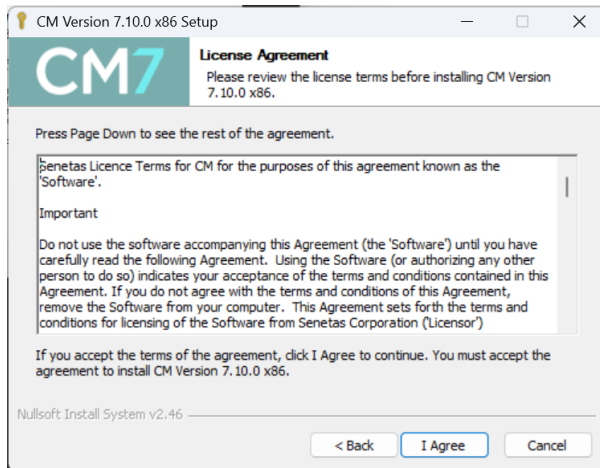


Figure 65: License agreement screen

After you accept the agreement, the install process displays any optional configuration parameters and after selection you should click the **Next** button to continue.

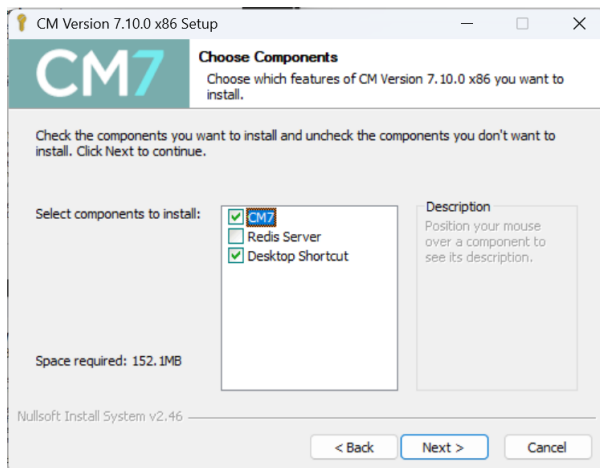


Figure 66: Required components screen

The next screen allows you to either install CM7 in the default location or select an alternate location. Clicking the **Next** button will install CM7.

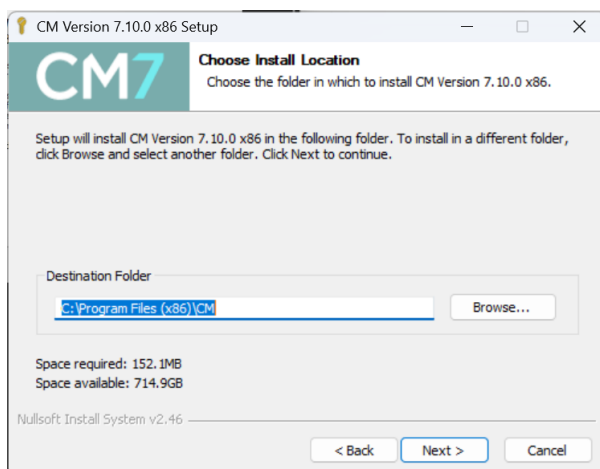
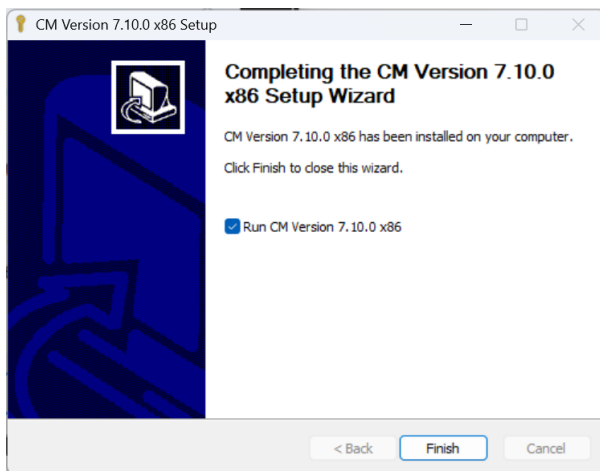


Figure 67: Install location screen

When the installation is complete, the completion screen is displayed after which you can click **Finish** to start CM7 or Exit.

**Figure 68:** Install completed screen

Linux CM7 installation

The Debian Bullseye CM7 distribution is available for 64-bit systems.

The command line installation instruction is:

```
dpkg -i <packagename>.deb
```

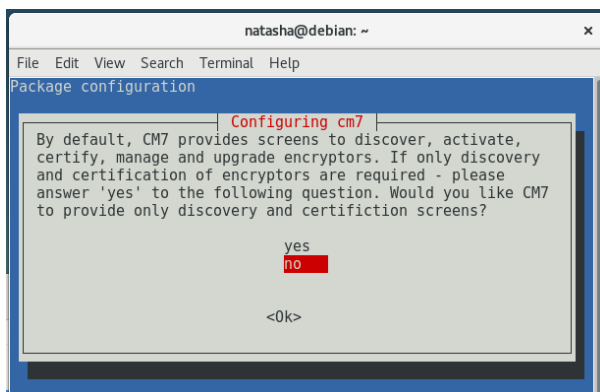
An example is shown below:

```

natasha@debian: ~
File Edit View Search Terminal Help
natasha@debian:~$ su
Password:
root@debian:/home/natasha# dpkg -i CM7_7.10.0_38_amd64.deb

```

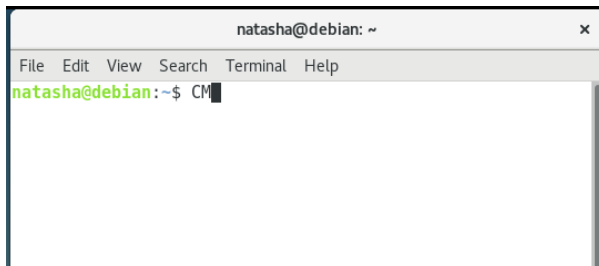
CM7 has a range of functional screens that can be accessed: Discover, Activate, Certify, Key, Manage and Upgrade. If a requirement is to limit what functions can be controlled using CM7, these can be restricted during the installation process.



Following installation CM7 can be started by typing **CM** at the command prompt.



NOTE: This is case sensitive.



```

natasha@debian: ~
File Edit View Search Terminal Help
natasha@debian:~$ CM

```

The Redhat CM7 distribution is also available for 64-bit systems.

The command line installation procedure is:

```
rpm -i -ignorearch <packagename>.rpm
```

NOTE: The **ignorearch** switch ensures that AMD64 and Intel architectures are available as targets.

WARNING: If any additional problems are encountered the **--force** switch may be appropriate.

The manager is installed in `/usr/local/bin/CM` which should be in the path:

```
~/ .config/CM
```

The installation process stores the required fonts in the `/usr/local/Qt-5.2.1/lib/fonts` directory. Should there be any font related issues then these should be copied to `/usr/share/fonts/` after which **fc-cache** should be executed.

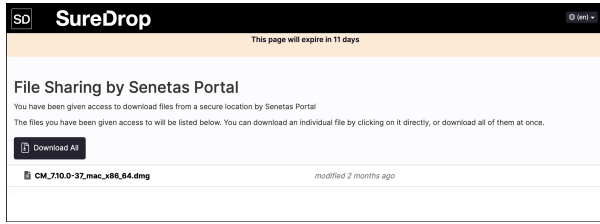
MacOS CM7 installation

You will most likely receive an email inviting you to download an image of the Cypher Manager software. The email will be similar to that shown below:

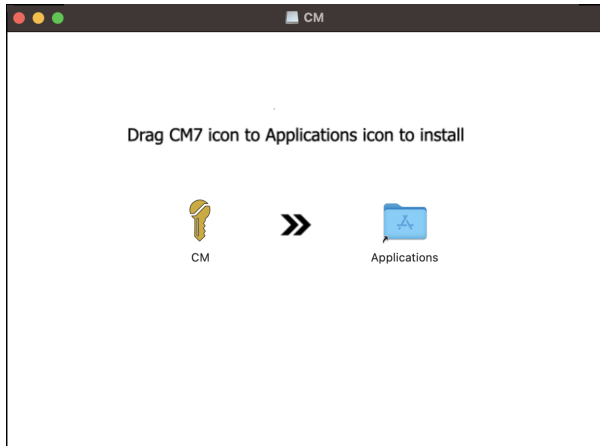


Click the **Go To Shared Files** link and download the software image.

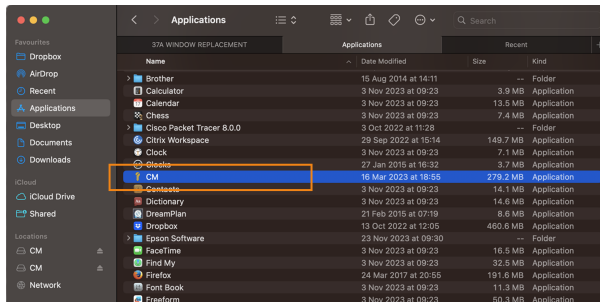




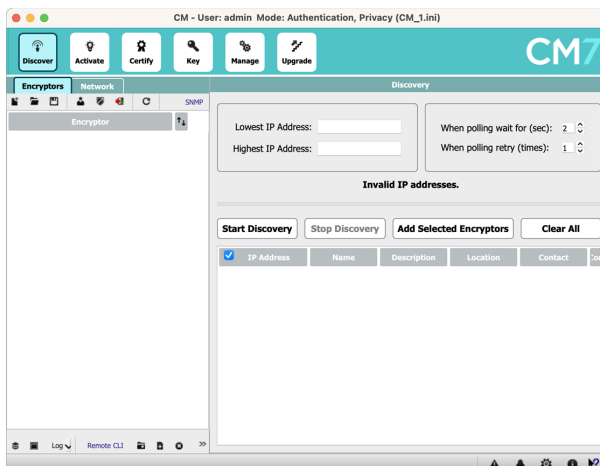
Drag the Cypher Manager icon onto the Applications folder.



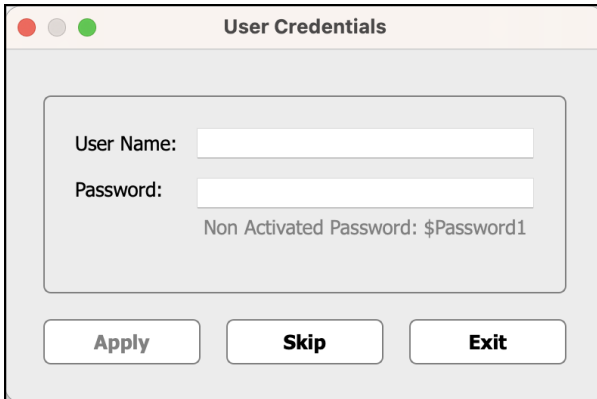
After Cypher Manager has been successfully copied to the host computer, **CTRL-click** on the CM key icon in the MacOS Applications folder.



The main Cypher Manager interface will be displayed:



When the user credentials dialog box appears, enter the default username and password if encryptors have not been activated or the appropriate details if the computer is being added to an established network.



Cypher Manager will then be able to manage encryptors on the network.

Launching and Logging in to CM7

User credentials, which are case sensitive, are held securely within each encryptor and are used to authenticate your access rights whenever you login to an encryptor.

Prior to performing any management function it is recommended that you provide your credentials to CM7. These are entered using the login screen which is displayed whenever you launch the CM7 application.

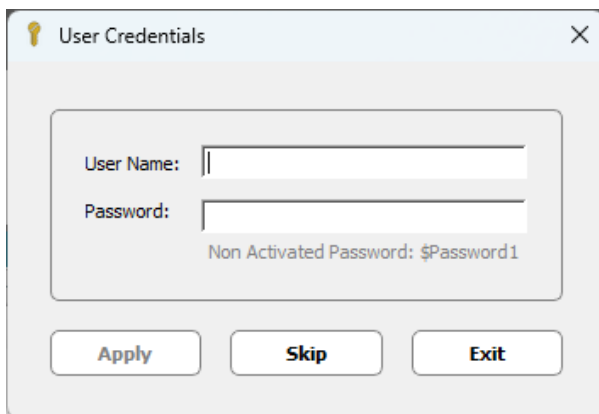


Figure 69: Login dialog

NOTE: The 'Skip' option allows login using the default credentials. This option is convenient when initially activating units.

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

The user account within an encryptor is identified by the 'User Name' and the user's right to access the unit is authenticated with the supplied 'Password'. Privacy refers to the security afforded the SNMPv3 traffic between CM7 and the encryptor that is being managed.

User names can only contain alphanumeric, underscore, dot and dash characters. All other characters are stripped or discarded.

NOTE: By default privacy is enabled and CM7 uses a Diffie-Hellman key exchange to authenticate the user and ensure privacy by encrypting each SNMPv3 request.

CM7 keeps the Names and IP addresses of all of the encryptors that have been 'discovered' in its database. These are used to populate the Encryptor selector so that the login process can be as simple as entering your credentials and selecting the desired unit.

If you have different user account names and/or passwords on each encryptor you will need to log out and back in every time you want to manage a different unit. It is usually more convenient to use the same account names and passwords on all encryptors so that they can be managed from a single CM7 login session.

Configuring CM7

The CM7 user interface can be customised to meet the preferences of the user, the settings being saved in a CM.ini file, or if selected, in a database on a Configuration server.

The CM7 Settings screen shown in Figure 70 below is accessed by clicking on the 'cog' icon at the bottom right of the primary CM7 screen.

NOTE: The help button at the bottom right of the CM Settings screen can be used to display the functionality provided by each of the fields.

Global Login	<input checked="" type="checkbox"/> true
Explicit Login	<input type="checkbox"/> false
Non Activated Password	\$Password1
Station ID	0
Ticket Request Password	*****
Discovery Polling Timeout(sec)	2
Discovery Polling Retries	0
Font Size	14
Display Language	English
Hide Not Applicable Items Manage ...	<input checked="" type="checkbox"/> true
Number of Tiled Manage Windows ...	2
Session Timeout(min)	20
Manage Windows Refresh Rate(sec)	50
Encryptor List Refresh Rate(sec)	40
Network View Refresh Rate(sec)	120
Enable Trap Listener	<input type="checkbox"/> false
Trap Listener Port	162
Display Reports	<input checked="" type="checkbox"/> true
Display Warnings	<input checked="" type="checkbox"/> true
Display Errors	<input checked="" type="checkbox"/> true

CM Settings Location
INI File: [C:/Users/richard.tuft/AppData/Roaming/CM/CM2.ini]

Remote CLI Key
[C:/Users/richard.tuft/AppData/Roaming/CM/CM_REMOTECLI_1.key] Show New

■ Stop Syslog Service Export Syslog Delete Syslog

Start writing to a new syslog file every 6 days

CA/Key Management

Save Close ?

Figure 70: CM7 Settings



The top frame of the window displays the current version number of CM7. This can be compared to the latest available version on the customer portal.

The remaining fields are functionally grouped and provide the following customisation.

Explicit Login - when enabled only the entered credentials are used to login to encryptors. If a login is unsuccessful then the next login attempt is only made after credentials are entered into the Login dialog.

Non Activated Password - specifies the password that will be used to access encryptors that have yet to be activated. This defaults to \$Password1, however this can be changed if required.

Station ID - by selecting a different station ID than other users you provide CM7 with the ability to concurrently manage individual users. It is recommended that in organisations where multiple managers may exist, each user workstation is configured with a unique ID.

Ticket Request Password -

Discovery Polling Timeout(sec) - the default timeout discovery period of 2 seconds seldom requires changing. However in noisy environments or within large networks it can be increased to allow for any delays that exist.

Discovery Polling Retries - the default value of 1 is normally adequate. However in noisy environments a higher value may be required.

Font - The point size of the CM7 interface is configurable via the Settings dialog. You can select integer values from 9 to 18 point. The default size is 11 point.

Hide Not Applicable Settings - by default, any settings that do not apply to the current encryptor model or context are hidden. Enabling this selector shows all variants.

Number of Tiled Manage Windows Across - leaving this setting at the default of 2 will result in side-by-side display of up to 2 encryptors. Additional encryptors will be tiled in the next available slot within one of the columns.

Session Timeout(min): - by default CM7 sessions timeout at 5 minutes. This can be increased or decreased (to a maximum of 60 minutes) to meet user needs, however the security requirements of your organisation should be considered.

Manage Windows Refresh Rate(sec) - by default, the currently displayed Manage Window content is refreshed every 15 seconds. This can be increased or decreased to meet your needs.

Encryptor List Refresh Rate(sec) - by default, the encryptor list is refreshed every 20 seconds. This can be increased or decreased to meet your needs.

Network View Refresh Rate(sec) - by default, the network view is refreshed every 60 seconds. This can be increased or decreased to meet your needs.

Enable Trap Listener - enabling the trap listener allows CM7 to receive any traps that are sent to its configured trap address.

Trap Listener Port - allows you to change the SNMP trap listener port

Display Reports - adds informative messages to the CM7 log window

Display Warnings - adds warning messages to the CM7 log window

Display Errors - adds error messages to the CM7 log window

CM Settings Location - if the CM settings are held in an INI file this allows selection of the path used to store the settings file. Either the **Current User Path** or the **Public Path** will have been selected when CM7 was installed, however this can be changed if desired.

If the CM settings are held in a Configuration server database then this allows the selection of the Server and Database as shown in the modified dialog below.



CM Settings Path

Server IP: Port:

Database Name:

CA/Key Management - clicking on this button opens the Create CA screen, which allows CM7 to be configured as a Certificate Authority and allows the definition of KDK keys for use in TIM mode

Save - saves the current settings

Close - exits from this screen without saving any changes to the CM7 settings



Creating the PKCS#12 file

The Certificate Authority (CA) 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 the CM7 itself or, alternatively, the file can be sourced from an external CA.

Figure 71 below shows the internal CA creation process.

CA/Key Management

Create New CA | Advanced | EC Parameters | Export CA Certs | KDK

This screen generates the local CA keys and root certificate in a PKCS#12 file that can be used to certify encryptors.

1. Set the **Key Type** for the CA certificate.
2. Set the **Serial Number** for the CA certificate.
3. Choose the **CA Issuer Name** for the CA certificate.
4. Select the **Validity Period** for the CA certificate.
5. Select name and location of the P12 file.
6. Click '**Create CA File**' button.
7. To encrypt the P12 file choose and confirm the CA password.

CM will securely wrap the CA certificate and keys in a password protected P12 file for local storage. This password will be required when signing all encryptor certificates.

Key Type: RSA2048, RSA 2048bit Add Custom

Serial Number: a9:5d:29:d6:00:00:00:00

CA Issuer Name

Attribute Name: C = country

Attribute Value: AU

Separator: ,

Distinguished Name: C=AU,O=Organisation,CN=CommonName,UID=1567555131

Validity Period

Not Before: 2019-09-03 09:58

Not After: 2034-09-04 09:58

CA File: C:/Users/alan.williamson/AppData/Roaming/CM/CM_CA1.p12

Create CA File Close

Figure 71: Create Internal CA screen

Key Type - allows the selection of the key type that will be used when signing certificates. This can be RSA-2048 or any of a number of supported elliptic curves, including customer-supplied custom curves. This default key type can be overridden when certificates are signed.

The '**Add Custom**' button allows the selection of additional user-defined Elliptic Curve types. However, the parameters for these must be predefined as described on page 149.

Serial Number - specifies the initial serial number that will be used on signed certificates.

CA Issuer Name - allows definition of the fields that make up the distinguishing name of the CA. These should be assigned to clearly identify the CA. The validity indicator is green when all of the sub-fields are valid. It is important to note that a different name must be used for each CA that will be used to sign encryptors. (If the same name is used the PKI process may locate and use the incorrect certificate resulting in an authentication error).

Validity Period - defines the date range over which the CA will be valid. The default is 15 years.

CA Password - identifies the password that will be required by a user in order to sign certificates using this PKCS#12 file. Re-entry is required to ensure the entry is correct and the validity indicator will be green if the passwords meet the password rules.

CA File - shown if an INI file is selected as the store for the PKCS#12 file. In this case, the file location and name is shown and the 'browse' button can be used to specify these.

CA - shown if a Configuration server and database are being used to store the PKCS#12 file. See "CA Configuration server and database selection" on page 144 See "CA Configuration server and database selection" on page 144

Figure 72: CA Configuration server and database selection

Create CA File - used to create and save the PKCS#12 file in the selected location.

Certificate hash algorithm

The certificate signing algorithm determines the signature hash algorithm used, as indicated in the following table:

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

Certificate Authorities

Each of the encryptors within a security domain must have at least one certificate that has been signed by the same Certificate Authority. The Senetas CM7 network management tool has a CA that is able to sign all of the target encryptors, and if required any third party PKI compatible CA can be used.

In many instances, particularly where a small network is being managed, CM7 is a logical choice. For larger networks or when your organisation has established security processes an organization wide CA may be appropriate. The remainder of this section applies when CM7 is used.

CM7 allows you to sign certificates using one of the following:

- RSA (Rivest-Shamir-Adleman) which uses 2048 bit (or optionally 4096 bit) keys. This is the default and is considered by NIST to be secure



- ECC (Elliptic Curve Cryptography) which is both faster and more secure than RSA and is preferred by many cryptographic professionals
- Brainpool (an ECC variant) which while based on ECC does not use NIST parameters and is therefore preferred by some end users
- QRA (hybrid implementation) which are based on NIST candidate Quantum Resistant Algorithms and prove extended security pending ratification

NOTE: For most applications, RSA is considered adequate. Your security policy will determine which should be used.

Additional information can be found at https://en.wikipedia.org/wiki/Elliptic-curve_cryptography#Implementation

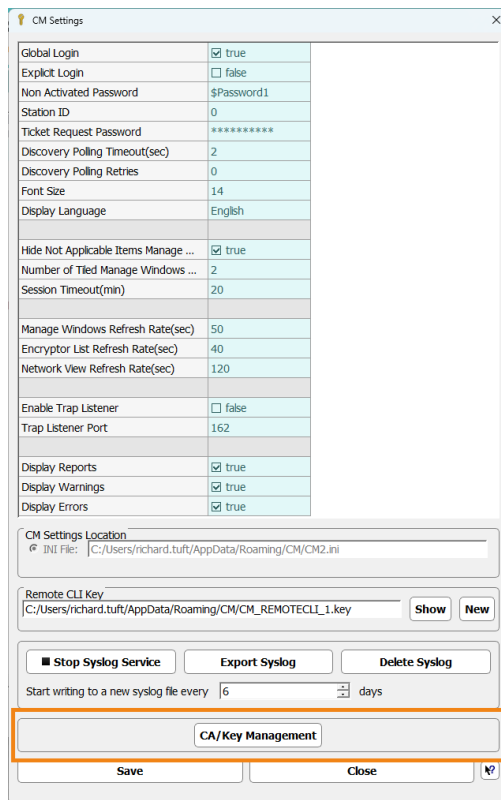
Certificate Chain Validation

CM7 ensures that any CA file that is opened is validated by confirming that the entire certificate chain is present and valid.

- If no valid certificate chain can be established – an error is displayed at the bottom of the **nternal CA** tab
- If validation succeeds the CA file is successfully loaded

Permitted byte-size of CA serial numbers

CAs may have a serial number that is longer than 8 bytes. When creating a CA in 'CA/Key Management' dialogue accessed from the 'CM Settings' interface.



The default 8 byte serial number can be extended by adding bytes in :XX format where X is a hex character from 0 to F.



7. To encrypt the P12 file choose and confirm a CA password.

Key Type: RSA2048, RSA 2048bit Add Custom

Serial Number: a2:28:2f:cb:00:00:00:00

CA Issuer Name

Attribute Name: C = country

Attribute Value: AU

Separator: ,

Advanced CA functions

The Advanced tab of the Certification Authority screen is used to perform specific CA functions. These include the generation of CSRs, the signing of these and the subsequent saving of the signed file.

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 = countrv

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 73: Advanced CA functions

Certificate Signing Requests

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

The pre-defined key types include:

RSA2048, RSA 2048bit
 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, NIST/SECG curve over a 283 bit binary field
 sect283r1, NIST/SECG curve over a 283 bit binary field
 sect409k1, NIST/SECG curve over a 409 bit binary field
 sect409r1, NIST/SECG curve over a 409 bit binary field
 sect571k1, NIST/SECG curve over a 571 bit binary field
 sect571r1, NIST/SECG curve 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 (see EC parameters screen on page 149) can be added to the "Generate From ..." list using the 'Add Custom' button, which opens the following screen to allow selection of the required parameter file.

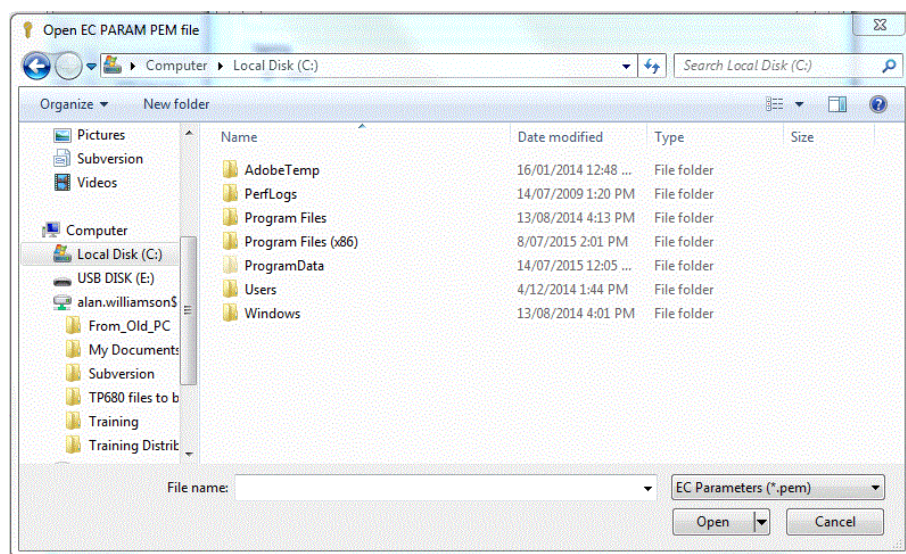


Figure 74: EC parameters selection

Each CSR requires a **Distinguishing Name** that includes a number of attributes that are used to identify the certificate.

In the case of CSRs that define custom EC parameters, the DN must include the following three attributes:

Title - which must be ECPARAM

Name - which is free form and used to identify the curve, for example, 'EC192 curve'

Description - which is free form and used to describe the curve in more detail

Signing the CSR

The Signing panel allows the CSR to be specified as 'self signed' or signed using a PKCS#12 file.

If a PKCS#12 file is used and this file is held in an INI file then it is selected using the following dialog.

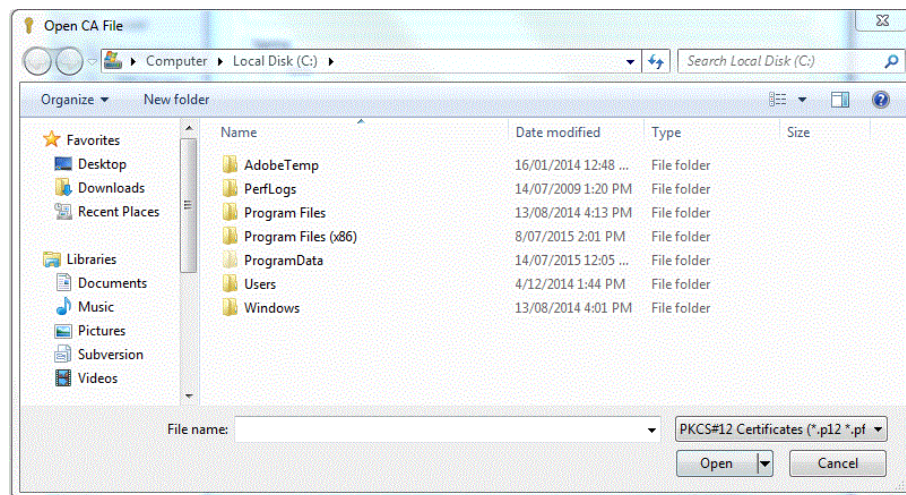


Figure 75: Selecting the PKCS#12 file

If the PKCS#12 file is held in a Configuration server database then the following modified dialog allows you to select one of the databases from the current server.

Saving the CSR

The 'Save As' selector allows the CSR to be saved to file system of the CM7, as either a PKCS#12 file or, for Elliptic Curve parameters, a .PEM file. In the case of the parameter file there is no requirement to save the private key of the CSR.

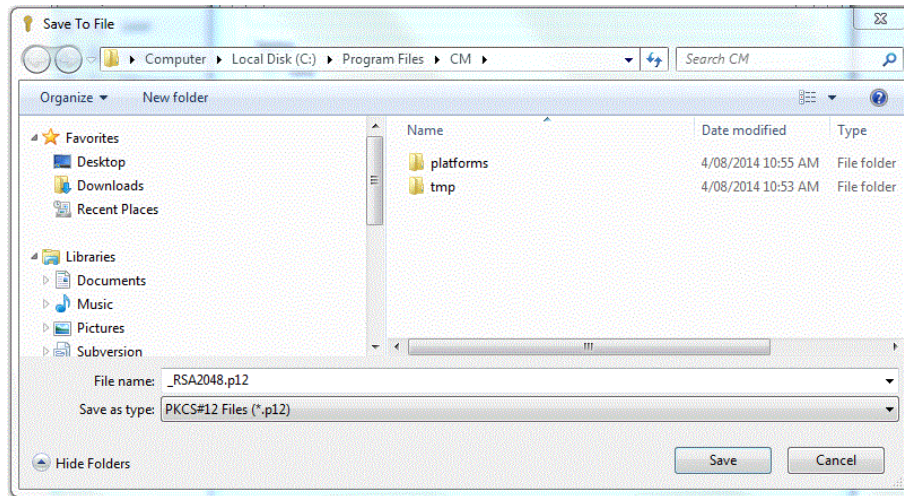


Figure 76: Save CSR dialog

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

Elliptic Curve Parameters screen

In order for an encryptor to generate an EC certificate it must be provided with Elliptic Curve parameters. These parameters are specified using the 'EC Parameters' screen, after which they are saved on the clipboard or in a file so that they can be loaded into the encryptor.

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 77: EC Parameters screen

The curve data is entered into the fields of the parameters screen. Note that the X and Y parameters and the G parameters are mutually exclusive and only one is required. When all of the parameters have been entered the 'From Curve Data' button is used to create the parameters and display them along with a validity indicator in the area of the text box at the bottom of the screen.

The parameters can be saved to the clipboard or to a 'pem formatted' file so that they are available for use as Custom key types when generating certificates. See "Certificate Signing Requests" on page 147.

Importing and exporting CA files

The PKCS#12 files that are used to sign certificates can be imported into or exported from Configuration server databases.

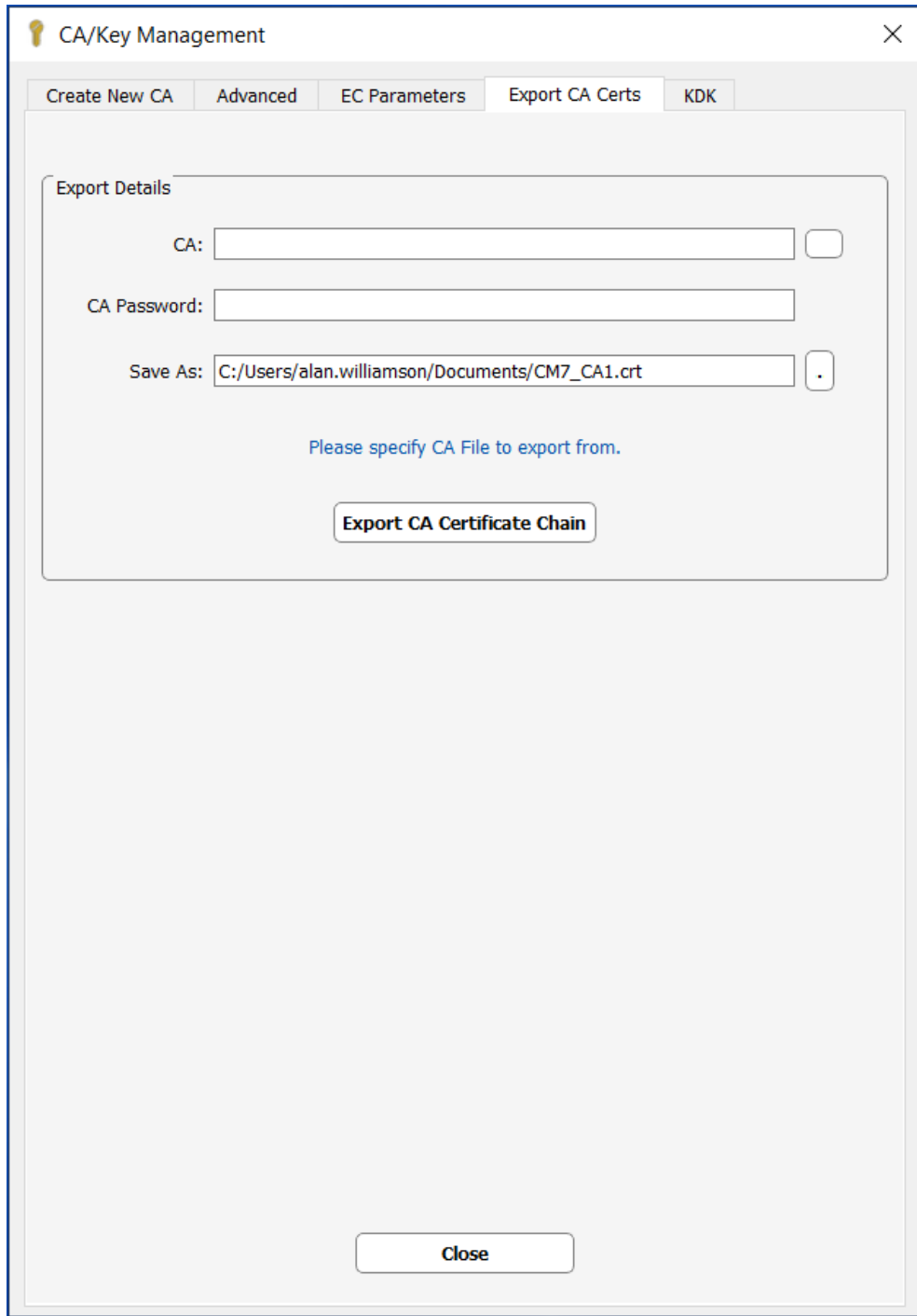


Figure 78: Database Import/Export

For CA imports:

- **Import CA File** - selects the location and PKCS#12 file to be imported. The 'browse' button allows the file to be located within the CM7 host file system
- **Import To CA Name** - allows specification of the database name

For CA exports:



- **Export CA** - allows selection of a database located on the currently selected server
- **Export To CA File** - allows specification of the PKCS#12 file name. The 'browse' button allows selection of a target directory

QRA-based key generation

Quantum Resistant Algorithms are being introduced to provide protection against brute force attacks that could be used to break the security of the encryptors encrypt processes. Currently QRA techniques are still under development and therefore NIST requires that they be used in conjunction with RSA/ECDSA.

This hybrid approach is supported by Senetas encryptor firmware and allows use of all of the QRA candidates.

NOTE: Encryptors configured with a ancillary QRA certificate cannot successfully establish a secure connection with a device running v5.1.x or earlier and in order to use QRA certificates in connections all devices in the network need to use v5.2.0 or later.

Quantum Resistant Algorithms:

QRAs are used both within the Key Encapsulation Mechanisms (KEMs) that are used to establish AES symmetric keys, and the Signature Schemes used to sign messages.

The KEM finalists include Classic McEliece, Kyber, NTRU and SABER and the signing finalists include Dilithium, Falcon and Rainbow.

The hybrid scheme requires that each encryptor has both a signed RSA/ECDSA and a signed QRA certificate. During session establishment processes are used to create and exchange AES-256 bit keys that are then XORed together. The resulting DEK provides the assured protection of the current RSA/ECDSA model extended by the selected QRA algorithm.

KEM and QRA ancillary certificates provided by the encryptors and CM7 have been updated to align with the NIST 3rd round finalists.

CAUTION: In order to sign and install QRA certificates in v5.5.0, CM7 must be upgraded to version 7.10.0. Encryptors running v5.2.1 firmware and using QRA certificates must use CM version 7.9.0

QRA algorithms

The supported quantum-resistant KEM algorithms are:

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

The available QRA certificates are:



- DILITHIUM2
- DILITHIUM3
- DILITHIUM5
- DILITHIUM2-AES
- DILITHIUM3-AES
- DILITHIUM5-AES
- Falcon-512
- Falcon-1024
- 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

WARNING: It is not recommended to use the SPHINCS certificates. Due to their size, some of the SPHINCS certificates may not install and if installed successfully could degrade the manageability of the certificates may not install and if installed successfully could degrade the manageability of the encryptor.

NOTE: Senetas recommends the use of DILITHIUM or Falcon certificates

Hybrid connections

A maximum of 16 hybrid connections is supported per device:

- CN4010 supports 16 hybrid connections
- CN6140 1G supports 16 hybrid connections
- CN6140 4x1G
 - if all 4 slots are running, then each slot supports 4 hybrid connections
 - if 3 slots are running, then each slot supports 5 hybrid connections
 - if 2 slots are running, then each slot supports 8 hybrid connections
 - if only 1 slot is running, then the slot supports 16 hybrid connections
- CN6140 2x10G
 - if all 2 slots are running, then each slot supports 8 hybrid connections
 - if only 1 slot is running, then the slot supports 16 hybrid connections

CAUTION: If more than the maximum recommended hybrid connections are in use, the device may become unmanageable.





KDK Key generation

In order to establish secure security associations encryptors configured in TIM mode that use the KDF key derivation function must be seeded with identical KDK keys.

To generate KDK keys that will be available for distribution to encryptors, select the KDK tab to display the following dialog:

The screenshot shows a dialog box titled "CA/Key Management" with a "KDK" tab selected. The dialog contains the following elements:

- Instructions: "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: A text input field with a password mask (dots) and a visibility icon.
- Hash: A text input field containing the value "59B5EFD8A83722E4763058884005C78EC8276645602E6FC99964A5ACFD68".
- Autofill KDK: A dropdown menu with "Generate in CM7" selected and a refresh icon.
- KDK File: A text input field containing the path "in.williamson/AppData/Roaming/CM/CM_KDK_33AA5985EFD8A83722E4.enc".
- Buttons: "Create KDK File" and "Close".

Keys can be manually entered (unless in FIPS mode), or more usually generated using the **Autofill KDK** selector which allows either CM7 or any of the listed encryptors to be used as the key source.

kdf and **FIPS**

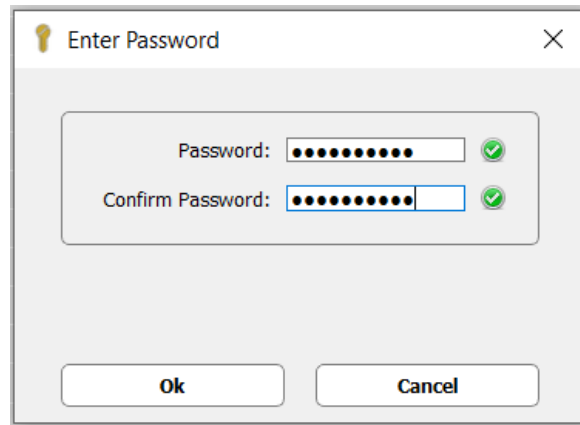
When FIPS mode is enabled, you will not be able to use the **kdf -g** and **kdf -k** commands via the local CLI to generate a key. The KDF may still be entered using CM7, SNMPv3 or the remote CLI.

When FIPS mode is disabled, all four methods to enter the KDF - local CLI, CM7, SNMPv3 and remote CLI are available.

NOTE: Only hardware-based encryptors with firmware releases of v5.1.0 or later are available for use KDK Key Generators.

By default CM7 will generate a key file in a folder in the AppData path for the loggedin user. The filename has a suffix based on the hash of the KDK. While not recommended, both the file location and filename can be changed.

The **Create KDK File** button requests a password that will be used to protect the file and then when OK is clicked, generates it in the specified location.



Following creation, additional keys can be generated should these be required.

Deleting PKCS#12 files

The Delete CA tab can be used to list and then selectively delete PKCS#12 (CA) files from the current Configuration server.

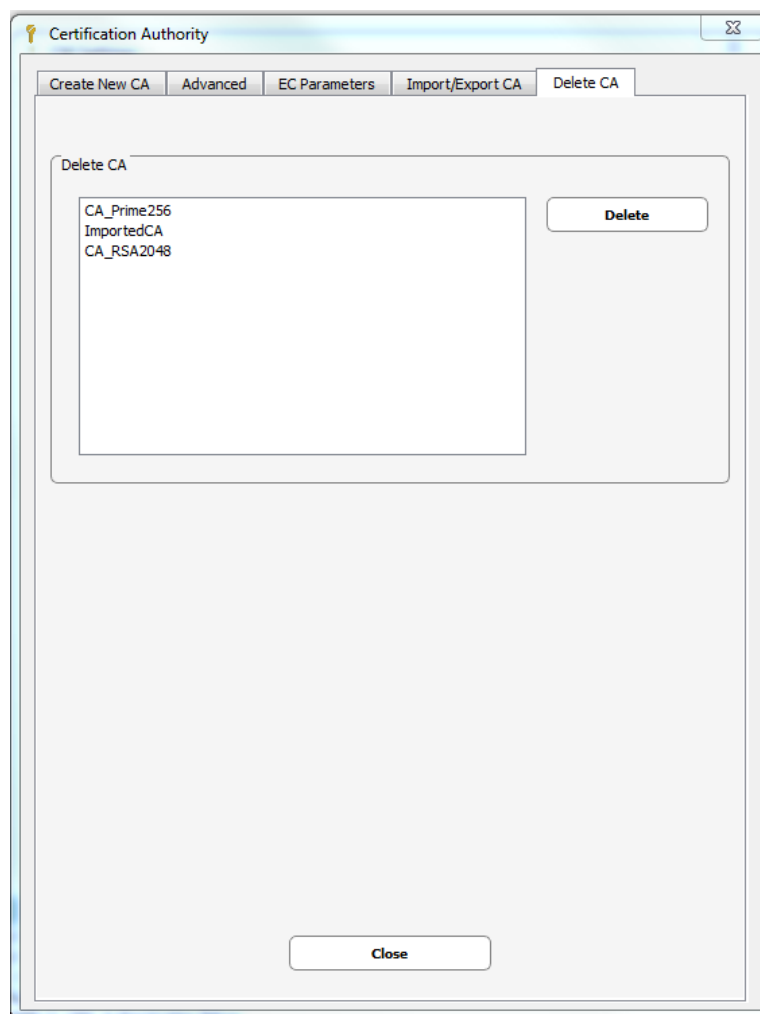
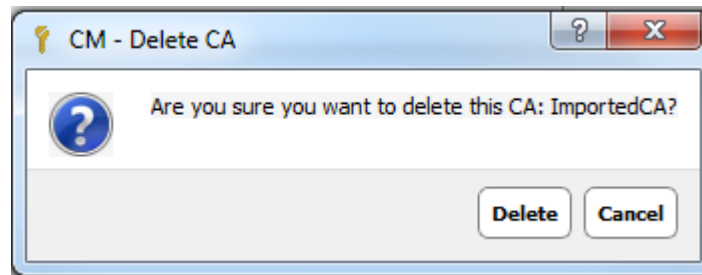


Figure 79: Delete CA files from Configuration server

The CA file that is to be deleted is selected and the Delete key pressed. A warning is raised to allow confirmation of the deletion.



Initial configuration settings

The first time CM7 is run following installation, it prompts the user for the location where the CM configuration settings will be installed. As shown in Figure 80 below, the path can be to an INI file in a defined directory or in a Configuration server database.

Configuration server databases provide a convenient way of sharing lists of encryptors and PKCS#12 files. For example, you could have lists for different support groups, lists for geographies, lists for departments, etc. The configuration server can be on a central server or on your local system.

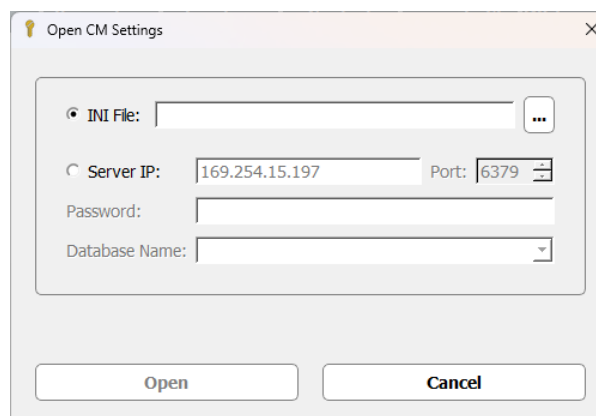


Figure 80: Select CM7 settings location

If a .INI file is to be used then the 'browse' button to the right of the INI file selector allows you to change the default location.

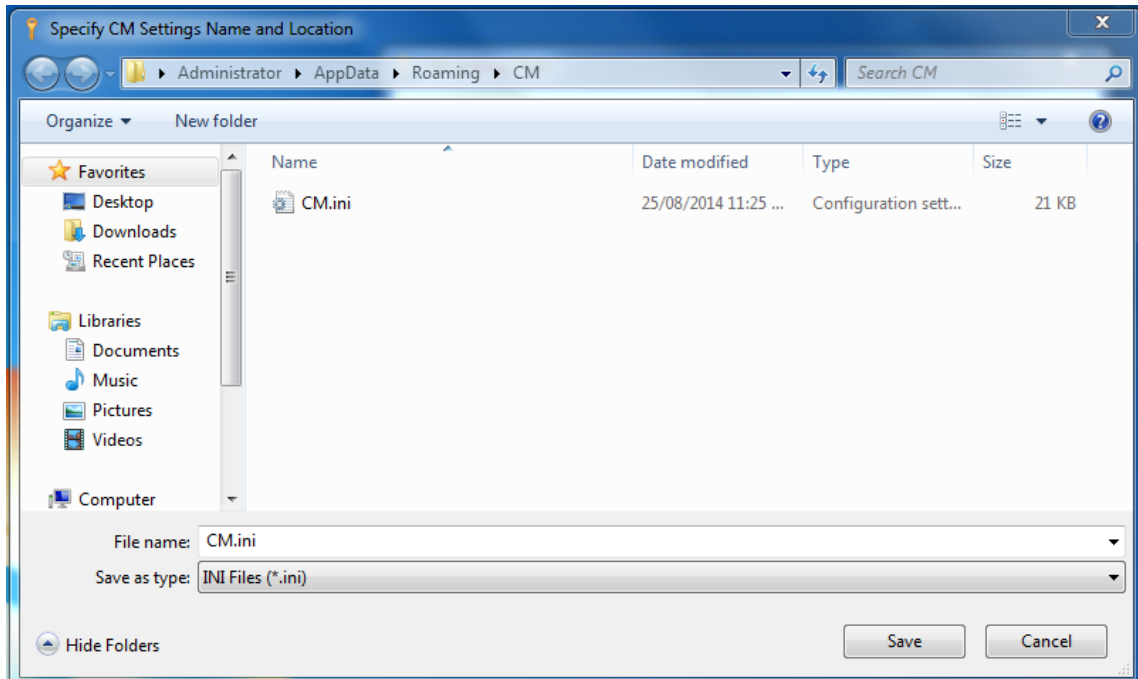


Figure 81: Selecting an alternative INI file location

If a Configuration server database is to be used then the Server IP and Port selectors can be used to specify the database location. When the IP address is entered and the <Enter> key is pressed (or the refresh symbol clicked) then CM7 attempts to connect to the server and if this is successful the 'success indicator' to the right is shown as a green tick. If a connection cannot be made, perhaps because the server is not running, then the indicator will be red. Hovering over the indicator will display the status of the server. Note however, that the messages are server dependent and not documented here. IP address 127.0.0.1 can be used for a server located on the CM7 system.

After the server is specified, the Database Name selector is filled with the names of the databases hosted on that server. Creating a database with the same name as an existing database will raise a warning to indicate that existing settings will be overwritten.

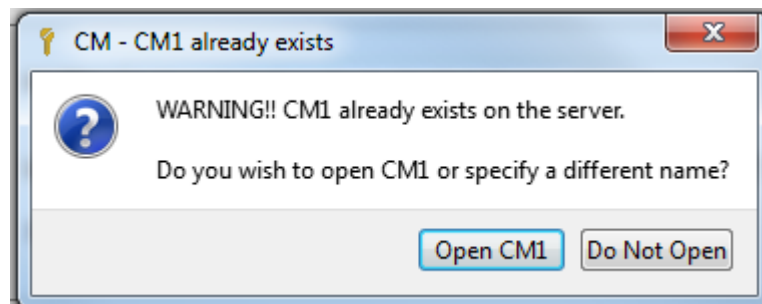


Figure 82: Overwriting an existing database

If you would like to delete a database then it can be selected and the 'delete symbol' to the right of the Database Name clicked. A warning is raised to allow you to confirm that the specified database is to be deleted.

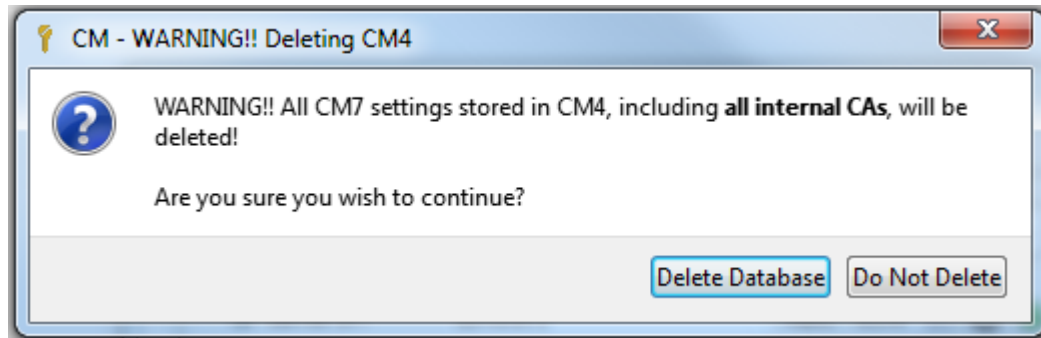


Figure 83: Delete database warning

NOTE: The delete function is hidden if the selected database is open.

Moving CM7 to a new PC

To move CM7 to a new PC you should follow the following steps:

1. Determine the location of the CM.INI file for the existing installation by examining the 'path' on the CM7 settings pane
2. Copy the CM.INI file to a memory stick
3. Install CM7 on the new machine
4. Examine the 'path' to determine the location of the CM.INI file of the new installation
5. Replace the CM.INI file with the one that was saved on the memory stick



CM7 Screen selection

To select a particular function, simply click on the required screen button.

Screen selection buttons

Switch between primary CypherManager operations

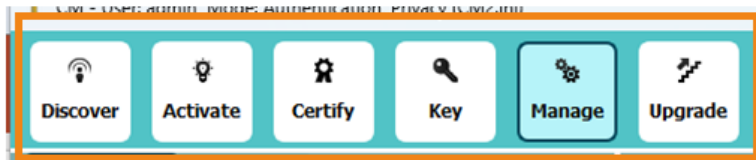


Figure 84: Functional navigation

- **Discover** - allows you to discover encryptors using their IP address. See "Discover screen" on page 162
- **Activate** - allows you to activate encryptors that you have discovered. See "Activate screen" on page 162
- **Certify** - allows you to certify activated encryptors using the internal CA of the CM7 or an external CA.
- **Key** - allows you to distribute previously defined Key Derivation Keys (KDK's). See "Key Screen (only layer 3/4)" on page 171
- **Manage** - allows you to manage a selected encryptor. See "Manage screen" on page 173
- **Upgrade** - allows you to upgrade the firmware of a selected encryptor. See "Upgrade screen" on page 221

CM7 Multi-User Mode

Multi-user mode allows users to have different credentials for specific encryptors or encryptor groups.

The 'Global Login' mode is part of the the 'CM Settings' dialog and applies the entered user credentials to all discovered encryptors..

NOTE: By default 'Global Login' is enabled.

When Global Login is **disabled**, different user credentials can be provided for different encryptor groups or encryptors.

- Select individual encryptors or encryptor groups via the Encryptor tree.
- Enter credentials through the User Credentials dialogue, which can be activated by selecting 'Enter User Credentials' either from the right-click menu or the top toolbar of the encryptor tree.

While Global Login is disabled, a login dialogue will not be presented at CM7 start-up and should be set individually to different encryptor groups/encryptors. In multi-user mode, different security levels can be set for different encryptor groups/encryptors and the 'Logout' option is also available for selected encryptors.

The default session timeout has been increased to 60 minutes while in multi-user mode. When the session timeout occurs, the SNMP connection to all encryptors will be stopped.

The status tooltip, which is displayed when the cursor is 'hovered' over an encryptor name in the Encryptor tree, now includes SNMP User and Security Level information.

SNMP security level

The default security level setting for CM7 is '*SNMPv3: Authentication, Privacy*' which provides a Diffie-Hellman authenticated connection. You can use the settings shown in Figure 85 on the facing page to change this if required.

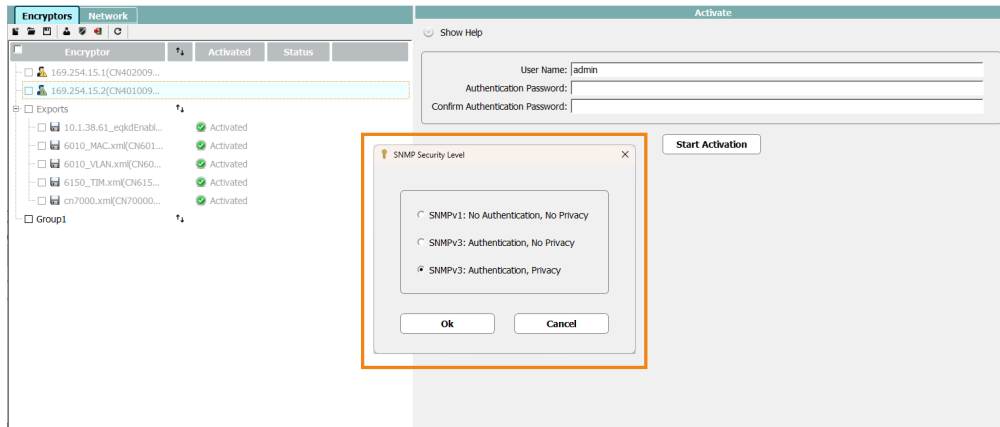


Figure 85: SNMP Security level settings

The 'SNMPv1: No Authentication, No privacy' setting is used to provide users with read-only access.

The 'SNMPv3: Authentication, No Privacy' setting is provided to allow operation with encryptions that feature earlier versions of firmware that do not support the Diffie-Hellman protocol.

Multi-slot management

For multi-slot encryptions the options available depend on whether you are managing the **host** or an individual **slot**. The initial login as an administrator provides limited management functionality. In particular, the **slot** command which is used to configure individual slots is only available when managing the host. Logging in as a user configured for a particular slot (or slots) provides access to the standard management functions as shown in on page 173.

The CLI also supports the slot command as described on page .

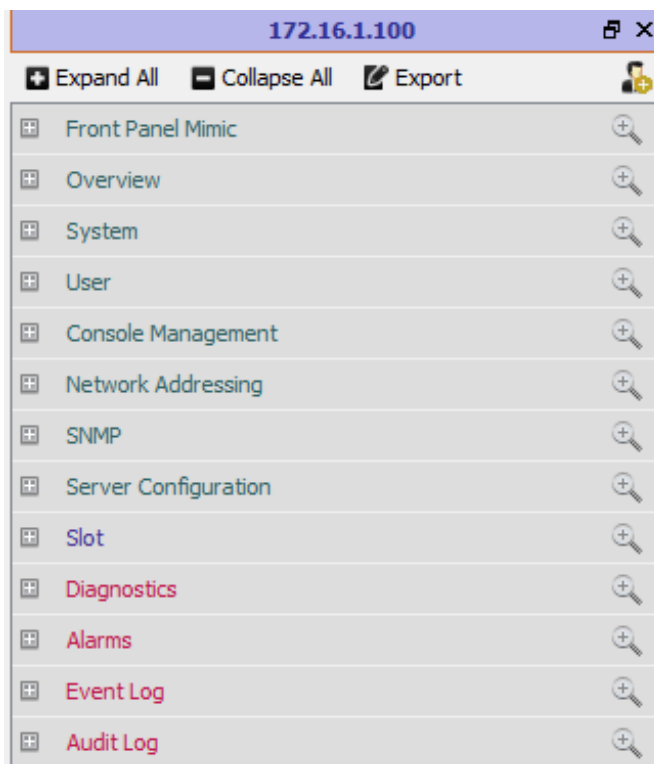


Figure 86: Host Management options for Multi-slot encryptions

Discover screen

Encryptors are discovered by selecting the CM7 Discover function, entering the lowest and highest management IP addresses to be polled and then starting the discovery process.

The discovered units are displayed so that they can be selected and added to the discovered encryptor list. If an encryptor is a multi-slot unit then its slots will also be discovered and grouped after the host unit.

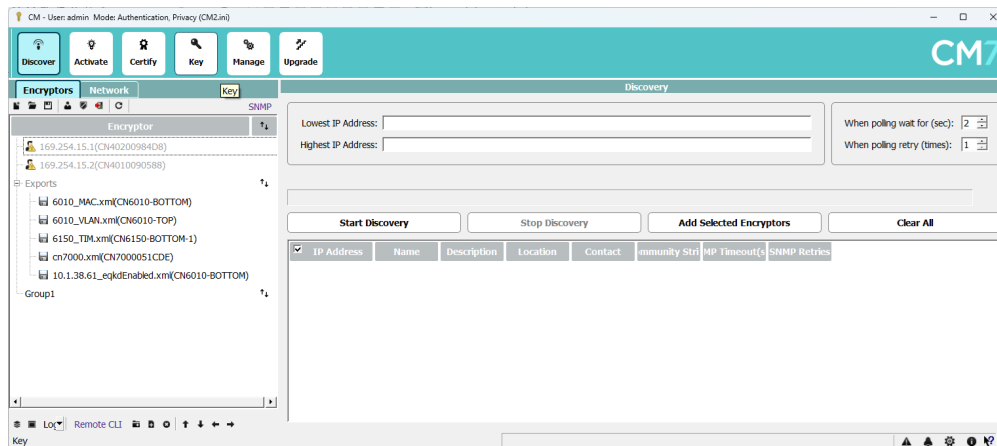


Figure 87: Discover encryptors

The polling period can be increased to allow for network delays and the number of retries can also be increased should this be necessary in noisy environments.

Configuration servers

CM7 introduced support for 'configuration servers' in version 7.5.1. Configuration servers provide access to configuration databases into which the discovered encryptors list can be saved. Having a number of defined configuration databases makes it simple for users to share access to groups of encryptors in which they have a common interest.

CM7 currently supports the open 'Redis' configuration server. However this does need to be installed separately.

Activate screen

When an encryptor is shipped it has default credentials which must be changed prior to loading certificates and configuring the unit to meet the requirements of the network. This process is referred to as 'activation'.

NOTE: Activation can also be performed using the CLI.

The default credentials comprise a single administration account named 'admin' which has a known password, '\$Password1'. The credentials will be reset to this 'factory default' state if an encryptor is 'tampered' or 'erased'.

When in the factory default (non-activated) state, the facilities for Certification are disabled and the facility to Activate is enabled. Selecting the Activate function opens the activation screen, which includes a list of the required steps.



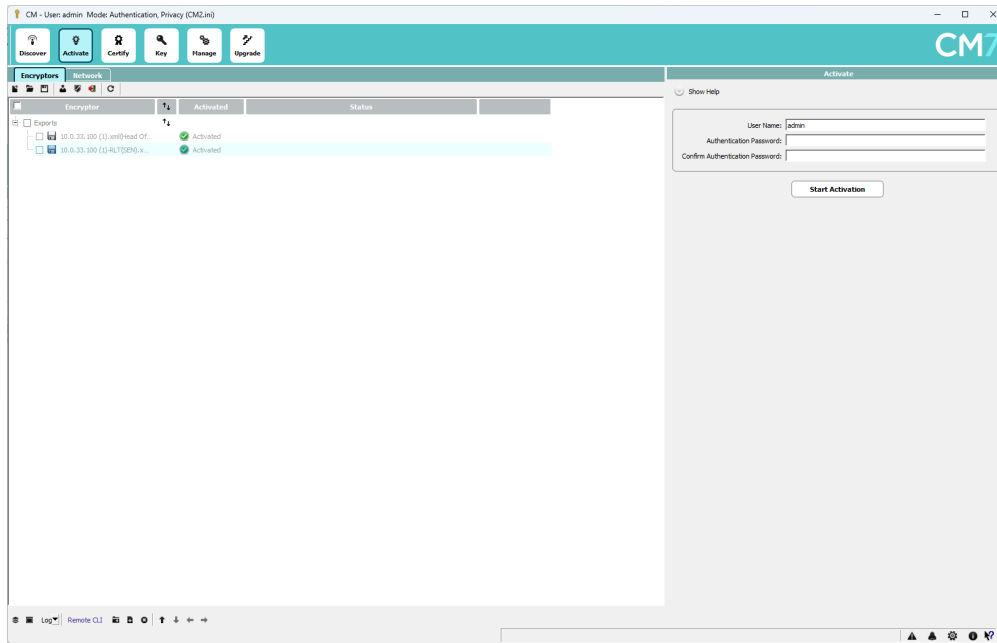


Figure 88: CM7 Activate screen

These steps are described in more detail below, with the on-screen step number identified with an [n] reference.

- Instructions are displayed as shown in Figure 89 on the next page
- The first step is to place the target encryptor in 'Activate mode'[2].
- After the encryptor has been placed in Activate mode, CM7 is used to request a CSR from the unit; this will be used as a secure medium for transferring the new credentials to the encryptor
- The hash of the retrieved CSR is compared to the hash of the encryptor [5]. This is a necessary step to prevent man-in-the-middle attacks
- The new credentials which include a valid password (which cannot be \$Password1) are entered [3] and sent to the encryptor [4]
- The hash of the CSR reloaded to the encryptor is now compared by the certifiers to the updated hash displayed by CM7 [6]. (Again, a necessary step to thwart any attempted man-in-the-middle attacks.)
- Assuming that the hashes match and the update is acknowledged then the new credentials are used to login to the activated units or continue to select and activate additional units



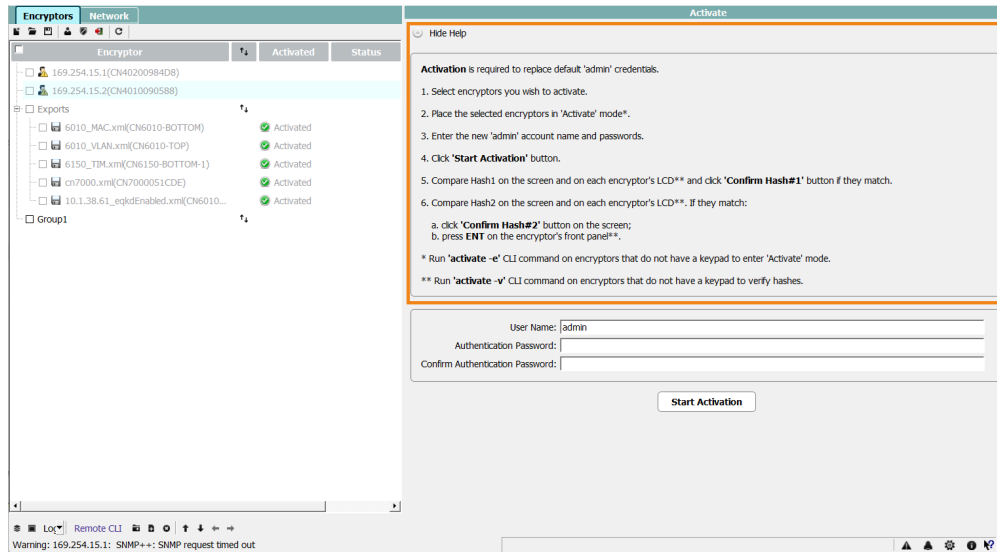


Figure 89: Activation dialog

Following activation, the certification facility is enabled and certificates signed by either CM7 or an external CA can be installed. See "Certify screen" on page 164.

NOTE: If the encryptor will operate in TIM mode then certification is not required.

Certify screen

The certification screen has two tabs, one that allows certification using the internal CA of the CM7 and the other that allows CSRs to be exported from encryptors so that they can be signed and reloaded.

CM7 supports Elliptic Curve Cryptography (ECC).

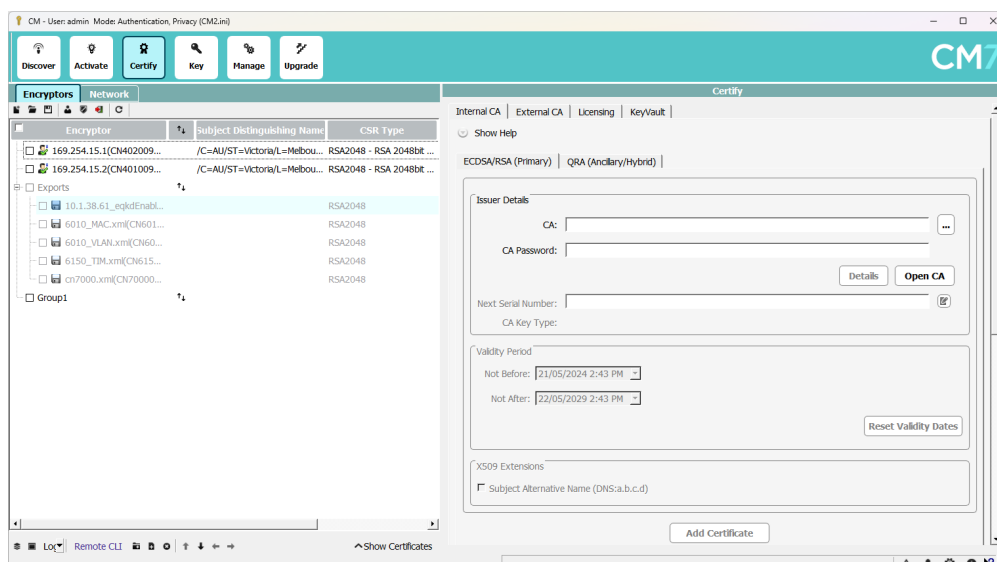


Figure 90: Licence dialog

WARNING: Certification requires administrator privileges and that the encryptor be activated.



Internal Certification

Figure 91 below shows the instructions and required fields for internal certification.

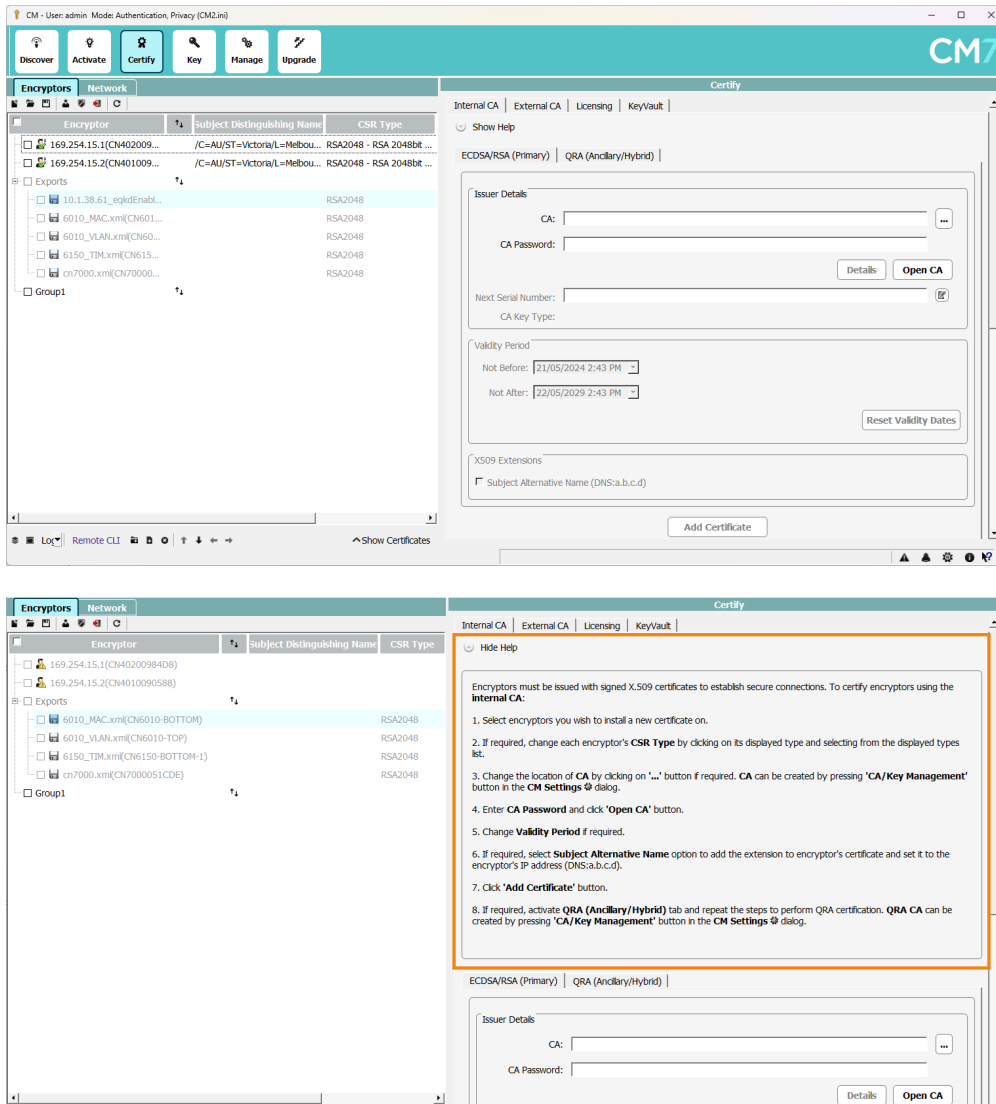


Figure 91: Internal certification

Certification requires the use of a previously created PKCS#12 file. If the PKCS#12 file is located in a file directory then the 'browse' button can be used to select it. If the PKCS#12 is located in a database on a Configuration server then the following modified dialog can be used to select the desired database.

New Certificate Details

Issuer Details

CA: CA_RSA2048

CA Password: ●●●●●●●●

Details Open CA

By default the expiration period of an encryption certificate will be set to five years. However this can be changed.

Following the selection of the encryptors that are to be certified, as shown below, the CSR Type of each unit can be changed to select one of the available elliptic curve key types rather than the default RSA 2048-bit type.

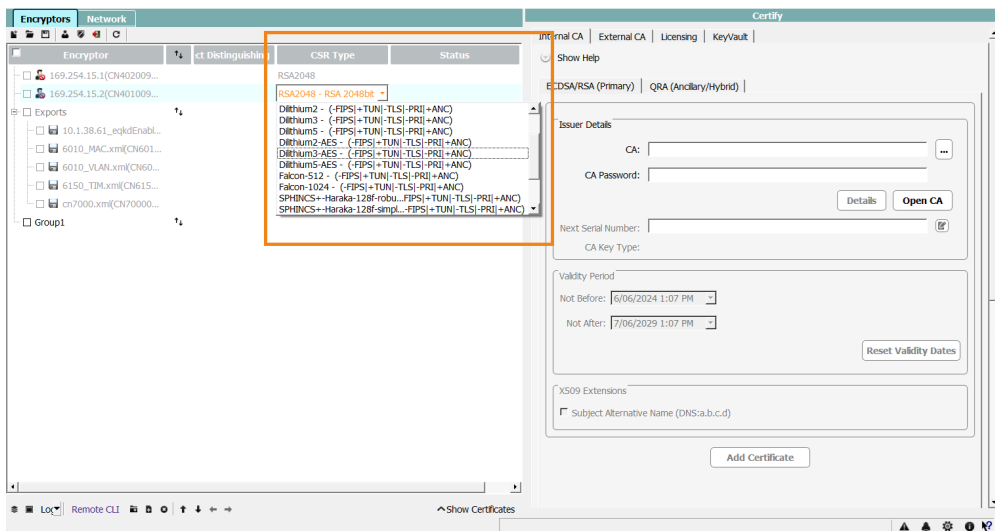


Figure 92: Selecting a different CSR Type

The required certification steps are:

- **CA file/CA** - specifies the PKCS#12 file and its location. This file can be created by CM7 or supplied by another CA.
- **CA password** - the CA password as required to sign the certificate. This is defined when the PKCS#12 file is created.
- Following entry of these details, click on the '**Open CA**' button to display the PKCS#12 details. (Refer to 'Signing behaviour', below.)
- You can click on the **Details** button to show the detail of the CA as shown in Figure 93 on the facing page.
- The **Next serial Number** field displays the serial number that will be allocated to the certificate.
- The **Validity Period** of the signed certificate defaults to one year, however, this can be extended.
- Click on **Add Certificate** to add signed certificates to each of the selected encryptors.

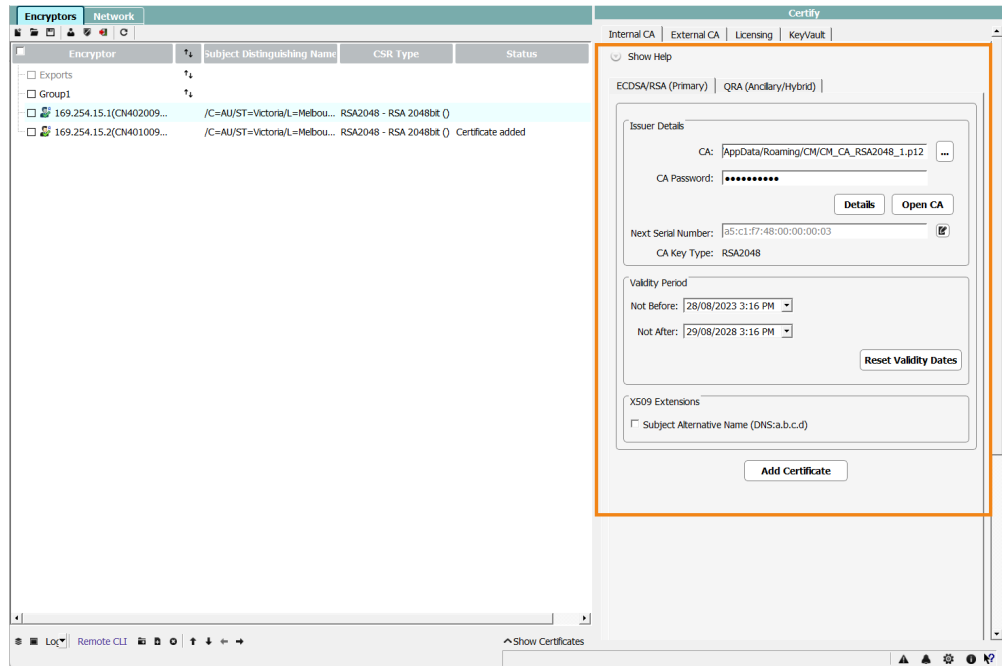


Figure 93: Certificate Authority details

After the certificates have been added, selecting an encryptor allows the "Show Certificates" button at the bottom of the screen to display the units certificate table.

Signing behaviour:

CM7 ensures that the CSR of the encryptor matches that of the Certificate Authority being used to sign it.

- **RSA CA:** If the CSR of the encryptor does not match that of the CA it will be set to that type. CM7 will not reset the encryptors type, it will remain an RSA type. If the encryptors type is already RSA, it will not be modified.
- **Elliptic Curve CA:** If the CSR of the encryptor does not match that of the CA it will be set to that type. CM7 will not reset the encryptors type, it will remain an EC type. If the encryptors type is **ANY** EC it will not be changed, the CSRs do not have to match exactly.
- **QRA CA:** If the CSR of the encryptor does not match that of the CA exactly it will be set to the CSR of the CA; the encryptor CSR must match the CA CSR EXACTLY. CM7 will not reset the encryptor type; it will stay as the QRA type of the CA. If the CSR type of the encryptor exactly matches that of the CA, it will not be modified.

External certification

Figure 94 on the next page shows the instructions for external certification.



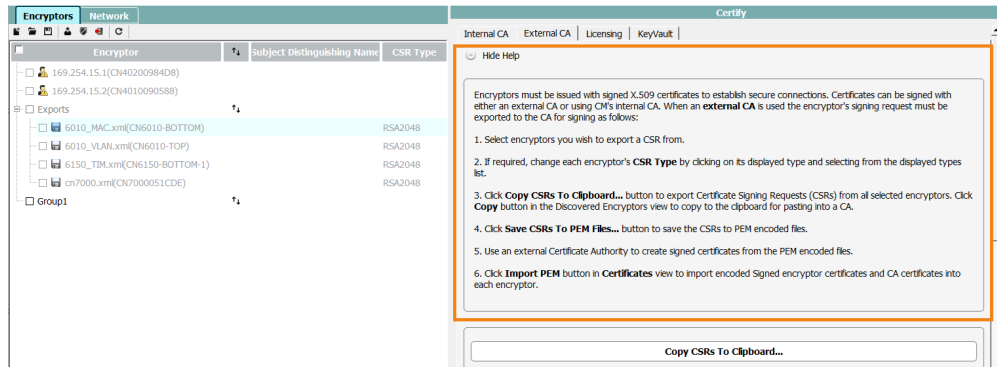


Figure 94: External certification

Copy CSRs to Clipboard - used to retrieve a CSR from the encryption and copy it to the clipboard from where it can be sent to the external certificate authority. Selecting the copy function displays a 'Copy' button which must be selected to perform the function.

Save CSRs to PEM Files - used to retrieve and save a CSR into a PEM file for subsequent use by the external CA.

CM7 Licensing pane

When the CM7 licensing screen is selected the instructions and fields shown in Figure 95 below are displayed. As described in the following sections there are two forms of license available; licenses that are signed by Senetas, and licenses that are signed by a third party.

Senetas signed licenses

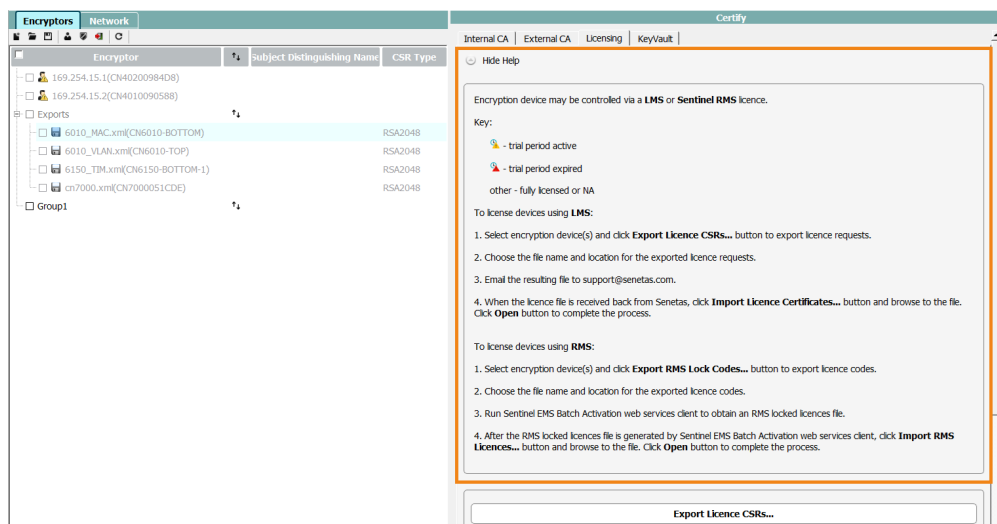


Figure 95: Licence dialog

Export Licence CSRs - allows the exporting of an encryption CSR that will be sent to the appropriate company or agency for signing.

Follow these steps to obtain signed licences:

1. Export licence information using the “Export Licence CSRs...” button on the Licensing tab of the CM7 Certify screen.
2. Forward the exported licences to: support@senetas.com
3. “Export Licence CSRs...” from CM7 and then supply them to the address provided.
4. The signed licences will be shared with you via Suredrop.
5. Upload the signed certificates to the Encryptor using the “Import Licence Certificates...” button on the Licensing tab of the CM7 Certify screen.

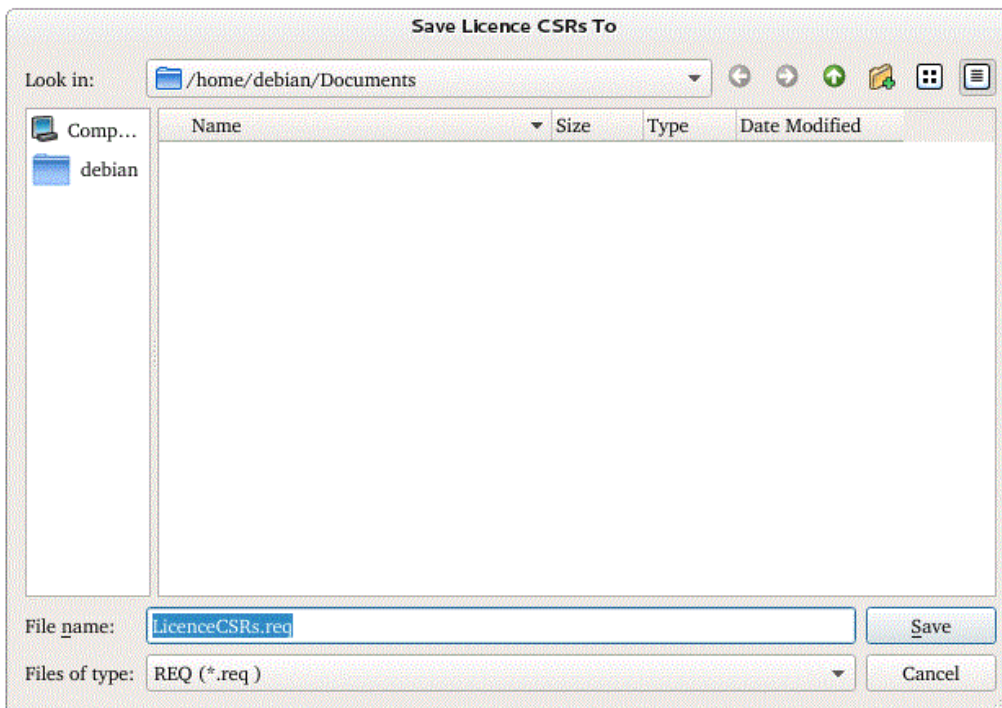


Figure 96: Exporting a licence CSR

Import Licence Certificates - allows the loading of a signed licence file to the encryptor. The dialog is as follows:

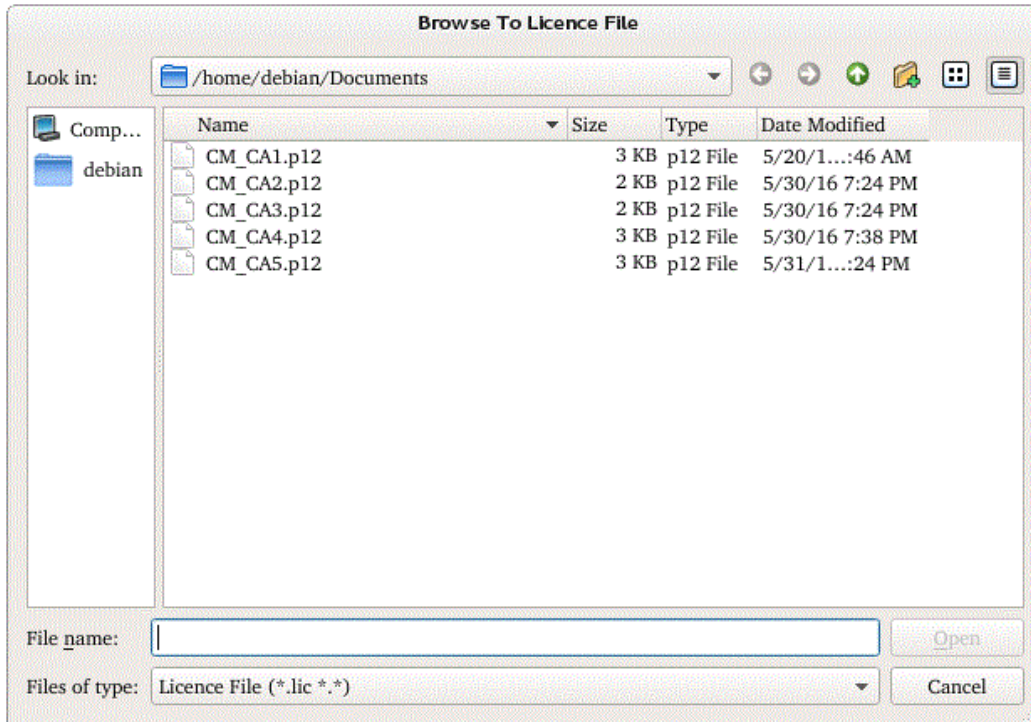


Figure 97: Importing a signed licence

KeyVault

CM7 can be used to sign certificates from credentials held within a key vault. This functionality is accessed using the CM7 Certification button and then the Certify tab as shown below.

NOTE: KeyVault is not supported on multi-slot encryptors.

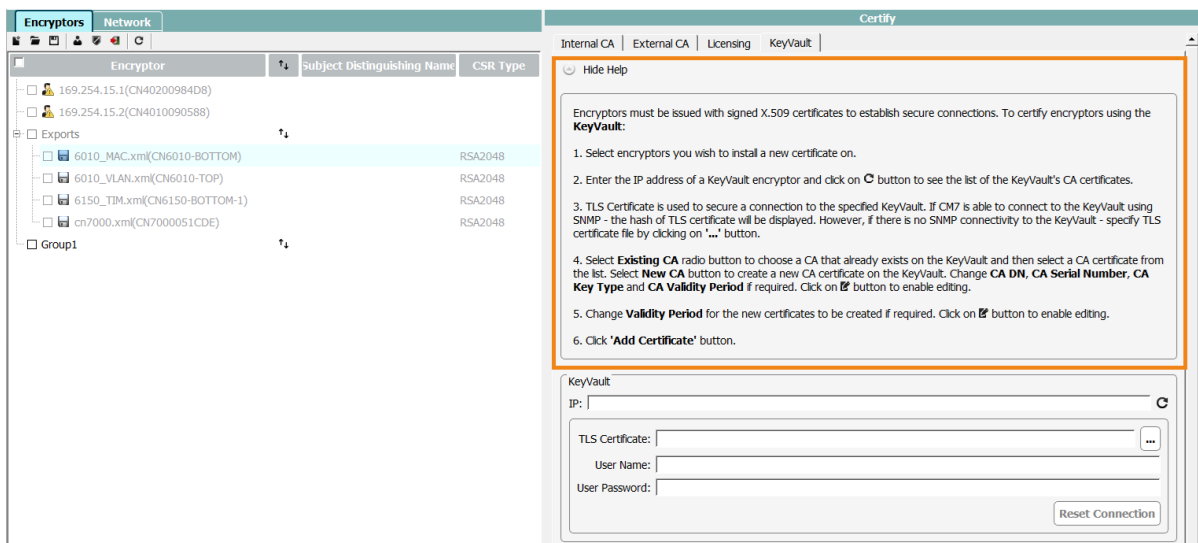


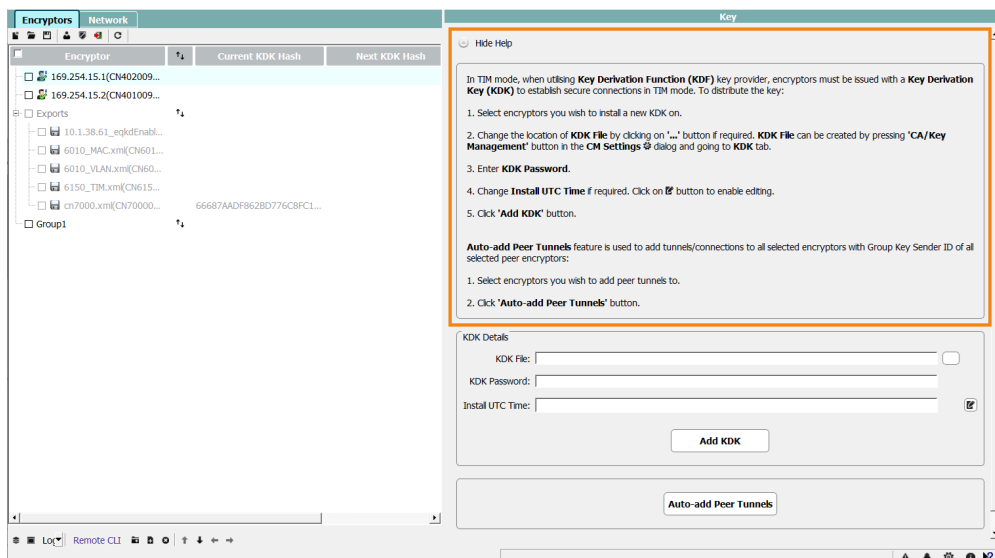
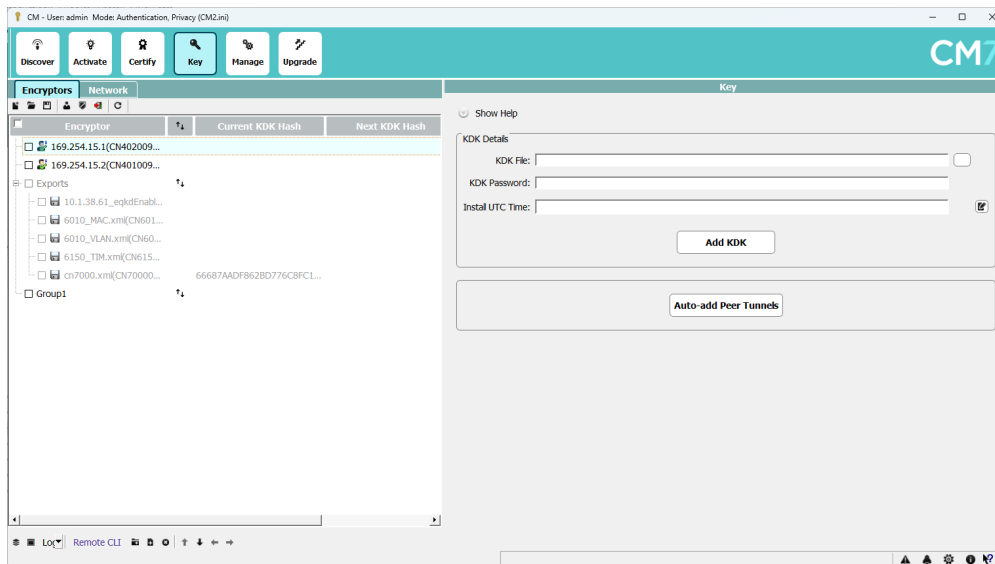
Figure 98: Signing Certificates with KeyVault

The required steps are shown at the top of the screen.

Key Screen (only layer 3/4)

In order to establish secure connections TIM mode encryptors operating in KDF mode must be provisioned with a key derivation key (KDK). These keys will have been created within CM7 using the KDK generation process described on page 155

To initiate key distribution select the 'Key' button at the top left of the screen to display the available encryptors and the following dialog.



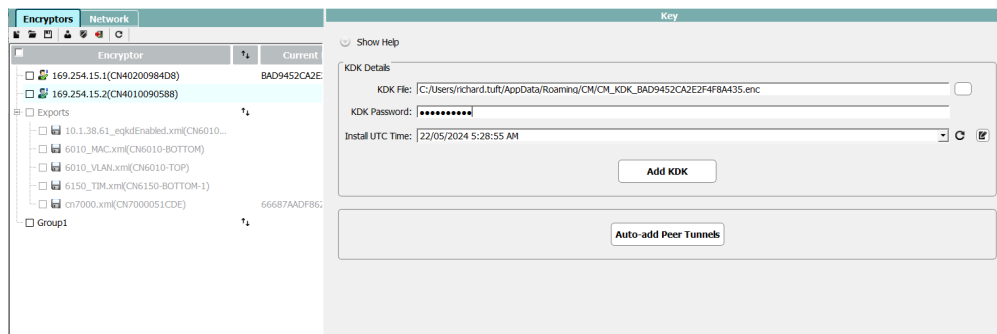
NOTE: By default the last KDK key file that was created will be selected, however you can use the browse button to select any others that may exist.

The assigned Password must be entered to open the file.

If the Key is to be applied immediately then the **Install UTC Time** selector should be left blank. If the Key is to be applied at a later specified time then the selector can be used to select the required Date/Time.

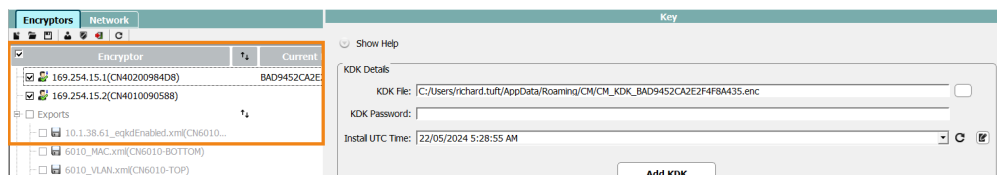
NOTE: The edit button to the right of the selector can be used to clear the selector.





Prior to selecting the **Add KDK** button, the required encryptions should be selected in the Encryptions list.

NOTE: The checkbox at the top left can be used to select or clear all of the available TIM mode units in the list.

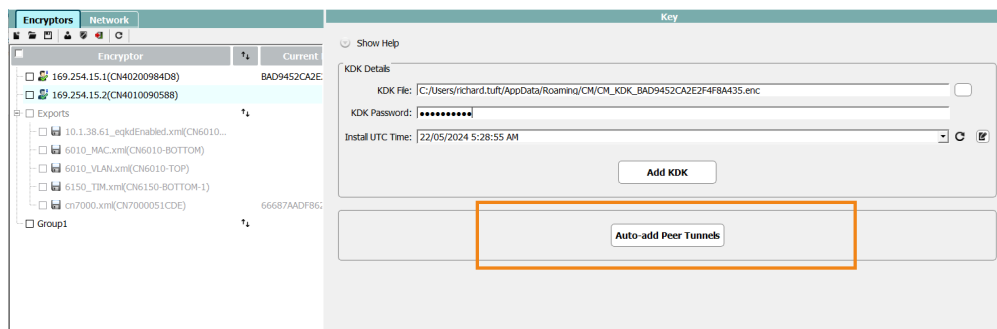


Following key distribution, the display will show a hash of the Current key in use and also if specified a hash of the key that will be in use following the scheduled update.

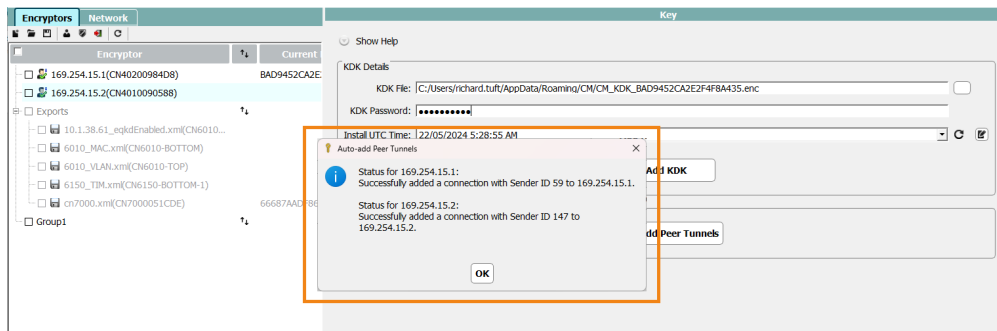
NOTE: If the 'UTC Time' field was left blank, connections to the encryption will restart using the new key. If the key generation defaults are left in place, the displayed hashes can be matched with the KDK key file names to identify the file used for distribution.

Auto-add Peers

You can create tunnels between two or more encryptions by clicking on the **Auto-add Peer Tunnels** button.



If appropriate pairs of encryptions are available, network tunnels will be created between them.

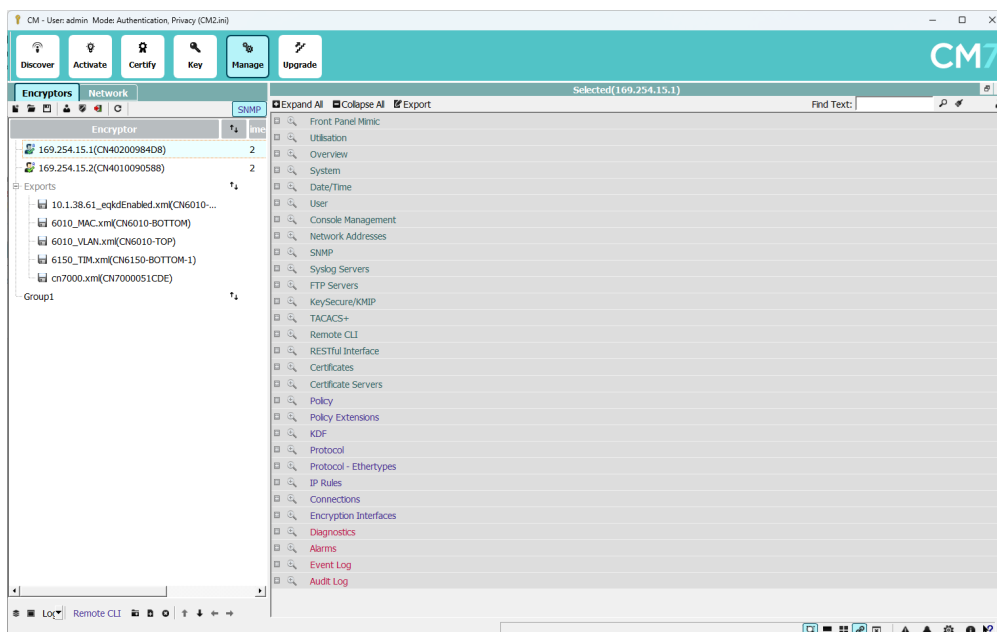


Manage screen

Selecting the Manage icon and double clicking the desired encryptor within the navigation pane displays all the available information and configuration items as shown in the following figure(s). The items can be expanded either individually by selecting them, or all items can be expanded or collapsed using the selectors at the top of the list. The magnifier icon can be used to display an item in full screen mode. Each of the available options are described in the sections that follow, note however that depending upon the encryptors current configuration, not all of the listed options may appear.

The Export button can be used to export the selected encryptors configuration so that it can be shared with support personnel should assistance be required in resolving installation or operational issues. The file does not contain any sensitive information such as user names and credentials, etc. Note that the file will contain the IPv4 address of the encryptor and this should be obfuscated if it is deemed sensitive.

The 'Find Text:' field at the top of the screen allows you to locate options using their field names. For example, entering 'IP Address' and clicking the Enter key or the magnifier would expand and display all of the panes that contain that text with the matching options highlighted in yellow. The entry text is case insensitive and the brush next to the magnifier clears the selection.



Global configuration settings must be identical on all encryptors within a logically connected network. It is recommended that CM7 encryptor grouping be used so that color coding can be used to quickly identify settings that differ.

Management options

Each of the configuration group panes has a header that provides icons related to the details being displayed. These may differ from pane to pane since not all of them are applicable to all groups.



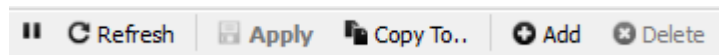


Figure 99: Configuration options

The **'Pause'** button can be used to inhibit or enable the periodic update of the screen. This is useful when comparing data such as network frame counts, etc.

The **'Refresh'** button is used to force an update of the screen data. This can be used to request an update ahead of the periodic refresh.

The **'Apply'** button is used to save any pending changes that you have made to the encryptor. This is required if those changes are to be retained.

The **'Copy To..'** button displays a list of peer encryptors and allows you to select those that you want to copy this panes settings to. This is used for User accounts, server setup, etc.

The **'Add'** button is used to create additional entries in the pane. This applies to all multi-line panes such as Servers, user accounts, etc.

The **'Delete'** button is used to delete selected entries from the pane. It is used to remove unwanted user accounts, certificates, etc.

When changes have been made and the Apply button has not been used, a **'Discard'** button is also displayed so that the entry can be cancelled.



Right clicking within a configuration group's pane displays up a pop-up menu containing the available options particular to that configuration group.

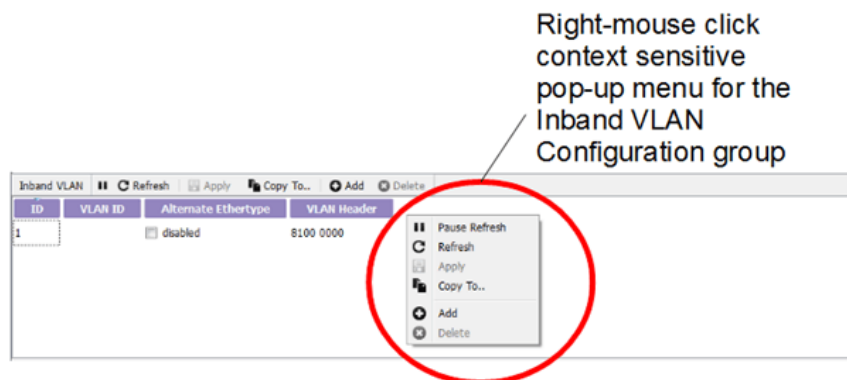


Figure 100: Group configuration options

NOTE: The available options in the pop-up menu are the same as the icons on the Group Configuration Pane. If a menu item is disabled then it is not applicable.

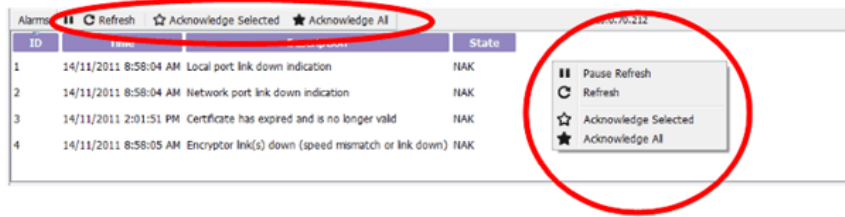


Figure 101: Common options

When changes have been made to the content of a pane, the 'Apply' and 'Discard' buttons will remain colored until one of these is selected. If you exit from the management functions without doing this, the following screen will be displayed to remind you of the pending changes.

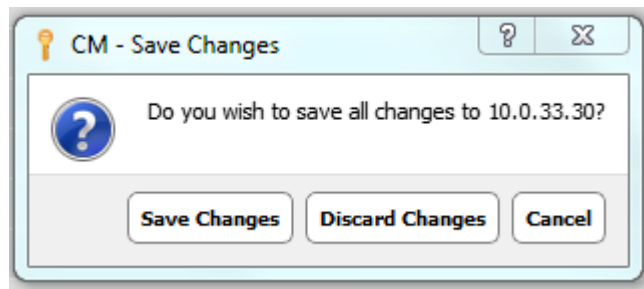


Figure 102: Save changes dialog

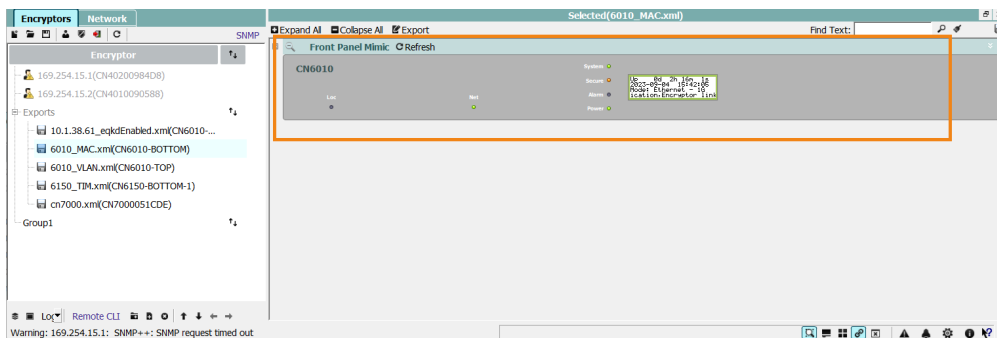
Some of the elements that are unique to a particular pane are highlighted within the relevant sections that follow.

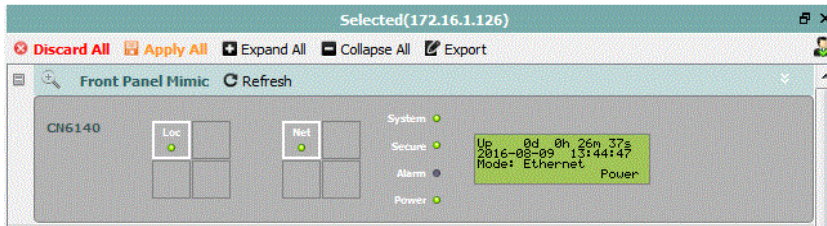
The options displayed can vary depending upon the type of encryptor selected and the 'Hide Not applicable Setting' option. See "Configuring CM7" on page 140

Front panel mimic

The Front Panel Mimic selector displays in a simplified way the current status of the front panel of an encryptor. While the actual content depends on the model and encryptor type, the content of the LCD display, and the state of all of the current LEDs is usually included.

NOTE: The images included in this manual are representative of the encryptor family.





When an encryptor has multi-slot capability and a slot is being managed the mimic shows a border around the selected slot.

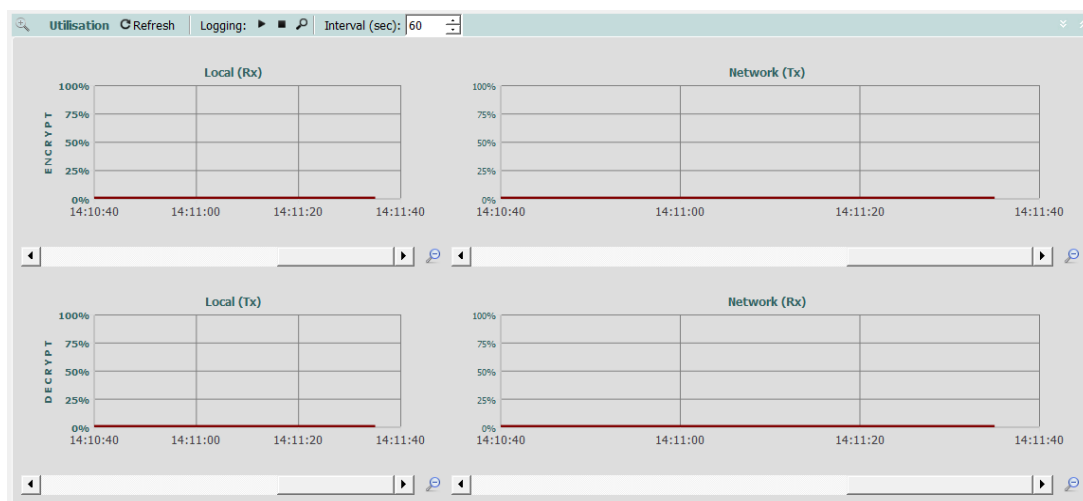
The alarm line of the display, adjacent to the Alarm LED, has a character indicating the state of each slot:

- '!' indicates an unacknowledged alarm
- '*!' an acknowledged alarm
- '^' an inactive, unacknowledged alarm.



Utilization

The Utilization pane displays graphics that include metrics for the traffic flowing through both the ingress and egress ports in both directions.



The **Logging** selectors at the top of the screen can be used to enable or disable a 'Long term logging' facility that facilitates the monitoring of utilisation statistics over longer periods of time. This feature installs a service called 'CMOidLoggerService' that runs independently of CM7, retrieving utilisation values from selected encryptors and writing them to a .csv file. SNMPv1 must be enabled for this feature to work.

Logging is enabled for a particular encryptor by clicking on the 'Logging: Start' button. The 'Logging: Stop' button will stop the logging, and the 'Logging: View' button will open a 'CM7 OID Logger' window, which will display the logged values in both a numeric and graphical format.



On Windows, once logging is opened for the first time from CM7, an icon will be added to the 'SysTray' task-bar, which will allow users to open the CM7 OID Logger by clicking on its icon in the 'SysTray'. The system tray (or 'SysTray') is a section of the task-bar in the Microsoft Windows desktop user interface that is used to display the clock and icons of certain programs so that a user is continually reminded that they are present and can easily access them.

The 'CM7 OID Logger' allows users to add any OID for long-term logging. The user is also able to right-click on any panel of the Manage window and add or remove the OIDs from that panel to the OID Logger. It is also possible to enable or disable logging for a specified IP address.

System pane

The System display provides system level information, allows authorised users to enable or disable key features and shows the status of hardware modules.

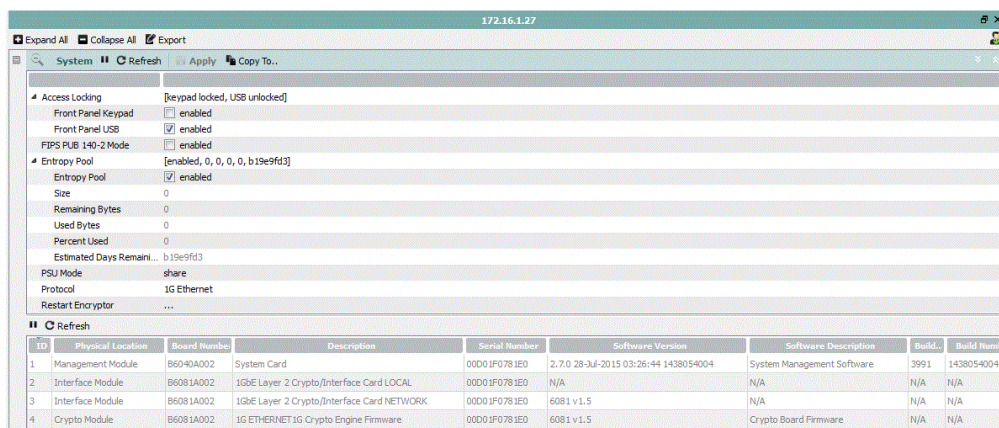


Figure 103: System display

Local Time - the date and time can be entered. These can also be updated via the **date** CLI command or if configured via the NTP server(s). See "NTP Server Configuration" on page 179 on page 184

NOTE: on page 184

Access locking

- **Front Panel keypad** - this allows the front panel to be locked so that the configuration cannot be changed
- **Front Panel USB** - this allows the USB socket to be locked so that inserted USB sticks are ignored. The USB socket must be unlocked before any firmware upgrades to be loaded

NOTE: Senetas encryptors support only USB drives that are configured with the FAT or FAT32 format.

FIPS PUB 140-3 Mode - this allows the FIPS mode of the encryptor to be enabled or disabled. By default FIPS mode is enabled.

Entropy Pool - enables/disables the use of a user-provided entropy pool in place of the hardware derived entropy of the encryptor.

- Size - total size of the entry pool in bytes
- Bytes remaining - remaining bytes before pool is exhausted
- Bytes used - bytes consumed to date



- Estimated days remaining - based on current consumption rate over previous days (7 days rolling), allow 24 hours for initial calculation

Restart Encryptor - this allows the encryptor to be restarted with an option to first erase the unit. A warning dialog is displayed to allow confirmation. Following a non-erase restart, the unit will re-establish connections based on the current mode and policy settings.

Management Module - provides details of the encryptor management module

- **ID** - identifies the unit within the encryptor
- **Physical Location** - describes the module location
- **Board Number** - identifies the module type by manufacturing code
- **Description** - a functional description of the module
- **Serial Number** - the serial number of the module
- **Software version** - the version of software loaded into the module
- **Software description** - a functional description of the software
- **Build ID** - the build identifier the software
- **Build Number** - the sequence of the build
- **Build Date And Time** - the date and time the build was performed

Interface Module - provides details of the **network** interface module of the encryptor

- refer to descriptions above

Interface Module - provides details of the **local** interface module of the encryptor

- refer to descriptions above

Date/Time pane

The Date and Time display shows the current date and time and the time zone and allows these to be set either directly or from the clock of the management system.

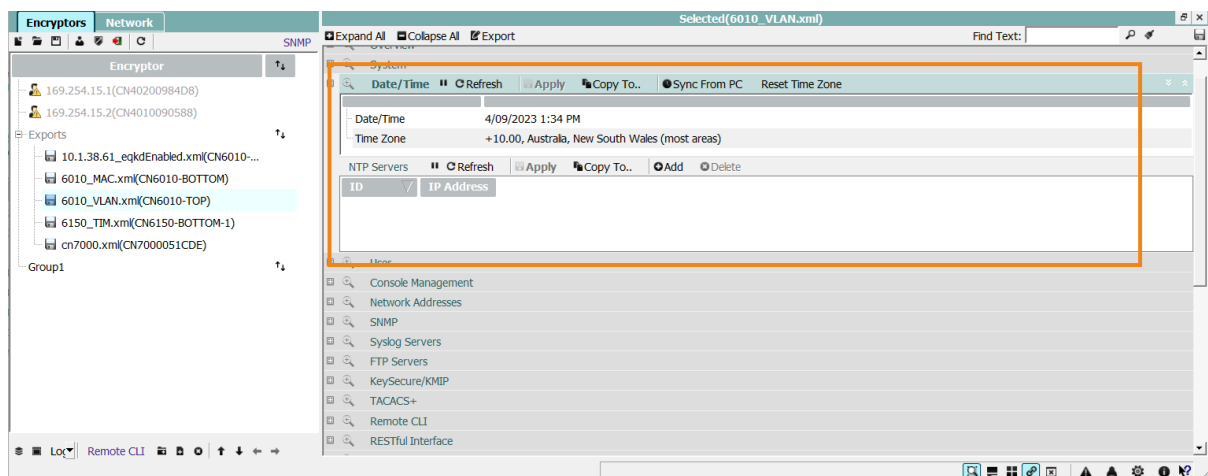


Figure 104: Date and Time setup



Local Time - the date and time can be entered. These can also be updated via the **date** CLI command or, if configured, via the NTP server(s).

NOTE: The date and time format will be determined by the settings of the platform that CM7 is running on.

Time Zone - the time zone that the encryptor is located in.

Time Zones

The advantage of using time zones is that it allows encryptors in different zones to display their local time while providing synchronised UTC event logging in Syslog servers. It is recommended that, if used, the time zones are set prior to setting the local time on the encryptor because setting a time zone other than UTC applies the offset to the current local time. This might require that the local time be reset.

If the time is set using the “Set Time From PC” button, it is assumed that the PC and encryptor are in the same timezone; if they differ the correct Local Time must be entered manually.

NTP Server Configuration

The NTP Server Configuration option allows an administrator to configure up to 10 NTP servers.

The Add button is used to add an additional NTP server to the configuration. The IPv4 or IPv6 address is entered into the address box and the Apply button pressed to save the entry.

The Delete button can be used to remove a selected address from the list.

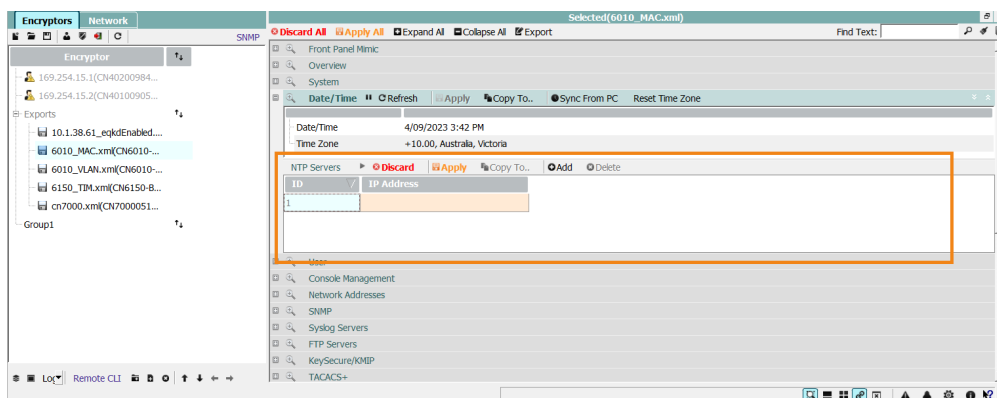


Figure 105: NTP configuration

ID - the index of the NTP server. Used when editing server parameters using the CLI.

IP Address - the IP address of the server in dotted notation form; an IPv4 example being 178.12.3.1. This is used by the encryptor to contact the server.

NTP overview

NTP servers can be defined such that all client encryptors have their date and time synchronised.

NTP servers use the RFC1305 (without authkey) message format.

Unless enabled by the definition of NTP server addresses, the facility is disabled. This is the default.

When enabled, Audit log, Event log, and if configured, Syslog entries are stamped using a date and time derived from external NTP servers.



NOTE: NTP servers provide the most accurate way of synchronising the date and time across all encryptors within the network. In instances where NTP servers are not available, encryptor date and time will be maintained by each encryptors real time clock and this is adequate for most purposes. The real benefit of using NTP servers is when you are also configuring syslog servers and you want the date and time to be synchronised with other network devices.

User

The User configuration selector allows you to examine and modify the access controls associated with users. When shipped, an encryptor has a single administrator account that has the admin/\$Password1 credentials. If the unit is erased or tampered with then these are re-established.

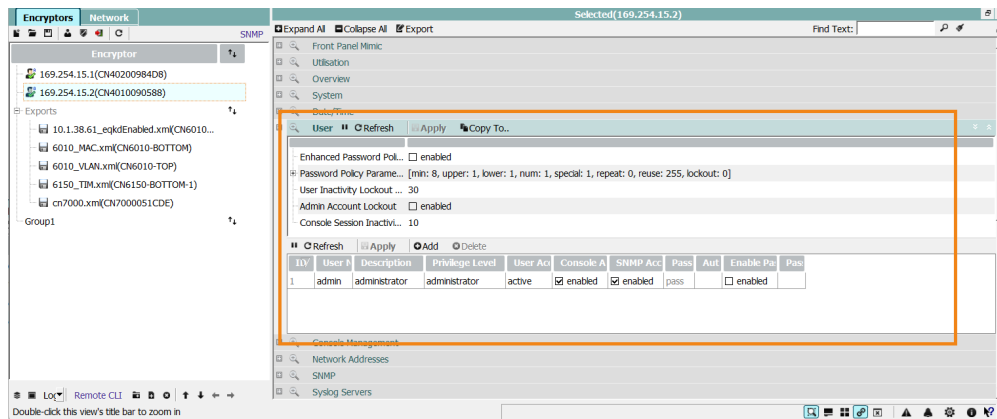


Figure 106: User access control

The top section of the screen has the fields that are common to all users. These include password policy and inactivity lockout.

Default Password Behaviour

Upon startup of a new (or freshly erased) Encryptr, the user will be presented with a single admin user, with a default password.

In this unactivated state, the admin user is allowed to:

- activate the Encryptr - by setting a new password
- enable the Enhanced Password mode features
- modify the Password Policy parameters
- modify the User Inactivity Lockout Period

NOTE: Users cannot be created until the Encryptr has been activated.

Password Policy Parameters

The default Password Policy Parameters are shown in the table below.

Requirement	Default Value
Minimum Password Length	8
Minimum of Uppercase Characters	1
Minimum of Lowercase Characters	1



Requirement	Default Value
Minimum of Numeric Characters	1
Minimum of Special Characters	1
Minimum of Consecutive Repeat Characters	0
Reuse History	255
Change Lockout Period	0

Enhanced Password Mode is disabled by default. When enabled, the following functionality applies:

- User lockout if 2 unsuccessful attempts within an hour
- Password lexical checking at login
- Logging of failed login attempts
- Disallowing of matching password and UserID
- Password expiry for users on CLI and SNMP/RESTful

NOTE: This setting can only be modified using an administrator account irrespective of the activated state of the encryptor.

The lower section of the screen has a single line entry for each of the user accounts. Up to 30 accounts can exist and accounts can be added and deleted or selected for editing. The fields are:

- **User Name** - short form name used as login ID
- **Description** - a long form of the user name that is used for reporting purposes
- **Privilege level** - the assigned authority level of the user: Administrator, Supervisor, Operator, or Maintainer
- **User Account** - defines status, active or disabled
- **Console Access** - enabled or disabled to specify whether CLI access is allowed
- **SNMP Access** - enabled or disabled to specify if SNMP management access is allowed

Console Management

The Console Management display allows you to update the information that will be displayed when the CLI is used.



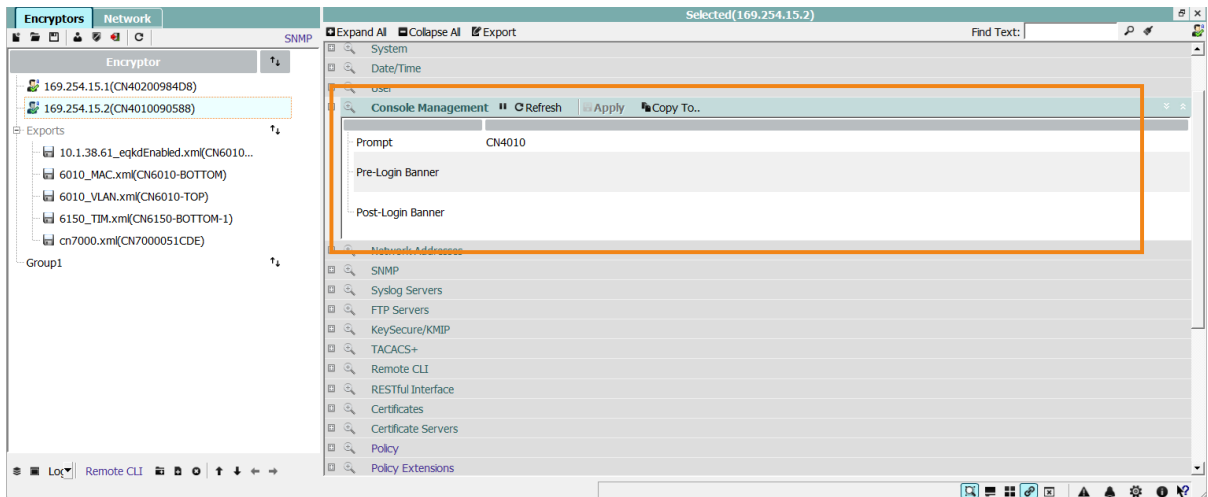


Figure 107: Console messages

Pre-Login Banner - The message that will be displayed on the terminal screen prior to the user logging into the encryptor. This will typically be used to advise the user of security requirements, etc.

Post-Login Banner - The message that will be displayed on the terminal screen after the user logs in. Typically this message reinforces the security requirements, for example, advising the user not to leave their terminal unattended.

Prompt - the text that will be displayed ahead of the '>' symbol as the prompt for user input on the CLI. Typically this would be the encryptor model and/or location.

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

Network addresses

The Network Addresses selector allows you to define the addresses that are used by SNMP to communicate with the encryptor. The front panel address can have both IPv4 and IPv6 addresses.

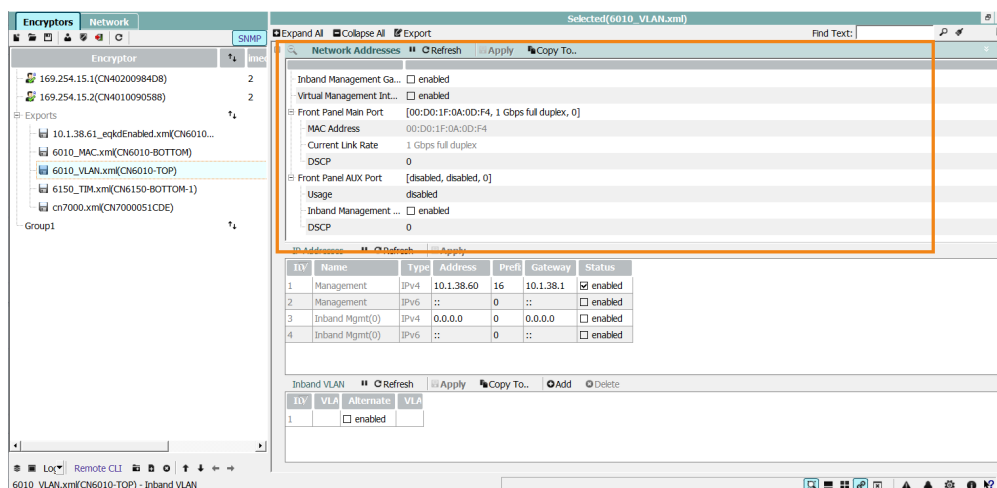


Figure 108: Network addresses

The display has three sections; the top allows the inband gateway functionality of the encryptor to be enabled or disabled and shows the front panel NIC address and operation mode. The fields are as follows:



- **Inband Management Gateway** - when enabled, the encryptor will operate as an inband gateway that allows the management of configured remote encryptors
- **Front Panel Main Port** - the physical address of the primary front panel port
- **Front Panel Aux Port** - the physical address of the auxiliary front panel port

The second section of the display shows the available IP addresses including IPv4 and IPv6 addresses for the front panel port, management and inband management ports. Each of these can be edited by selecting the required field, making the change and clicking 'Apply'.

The screenshot shows the 'Encryptions Network' configuration window. The 'IP Addresses' section is highlighted with an orange box. It contains a table with the following data:

ID	Name	Type	Address	Prefix	Gateway	Status
1	Management	IPv4	10.1.38.146	16	10.1.1.254	<input checked="" type="checkbox"/> enabled
2	Management	IPv6	::	0	::	<input type="checkbox"/> enabled
3	Inband Mgmt(0)	IPv4	0.0.0.0	0	0.0.0.0	<input type="checkbox"/> enabled
4	Inband Mgmt(0)	IPv6	::	0	::	<input type="checkbox"/> enabled
5	Aux Mgmt	IPv4	10.1.38.246	16	10.1.1.254	<input checked="" type="checkbox"/> enabled
6	Aux Mgmt	IPv6	::	0	::	<input type="checkbox"/> enabled
7	Inband Aux(0)	IPv4	0.0.0.0	0	0.0.0.0	<input type="checkbox"/> enabled
8	Inband Aux(0)	IPv6	::	0	::	<input type="checkbox"/> enabled

Below the table is the 'Inband VLAN' section, which is also highlighted with an orange box. It contains a table with the following data:

ID	VLAN ID	Alternate Ethertype	VLAN Header
1		<input type="checkbox"/>	enabled

The fields are:

- **Address** - the IP address of the encryptor in 'dotted' (CIDR) notation
- **Prefix** - the network mask that applies to the IP address
- **Gateway** - the gateway address
- **Status** - set to enabled or disabled to allow access to the address

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.

The screenshot shows the 'Encryptions Network' configuration window. The 'Inband VLAN' section is highlighted with an orange box. It contains a table with the following data:

ID	VLAN ID	Alternate Ethertype	VLAN Header
1		<input type="checkbox"/>	enabled

NOTE: Inband management within VLAN (VPLS) networks requires that at least one entry be present. The untagged entry exists by default however additional entries may be required. Refer to the CLI **inband_vlan** command for details.



SNMP

The SNMP selector allows you to set SNMP management parameters and define the addresses that the encryptor will send SNMP trap messages to. Up to 8 addresses can be defined and each of these can be individually enabled or disabled.

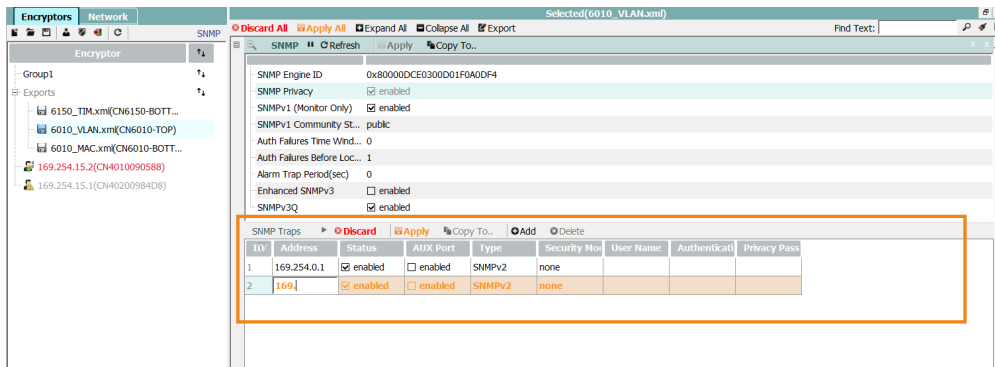


Figure 109: SNMP trap configuration

The upper section of the display is used for SNMP management parameters:

SNMP Privacy - by default SNMP privacy is enabled which means that traffic between CM7 and the encryptor is encrypted.

SNMPv1 (Monitor Only) - when enabled, SNMPv1 can be used to monitor, not manage, the status of the encryptor. By default this is disabled and only SNMPv3 can be used to manage the encryptor via the front panel.

SNMPv1 Community String - configures the SNMPv1 community string used to authenticate clients during SNMPv1 access and to identify sent trap messages. Changing the string will log an audit message. A reboot is required for the new value to take effect.

Auth Failures Time Window - sets the time in minutes for which a user will be locked out on consecutive authentication failures. This feature is only operational for SNMPv3 AUTHPRIV.

Auth Failures Before Lockout - sets the number of consecutive SNMPv3 AUTHPRIV failures that will result in the user being locked out for the Auth Failures Time Window.

Alarm Trap period - specifies the period in seconds between traps sent for active unacknowledged alarms. A value of 0 specifies that a trap will only be sent when the alarm becomes active and not periodically.

The lower section is used to define up to 8 SNMP trap receivers. CM7 can itself be defined as a trap receiver, however for these to be received CM7 must be enabled as a listener. See "CM7 Settings" on page 140.

Address - the IP address of the SNMP receiver

Status - set to enable or disable the receiver

Syslog Server Configuration

The Syslog Server Configuration option allows an administrator to configure up to 10 Syslog servers by specifying their IPv4 or IPv6 addresses. The facility allows centralised logging of both event and audit messages so that these can be correlated with those from other network devices. Syslog messages use the standard non-secure RFC5424 format.



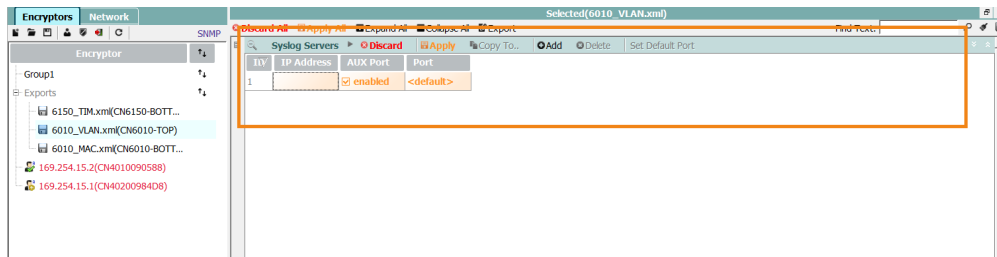


Figure 110: Syslog configuration

ID - the index of the Syslog server. This is used when editing server parameters using the CLI.

IP Address - the IP address of the server in dotted notation form; an IPv4 example being 178.12.3.1. This is used by the encryptor to contact the server.

The user supplied addresses are validated. Note that to eliminate any associated security issues, DNS lookup is not supported.

The encryptors internal audit and event logs are associated with syslog LOCAL4 and LOCAL5 facilities respectively.

Syslog servers can also be configured using the CLI as described on page .

Syslog Overview

All audit and event logs entries can be directed to external syslog servers

Unless enabled by the definition of syslog server addresses, the syslog facility is disabled. This is the default.

Syslog entries are date/time stamped using the encryptors date and time which can be derived from an external NTP server.

When Syslog is configured, the use of NTP servers is recommended.

If NTP is configured it is assumed that both Syslog and NTP server(s) exist within the same secure protected network and no additional security is required.

NOTE: Both Syslog and NTP are disabled by default and must be configured by an administrator.

CM7 Syslog Service

Upon installation of CM7 (Windows) install, a new *syslog service* (listening on port 514) starts automatically and runs in the background. The service runs regardless of whether CM7 is open or not.

NOTE: On Linux and MacOS a CM7 install doesn't start CMSyslogService, so it must be started by a user via 'CM Settings' dialogue.

The IP address of the computer running CM7 needs to be added to the table of Syslog Servers on those encryptors from which you wish to receive syslog entries.

The CMSyslogService can be started or stopped using two methods:

- via the Control Panel >> Services dialog of the operating system
- via CM7

WARNING: If the service is to be manually stopped and started via CM7, CM7 must be run with administrative privileges.



NOTE: If the button 'Stop Syslog Service' or 'Start Syslog Service' is pressed as a non-administrator user, the error message "Unable to stop CMSyslogService: administrator privileges are required." will be displayed.

When 'System syslog' is enabled and the encryptor is logging to the CM7 Syslog service, a text file beginning with 'CM7_Syslog....txt' is created, stored and appended to. Depending on your operating system, the log file is stored at:

- C:\ProgramData\Senetas' (Windows)
- /home/username/.config/Senetas folder (MacOS)

Export Syslog

If you need to share the Syslog file, use the Export Syslog button on the CM7 Settings dialog box to export the file. If no file exists, the error message "Syslog is empty - nothing to export." is shown.

Delete Syslog

To delete the 'CM7_Syslog.txt' file, 'Delete Syslog' button from CM7 'Settings' dialogue box may be used. If no file is found, the error message "Syslog is empty - nothing to delete." is displayed.

Logging interval

CM7 writes the system syslog extended logging into a new file at a set interval. The default interval is 7 days.

Using the Settings dialog box in CM7 the interval can be changed to any value between 1 and 24 days.

Filename format

The syslog file name format is as follows:

- Current File: "CM7_Syslog<StartDateTime>.txt"
- Previous File(s): "CM7_Syslog<StartDateTime>--<EndDateTime>.txt"
- (Start/EndDateTime is in the format yyyy-mm-dd_hhmmss)

The filename of the current syslog file will display the time at which it was created

A syslog file is not created until the first system syslog message is logged by the encryptor

Attempting to export or delete the syslog file during this period will result in a 'Syslog is empty...' error message

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

If the syslog file is deleted, CM7 will continue writing to the pre-existing period as an endpoint. i.e. if 6 days have elapsed during a 7 day syslog interval and the file is deleted, the newly created file will only be active for one day.

When logged in as an administrator, modifying the Syslog file interval will cause the CM7 SyslogService to be restarted and the new period applied immediately.

A new log file is only created after the next syslog message is logged.

Modifying the syslog file interval, whilst running CM7 as a non-administrator user, will not come into effect until the conclusion of the currently active period i.e. If 4 days have elapsed during a 7 day window and the syslog file interval is set to 2 days - this updated interval will not come into effect until the end of the initial 7 day period.

- This includes times when the syslog file is deleted prior to the conclusion of the initial period

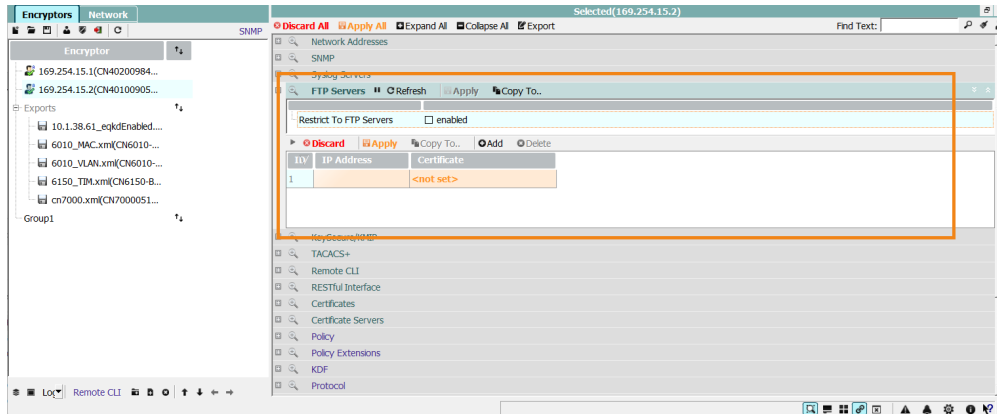


FTP/FTPS server configuration

CM7 includes an FTP server which allows users to upgrade encryptor firmware without the need for external resources.

Both the FTP and FTPS protocols are supported.

NOTE: Where remote encryptors need to be upgraded, the FTPS protocol should be used to provide a secure connection between them and the computer running CM7.



Restrict to FTP Servers - if enabled, FTP requests to IP addresses that have not been defined in the encryptors FTP Server table will be rejected.

ID - the numeric index of a configured server

IP Address - the IP address of the FTP/FTPS Server

Certificate - the Certificate

To configure an FTPS Server, an FTP Server key and certificate must be created and stored in a password-protected p12 file. This can be achieved by clicking on the 'New' button next to the 'Private Key' text box. When upgrades are initiated by a user, the FTP Server certificate is extracted from the p12 file and added to the FTP Server table on the encryptors that are being upgraded.

Caveats:

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

KeySecure

The SafeNet KeySecure Platform consists of two required components: the ProtectApp ICAPI KMIP client, and KeySecure. The client requests cryptographic operations to be performed by KeySecure through one of the Cryptographic Providers, or the XML interface. KeySecure performs all the desired operations and returns the data to the client, thus providing cryptographic functionality over the network.

The CM7 KeySecure option allows you to configure a KeySecure server so that it provides keys for an encryptor.



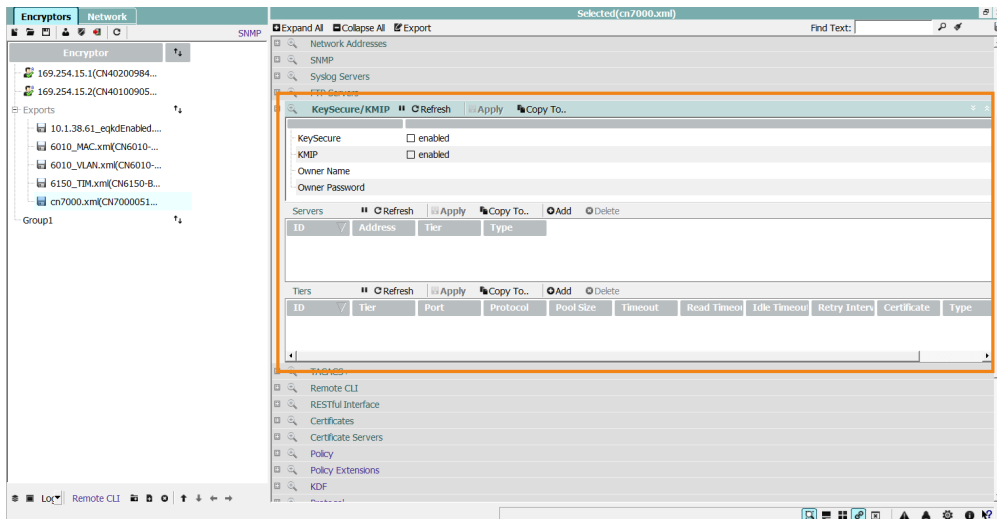


Figure 111: KeySecure configuration

- **KeySecure** - enables or disables key provision.
- **Owner Name** - the name of the client account within the KeySecure system
- **Password** - the password for the account

NOTE: When KeySecure is used with a virtual encryptor, for example the , the credentials must be re-entered each time you connect to the unit.

Up to 10 Key servers can be configured, each being added by clicking on the Add selector and entering the IP address of the server.

KeySecure tiers

The KeySecure platform provides a multi-tier load balancing feature that allows you to create up to three levels of load balancing groups, called tiers. When one tier is unreachable, the system fails over to the next tier. Unless you provide a global without a tier suffix, tiers must be configured in order, that is, you cannot have tier 3 without tier 1 and tier 2.

The fields required to define a tier are:

- **ID** -
- **Tier** - the tier number which is used to access the configuration.
- **Port** - the port number
- **Protocol** - the protocol used. This can be ssl or tcp. Connections using ssl are authenticated whereas those using tcp are not. For this reason ssl connections are recommended.
- **Pool** - the communications pool size
- **Read timeout** -
- **Idle timeout** -
- **Retry interval** -
- **Certificate** - the identifier of the certificate that will be used to authenticate the connection.



TACACS+

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

The implementation of TACACS+ includes the use of the MD5 hashing algorithm which means that when it 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.

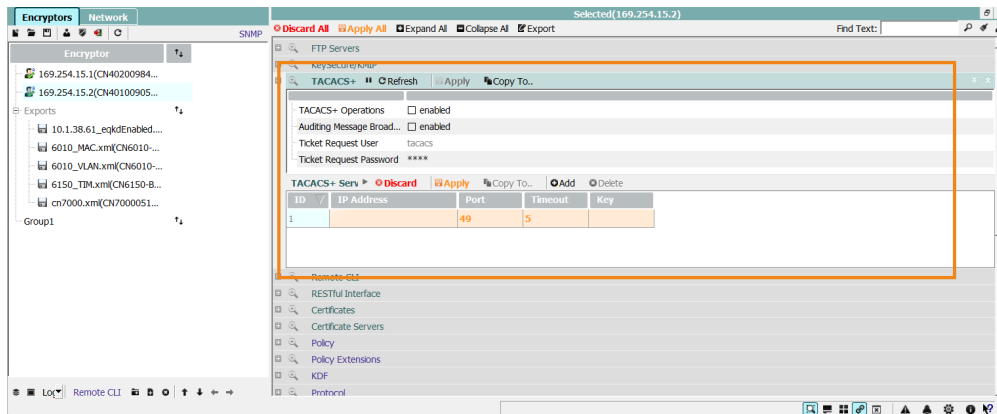


Figure 112: TACACS+ AAA configuration

The fields are as follows:

TACACS+ Operations - enable or disable global TACACS+ operation

Auditing Message Broadcast - enable or disable the broadcasting of auditing messages to all TACACS+ servers. When disabled (the default), send messages to only the active server, that is, the server that provided the authentication/authorization.

Ticket Request User - the predefined user name that will be used by CM7 to send the ticket request to the TACACS+ server.

Ticket Request Password - the password to verify that the TACACS+ connection is to be authorized based on the CM7 supplied Ticket Request password.

The lower section of the screen is used to add, edit or delete TACACS+ servers using their IP address.

TACACS+ user

Different types of users within the TACACS+ system are identified by different numbers which map to the equivalent user level of a Senetas encryptor.

TACACS+ user level	Senetas HSE user identifier
15	Admin
10	Supervisor
5	Operator
3	Upgrader

Remote Secure Shell CLI access

The Command Line Interface (CLI) is accessible via a remote secure shell (SSH) facility which provides management functions similar to those provided by the CM7. SSH is disabled by default and must be enabled using the CM7 interface shown above or via the local/physical CLI.



NOTE: A maximum of 10 concurrent remote CLI sessions are supported.

The ability to remotely manage an encryptor via SSH facilitates remote scripting by the user for the purposes of configuring/certifying the devices as well as verifying current configuration status and general health monitoring.

Prior to enabling CLI access, an SSH key pair must be generated and the Public Key added to each of the required encryptors.

SSH key pair creation

The public/private key pair that is required for SSH authentication can be generated using the Remote CLI pane of the CM7 interface.

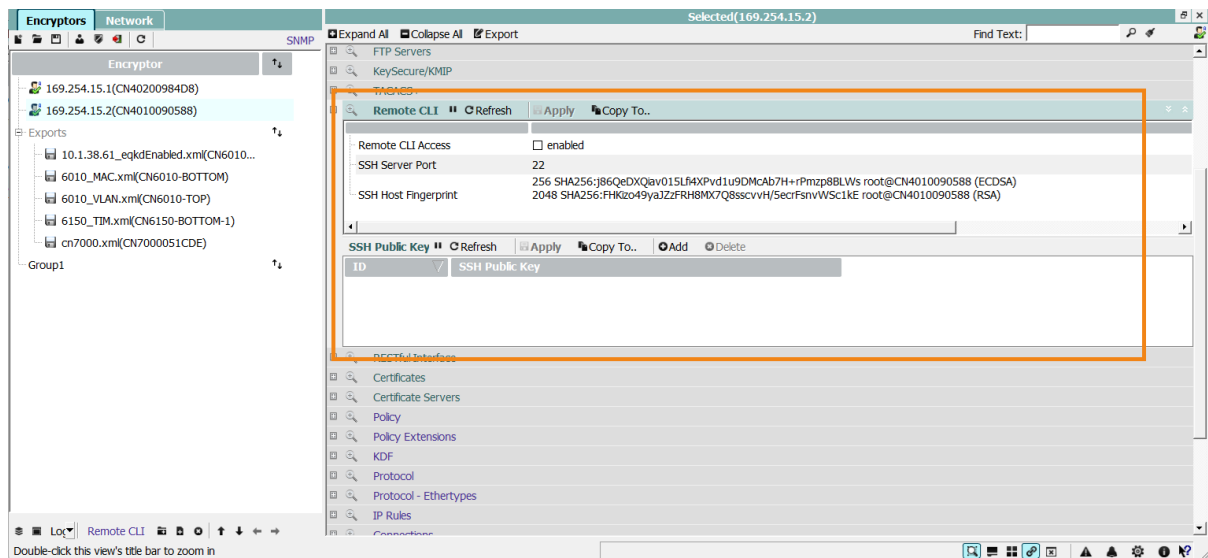
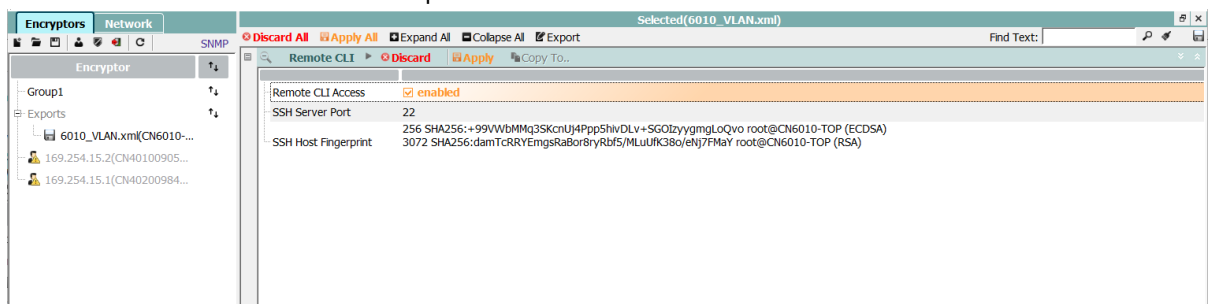


Figure 113: CM7 Remote CLI pane

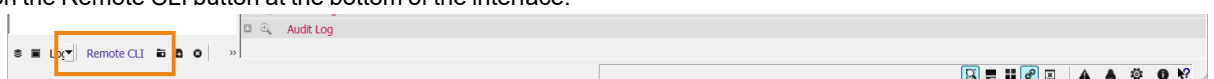
NOTE: Only ECDSA keypairs are valid for SSH use.

To enable CLI Access on an encryptor perform the following:

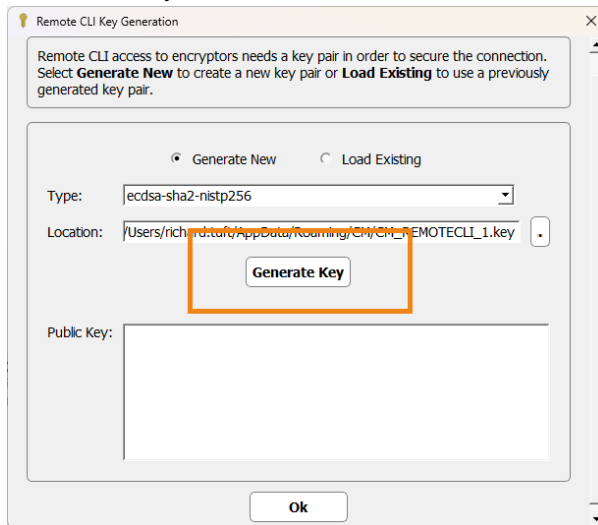
1. Open CM7, connect to the encryptor and navigate to the Remote CLI pane.
2. Enable Remote CLI Access and check that the port is 22.



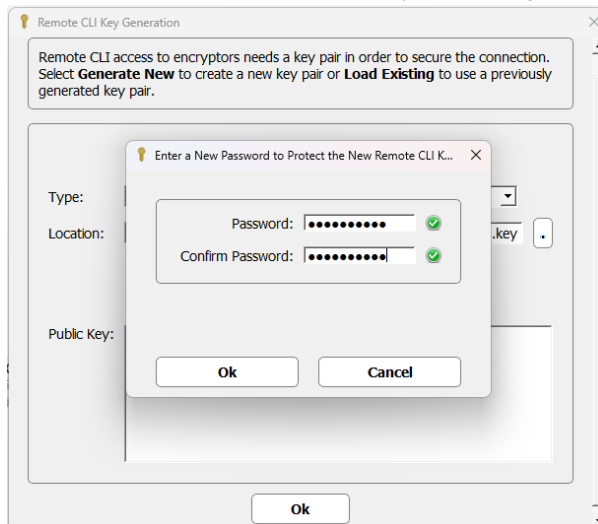
3. Click on the Remote CLI button at the bottom of the interface.



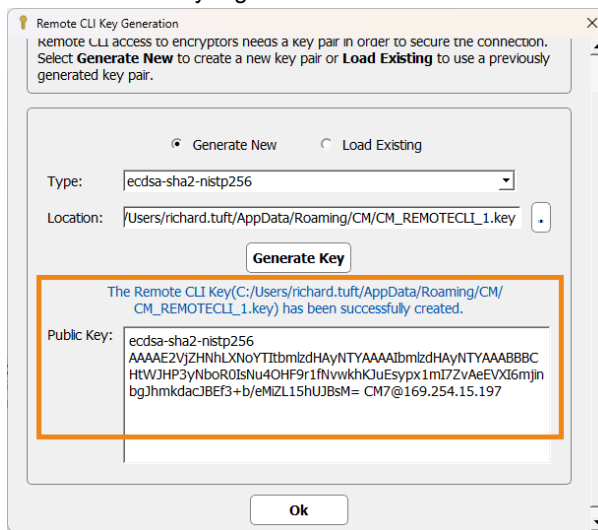
- A Remote CLI Key Generation dialog window is displayed.
- Click the Generate Key button.



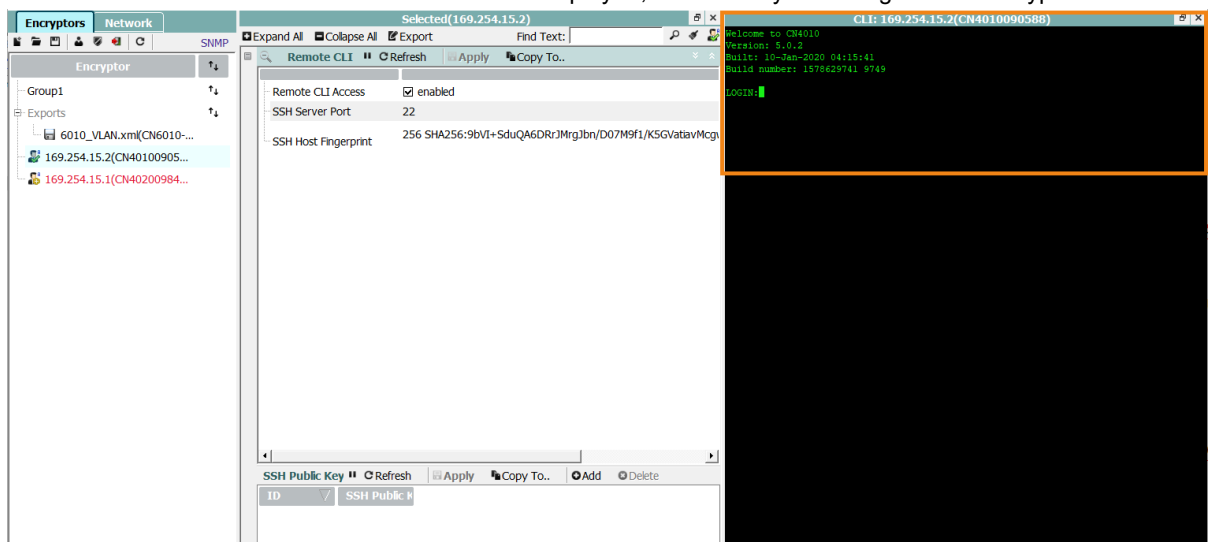
- Enter and then confirm a password for the key via a dialog window similar to that shown below.



7. Click OK and a Public Key is generated and saved.



8. Click the OK button and a terminal session window will be displayed, from which you can login to the encryptor.



NOTE: The Remote CLI in CM7 has been upgraded from a text editor to a full terminal with emulator capabilities.

Certificates

The CM7 Certificates option allows you to view existing certificates (and Import PEM), delete certificates, or set an EN certificate as the default.

NOTE: 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.



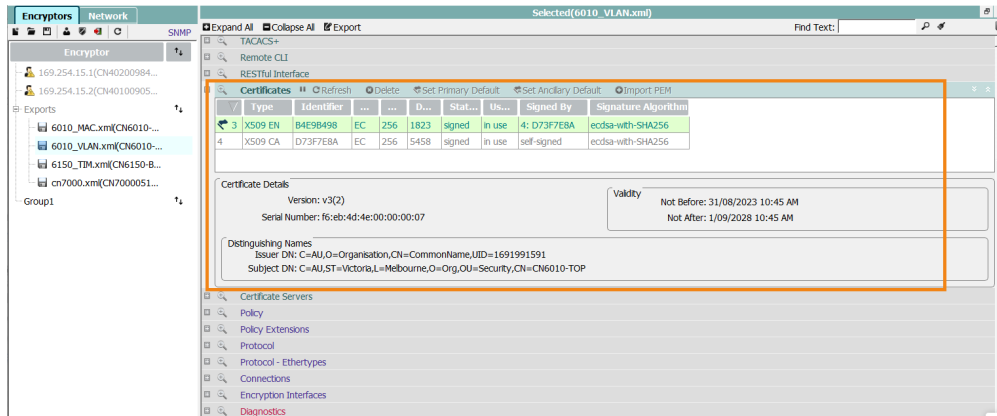


Figure 114: Certificate details

The upper section of the display shows the currently loaded certificates. Each certificate has an index; index 1 is reserved for a (deprecated) V1 certificate, index 2 is reserved for a V2 certificate, and indexes 3 and above are used for X.509 certificates and Elliptic Curve parameter files. The details included are:

- **ID** - index that identifies the certificate. If a certificate is defined as the default encryption certificate then the ID will have a flag displayed next to it and the line will be shaded green
- **Type** - The type of certificate. Types allowed are: X509 EN (Encryption), X509 CA (Certificate Authority), X509 OT (Other), and ECParam. The ECparam type identifies custom Elliptic Curve parameters that have been loaded into the encryptor
- **Identifier** - a unique hash code derived from the content of the certificate
- **PK Type** - specifies the type of key used to sign the certificate. This can be RSA , ECDH or QRA.
- **PK Size** - specifies the length of the key used to sign the certificate
- **Days remaining** - shows the number of days left before the certificate will expire
- **Status** - shows the current status; signed, unsigned or expired
- **Usage** - shows the current utilization of the certificate. This can be 'in use' or 'not in use'

NOTE: . When operating in TIM mode this field is not applicable

- **Signed By** - the ID and hash of the CA certificate that signed this certificate. In the case of the CA certificate it may be self-signed

The lower section of the display shows the details of the certificate selected in the certificate list. These include:

- **Version:** - shows 1, 2 or 3 depending on whether the certificate type is V1, V2 or V3 (X.509). V1 and V2 have been deprecated
- **Serial Number:** - a unique number assigned by the Certificate Authority (CA) when the certificate was signed and loaded
- **Validity** - the date/time range within which the certificate is valid
- **Distinguishing Names** - the Issuer and Subject details loaded by the CA

If the selected entry is an ECParam type, then the Distinguishing Name will include the Title, Name and Description attributes.



Certificate installation at the host level

Multi-slot encryptors (CN6140 2x10G, CN6140 4x1G and CN6140 4 x 10G) can have certificates loaded onto host encryptors. The following services operate on the host device:

- FTPS
- CipherTrust Manager using SSL
(CM is *NOT* available on individual slots using TCP or SSL.)
- OCSP
- RESTful

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

NOTE: It is possible to configure installed certificates as the default primary or default ancillary certificate. However, this shall be ignored by the host as connections are not applicable.

Certificate Servers

The Certificate Server option allows you to configure the Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP) servers that the encryptor can use to determine the validity of its X.509 certificates. Up to 10 servers can be specified.

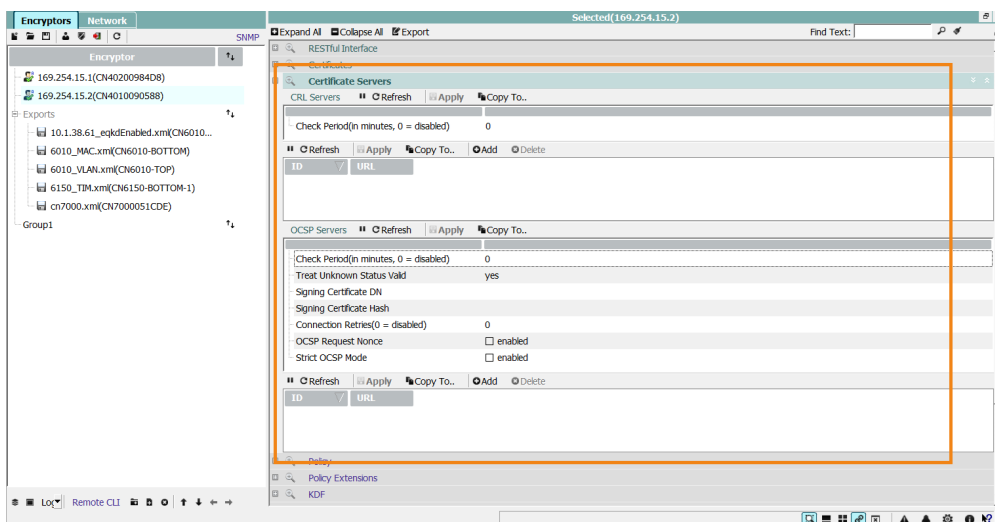


Figure 115: Certificate server configuration

Check Period(in minutes) - specifies the period between certificate checks. A value of 0 disables checking.

ID - the index of the server. This is used when editing server details using the CLI. See the `curl` command on page

URL - specifies the IP address of the server. For example 172.30.2.1.

Configuring OCSP and CRL servers

The Senetas encryption products support online certificate status checking (OCSP) and Certificate Revocation List (CRL) mechanisms. The purpose of these is to provide a mechanism to check if an encryptor certificate has been revoked for any reason and to prevent that encryptor from joining the network, or to remove it from the network.



Support for the revocation of certificates can be provided by configuring OCSP or CRL servers within an encryptor.

Configuration is performed using the CLI **ocsp** and **crl** commands or via the CM7 Certificate Servers tab.

WARNING: Name resolution is not supported and servers must be specified using IP addresses.

The CRL is a simple list of revoked certificates and as such can grow to be a very large file that is inefficient to process on a regular or session by session basis. OCSP provides a more efficient way to validate X.509 certificates and is therefore the recommended method.

NOTE: It is recommended to use an FTP server, which must be entered in the FTP servers list on the Encryptor with a matching certificate.

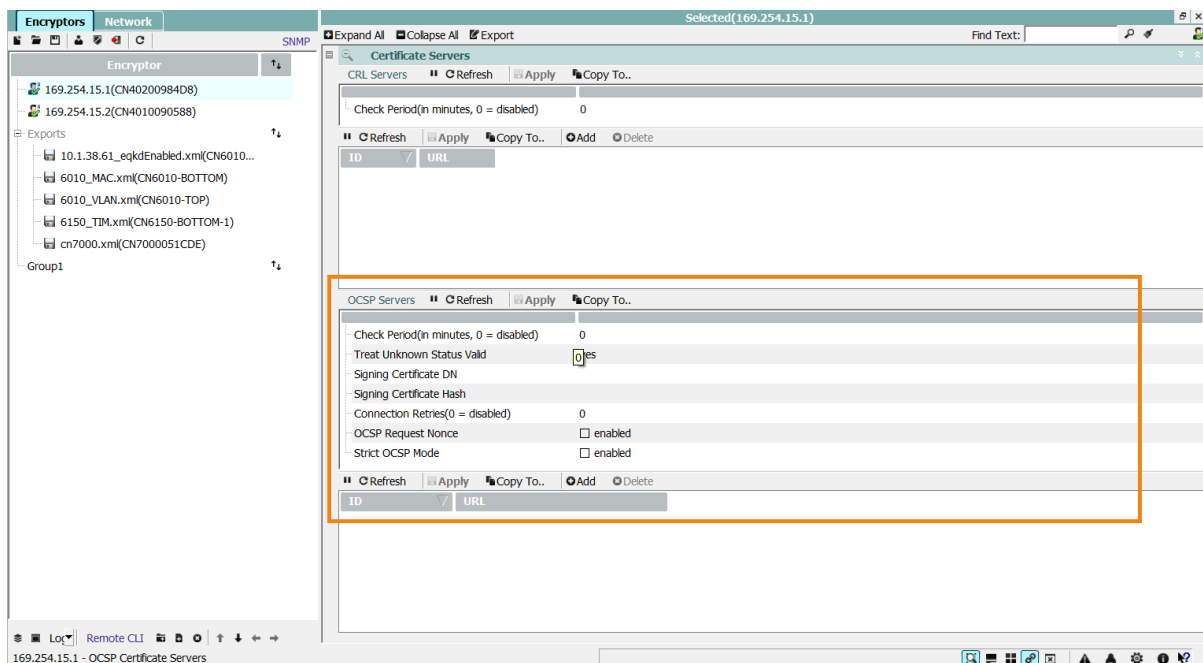
The OCSP allows the encryptor to check the validity of its certificate(s) against one or more OCSP servers. The server, sometimes referred to as the Responder, uses the serial number of a certificate to validate the certificate and return one of the following statuses:

- 'good'
- 'revoked'
- 'unknown'

If the OCSP server cannot be contacted, the OCSP server is deemed 'unreachable'.

NOTE: Neither CA certificates nor QRA certificates can be revoked via OCSP.

All of the OCSP configuration may also be accessed via the CM7 Manage Screen, Certificate Servers pane, OCSP Servers section.



The minimum suggested settings for an encryptor using OCSP are the default ones, but for additional security and resilience, the following settings are recommended:



- 'Treat certificates with an unknown OCSP status as valid' disabled
- Use of OCSP nonce be enabled
- HTTPS be configured to access the OCSP
- 'Strict OCSP' handling with Retries be enabled

Enhanced certificate security

Nonce values

You can also utilise the security enhancement of a *nonce* in OCSP requests, which mitigates replay attacks.

A nonce is an arbitrary number used only once in a cryptographic communication, in the spirit of a nonce word. They are often random or pseudo-random numbers. To ensure that a nonce is used only once, it should be time-variant or generated with enough random bits to ensure an insignificantly low chance of repeating a previously generated value.

This feature can be activated by the CLI command **ocsp -n <y/n>**. The feature is *disabled* by default.

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

Strict OCSP

The concept of "Strict OCSP" further tightens the security mechanism of OCSP requests. When run in STRICT mode, all OCSP failures including certificate revocation responses or OCSP request failures result in a certificate validation failure. Only certificates that receive a OCSP *good* response are considered passing validation.

Strict OCSP is enabled via the CLI **ocsp -s** command but is disabled by default.

Attempting to enable 'Strict OSCP' mode will be prevented if more than one server is configured.

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

All OCSP settings must be configured prior to enabling the 'Strict OCSP' feature.

NOTE: You must disable "Treat certificates with an unknown OCSP status as valid" before enabling 'Strict OCSP.'

The encryptor shall contact OCSP server(s) periodically at the configured OCSP update interval. The behaviour of the encryptor, for the four possible OCSP responses, is summarised below:

OCSP Response	Qualifier	OSCP Action	Strict OCSP Enabled
GOOD	Previous response "GOOD"	No Action	Same
	Certificate previously not "GOOD"	Relevant connections set to "UP" state	Same
REVOKED	Certificate previously "REVOKED"	No Action	Same
	Certificate not previously "REVOKED"	Relevant connections set to "FAULT" state	Same
UNKNOWN	"Treat unknown certificate as valid" Enabled	Treat as "GOOD"	Not Applicable
	"Treat unknown certificate as valid" Disabled	Treat as "REVOKED"	Same



OCSP Response	Qualifier	OSCP Action	Strict OCSP Enabled
UNREACHABLE	"Treat unknown certificate as valid" Enabled	Treat as "GOOD"	Not Applicable
	"Treat unknown certificate as valid" Disabled	Treat as "REVOKED"	Not Applicable
	"Retry Limit" = 0	Not Applicable	Treat as "UNKNOWN"
	"Retry Limit" > 0	Not Applicable	Continue to retry until "Retry Limit" is reached or a response is received. If "Retry Limit" reached, treat as "UNKNOWN"

CM7 supports the configuration of up to 10 servers. In addition, you can specify how often the validity of a certificate is checked by defining the frequency in minutes and whether an 'unknown' response should be treated as valid or invalid.

NOTE: The default OCSP check period value of 0 disables OCSP server support.

Server configurations

A typical OCSP configuration entry would be:

```
http://192.168.0.1:443/ocsp/
```

The (CRL) facility provides a means of checking whether a certificate has been flagged in a named 'bad certificate list'. CM7 allows up to 10 CRL servers to be configured, and as with the OCSP servers the check period can be 0 or set to N to specify that a named file be downloaded and checked every N minutes. Each entry defines both the server IP address and the name of the CRL file that will be returned to the encryptor.

A typical CRL configuration entry would be:

```
http://192.168.0.2/localFTP/crls/cert.crl
```

Slot

The **Slot** panel shows the status of the slots in the encryptor, such as running or stopped. For example, if in 2 x 10Gbps configuration, the panel will only show two slots.

Specific licenses are applied to slots via this panel.

Slots can be started, stopped or erased via the Slots panel.

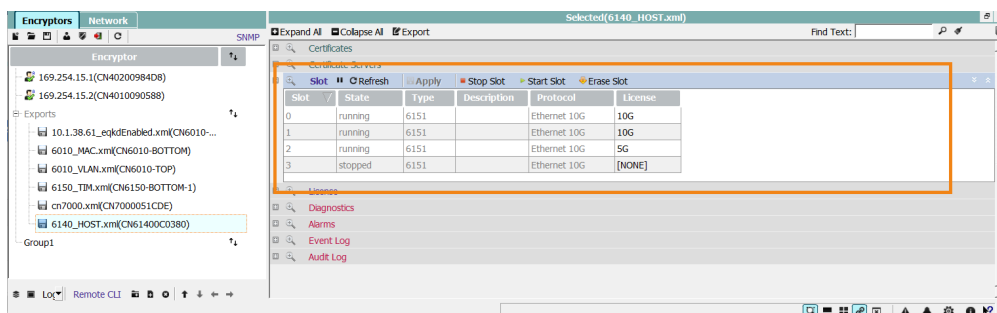


Figure 116: Slot dialog



License

The **License** panel displays what licenses are available. The displayed list takes into account the protocol to which the encryptor is set, for example, 1Gbps or 10Gbps slotted.

Licenses listed are only shown if appropriate to the link speed of those slots configured for the encryptor.

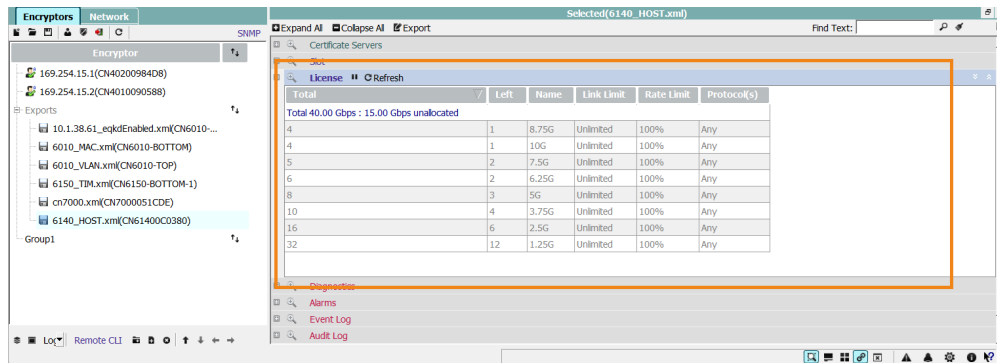
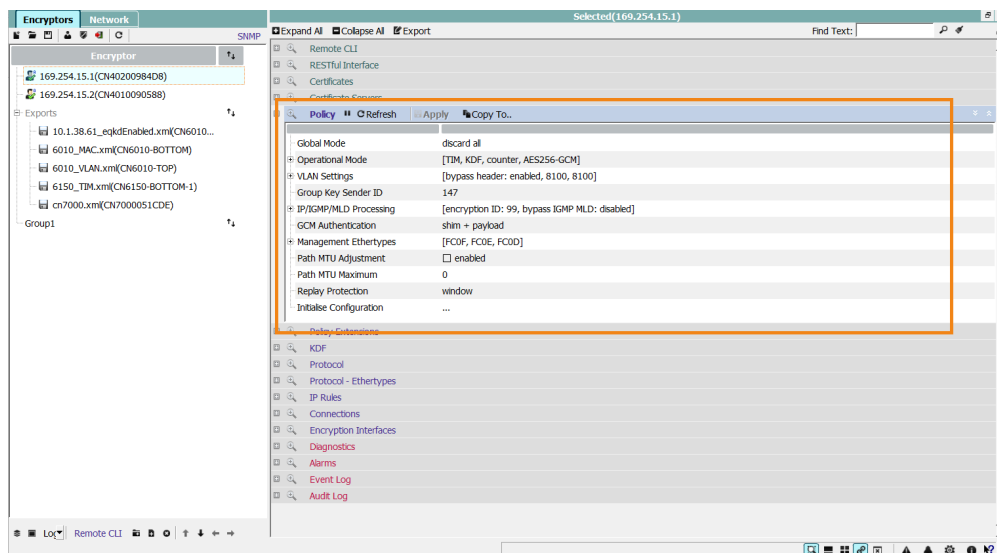


Figure 117: License dialog

Policy

The Policy option allows you to examine and update the policy that will be applied to connections. The contents of the fields will change depending upon the unit being managed.

NOTE: The "Hide Not Applicable Settings" selector allows you to hide or show features that are not applicable to the encryptor you are managing. Refer to "Configuring CM7" on page 140



Policy	
Global Mode	encrypt all
Operational Mode	[line mode, AES256-GCM]
Line Mode	<input checked="" type="checkbox"/> enabled
Crypto Mode	AES256-GCM
Transec	[enabled, 1000, 49019.60, 40.00, 400000000, 01:00:5e:00:fc:0f, 00:d0:1f:07:80:a6]
Transec Mode	<input checked="" type="checkbox"/> enabled
Frame Length	1000
Frames Per Second	49019.60
Bandwidth(%)	40.00
Bandwidth(Bits Per Sec...)	400000000
Destination MAC	01:00:5e:00:fc:0f
Source MAC	00:d0:1f:07:80:a6
Header Bytes	
CTR Mode Shim	[32, observe MTU: enabled]
Shim Rate	32
Prevent MTU Overflow	<input checked="" type="checkbox"/> enabled
VLAN Settings	[bypass header: enabled, 8100, 8100]
Bypass VLAN Header(s)	<input checked="" type="checkbox"/> enabled
Default Ethertype	8100
Alternate Ethertype	8100
IGMP/MLD Processing	[encryption ID: 99, bypass IGMP MLD: disabled, bypass IP multicast header: disabled]
IP Protocol Encryption ID	99
Bypass IGMP/MLD	<input type="checkbox"/> enabled
Bypass IP Multicast Hea...	<input type="checkbox"/> enabled
GCM Authentication	entire frame
Management Ethertypes	[FC0F, FC0E]
Management Frames	FC0F
Sender ID Frames	FC0E
Key Distribution Interface	network
Initialise Configuration	...

Policy	
Global Mode	discard all
Operational Mode	[TIM, KDF, AES256-CTR]
Connection Mode	TIM
Key Provider	KDF
Crypto Mode	AES256-CTR
Group Key Sender ID	46
> IGMP/MLD Processing	[encryption ID: 99, bypass IGMP MLD: disabled]
> Management Ethertypes	[FC0F, FC0E]
Initialise Configuration	...

Figure 118: TIM mode Layer 2 Policy definition

- **Global Mode** - top level mode that specifies whether the encryptor is in 'Discard', 'Bypass', or 'Encrypt'
- **Operational Mode** - shows the current operating mode of the encryptor which summarizes the connection and cryptographic modes
- **Line Mode** - enabled to specify that the unit is in Point-to-point (Line) mode. This must be disabled to allow selection of Multipoint (VLAN, MAC) modes.



- **Connection Mode** - displayed to allow selection of MAC, VLAN or TI mode. When in MAC mode, the option to enter Line mode is displayed. The connection mode can also be set from the CLI using the **con** command.
- **Key Provider** - allows selection of the key provider used in TIM mode. The available values are KDF which specifies a Key Derivation Function and KMIP which specifies a KMIP Key server. Changing the Key Provider requires the user to restart the connections to enable immediate change over to the new provider.
- **TRANSEC** - displayed when Line mode is enabled to allow TRANSEC to be enabled and then the definition of the Transport Frame header.
- **TRANSEC mode** - enables or disables TRANSEC
- **Frame length** - configures the length in octets of the Transport Frame (For 10Gbps models this must be a multiple of 8 octets; if it is not, it will be rounded down, for example, 159 will become 152.)
- **Frames Per second** - specifies the transmission speed of TRANSEC traffic
- **Bandwidth(%)** - specifies the bandwidth of the TRANSEC link in bits per second
- **Destination MAC** - specifies the MAC address of the remote peer encryptor
- **Source MAC** - specifies the MAC address of the local encryptor
- **- Header bytes -**
- **Crypto Mode** - specifies the encryption algorithm and encryption sub-mode
- **CTR Mode Shim** - when in CTR mode, shows the configuration of shimming
- **Shim Rate** - when in CTR mode, specifies the frequency of shim insertion
- **Prevent MTU Overflow** - when in CTR mode, 'Enable' prevents shimming if it would cause an MTU overflow
- **VLAN Settings** - shows the current VLAN-related settings
- **Bypass VLAN Headers** - when enabled VLAN headers are bypassed (not encrypted)
- **Default Ethertype** - specifies the ethertype used to identify VLAN headers
- **Alternate Ethertype** - used to specify an alternate VLAN identifier; sometimes required by network vendors
- **IGMP/MLD Processing** - shows status of IGMP/MLD processing
- **IP Protocol Encryption ID** - specifies the ID used to identify frames that have been subject to IGMP/MLD processing
- **Bypass IGMP/MLD** - set to 'Enable' to apply processing to IGMP/MLD frames
- **Bypass IP Multicast Header** - set to 'Enable' to bypass IGMP/MLD Multicast headers
- **Management Ethernets** - shows the current values used to identify management frames
- **Management Frames** - ethertype reserved for management frames
- **Sender ID Frames** - ethertype reserved for Sender ID frames
- **Control Plane Ethertype** - ethertype reserved for out-of-band control plane traffic
- **Key Distribution Interface** - the default value of *network* determines that keys will be distributed over the encrypted network. The alternate value of *local* allows key distribution via the front panel management port.
- **Initialise Configuration** - allows selection of:
 - Initialise config all
 - initialise CI and MAC addresses



- initialise global operation mode



Policy Extensions

The Policy Extension option allows you to configure a number of extended options related to the encryptors policy.

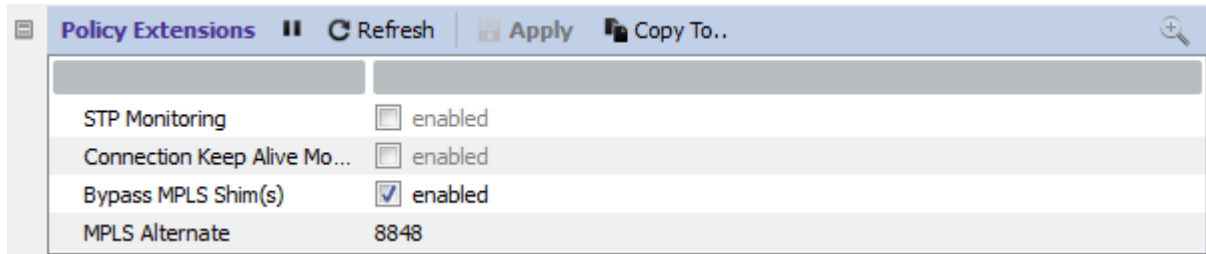


Figure 119: Policy extension configuration

- **STP Monitoring** - when enabled, allows the encryptor to monitor of BPDU messages such that time-out will result in a reloading of the MAC table
- **Connection Keep Alive Monitoring** - when enabled, allows the encryptor to monitor the connection and advises if it is inactive
- **Bypass MPLS Shim(s)** - when enabled (the default), ensures that MPLS tags are left unencrypted
- **MPLS Alternate** - specifies any alternate value for the identification of MPLS tags

Key Derivation Function

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

NOTE: The KDK is treated as a critical security parameter and is tamper protected

Once seeded with the Key Derivation Key, Senetas encryptors are able to algorithmically generate consecutive AES keys that are independent and exhibit optimal forwards and backwards secrecy.

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

The Key Derivation Function (KDF) pane within CM7 is used to create the key that will be used to encrypt traffic.

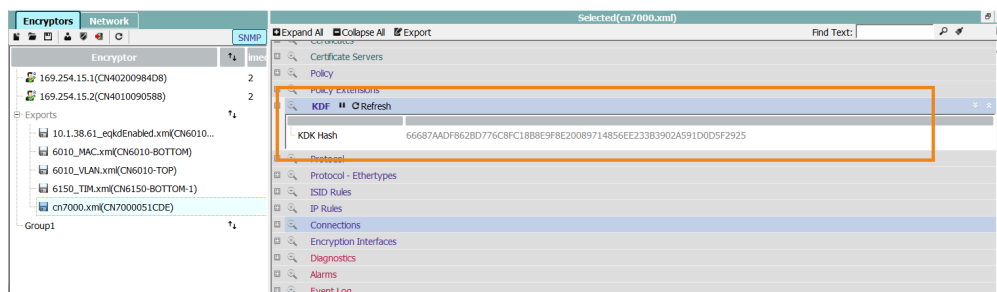


Figure 120: Key Derivation Function

- **Key** - provides a "once-off" display of the generated key which can be copied and pasted to peer encryptors. After this the key will no longer be displayed.



- **Hash** - shows a hash of the created key which can be used to compare the key with those in peer encryptors

Protocol

The Protocol option is used to refine the Ethernet policy to meet the specific needs of the network. A table defines a group of multicast addresses which by default are encrypted but can be bypassed. In addition, when in Multipoint VLAN mode, additional MAC addresses can be added to this table.

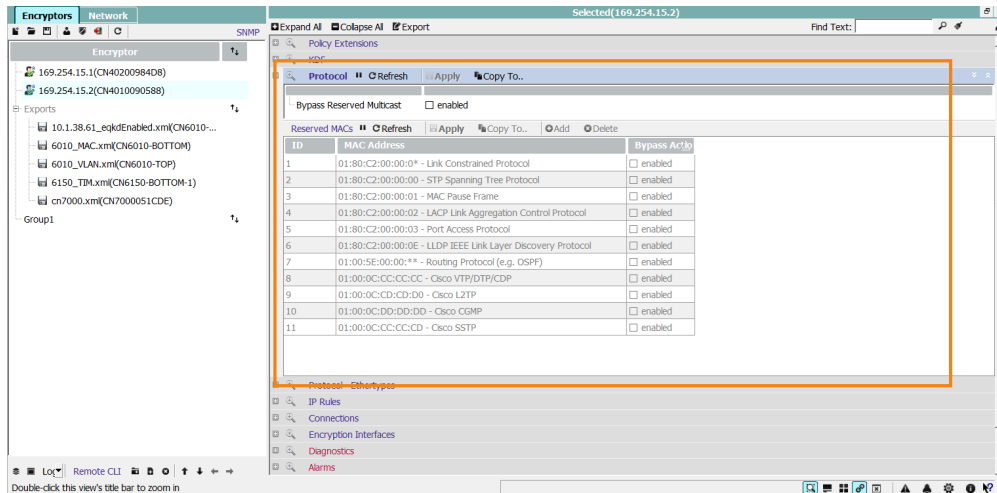


Figure 121: Protocol configuration

Bypass Reserved Multicast - when enabled all of the traffic sent to the listed multicast MAC addresses will be left unencrypted. For security/certification reasons the default is disabled.

Because of the standards for multicast IP to MAC address mapping, there are 32 IP multicast addresses that map to one MAC multicast address. Before enabling Bypass Reserved Multicast you should ensure that none of the MAC addresses in the table also map to other IP multicast traffic on your network that should be encrypted. If this is the case than you should leave Bypass reserved Multicast disabled and add **only** those MAC addresses that need bypassing to the Reserved MAC address table as shown above.

Unknown Network Traffic Adopts Pending Action - when enabled and in MAC mode, if the destination MAC (DA) address of frames received on the network port does not exist in the local MAC table the frame is discarded. If the DA MAC address of frames received on the local port does not exist in the network MAC table then the pending action setting is followed.

Unknown Multicast Action - specifies the action to be taken if traffic to an unknown multicast address is detected. Only applicable when in Multipoint MAC mode.

Unknown VLAN Action - specifies the action to be taken if traffic with an unknown VLAN tag is detected. Only applicable when in Multipoint VLAN mode.

The lower section of the display lists the MAC addresses that will be bypassed when **Bypass Reserved Multicast** is enabled. This includes any additional MAC addresses added using the 'Add' selector, the figure showing the address 09:02b:00:00:05 being added.

Protocol - Ethertypes

The Protocol - Ethertypes option allows you to configure the default and individual ethertype policy of the encryptor. Up to 15 ethertypes can be configured.



The top screenshot shows the configuration for 6010_MAC.xml. The 'Unlisted Ethertype Action' is set to 'broadcast: discard, multicast: discard, unicast: L2, offset: disabled, 0'. The 'Ethertypes' table is as follows:

IDV	Type	Broadcas	Multicast	Unicast A	Mutation I	Muta	Injected	Observe C	Offs	Loc	Net
1	05FF (LENGTH)	bypass	bypass	L2	<input type="checkbox"/> enabled	0000	bypass	<input type="checkbox"/> use ...	0	0	0
2	0800 (IPv4)	bypass	discard	L2	<input checked="" type="checkbox"/> enabled	F800	discard	<input type="checkbox"/> use ...	20	0	0
3	0806 (ARP)	bypass	discard	bypass	<input type="checkbox"/> enabled	F806	bypass	<input type="checkbox"/> use ...	0	0	0
4	86DD (IPv6)	bypass	discard	L2	<input checked="" type="checkbox"/> enabled	F6DD	discard	<input type="checkbox"/> use ...	40	0	0
5	8808 (MAC-C)	bypass	bypass	bypass	<input type="checkbox"/> enabled	F808	bypass	<input type="checkbox"/> use ...	0	0	0
6	8809 (SPMA)	bypass	bypass	bypass	<input type="checkbox"/> enabled	F809	bypass	<input type="checkbox"/> use ...	0	0	0
7	88CC (LLDP)	bypass	bypass	bypass	<input type="checkbox"/> enabled	F8CC	bypass	<input type="checkbox"/> use ...	0	0	0
8	9000 (LOOPBACK)	bypass	bypass	bypass	<input type="checkbox"/> enabled	F000	bypass	<input type="checkbox"/> use ...	0	0	0

The bottom screenshot shows the configuration for 6150_TTM.xml. The 'Unlisted Ethertype Action' is set to 'broadcast: discard, multicast: discard, unicast: discard'. The 'Ethertypes' table is as follows:

IDV	Type	Broadcast A	Multicast Ac	Unicast Acti	Injected Ac	Local Frame	Network Fra
1	05FF (LENGTH)	bypass	bypass	bypass	discard	0	0
2	0800 (IPv4)	bypass	bypass	L3/L4	discard	0	0
3	0806 (ARP)	bypass	bypass	bypass	discard	0	0
4	86DD (IPv6)	bypass	bypass	bypass	discard	0	0
5	8808 (MAC-C)	bypass	bypass	bypass	discard	0	0
6	8809 (SPMA)	bypass	bypass	bypass	discard	0	0
7	88CC (LLDP)	bypass	bypass	bypass	discard	0	0
8	9000 (LOOPBACK)	bypass	bypass	bypass	discard	0	0
9	8847 (MPLS-U)	bypass	bypass	L2	bypass		

Figure 122: Ethertype Policy configuration

- **Unlisted Ethertype Action** - shows the actions that will be taken by ethertypes that are not in the ethertype table. Action can be Discard, Bypass, FollowCI (usually Encrypt) Layer 2 (L2) or Layer 3/4 (L3/L4)
- **Broadcast** - set to FollowCI, Bypass, or Discard
- **Multicast** - set to FollowCI, Bypass, or Discard
- **Unicast** - set to FollowCI, Bypass, or Discard
- **Broadcast** - set to FollowCI, Discard, Bypass, Layer 2 (L2) or Layer 3/4 (L3/L4)
- **Multicast** - set to FollowCI, Discard, Bypass, Layer 2 (L2) or Layer 3/4 (L3/L4)
- **Unicast** - set to FollowCI, Discard, Bypass, Layer 2 (L2) or Layer 3/4 (L3/L4)
- **Offset** - set to Observe to leave payload bytes unencrypted, usually set to ignore to leave bytes encrypted
- **Offset Bytes** - if Offset is to be observed, specifies then number of octets to be left unencrypted

The encryptor is pre-configured with ethertype polices for each of the connection modes. The existing policies can be modified and additional policies up to a total of 15 can be added.



- **ID** - an index used when editing the table using the **ethertypes** CLI command
- **Type** - the value of the ethertype and, where known, its functional description
- **Observe Offset** - specifies whether an offset should be applied to the encryption of the payload
- **Offset** - the length in octets of any offset
- **Broadcast Action** - the action to be applied to Broadcast traffic. This can be set to:
 - Discard
 - Bypass
 - FollowCI
- **Multicast Action** - the action to be applied to Multicast traffic - can be Discard, Bypass or FollowCI
- **Unicast Action** - the action to be applied to Unicast traffic - can be Discard, Bypass or FollowCI
- **Broadcast Action** - the action to be applied to Broadcast traffic - can be Discard, Bypass, Layer 2 (L2) or Layer 3/4 (L3/L4)
- **Multicast Action** - the action to be applied to Multicast traffic - can be Discard, Bypass, Layer 2 (L2) or Layer 3/4 (L3/L4)
- **Unicast Action** - the action to be applied to Unicast traffic - can be Discard, Bypass, Layer 2 (L2) or Layer 3/4 (L3/L4)
- **Mutation** - if enabled, specifies that this ethertype will be mutated using the Mutation Value
- **Mutation Value** - specifies the ethertype that should be substituted for this ethertype
- **injected Action** (Layer 2) - specifies the action to be taken if Mutation is enabled and the ethertype is seen on the network port
- **injected Action** (Layer 2/3/4) - specifies whether to bypass or discard injected frames from the network that would normally be encrypted. Ignored for IPv4 (0x0800) and IPv6 (0x86DD); these are processed as per the IP Rules table. (The absence of a shim identifies injected frames)

The following section lists the Ethertypes that are typically pre-defined and describes the rationale for their default settings.

- **05FF (Length)** - length encoded frames
- **0800 (IPv4)** - defines standard user traffic. It is encrypted and typically mutated to prevent the core network from making packet changes based on the assumption that it contains unencrypted data.
- **0806 (ARP)** - usually left unencrypted so that the core network can be interrogated.
- **86DD (IPv6)** - defines standard user traffic. It is encrypted and mutated, refer to IPv4 above.
- **8847 (MPLS-u)** - defines how labels are assigned to data packets for routing.

IP Rules

The entries within the IP Rules table determine the policy that will be applied to traffic flowing through encryptors configured in TIM mode.

NOTE: Since the TCP checksum is based on the IP header, Layer 3 encryption for TCP traffic on NAT based networks will not work as expected. In such cases, Layer 4 encryption policy is recommended.



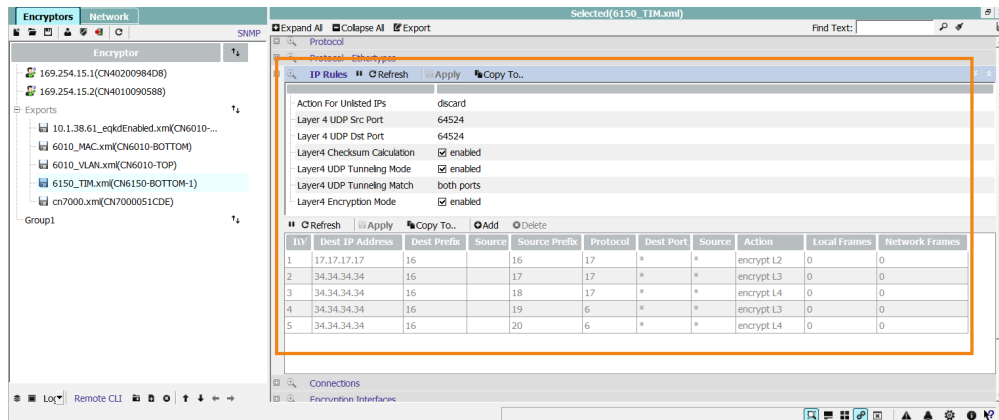


Figure 123: CM7 IP Rules pane

Action for Unlisted IPs - specifies the action that will be taken for IP addresses that are not specified in the IP Rules table. The action can be discard, bypass, encrypt L2, encrypt L3, or encrypt L4. When the action is set to encrypt L4, UDP and TCP packets will be encrypted at L4 and all other packets will be encrypted at L3. Earlier releases (that support IP rules) were discarding.

Layer4 Checksum Calculation - specifies whether the Layer 4 checksum should be calculated as per RFC791 (IPv6 extension headers and IPv4 options are not supported). Applicable to all platforms that support TIM mode. When disabled encryptors operate in Cut-through mode which is the default for FPGA based encryptors and no checksum checks or corrections are performed. When enabled the encryptor will operate in Store and Forward mode, performing L3 and L4 checksum updates and checks; this is always the case for DPDK based encryptors.

Checksum calculations are off by default however it should be enabled whenever layer 4 encryption is being used. Refer to the discussion at the end of this section. This can also be enabled/disabled by the ***iprules -I*** CLI command.

Traffic is matched against each entry using a Longest Prefix Match. If a LPM match is found and a layer 4 action is configured then further matching is performed based on the specified protocol and port number. If the rule is applicable then the action is applied to the traffic.

If TCP is configured for L4 encryption all SYN / ACK frames with a zero TCP payload are bypassed as there is no payload to encrypt, and authentication is not performed as an authentication trailer cannot be added. If the policy is set to **encrypt** at L3 then these frames will be encrypted and if the policy is set to **discard** then these frames will be discarded.

- **ID** - specifies the assigned rule index
- **Dest IP Address** - identifies the destination IP address that is used for the Longest Prefix Match
- **Dest Prefix** - specifies the destination prefix used for the Longest Prefix Match
- **Source IP Address** - identifies the source IP address that is used for the Longest Prefix Match
- **Source Prefix** - specifies the source prefix used for the Longest Prefix Match
- **Protocol** - specifies the protocol for Layer 4 rule matching
- **Dest Port** - specifies the destination port number that is used for Layer 4 rule matching
- **Source Port** - specifies the source port number that is used for Layer 4 rule matching
- **Action** - specifies the action for the rule entry. Can be 'discard', 'bypass', 'encrypt L2', 'encrypt L3', or 'encrypt L4'

In the above figure, network traffic to the destination subnets is treated as follows:

- Entry 1 encrypts the 17.17.17.17/16 subnet at Layer 2
- Entry 2 encrypts the 34.34.34.34/17 subnet at UDP Layer 3



- Entry 3 encrypts the 34.34.34.34/18 subnet at UDP Layer 4
- Entry 4 encrypts the 34.34.34.34/19 subnet at TCP Layer 3
- Entry 5 discards the 34.34.34.34/20 subnet at TCP Layer 4
- All other traffic is discarded (Action For Unlisted IPs)

For a Layer 4 Action, the TCP Protocol number 6 or UDP Protocol number 17 must be specified.

Note that if a destination subnet is behind a NATed network device then the externally-facing NATed IP address(es) should be specified in the IP Rules table.

The IP Rules table can also be viewed and configured via the CLI ***iprules*** command. For details on how to use this command enter `iprules -h` in the CLI.

Layer 4 Checksum calculation

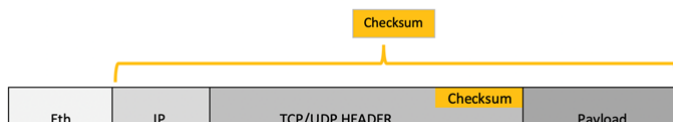
If the encrypted data traverses a network that performs any of the following then the Layer 4 checksum calculation feature must be enabled:

- Network Address Translation (NAT)
- Port Address Translation (PAT)
- Deep packet inspection to L4

The reason for this is that in an FPGA-based, cut-through design, the checksum must be calculated and sent before the payload is received.

WARNING: Enabling the feature solves does make the encryptor a store-and-forward device which has an impact on latency.

As shown in the following diagram the TCP/UDP header checksum is calculated over the IP_HDR + L4_HDR + PAYLOAD fields.



IP Rules for Virtual management

The encryptor architecture determines whether IP Rules are required when using Virtual management.

In the diagram that follows, Encryptor A is being managed via its Local port, and Encryptor B is being managed via its Network port.



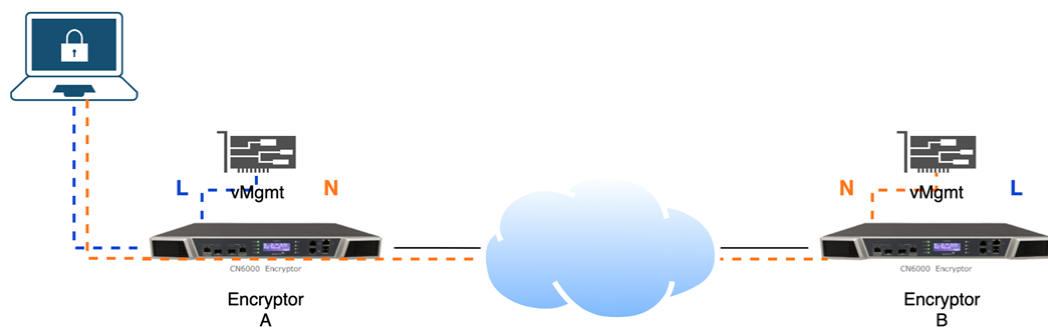


Figure 124: Virtual management of encryptions

For the CN series that are FPGA based, Virtual management traffic is bypassed and not encrypted. On DPDK-based encryptions (such as CN7000 and CV1000), Virtual Management traffic can be bypassed or encrypted (L3/L4) by utilising IP Rules either via the unlisted IP Rule action or configuring specific IP Rules.

When the encryptions are managed via a Local port, an IP Rule is required to bypass management traffic to encryptions that are in the same management domain and managed via their Network port.

When the encryptions are managed via their Network port, no IP Rules are required.

Connections

The Connections option allows you to configure and examine the connections between encryptions.

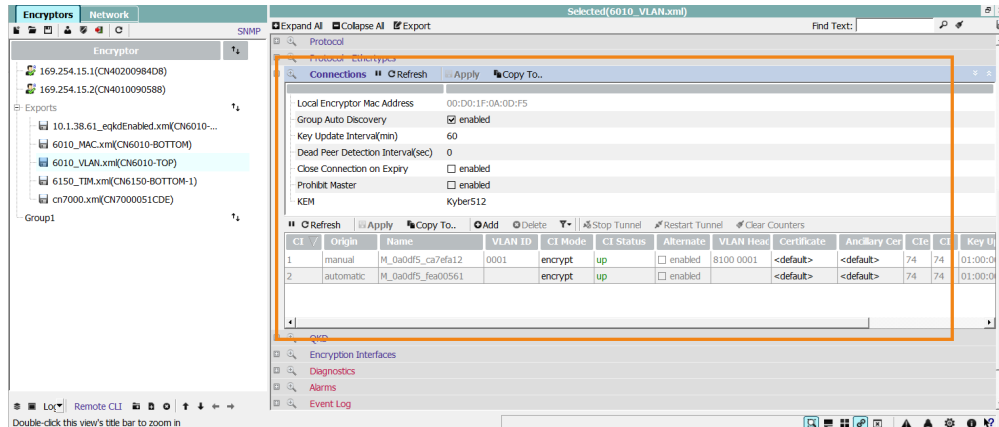
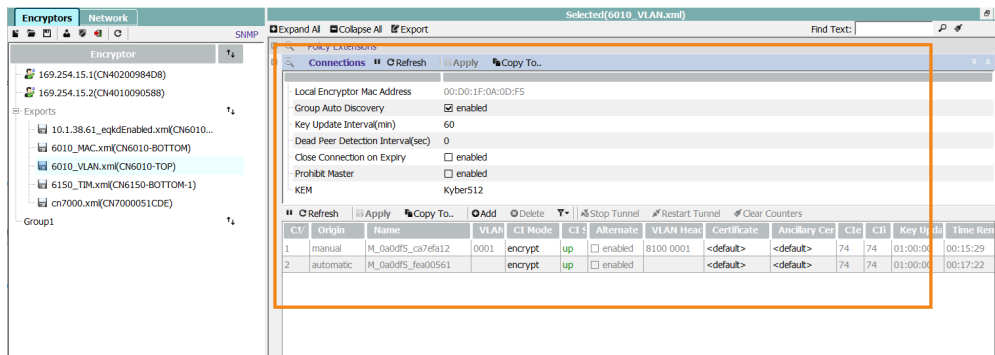


Figure 125: Ethernet Connections configuration

NOTE: The number of connections will depend on the modes of operation and the topology of the network.

VLAN mode connections

The example below is for an Ethernet connection in VLAN mode.



The upper section of the display contains parameters that apply to all connections.

- **Local Encryptor MAC Address** - displays the MAC address of this encryptor
- **Group Auto Discovery** - when enabled, then the encryptor will automatically establish multicast and VLAN connections
- **Key Update Interval(min)** - displays the update period for the Key Encryption Keys - the default is 60 minutes
- **Dead Peer Detection Interval(sec)** - sets the period in which if a 'chirp' is not seen a master encryptor will enter 'dead peer mode' (See note below.)
- **Close Connection on Expiry** - if enabled then certificate expiry will result in any associated connections being closed. (Only applicable to layer 2 encryptors operating in Point-point (Line) and/or MAC mode.)
- **Prohibit Master** - Prevents the Encryptor from becoming the master
- **KEM** - the Key Encapsulation Mode that is to be used to encrypt the DEK

The lower section of the display shows the individual connections that currently exist between this encryptor and its peers. The columns of this section of the pane are:

- **ID** - the connection identifier
- **Origin** - an identifier of the source of connection establishment - this can be 'system' or a manual entry
- **Name** - prefix of M indicates unit is key master, prefix of S indicates slave. Suffix is MAC address of master. For Unicast text is the user supplied name.
- **CI Mode** - current mode of connection - Bypass, Discard or 'follow CI', which indicates that the mode will be determined by the remote MAC or VLAN policy
- **CI Status** - displays the current connection status. Can be Start, Flow1, Flow2, Flow3, Up or Fault.
- **VLAN ID** - displays the VLAN ID number
- **Alternate Encryption** - displays an alternative encryption protocol/method
- **VLAN Header** - displays the VLAN header
- **Certificate** - the identifier of the certificate used to establish the connection. This will be either the <default> certificate or the hash of another EN certificate on the encryptor.
- **Ancillary Certificate** - the identifier of the certificate used to establish the ancillary (QRA) connection. This will be either the <default> certificate or the hash of another EN certificate on the encryptor.
- **Cle** - count of key updates on egress port
- **Cli** - count of key updates in ingress port
- **Time Remaining** - time until the next key update



Dead peer detection (Layer 2 VLAN only)

Periodic 'chirp' messages are transmitted and if a 'master' does not receive a chirp within the specified 'Dead Peer Detection Interval' they enter 'dead peer mode' and all traffic is discarded. If a chirp is received from a slave, the master will exit dead peer mode and resume normal operation.

NOTE: While enabling this feature is recommended, it should only be used where it can be enabled on all encryptors.

Line mode connections

The example below is for an Ethernet connection in Line mode.

CV	Origin	Name	Remote MAC	CI Mode	CI Status	VLAN Head	Certificate	Ancillary Cer	CTE	CTI	Key Update	Time Rem
1	system		00:00:00:00:00:00	encrypt QKD	start		<default>	<default>	0	0	00:00:00	00:00:00

The upper section of the display contains parameters that apply to all connections.

- **Local Encryptor MAC Address** - displays the MAC address of this encryptor
- **Key Update Interval(min)** - displays the update period for the Key Encryption Keys - the default is 60 minutes
- **Authentication Interval(hours)** - displays the time between certificate authentication requests (only applicable to layer 2 encryptors operating in Point-point (Line) and/or MAC mode)
- **Close Connection on Expiry** - if enabled then certificate expiry will result in any associated connections being closed (only applicable to layer 2 encryptors operating in Point-point (Line) and/or MAC mode).
- **KEM** - the Key Encapsulation Mode that is to be used to encrypt the DEK

The lower section of the display shows the individual connections that currently exist between this encryptor and its peers. The columns of this section of the pane are:

- **ID** - the connection identifier
- **Origin** - an identifier of the source of connection establishment - this can be 'system' or a manual entry
- **Name** - prefix of M indicates unit is key master, prefix of S indicates slave. Suffix is MAC address of master. For Unicast text is the user supplied name.
- **Remote MAC** - The MAC address of the remote peer
- **CI Mode** - current mode of connection - Bypass, Discard or 'follow CI', which indicates that the mode will be determined by the remote MAC or VLAN policy
- **CI Status** - displays the current connection status. Can be Start, Flow1, Flow2, Flow3, Up or Fault.
- **VLAN Header** - displays the VLAN header
- **Certificate** - the identifier of the certificate used to establish the connection. This will be either the <default> certificate or the hash of another EN certificate on the encryptor.



- **Ancillary Certificate** - the identifier of the certificate used to establish the ancillary (QRA) connection. This will be either the <default> certificate or the hash of another EN certificate on the encryptor.
- **Cle** - count of key updates on egress port
- **Cli** - count of key updates in ingress port
- **Key Update** - the time between key updates. Can be set in the range 1 to 60 minutes.
- **Time Remaining** - time until the next key update
- **Rx Frames** - a count of the frames received on this connection since the connection was established or the last 'Clear Counters' command
- **TX Frames** - a count of the frames transmitted on this connection since the connection was established or the last 'Clear Counters' command

MAC mode connections

The example below is for an Ethernet connection in VLAN mode.

The screenshot displays the 'Encryptions Network' interface. The left pane shows a tree view of configurations, with '6010_VLAN.xml(CN6010-TOP)' selected. The main pane shows the 'Policy Extensions' for 'Selected(6010_MAC.xml)'. The 'Connections' tab is active, showing a list of connections with columns: C/I, Origin, Name, Remote MAC, CI Mode, CI Status, VLA, Certificate, Ancillary Cert, CTS, CII, Key Update Interval, and Time Rem.

C/I	Origin	Name	Remote MAC	CI Mode	CI Status	VLA	Certificate	Ancillary Cert	CTS	CII	Key Update Interval	Time Rem
1	system	Pending	00:00:00:00:00:00	discard	up	N/A	<-default>	0	0	00:00:00	00:00:00	
2	system		00:00:00:00:00:00	discard	up	N/A	<-default>	0	0	00:00:00	00:00:00	
3	system		00:00:00:00:00:00	bypass	up	N/A	<-default>	0	0	00:00:00	00:00:00	

The upper section of the display contains parameters that apply to all connections.

- **Local Encryptor MAC Address** - displays the MAC address of this encryptor
- **Unicast Auto Discovery** - when enabled, connections will be automatically created based on the network traffic
- **Group Auto Discovery** - when enabled, then the encryptor will automatically establish multicast and VLAN connections
- **Delete Multicast Connections** - sets period that Multicast connections will be retained after last traffic is seen
- **Key Update Interval(min)** - displays the update period for the Key Encryption Keys - the default is 60 minutes
- **Authentication Interval(hours)** - displays the time between certificate authentication requests. (Only applicable to layer 2 encryptors operating in Point-point (Line) and/or MAC mode.)
- **Close Connection on Expiry** - if enabled then certificate expiry will result in any associated connections being closed. (Only applicable to layer 2 encryptors operating in Point-point (Line) and/or MAC mode.)
- **VLAN ID Override**- enables the use of a specific VLAN ID for management traffic instead of a learnt VLAN ID
- **VLAN ID Override Tag** - when override enabled this VLAN ID will be used to send multicast management traffic
- **Prohibit Master** - Prevents the Encryptor from becoming the master
- **KEM** - the Key Encapsulation Mode that is to be used to encrypt the DEK

The lower section of the display shows the individual connections that currently exist between this encryptor and its peers. The number of connections will depend on the modes of operation and the topology of the network.



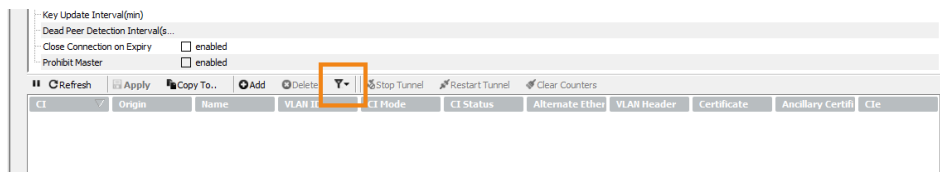
- **ID** - the connection identifier. For Multipoint MAC, indexes 1, 2 and 3 are reserved
- **Origin** - an identifier of the source of connection establishment - this can be 'system' or a manual entry
- **Name** - prefix of M indicates unit is key master, prefix of S indicates slave. Suffix is MAC address of master. For Unicast text is the user supplied name.
- **Remote MAC** - The MAC address of the remote peer
- **CI Mode** - current mode of connection - Bypass, Discard or 'follow CI', which indicates that the mode will be determined by the remote MAC or VLAN policy
- **CI Status** - displays the current connection status. Can be Start, Flow1, Flow2, Flow3, Up or Fault.

Filter connections

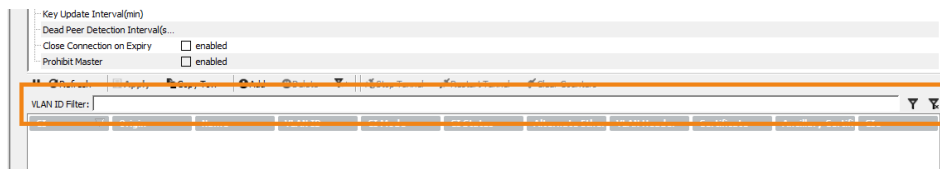
When you have multiple entries in the Connections table, you can apply a filter to show a specific connection or a small subset of the entries. You can filter using:

- In VLAN mode: VLAN IDs and VLAN ID ranges.
- In MAC mode: Remote MACs and Remote MAC ranges
- In TIM mode: KeyID.

The filter functionality is accessed by clicking on the 'Filter' icon.



This action will expand the filter toolbar.



The Filter field contains a text box for typing in VLAN ID and/or VLAN ID ranges separated by a comma in the following format:

LowestVLANID1-HighestVLANID1, VLAN ID, LowestVLANID2-HighestVLANID2

or

LowestRemoteMAC1-HighestRemoteMAC1, RemoteMAC, LowestRemoteMAC2-HighestRemoteMAC2, ...

After specifying the range, the 'Filter' icon on the right of the range text box will activate the filter. The 'Clear Filter' icon clears the range text box and removes the filter from the connections display.

When the operational status of an encryptor is TIM, 'Fault' indicates that a key could not be retrieved and 'Up' indicates that a key is available irrespective of the global mode.

NOTE: Data connectivity may still not be available due to factors such as time synchronization or a mismatched KDK .

Transport Independent Mode (TIM) connections

The following example is for a TIM Ethernet connection:



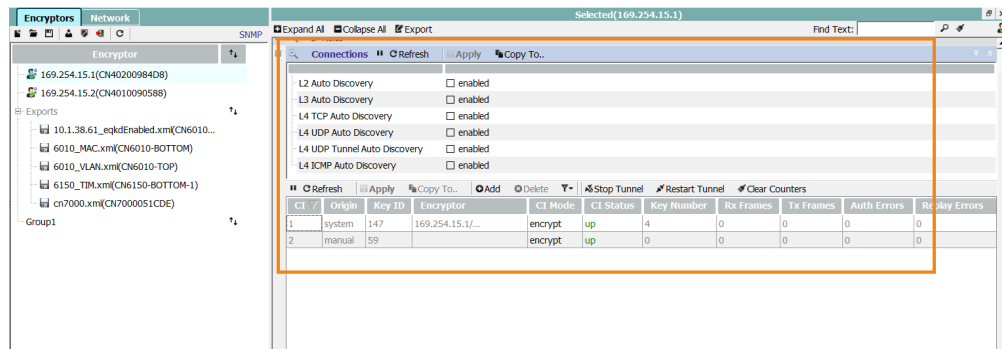


Figure 126: Configuring Ethernet connections in Transport Independent Mode (TIM) mode)

The upper panel includes the parameters that are common to all connections.

Auto-Discovery is the process of automatically adding remote Key Identifier (KID) connections when a shimmed frame is received on the network port for which there is no connection entry (CI). It is typically just a commissioning step and depending on the installation should be disabled after all connections are discovered.

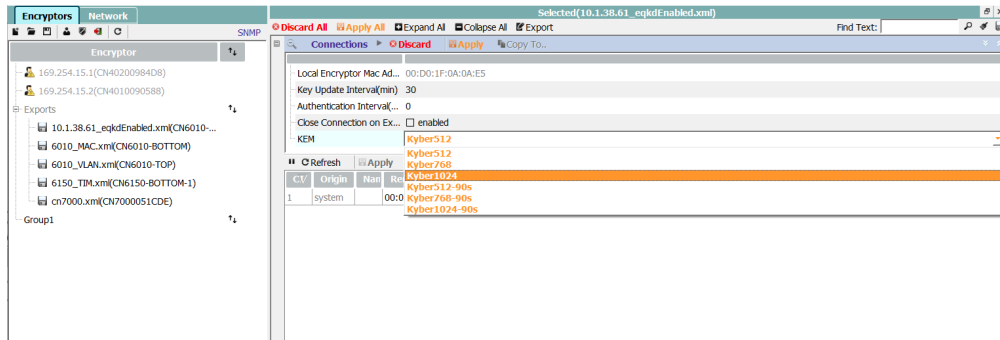
Auto-Discovery for each of the layers can be enabled or disabled from CM7 as shown above, or from the CLI using the **autodisco** command.

NOTE: If Quantum Resistant Algorithms (QRA)-based connections are to be used, then the Key Encapsulation Mode needs to be configured as described below.

The lower section shows the detail for each connection to a remote peer.

- **ID** - the connection identifier.
- **Origin** - an identifier of the source of connection establishment - this can be 'system' or a manual entry
- **Key ID** - the unique network wide value that identifies the pool of keys used for encryption
- **Encryptor** - the IP address and the name (sysMgmtHostName) of the encryptor with a Sender Id (gEthSenderId) matching the Key Id of the connection.
- **CI Mode** - the mode of the connection: discard, bypass, encrypt
- **CI Status** - the status of the connection
- **Key Number** - the assigned count of keys assigned
- **Rx Frames** - the frames received on the connection
- **Tx Frames** - the frames transmitted on the connection
- **Auth errors** - a count of the authorization errors (if any)
- **Replay Errors** - a count of the replay errors (if any)

Quantum Resistant Algorithms require that the Key Encapsulation Mechanism be specified. See "QRA-based key generation" on page 152



Quantum Key Distribution (only layer 2)

The QKD option allows the configuration of Quantum Key Distribution (QKD) unit support, and the display of related statistics.

The ETSI mode is enabled or disabled via the CM7 System pane or the **eqkd** (front panel serial console) CLI command. Enabling or disabling a QKD unit requires an encryptor reboot.

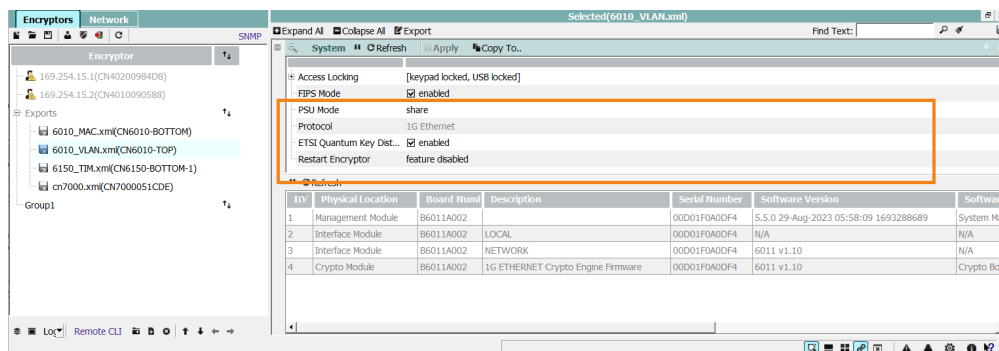


Figure 127: QKD mode selection

When QKD is enabled, a pane showing the configuration parameters and QKD statistics is displayed:

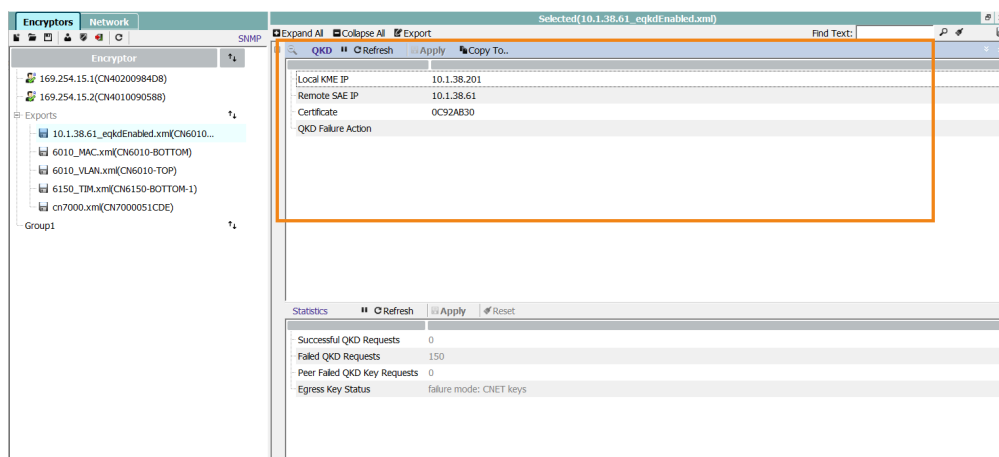


Figure 128: eQKD configuration and statistics

WARNING: QKD or eQKD can only be enabled in VLAN and Line operational modes.



QKD configuration

At each endpoint, configure the following parameters:

Local KME IP - the local Key Management Entity (QKD device), with IP accessibility from the front panel management port.

Remote SAE IP - the remote Encryptions front panel IP address

Certificate - select the certificate hash for the secure HTTPS connection to the KME (QKD) device. This can be the CA certificate for host only authentication, or a signed end user certificate for client authentication. QKD tunnels (proprietary and ETSI) support both EC and RSA keys and QRA based hybrid certification, see "QRA-based key generation" on page 152.

Failure to retrieve QKD keys from KME devices at either end will cause the unit to revert to using internal classical **CNET** keys. All Senetas encryptors on the network must be operating with the same firmware version.

QRA support

All Senetas encryptors support Quantum Resistant Algorithms.

QKD statistics

The lower section of the QKD setup screen shows the current statistics for the unit.

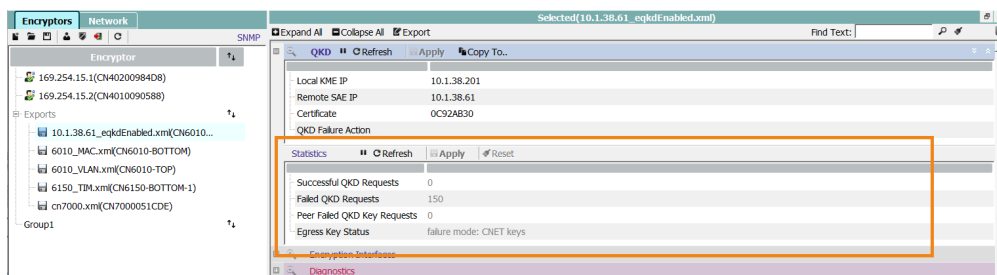


Figure 129: QKD statistics

The information provided is:

- **Successful QKD Requests** - the number of QKD keys successfully received from the QKD unit
- **Failed QKD Requests** - the number of QKD keys requested from the QKD unit but not received
- **Peer Failed QKD Key Requests** - the number of QKD key requests that the peer of this encryptor reported as failed
- **Key Update Failures** - the number of failed key updates due to QKD failure
- **Egress key Status** - the type of keys currently being used for key exchanges

Encryption Interfaces

The Encryption Interfaces option allows you to examine and configure the Local and Network Interfaces.

The configuration detail determines the characteristics of the connection that is established.

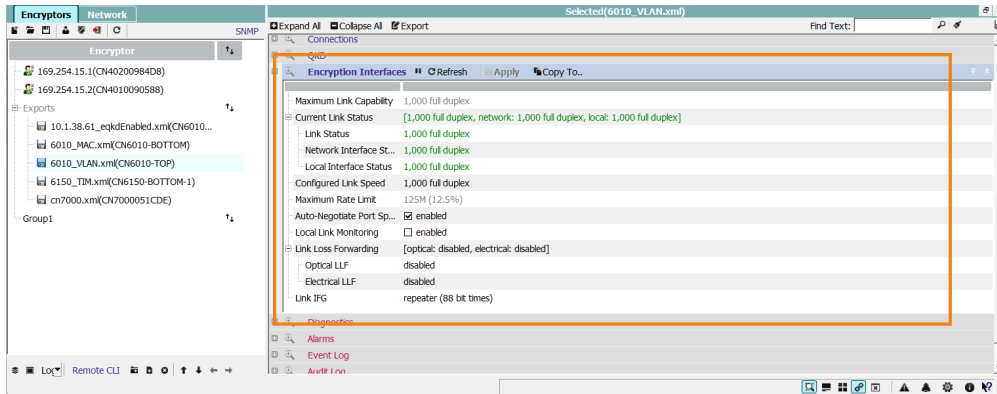


Figure 130: Ethernet encryption Interface configuration

- **Maximum Link Capability** - specifies the maximum speed that the link can operate at
- **Current Link Status** - shows the current status of the link and the local and network ports
- **Link Status** - shows the speed and mode of the link
- **Network Interface status** - shows the speed and status of the network port; this can be edited
- **Local Interface Status** - shows the speed and status of the Local port; this can be edited
- **Configured Link Speed** - shows the configured link speed
- **Local Link Monitoring** - when enabled, sets the unit into global discard mode if a link loss is detected on the local port. Once set to discard, the unit will not pass traffic until an admin or supervisor user resets the unit to encrypt.

Local Link Monitoring (LLM)

If a local link goes down after LLM was enabled, LLM will move global mode from *secure/bypass* to *discard*

If the local link is already down at the time LLM is enabled, the global mode will not be updated

NOTE: An administrator can always change the **global mode** from *discard* to *secure/bypass* even if LLM has enabled and a local link is down.

- **Link Loss Forwarding** - shows the status of the LLF as per the following options
 - **Optical LLF** - control of Optical Link Loss Forwarding in which loss of an optical signal on one port results in the signal being turned off at the other port. The available settings are:
 - 'Local', loss at Local port will turn off the network port laser
 - 'Network', loss at the Network port will turn off the local port laser
 - 'Bi-directional', loss at either port turns off the other ports laser
 - **Optical LLF Tied to session** - If enabled and Optical LLF is enabled, output laser will not turn on until a secure connection is re-established
 - **Electrical LLF** - for units with RJ45 interfaces, enabled / disabled electrical LLF. Loss of input connection on either port drops output on opposite port
 - **Electrical LLF Tied to Cl#** - If enabled and electrical LLF is enabled, link remains down until secure connection is re-established



Link Loss Forwarding (LLF)

Although Link Loss Forwarding can be enabled to propagate the state of the link across the Local and Network ports of the encryptor, there are a number of considerations:

- There are separate settings for Copper and Optical Link Loss Forwarding
- LLF only operates if the Local and Network ports use the same media, that is, both are copper or both are optical
- **Link IFG** - allows change of Interframe gap. On 1 Gbps and 10 Gbps units this is set to 88 bit times to allow full line rate on dark fibre connections. Link IFG is not configurable on 100 Gbps encryptors
- **Auto-Negotiate Port Speed** - enabled / disabled which allows unit to communicate with Local device to determine correct speed

Diagnostics

The Diagnostics option allows you to diagnose the operation of the encryptor by examining the battery status, the management and interface temperatures, the front panel status indicators and the interface status and statistics. For discussion purposes, the available information has been separated into three figures: one for the battery, temperature, front panel and Management port, one for the Local Interface and one for the Network Interface.

The lower portion of the screen shows the ethertype counts which can be enabled to display the ethertypes of all traffic. These are not included for 100Gbps encryptors.

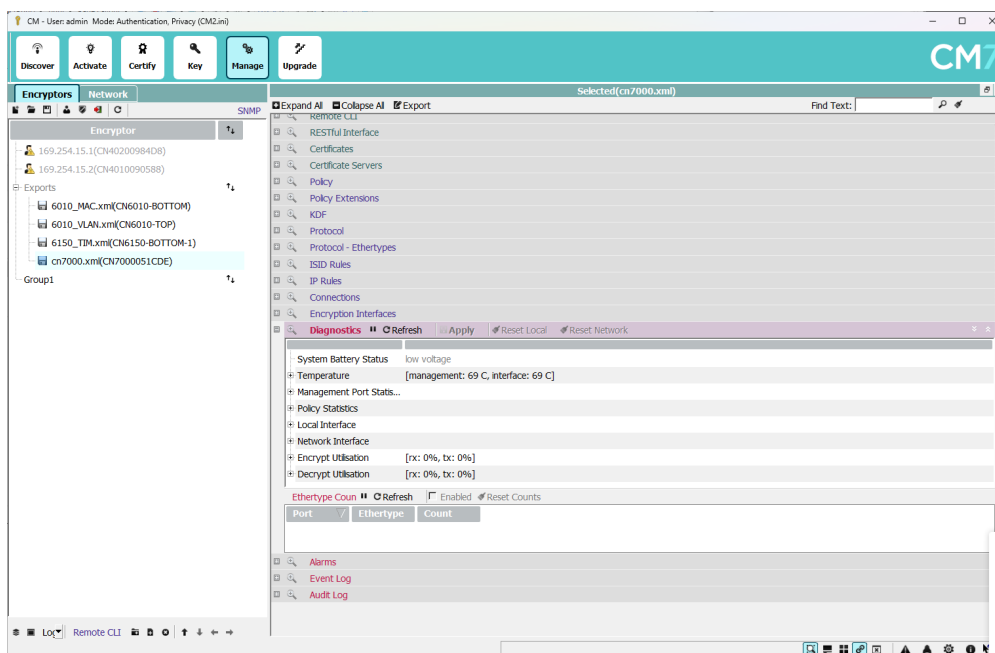


Figure 131: Management Diagnostics

System Battery Status - indicates whether the battery is normal or requires replacement

Temperature - summarizes the internal temperatures of encryptor as follows:

- **Management Module** - shows the temperature of the management module
- **Interface Module** - shows the temperature of the interface module

Front Panel Indicators - shows the state of the units front panel indicators

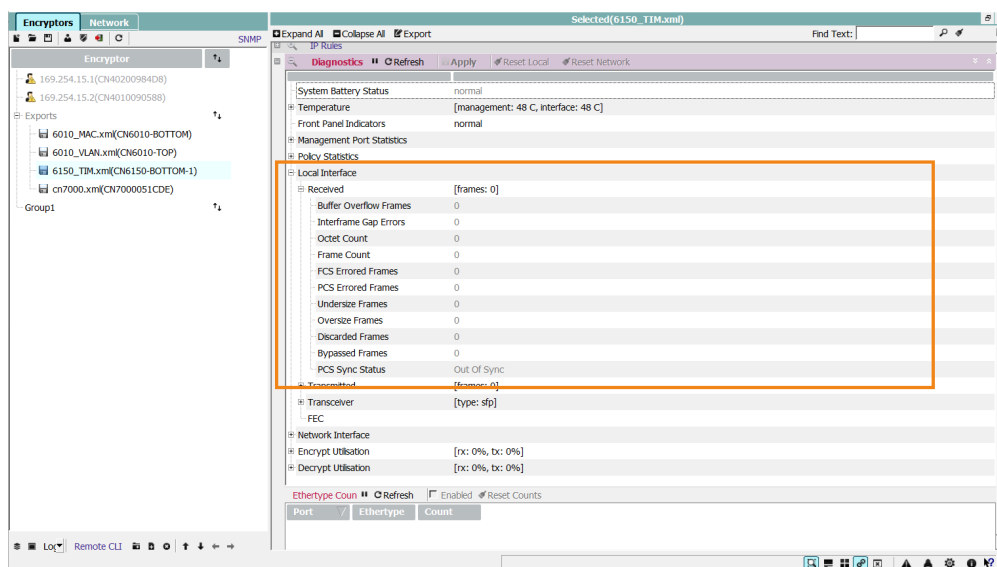
Management Port Statistics



- **Ethernet IP** - summarises the front panel Ethernet traffic
- - **Packets In** - provides a count of the packets sent to the front panel
- - **Packets Out** - provides a count of the packets sent from the front panel port
- - **Header errors** - provides a count of the frames that had header errors
- - **Address errors** - provides a count of the frames that had address errors
- - **Discards** - provides a count of the packets discarded
- Ethernet ICMP - Internet Control Message Protocol traffic
- - **Messages In** - ICMP messages received
- - **Messages Out** - ICMP messages sent
- - **Errors** - count of errors detected
- **Ethernet UDP** - User Datagram Protocol details
- - **Datagrams In** - number of datagrams received
- - **Datagrams Out** - number of datagrams sent
- - **Errors** - number of UDP errors detected

Local interface - displayed in Figure 132 on the facing page

Network Interface - displayed in Figure 133 on page 220



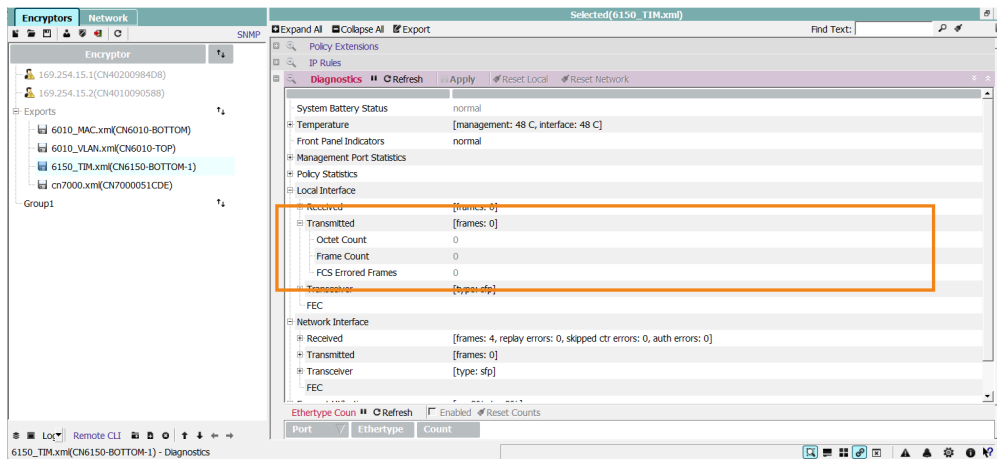


Figure 132: Local interface Diagnostics

Received - summarises the status of the received Local port traffic as detailed below:

- **Buffer Overflow Count** - Count of frames received on the local port and discarded due to internal buffer overflow
- **Interframe gap Errors** - a count of any interframe gap errors
- **Octet Count** - a count of the bytes received on the Local port
- **Frame Count** - a count of the frames received on the Local port
- **FCS Errored Frames** - a count of the frames that had FCS errors
- **PCS Errored Frames** - a count of the frames that had PCS errors
- **Undersize Frames** - a count of the frames that were undersize
- **Oversize Frames** - a count of the frames that were oversize
- **Discarded Frames** - a count of the frames that were discarded
- **PCS Sync Status** -

Transmitted - summarises the status of the transmitted Local port traffic as detailed below:

- **Octet Count** - a count of the octets sent by the encryptor
- **Frame Count** - a count of the frames sent by the encryptor
- **FCS Errored Frames** - a count of the frames with FCS errors

The **Reset Local** button at the top of the display resets the following:

- local port statistics
- local ethertype statistics (TIM operational mode only)
- local IP Rules table statistics



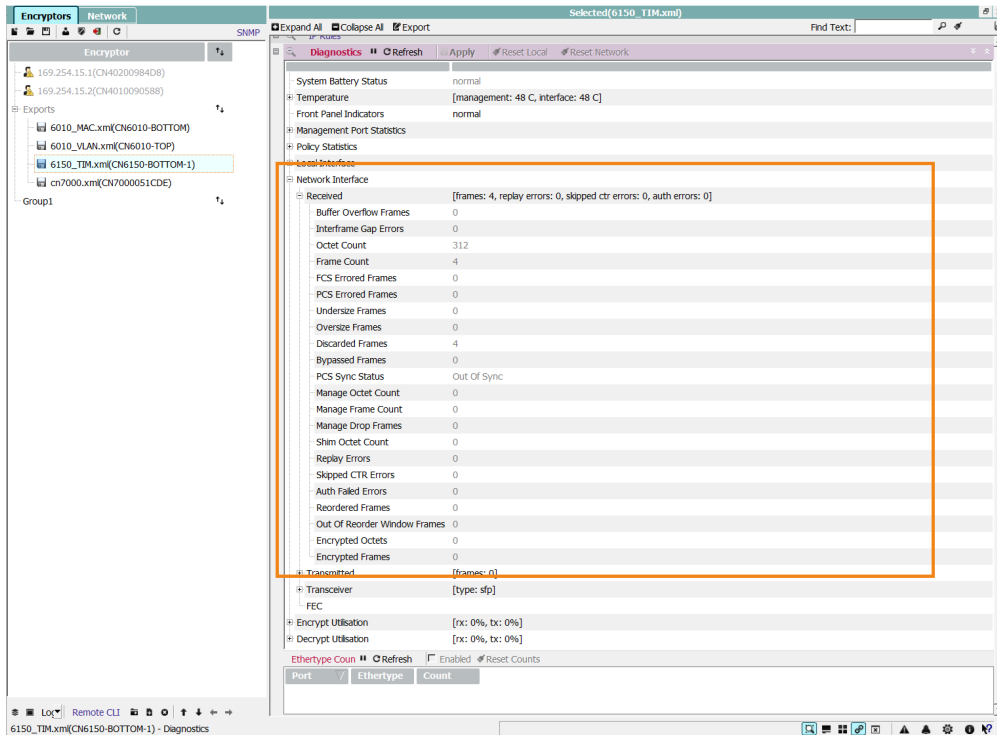


Figure 133: Network interface Diagnostics

For details of each of the available fields refer to the Local interface above.

The **Reset Network** button at the top of the display resets the following:

- network port statistics
- network ethertype statistics (TIM operational mode)
- network IP Rules table statistics
- Tx and Rx tunnel/connection statistics

Alarms

The Alarms option allows you to examine and optionally acknowledge encryptor alarms. All alarms can be acknowledged or individual alarms can be selected and acknowledged. It may be necessary to use the Refresh button to see the updated state of the alarms.

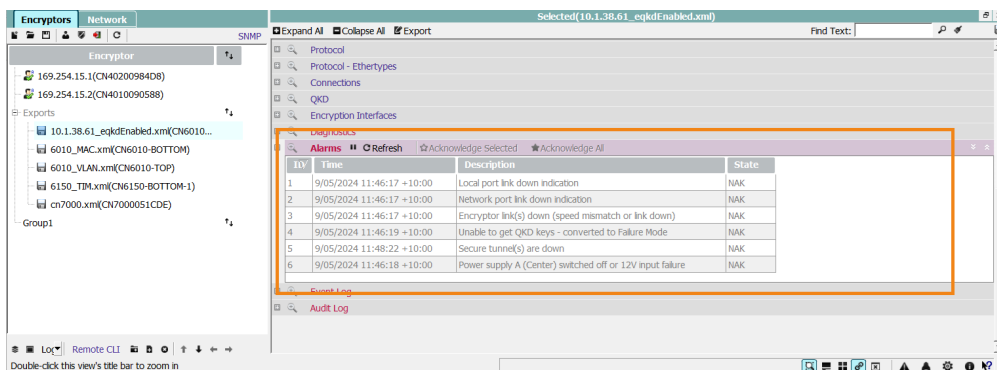


Figure 134: Encryptor Alarms

- **ID** - sequential index of alarm entry
- **Time** - time the alarm was raised
- **Description** - a description of the cause of the alarm
- **State** - the current state of the alarm, which can be 'active' or 'inactive' and is flagged as acknowledged (ACK) or unacknowledged (NAK)

Audit Log

The Audit Log option allows you to examine the audit log, which includes all of the activities that have been executed by the users who have accounts within the encryptor. The Audit log can be saved as a text file and, if desired, cleared. The 'Description Filter:' field can be used to search for and highlight all of the entries that match an entered term.

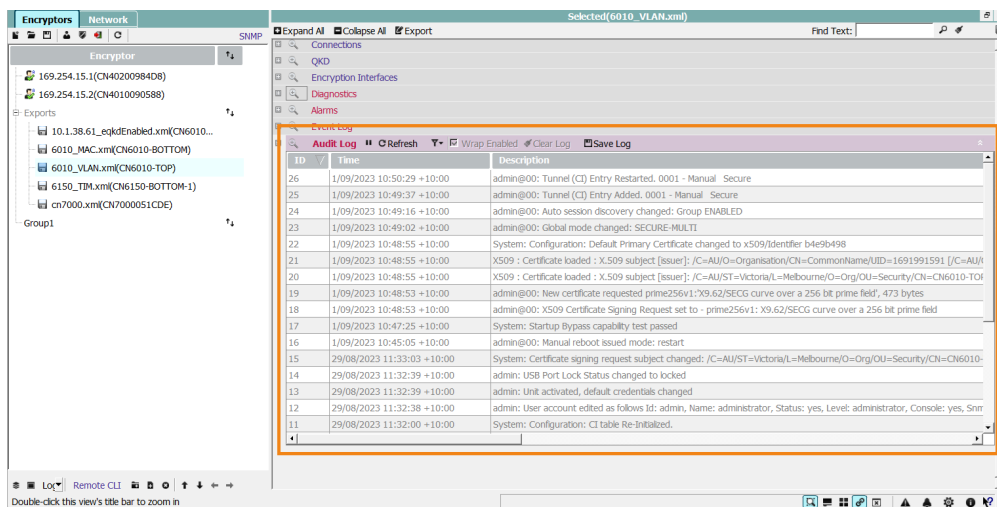


Figure 135: Audit Log

- **ID** - a sequential number that identifies the order in which the operation was logged
- **Time** - the date and time that the operation was performed
- **Description** - a description that includes the users identifier and the operation that was performed

Event Log

The Event Log option allows you to examine the events that have been generated within the encryptor. The log can be saved to a text file, and if desired, cleared. The 'Description Filter:' field can be used to search for and highlight all of the entries that match an entered term.

Figure 136: Event Log

- **ID** - a sequential number that identifies the order in which the event was logged
- **Time** - the date and time that the event occurred
- **Description** - a description that shows the nature of the event

Upgrade screen

The firmware of an encryptor can be updated using either CM7 as described in this section or by using a USB file.

When the Upgrade interface is selected, the instructions and fields shown in Figure 137 on the next page are displayed.



NOTE: An upgrade will require a reboot of the encryptor which will check the validity of the default certificate. If the certificate has expired then traffic will not restart. It is recommended that the validity of the certificate be checked prior to performing an upgrade.

The four upgrade tasks are:

- External Upgrade
- Internal Upgrade
- Backup
- Restore

WARNING: Backup and Restore are only functional when using versions of the firmware prior to 5.x.

External upgrade

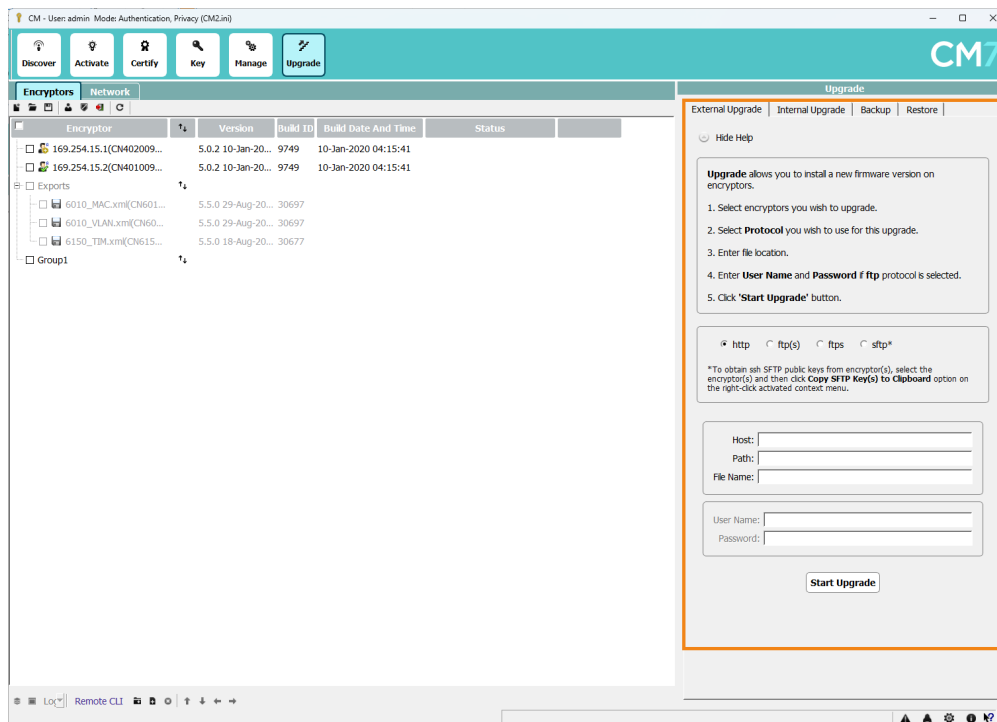


Figure 137: External upgrade dialog

Protocol - Select the appropriate communication method for the upgrade process: HTTP, FTP(S), FTPS or SFTP*

FTP(S)

- The FTP(S) option uses (unencrypted) FTP if a certificate is not configured in the FTP server table of your encryptor
- If a certificate is configured, encrypted FTPS is used.

Explicit FTPS

- is used when



- Both FTP and explicit FTPS use default port 21 at the FTP / FTPS server.
- The ftps option always uses encrypted FTPS. A certificate must be configured in the encryptor's FTP server table. Implicit FTPS is used.
- Implicit FTPS uses default port 990 at the FTPS server.

Host - defines the IP address of the server on which the upgrade image has been loaded

Path - defines the location of the file on the server

File Name - defines the name of the upgrade image

User Name - defines the HTTP or FTP user name

Password - defines the password that allows access to the server

WARNING: When attempting to upgrade an encryptor over inband management, the file transfer time could take longer than five minutes.

Internal upgrade

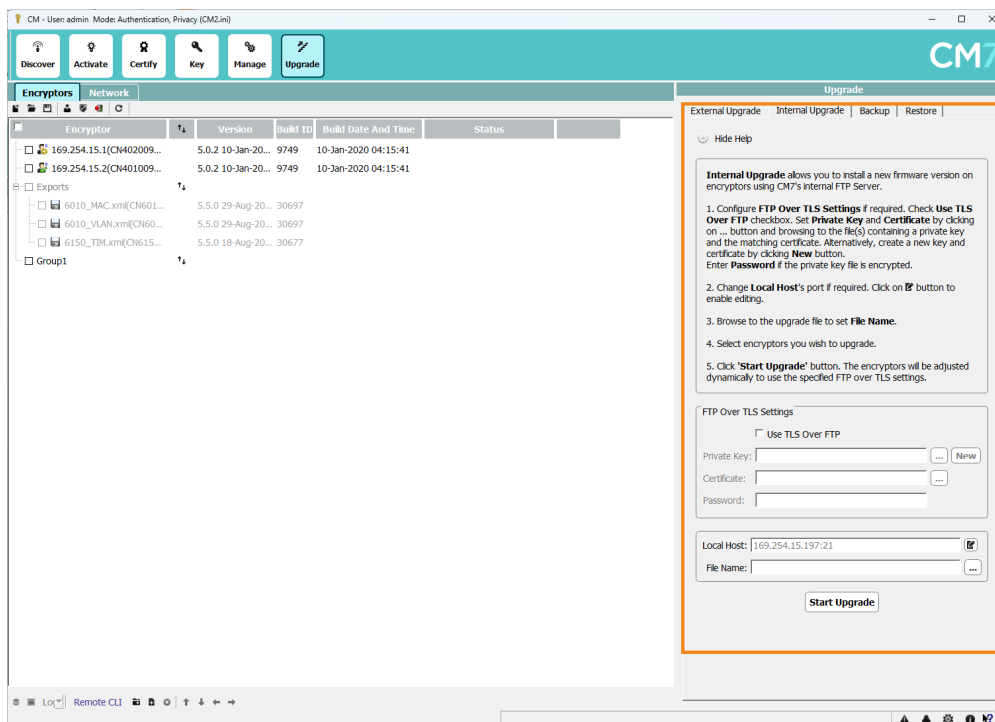


Figure 138: Internal upgrade dialog

NOTE: An upgrade will require a reboot of the encryptor which will check the validity of the default certificate. If the certificate has expired then traffic will not restart. It is recommended that the validity of the certificate be checked prior to performing an upgrade.

Private Key -

Certificate -

Password - defines the password that allows access to the server

Local Host -



File Name - defines the name of the upgrade image

Exiting from CM7

The simplest way to exit CM7 is to 'Close' the main window.

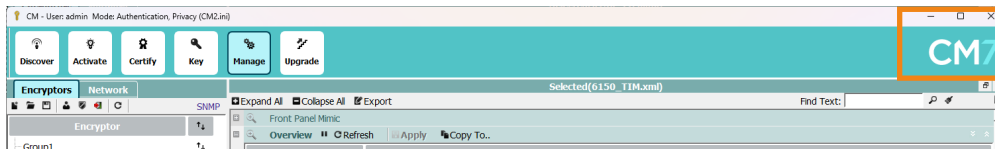


Figure 139: Exit via CM7Close button

It is also possible to exit from CM7 by clicking on 'Log out the current SNMP user' which requires confirmation.

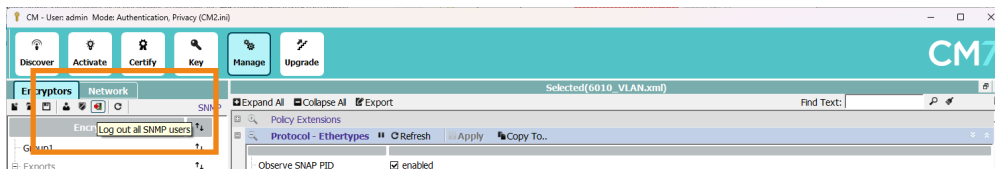


Figure 140: Exit via Logout Icon

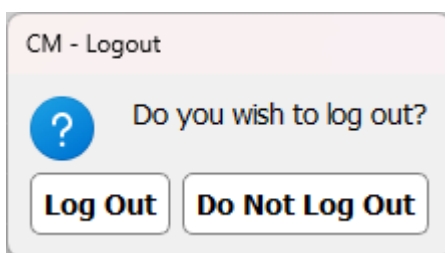


Figure 141: Logout confirmation dialog

Or if you are in the user credentials screen (see Figure 1 on page 1) you can just select 'Exit'.

Section 4: Command Line Interface (CLI)

CLI Management

Encryptors can be managed via a serial port that supports a Command Line Interface (CLI).

NOTE: Details of the required physical connection and its configuration are provided in the installation manual for the encryptor.

All Senetas encryptors provide a Command Line Interface (CLI) that can be accessed using a terminal emulator connected to the serial 'craft' interface. The functionality provided by the CLI is similar to that provided by CM7, however the latter is required for the activation and/or certification of units.

The CLI information is organised as follows:

- description of access
- login process
- command formatting
- alphabetic listing of commands

The sections that follow describe the overall functionality of the CLI. An alphabetic listing of available commands begins on page 225.

The Command Line Interface (CLI) is provided via an RS232 serial connection that allows a PC to log onto and issue commands to the encryptor. The PC requires a suitable terminal emulation program. The CLI provides the ability to configure and manage most of the settings of an encryptor.

CLI connection

The Command Line Interface (CLI) operates through the serial connection. It requires a user account on the encryptor and the user must login with the same authentication password as used with CM7. The CLI enforces a 3-try, 3-minute lockout process to prevent automated attacks; a session timeout is used to log the user out after 10 minutes of inactivity.

The CLI provides a comprehensive management capability including the ability to configure encrypted connections, manage user accounts and view log records and alarms.

Customising the CLI

A number of CLI messages can be tailored to the needs of users. The pre-login and post-login messages can be used to provide network advice and identify and confirm the specific encryptor that has been discovered and subsequently logged in to.

The Prompt message is shown ahead of the CLI command prompt and is usually set to a string that uniquely identifies the unit that you have logged in to.

The Command Line Interface can be customised as follows:

- Configurable prompt
- Configurable pre-login and post-login banner messages

The prompt is the text string that is displayed ahead of the '>' symbol to identify the encryptor to which you are connected. It can be used to show the logical name of the unit within the network, or perhaps the physical location.

The pre-login banner message is displayed on the controlling terminal prior to the LOGIN prompt. It lets the user know that they have a physical connection to the unit.



The post-login banner message is displayed after a successful login to the CLI. It can be used to provide confirmation of the identity of the encryptor, or provide other management information to the user.

Table 41. CLI user prompts

Feature	Description
Pre-Login Banner	The message that will be displayed before the user logs in
Post-Login Banner	The message that will be displayed after the user logs in
Prompt	The prompt that will be displayed in the CLI

Examples of these messages are:

```
This message is shown when connected to the CLI prior to logging in.
LOGIN:admin
PASSWORD:*****
This message is shown after logging in on the Command Line Interface and prior to the
prompt.
CN6140_A>
```

The 'CLI prompt' can also be set using the CLI **prompt** command as shown on page .

When a user connects to the console port, the encryptor will prompt for a user name and user authentication password. Access is denied if the user name and/or password are invalid. After three failed attempts the console will be locked for three minutes.

After access is granted, the console port presents a command prompt and provides access to the command line interpreter so that configuration parameters can be viewed and/or changed. The CLI enforces the same user-role privileges as those required for SNMP management.

Users are automatically logged out if there has been no user input on the console port for ten minutes.

A list of available commands can be obtained by typing help. Additional help can be obtained on each command by appending -h to any of the commands.

Commands give appropriate error messages when used incorrectly or with incorrect parameters.

The console supports a command history buffer that is 25 commands deep. The buffer may be accessed by using the up and down arrow keys to cycle through it.

Hosts and slots

Encryptors that support the multi-slot architecture use the **slot** command to configure and manage the available slots. The initial login to the CLI provides access to the host after which the slot command access the selected slot.

Commands

Each of the commands is described in the Command Line Interface section beginning on page 225. The summaries include a table that defines the applicability of the command, a description, the command format and examples of its use.

Where a command requires a hexadecimal argument, the value is usually entered in the 4 character (hhhh) form. CLI output will usually display hex values in the Hhhh form, however this document specifies them using the 0xhhhh form.

NOTE: The encryptor will not be damaged by anything you type into the CLI.



Section 5: SNMP Management

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

The way in which CM7 connects to an encryptor is usually dictated by the type of network that is available. The sections that follow discuss each of the approaches that can be taken and the reasons why they would be selected.

After you have selected the method that best suits your needs, you can refer to the appropriate configuration information in the sections that follow.

Management connections:

Encryptors are managed using a connection to their management ports.

Each encryptor is supplied with cables for both the Serial and Ethernet ports.

Authentication only (authNoPriv)	A users' credentials are authenticated before they can access the encryptor
Authentication and Privacy (authPriv)	SNMP traffic between CM7 and the encryptor is encrypted

NOTE: If an encryptor does not respond to the CM7 SNMP request, it may be necessary to cancel and re-issue it.

SNMP connections	227
Direct connection to front panel	228
In-band overview	229
Out-of-band management	234

SNMP connections

Encryptors can be managed locally by CM7 via the RJ45 connector on the front panel using Simple Network Management Protocol version 3 (SNMPv3).

SNMPv3 is an industry standard that addresses the deficiencies in the two earlier versions of the protocol by adding support for authentication and encryption. SNMPv3 security uses the concept of a user for which security parameters (levels of security, authentication, privacy protocols, and keys) are configured for both the agent and the manager. The security model protects against message delays and message replay by using time indicators and request IDs. Management packets can be sent with authentication only – authNoPriv - or with both authentication and privacy (encryption) - authPriv.

UDP (User Datagram Protocol):

The UDP protocol is connectionless, which means that the management system issues commands which are never acknowledged by the encryptor.

UDP works well in any network and CM7 can change both the retry and timeout parameters to accommodate both noise and network delays.



Direct connection to front panel

A direct connection from the system hosting CM7 to the RJ45 connector on the front panel is the simplest means of managing an encryptor. For this to operate, a common subnet is required and switches are often used to connect to and manage multiple units.

This connection method is suitable for local connections in data centres or for test set-ups used to configure units prior to deployment. The system on which CM7 is running needs to be able to access the front panel IP address of each encryptor.

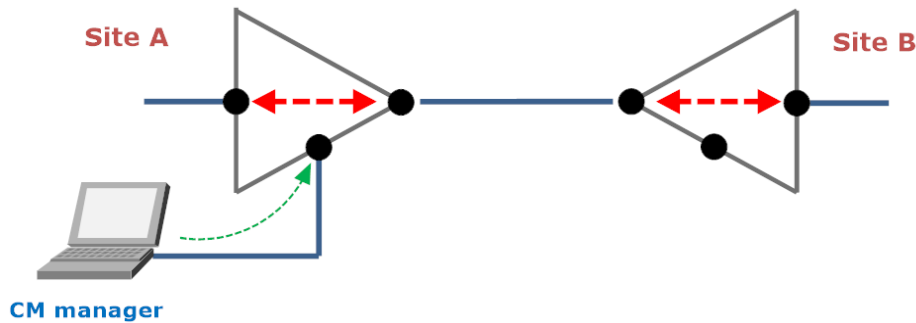


Figure 142: Direct Connect Management

Which connection?

The simplest way of managing an encryptor is via a direct connection to the front panel of a local unit or via a Layer 3 network to remote units.

In some cases an out-of-band connection may not be available and the 'in-band' method may be required.

SNMPv3Q

To defend against the quantum threat, the current SNMPv3 Diffie-Hellman(DH) kick-start mechanism now provides parallel (Hybrid) DH and QRA KEM mechanisms. The encryptor (SNMP agent) and CM7 (SNMP browser) will be able to determine both the DH Key and KEM shared secret which will then be XORd together, providing quantum resistant operations.

This hybrid DH kickstart method can be enabled via the CLI command ***snmpcfg -q on | off*** or via CM7 'SNMP' pane, 'SNMPv3Q' tick box in the 'Manage' screen.

'Enhanced SNMPv3' must be enabled for SNMPv3Q to function.

NOTE: Other third party SNMP browsers may not support this hybrid SNMP DH kick-start mechanism. Please ensure that CM 7.10.0 or later is installed to make use of this feature.

CM7 will be capable of managing a mixture of SNMPv3Q disabled and enabled encryptors simultaneously.

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

SNMP Enhanced Algorithm Support

Senetas encryptors also support SHA512 for authentication and AES256 for privacy for SNMPv3.

Enhanced algorithm support can be enabled in two ways:

- via the CLI command ***snmpcfg -e on | off***
- via the CM7 'SNMP' pane and selecting the 'Enhanced SNMPv3' tick box in the 'Manage' screen.

NOTE: In order to provide backward compatibility, if this configuration is disabled, SNMPv3 will use SHA1 for authentication and AES128 for privacy.

When an encryptor is first upgraded to v5.5.0, the default setting for 'Enhanced SNMPv3' will be **disabled**. However, ALL subsequent triggers, such as a factory erase or re-upgrading to v5.5.0, shall retain whatever setting had been selected for 'Enhanced SNMPv3' configuration prior to the trigger.

CM 7.10.0 will automatically determine whether a particular encryptor is configured for SHA1/AES128 (Enhanced SNMPv3 disabled) or SHA512/AES256 (Enhanced SNMPv3 enabled) and is capable of managing both simultaneously.

References:

OAEP see - https://en.wikipedia.org/wiki/Optimal_asymmetric_encryption_padding

<https://www.cyber.gov.au/acsc/view-all-content/guidance/asd-approved-cryptographic-algorithms>

In-band overview

Inband management is considered to be a preferred method of managing encryptors since it operates irrespective of the encryptor state and does not require the use of a secondary network. It is available for models that encrypt using supported protocols.

Inband connection

To provide the IP connectivity over the network, one encryptor must be configured as an inband management gateway capable of forwarding IP packets (received from the front panel Ethernet port) to peer encryptors that are connected via the network.

References to the "local or gateway encryptor" refer to the encryptor that is managed directly via the front panel Ethernet port. References to a "remote encryptor" refer to an encryptor that is logically connected to the gateway encryptor through the data network.

The appendix describes the general theory of operations for inband management and then outlines the technology-specific differences and/or limitations.

In-band connection via a local encryptor

An alternative approach (unless operating in TIM mode) is to configure the local encryptor as a gateway that can be used to manage remote units 'in band' over the same network that the encryptors are being used to secure. The management traffic is not encrypted by the units, but is secured by SNMPv3 encryption.

Each of the remote encryptors has a 'virtual IP' address assigned to it so that it can be discovered by CM7. The system on which CM7 is running must have a route added so that traffic directed to these virtual addresses is sent to the local gateway encryptor. See "Configuring Inband management" on page 1 for further details.



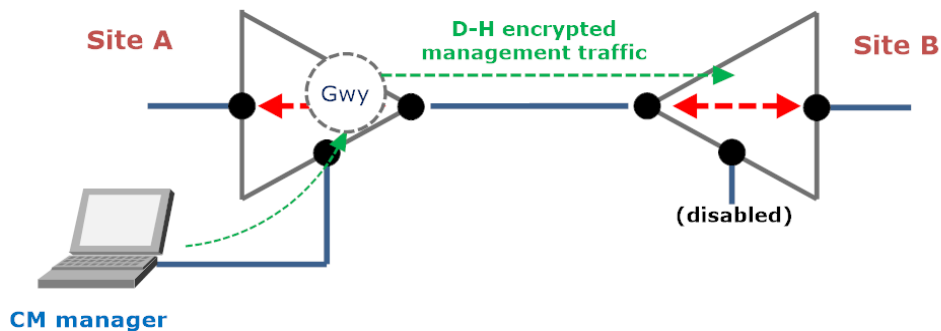


Figure 143: In-band Management

Multi-slot configurations

The management of hosts in remote encryptors is not supported via in-band management .

Virtual IP addresses

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

The virtual IP addresses assigned to the remote units are only used by the gateway encryptor and do not exist on any network.

Inband management concept

Inband management is achieved by configuring an encryptor to act as a management gateway device referred to as the 'gateway encryptor'. The gateway encryptor connects between the computer on which the management application (CM7) is running and the remote encryptors you want to manage.

NOTE: Only one encryptor can act as the gateway encryptor.

Management IP packets are sent from the PC to the front panel of the gateway encryptor which then forwards them over the network to the remote device(s). It is this gateway mechanism that provides the underlying support for inband management.

When acting as a gateway on non-Ethernet configurations, the encryptor resolves IP destination addresses to network connections to determine where to send each management packet. To achieve this, when a packet arrives which must be forwarded to an unknown destination, the encryptor performs a broadcast to other encryptors in the network to try and resolve the address (similar to the way ARP works on an Ethernet network).

Inband management can be configured on a local unit using the command line interface (see the 'ip' command in the CLI guide) or on remote units using CM7 as described in the next section.

The following settings are configurable via the command line IP command:

- Management IPv4 address, mask and gateway – IPv4 address of the front panel Ethernet port used for management.
- Management IPv6 address, mask and gateway – IPv6 address of the front panel Ethernet port used for management
- Inband management port of IPv4 and IPv6 addresses used for inband management
- Inband gateway function – enable or disable
- Management port settings - auto-negotiate, speed and duplex
- Inband VLAN tag (Ethernet only) – used in line mode to define a VLAN tag which is added to inband traffic

After entering the IP command, the console displays the current setting for each field in parentheses and allows the user to type in a new value if desired. Pressing ENTER accepts the current value. Each field uses a 4-byte value displayed in the dotted decimal notation, for example, 203.21.127.32.



Enabling Inband management

Inband management is enabled and configured from the CLI IP command (see Console command reference) or from CM7.

Inband configuration

The inband configuration of remote encryptors requires that the following LAN rules are observed:

- Because only IP packets that belong to the subnet defined by the inband IP address will be forwarded from the front panel Ethernet port to the network encryption port, all inband management virtual IP addresses must be on the same subnet
- The PC running CM7 must have a Static Route added to its stack to ensure that inband packets are routed to the front panel of the gateway encryptor. In the example that follows the command on the PC would be:

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

NOTE: Running the ADD ROUTE command may require elevated privileges which requires that you right click on "Command Prompt" and select "Run as administrator".

Note that if the management traffic is routed to the front panel of the gateway encryptor then the router may require the addition of a static route.

The local encryptor will not respond to an ARP of its inband IP address or any known remote encryptor inband IP addresses. It will only respond to an ARP of its local IP address.

The figure below shows a management PC connected to the front panel of an encryptor that has been configured to allow inband management of remote encryptors. The configuration process establishes IP and Gateway address for both the front panel and inband interfaces on both the local (gateway) and remote (managed) encryptor(s). (If required the local front panel can also have IPv6 addresses specified.)

The most important things to note in this example are:

- On the remote encryptor make sure that the default and inband gateways both point to the inband IP address of the gateway encryptor.
- Ensure that the network masks are set correctly for both the management Ethernet port and inband addresses.
- Ensure that the static route on the management PC is set correctly so that all packets to the inband network are routed to the management Ethernet port of the gateway encryptor.
- Ensure that the inband encryptor has the Management Gateway function is enabled via the CM7 Network address pane as described on page 182.
- Ensure that the inband encryptor has the Management Gateway function is enabled via the CM7 Network address pane as described on page 182.
- If a remote (non-gateway) encryptor has a firmware release lower than v5.0x the encryptors front panel should be disabled to prevent loops.

In the case of the local gateway encryptor where inband management is enabled, management traffic is redirected via the gateway (192.168.0.1) to the inband address of the remote encryptor (192.168.0.2). Note that non-management traffic (that is data addressed to a subnet other than 10.0.0) would be directed via the front panel gateway (10.0.0.8).



Table 42. 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

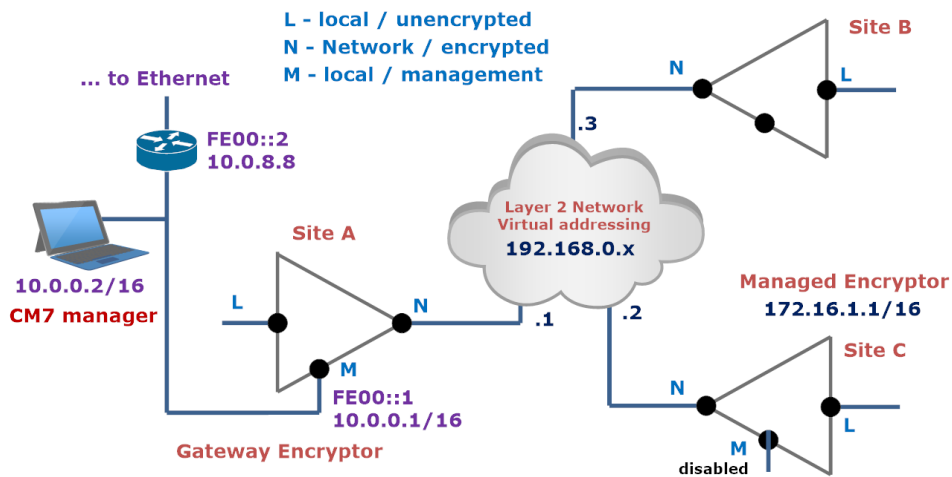


Figure 144: Inband configuration

Table 43. Managed 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

For the above the network in which CM7 is located will require the following ROUTE ADD command to ensure that traffic is routed to the encryptors.

```
ROUTE -p ADD 192.168.0.0 MASK 255.255.255.0 10.0.0.1
```

NOTE: The `-p` switch is required to make the command persistent across reboots of the CM7 manager host system. As an alternative, the command can be added to a startup batch file.



Inband for Multi-slot encryptors

Senetas multi-slot encryptors, for example the CN6140, are managed via a front panel 'host' IP address and a 'slot' IP address for each of the encryptors. Inband management requires that each of these is assigned a virtual IP address and the appropriate 'add route' commands are added to the management system. These steps ensure that both the local and remote encryptors can be managed, note however, that remote hosts cannot.

A common configuration used for 'multi-tenant' environments is one where a multi-slot encryptor is located at a central service provider and 'tenant' encryptors are located remotely at tenant sites. In this scenario each remote tenant can administratively manage in-band both their local unit and their assigned 'slot(s)' at the central site. The service provider is provided with 'supervisor' access to manage the central slot and the network parameters of the local and remote slots.

The CN6140 platform in multi-slot mode supports a two slot configuration at the 10G speed for line, VLAN, MAC and TIM operational modes.

A CN6140 encryptor now supports the following configurations:

- CN6140 1x1G Line, MAC, VLAN, TRANSEC and TIM
- CN6140 1x10G Line, MAC, VLAN, TRANSEC and TIM
- CN6140 2x10G Line, MAC, VLAN and TIM
- CN6140 4x1G Line, MAC, VLAN and TIM
- CN6140 4x10G Line

To modify the CN6140 platform from single slot mode to multi-slot mode or to select which multi-slot configuration to run, please use one of the following methods:

- the ***protocol -s*** CLI command
- the equivalent SNMP OID command
- the 'Protocol' field in the 'Manage' screen of the CM7 'System' pane.

Multi-slot encryptors operation in TIM mode do not support inband management, however Virtual management can be used if they are configured for 1 x 1Gbps or 1 x 10Gbps operation.

Routing considerations

All of the management traffic used to configure and/or monitor the state of an encryptor is based on the SNMPv3 standard using the UDP protocol on port 161.

Each encryptor has a configurable 'front panel' Ethernet address which can be defined using the IPv4 and/or IPv6 format.

Management traffic is routable and therefore, provided that the 'front panel' Ethernet connection of a unit can be accessed, the unit can be managed. As a general rule the accessibility of an encryptor can be determined by 'pinging' its management address.

Address translation, Port forwarding

Encryptors may be located within a subnet that is accessed via a router that applies network address translation (NAT) to the traffic. In these cases the network may use a single IP address for all units and differentiate between them via a unique port number. CM7 supports these configurations by allowing encryptors to be discovered using the unique IP address-Port combination. Refer to page 162 for details of the discovery process.



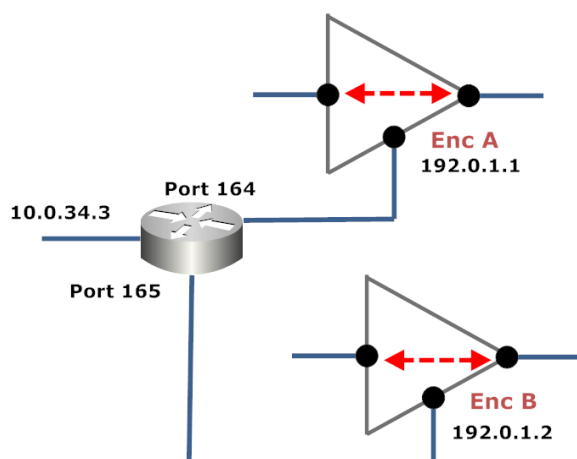


Figure 145: Address translation

The above example illustrates how two encryptors are accessed via a router at 10.0.34.3 in which the routing rules provide for translation to the encryptor IP addresses based on the port number of the traffic's .

Virtual management

Virtual management allows encryptors operating in TIM mode to be managed via the local interface or the network interface as a part of crypto stream.

WARNING: Virtual Management is not supported on multi-port CN6140 configurations operating in TIM mode.

On FPGA based encryptors Virtual Management traffic is bypassed and not encrypted. On DPDK based encryptors (for example, CN7000 and CV1000 models), Virtual Management traffic can be bypassed or encrypted (L3/L4) by utilising IP Rules either via the unlisted IP Rule action or configuring specific IP Rules.

Caveats:

- Enabling or disabling Virtual management will reboot the encryptor
- With the exception of a factory erase (i.e. **erase -f**), Virtual Management configuration is persistent across all reboots and erases.
- Virtual Management does not support IPv6 addresses.

Virtual Management can be enabled using CM7 or the **ip -v** CLI command or the equivalent SNMP OID. The features state is visible and configurable in all modes but it is only functional in TIM mode.

WARNING: When attempting to upgrade an encryptor over inband management, the file transfer time could take longer than five minutes.

Out-of-band management

If the unit to be managed is in a different location, then the SNMPv3 traffic can be routed via a Layer 3 network to the front panel of the encryptor. Because the SNMPv3 traffic is encrypted the connection is secure.

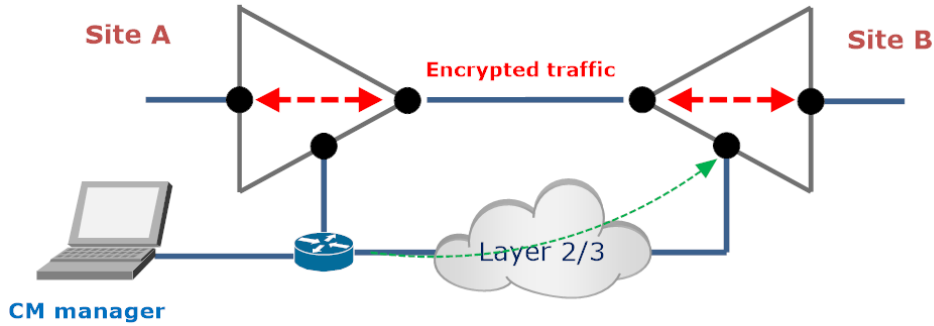


Figure 146: Out-of-Band Management

In-line management through the encryptors

In this mode of operation the management traffic is inserted into the data being encrypted by the units and connected back to the physical front panel of the remote unit(s). **This method is not recommended as the operational state of the encryptors can impact connectivity.** Note - the alternative 'in line bypass' mode can be used for encryptors located within Shortest Path bridging networks.

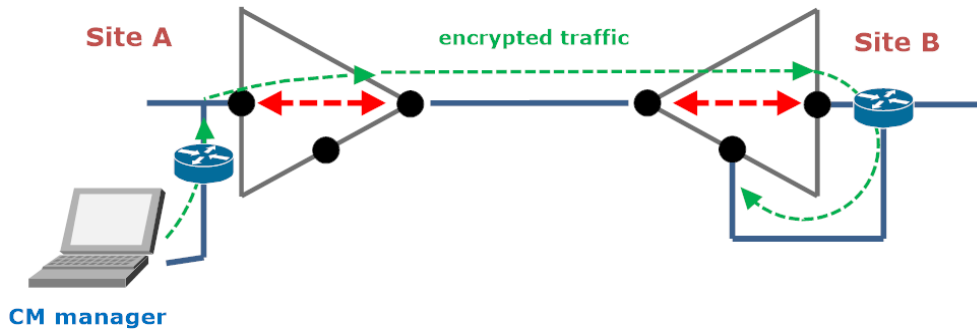


Figure 147: In-line Management

Section 6: Encryptor Troubleshooting

This section describes common situations where operation of an encryptor may not be as expected.

Configuration Export	236
Configuration Import	236
Traffic analysis	236
Ethertype diagnostics	237
ePing command	237
Cannot add a connection to the connection table	237
Traffic processing (only layer 3, 4)	240
Safety warnings	241

Configuration Export

The non-secure configuration parameters of the encryptor can be exported to a text file using the CM7 menu item.

The purpose of this file is to provide a source of information that can be used by both local staff and support personnel to determine the probable cause of any problems.

NOTE: No security information is included in the file.

If you require assistance in diagnosing problems then you should provide support staff with details of your configuration(s).

CM7 allows you to export the configuration via the 'Export Config' button at the top of the management pane. You can then post the resulting XML file on the Customer support portal.

Configuration Import

From the CM7 management window, select and open the XML file containing the configuration settings for an encryptor.

Once the XML file has been opened it will be displayed in the list of encryptors in the left-hand panel of the CM7 interface, Select the specific pane you need to modify.

A group of settings (in a pane) can be imported back into one or more encryptors.

In the sections that follow a number of frequently asked questions are listed, followed by suggested causes and suggested solutions or further steps to take to diagnose a problem.

Traffic analysis

Wireshark is a free program used for network analysis. It can be used to produce PCAP files that can be shared with support.



Ethertype diagnostics

The CN Series encryptors contain a diagnostic facility that can display a count by ethertype of all received Ethernet frames. This facility introduces additional processing and it is recommended that it is disabled unless required.

The CLI **etherypes** command as described on page can also be used.

These counts can be used to determine whether there is any unexpected traffic within the network that may be the cause of problems. If this is the case then CM7 or the CLI **etherypes** command can be used to modify the policy to address this.

ePing command

The CLI eping command described on page , is similar to the network ping command in that it can be used to send an Ethernet frame to one or more peer encryptors and then display any returned frames. The command can be sent to the broadcast domain or a specific MAC address and the frame can be of variable length and tagged with one or two VLAN tags.

The command is used to test both the connectivity to remote units and to determine that they are operational and able to respond to management requests.

This section is a general troubleshooting guide to help diagnose and fix problems that may occur during the course of configuring and operating Senetas encryptors. Specific information for each of the protocols is provided in their own chapter.

Cannot add a connection to the connection table

No valid certificate

An encryptor needs to have a valid certificate loaded before any connections or user accounts can be created. (See "User account management" on page 122)

The Secure LED is red when the encryptor does not have a valid certificate and turns green once one has been loaded.

There are a number of possible reasons why a session between two encryptors will fail to establish itself. The most common reasons are listed here.

The connection status itself (UP, DOWN, FLOW1 etc together with the event log messages are the most powerful diagnostic tools available.

The recommended diagnostic method is:

1. Firstly ensure that the network is working correctly without the encryptors installed
2. Configure the encryptors into bypass mode, insert one or both into the network and ensure everything is working
3. Switch to secure mode and test again

In addition, you can use the CLI eping command to test connectivity between encryptors. Note that on some provider networks VLAN tagging may be required. This command can be used when:

- Connections do not come up
- Connections come up, but no end to end traffic is seen
- Connections come up, but traffic is intermittent

Certificates signed by different CAs

Each encryptor in a network must be signed by a root CA for that network. Encryptor authentication is based on signed X.509 certificates loaded into each unit from the root CA.



If two encryptors which have certificates signed by different CA's (i.e. different copies of CM7) attempt to establish a secure connection then they will fail the authentication stage and the connection will be rejected.

In this case an authentication failed message will be logged in the event log.

Certificate expired

Certificates have a validity period (default of one year but user configurable). The validity period is used as part of the peer-to-peer authentication process between encryptors.

If either of the two encryptors have a certificate that has expired, the connection will be rejected. An event log message is logged.

Incompatible security settings

The security settings for each connection (i.e. encryption algorithm, mode and key length) are exchanged during the key exchange process.

Connections with incompatible settings cannot be established.

An event log message is logged.

FIPS mode incompatibility

Encryptors must be set to the same FIPS mode (on or off), as this determines the message digest algorithm employed during authentication.

An authentication failed message is logged.

Cable plugged in to wrong port

Secure connections are established between the network interfaces of peer encryptors.

If the network cable is plugged into the local port of the encryptor by mistake then received traffic will be discarded by the encryptor and no session will be established.

In this fault state it appears to the user as if the encryptors are not talking to each other as they will never get further than the RESTART or FLOW1 states.

No message is logged.

Certificates cannot be installed

Internal key generation not completed

Before a certificate can be loaded the encryptor must have completed generating its own internal RSA key pair. A new key pair is generated every time a new certificate is loaded into the encryptor. This is normally a very fast process that would not be noticed by the user.

An encryptor indicates if it is still generating an internal key by flashing the secure LED orange. Once this has been completed the secure LED will turn red (if no certificate currently loaded) or green (if a certificate already exists).

Validity period

Encryptors will only accept a certificate that is currently valid (i.e. the 'Not Before' and 'Not After' times on the certificate must be respectively before and after the current time on the encryptor). This is usually performed using the 'Set Time' button.

If the time on the PC that is loading the certificate is ahead of the time on the encryptor then the default 'Not Before' date (set to the PC's current time) would cause the certificate to be invalid and rejected by the encryptor.

In this circumstance, either set the time on the PC slightly before the encryptor or manually adjust the certificate 'Not Before' time backwards (e.g. one hour) when loading it.



Password lexical checking is enforced and places strict requirements on the syntax of user passwords (see management section for details).

If the administrator password details that are loaded as part of the certification processes do not meet the lexical requirements then the new account and hence the certificate itself will be rejected.

Certificate details will not display

The details of certificates are normally displayed whenever a certificate is selected. If this does not happen then the most likely cause is a management network issue.

Certificate, users, disappear after a reboot/restart

Time not set

Encryptors rely on an internal real time clock to be set to a valid time during initial configuration. In the factory default state the encryptors real time clock does not have a valid time.

This is necessary because many of the security functions of the encryptor use time as part of the authentication process.

Encryptor tampered

The Series has a tamper mechanism that detects any attempt to access the enclosure.

If a tamper is detected the encryptor will return to a factory default state and lose all previously configured settings.

No logical network connection

The network port of the encryptors must be logically connected across the network.

If there is no connection across the network between the two encryptors then they will be unable to talk to each other to establish the session.

Master key issues

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 will start with an M or S to indicate if the encryptor is a Key Master or Slave for each connection.

On any VLAN or multicast connection there should only be one Master but there may be many Slaves. The Key Master is responsible for distributing encryption keys to all the Slave encryptors in the group. During normal operation the Master sends a keep-alive message to all group members every 3 seconds.

The protocol has been designed to be fault-tolerant. In the event of a device or network failure resulting in the loss of the Master the other group members will negotiate and one of the Slave encryptors will automatically assume the role of Master.

An encryptor will assume the Master role if it stops receiving keep-alive messages and cannot find any other peer encryptors to negotiate with. So if, for example, the whole network is down and the encryptors are unable to communicate then they will ALL report a connection status of UP but will ALL assume the Master role and NO data will flow as there is no network connectivity between them.



When this condition is detected, the units are placed in 'dead peer' mode and the traffic discarded. Restoration of connectivity allows the unit to exit from the dead peer mode and resume normal operation.

What we want to see on the connections is one encryptor reporting M(aster) and all the others reporting S(ave) this proves that the encryptors have successfully completed the key agreement and that the network is up and operating correctly.

VLAN connectivity issues

Setting VLAN mode does not enable auto-discovery

By design auto-discovery of VLAN connections is not enabled. For VLAN configurations it is considered best practice to enable auto-discovery to allow the encryptors to learn the available/required VLAN associations and then to disable the facility to inhibit further learning.

VLAN connections do not automatically restart

Discovered VLAN connections are stopped whenever the global mode is changed from 'Secure' to 'Discard' or 'Bypass'. Each connection must be individually restarted before it will be secured.

Traffic processing (only layer 3, 4)

When diagnosing network traffic issues it is recommended that protocols be tested separately as this makes it easier to determine the source of the problem. For example a firewall may be dropping TCP timestamped packets while UDP encrypted data is traversing the network.

The following can assist with troubleshooting:

- When operating in TIM mode a remote encryptor is identified by its KID 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 (and auto-discover) one at a time and verify if the remote encryptor gets discovered. (Then delete the remote encryptor specific CI and test with the other protocol)

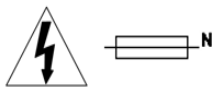
Cable problems

Occasionally, a damaged or faulty cable may be used to connect equipment within the network infrastructure of an organisation. Sometimes, every other possible cause is blamed for a network error. If practical, copper and fibre optic cables should be checked to see if they are the possible culprit.

NOTE: It is recommended that cables be checked in a test environment before plugging them into mission-critical networks.



Safety warnings



CAUTION: Double pole/neutral fusing

ATTENTION: Fusion pôle double/neutre



WARNING: Disconnect all power supply cords before servicing.

ATTENTION: Débrancher tous les cordons d'alimentation avant l'entretien.



CAUTION: Risk of explosion if battery is replaced by an incorrect type. Dispose of used batteries in accordance with local laws. Do not charge, heat, open or dispose of in a fire.

ATTENTION: Risqué d'explosion si la batterie est remplacée par un type incorrect. Jetez les piles usagées conformément aux lois locales. Ne pas charger, chauffer, ouvrir ou éliminer dans un incendie.



CAUTION: For continued protection against risk of fire, replace only with the same type and rating of fuse.

ATTENTION: Pour une protection continue contre les risques d'incendie, remplacer uniquement avec le même type et calibre du fusible.

Section 7: CLI Command Library

Each of the available commands is described in this section. The command summaries include a table that defines the applicability of the command, a description, the command format and examples of its use.

Where a command requires a hexadecimal argument, the value is usually entered in the 4 character (hhhh) form. CLI output will usually display hex values in the Hhhhh form, however this document specifies them using the 0xhhhh form.

activate

The **activate** command is used on encryptors that support X.509 certificates to change the default credentials prior to loading certificates.

Format:

<code>activate<CR></code>	
<code>-e</code>	enable encryptor for activation
<code>-d</code>	disable activation
<code>-l</code>	perform local activation
<code>-v</code>	verify hash code

```
CN6140_A>activate -e
Activate mode enabled. Awaiting Hash!
CN6140_A>activate -v
EF3233252A3B57A127E7812EAB274363EA4562FB3213BA68231EF3a
Confirm (y/n)?y
Encryptor is activated
```

Activate locally using the CLI

```
CN6140_A>activate -l
Account [admin]
Password>newPassword
Password>newPassword
Confirm[y/n]y
Encryptor is activated
CN6140_A>
```

Encryptors whose firmware supports the PKI infrastructure and associated certificates implement the **activate** command.

The **activate** command provides a secure method of changing the credentials of the 'admin' account from the default settings of admin/\$Password1 to those specified by the customer, thus 'activating' the unit. Certificates cannot be loaded until the encryptor has been activated.

Activation requires that the encryptor be placed in activate mode (-e) after which CM7 displays the activation digest of the encryptor and allows entry of the new credentials. When the supplied credentials have been transferred to the encryptor and the digest verified (-v), the unit is activated.

The -l option allows activation to be performed using the CLI only. When the command is executed the user is asked to enter the new credentials. Note that local activation should only be used in a secure environment where the management system is local to the CLI port.



alarm

The **alarm** command is used to display the current state of the alarm table and allows Administrators and Supervisors to acknowledge individual alarms.

Format:

alarm<CR>	List all active alarms
-a <x> <y>	Acknowledge alarms x,y, etc. Where x > y
-a *	Acknowledge all alarms
-n	Print the number of active alarms

Example:

```
alarm -a Acknowledge all alarms
CN6140_A>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
```

Alarm conditions that occur will be listed in the table with a state of ACTIVE_NAK (not acknowledged) at the same time an event log message is logged and a trap will be sent out if one or more trap handlers are configured.

Once acknowledged, an alarm state becomes ACTIVE_ACK (acknowledged); the alarm will remain in the table until the condition goes away.

If an alarm condition occurs and disappears before a user has acknowledged it then it will remain in the table in a state of INACTIVE_NAK. As soon as the alarm is acknowledged it will disappear from the alarm table as it is no longer in the active condition.

audit

The **audit** command is used to list records in the audit log.

Format:

audit<CR>	List the audit log
-l <n>	List the last n records in the log
-s <n>	List records in the log starting from n
-n	Print the number of records in the log
-c	Clear the audit log
-w <on off>	Turn wrapping on or off

Example:

```
CN6140_A>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
```



The audit log is a non-volatile record of changes made to the system configuration. Each record is time-stamped and contains the id of the user making the change as well as a detailed description of exactly what was done.

The records are displayed one page at a time and there are twelve records in each page. After the first twelve audit records have been displayed, you can:

- press <enter> to display the next record
- press the <space bar> to display twelve more records
- press <C> to display all the remaining records in the audit log

The audit log (like the event log) has a maximum record count of 4000. When the log fills up, new messages can either be discarded (wrapping mode disabled) or added to the log, replacing the previous oldest message (wrapping mode enabled).

The audit command allows Administrators to set the wrapping mode for the log as well as the ability to clear the log.

autodisco

For encryptors configured as layer 2 units the **autodisco** command turns MAC address auto-discovery on or off and allows the Multicast session timeout period to be specified.

For encryptors configured in TIM mode the **autodisco** command turns auto-discovery of any of Layer 2, 3 or 4 on or off.

Format:

<code>autodisco<CR></code>	display current automatic session discovery status
<code>[-e[u m]]</code>	'u' or 'm' to limit to Unicast or Multicast
<code>[-d[u m]]</code>	
<code>[-a minutes]</code>	-a for Multicast only, specifies the time in minutes after there is no traffic that the session is removed
<code>-e</code>	Enable autodiscovery
<code>-d</code>	Disable autodiscovery
<code>-e L2</code>	Enable auto discovery at Layer2
<code>-d L2</code>	Disable auto discovery at Layer2
<code>-e L3</code>	Enable auto discovery at Layer3
<code>-d L3</code>	Disable auto discovery at Layer3
<code>-e L4T</code>	Enable auto discovery at Layer4 TCP
<code>-d L4T</code>	Disable auto discovery at Layer4 TCP
<code>-e L4U</code>	Enable auto discovery at Layer4 UDP
<code>-d L4U</code>	Disable auto discovery at Layer4 UDP

Example 1: View current setting

```
CN6140_A>autodisco
Automatic session discovery: enabled
Layer2 Autodiscover : disabled
Layer3 Autodiscover : disabled
Layer4 TCP Autodiscover : disabled
Layer4 UDP Autodiscover : disabled
```

Example 2: Enable automatic session discovery



```
CN6140_A>autodisco -e
Automatic session discovery enabled
```

Point-to-Point (Line) mode

Auto-discovery is not required when an encryptor is operating in this mode.

Multipoint MAC mode

Auto-discovery allows for the automatic creation of connections from observed traffic. When enabled, Ethernet frames passing between local and remote encryptors with previously unknown source/destination MAC addresses will initiate the connection auto-discovery process.

The auto-discovery mechanism applies only for newly discovered MAC addresses, whilst the global setting is set to Secure. In this case, when a new MAC address is discovered the encryptor will assign it to the pending (connection identifier CI = 1) connection whilst it determines whether there is a remote encryptor protecting the address.

The CN Series uses a proprietary encryptor resolution protocol (ERP) to bind unknown MAC addresses to protecting encryptors. Through ERP management frame negotiation the identification of the remote encryptor can be established. If an existing connection exists then the unknown MAC address is assigned to that CI or in the case where no connection exists a new session establishment process is initiated.

The auto-discovery feature allows simple deployment of encryptors into a meshed network since the encryptors will automatically learn the topology and establish secure connections between themselves.

For security reasons it is recommended that once encryptors have been deployed and have learnt the network topology, auto-discovery be disabled to block all unknown MAC addresses.

Auto-discovery **MUST**, however be enabled for Spanning Tree Monitoring to operate.

Multipoint VLAN mode

Auto-discovery is off by default. The VLAN ID must be correctly specified prior to enabling auto-discovery.

Transport Independent Mode (TIM)

When operating in TIM mode auto-discovery can be enabled or disabled in a hierarchical manner. This means that if auto-discovery is enabled for layer 4 TCP or layer 4 UDP, the Layer 3 and Layer 2 auto-discovery modes are also enabled. And if auto-discovery for Layer 2 is disabled, then Layer 3 and 4 auto-discovery gets disabled accordingly. This is to prevent aliasing and false positive KID matches.

autopop

The **autopop** command enables or disables auto-population of connections.

Format:

<code>autopop<CR></code>	Display current Automatic population status
<code>-e</code>	Enable auto population of CIs
<code>-d</code>	Disable auto population of CIs

When auto population is enabled, the connection table will be cleared, the encryptor will reboot and as a result the IP Rules table will be cleared.

Example 1: Enable auto population

```
CN6140_A>autopop -e
Warning this command will delete existing connections and reboot the encryptor
```



```
Do you wish to proceed (y/n) Y
Automatic Populate enabled
CN6140_A>
```

banner

The **banner** command is used to view and modify the Pre-Login and Post-Login strings that are displayed on the CLI console prior to and after the user logs in.

Format:

banner<CR>	Display current Banners
-r <string>	Update pre-login banner
-o <string>	Update post-login banner

Example 1: View current settings (no banners)

```
CN6140_A>banner
Pre-login Banner:
Post-login Banner:
CN6140_A>
```

Example 2: Set Pre-login Banner

```
CN6140_A>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
CN6140_A>
```

During entry of banner text each line is prefixed with the count of the number of characters already entered.

Pressing <CTRL>D on the first line and then accepting the entry clears the banner text.

certificate

The **certificate** command indicates the status of the certificate of an encryptor. Multiple certificates are supported and these can be signed by different Certificate Authorities.



Format:

certificate<CR>	Display certificates
-p <idx>	Print certificate details
-i	Install PEM encoded X.509 certificate from CLI
-r	Print X.509 certificate signing request
-e	Set x509 Certificate Signing request type
-s	Display and set certificate signing request subject
-d	Delete certificate
-c	Set default certificate (Primary)
-C	Set default certificate (Ancillary)
-k <	Create CA Signing certificate
-d <DN>	CA DN (required)
-a <validity>	validity period in days (default is 10 years)
-s <serial>	serial number override: integer or 0x string (default is XX:XX:XX:XX:00:00:00:00)
>	e.g. -k -d /C=AU/CN=CA1 -a 7300 -s 0xaab-bccdd00000000
-q <	Create Encryptor certificate
-d <DN>	DN (required)
-a <validity>	validity period in days (default is CA end date)
-s <serial>	serial number override: integer or 0x string
>	e.g. -q -d /C=AU/CN=Encryptor1
-h	This help message

The certificate display shows whether or not a valid certificate has been loaded into the unit, and if so the details of the certificate including the Certificate Authority and the validity period.

Example:

```
CN6140_A>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
```

For RSA/ECDSA keys the key size is the physical key size and for QRA keys it is that of a symmetric DEK key that has equivalent strength.

NOTE: In legacy firmware, prior to the introduction of 'Activation' the -e, -d and -v commands were used to enable, disable, and to verify certificate mode. This mode of operation is no longer supported.



Self revocation of certificates used in tunnels

An encryptor shall validate its own certificate prior to commencing the session key establishment or key exchange process. Prior to the flow 1 message being sent, if the certificate is found to be invalid:

- the process is aborted
- the tunnel placed into fault state
- appropriate event message logged

NOTE: Self revocation is only possible in Line and TRANSEC mode, in addition to unicast tunnels in MAC mode.

If the certificate is valid, the flow 1 message is sent and the peer encryptor shall continue to authenticate the received certificate as per previous behaviour.

The **-e** option can be used by an administrator to set the CSR algorithm of an activated encryptor. The available algorithms is determined by the FIPS mode of the encryptor.

Quantum Resistant Algorithms

Support for quantum resistant algorithms was introduced in v5.2.0 of the firmware, the result being that 75 or more algorithms became available. Encryptors will offer a build dependant selection list as described below.

The list includes all QRA signing algorithms, regardless of whether FIPS mode is enabled or disabled.

Non FIPS approved RSA/ECDSA algorithms remain hidden unless FIPS mode is disabled.

The following usage flags in the CSR list provide selection guidance.

Usage Flag	Description
+FIPS	algorithm is FIPS approved
-FIPS	algorithm NOT FIPS approved
+TUN	algorithm may be used for tunnel encryption
-TUN	algorithm not available for tunnel encryption
+TLS	algorithm may be used for TLS connection (HTTPS/FTPS)
-TLS	algorithm not available for TLS connection
+PRI	may be selected as Primary (Default) tunnel certificate (currently can only be RSA/ECDSA approved algorithm)
-PRI	Not usable/selectable as Primary (Default) tunnel certificate
+ANC	may be selected as Ancillary (Default) tunnel certificate (currently can only be QRA approved algorithm)
-ANC	Not usable/selectable as Ancillary (Default) tunnel certificate

When certifying a unit for the first time, the Primary Default certificate is automatically set ONLY if that certificate is suitable as the primary default (e.g. RSA or ECDSA).

The ancillary default certificate is not set automatically and clearing it (0 value) will disable all QRA functionality.

It is expected that ALL encryption devices which are required to interoperate be set to the same configuration with regard to QRA operation and matching KEM selection.

NOTE: In the following example not all of the currently available algorithms may be shown.

Example:

```
CN6140_A>certificate -e
```



idx	Short Name	Comment
*1	: RSA2048	RSA 2048bit (+FIPS +TUN -TLS +PRI -ANC)
2	: secp256k1	SECG curve over a 256 bit prime field (+FIPS +TUN +TLS +PRI -ANC)
3	: secp384r1	NIST/SECG curve over a 384 bit prime field (+FIPS +TUN +TLS +PRI -ANC)
4	: secp521r1	NIST/SECG curve over a 521 bit prime field (+FIPS +TUN +TLS +PRI -ANC)
5	: prime156v1	X9.62/SECG curve over a 256 bit prime field (+FIPS +TUN +TLS +PRI -ANC)
6	: sect283k1	NIST/SECG curve over a 283 bit binary field (-FIPS +TUN +TLS +PRI -ANC)
7	: sect283r1	NIST/SECG curve over a 283 bit binary field (-FIPS +TUN +TLS +PRI -ANC)
8	: sect409k1	NIST/SECG curve over a 409 bit binary field (-FIPS +TUN +TLS +PRI -ANC)
9	: sect409r1	NIST/SECG curve over a 409 bit binary field (-FIPS +TUN +TLS +PRI -ANC)
10	: sect571k1	NIST/SECG curve over a 571 bit binary field (-FIPS +TUN +TLS +PRI -ANC)
11	: sect571r1	NIST/SECG curve over a 571 bit binary field (-FIPS +TUN +TLS +PRI -ANC)
12	: c2pnb272w1	X9.62 curve over a 272 bit binary field (-FIPS +TUN +TLS +PRI -ANC)
13	: c2pnb304w1	X9.62 curve over a 304 bit binary field (-FIPS +TUN +TLS +PRI -ANC)
14	: c2tnb359v1	X9.62 curve over a 359 bit binary field (-FIPS +TUN +TLS +PRI -ANC)
15	: c2pnb368w1	X9.62 curve over a 368 bit binary field (-FIPS +TUN +TLS +PRI -ANC)
16	: c2tnb431r1	X9.62 curve over a 431 bit binary field (-FIPS +TUN +TLS +PRI -ANC)
17	: brainpoolP256r1	RFC 5639 curve over a 256 bit prime field (-FIPS +TUN +TLS +PRI -ANC)
18	: brainpoolP256t1	RFC 5639 curve over a 256 bit prime field (-FIPS +TUN +TLS +PRI -ANC)
19	: brainpoolP320r1	RFC 5639 curve over a 320 bit prime field (-FIPS +TUN +TLS +PRI -ANC)
20	: brainpoolP320t1	RFC 5639 curve over a 320 bit prime field (-FIPS +TUN +TLS +PRI -ANC)
21	: brainpoolP384r1	RFC 5639 curve over a 384 bit prime field (-FIPS +TUN +TLS +PRI -ANC)
22	: brainpoolP384t1	RFC 5639 curve over a 384 bit prime field (-FIPS +TUN +TLS +PRI -ANC)
23	: brainpoolP512r1	RFC 5639 curve over a 512 bit prime field (-FIPS +TUN +TLS +PRI -ANC)
24	: brainpoolP512t1	RFC 5639 curve over a 512 bit prime field (-FIPS +TUN +TLS +PRI -ANC)
25	: DILITHIUM_2	(-FIPS +TUN -TLS -PRI +ANC)
26	: DILITHIUM_3	(-FIPS +TUN -TLS -PRI +ANC)
27	: DILITHIUM_4	(-FIPS +TUN -TLS -PRI +ANC)
28	: Falcon-512	(-FIPS +TUN -TLS -PRI +ANC)
29	: Falcon-1024	(-FIPS +TUN -TLS -PRI +ANC)
30	: MQDSS-31-38	(-FIPS +TUN -TLS -PRI +ANC)
31	: MQDSS-31-64	(-FIPS +TUN -TLS -PRI +ANC)
32	: Rainbow-Ia-Classic	(-FIPS +TUN -TLS -PRI +ANC)
33	: Rainbow-Ia-Cyclic	(-FIPS +TUN -TLS -PRI +ANC)
34	: Rainbow-Ia-Cyclic-Compressed	(-FIPS +TUN -TLS -PRI +ANC)
35	: Rainbow-IIIC-Classic	(-FIPS +TUN -TLS -PRI +ANC)
36	: Rainbow-IIIC-Cyclic	(-FIPS +TUN -TLS -PRI +ANC)
37	: Rainbow-IIIC-Cyclic-Compressed	(-FIPS +TUN -TLS -PRI +ANC)

Enter CSR type idx : 30

X.509 Certificate Signing Request set to [MQDSS-31-38]

Profiling MQDSS-31-38

Generating new key pair : 00.014836149 (secs)



Public Key Length : 46

Secret Key Length : 26

Length Signature : 28400

CSR Sign : 00.251873171 (secs)

CSR Verify : 00.179767866 (secs)

CN6140_A>

* indicates the currently selected KEM

The -k option is used to create a CA signing certificate. The distinguishing name is required.

Example:

```
CN6140_A>certificate -k -d /CN=DRBG-ROOT-CA
Got spare key
Created CA Signing cert
CN6140_A>certificate -q -d /CN=REST-SRV-CERT
X.509v3 Certificates:
  Id  Type    Identifier Alg Size  Expiry  State  In Use  Signed by
   3  x509 En  6ba56b01  RSA 2048  3649   Valid  No     self    /CN=DRBG-
  ROOT-CA
Enter certificate index: 3
Got spare key
Created Encryptor cert
CN6140_A>
```

The new HTTPS RESTful encryptor certificate is identified as 44891898

```
CN6140_A>certificate
Encryptor is activated
Default certificate           : Not set
No V1 or V2 certificates loaded.
X.509v3 Certificates:
  Id  Type    Identifier Alg Size  Expiry  State  In Use  Signed by
   3  x509 En  44891898  RSA 2048  3649   Valid  No     6ba56b01 /CN=REST-
  SRV-CERT
   4  x509 En  6ba56b01  RSA 2048  3649   Valid  No     self    /CN=DRBG-
  ROOT-CA
CN6140_A>
```



community

The **community** command is used to view and modify the Community string that is used in SNMPv1 messages.

Format:

<code>community<CR></code>	Display the current Community string
<code>-s name</code>	Set the SNMP community string

The encryptor must be rebooted for the new value to take effect.

con

The **con** command is used to view and modify the multipoint connection policy of an Ethernet encryptor.

Format:

<code>con <CR></code>	Display current Connection policy
<code>-m</code>	Enable MAC Connection mode
<code>-v</code>	Enable VLAN Connection mode

The connection policy defines the remote ID on which the connection policy will be based when the encryptor is in Multipoint mode. The command is not available if the encryptor is in Point-to-Point/Line mode.

When in 'MAC mode' the policy is based on the destination MAC address of the Ethernet frame and when it is in 'VLAN mode' it is based on the VLAN tag(s) within the Ethernet frame.

When in TIM mode the policy is based on the rules defined within the IP Rules table. Inband management is not available in TIM mode and all inband settings are ignored.

NOTE: When in TIM mode, the default crypto mode is GCM256 rather than CTR256.

Virtual management can be used to manage the encryptor via the Local or network port.

controlplaneif

The **controlplaneif** command is used to set the port over which key distribution will occur. The default is the Network port.

When VLAN is used as the policy for Ethernet encryption, keys are distributed using multicast management frames and certain topologies (for example, those using Link Aggregation) will limit the distribution of these. If the limitation exists, keys can be distributed via the front panel management port of an encryptor and its associated Layer 2 network.

Format:

<code>controlplaneif<CR></code>	Display current status
<code>[net man]</code>	Set key distribution port to either the Network port or Management port

crl

The **crl** command is used to view or modify the CRL server entries for an encryptor.

NOTE: It is recommended to use an FTP server. This must be entered in the FTP servers list on the Encryptor with a matching certificate.



Format:

crl<CR>	Print CRL server entries
-a <url>	Add CRL server entry
-c	Clear all stored CRLs
-d <idx>	Delete CRL server entry
-e <idx>	Edit CRL server entry
-p [idx]	Print CRL server entry details
-u [update interval]	Display or update CRL update interval

Example:

```

CN6140_A>crl -a http://10.0.1.34/crlfile.crl
CRL entry added
CN6140_A>
CN6140_A>
CRL update interval is 1 minutes
Index URL
1 http://10.0.1.34/crlfile.crl
CN6140_A>

```

crypto

<< This CLI command can be used with Layer 2 encryption only. >>

The **crypto** command is used change the encryption algorithm, mode and key size that an encryptor uses.

Format:

crypto<CR>	Display current crypto mode status
-s	Set the crypto mode

Example:

```

CN6140_A>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]
CN6140_A>

```



In order for the cryptographic mode to be changed, the encryptor must have its global processing policy set to Bypass or Discard. For CFB mode, 'observe SNAP PID' must be enabled so that intermediate networking devices do not drop encrypted SNAP PID frames.

NOTE: Virtual encryptors do not currently support GCM mode.

date

The **date** command is used to view and change the internal date and time of an encryptor. The command uses the international date format (ISO 8601), yyyy-mm-dd hh:mm:ss.

Format:

date<CR>	View date and time
<date>	Set the 'date' part as specified
<time>	Set the 'time' part as specified

Example 1: View current settings

```
CN6140_A>date
2004-11-01 16:27:41 up 3 days 00:05
```

Example 2: Set date:

```
CN6140_A>date 2004-10-28
Setting to Thu Oct 28 16:28:27 2004
```

Example 3: Set time:

```
CN6140_A>date 13:11:20
Setting to Thu Oct 28 13:11:20 2004
```

Without any flags, this command will display the unit's current date and time and also how long it has been since the unit was last restarted. The date and or time may be set using the format shown above. This command allows independent setting of the date and time or the coordinated setting of both the date and the time. As long as the format is correct, the command will accept the input and adjust the date/time accordingly.

Encryptors with firmware prior to v2.4 do not support the notion of time zones. All peer encryptors (with secure connections between them) must be set to a common reference time so that the secure session establishment process can successfully authenticate each others credentials (including certificate validity period).

NOTE: 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, which will result in all certificate, user and connection information being erased when the unit next reboots

entropy

The **entropy** command is used to 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 will use internal noise sources for entropy.



NOTE: Senetas encryptors support only USB drives that are configured with the FAT or FAT32 format.

Format:

entropy<CR>	View entropy pool status
-d	disable entropy pool loading
-e	enable entropy pool loading

Example:

```
CN6140_A>entropy -e
```

If the entropy pool is not enabled then attempting to view the entropy pool status generates an 'External entropy pool loading is disabled!' message.

eping

The **eping** command constructs a proprietary Senetas Ethernet frame and transmits it out of the network port. It is primarily provided for diagnostic purposes.

Format:

eping<CR>	This help message
-m <mac>	Ping the MAC address specified
-b	Broadcast destination
-l <size>	Send specified buffer size (64-1530)
-c <count>	Repeat specified times (1-10)
-v [<id>[<id>]]	Specify VLAN id(s) in decimal e.g. 110 <outer><inner>: 120 110
-v [<tag>[<tag>]]	Specify VLAN tag(s) in hex e.g. :81000003 <outer><inner>: 8100000a8100000b
-d <vlan>	VLAN Double Tagged Frame (e.g. 9100XXXX8100XXXX)

The **eping** command can be targeted at an individual encryptor using the -m command or all encryptors using the -b command.

A response verifies that there is a connection from the local encryptor to the remote encryptor(s) and that the responding unit(s) are operational and able to respond to management traffic.

The request frame includes:

- the network port MAC address of the local encryptor as the source address
- a specified network port MAC Unicast address or Broadcast address as the destination address
- 0xFC0F as the ethertype
- 'eping' as the subtype
- an empty payload whose length defaults to 64 bytes. (By using the -l command, length can be up to 1500 bytes.) The specified length does not include the FCS character of the frame.

NOTE: The -v (or -d) command is used to tag the sent frame with a tag (or tags) so that it can traverse a VLAN tagged network. The tagging can use a decimal or hex value. This is used to test for reachability in service provider networks.

The returned frame has the MAC of the responder as the source, a destination address of the local encryptor, the same ethertype and subtype, and the payload of the sender.



The `-c <count>` option allows the eping to be repeated up to 10 times. The sending encryptor introduces a nominal 5-second delay between requests.

eqkd

The **eqkd** command enables standards-based quantum key distribution (QKD) management.

NOTE: This command is only applicable to Layer 2 encryptors.

Host Format:

eqkd<CR>	View current QKD settings
-c	Edit QKD Local and Remote IP address QKD ID
-i	View/Edit CNET QKD ID

Slot Format:

eqkd<CR>	View ETSI QKD configuration settings/status
-e	Enable ETSI QKD mode
-d	Disable ETSI QKD mode
-f	Edit QKD failure action to CNET_KEYS or PREV_KEYS>
-k <IPv4 IPv6>	Set default Key Management Entity (KME) IPv4/IPv6 address
-r <IPv4 IPv6>	Set default remote Secure Application Entity (SAE) IPv4/IPv6 address
-c	Set https certificate (server or end user certificate)
-s	Get status from server
-S	Get status from server

Host example:

```
CN6140_A>eqkd -c
QKD Local IP Address: (10.100.100.2)
QKD Remote IP Address: (10.100.100.1)
QKD Local PPP IP Address: (10.10.100.2)
QKD Remote PPP IP Address: (10.10.100.2)
Confirm changes ? (y/n)
CN6140_A>eqkd -i
CNET's QKD ID: (1)
```

Slot examples:

```
CN6140 (slot 0)qkd -e
Enabling QKD requires a slot reboot.
Confirm changes ? (y/n)

CN6140 (slot 0)qkd -d
Disabling QKD requires a slot reboot.
Confirm changes ? (y/n)
```



```
CN6140 (slot 0)qkd -f
QKD Failure Action (CNET_KEYS or PREV_KEY): (CNET_KEYS)
```

```
CN6140 (slot 0)eqkd
QKD functionality is enabled
QKD local KME IPv4/IPv6 address: 0.0.0.0
QKD remote SAE IPv4/IPv6 address: 0.0.0.0
QKD Failure Action: CNET_KEYS
Statistics...
-----
Successful QKD requests 2592
Failed QKD requests 0
QKD failure mode conversions 4
QKD failure mode recoveries 4
QKD conversion failures 4
QKD recovery failures 4
QKD failed peer requests 10
QKD failed key updates 10
Egress key status QKDKEY
```

eQKD is only available in the following operational modes:

- VLAN
- Line
- TRANSEC

erase

The **erase** command erases the current configuration of the unit and reboots it into factory default state.

Format:

<code>erase<CR></code>	erases the encryptor configuration
<code>- f</code>	fully erase unit including the front panel IP addresses

Example:

```
CN6140_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 . . .
```

All user and connection entries will be deleted and the certificate of the unit destroyed. (The configured IP address and the connection mode and any virtual management configuration will be preserved unless the -f option is used).

WARNING: After an erase command has been issued, no traffic will flow through the encryptor and the unit will need to be reconfigured.



ethertypes

<< This CLI command can be used with Layer 2 encryption only. >>

The **ethertypes** command is used to set the policy for frame processing by ethertype.

Format:

ethertypes<CR>	List all ethertypes
-s	Show Ethernet Type statistics
-a	Add an ethertype
-d <ETHERTYPE>	Delete ethertype <et>
-d *	Delete all ethertypes
-e	Edit ethertype
-1 <ETHERTYPE>	Set control plane ethertype 1 to ETHERTYPE (hex)
-2 <ETHERTYPE>	Set control plane ethertype 2 to ETHERTYPE (hex)
-3 <ETHERTYPE>	Set control plane ethertype 3 to ETHERTYPE (hex)
-r	reset all diagnostic counts
-s	Show count of frames bypassed or dis- carded due to policy
-c	Toggle ethertype diagnostics on/off
-l	List ethertype diagnostic counts

The ethertypes help (-h) command displays a number of the common ethertypes:

ARP	0x0806
IPv4	0x0800
IPv6	0x86DD
Loopback	0x9000
MPLS (unicast)	0x8847
MAC Control Frame	0x8808
VLAN	0x8100

NOTE: The bypass/discard count displayed by the -s option is not available from CM7.

Example 1: View current settings

```
CN6140_A>ethertypes
Offset Encryption Mutate Mutated Injected
Ethertype (Name) Enable Offset Enable Ethertype 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 Ethertype table							
Diagnostic counts disabled.							
Control plane ethertype : fc0f							

Example 2: Edit ethertype for IP packets: (0800)

```

CN6140_A>ethertypes -e
Enter Ethertype [(O)ther, Value (Hex)]: 0800
Type exists
Offset Enable: <(Y)es | (N)o>: [No]
Mutation Enable: <(Y)es | (N)o>: [Yes]
Enter Mutated Ethertype (H0600->Hffff) [Hf800]:
Unicast Action: <(F)ollow CI | (D)iscard | (B)ypass>: [Follow CI]
Multicast Action: <(F)ollow CI | (D)iscard | (B)ypass>: [Follow CI] b
Broadcast Action: <(F)ollow CI | (D)iscard | (B)ypass>: [Follow CI] b
Injected NonMutated Action: <(D)iscard | (B)ypass>: [Bypass] d
Updated existing ethertype

```

Policy can be set for up to 15 different ethertype values and those which are not explicitly listed are handled under the 'Other' policy. Ethertype H05FF represents length-encoded frames.

The policy options for each ethertype are:

Encryption offset

- Optionally delays the encryption start point in the frame by the specified number of octets and allows a portion of the Ethernet payload to be passed in the clear.

Ethertype mutation

- Optionally changes the ethertype of the encrypted frame transmitted by the encryptor to a specified value (configured per ethertype).

For example:

This shows the behaviour of Ethernet frames carrying an IP payload when mutated from an ethertype of H0800 to HF800.

Mutation effectively hides the traffic type of the encrypted traffic which can prevent interoperability issues with certain types of network equipment that may have difficulty transmitting encrypted traffic.



This can happen when the core switches make assumptions about the contents of the Ethernet frames that are not valid for encrypted traffic. As an example, if the Ethernet frame is carrying an IP payload then the encryptor will (unless an offset is specified) encrypt the entire IP header as it is simply part of the Ethernet payload. Some layer 2 switches may, however, (upon seeing a 0800 ethertype) expect to see a valid IP header in the Ethernet payload and if not present may not pass the frame. In these circumstances mutation disguises the IP payload type and prevents the core switches from dropping the frame. The recommended action is to enable mutation to reduce the likelihood of interaction with equipment between the encryptors causing problems.

Injected non-mutant traffic



If mutation is enabled for a given ethertype then the injected non-mutant policy specifies how the encryptor should process frames it receives on its network port that are not mutated. For example, if the encryptor is configured to mutate IP frames (to HF800) then all encrypted IP traffic received from peer encryptors will have an ethertype of HF800. However, any IP traffic inserted by network equipment between the encryptors (for example, destined for routers behind the encryptors) will be received by the encryptors with an ethertype of H0800 as shown.

The injected non-mutant policy specifies whether these frames should be bypassed or discarded by the encryptor.

The recommended action is 'Discard' to prevent network traffic from interfering with the cryptostream.

Action per address class

Traffic on each ethertype can have different policies applied for each address class (unicast, multicast and broadcast).

The mode of operation (line or multipoint) will determine what options are available.

Ethertype diagnostics

The CN Series has a diagnostic capability which when enabled counts by ethertype the Ethernet frames that are received and passed through the encryptor on both the local and network ports. These are stored in a table for diagnostic purposes.

This feature is controlled using the `-c`, `-r` and `-l` flags with the `ethertypes` command or can be enabled via CM7.

NOTE: The inbuilt diagnostics incur a processing overhead and therefore they should be turned off during normal operation. Whenever the encryptor is rebooted the feature is turned off.

Control plane ethertype

By default, all encryptor management traffic (Line, Transec, MAC, VLAN with SenderID disabled) uses the reserved FC0F ethertype. However if encryptors are nested then this needs to be changed so that management traffic can be sent to the local port(s) of inner encryptors. The ethertype of each pair needs to be set to a unique value using the `-1 hhhh` command, where `hhhh` is a hex value.

When in TIM mode, the most significant byte of this field defines the most significant byte of the ethertype used when encrypting at layer 2.

The encryptors must be restarted before the new value will take effect.

Out-of-band ethertype

The `-3 hhhh` command is used to set the hex value (typically FC0D) that will be used to allow out-of-band control plane traffic to be bypassed through an encryptor when it is presented on the local interface of the encryptor. The ethertype must also be manually added to the ethertype table.

NOTE: When in TIM mode this field is ignored.

event

The **event** command displays the event log, allows the log to be cleared and controls the wrapping mode of the log.

Format:

event<CR>	List the events
<code>-l <n></code>	List the last n records in the log
<code>-s <n></code>	List records in the log starting from n
<code>-n</code>	Print the number of records in the log



event<CR>	List the events
-c	Clear the event log
-w <on off>	Turn wrapping on/off

Example: CN6140_A>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
(6): 24/11/2003 16:44:21 System started
(7): 24/11/2003 16:44:23 Alarm set: Network interface loss of signal
(8): 24/11/2003 16:44:23 Alarm set: Local interface loss of signal
(9): 02/12/2003 15:13:08 System started
(10): 02/12/2003 15:13:10 Alarm set: Network interface loss of signal
(11): 02/12/2003 15:13:10 Alarm set: Local interface loss of signal
(12): 02/12/2003 15:13:16 Alarm set: Network port link down indication
(13): 02/12/2003 15:13:16 Alarm set: Local port link down indication

```

The event log is a non-volatile record of significant events that have occurred. Each record is time-stamped and contains a detailed text description of the event details.

The event log (like the audit log) has a maximum record size of 4000. When the log fills up, new messages can either be discarded (wrapping mode disabled, the default) or added to the log, replacing the previous oldest message (wrapping mode enabled).

The event command allows Administrators to set the wrapping mode for the log as well as the ability to clear the log.

fips

The **fips** command sets and displays the operational mode of the unit (FIPS or NON_FIPS).

Format:

fips<CR>	Show current states
on	Enable FIPS mode (will erase/reboot)
off	Disable FIPS mode (will erase/reboot)

Example:

```

CN6140_A>fips
FIPS mode enabled

```

FIPS certification

FIPS 140 is a US government security standard that sets requirements for cryptographic devices. If the encryptor is operating with FIPS mode enabled (the default) it is in compliance with all the security requirements in the FIPS 140 standard.



WARNING: If FIPS mode is disabled then the encryptor operates in one or more ways that does not meet the FIPS 140 standard.

Changing FIPS mode reboots the encryptor and removes all certification and user credentials. This is required to ensure the security requirements are maintained.

Currently the only non-FIPS conforming feature is the ability to manage the encryptors with SNMP privacy options disabled.

In normal use FIPS mode should be enabled. Non-FIPS mode is provided primarily for compatibility with legacy products.

ftpcfg

The **ftpcfg** command is used to configure and manage the access to remote FTP servers.

Format:

ftpcfg<CR>	Show FTP remote server settings
-a	Add remote FTP server entry.
-d <idx>	Delete FTP remote server entry.
-e <idx>	Edit FTP remote server entry.
-c	Clear all remote FTP server settings.
-r <on off>	Restrict FTP access to listed servers only.
-s	Show public key for SFTP upgrades.

global

The **global** command sets the top level processing policy for received Ethernet frames in both Point-point (line) and multipoint modes.

Format:

global<CR>	Display current global mode status
-b	Set global mode to Bypass
-d	Set global mode to Discard
-e	Set global mode to Encrypt

Example 1: View current settings

```
CN6140_A>global
Global mode: bypass
```

Example 2: Set global mode to encrypt

```
CN6140_A>global -e
Global mode set to encrypt
```

WARNING: All operational modes, except TIM, must have valid certificates loaded onto the encryptor to enable changing the Global mode to 'encrypt'.

See "Multipoint VLAN Policy" on page 90 for an example of frame processing hierarchies.

The global policy can be set to one of the following three settings:



- **Bypass** - all Ethernet frames are passed through the encryptor regardless of any other policy settings
- **Discard** - all Ethernet frames are discarded by the encryptor regardless of any other policy settings
- **Encrypt** - all Ethernet frames have ethertype and if applicable Remote ID (MAC or VLAN) policies applied to determine the ultimate action that is applied to them

help

The **help** command displays information on the available console commands. Individual command may be run with the **-h** flag to get help on that commands.

Format:

<code>help<CR></code>	List all of the available commands

Example:

```
CN6140_A>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
passphrase - Set SafeNet sael compatible passphrase
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
```

The help command lists all the available console commands and a brief description of their function.

NOTE: Further information can be found on any individual command by typing the **command name**, followed by **-h**.

helpall

The **helpall** command displays help information about all the available console commands.

NOTE: Individual command may be run with the **-h** flag to get help information for a specific command.



Format:

<code>helpall<CR></code>	List help information for all possible commands
<code>-h</code>	This help message

The help command lists all the available console commands and a brief description of their function.

Further information can be found on any individual command by typing command `-h`.

history

The **history** command shows the command history for the current CLI session.

Format:

<code>history<CR></code>	List command history

Example:

```
CN6140_A>history
01: date
02: users
03: pvc
04: help
05: ip -s
06: pvc
07: sessions
08: fips
09: history
```

Previous commands are stored in a 25-deep command history buffer. The up arrow and down arrow keys cycle forwards and backwards through the buffer and allow any previous command (and all its parameters) to be executed by pressing ENTER.

NOTE: Every time a user logs in and out of the console the history buffer is cleared.

hostname

The **hostname** command is used to set the hostname of the encryptor.

Format:

<code>hostname<CR></code>	Display current hostname
<code>-s <hostname></code>	Set the hostname

inband_vlan

The **inband_vlan** command is used to specify the VLAN tag(s) that will be used for in-band management frames. When operating in networks that use VLAN tagging entries for each of the VLANs in use must be added to the `inband_vlan` table of the in-band management encryptor so that remote encryptors can be managed.



Format:

<code>inband_vlan<CR></code>	List all inband VLAN tags
<code>-a</code>	Add untagged tag
<code>-a [<id> [<id>]]</code>	Add VLAN id(s) in decimal
	e.g. 110
	<outer><inner> : 120 110
<code>-a [<tag> [<tag>]]</code>	Add a single or double VLAN tag in hex
	e.g.81000003
	<outer><inner> : 8100000A81000003
<code>-e <idx> [<id> [<id>]]</code>	Edit given record (see examples above)
<code>-e <idx> [<tag> [<tag>]]</code>	Edit given record (see examples above)
<code>-d <idx> [<idx>..]</code>	Delete given records
<code>-d *</code>	Delete all records

All the VLAN tags that are required to reach each of the remote peer units must be manually added to the in-band VLAN table.

During the first connection through the network each encryptor will learn which VLAN it should use to reach each peer unit and add its MAC address to the `inband_vlan` table. This is a once-off process. Should there be reachability issues then the entry can be deleted from the in-band table using the `-d <idx>` command, and the VLAN ID re-added so that it will be re-learnt.

The remote in-band VLAN MAC address does not persist across encryptor reboots. If a remote unit is replaced (and therefore the MAC address will change) the in-band management encryptor should that encryptors record deleted and re-added.

NOTE: The learnt MAC address is only visible from the CLI.

When managing the encryptors through the network, the encryptor will tag the management frames with the VLAN number used to reach the remote unit.

```

CN6140_A>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

```

There must be at least one entry in the `in-band_vlan` table and by default this is the untagged entry.

In the case of encryptors where the auxiliary (provider) front panel port is enabled, both the provider and customer will use the same VLANs to manage the remote encryptors but will keep using different subnet and gateway to do so.



initcfg

The initialise configuration (**initcfg**) command is used to re configure the encryptors security policy to known starting conditions.

Format:

initcfg<CR>	Displays this help
-a	Reset tunnel/CI, MAC and global config to defaults and reboot
-c	Reset tunnel/CI, 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)

Example: Reset global config

```
CN6140_A>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
```

This command affects the operating mode, ethertype policy, connection identifiers, MAC tables, ethertype diagnostics, state and global policy only; it will not change any other configuration settings or erase the X.509 certificate.

-a flag

Resets all security policies to factory default settings as follows:

```
Setting Value after command
Operating mode Meshed
Global policy Discard
Auto-Discovery policy Enabled
MAC address table cleared
All tunnel connections cleared
IPRules table cleared
Tunnels All existing entries deleted, tunnels set to:
CI Origin Action State Peer Name Remote Encryptor MAC MAC Header
-----
0001 PENDING Discard Up N/A
0002 System Discard Up N/A
0003 System Bypass Up N/A
Ethertype policy
Set to:
Offset Encryption Mutate Mutated Injected
Ethertype Enable Offset Enable Ethertype Unicast Multicast Broadcast NonMutant
-----
H05ff N H0 NA UseCI Bypass Bypass NA
H0800 N H14 Y Hf800 UseCI Discard Bypass Discard
H0806 N H0 N Hf806 Bypass Discard Bypass Bypass
H86dd N H28 Y Hf6dd UseCI Discard Bypass Discard
```



```
H8808 N H0 N Hf808 Bypass Bypass Bypass Bypass
H8809 N H0 N Hf809 Bypass Bypass Bypass Bypass
H88cc N H0 N Hf8cc Bypass Bypass Bypass Bypass
H9000 N H0 N Hf000 Bypass Bypass Bypass Bypass
Other N H0 NA UseCI Discard Discard NA
Local/Network MAC tables
All entries are deleted
Executing this command forces a reboot of the encryptor.
```

-c flag

Resets connection policies as follows:

```
Setting Value after command
Operating mode NO CHANGE
Global policy NO CHANGE
Auto-Discovery policy NO CHANGE
MAC address table cleared
All tunnel connections cleared
IPRules table cleared
Tunnels All existing entries deleted, tunnels set to:
CI Origin Action State Peer Name Remote Encryptor MAC MAC Header
----
0001 PENDING Discard Up N/A
0002 System Discard Up N/A
0003 System Bypass Up N/A
Ethertype policy NO CHANGE
Local/Network MAC tables Deleted
```

-g flag

Resets global policies as follows:

```
Setting Value after command
Operating mode Meshed
Global policy Discard
Auto-Discovery policy Enabled
Tunnels
NO CHANGE
Ethertype policy
Set to:
Offset Encryption Mutate Mutated Injected
Ethertype Enable Offset Enable Ethertype Unicast Multicast Broadcast NonMutant
-----
H05ff N H0 NA UseCI Bypass Bypass NA
H0800 N H14 Y Hf800 UseCI Discard Bypass Discard
H0806 N H0 N Hf806 Bypass Discard Bypass Bypass
H86dd N H28 Y Hf6dd UseCI Discard Bypass Discard
H8808 N H0 N Hf808 Bypass Bypass Bypass Bypass
H8809 N H0 N Hf809 Bypass Bypass Bypass Bypass
H88cc N H0 N Hf8cc Bypass Bypass Bypass Bypass
H9000 N H0 N Hf000 Bypass Bypass Bypass Bypass
Other N H0 NA UseCI Discard Discard NA
```



Local/Network MAC tables NO CHANGE

Test mode levels

-1|2|3|4 flag

The `initcfg` command also provides a number of configuration test levels. These are a sequence of pre-determined policy settings intended to assist in problem resolution during network installation or testing.

These test levels replace the normal defaults with pre-defined settings for the purposes of detecting non-compliant network behaviour.

The intent is for tests to be carried out sequentially from numerically low to high-level settings in order to assist in profiling the operational network.

The test levels may assist in resolving traffic flow problems of the following nature:

- Inability to pass encrypted traffic
- Intermittent connectivity when encrypting traffic
- Inability to pass traffic of a particular ethertype

These settings are intended for network testing only and should not be used for operational purposes.

Line Mode - Test Level 1

Level 1 tests for basic connectivity and encryption. At this level, the crypto-stream is stripped down to a single ethertype (IPv4), with mutation enabled and injected non-mutant handling set to discard.

```

CN6140_A>initcfg -1
Setting of Level 1 defaults is testing/commissioning purposes only.
do you wish to proceed ? (y/n) y
Are you sure ? (y/n) y
Resetting config. . .Done.
CN6140_A>policy
Policy parameter(s) Status
-----
Bypass Reserved Multicast enabled
CN6140_A>ethertypes
Offset Encryption Mutate Mutated Injected
Ethertype Enable Offset Enable Ethertype Unicast Multicast Broadcast NonMutant
-----
H05ff N H0 NA Bypass Bypass Bypass NA
H0800 N H14 Y Hf800 UseCI Bypass Bypass Discard
H0806 N H0 N Hf806 Bypass Bypass Bypass Bypass
H86dd N H28 N Hf6dd Bypass Bypass Bypass Bypass
H8808 N H0 N Hf808 Bypass Bypass Bypass Bypass
H8809 N H0 N Hf809 Bypass Bypass Bypass Bypass
H88cc N H0 N Hf8cc Bypass Bypass Bypass Bypass
H9000 N H0 N Hf000 Bypass Bypass Bypass Bypass
Other N H0 NA Bypass Bypass Bypass NA
9 Records in Ethertype table
Diagnostic counts disabled.
CN6140_A>global -e
Global mode set to encrypt

```



```
CN6140_A>
```

Successful testing at this level verifies:

1. Management ethertype (0xFC0F) traverses network.
2. Session establishment is working.
3. IPv4 Traffic traverses networks - that is, Mutated type traverses network.

Line Mode - Test Level 2

Level 2 testing expands on the crypto stream by the inclusion of ARP and IPv6 traffic.

This level has been added to increase the complexity of the crypto stream which will potentially increase the error rate. It may pick up issues such as packet re-ordering.

```
CN6140_A>initcfg -2
Setting of Level 1 defaults is testing/commissioning purposes only.
do you wish to proceed ? (y/n) y
Are you sure ? (y/n) y
Resetting config. . .Done.
CN6140_A>policy
Policy parameter(s) Status
-----
Bypass Reserved Multicast enabled
STP Monitoring disabled
CN6140_A>ethertypes
Offset Encryption Mutate Mutated Injected
Ethertype Enable Offset Enable Ethertype Unicast Multicast Broadcast NonMutant
-----
H05ff N H0 NA NA UseCI Bypass Bypass NA
H0800 N H14 Y Hf800 UseCI Bypass Bypass Discard
H0806 N H0 N Hf806 Bypass Bypass Bypass Bypass
H86dd N H28 Y Hf6dd UseCI Bypass Bypass Discard
H8808 N H0 N Hf808 Bypass Bypass Bypass Bypass
H8809 N H0 N Hf809 Bypass Bypass Bypass Bypass
H88cc N H0 N Hf8cc Bypass Bypass Bypass Bypass
H9000 N H0 N Hf000 Bypass Bypass Bypass Bypass
Other N H0 NA UseCI Bypass Bypass Bypass NA
9 Records in Ethertype table
Diagnostic counts disabled.
CN6140_A>
```

Line Mode - Test Level 3/4

Level 3 testing enables encryption of length-encoded packets to identify potential issues with control plane packet handling. It is recommended that you test at this level for at least 20 minutes to detect any protocol timeouts that might occur.

Level 4 is the same as level 3 except that Bypass Reserved Multicast is set to disabled. If corruption/packet loss occurs at level 4 and not level 3 then perhaps reserved multicast packets are being injected into the crypto stream by network equipment.

```
CN6140_A>initcfg -3
Setting of Level 1 defaults is testing/commissioning purposes only.
do you wish to proceed ? (y/n) y
Are you sure ? (y/n) y
Resetting config. . .Done.
```



```

CN6140_A>policy
Policy parameter(s) Status
-----
Bypass Reserved Multicast enabled
STP Monitoring disabled
CN6140_A>ethertypes
Offset Encryption Mutate Mutated Injected
Ethertype Enable Offset Enable Etherbyte Unicast Multicast Broadcast NonMutant
-----
H05ff N H0 NA UseCI UseCI UseCI NA
H0800 N H14 Y Hf800 UseCI UseCI UseCI Discard
H0806 N H0 Y Hf806 UseCI UseCI UseCI Discard
H86dd N H28 Y Hf6dd UseCI UseCI UseCI Discard
H8808 N H0 N Hf808 Bypass Bypass Bypass Bypass
H8809 N H0 N Hf809 Bypass Bypass Bypass Bypass
H88cc N H0 N Hf8cc Bypass Bypass Bypass Bypass
H9000 N H0 N Hf000 Bypass Bypass Bypass Bypass
Other N H0 NA Bypass Bypass Bypass NA
9 Records in Etherbyte table
Diagnostic counts disabled.
CN6140_A>

```

Multipoint Mode - Test Level 1

Level 1 tests for basic connectivity and encryption. At this level, the crypto-stream is stripped down to a single etherbyte (IPv4), with mutation enabled and injected non-mutant handling set to discard.

Successful testing at this level verifies:

1. Management etherbyte (0xFC0F) traverses network.
2. Session establishment is working.
3. The mutated IPv4 Traffic traverses the network.

```

CN6140_A>initcfg -1
Setting of Level 1 defaults is testing/commissioning purposes only.
do you wish to proceed ? (y/n) y
Are you sure ? (y/n) y
Resetting config. . .Done.
CN6140_A>tunnels
Interface (tunnel/CI) MAC address : 00:d0:1f:09:01:07
Front Panel Management MAC address : 00:d0:1f:09:01:12
CI Origin Action State Peer Name Remote Encryptor MAC MAC Header
-----
0001 PENDING Bypass Up N/A
0002 System Discard Up N/A
0003 System Bypass Up N/A
CN6140_A>ethertypes
Offset Encryption Mutate Mutated Injected
Etherbyte Enable Offset Enable Etherbyte Unicast Multicast Broadcast NonMutant
-----
H05ff N H0 NA Bypass Bypass Bypass NA
H0800 N H14 Y Hf800 UseCI Bypass Bypass Discard
H0806 N H0 N Hf806 Bypass Bypass Bypass Bypass

```



```

H86dd N H28 N Hf6dd Bypass Bypass Bypass Bypass
H8808 N H0 N Hf808 Bypass Bypass Bypass Bypass
H8809 N H0 N Hf809 Bypass Bypass Bypass Bypass
H88cc N H0 N Hf8cc Bypass Bypass Bypass Bypass
H9000 N H0 N Hf000 Bypass Bypass Bypass Bypass
Other N H0 NA Bypass Bypass Bypass NA
9 Records in Ethertype table
Diagnostic counts disabled.
CN6140_A>

```

Multipoint Mode - Test Level 2

Level 2 testing expands the basic functionality test by encrypting length-encoded and other unlisted ethertypes. Test failure at this point would indicate the possible use of ethertype logging (ethertypes -c|-r) to detect other ethertypes seen on the network. Once detected, specific ethertype entries can be added to the ethertype table for individual handling.

NOTE: There are only two test levels in multipoint / meshed mode.

```

CN6140_A>initcfg -2
Setting of Level 2 defaults is testing/commissioning purposes only.
do you wish to proceed ? (y/n) y
Are you sure ? (y/n) y
Resetting config. . .Done.
CN6140_A>tunnels
Interface (tunnel/CI) MAC address : 00:d0:1f:09:01:07
Front Panel Management MAC address : 00:d0:1f:09:01:12
CI Origin Action State Peer Name Remote Encryptor MAC MAC Header
-----
0001 PENDING Bypass Up N/A
0002 System Discard Up N/A
0003 System Bypass Up N/A
CN6140_A>ethertypes
Offset Encryption Mutate Mutated Injected
Ethertype Enable Offset Enable Ethertype Unicast Multicast Broadcast NonMutant
-----
H05ff N H0 NA UseCI Bypass Bypass NA
H0800 N H14 Y Hf800 UseCI Bypass Bypass Discard
H0806 N H0 N Hf806 Bypass Bypass Bypass Bypass
H86dd N H28 Y Hf6dd UseCI Bypass Bypass Discard
H8808 N H0 N Hf808 Bypass Bypass Bypass Bypass
H8809 N H0 N Hf809 Bypass Bypass Bypass Bypass
H88cc N H0 N Hf8cc Bypass Bypass Bypass Bypass
H9000 N H0 N Hf000 Bypass Bypass Bypass Bypass
Other N H0 NA UseCI Bypass Bypass NA
9 Records in Ethertype table
Diagnostic counts disabled.
CN6140_A>

```

inventory

The **inventory** command is used to list the details of the control and interface modules of the encryptor.



Format:

<code>inventory<CR></code>	Display inventory details

Example: View inventory

```

CN6140_A>
CN6140_A>inventory
=====
Management Module
-----
Board Number = B2010A005-51
Description = System Module
Serial Number = 00D01F030219
Software Version = 2.7.1
Software Description = System Management Software
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
Software Description = Interface Module Firmware
Build ID = N/A
Build Number = N/A
Build Date & Time = N/A
CN6140_A>

```

ip

The **ip** command is used to configure the IP addresses of the management port:

- IPv4 (idx=1)
- IPv6 (idx=2)

and the inband addresses:

- IPv4 (idx=3)
- and IPv6 (idx=4)

Format:

<code>ip<CR></code>	Show IP management settings
<code>-s <idx><addr>/<prefix><gw></code>	Edit IPv4/IPv6 management settings
<code>-e <idx></code>	Enable interface entry (idx = 1-4)
<code>-d <idx></code>	Disable interface entry (idx = 1-4)



<code>ip<CR></code>	Show IP management settings
<code>-i <-e -d></code>	Enable/disable this device as Inband gateway
<code>-c <value>/<></code>	Set/reset DSCP value
<code>-x <value>/<></code>	Set/reset DSCP value on auxiliary interface.
<code>-v <-e -d></code>	Enable/Disable Virtual Management interface. (TIM mode only) Enabling this will disable the physical Management interface.

Example 1: View current settings:

```

CN6140_A>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

Auxiliary Management Port: Disabled
Inband Management Gateway Enabled: N
Main Interface DSCP value: 0
Aux. Interface DSCP value: 0
Front Panel Ethernet Port:
Configured: Auto Negotiation: Enabled
Maximum Advertised Rate: 100 Mbit/s, Full Duplex.
Current Status: Link State: Up
Auto Negotiation Status: Complete
Actual Rate: 100 Mbit/s, Full Duplex.
Link Partner: Maximum Advertised Rate: 100 Mbit/s, Full Duplex.

```

Example 2: Set new IPv4 address:

```
CN6140_A>ip -s 1 10.0.33.80/16 10.0.1.254
```

Example 3: Set new IPv6 address:

```
CN6140_A>ip -s 2 2001:0db8:3c4d:0015:0:0:abcd:ef12/32 2001::abcd:1234
```

-s flag

The IP address table consists of four fixed entries:



1. Management port IPv4 address.
2. Management port IPv6 address.
3. Inband management IPv4 address.
4. Inband management IPv6 address.

Each entry can be configured using `ip -s <idx> addr/prefix gw`.

Where:

- <idx> is the table index (1,2,3 or 4)
- addr/prefix is the v4 or v6 address and prefix
- gw is the default gateway for this port

IPv6 addresses are entered using the standard address format and abbreviations.

-e flag -d flag

These flags are used to either disable or enable the related option.

-i flag

Enables or disables inband management gateway capability. When acting as an inband gateway the encryptor will bridge management traffic across the network from the management PC (running CM7) to the remote encryptor(s).

The inband gateway forwards IP packets received on its front panel Ethernet port to remote encryptors across the network on the inband subnet and forwards responses from the inband subnet back out of the front panel to the management PC.

-c flag

Sets (or resets) the main ports DSCP value. The DSCP (Differentiated Services Code Point) value may be required to meet the QoS policy requirements of the management network.

-x flag

Sets (or resets) the auxiliary ports DSCP value.

-a flag

Sets the state of the auxiliary management interface. The options are:

disabled (the default) which makes the interface unavailable

isolated, which enables a separate interface that allows an isolated network to manage the encryptor.

bridged, which allows the encryptor to pass through front panel management commands to additional encryptors that are linked via the auxiliary port to their front panel.

-g flag

Enables the auxiliary port (if in isolated mode) to be used as an gateway to inband gateway for the management of remote encryptors.

-v flag (TIM mode only)

Specifies whether Virtual management is enabled or disabled. If enabled then front panel management is disabled and vice versa.



iprules

The **iprules** command is used when an encryptor is operating in TIM mode to establish the IP policy rules for L3/L4 Ethernet traffic

The IP Rules table further defines IPv4/IPv6 policy lookups based on the destination and source IP addresses, IP next protocol fields and the destination and source TCP/UDP port numbers.

The IP address searches are based on a longest prefix match (LPM), and several subnetted entries may be required to fully prescribe policy.

The Ethertype policy (for IPv4 or IPv6 only) must be set to L3 or L4 for the IP Rules to take effect.

Iprules can be either added or deleted. Edit operations are not allowed on existing Iprules.

The IP Rules feature allows the user to specify a destination and source IP address and subnet mask, the IPv4/IPv6 protocol/next header, and the destination and source TCP/UDP port numbers (if applicable) to:

- Encrypt at layer 2
- Encrypt at layer 3
- Encrypt at layer 4
- Bypass
- Discard

Any combination of the above can simultaneously be active. For example, one subnet can be encrypted at L3, another at L2, and another is discarded, etc.

Format:

-a <dst_addr>/<prefix>	Add IP rule. Port numbers only valid for TCP/UDP
<src_addr>/<prefix>	Specify 0.0.0.0/0 for wildcarding Source IP.
<protocol_id>	Protocols and ports can be wildcarded using *
<dst_port><src_port>	or by not specifying them at all on the cmd line.
<d b c12 c13 c14 ltu>	Layer4 tunnelling (ltu) only valid for TCP/UDP
-d <idx>	Delete IP rule
-c	Clear all rules
-u <d b c12 c13 c14 ltu>	Action for unlisted IP addresses
-l <-e -d>	Enable/Disable the Layer4 (TCP/UDP) Checksum calculation

Iprules is used to set specific policies for each subnet of IP addresses that can be further fine grained for specific transport layer protocols. For TCP/UDP over IP, specific policies can be set for port numbers as well. In case of multiple rules with similar IP address and subnets, it is always the longest matching subnet prefix that will take precedence. The c12|c13|c14|ltu argument can be used to set the protocol layer at which encryption is needed. c14 implies encryption of layer 4 payload and is only supported for TCP/UDP.



Layer 4 checksum calculation should be enabled whenever L4 encryption is used. When enabled processing is changed from cut-through to store-and-forward. Enabling L4 calculation also allows L3 encryption to be used for NAT (not PAT) For DPDK based encryptors the feature is enabled by default, and for FPGA based (low latency) encryptors it is disabled by default. Refer to the note below and the CM7 section See "IP Rules" on page 205

Displaying the current IP rules (this is a v5.1.x example. An example for v5.2.x on would include both destination and source IP addresses and ports)

```
CN6140_A>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

Setting an IP rule

```
CN6140_A>iprules -a 200.0.0.10 * c13
Action set to CryptLayer3!
CN6140_A>iprules -u b
Unlisted IP address Default action set to bypass!
CN6140_A>iprules
```

Index	Address	Netmask	Protocol	Port	Action
1	200.0.0.10	32	*	*	Layer 3

```
Default action set to: Bypass
CN6140_A>
```

L4 checksums:

When encrypting at L4 UDP and the encryptor is in cut-through mode (i.e L4 Checksum Calculation disabled) the encryptor does not update the UDP length field with the excess bytes due to the L4 Senetas shim and trailer. Therefore it is recommended that users ensure that 'L4 Checksum Calculation' is enabled when L4 encryption is required (i.e. L4 action in a listed IP rule or Unlisted IP rule action set to L4). If the user attempts to add a L4 IP rule (whether listed or unlisted) and 'L4 Checksum Calculation' is disabled they are warned via CLI or CM7 that the rule can not be added until 'L4 Checksum Calculation' is enabled. However, once the L4 rule exists we do not prevent the user from disabling the 'L4 Checksum Calculation'.



kdf

The **kdf** command is used to generate and display a new Key derivation key. The key can be copied and distributed to peer encryptors to enable encryption.

WARNING: When a kdf is generated, any existing Key derivation key within the encryptor is automatically erased.

If a KDK key is to be activated at a given date and time and NTP causes the time to shift more than an hour, the KDK key will be removed and a new KDK key is required to be generated.

Format:

kdf<CR>	View
-g	Generate and display a new Key Derivation Key
-k <key>	Paste Key Derivation Key to encryptor

kdf and FIPS

When FIPS mode is enabled, you will not be able to use the **kdf -g** and **kdf -k** commands via the local CLI to generate a key. The KDF may still be entered using CM7, SNMPv3 or the remote CLI.

When FIPS mode is disabled, all four methods to enter the KDF - local CLI, CM7, SNMPv3 and remote CLI are available.

Examples:

Pressing <CR> displays the SHA-256 hash of the encryptors kdf key. This can be used to verify that the same key has been installed on all of the encryptors.

```
CN6140_A>
Installed key Derivation status ...
HASH: :
9a7c80afa55d9d8550a4498961cf3c9b172210bf63897b60e0560fc818acba294
```

The **-g** option is used to generate a new kdf key using the entropy source of the encryptor.

```
CN6140_A>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
CN6140_A
```

When a key is generated its value is displayed once (and once only). The kdf key value should then be installed on all encryptors within the same network using the -k option.

```
CN6140_A> kdf -k 8b0bf71ad7a70e434063dccc21c5fbf3fd9608eb324321ed56288bfabec5039e
Key derivation key successfully installed
```



```

HASH:

```

```

9b9a1cba7e56d9e5cf73e10998ea83e00a51c502fcb26d70b7ab41503c4f46c8

```

kem

The **kem** command is used to display the quantum resistant algorithms used to create key encapsulations.

A key encapsulation mechanism (KEM) is used to secure symmetric key material for transmission using asymmetric (public-key) algorithms. The symmetric key is then used to encrypt the longer message. First generate a random symmetric key and then encrypt it using the chosen public key algorithm. The recipient then decrypts the public key message to recover the symmetric key.

Format:

<code>kem <CR></code>	Print QRA Key Encapsulation algorithms
<code>-e</code>	Edit QRA Key Encapsulation selection
<code>-h</code>	This Help message

keypad

The **keypad** command is used to lock and unlock the front panel keypad.

Format:

<code>keypad<CR></code>	Display current front panel keypad status
<code>[lock unlock] <CR></code>	Lock or unlock the front panel keypad

Example:

```

CN6140_A>keypad

```

```

Front panel keypad is unlocked

```

The front panel keypad is used to examine and change a number of Encryptor settings. When locked, changes cannot be made.

keyprovider

The **keyprovider** command is used to specify the key provider that will be used within a network that is using encryptors that have been configured to run in Transport Independent Mode. The synchronization of keys can be based on time or a counter.

Format:

<code>keyprovider<CR></code>	View the currently selected key provider type
<code>-s</code>	Set the key provider
<code>-k <time/ctr></code>	Set the key sync mode to time / counter

The key provider cannot be set to KMIP on multi-slot encryptors.

Changing the key provider requires the user to restart the connections to enable immediate change over to the new provider.

With time based synchronization all key changes are synced with respect to time every 30 minutes and all encryptors need to share a common NTP source.

With counter based synchronization all key changes are synced with respect to the frame counter that is held in a shim, the time dependency is removed, and no NTP source is required. The shim size for L2, L3 and L4 UDP is 10 octets and for L4 TCP it is 12 octets.



Example 1: View current settings

```
CN6140_A>keyprovider<CR>
Key Provider mode is : Key Derivation Function
Key Sync mode is : TIME
CN6140_A>
```

Example 2: Select KMIP (and then KDF) as key provider

```
CN6140_A>keyprovider -s<CR>
-->[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]

CN6140_A>keyprovider -s
   [01] Key Derivation Function
-->[02] Key Server [KMIP]

Key Provider Mode set to: Key Derivation Function
CN6140_A>
```

CAUTION: 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.

Example 3: Select counter based synchronization

```
CN6140_A>keyprovider -k ctr

Warning this command will reset the tunnel/CI, MAC
data to their factory defaults and reboot the unit!
do you wish to proceed ? [y/n] n
CN6140_A>
```

kscfg

The **kscfg** CLI command allows the user to enable, disable, and configure KeySecure remote server configuration, including client authentication if global keys are not being used.

Format:

kscfg<CR>	Show KeySecure remote server settings
-a <IPv4 or IPv6 addr><tier>	Add KeySecure remote server entry e.g. 192.168.1.10 1



kscfg<CR>	Show KeySecure remote server settings
-e	Enable KeySecure
-d	Disable KeySecure
-r <idx>	Delete KeySecure remote server entry
-c	Clear all KeySecure remote server settings
-s <username <pwd>	Set KeySecure client authentication

Example:

To connect an encryptor to a single KeySecure server, you need to specify the IP Address of the server and a tier. An initial tier 1 will be provided with default values for a TCP connection. SafeNet recommends this as a first step to test connectivity, and then to progress to an SSL connection.

The following commands adds a remote server entry for tier 1, displays the KeySecure settings and then enables KeySecure on the unit.

```
CN6140_A kscfg -a 192.168.1.10 1 <CR>
CN6140_A kscfg <CR>
KeySecure remote server settings
Index   Address      Tier
-----  -
1       192.168.1.10 1
CN6140_A kscfg -e <CR>
KeySecure remote server enabled, config written
```

kstier

The **kstier** CLI command allows the user to add, delete and edit KeySecure tier configurations, supporting Load Balancing Groups and Multi-Tier Load Balancing.

Format:

kstier<CR>	Show KeySecure tier settings
-a <port> <proto> <conn pool size> <timeout> <read timeout> <idle timeout> <retry interval> [<certificate idx>]	Add KeySecure tier entry e.g.: 9000 ssl 300 30000 30000 600000 600000 6
-d <idx>	Delete a KeySecure tier entry
-e <idx> <port> <proto> <conn pool size> <timeout> <read timeout> <idle timeout> <retry interval> [<certificate idx>]	Edit KeySecure tier entry eg: 1 9040 ssl 200 20000 20000 500000 500000 6
-c	Clear all tier settings

Parameters:

- port: - the port of the remote KeySecure server. This port will be common to all servers in the tier.
- protocol: - the protocol of the connection to the remote KeySecure server, either TCP or SSL.
- connection pool size: - the maximum number of connections to KeySecure allowed.



- connection timeout: - specifies how long we will wait(in milliseconds) for the connection to KeySecure before timing out.
- connection read timeout: - specifies how long we will wait trying to read data from KeySecure before timing out.
- connection idle timeout: - specifies how long idle connections will remain open before being closed.
- connection retry interval: - specifies how long we will wait before trying to reconnect to an uncontactable KeySecure server.
- certificate index: - the certificate to use for the connection to KeySecure when the protocol is SSL

Example:

To add a tier configuration the -a command is used. If the protocol is SSL then a certificate index can be provided, or if this is left out, the available certificates will be listed so that you can enter the certificate index.

```

CN6140_A kstier -a 1234 ssl 300 30000 30000 600000 600000<CR>
N V1 or V2 certificates loaded.

X.509v3 Certificates:
  Id  Type   Identifier  Alg Size  Expiry  State  In Use  Signed by
3634 Valid   No    c059db9a  /C=AU/ST=Victoria/L=Melbourne/O=Org/OU=Security/CN=encryptor
  4   x509 En   c9e271a5  RSA 2048  7276  Valid  No    self    /C=AU/CN=keyID1
  5   x509 En   df34d955  RSA 2048  7278  Valid  No    self    /C=AU/CN=keyID2
  6   x509 En   98018d83  RSA 2048
3216 Valid   No    self      /CN=595930804784475049752986231035097958713543161738
  7   x509 En   c059db9a  RSA 2048
2609 Valid   No    self      /C=AU/ST=Victoria/L=Melbourne/O=Senetas/OU=S-
SecurityLic/CN=Licensing

Enter certificate index: 6
CN6140_A kstier<CR>
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

CN6140_A

```

line

The **line** command is used to enable or disable Point-to-Point (line) mode of operation.

Format:

line<CR>	Display current line mode status
-e	Enable Line mode
-d	Disable Line mode

Example 1: View current setting

```

CN6140_A>line
Line mode: disabled

```



Example 2: Enable line mode

```

CN6140_A>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 . . .
CN6140_A>

```

NOTE: Changing between Point-to-point and Multipoint modes will reboot the encryptor.

linkspeed

The **linkspeed** command is used to set the physical interface connection parameters for both Local and Network ports.

Format:

linkspeed<CR>	Display current link speed
-a <e d>	Enable/disable autonegotiation
-s	Set the link speed
-m <e d>	Enable/disable local link monitoring
-f	Set Link Loss Forwarding (LLF) action
-c <e d>	Enable/disable Tie LLF to connection status (line mode only)

Example: View current settings (1 Gbps encryptor)

```

CN6140_A>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
Current flow-control status (Network) passthru
Current flow-control status (Local) passthru

```

Example: View current settings (100 Gbps encryptor)

```

CN6140_A>linkspeed
Link parameter                Status
-----
Maximum rate limit 100G (100%)

```



```

Maximum link capability 100Gb/s Full Duplex
Configured link speed 100Gb/s Full Duplex
Current link status 100Gb/s Full Duplex
Current link status (Network) 100Gb/s Full Duplex
Current link status (Local) 100Gb/s Full Duplex
Local link monitoring disabled
Optical Link Loss Forwarding set to: disabled
Optical LLF tied to connection status (line mode) disabled
Current flow-control status (Network) passthru
Current flow-control status (Local) passthru
Current FEC control status (Network) off
Current FEC control status (Local) off
CN6140_A>

```

Example: Disable auto-negotiation (10Mbps, 100Mbps, 1Gbps only)

```

CN6140_A>linkspeed -a -d
Auto Negotiation disabled

```

Example: Set maximum link speed to 1Gb/s

```

CN6140_A>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

```

The local and network ports are usually configured identically since the encryptor is a “bump in the wire (fibre)” device.

-a flag

Allows auto-negotiation to be enabled or disabled. (The is not applicable to 100 Gbps units.)

Disabling this may be necessary when connecting to Ethernet devices that don’t correctly support auto-negotiation.

-s flag

Sets the physical connection speed to the specified value.

-m flag

Local link monitoring is a feature that is used to set the unit into global discard mode in the event of link loss being detected on the local port (for example, the local port cable is unplugged).

Once in global discard mode the encryptor will not pass traffic until an administrator or supervisor has logged in and changed the global mode back to secure.



-f flag

Link Loss Forwarding (LLF) is used on optical Ethernet links to propagate a loss in received signal on one port to the transmitter on the opposite port.

LLF is used to ensure that transmission loss can be propagated u and /downstream so that other network equipment can detect the failure and take appropriate action, for example, switching to alternative network paths.

For example, a loss of Rx signal on the Network port will be forwarded to the Local port by turning off the Tx laser on the local port.

Link loss can be propagated in either a single direction or in both directions.

```
CN6140_A>linkspeed -f
Optical Link loss forwarding options:
-> disabled (1)
propagate Net->Loc (2)
propagate Loc->Net (3)
propagate Loc<->Net (4)
```

-r flag

Configure forward error correction (FEC) on the local, network, or both of the optical interfaces.

-c flag

In line mode of operation, by tying LLF to connection status, it is also possible to disable the local port transmitter until the secure connection has been successfully established.

If enabled then the local port Tx laser will not be turned on (indicating link up) until the encryptor has successfully completed its key negotiation and is ready to securely pass traffic.

locmacs

The **locmacs** command, which is only applicable in Multipoint MAC mode, lists the MAC addresses that the encryptor has learnt from the protected network and loaded into the locmacs table (that is, on the local port).

Format:

locmacs<CR>	List all local MAC addresses
-a <mac>	Add a local MAC address
-d <mac>	Delete a specified local MAC address
-d *	Delete all local MAC addresses
-n	Display count of local MAC addresses

Each learnt MAC address is listed in this table but unlike the netmacs table, local MAC addresses are not tied to a connection identifier.

Example: View local MAC table

```
CN6140_A>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
00:e0:81:40:a9:8b
00:80:2d:6e:ee:81
00:13:72:09:1f:cd
00:15:60:fe:59:00
00:15:60:fe:59:2c
00:12:3f:75:25:ff
12 Valid records

```

NOTE: This command allows MAC values to be manually added or deleted from a MAC table but it is recommended to use auto-discovery mode to automatically populate this table to avoid misconfiguration.

logout

The **logout** command logs the current user out of the console and returns to the login prompt.

Format:

logout<CR>	Logout from the CLI

Example:

```

CN6140_A>logout
Welcome to CN6140_A Encryptor
Version: 4.0.0
Built: 14-Jul-2010 12:56:48
Build number: 1279076208 C198
LOGIN:

```

A login requires entry of the identifying credentials - ID and password - of the user. If a non-administrative user login fails due to lexical checks, as shown below, then they are locked out. Administrative users are able to change their password.

The examples that follow are for an administrative user, 'admin', and a non-administrative user 'operator'.

```

LOGIN:admin
PASSWORD:*****
Password no longer meets lexical check
Auth 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
Record updated
CN6140_A>

```

```

LOGIN:operator
PASSWORD:*****
Password no longer meets lexical check
LOGIN:

```



mode

The **mode** command switches between layer 2 and IPsec modes. The command only applies to CS10 and CS100 Series encryptors.

Format:

mode<CR>	Display current operating mode
-e	Set operating mode to Ethernet (layer 2)
-i	Set operating mode to IPsec (layer 3)

Example:

```
CN6140_A>mode -e
Warning changing operating mode to ethernet requires a reboot
do you wish to proceed ? (y/n) y
Are you sure ? (y/n) y
Changing to ethernet operating mode
Rebooting . . .ÿ
```

mpls

<< This CLI command can be used with Layer 2 encryption only. >>

The **mpls** command sets the policy for processing Ethernet frames that are tagged with labels on Multi-Protocol Label Switched networks.

Format:

mpls<CR>	Display MPLS shim bypass status
-p <e d>	Enable/disable shim header bypass
-a	Set alternate MPLS tag ethertype (H8847 is built in)

Example: View current settings

```
CN6140_A>mpls
MPLS parameter Status
-----
Protocol shim(s) bypass enabled
Alternate MPLS ethertype H8848
```

MPLS uses labels to forward packets across the network (conventional network layer forwarding uses network protocol layer headers, for example, IP addresses) and is usually used for 'class of service' or traffic engineering purposes.

Layer 2 Ethernet networks carry MPLS labels in shim headers. The shim header is inserted between the link layer and the network layer, Ethernet uses values 0x8847 and 0x8848 to indicate the presence of a shim header.

Ethertype value 0x8847 indicates that a frame is carrying an MPLS unicast packet and ethertype 0x8848 is used to indicate that a frame is carrying an MPLS multicast packet.

If the Protocol Shim Bypass feature is enabled the encryptor will detect and ignore the unicast (0x8847) MPLS shim and base its policy on the ultimate ethertype in the tagged frame. The multicast shim can also be detected in the Alternate MPLS ethertype field which is by default set to 0x8848.



If the Protocol Shim Bypass feature is disabled then the encryptor will not automatically detect the presence of MPLS shims. If a shim is present (unicast or multicast) then the encryptor will treat this as the ultimate ethertype and determine the policy from the ethertypes table (if no explicit policy is listed then it will be processed according to the 'other ethertypes' rule).

netmacs

The **netmacs** command, which is only applicable in Multipoint MAC mode, lists the MAC addresses that an encryptor configured with MAC based policy has learnt from the unprotected network and loaded into the netmacs table. (that is, on the network port).

Format:

<code>netmacs<CR></code>	List all network MAC addresses
<code>-a <mac></code>	Add a network MAC address to connection specified by CI
<code>-a <mac> -m</code>	Add a network MAC address to connection specified by rem MAC
<code>-e <mac></code>	Edit (move) a network MAC address
<code>-d <mac></code>	Delete a specified network MAC address
<code>-d *</code>	Delete all network MAC addresses
<code>-l <CI></code>	List network MAC addresses for connection specified by CI
<code>-l <mac> -m</code>	List network MAC addresses for connection specified by rem MAC
<code>-n</code>	Display count of network MAC addresses

Example 1: List network MAC table

```
CN6140_A>netmacs
Network Mac CI
-----
00:d0:1f:01:06:4c 0001
1 Valid record
```

Example 2: Move MAC address to a new connection identifier

```
CN6140_A>netmacs -e 00:d0:1f:01:06:4c
Enter CI to associate mac address with : 2
Moved mac address
```

Example: List all MAC addresses associated with connection id 1

```
CN6140_A>netmacs -l 1
Network Mac CI
-----
00:d0:1f:01:06:4c 0001
1 Valid record
```

Each learnt MAC address is tied to an encrypted tunnel whose connection identifier (CI) is listed in the table.

The netmacs command allows this table to be edited and entries can be manually added or deleted.



It is recommended that auto-discovery be used to populate this table since manual editing can be difficult and lead to errors.

Once MAC addresses have been learnt, auto-discovery can be disabled and any specific MAC addresses that should not be in the table can then be manually deleted if necessary.

ntpcfg

The **ntpcfg** command is used to configure the addresses of NTP servers that will be used by the encryptor to establish its date and time. The validity of the addresses is checked and the presence of at least one valid address enables the use of an NTP server for the maintenance of the encryptors time.

Format:

ntpcfg<CR>	Show NTP server connections
-a <IPv4 IPv6 addr>	Add NTP server entry.
-d <idx>	Delete NTP server entry.
-c	Clear all NTP server settings.
-p	Print current NTP status.

Example:

```
CN6140_A>ntpcfg
NTP server details
Index Address
-----
1 192.189.54.17
2 1.1.1.1
3 1.1.1.2
4 ::2
CN6140_A>
```

ocsp

<< This CLI command can be used with Layer 2 encryption only. >>

The **ocsp** command is used to view and update details of the Online Certificate Status Protocol (OCSP) servers configured within the encryptor.

Format:

ocsp<CR>	Print OCSP server entries
-a [ssl] <url>	Add OCSP server entries
-c	Set certificate to use for signing OCSP requests
-d <idx>	Delete OCSP server entry
-e <idx> [ssl] <url>	Edit OCSP server entry
-p <idx>	Print OCSP server entry details
-u [update interval]	Display or set OCSP update interval
-v <y n>	Treat certificates with an unknown OCSP status as valid

Example 1: Adding an OCSP server



```
CN6140_A>ocsp -a y http://10.0.33.100
OCSP entry added
CN6140_A>
```

Example 2: Print entry details

```
CN6140_A>ocsp -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
CN6140_A>
```

overview

The **overview** command is used to view and modify the encryptors contact details, location information, and comments field.

Format:

community<CR>	Show overview
-c <contact>	Set the contact details (quoted string)
-l <location>	Set the location information (quoted string)
-m <comment>	Set the comments (quoted string)

Example 1: Display current overview

```
CN6140_A>overview
Contact :
Location :
Comment :
CN6140_A>
```

Example 2: Setting contact details

```
CN6140_A>overview -c "for Support call +1 555 123456"
CN6140_A>
```

NOTE: To clear an entry specify the required option and an empty string ("").

password

The **password** command is used to view and modify the user password policy. Enhanced mode can be enabled to allow the enforcement of AR-25-2.

Format

password<CR>	Show current password policy
-r <0-255>	Password reuse history size



<code>password<CR></code>	Show current password policy
<code>-o <0 1-240></code>	Password change lockout period
<code>-e [on off]</code>	Enhanced password mode
<code>-m <8-29></code>	maximum length
<code>-u <1-2></code>	Minimum uppercase characters
<code>-l <1-2></code>	Minimum lowercase characters
<code>-n <1-2></code>	Minimum numerical characters
<code>-s <1-2></code>	Minimum special characters

Example 1: View password policy

```

CN6140_A>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

```

Example 2: Set password parameters

```

CN6140_A>
CN6140_A>password -u 2
Minimum uppercase characters: 2
CN6140_A>password -l 2
Minimum lowercase characters: 2
CN6140_A>password -n 2
Minimum numerical characters: 2
CN6140_A>password -s 2
Minimum special characters: 2
CN6140_A>password -m 15
Minimum password length: 15
CN6140_A>
CN6140_A>password
Password enhanced mode: Disabled
Password lexical check: Enabled
Password reuse history: 255
Password requirements:
1. Length of 15-29 characters
2. At least 2 uppercase alpha characters
3. At least 2 lowercase alpha characters
4. At least 2 numerical characters

```



```
5. At least 2 special characters
```

```
CN6140_A>
```

As a default, lexical checking requires that all user passwords have:

- A minimum of 8 and up to 29 characters
- At least one upper-case alphabetic character
- At least one lower-case alphabetic character
- At least one digit
- At least one special character

These defaults can be changed using the -m, -u, -l, -n, and -s commands.

Default Password Behaviour

When an encryptor is started for the first time or following erasure (planned or via tampering) there is a single user account on the machine. This account has administrator privileges and a default password.

In this unactivated state, this admin user is allowed to:

- activate the Encryptor - by setting a new password
- enable the Enhanced Password mode Features
- modify the Password Policy Parameters
- modify the User Inactivity Lockout Period

Users cannot be created until the Encryptor has been activated.

Password Policy Parameters

The default Password Policy Parameters are shown in the table below.

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

Enhanced Password Mode

Enhanced Password Mode is disabled by default. When enabled, the following functionality applies:

- User lockout if 2 unsuccessful attempts within an hour
- Password lexical checking at login
- Logging of failed login attempts



- Disallowing of matching password and UserID
- Password expiry for users on CLI and SNMP/RESTful

This setting can only be modified using an administrator account irrespective of the activated state of the encryptor.

Password Expiry

An administrator user account is able to set an expiry date for encryptor management access on user accounts individually.

The default setting for passwords is that they do not expire.

NOTE: There are no alarms or warnings that the password expiry date is about to be reached, and therefore the onus is upon the user to track these as necessary.

For Operator, Upgrader and Supervisor user's passwords to expire (for console, SNMP and RESTful access):

- The user's password expiry must be set to a non-zero value; and
- The encryptor's 'enhanced password mode' must be enabled

For Administrator user's passwords to expire for console access (only):

- The user's password expiry must be set to a non-zero value; and
- The encryptor's 'enhanced password mode' must be enabled; and
- 'Admin Lockout' must be disabled

For Administrator user's passwords to expire (for console, SNMP and RESTful access): The user's password expiry must be set to a non-zero value; and

- The encryptor's 'enhanced password mode' must be enabled; and
- 'Admin Lockout' must be enabled

After a password has expired the behavior at a new console session, is as follows:

- Operator, Upgrader and Supervisor accounts logging in to the CLI will be met with a message stating that the login was rejected due to an expired password and the login will be rejected. An active admin account must be used to change the password of these expired accounts

Admin accounts logging in to the CLI:

If 'Admin Lockout' disabled:

- user will be told that their password has expired and then will be prompted to change their password

If 'Admin Lockout' enabled:

- user will be denied access and NOT prompted to change their password. Another active admin account must be used to change the password of the expired admin account

Any existing actively open CLI sessions will continue to successfully operate if the password expires during the open CLI session and thus the above do not apply

- After an Operator, Upgrader and Supervisor password has expired, at the next SNMP request (read or write) or CM7 (refresh or apply) the request shall immediately fail. An active admin account must be used to change the password of these expired accounts
- After an Administrator password has expired and 'Admin Lockout' is enabled, at the next SNMP request (read or write) or CM7 (refresh or apply) the request shall immediately fail



- After an Administrator password has expired and 'Admin Lockout' is disabled, management of the device via SNMP or CM7 shall continue successfully (SNMP access is not blocked due to an expired admin password)
- After an Operator, Upgrader and Supervisor password has expired, at a new RESTful session, the request shall immediately fail. An active admin account must be used to change the password of these expired accounts.
- After an Administrator password has expired and 'Admin Lockout' is enabled, at a new RESTful session, the request shall immediately fail. Another active admin account must be used to change the password of this expired admin account.
- After an Administrator password has expired and 'Admin Lockout' is disabled, management of the device via RESTful shall continue successfully (RESTful access is not blocked due to an expired admin password)

For Operator, Upgrader and Supervisor user's passwords NOT to expire (for console, SNMP and RESTful access):

- The user's password expiry is set to zero; and/or
- The encryptor's 'enhanced password mode' is disabled

For Administrator user's passwords NOT to expire (for console, SNMP and RESTful access):

- The user's password expiry must be set to zero; and/or
- The encryptor's 'enhanced password mode' must be disabled; and/or
- 'Admin Lockout' must be disabled

policy

The **policy** command is used to configure a number of miscellaneous Ethernet policy settings. The operational mode of the encryptor determines which of the options are displayed and therefore the following table may be specific to this document.

Format:

<code>policy<CR></code>	Display current misc policy settings
<code>-s <-e -d></code>	Enable/Disable STP monitoring to delete local MAC addresses
<code>-k <-e -d></code>	Enable/Disable Tunnel keep alive monitoring
<code>-p -e <idx></code> <code>-p -d <idx></code>	Edit (by index) bypassing of a specified MAC Address when in VLAN connection mode Delete (by index) bypassing of a specified MAC Address when in VLAN connection mode
<code>-m <-d -b></code>	Enable/Disable Bypass/Discard of Default Multicast/VLAN action
<code>-p -a <mac></code>	Enable/Disable bypassing a specified MAC address when in VLAN connection mode
<code>-a <all l2></code> <code>-b <-e -d></code> <code>-l <-e -d></code> <code>-f <-e -d></code> <code>-e <id></code>	in GCM mode, authenticate entire packet or shim + payload Enable/Disable bypass of reserved multicast addresses Enable/Disable of Bypass IGMP or MLD packets Enable/Disable of Bypass IP multicast header Set the IP Protocol Encryption Identifier
<code>-i <-e -d></code>	Observe pending action for unknown (DA) on ingress
<code>-r <-e -d></code>	Enable/Disable Limited KID range for TIM mode



<code>policy<CR></code>	Display current misc policy settings
<code>-z <-e -d> tcp</code>	Enable/Disable bypass of zero payload tcp frames
<code>-z <-e -d> udp</code>	Enable/Disable bypass of zero payload udp frames
<code>-z <-e -d> icmp</code>	Enable/Disable bypass of zero payload icmp frames
<code>-z <-e -d> ip</code>	Enable/Disable bypass of zero payload ip frames
<code>-A <-e -d></code>	Enable/Disable Path MTU adjustment
<code>-M <mtu></code>	Path MTU Maximum (576...10000 bytes, 0 = disabled)
<code>-w strict window disabled</code>	
<code>-h</code>	This help message

Example 1: View current policies

```

CN6140_A>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

```

Example 2: Enable STP monitoring

```

CN6140_A>policy -s -e
STP monitoring enabled

```

- Bypass reserved multicast addresses
- Enable STP monitoring (Multipoint only)
- Enable tunnel keep alive monitoring (Multipoint only)
- Observe pending action for unknown DA on ingress (Multipoint only)

Bypass reserved multicast addresses

Some multicast addresses are reserved and may need to be bypassed by the encryptor to allow certain network protocols to function correctly.

NOTE: If bypass reserved multicast is enabled (policy -b) then IPv4 frames within the address range 01:00:5e:00:00:** are bypassed regardless of the **policy -f** setting.

Bypassing multiple VLANs

When FIPS mode is enabled, you are not able to bypass VLAN traffic by using the **-m -b** options as this is considered insecure. To do this you must either disable FIPS or manually add in all of the required VLANs.

Enable STP monitoring

STP monitoring allows operation on networks that use the Spanning Tree Protocol (STP) to provide failover to redundant links in the event of an active-link failure.



The Spanning Tree Protocol provides path redundancy whilst preventing undesirable loops in the network. STP defines a tree that spans all switches in a meshed network and forces certain redundant paths into a blocked state. If one network segment becomes unreachable, the algorithm reconfigures the topology and activates the standby path.

To maintain an STP topology, all switches advertise their knowledge via configuration messages. When a topology change occurs, a topology change message is sent on the affected links which informs the switches of the change and a new path is selected.

STP monitoring makes use of the above information to enable failover between encryptors. When STP monitoring is enabled, the encryptor will detect STP configuration and topology change messages and purge the local MAC address table.

As a result, when the Spanning Tree Topology reconverges and starts forwarding data, new MAC addresses will be identified on the local port of the encryptor and the auto-discovery feature causes the encryptor to notify all other encryptors that it is protecting these MAC addresses, completing the failover process.

The encryptor detects a topology change under the following conditions:

- BPDU Topology Change message
- BPDU Configuration message with Topology Change flag set
- BPDU Configuration message with Topology Change Acknowledge flag set
- BPDU Configuration message absence at least 3 Hello time periods followed by BPDU configuration message reception

NOTE: STP monitoring requires that auto-discovery is enabled in the configuration so that new MAC addresses can be learnt.

STP Monitoring does not have any adverse effects on the encryptor throughput or latency. STP monitoring only operates in multipoint mode as there is no dependency on MAC addresses in line mode.

Enable bypass of IGMP/MLD traffic

When this setting is disabled, IGMP/MLP data plane traffic will be treated in the same way as other traffic in the multicast DA group.

When enabled, the following frames are bypassed:

- Multicast IPv4 (0x0800) frames with IP protocol equal to IGMP (2)
- Multicast IPv6 (0x86DD) frames with IP protocol equal to ICMPv6 (58 decimal) and ICMPv6 type of 130, 131, 132, or 143

```
CN6140_A> policy -l
disabled : normal policy processing
enabled :
The follow packets are bypassed;
If the packet is an IGMP packet.
If the packet is an MLD packet with type code 130, Multicast Listener Query
If the packet is an MLD packet with type code 131, Multicast Listener Report
If the packet is an MLD packet with type code 132, Multicast Listener Done
If the packet is an MLD packet with type code 143, Multicast Listener Discovery (MLDv2) reports
```

NOTE: If global mode is set to discard or bypass then this feature is ignored and that in order to pass IGMP control plane frames, Bypass Reserved Multicast must also be enabled.

Enable bypass of Multicast IP header

```
CLI> policy -f
bypass IP Multicast Header:
disabled : normal frame encryption at Layer 2.
enabled :
```



Shim insertion and encryption occurs after the IPv4/IPv6 header if the IPv4 multicast address is within the range 01:00:5e:**:** or IPv6 address is within the range 33:33:**.

The IPv4/IPv6 protocol/next header field is replaced with the IP Protocol Encryption Identifier (default 99/0x63) that is set via the CLI policy `-e` command. The original protocol/next header field is transmitted in the shim (in the clear, this is encrypted in TIM operational mode).

NOTE: If global mode is set to Discard or Bypass then this feature is ignored.

Enable Tunnel Keep Alive Monitoring

Tunnel Keep Alive Monitoring (TKAM) is a protocol-independent mechanism for detecting network failover.

When TKAM is enabled, the 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 then the encryptor will automatically purge the network MAC addresses associated with that connection, thus allowing new MAC addresses to be learnt (requires auto-discovery to be enabled).

NOTE: Tunnel Keep Alive Monitoring only operates in multipoint mode and requires auto-discovery to be enabled.

Observe pending action for unknown DA on ingress

When a frame is received on the network port of the encryptor, the destination MAC address is compared with the known addresses in the discovered local MAC table.

If the destination address is not known then, by default, the frame is discarded. The Observe pending action for unknown DA on ingress option specifies that frames with unknown destination addresses should observe the pending action instead of being automatically discarded.

Key /Sender ID change

When in TIM mode, changes to the Key/SenderID will cause the encryptor to reboot clearing the connections and IP Rules table.

profile

The **profile** command allows the administrative mode of the user to be set to either the 'standard' or a 'simplified' mode.

The standard mode provides four roles; 'Administrator', 'Supervisor', 'Operator' and 'Upgrader', whereas the simplified mode has two roles; 'Administrator' and 'Operator'.

For multi-slot encryptors the command is valid when in either 'Host' or 'Slot' mode.

Format:

<code>profile <CR></code>	Display current Profile mode status
<code>-f</code>	Full/Standard administrative mode
<code>-s</code>	Simplified administrative mode

CAUTION: Changing this setting will require an erase and reboot.

Examples:

```
CN6140_A>profile
```



```

Profile: Full/Standard
CN6140_A>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

```

prompt

The **prompt** command allows the console prompt to be customized to a more meaningful name, such as encryptor location or asset number.

The same prompt is used for all users logged into the CLI. The customized value is stored in non-volatile memory and is therefore preserved across reboots.

Format:

prompt name<CR>	Set the CLI prompt to name (maximum of 30 characters)

Example:

```

CN6140_A>prompt Adelaide1
Adelaide1>

```

protocol

For the CN6140 encryptor the **protocol** command allows the selection of one of the licensed options. The available options, which are determined by the loaded license, include 1-4 1Gbps links OR 1-4 10Gbps links. Note that executing the protocol command will delete any s-Box definition files and force a reboot of the encryptor.

Format:

protocol<CR>	Display current protocol status
-s	Set the protocol status

Example: Selecting a CN6140 speed

```

CN6140_A>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)

```

psu

The **psu** command allows the source of power for the encryptor to be defined.



Format:

psu<CR>	Show Power Supply Unit (PSU) mode of operation
-s	Share (normal share mode, not necessarily 50/50 load share)
-a	Prefer A (PSU-A primarily used, PSU-B used only if PSU-A fails)
-b	Prefer B (PSU-B primarily used, PSU-A used only if PSU-B fails)

qkd

The **qkd** command allows CN8000 host and slot QKD parameters to be set and viewed.

Host Format:

qkd<CR>	View current QKD settings
-c	Edit QKD Local and Remote IP address QKD ID
-i	View/Edit CNET QKD ID

Slot Format:

qkd<CR>	View current QKD settings
-e	Enable QKD connectivity for this slot (requires host support)
-d	Disable QKD connectivity for this slot
-f	View/Edit QKD failure action to CNET_KEYS or PREV_KEYS

Host example:

```
CN6140_A>qkd -c
QKD Local IP Address: (10.100.100.2)
QKD Remote IP Address: (10.100.100.1)
QKD Local PPP IP Address: (10.10.100.2)
QKD Remote PPP IP Address: (10.10.100.2)
Confirm changes ? (y/n)
CN6140_A>qkd -i
CNET's QKD ID: (1)
```

Slot examples:

```
CN8000 (slot 1)>qkd -e
Enabling QKD requires a slot reboot.
Confirm changes ? (y/n)
CN8000 (slot 1)>qkd -d
Disabling QKD requires a slot reboot.
Confirm changes ? (y/n)
CN8000 (slot 1)>qkd -f
```



```

QKD Failure Action (CNET_KEYS or PREV_KEY): (CNET_KEYS)

CN8000 (slot 1)>qkd
QKD operation: enabled
QKD Failure Action: CNET_KEYS
Statistics...
-----
Successful QKD requests 2592
Failed QKD requests 0
QKD failure mode conversions 4
QKD failure mode recoveries 4
QKD conversion failures 4
QKD recovery failures 4
QKD failed peer requests 10
QKD failed key updates 10
Egress key status QKDKEY

```

qsfp

The **qsfp** command provides information that is reported by the QSFP28 transceivers plugged into the network and/or local ports of 100 Gbps encryptors.

Format:

qsfp<CR>	Display local and network port QSFP28 information
-l	Display local port QSFP28 information
-n	Display network port QSFP28 information
-d	Display QSFP28 diagnostics
-v	Display verbose QSFP28 information
-c [-e -d]	Enable/Disable or print current status of Ignore CDR alarm

Example: View QSFP28 local information and diagnostics

```

CN6140_A>qsfp -lvd
=====
QSFP LOCAL PORT SERIAL DIGITAL DIAGNOSTICS
=====
Vendor Name = FINISAR CORP.
Vendor Part Number = FTLC9551RENM
Vendor Serial Number = KBL01XS
Vendor Revision = 00
Date Code = 070519
Extended Identifier = Power Level 2 Module (2.5 W Maximum)
Extended Identifier = Module with CDR function
Extended Identifier = TX Ref Clock Input Not Required
100 GbE Compliance = 10GBASE-LR & 10GBASE-LW
100 Gb FC Compliance = 1200-SM-LL-L
Lower Speed Links = N/A

```



```

Encoding Support = 64B/66B & 8B10B & SONET Scrambled & NRZ
Bit Rate (min-max) = 9900 - 11100 Mbits/s
Length (SMF) = 10 km
Length (EBW 50/125 um) = 0 m
Length (50/125 um) = 0 m
Length (62.5/125 um) = 0 m
Length (Copper) = 0 m
Device Technology = No wavelength control
Device Technology = Uncooled transmitter device
Device Technology = PIN detector
Device Technology = Transmitter NOT Tunable
Transmitter Technology = 1310nm DFB
CDR Support = 9.95 & 10.3 & 10.5 & 10.7 & 11.1 & XFI L/B
Vendor OUI = 009065
Wavelength = 1310.00 nm
Wavelength Tolerance = +/- 20.000 nm
Max Case Temperature = 70 (C)
Max Power Dissipation = 2500 mW
Max Power Power Down = 1500 mW
Max current +5V = 350 mA
Max current +3V3 = 300 mA
Max current +1V8 = 0 mA
Max current -5V2 = 0 mA
Diagnostic Monitoring = No BER Support
Received Power = Average Power
Enhanced Options = Soft TX_DISABLE & Soft P_down
Auxiliary A/D Input 1 = +3V3 supply voltage
Auxiliary A/D Input 2 = +5V supply voltage

```

```

=====
| Warning Limits | Alarm Limits | Flags |
-----

```

Parameter	Measured	High	Low	High	Low	Warn	Alarm
-----	-----	-----	-----	-----	-----	-----	-----
-----	-	-	-	-	-	--	
Temperature (C)	+349.43	75	-10	+11078	-13	OK	OK
AUX1 +3V3 (V)	+3.31	+3.50	+3.10	+3.63	+3.00	OK	OK
AUX2 +5V (V)	+4.87	+5.30	+4.70	+5.50	+4.50	OK	OK
TX Bias (uA)	40720	65000	25000	70000	20000	OK	OK
TX Power (dBm)	-2.43	+1.00	-6.50	+1.50	-7.00	OK	OK
RX Power (dBm)	-35.23	+2.00	-18.02	++2.50	-20.00	LOW	LOW

```

=====

```

reboot

The **reboot** command performs a complete reboot of the unit. During the reboot process no traffic will pass through the encryptor.



Format:

<code>reboot<CR></code>	Reboot the encryptor

Example: Reboot unit

```
CN6140_A>reboot
Are you sure you want to reboot the unit ? (y/n)
```

rest

The **rest** command is used to enable or disable RESTful servers which can be used to provide remote monitoring of encryptors via a web browser.

The RESTful interface access is controlled via the user console access rights, that is, the user must be authorized.

Format:

<code>Rest<CR></code>	View RESTful server configuration settings
<code>-e</code>	Enable RESTful server
<code>-d</code>	Disable RESTful server
<code>-s</code>	Set https server certificate (end user certificate)

Example: configure the server

```
CN6140_A>rest -s
No V1 or V2 certificates loaded.

X.509v3 certificates:
  Id  Type      Identifier  Alg Size  Expiry  State  In Use  Signed by
  ---  ---      -
  3   x509 En   675af1b2   RSA
2048  362 Valid   No        944e5b3e /C=AU/ST=Victoria/L=Melbourne/O=Org/OU=Security/CN=
Encryptor
  4   x509 CA    944e5b3e   RSA
2048  1689 Valid  No        Self      /C=AU/O=Organisation/CN=CommonName/UID=1495261784

Enter certificate Index or CR for none: 3

CN6140_A>
```

Verify the selection and then enable the web server access.

```
CN6140_A>rest
REST server is disabled
REST https server certificate hash: 675af1b2
CN6140_A>rest -e
Enabled RESTful server.
CN6140_A>
```



The web server should now be operational and this can be verified through an initial HTTP(s) request.



```

https://10.65.65.81:7437//json/param/sysEquipCount
{
  "sysEquipCount.0": "3"
}

```

Standard encryption role based access control will require username and password to be provided for client authentication.

sfp

The **sfp** command displays information that is reported by the Small Form Pluggable transceivers plugged into the local and network ports.

Format:

sfp<CR>	Display local and network sfp information
-l	Display local sfp information
-n	Display network sfp information
-d	Display sfp diagnostics
-v	Display verbose sfp information

Example: View local SFP information and diagnostics

```

CN6140_A>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
SONET Compliance = OC-48 Intermediate Reach
Ethernet Compliance = 1000BASE-LX
FC Link Length = Long Distance (L)
FC Tx Technology = Longwave Laser (LC)
FC Tx Media = Single Mode (SM)
FC Speed = 200 MBytes/s & 100 MBytes/s
Encoding = SONET Scrambled
Nominal Bit Rate = 2500 Mbits/s
Link length (9/125) = 20000 m
Link length (50/125) = 0 m
Link length (62.5/125) = 0 m
Link Length (Copper) = 0 m
Vendor OUI = 009065
Laser Wavelength = 1310 nm
Bit Rate Max (%) = 0

```



```

Bit Rate Min (%) = 0
Diagnostic Monitoring = Implemented
SFF-8472 Compliance = Revision 9.3
=====
| 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

<< This CLI command can be used with Layer 2 encryption only. >>

The **shim** command is used to specify the shim insertion rate for CTR and GCM encryption modes. For example a value of 1 is used to shim every frame and a value of 32 shims every 32 frames.

The lower the shim rate, the higher the throughput at the cost of error extension if loss occurs. If a transmission error occurs then data loss will continue until the next synchronization shim. It is recommended that for high availability environments the shim rate is set to 1.

Ethernet encryptors operating at 10 Gbps or above require the use of counter (CTR) or Galois counter mode (GCM) and, therefore, frames containing user data need to have a Shim Header added to allow resynchronization should this be required.

NOTE: A shim rate of greater than 1 can only be used if the operational mode of the encryptor is Point-Point (line) mode or multipoint MAC mode (unicast tunnels), where the default rate is 32.

Format:

shim<CR>	Display current shim setting
-r <0-32767>	Set shim insertion rate (0 = disable)
-m <-e -d>	Enable/disable MTU overflow on shim insertion

WARNING: It is not recommended to use a shim rate setting of 0 because this completely disables shim insertion.

All LLC_SAP or LLC_SAP_SNAP frames are shimmed. This is to prevent network equipment misinterpreting encrypted length encapsulated frames.

The **-m** option can be used to prevent a shim being inserted where this would exceed the MTU of a network. The frame length is 256 at speeds up to 1Gbps, and 1518 at 10 Gbps and above.

Example: View shim settings

```

CN6140_A>shim
SHIM parameter Status
-----
SHIM rate 32

```



NOTE: For Australian instances, Type identifies the slot. 6151 refers to either a 10G or 1G Ethernet "slot" encryptor. In the above example no licenses have been applied to slots.

Example: Assign a 5 Gbps license to slot 0 and show assignment

```
CN6140_HOST>slot -l 5G 0
Updating slot 0 to license 5G
CN6140_HOST>slot
Slot Status   Type   Protocol   License  Description
-----
0   Stopped 6151 Ethernet 10G      5G
1   Stopped 6151 Ethernet 10G      [NONE]
2   Stopped 6151 Ethernet 10G      [NONE]
3   Stopped 6151 Ethernet 10G      [NONE]
CN6140_A>
```

snap

<< This CLI command can be used with Layer 2 encryption only. >>

The **snap** command sets the policy for processing Ethernet frames that are in the IEEE 802.3 LLC SNAP format.

Format:

snap<CR>	Display current SNAP PID ethertype status
-p <-e -d>	Enable/disable Observe SNAP PID for ethertype

Example 1: View snap header settings

```
CN6140_A>snap
SNAP parameter Status
-----
Observe SNAP PID for ethertype processing enabled
```

Example 2: Disable SNAP processing

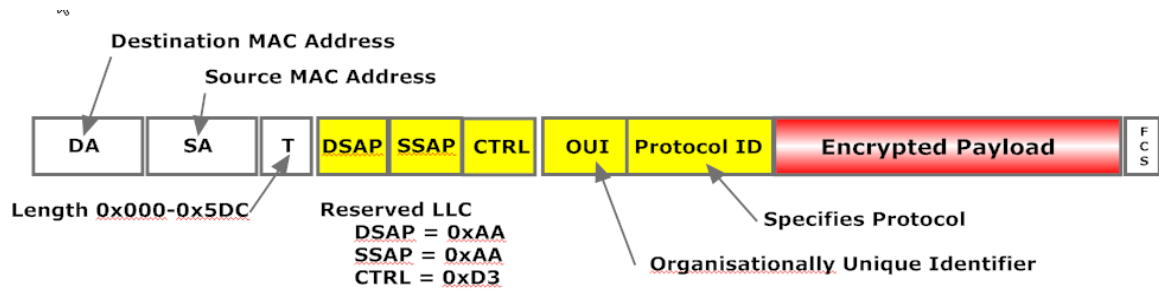
```
CN6140_A>snap -p -d
SNAP PID for ethertype processing disabled
```

Frames with the IEEE 802.3 LLC SNAP format (see IEEE 802.3 SAP SNAP (with 802.2 LLC header and SNAP Header) are length-encoded and contain an additional SNAP header Protocol ID field as follows:

If the SNAP PID for ethertype processing is enabled then the frame will be encrypted as indicated.

If the SNAP PID for ethertype processing is disabled then the frame will be processed as per the action specified for length-encoded frame in the Ethertype table under value H05FF.





snmpcfg

The **snmpcfg** command is used to configure the SNMPv3 privacy settings.

Format:

snmpcfg<CR>	Show/Modify current state
-p [on off]	Enable/Disable SNMP privacy
-v [on off]	Enable/Disable SNMPv1
-w x	Time window (mins) for USM auth errors (0 = disabled)
-f x	Number of USM auth errors before lockout (if time window enabled)

Example 1: View current SNMP privacy settings

```
CN6140_A>snmpcfg
SNMP Privacy mode enabled
```

Example 2: Disable SNMP privacy settings

```
CN6140_A>snmpcfg -p off
Disable SNMP Privacy selected. Validation...succeeded.
SNMP Privacy Disabled
```

- If SNMP privacy is enabled then all SNMP commands and responses will be encrypted as well as authenticated.
- If SNMP privacy is disabled then SNMP commands and responses will be authenticated only.

Privacy can only be disabled if the unit is configured with FIPS mode disabled (because SNMP privacy is mandatory for FIPS compliance). See "Encryptor management" on page 115

snmptraps

The **snmptraps** command is used to add or delete entries in the SNMPv3 trap list.

Format:

snmptraps<CR>	Show SNMPv3 trap server list
-a <IPv4 IPv6addr>	Add SNMPv3 trap server entry
-v <2 3>	SNMP trap type (Default is v2)
-s <	SNMPv3 trap type server security model:
AuthPriv	- authentication and privacy



snmptraps<CR>	Show SNMPv3 trap server list
AuthNoPriv	- authentication only
NoAuthNoPriv>	- no authentication and no privacy
-e <idx>	Enable SNMPv3 trap server entry
-d <idx>	Disable SNMPv3 trap server entry
-r <idx>	Remove SNMPv3 trap server entry
-p	Purge all SNMPv3 trap server entries

sshaux

The **sshaux** command is used to provide tertiary SSH access of remote devices.

NOTE: Only EC key exchange algorithms are supported when using auxillary port.

Format:

sshaux <CR>	Show current configuration
-a	Enable remote auxillary management port
-e	Access AUX port via CLI
-c	Connect using public key authentication
-p	Enforce PAM (username/password) for login
-s	Set the default SSH destination

Example:

```
CN6140_A>sshaux -a
SSHAUX enabled
```

sshcli

The **sshcli** command is used to enable or disable SSH CLI access.

SSH public keys can be added to a table and the SSH server port can be specified.

NOTE: Only ECDSA keypairs are valid for SSH use.

Format:

sshcli <CR>	Show SSH public keys
-a <"key string">	Add SSH public key entry (double quote key)
-e	Enable remote SSH CLI access
-d	Disable remote SSH CLI access
-p	Set SSH server port number
-r <idx>	Remove SSH public key entry
-c	Clear all SSH public key entries
-l <e d>	Enable/Disable SSH verbose logging to be sent to the event log

Example:

```
CN6140_A>sshcli -e
SSH enabled
```



CLI Logging

NOTE: Verbose logging can only be modified by a user with *administrator* privileges.

When accessing the CLI of a device via SSH, using either the Remote CLI of CM7, or a 3rd party tool, extra messages can be seen in the event log relating to SSH.

When verbose logging is enabled, both successful and unsuccessful authentication attempts are logged to the Event Log.

NOTE: It is recommended that this feature is left in the disabled state, unless diagnosing connectivity issues.

stats

The **stats** command lists the statistics for the local and network ports.

Format:

stats<CR>	Show Local/Network port statistics
-l	Show Local port statistics
-n	Show Network port statistics
-r	Reset statistics
-u	Instantaneous Utilisation Bandwidth
-p	Policy Stats

The Reset command, -r, resets the following statistics:

- local port statistics
- network port statistics
- protocol statistics (TIM operational mode)
- ethertype statistics (TIM operational mode)
- Tx and Rx tunnel/connection statistics

Example: Show all port statistics

```
CN6140_A>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 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 = 0
Rx PCS Sync Status = In Sync
Rx Manage Octet Count = 0
Rx Manage Frame Count = 0
Rx Manage Drop Frames = 0
Rx KID Discovery Dropped frames
Tx Octet Count = 71202
Tx Manage Octet Count = 71358
Tx Frame Count = 343
Tx Manage Frame Count = 343
Tx FCS Errored Frames = 0
Rx Shim Octets = 0
Tx Shim Octets = 0
Tx Encrypted Octets = 0
Tx Encrypted Frames = 0
Rx Encrypted Octets = 0
Rx Encrypted Frames = 0
Failed Auth Frames = 0
Replay Error Frames = 0
Skipped Counter Frames = 0

```

```
FPGA Resets = 0
```

```
CN6140_A>
```

NOTE: The skipped count is only valid in point-to-point (line) mode.

Example: Show utilization

```

CN6140_A> stats -u
Encrypt Utilisation:
Rx Total          100.000%
Rx FCS Errors     1.000%
Rx Discard Policy  9.000%
Rx Dropped Rate Limit 0.000%
Rx Dropped Overflow 0.000%
-
Tx Total 94.000%
Tx Bypass Policy  41.000%
Tx Secure Policy  50.000%

```



Tx FCS Errors	1.000%
Tx Management	1.000%
Tx Crypto Excess	1.000%
Decrypt Utilisation:	
Rx Total	94.000%
Rx FCS Errors	1.000%
Rx Discard Policy	0.000%
Rx Dropped Rate Limit	0.000%
Rx Dropped Overflow	0.000%
Rx Bad Authentication	0.000%
Rx Management	1.000%
Rx Crypto Excess	1.000%
-	
Tx Total	91.000%
Rx Bypass Policy	41.000%
Rx Secure Policy	50.000%
Tx FCS Errors	1.000%
CN6140_A>	

Example: Show policy statistics

```
CN6140_A>stats -p
```

Local Policy Statistics	
L2 Encrypted	= 0
L3 Encrypted	= 0
L4 TCP Encrypted	= 0
L4 UDP Encrypted	= 0
Malformed Frames	= 0
Not matching iprule	= 0
Res. Multicast bypass	= 0
Network Policy Statistics	
L2 Encrypted	= 0
L3 Encrypted	= 0
L4 TCP Encrypted	= 0
L4 UDP Encrypted	= 0
Malformed Frames	= 0
KID out of range	= 0
Unknown KID	= 0
Not matching iprule	= 0
Res. Multicast bypass	= 0
CN6140_A>	

syslog

The **syslog** command is used to configure syslog server entries for an encryptor.

Up to 10 distinct servers can be configured using the IPv4 or IPv6 address notation. DNS lookup is not supported.



NOTE: The auxiliary port can be specified if the servers are located on that network.

Format:

syslog<CR>	Show syslog server connections
-a <IPv4 Ipv6addr>	Add syslog server entry
-d <idx>	Delete syslog server entry
-p	Purge all syslog server entries
-f <on off>	Enable RFC3164 extended time stamps
-s <on off>	Control tunnelling of syslog messages via SSH

Examples:

```
CN6140_A> syslog -a fc0f:1234::1
Restarting system log daemon: syslogd.

CN6140_A>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
CN6140_A>
```

IPv4 or IPv6 are automatically checked. Invalid address entries are rejected.

```
CN6140_A>syslog -a 0.0.0.0
Invalid IP Address - 0.0.0.0
CN6140_A>syslog -a ::
Invalid IP Address - ::
CN6140_A>syslog -a notanaddress
Invalid IP address. Require standard dot notation IPv4 or IPv6 address.
CN6140_A>
```

Message timestamping

NOTE: The timestamp may only be changed by a user with administrator privileges.

This setting is enabled by default, but is configurable via the CLI command.

When disabled, the log message will not be time stamped on the wire but each receiving server will continue to time stamp the messages on receipt.

SSH tunnelling of syslog messages

NOTE: SSH tunnelling may only be changed by a user with administrator privileges.

The following steps will enable SSH tunnelling of syslog messages:



1. Configure an SSH CLI port on the encryptor; for example, port 2222
2. Enable SSH CLI
3. Install the syslog ECDSA server public key into the SSH CLI table
4. Ensure the syslog server is configured to listen for TCP on a specified port; for example, port 9123
5. Ensure the syslog server:
 - a. has a reverse SSH tunnel listening on encryptor port 9100 at 127.0.0.1
 - b. transmits the IP address to the syslog server on port 9123
 - c. has the port number 2222 configured for SSH CLI at the encryptor
6. Add 127.0.0.1 port 9100 to the syslog table of the encryptor
7. Enable syslog over SSH on encryptor

WARNING: SSH CLI must be enabled on the encryptor and the public key of the syslog server must be added to the SSH CLI table.

In this example, enabling this feature with a 127.0.0.1 entry in the syslog table provides for remote port forwarding of all syslog messages over SSH.

tacacs

The **tacacs** command allows TACACS+ server connections to be defined and managed.

NOTE: Entries can be added for IPv4 and/or IPv6 servers.

Format:

<code>tacacs<CR></code>	Show TACACS+ server connections.
<code>-a <IPv4 or IPv6 addr[:port]></code>	Add TACACS+ server entry.
<code><timeout> <key></code>	e.g. IPv4 a.b.c.d:port / IPv6 [::]:port
<code>-e</code>	Enable TACACS+
<code>-d</code>	Disable TACACS+
<code>-p</code>	Change password for TACACS+ account
<code>-r <idx></code>	Remove TACACS+ server entry.
<code>-c</code>	Clear all TACACS+ server settings.
<code>-b <on off></code>	Broadcast audit notifications to all servers.
<code>-s <password></code>	Set SNMPv3 USM TACACS+ user password
	NB: This is not your user password (use -p)

Example:

```
CN6140_A>tacacs
```

timezone

The **timezone** command is used to set the timezone of the encryptor to that of its physical location. The command was introduced in version 2.4.0.



Format:

<code>timezone<CR></code>	List all timezones
<code>-s</code>	Set the time zone

Example:

```

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
(6) New South Wales - Yancowinna
(7) Queensland - most locations
(8) Queensland - Holiday Islands
(9) South Australia
(10) Northern Territory
(11) Western Australia - most locations
(12) Western Australia - Eucla area
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)

```

In some cases a region only has a single country (e.g. Australia, Antarctica, etc.) and step 2 is skipped. In many cases a country only has a single timezone and step 3 is skipped. When a timezone is accepted the system timezone files (timezone and localtime) are set and the time-dependant services are restarted (syslog and ntp). The user can exit the command by pressing **Enter** at any time.

The special region **Etc** allows the user to set an offset from UTC or to set the timezone back to UTC or GMT. All of the timezones in this region are derived from the encryptor. The offsets in the timezone names in the **Etc** region are the opposite of the offset that will be set. for example, GMT+10 will actually set an offset to GMT of -10 hours.

Timezone options for Etc:

1. GMT (19) GMT-12
2. GMT+0 (20) GMT-13
3. GMT+1 (21) GMT-14
4. GMT+10 (22) GMT-2
5. GMT+11 (23) GMT-3



6. GMT+12 (24) GMT-4
7. GMT+2 (25) GMT-5
8. GMT+3 (26) GMT-6
9. GMT+4 (27) GMT-7
10. GMT+5 (28) GMT-8
11. GMT+6 (29) GMT-9
12. GMT+7 (30) GMT0
13. GMT+8 (31) Greenwich
14. GMT+9 (32) UCT
15. GMT-0 (33) UTC
16. GMT-1 (34) Universal
17. GMT-10 (35) Zulu
18. GMT-11

When you select a timezone, information for that timezone is displayed including the general offset to UTC (which does not factor in daylight saving). If this timezone is accepted then the real offset from UTC (including daylight saving adjustment) is displayed along with UTC and local times and timezone name.

transec

The **transec** command is used to set enable or disable TRANSEC framing and set the parameters required to generate transport frames.

Format:

<code>transec<CR></code>	Display TRANSEC mode status
<code>-a <dst> <src> [header]</code>	Set header information (hex)
<code>-r <rate></code>	Set rate (frames/sec)
<code>-b <rate></code>	Set rate (bits/sec)
<code>-c <rate></code>	Set rate (percentage)
<code>-e</code>	enable TRANSEC mode
<code>-d</code>	Disable TRANSEC mode
<code>-p</code>	Display TRANSEC configuration information
<code>-l <length></code>	Set frame length (bytes)
<code>-t <ETHERTYPE></code>	Set frame ethertype (hex)

Example: View TRANSEC status

```
CN6140_A>transec
Transec mode is disabled
```

Example: Enable TRANSEC mode

```
CN6140_A>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 . . .

```

When configuring the maximum throughput of the link an allowance should be made for the client traffic and the encryptor management traffic.

On 10Gbps models the transport frame length must be a multiple of 8 octets and if the set length is not a multiple of 8 it will be rounded down, for example, 159 would become 152.

tunnels

<< This CLI command can be used with Layer 2 encryption only. >>

The **tunnels** command is used to view and control connections. Available commands may vary depending on current policy.

Format:

tunnels<CR>	List all tunnels (connections)
-a	Add a tunnel
	<sec dis byp> [<id> [[<id>]] add VLAN id (s) in decimal
	-a sec add <cr> null tag session
	-a sec 110 <cr> add 1 tag session
	-a sec 120 110 <cr> add 2 tag session
	<sec dis byp> [<tag> [[<tag>]] add single or double VLAN tag in hex
	-a sec 81000FFF <cr> add 1 tag session
	-a sec 91000FFF81000123 <cr> add 2 tag session
-d <CI>	Delete tunnel specified by CI
-d *	Delete All tunnels
-e <CI>	Edit a tunnel specified by CI
-l <CI>	List tunnel specified by CI
-l *	List all tunnels
-s <CI>	Stop tunnel specified by CI
-s *	Stop all tunnels
-r <CI>	Restart tunnel specified by CI
-r *	Restart all tunnels
-k <n>	CI Key update interval (1-60 minutes)



tunnels<CR>	List all tunnels (connections)
-i <n>	Re-Authentication update interval (hours, 0 = disabled)
-c <CI>	Set certificate to use for specified CI
-f <CI>	Clear CI counts
-x [on off]	Enable or disable X.509v3 certificate expiry checks for established tunnels
-p <n>	Peer Detection interval (0-10 seconds) 0=disabled
-P [on off]	Prohibit acting as a group key master

The identifier 'CI' is used to refer to the 'connection index' associated with the path through an encryptor. In line mode an encryptor only has one (connection/tunnel/pt-pt) CI, in multipoint MAC mode it may have up to 511 connections (three of which are reserved by the system). In multipoint VLAN mode there can be a number of unique connections for single or double tagged frames.

If auto-discovery is enabled and the encryptor connection policy is MAC based then the encryptors will automatically learn the MAC addresses of remote encryptors from network traffic, dynamically establish secure connections and add them to the table. If auto-discovery is disabled the user is required to manually enter the tunnel/connection details.

If auto-discovery is enabled and the encryptor connection policy is VLAN ID based then the encryptors will automatically learn the VLAN IDs.

Example: View tunnel status (when in MAC mode)

```
CN6140_A>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
```

The purpose and operation of each of the available commands is as follows:

-k

Used to set the key update period between 1 and 60 minutes.

-a

Used to manually add a connection to the encryptor.

Example: Manually add a new secured connection using the `-a` command:

```
CN6140_A>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
```

If the 'Extra header length' is greater than zero then the VLAN tag is requested as a hexadecimal number. In the following example the entry is made up of the VLAN ethertype (0x8100) and a VLAN number of 16 (hex 0010).

Header content in HEX (0xn...): 0x81000010

Example: Manually add a new secured single tagged VLAN connection using the `-a` command:

```
CN6140_A>tunnels -a sec 110
```



The following commands have a connection index <CI> appended to operate on a single connection, or an * appended to operate on all connections

-l

Lists the current connection(s).

-s

Stops network traffic flowing on the connection(s).

-r

Forces the connection(s) to be renegotiated (with new session keys).

-d

Removes connection(s) (multipoint modes only).

-e

Change the following fields:

- Remote Encryptor MAC
- Address of the peer encryptor bound to this connection. (This field should never require editing as it is automatically learnt.)
- Remote Encryptor Name
- The peer encryptor's name. This is automatically learnt during session establishment. It is informational only; changes will not affect the operation of the connection but may lead to confusion if it does not match the name of the peer device.
- Tunnel Action: (D)iscard, (B)ypass or (S)ecure - the action to be applied to Ethernet frames on this connection.
- Extra header length (0,4,8) - specifies whether additional headers should be added to the encrypted frames. This is typically used to add one or more VLAN tags to the encrypted traffic, in which case the 'header content' can be changed.
- Header content in HEX (Hnnnn...)
- The VLAN tag; refer to the `-a` command above for format details.
- In multipoint VLAN mode the encryptor will detect the presence of VLAN tags from the first frame received on the local port on a given tunnel. The value can be manually changed using this command.
- In Point-to-point (line) mode VLAN tags are not learnt and must be manually entered if required.

-i

When the connections are based on an RSA certificate, specifies the certificate re-authentication period in hours. (0 = disabled).

-c

Allows a specific certificate to be associated with the connection.

-f

Clear the RX/TX counters for the specified connection

-p

Used to enable or disable dead peer detection.

-x

Used to enable or disable X509v3 certificate expiry checks for established connections. This is equivalent to the CM7 "Close Connection on expiry" setting.

-P

Used to enable or disable the ability of the unit to become the group key master when in VLAN or multicast MAC mode.

upgrade

The **upgrade** command is used to initiate a firmware upgrade using an image supplied via a USB memory stick.

NOTE: Senetas encryptors support only USB drives that are configured with the FAT or FAT32 format.

Format:

<code>upgrade<CR></code>	Initiate the upgrade

The command provides an alternative means of installing firmware on encryptors that do not have a front panel keypad.

Prior to issuing the command the user must log in to the encryptor using an 'admin' account.

usb

The **usb** command is used to prevent or allow access to the encryptor front panel USB interface via a logical locking mechanism.

Format:

<code>usb<CR></code>	Display current USB port status
<code>[lock unlock]</code>	Enable or disable the USB port

Example: Display current status

```
CN6140_A>usb
USB port is unlocked
```

NOTE: If the port is locked then the encryptor will not respond to any USB device that is plugged in, including memory sticks containing a valid firmware upgrade.

users

The **users** command allows the table of authorized system users to be viewed and edited.

Format:

<code>users<CR></code>	List the current user tables
<code>-a</code>	Add a user
<code>-e <INDEX></code>	Edit user INDEX
<code>-n</code>	Show the number of users
<code>-d <INDEX></code>	Delete user INDEX
<code>-u <days></code>	Number of days with no user login, after which the account is locked out
<code>-s <mins></code>	Period of time in a session with noactivity, after which the user is logged out



Example 1: Display current entries:

```

CN6140_A>users
Number of users in table is 1
Index UserId Active Level Console Snmp
-----
1 admin Yes Administrator Yes Yes
Example 2: Add a new user
CN6140_A>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

```

Example 2: Delete a user

```

CN6140_A>users -d 2
UserId Active Level Console Snmp
-----
Fred Yes Operator Yes Yes
Are you sure you want to delete entry ? (y/n) y
Record deleted

```

NOTE: Only an Administrator can add new accounts or make changes to existing accounts. (An unauthorised user is not permitted to change his or her own password.)

When editing or creating a new user the command prompts for each piece of information required, if a default value is offered the Administrator may accept it by pressing <enter>.

The expiry date can be left as [0000-00-00], that is, inactive, or set to any valid date that is at least 2 days in the future.

User authorisation works in conjunction with the login process in that it provides the required passwords and specifies the expiry date.

version

The **version** command displays the following information about the encryptor :

- software library
- version numbers
- software build date and time



Format:

<code>version<CR></code>	Display version information

Example: Display version information

```
CN6140_A>version
Software:
Version : 2.7.1
Build Number : 1283747687
Build Date : 06-Sep-2017
Build Time : 04:34:47
Library
Build ID: D753
```

vlan

<< This CLI command can be used with Layer 2 encryption only. >>

The **vlan** command sets the policy for Ethernet frames that have IEEE 802.1Q headers.

Format:

<code>vlan<CR></code>	Display current VLAN protocol tag(s) and bypass status
<code>-p <-e -d></code>	Enable/disable VLAN protocol bypass
<code>1</code>	Set VLAN primary ethertype (0x8100 is built-in)
<code>2</code>	Set VLAN alternate ethertype (0x8100 is built-in)
<code>-m <-e -d></code>	Enable/Disable Multicast mgmt VLAN substitution.
<code>-v</code>	Set VLAN tag(s) for Multicast VLAN substitution.
	e.g. <code>vlan -v 81000001</code> or <code>vlan -v 8100000181000002</code>
<code>-s</code>	Set the number of stacked VLAN Ids used to establish a VLAN connection

Example: View current settings

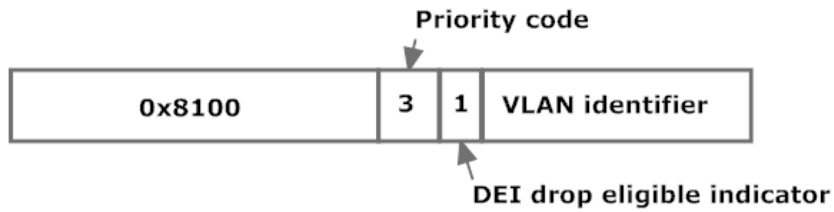
```
CN6140_A>vlan
VLAN parameter Status
-----
Protocol tag(s) bypass enabled
Alternate VLAN ethertype H8100
```

The IEEE 802.1Q header contains a 4-byte tag header including a 2-byte tag protocol identifier (TPID) and a 2-byte tag control information field (TCI) consisting of:

- Three-bit user priority
- One-bit canonical format indicator
- Twelve-bit VLAN identifier

By default, the CN Series enables VLAN tag bypass and will detect and bypass 802.1Q headers and use the type field that follows to determine the policy as shown:





A TPID value of 0x8100 is used to indicate the presence of an 802.1Q header. The **vlan** command allows an alternate value to be specified (alternate VLAN ethertype field); when set this causes the encryptor to parse for the presence of both 0x8100 AND the alternate value.

It is also possible that multiple VLAN tags can be inserted in an Ethernet frame (VLAN stacking or Q-in-Q). The CN Series supports stacking up to a maximum of 2 nested tags.



Section 8: Open Source Licences

The firmware at the heart of Senetas encryptors utilises a variety of open source applications.

Use of the Open Source components is subject to the applicable license agreements that are referenced below.

General Open Source license summary:

- [License GPL2](#)
- [License LGPL2.1](#)
- [License GPL3](#)
- [License BSD](#)
- [License BSD3](#)
- [License Apache v2](#)
- [Licence MIT](#)





Section 9: Alarms, event and audit logs

Each encryptor is able to provide details of any alarm conditions and supply details of any events and operator actions that have been logged within it.

CM7 allows the status of alarms and the content of the event and audit logs to be accessed for the selected encryptors by expanding the appropriate area as described in the following sections.

NOTE: Only a user with administration privileges can acknowledge alarms or clear the event and audit logs.

A count of the number of log entries is provided along with the number of unacknowledged alarms and SNMP traps received. In addition, if SNMP trap handling is enabled a count of the traps received is shown and if NTP servers are configured a count of these is provided.

Logs

The encryptor keeps two separate logs: an event log and an audit log. Both logs are kept in non-volatile memory and are therefore preserved across power cycles.

Each log can contain a maximum of 4000 records; when a log becomes full then it may be configured to either overwrite the oldest records (Wrap Enabled) or to stop logging new records (Wrap Disabled). This setting is configured through either the CLI or CM7.

Every log record is time-stamped and both logs can be viewed from either the CLI or remotely via SNMP management.

NOTE: The logs should be maintained and regularly examined to ensure any undesired events are detected.

Alarms

The Alarms tab lists each alarm that was raised, showing the date and time, the current state (active, inactive and acknowledged) and its description. See "Appendix A-3 Alarm messages" on page 341

When an alarm becomes active it will remain in the alarm table until acknowledged by a user (administrator or supervisor). This is true even if the alarm condition itself goes away.

Alarms can exist in one of the following states:

```
Alarm id(1): 15/09/2004 12:23:10 NACK Network port link down indication
```

```
Alarm id(2): 15/09/2004 12:24:10 NACK Invalid certificate alarm
```

Table 44. Alarm states

Alarm State	Meaning
Active unacknowledged	Alarm is currently active and has not been acknowledged by a user
Active acknowledged	Alarm is currently active and has been acknowledged by a user
Inactive unacknowledged	Alarm was active but was not acknowledged by a user before it became inactive
Inactive	Alarm is inactive and all previous alarms have been acknowledged

An alarm becoming active has the following effects:

1. The alarm is listed in the alarm table
2. The alarm LED on the front panel indicates the status of alarms in the following precedence:



- 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

3. A record is added to the event log indicating that an alarm has been set

4. When an alarm condition goes away an event is logged to indicate that the alarm was cleared

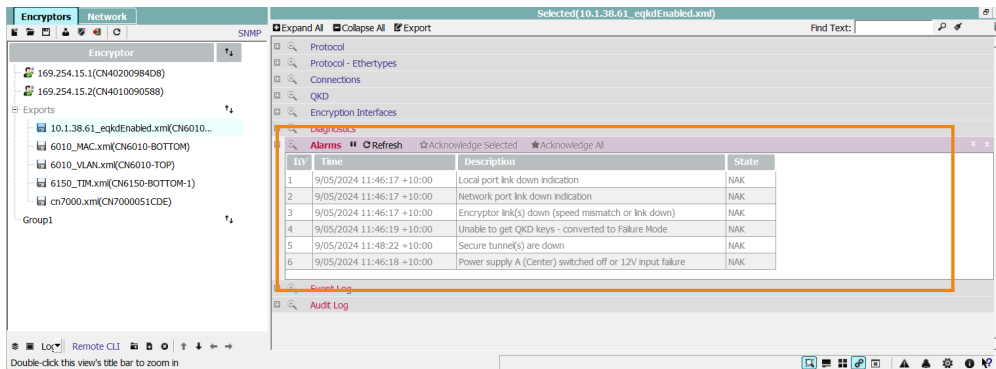


Figure 148: CM7 Alarm display

Event log

The event log (See "Appendix A-2 Event log messages" on page 334) is a record of "significant" happenings such as power up, self-test results, alarm conditions being set or cleared, etc. For example:

2004-09-14 11:48:40 Alarm cleared: Network interface path RDI

Each entry has a date/time stamp and a description of the event that occurred. The log can contain up to 4000 entries and it can be set to either wrap or truncate.

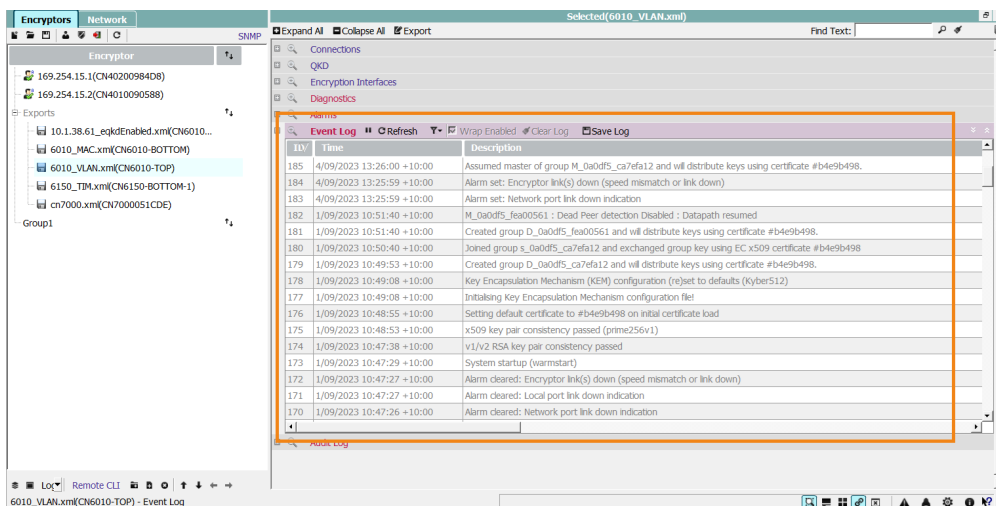


Figure 149: CM7 Event log display

The event log lists each event that has been logged, including the date and time and event description.

Audit log

The audit log (See " Appendix A-1 Audit log messages" on page 327) is a record of all configuration changes made to the encryptor.

Similar to the Event log, the list can be sorted, cleared and saved to a file on a network computer. The record indicates the name of the user making the change and exactly what change occurred. For example:

```
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 G832 ADM
```

The following screen shows the online view available from CM7

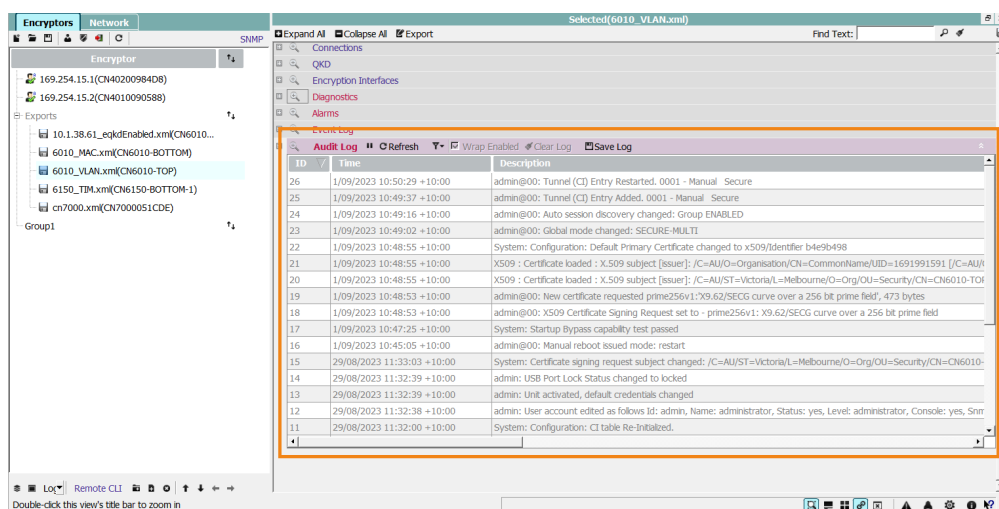


Figure 150: CM7 Audit log display

SNMP Traps

An SNMP trap is an asynchronous message sent by the encryptor to a pre-defined trap handler. Up to eight trap handler IP addresses can be defined and enabled so that alarms and events can be sent to specified trap handlers.

CM7 can operate as a trap handler, displaying the status of a number of encryptors. More usually, third-party network management systems such as Tivoli or NetView are used.

NOTE: In a Linux environment when you enable CM7 trap listening you must be running as root otherwise you will receive an authorization error.

Encryptors send SNMPv2 enterprise-specific trap messages to all defined handlers when an alarm is set or cleared; the trap message contains the text of the alarm description. See " Appendix A-4 SNMP trap messages" on page 344 for a full list of trap messages.

NOTE: For the new port to take effect you should disable traps prior to changing the port number and then re-enable the traps afterwards.

Each of the SNMP traps that have been generated by the encryptor is displayed in the SNMP Trap tab.



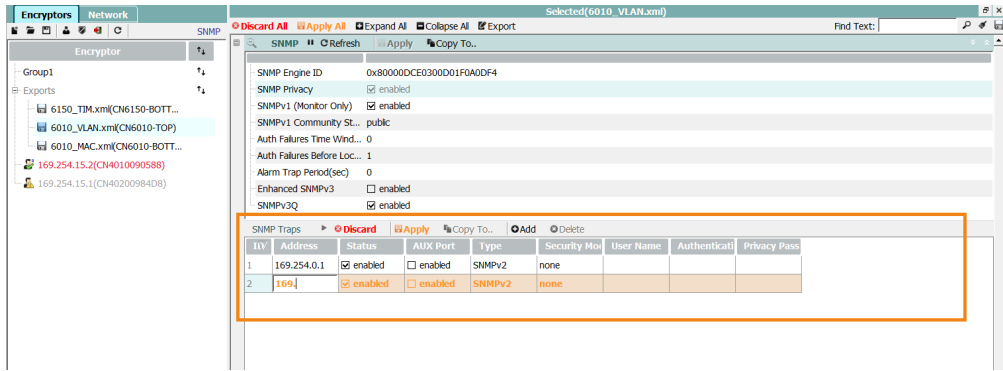


Figure 151: SNMP trap display

The SNMP Trap receivers can be defined via the CM7 SNMP pane allowing traps to be enabled on a specific port. Refer to "SNMP" on page 184



Appendix A-1 Audit log messages

Table 45. Audit log messages

Message
(Device) RSA Key Size Changed. Next certification will use:
Account inactive timeout period set to
Acknowledged active alarm
Alarm trap period set to
Audit log was corrupt and had to be recreated
Audit log wrapping
Auto discovery
Bypass of reserved Multicast changed to
Certificate authenticate failure
Certificate deleted
Certificate loaded
CI/Tunnel Key update interval changed to <minutes>
Cleared audit log
Cleared system log
CLI prompt set to
Configuration Reset and Reboot executed:
Configuration:
Configuration backup file created
Configuration restored from backup file
Connection started
Connection stopped
Control Plane Ethertype 1 changed to: <insert value>
Control Plane Ethertype 2 changed to: <insert value>
CRL entry added -
CRL entry changed -



Message
CRL entry deleted -
CRL :
Default Gateway IP address set to
Electrical Link Loss Forwarding changed to
Electrical LLF tied to connection status
Ethertype default broadcast action changed:
Ethertype default multicast action changed:
Ethertype default offset usage changed:
Ethertype default unicast action changed:
Ethertype Entry Added.
Ethertype Entry Deleted.
Ethertype Entry Edited.
Ethertype Notification.
FIPS Mode has been changed
Global Connection mode changed to
Global Connection mode Notification.
Global Crypto mode changed: Algorithm
Global mode changed:
Inband forwarding
IGMP/MLD Bypass <enabled/disabled>
Inband full arp
Inband gateway enable set to <insert value>
Inband Gateway IP address set to <insert value>
Inband IP address set to <insert value>
Inband management
Inband management circuit set to
Inband management VLAN tag change request -



Message
Inband management VLAN tagging
Inband network IP mask set to
Interframe gap changed:
IP address set
IP Multicast Header Bypass <enabled/disabled>
IP Protocol Encryption Identifier changed to: <insert value>
IP rules configuration : Layer4 mode encryption enabled/disabled
Keypad
L4 ICMP auto discovery:...
Led test mode
Line mode changed:
Link Autonegotiation changed:
Link control changed:
Link Loss Forwarding changed to
Link speed changed:
LLF on connection status (line mode) is
Local Link monitoring changed:
Local Time set to
Loopback set to
MAC Address Entry Added.
MAC Address Entry Deleted.
MAC Address Entry Edited.
MAC change Notification.
Mgmt channel settings restored to default.
Mgmt channel D_ID changed to
Mgmt channel RCTL changed to
Mgmt channel SOF k-word changed to



Message
Management session inactive timeout period set to
Manual reboot issued
MPLS bypass changed:
Multicast ageing changed to
Multicast Default action changed to
Multicast Management VLAN control changed:
Multicast Management VLAN tag value changed:
Network IP mask set
New certificate received from CA
New certificate requested
New MAC processing changed:
New SNMP trap destination added:
NTP server record added -
NTP server record changed -
NTP server record deleted -
NTP configuration
Number of stacked VLAN id(s) changed to
Number of stacked VLAN id(s) notification
Observe Pending action on ingress changed to
OCSP entry added -
OCSP entry changed -
OCSP entry deleted -
OCSP :
Out-Of-Band management
Password enhanced mode:
Password lexical checking
Password minimum length:
Password minimum lowercase characters:



Message
Password minimum numerical characters:
Password minimum special characters:
Password minimum uppercase characters:
Password reuse history size set to
Path MTU Adjustment:...
Path MTU Bypass:...
Path MTU Maximum changed to ... (bytes)
Power Supply mode changed to
Reserved MAC Address Added.
Reserved MAC Address Deleted.
Reserved MAC Address Edited.
Reserved MAC Address Notification.
Session added
Session deleted
Session edited
Shim insertion rate changed to
Shim MTU overflow prevention change to
SNMP Enhanced Algorithm support has been
SNAP observe PID as ethertype changed:
SNMP Privacy Mode has been
SNMP V1 read only access
SNMPV3Q Quantum Hybrid mode has been...
STP monitoring changed to
Syslog server record added -
Syslog server record changed -
Syslog server record deleted -
Syslog configuration
System log wrapping



Message
Three failed login attempts - console locked
Timezone set to
TRANSEC bandwidth usage changed to
TRANSEC frame length changed to
TRANSEC header changed
TRANSEC mode DISABLED
TRANSEC mode ENABLED
Trap destination deleted:
Trap destination updated:
Tunnel (CI) Entry Added.
Tunnel (CI) Entry Deleted.
Tunnel (CI) Entry Edited.
Tunnel (CI) Entry Started.
Tunnel (CI) Entry Stopped.
Tunnel (CI) Notification.
Tunnel Keep Alive changed to
Unit erased to factory default
USB Port Lock Status changed to
User account added
User account deleted
User account edited
User account made inactive:
Valid Certificate not loaded.
VLAN header bypass changed:
VLAN Tunnel (CI) Entry Added.
VLAN Tunnel (CI) Entry Deleted.
VLAN Tunnel (CI) Entry Edited.
VLAN Tunnel (CI) Notification.



Message

VLAN Tunnel (CI) Entry Started.

VLAN Tunnel (CI) Entry Stopped.

Zero payload frames Bypass:...

Message based on template: [IPv{4/6}] <name> ({En/Dis}abled) addr <IP address>/<prefix> gw <gateway address>

Example: [IPv4] Inband Mgmt (Enabled) addr 192.168.1.2/0 gw 192.168.1.1



Appendix A-2 Event log messages

Table 46. Event log messages

Message
AES128 Decrypt self-test FAILED
AES128 Decrypt self-test passed
AES128 Encrypt self-test FAILED
AES128 Encrypt self-test passed
AES256 Decrypt self-test FAILED
AES256 Decrypt self-test passed
AES256 Encrypt self-test FAILED
AES256 Encrypt self-test passed
Alarm cleared: Master unit has stopped supplying keys, Generating own keys
Alarm set: Master unit has stopped supplying keys, Generating own keys
Backup/Restore operation FAILED
Certificate is not current
Certificate load - encryptor is not activated
Certificate load - encryptor not in certificate mode
Certificate load - invalid or corrupt PEM file discarded
Certificate load - received public key doesnot match that sent
Certificate load - received signature not valid
Certificate load - received unknown digest type
Certificate load - RSA decrypt error
CRL failed validation
CRL load - not enough space available to load CRL:
CRL loaded
Crypto Bypass test FAILED
Crypto Bypass test passed
Crypto self-test FAILED



Message
Crypto self-test passed
DES Engine self-test FAILED
DES Engine self-test passed
DES112 (2 key) Decrypt self-test FAILED
DES112 (2 key) Decrypt self-test passed
DES112 (2 key) Encrypt self-test FAILED
DES112 (2 key) Encrypt self-test passed
DES168 (3 key) Decrypt self-test FAILED
DES168 (3 key) Decrypt self-test passed
DES168 (3 key) Encrypt self-test FAILED
DES168 (3 key) Encrypt self-test passed
DES56 (1 key) Decrypt self-test FAILED
DES56 (1 key) Decrypt self-test passed
DES56 (1 key) Encrypt self-test FAILED
DES56 (1 key) Encrypt self-test passed
DRAM self-test FAILED
DRAM self-test passed
DRBG800-90 Random Bit Generator self-test failed
DRBG800-90 Random Bit Generator self-test passed
DSA-1024 self-test FAILED
DSA-1024 self-test passed
DSA-2048 self-test FAILED
DSA-2048 self-test passed
DSA-3072 self-test FAILED
DSA-3072 self-test passed
DSA-512 self-test FAILED



Message
DSA-512 self-test passed
ECDH prime256v1 : KAT self-test passed
ECDH prime256v1 : KAT self-test FAILED
ECDH secp384r1 : KAT self-test passed
ECDH secp384r1 : KAT self-test FAILED
ECDH secp521r1 : KAT self-test passed
ECDH secp521r1 : KAT self-test FAILED
ECDSA prime256v1 SHA256 : KAT self-test passed
ECDSA prime256v1 SHA256 : KAT self-test failed
ECDSA prime256v1 SHA256 : self-test passed
ECDSA prime256v1 SHA256 : self-test FAILED
ECDSA prime256v1 SHA384 : self-test passed
ECDSA prime256v1 SHA384 : self-test FAILED
ECDSA prime256v1 SHA512 : self-test passed
ECDSA prime256v1 SHA512 : self-test FAILED
ECDSA secp384r1 SHA256 : self-test passed
ECDSA secp384r1 SHA256 : self-test FAILED
ECDSA secp384r1 SHA384 : self-test passed
ECDSA secp384r1 SHA384 : self-test FAILED
ECDSA secp384r1 SHA512 : self-test passed
ECDSA secp384r1 SHA512 : self-test FAILED
ECDSA secp521r1 SHA256 : self-test passed
ECDSA secp521r1 SHA256 : self-test FAILED
ECDSA secp521r1 SHA384 : self-test passed
ECDSA secp521r1 SHA384 : self-test FAILED
ECDSA secp521r1 SHA512 : self-test passed
ECDSA secp521r1 SHA512 : self-test FAILED
Error: <filename> failed Authentication/Decryption. Ensure file is not corrupt and has .ctam or .sfnt file extension
Failed attempt to login to console:
Forced password lexical checking on
Hardware Random Noise Generator self-test FAILED



Message
Hardware Random Noise Generator self-test passed
Hardware Random statistical check FAILED
Hardware Random statistical check passed
HMAC-SHA1 self-test FAILED
HMAC-SHA1 self-test passed
HMAC-SHA256 self-test FAILED
HMAC-SHA256 self-test passed
HMAC-SHA512 self-test FAILED
HMAC-SHA512 self-test passed
I2C self-test FAILED
Initialising event log due to size error
Initialising event log due to CRC error
KDF135 SNMP self-test passed
KDF135 SNMP self-test FAILED
KDF135 SSH self-test passed
KDF135 SSH self-test FAILED
KDF135 TLS self-test passed
KDF135 TLS self-test FAILED
LCD self-test FAILED
Logged into console:
Logged out of console:
Maximum number of outstanding X.509 certificate requests reached - deleting oldest key
OCSP: <insert message>
Password failed lexical check
Password failed reuse history check
RSA Engine self-test FAILED
RSA Engine self-test passed
RSA key pair consistency FAILED



Message
RSA key pair consistency passed
RSA-1024 Private Key Decrypt self-test FAILED
RSA-1024 Private Key Decrypt self-test passed
RSA-1024 Private Key Encrypt self-test FAILED
RSA-1024 Private Key Encrypt self-test passed
RSA-1024 Public Key Decrypt self-test FAILED
RSA-1024 Public Key Decrypt self-test passed
RSA-1024 Public Key Encrypt self-test FAILED
RSA-1024 Public Key Encrypt self-test passed
RSA-2048 Private Key Decrypt self-test FAILED
RSA-2048 Private Key Decrypt self-test passed
RSA-2048 Private Key Encrypt self-test FAILED
RSA-2048 Private Key Encrypt self-test passed
RSA-2048 Public Key Decrypt self-test FAILED
RSA-2048 Public Key Decrypt self-test passed
RSA-2048 Public Key Encrypt self-test FAILED
RSA-2048 Public Key Encrypt self-test passed
RSA-4096 Private Key Decrypt self-test FAILED
RSA-4096 Private Key Decrypt self-test passed
RSA-4096 Private Key Encrypt self-test FAILED
RSA-4096 Private Key Encrypt self-test passed
RSA-4096 Public Key Decrypt self-test FAILED
RSA-4096 Public Key Decrypt self-test passed
RSA-4096 Public Key Encrypt self-test FAILED
RSA-4096 Public Key Encrypt self-test passed
Session established



Message
Session FAILED - address compression failure
Session FAILED - address overlaps existing connection
Session FAILED - Certificate version mismatch
Session FAILED - encryption algorithm mismatch
Session FAILED - encryption mode mismatch
Session FAILED - No V1 certificate loaded
Session FAILED - No V2 certificate loaded
Session FAILED - received certificate is not current
Session FAILED - remote CA authentication failure on flow 1
Session FAILED - remote CA authentication failure on flow 2
Session FAILED - signature algorithm mismatch
Session FAILED - the certificate of the unit is not current
Session key update received
Session key update sent
Session warning - hash algorithm mismatch
SHA-1 self-test FAILED
SHA-1 self-test passed
SHA-256 self-test FAILED
SHA-256 self-test passed
SHA-512 self-test FAILED
SHA-512 self-test passed
SW self-test FAILED
SW self-test passed
System manual shutdown
System startup (coldstart)
System startup (warmstart)



Message

Thermostat self-test FAILED

User account expired due to inactivity:

User account information is weak - Rejected

Validate egress certificate #[certificate hash] failed for CI=[x]

Validate egress QRA certificate #[certificate hash] failed for CI=[x]

X.509 Certificate request error

X509 verify <insert message>

X9.31 Random Number Generator self-test FAILED

X9.31 Random Number Generator self-test passed



Appendix A-3 Alarm messages

Table 47. Alarm messages

Message
Audit log is full
Certificate has expired and is no longer valid
Configuration battery low warning
CRL file processing error occurred
Encryptor link(s) down (speed mismatch or link down)
FIPS EFP Voltage input out of range
FIPS EFP System Temperature out of range
Invalid certificate alarm
Local interface AIS
Local interface FERF
Local interface loss of cell delineation
Local interface loss of frame
Local interface loss of signal
Local interface RAI (Yellow)
Local port link down due to Electrical Link Loss Forwarding (ELLF)
Local port link down indication
Network interface AIS
Network interface FERF
Network interface loss of cell delineation
Network interface loss of frame
Network interface loss of signal
Network interface RAI (Yellow)
Network port link down from Electrical Link Loss Forwarding (ELLF)
Network port link down indication



Table 47. Alarm messages(continued)

Message
Power supply removed turned off or faulty
Secure tunnel(s) are down
Static sessions converted to Three Key Triple DES
System battery low warning
System log is full
System noise source failure
System power-up tests failed
System temperature alarm
Transmit Underrun
Unable to get QKD keys - converted to Failure Mode
WARNING - An integrity check has failed
WARNING - Audit log is over 75 percent full
WARNING - Bandwidth is being clipped
WARNING - Certificate will expire in less than 14 days
WARNING - Certificate will expire in less than 2 days
WARNING - Certificate will expire in less than 21 days
WARNING - Certificate will expire in less than 24 hours
WARNING - Certificate will expire in less than 28 days
WARNING - Certificate will expire in less than 3 days
WARNING - Certificate will expire in less than 4 days
WARNING - Certificate will expire in less than 5 days
WARNING - Certificate will expire in less than 6 days
WARNING - Certificate will expire in less than 7 days
WARNING - Default user credentials detected
WARNING - External Entropy file 80 percent exhausted
WARNING - External Entropy file 85 percent exhausted
WARNING - External Entropy file 90 percent exhausted



Table 47. Alarm messages(continued)

Message
WARNING - External Entropy file 95 percent exhausted
WARNING - External Entropy file 100 percent exhausted - reverting to internal source
WARNING - External Quantum Origin server unreachable
WARNING - Jumbo Packets present and dropped, please reduce MTU at source
WARNING: V2 Certificate required for group key encryption (Multicast/VLAN)
WARNING - System log is over 75 percent full
X.509 certificate verification error occurred



Appendix A-4 SNMP trap messages

Table 48. SNMP trap messages

OID	Meaning
OID: 1.3.6.1.4.1.3534.3.1.1.3.1.2	eventNetworkLinkUp NOTIFICATION-TYPE OBJECTS { sysLocalTime, sysAlarmDescr } “Link Up condition detected on network port”
OID: 1.3.6.1.4.1.3534.3.1.1.3.1.3	eventNetworkLinkDown NOTIFICATION-TYPE OBJECTS { sysLocalTime, sysAlarmDescr } “Link Down condition detected on network port”
OID: 1.3.6.1.4.1.3534.3.1.1.3.1.4	eventLocalLinkUp NOTIFICATION-TYPE OBJECTS { sysLocalTime, sysAlarmDescr } “Link Up condition detected on local port”
OID: 1.3.6.1.4.1.3534.3.1.1.3.1.5	eventLocalLinkDown NOTIFICATION-TYPE OBJECTS { sysLocalTime, sysAlarmDescr } “Link Down condition detected on local port”
OID: 1.3.6.1.4.1.3534.3.1.1.3.1.6	eventEncryptorLinkUp NOTIFICATION-TYPE OBJECTS { sysLocalTime, sysAlarmDescr } “Encryptor Link is Up (signifies both local and network ports are up)”
OID: 1.3.6.1.4.1.3534.3.1.1.3.1.7	eventEncryptorLinkDown NOTIFICATION-TYPE OBJECTS { sysLocalTime, sysAlarmDescr } “Encryptor Link is Down (signifies one or both of the local or network ports is down).”
OID: 1.3.6.1.4.1.3534.3.1.1.3.1.8	eventLogIn NOTIFICATION-TYPE OBJECTS { sysLocalTime, sysAlarmDescr } “A successful login has occurred on the CLI for the encryptor.”
OID: 1.3.6.1.4.1.3534.3.1.1.3.1.9	eventLogOut NOTIFICATION-TYPE OBJECTS { sysLocalTime, sysAlarmDescr } “A user has logged out of the CLI interface on this encryptor”
OID: 1.3.6.1.4.1.3534.3.1.1.3.1.10	alarmLogInFailed NOTIFICATION-TYPE OBJECTS { sysLocalTime, sysAlarmDescr } “A failed attempt to log into the CLI interface on this encryptor. A failed attempt is classified as three successive failed login attempts.”



Table 48. SNMP trap messages(continued)

OID	Meaning
OID: 1.3.6.1.4.1.3534.3.1.1.3.1.11	<p>eventColdStart NOTIFICATION-TYPE</p> <p>OBJECTS { sysLocalTime }</p> <p>"A unit cold start has occurred"</p> <p>NB: The standard net-snmp coldstart trap will be received in addition to a coldstart or warmstart trap given here. This should be ignored as it relates to the SNMP stacks state, and not the platforms state.</p>
OID: 1.3.6.1.4.1.3534.3.1.1.3.1.12	<p>eventWarmStart NOTIFICATION-TYPE</p> <p>OBJECTS { sysLocalTime }</p> <p>"A warmstart has occurred. Typically requested from a CLI or SNMP operation."</p>
OID: 1.3.6.1.4.1.3534.3.1.1.3.1.15	<p>certificateExpiry NOTIFICATION-TYPE</p> <p>OBJECTS { certificateDaysLeft }</p> <p>"Notification of an upcoming certificate expiry.</p> <p>Includes the OID of the certificateDaysLeft for the relevant certificate."</p>
OID: 1.3.6.1.4.1.3534.3.1.1.3.1.16	<p>fipsModeChange NOTIFICATION-TYPE</p> <p>OBJECTS { fipsMode }</p> <p>"Notification of a change in the FIPS mode, including the new fipsMode."</p>
OID: 1.3.6.1.4.1.3534.3.1.1.3.1.17	<p>auditPasswordLexicalChange NOTIFICATION-TYPE</p> <p>OBJECTS { sysLocalTime, sysAlarmDescr }</p> <p>"One of the following password lexical parameters changed:</p> <p>sysUserAccessPasswordMinLength</p> <p>sysUserAccessPasswordMinUppercase</p> <p>sysUserAccessPasswordMinLowercase</p> <p>sysUserAccessPasswordMinNumerical</p> <p>sysUserAccessPasswordMinSpecial"</p>
OID: 1.3.6.1.4.1.3534.3.1.1.3.1.1	<p>alarmRaised NOTIFICATION-TYPE</p> <p>OBJECTS { sysLocalTime, sysAlarmDescr }</p> <p>An alarm was raised by the encryptor:</p>
000 ALARM_SYS_TEMP "System temperature alarm"	
001 ALARM_RTC_BATTERY "System RTC battery low"	



Table 48. SNMP trap messages(continued)

OID	Meaning
002 ALARM_SRAM_BATTERY	"Configuration battery low warning"
003 ALARM_SYS_NOISE	"System noise source failure"
004 ALARM_LOCAL_LINK (set)	"Local link down"
004 ALARM_LOCAL_LINK (cleared)	"Local link up"
005 ALARM_NETWORK_LINK (set)	"Network link down"
005 ALARM_NETWORK_LINK (cleared)	"Network link up"
006 ALARM_INVALID_CERTIFICATE	"Invalid certificate alarm"
007 ALARM_SELF_TESTS_FAILED	"System power-up tests failed"
008 ALARM_SYSTEM_LOG_FULL	"System log is full"
009 ALARM_AUDIT_LOG_FULL	"Audit log is full"
010 ALARM_LOCAL_LOS	"Local interface loss of signal"
011 ALARM_LOCAL_LOF	"Local interface loss of frame"
012 ALARM_LOCAL_LCD	"Local interface loss of cell delineation"
013 ALARM_LOCAL_AIS	"Local interface AIS"
014 ALARM_LOCAL_FERF	"Local interface FERF"
015 ALARM_LOCAL_RAI	"Local interface RAI (Yellow) "
020 ALARM_NETWORK_LCD	"Network interface loss of cell delineation"
021 ALARM_NETWORK_AIS	"Network interface AIS"
022 ALARM_NETWORK_FERF	"Network interface FERF"
023 ALARM_NETWORK_RAI	"Network interface RAI (Yellow) "
024 ALARM_NETWORK_LOS	"Network interface loss of signal"
025 ALARM_NETWORK_LOF	"Network interface loss of frame"
030 ALARM_TRANSMIT_UNDERRUN	"Transmit Underrun"
031 ALARM_CERT_EXPIRES_IN_28_DAYS	"WARNING -Certificate will expire in less than 28 days"
032 ALARM_CERT_EXPIRES_IN_21_DAYS	"WARNING -Certificate will expire in less than 21 days"
033 ALARM_CERT_EXPIRES_IN_14_DAYS	"WARNING -Certificate will expire in less than 14 days"



Table 48. SNMP trap messages(continued)

OID	Meaning
034 ALARM_CERT_EXPIRES_IN_7_DAYS	"WARNING -Certificate will expire in less than 7 days"
035 ALARM_CERT_EXPIRES_IN_6_DAYS	"WARNING -Certificate will expire in less than 6 days"
036 ALARM_CERT_EXPIRES_IN_5_DAYS	"WARNING -Certificate will expire in less than 5 days"
037 ALARM_CERT_EXPIRES_IN_4_DAYS	"WARNING -Certificate will expire in less than 4 days"
038 ALARM_CERT_EXPIRES_IN_3_DAYS	"WARNING -Certificate will expire in less than 3 days"
039 ALARM_CERT_EXPIRES_IN_2_DAYS	"WARNING -Certificate will expire in less than 2 days"
040 ALARM_CERT_EXPIRES_IN_24_HOURS	"WARNING -Certificate will expire in less than 24 hours"
041 ALARM_CERT_EXPIRED	"Certificate has expired and is no longer valid"
042 ALARM_TOP_POWER_REMOVED	"Power supply A (Top) not present"
053 ALARM_BOT_TMP_FAIL	"Power supply B (Bottom) alarm -exceed temperature limit"
056 ALARM_LINK	"Encryptor link is down"
057 ALARM_LOCAL_LLF (set)	"Local link down due to Link Loss Forwarding (LLF)"
057 ALARM_LOCAL_LLF (cleared)	"Local link recovered from LLF"
058 ALARM_NETWORK_LLF (set)	"Network link down due to Link Loss Forwarding (LLF)"
058 ALARM_NETWORK_LLF (cleared)	"Network link recovered from LLF"
059 ALARM_QKD_FAIL (set)	"Encryptor converted to QKD Failure Mode"
059 ALARM_QKD_FAIL (cleared)	"Encryptor recovered from QKD Failure Mode"
060 ALARM_DEFAULT_USER	"WARNING -Default user credentials detected"
061 ALARM_DES_TO_3DES_UPGRADE	"Static sessions converted to Three Key Triple DES"
062 ALARM_POWER_REMOVED	"Power supply removed, turned off or faulty"
064 ALARM_LOCAL_ELLF	"Local port link down due to Electrical Link Loss Forwarding"
065 ALARM_NETWORK_ELLF	"Network port link down due to Electrical Link Loss Forwarding"
066 ALARM_TUNNEL_FAULT	"Secure tunnel(s) are down"
071 ALARM_V2_CERT_REQUIRED	"WARNING - V2 Certificate required for group key encryption"
072 ALARM_JUMBO_PACKETS	"WARNING -Jumbo packets present and dropped. Please reduce MTU at source"
073 ALARM_FPGA_SRAM_FAULT	"FPGA SRAM failed self tests"



Table 48. SNMP trap messages(continued)

OID	Meaning
074 ALARM_CRL_FILE_PROC_ERROR	"CRL file processing error occurred"
075 ALARM_PKI_VFY_ERROR	"X509 Certificate verification error occurred"
076 ALARM_MASTER_MISSING	"Master Unit has stopped supplying keys, Generating own keys"



Index

#	
0x8847 MPLS tag (H8847)	285
0x8847 Multicast MPLS tag (H8848)	285
10/100Base-T	16
10Base-T	2
100Base-TX	2
802.1D	285
802.1Q - VLAN headers	319
802.2	111
802.3	111
A	
A614xB	5
Access	
administrator	117
locking	177
Account(s)	
default	122
defining	116
management	122
maximum number	122
ACK frames	206
Action(s)	
injected	205
Multicast	204
Unicast	204
Activation	163, 247
CLI command	242
Local	242
non activated password	141
to commission unit	23
using CM7	25
using the CLI	25
activation - CLI command	242



Add Route	231
Address	
front panel IP	183
setup for QKD units	214
Administrator	181
role	122, 295
Advanced Encryption Standard	41
AES	
Advanced Encryption Standard	41
Alarm(s)	220, 323
acknowledging	323
battery low voltage	7
CLI command	243
indicator	323
messages	341
alarms - CLI command	243
Algorithm(s)	
signature hash	144
Algorithms	
encryption	39
TLS	39
AR-25	
password policy	117
standard	117
Architecture	
encryption	110
ARP	231
Attack(s)	
Man-in-the-middle	83
Audit	221
CLI command	243
Log	325
Messages	327
audit - CLI command	243
Authentication	
certificate validation interval	210-211



of user credentials	116
authNoPriv	227
authPriv	227
Auto Discovery	
Broadcast traffic	75
CLI command	244
Group	209, 211
in Point-point (Line) mode	109
Multicast	75
of MAC addresses	76
Unicast	211
Auto populate	
CLI command	245
facility	107
autodisco - CLI command	244
Auto-negotiation	
enabling	282
autopop - CLI command	245
B	
banner - CLI command	246
Battery	
CN6000 Series	7
Bill of material	
CN6000	21
Boot up sequence	12
BPDU messages	79
Broadcast	
encryption configuration	110
traffic	75
Build	
Date and time	178
Number	178
of software	178
Bullseye	136
Bypass	
enabling IP Multicast	200



Ethertype processing	204
MAC addresses	110
MPLS shims	202
Multicast addresses	203
Reserved Multicast	203
Bypass Reserved Multicast	
in VLAN mode	59, 74, 94
required for IGMP bypass	294
setting via CLI	293
setting via CM7	203
C	
CA - see Certificate Authority	146
CA/Key Management	
Certificate Authority creation	142
KDK key creation	142
CDR alarm	298
certificate - CLI command	246
Certificate Authority	
advanced functions	146
validity period	144
Certificate(s)	
CLI command	246
expiration period	166
for RESTful interface	250
hash algorithm	144
import PEM	192
serial number	166
servers	194
view certificates	192
Certification	
internal using CM7	165
with external CA	168
Certify	164
Chassis	7
Checksum calculation	
Layer 4	275



CI	
MAC connection index	76
CIDR	183
CLI	
setting Post-Login	181
setting Pre-Login	181
setting Prompt	181
Client frame	65
cloud-init	100
CM7	
CM.ini file	140
enable/disable entropy	177
installing	133
Linux installation	136
management options	173
moving to a new PC	159
protocol support	28
settings file	140
sorting encryptor list	132
starting on Linux	136
system requirements	134
Windows installation	134, 137
CN Series	
CN6140	3
enclosures	2
CN6000 Series	
AC Power Supply	8
battery	7
DC Power Supply	8
fan tray	7
indicators	4
network interfaces	5
CN6140	
features	4
Cog icon	140



Command Line Interface

activate	242
alarm	243
audit	243
autodisco	244
autopop	245
banner	246
certificate	246
community	251
con	251
controlplaneif	251
crl	251
crypto	252
date	253
entropy	253
eping	254
eqkd	255
erase	256
ethertypes	257
event	259
fips	260
ftpcfg	261
global	261
help	226, 262
history	263
hostname	263
inband_vlan	263
initcfg	265
inventory	270
ip	271
iprules	274
kdf	276
kem	277
keypad	277
keyprovider	277
kscfg	278



kscfg_tier	279
line	280
linkspeed	281
locmacs	283
logout	284
mode	285
mpls	285
netmacs	286
ntpcfg	287
ocsp	287
overview	288
password	288
policy	292
profile	295
prompt	296
protocol	296
psu	296
qkd	297
qsfp	298
reboot	299
rest	300
sfp	301
shim	302
slot	303
snap	304
snmpcfg	305
snmptraps	305
sshaux	306
sshcli	306
stats	307
syslog	309
tacacs	311
timezone	311
transec	313
tunnels	314
upgrade	317



usb	317
users	317
version	318
vlan	319
Commissioning	
activation using CM7	25
activation using the CLI	25
Process description	23
Community	
string	120, 184
community - CLI command	251
con - CLI command	251
Configuration	
BPDU messages	79
database	130, 165
exporting	173
Importing or exporting PKCS#12 files	150
initial settings	157
listing	236
server	165
server databases	157
servers (defined)	162
TIM mode via CLI	107
Connection Action Table	
Initialization	45
Connection(s)	
Action Table	76
adding manually	85
ancillary (hybrid) certificate	209, 211
available	43
certificate	209-210
close on certificate expiry	209-211
management	7
modes - Ethernet	43
Multicast retention period	211
Status	209-210, 212



System Pending	75
table, layer 2	208
Console	181
connection	16
inactivity lockout	117
Management	181
port	16
RS232 port	2
Control plane	
ethertype	110, 259
controlplaneif - CLI command	251
Craft (RS232) interface	7
Credentials	
authentication of	116
changing via Activation	162
default	23
crl - CLI command	251
CRL Certificate Revocation List	
CLI command	251
configuring servers	194
servers	194
Crypto	
CLI command	252
mode	200
crypto - CLI command	252
Cryptographic Modes	42
CSR	164
copy to clipboard	168
save to PEM file	168
CTR	
encryption mode	200
Customer VLAN	113
D	
Dark fibre	22
Data loss	
CM7 and CLI statistics	41



date - CLI command	253
Date and time	
CLI command	178, 253
Not Before	238
not set	239
of Software build	178
setting from CM7	24, 177, 179
source of	25
Days remaining	193
DB9 connector	16
DCE	16
Dead peer	
detection interval	209
operation	240
DEK - Data encryption key(s)	
egress	101
DHCP	23
Diagnostics	
Ethertype	237
ethertypes	217
local interface	219
Management	217
Network interface	220
Start up tests	12
start up tests	120
Diffie-Hellman	
agreement	116
security level	160
Discard(ed)	
frame count	41
L3 and L4 frames	101
Discharge	
damage to equipment	22
Discover(y)	
timeout	141
using CM7	141



Display	
errors in CM7 log window	141
information messages in CM7 log window	141
Distinguishing Names	193
Dropped frames	
in CFB mode	253
DTE	16
Dual supply	7

E

EC parameters	149
ECC - elliptic curve cryptography	164
ECDH	
See Elliptic Curve Diffie Hellman	193
Egress	
DEK	101
Electrical LLF	216
Elliptic Curve Diffie Hellman	149, 193
Emergency erase	6
Enabling Inband	231
Encryption	iii
interfaces	215
Latency	110
NTP based (TIM mode)	26
offset	59, 74, 93
Encryption Resolution Protocol - see ERP	77
Encryptor(s)	
Commissioning	23
connections	7
Interface configuration	216
keypad	2
locating	22
Multi-slot	161
Naming	24
operation modes	41
Restart from CM7	178
set Encryptor list refresh rate(sec)	141



set Network view refresh rate(sec)	141
unpacking	21
VLAN settings	200
Entropy	
CLI command	253
enable/disable via CLI	253
enable/disable	177
user defined	29
entropy - CLI command	253
Environment	
non-operating	21
operating	21
eping - CLI command	237, 254
eqkd - CLI command	255
Erase	
emergency, from CM7 or CLI	6
emergency, from front panel	6
erase - CLI command	256
ERP	
remote Name/Address resolution	77
Errors	
FCS	219
Local and Network ports	219
startup	13
Ethernet	
DIX format	111
encryption	39
encryption policy	40, 56, 71, 90
Ethernet II (DIX)	111
IEEE 802.3 SAP	111
MAC migration	77
MPLS	113
operation modes	41
performance	110
SAP format	112
SAP SNAP format	112



Ethernet encryption	
cryptographic modes	42
frame formats	111
Multicast Operation	109
operation modes	41
Performance	110
Policy	40, 90
refining policy	203
Unicast operation	109
Ethertype(s)	
0xFC0F Senetas reserved type	76
0xFC0F Senetas type	110
alternate	200
CLI command	257
control plane	110, 259
defined actions	204
diagnostics	217
H8100 - VLAN	113
H8847 - MPLS Unicast	285
mutation	58, 73, 93
policy	57, 72, 92, 203
table re-initialization	45
unknown action	204
ethertypes - CLI command	257
ETSI	
QRA support	215
standard support	214
Event	221
CLI command	259
log messages	334
Logs	324
event - CLI command	259
Exiting from CM7	224
Explicit Login	141
Export configuration	236



Exporting	
configurations	173
PKCS#12 files	150
External	
certification	168
F	
Fan tray	
CN6000 Series	7
FC0E/FC0D	
reconfiguration	76
FCS	
error count	219
errored frames	17, 19
Ethernet	40
FEC	
enabling forward error correction	283
FEC - Forward Error Correction	12
Fibre	
cleaning	17
FIPS	
compliance	12
mode	116
fips - CLI command	260
FIPS 140-2	
CLI command	260
compliance	177, 189
enable/disable from CM7	177
enabling/disabling	121
mode	116
Firmware	
installation	27
Multicast support	58, 73, 109
upgrades	122
upgrades using CM7	28
upgrades via USB - CN/CS series only	29
upgrading multiple encryptors	28



Flow-Control	
TRANSEC	64
FollowCI	43, 92
Ethertype action	92
Fonts	
issues with	137
Forward Error Correction	12
Frame(s)	
Ethernet format - TIM mode	114
Ethernet formats	111
L3 and L4 discarded	101
management ethertype	200
overhead	41
size range	2
TIM mode format	107
Front panel	175
keypad enable/disable	177
USB enable/disable	177
ftpcfg - CLI command	261
FTPS	
server	187
G	
Galois counter mode - see GCM	42
Gateway	232
configuration	231
enabling within encryptor	120
gEthSenderId	213
Global	
policy	199
global - CLI command	261
GMT	312
Group keys	44
for Multicast encryption	109
GTS Generic traffic shaping	64



H

Halt	
secure Configuration.CustomSbox_Cndx [19]	13
Hardware	
details	178
Hash algorithm	144
Help	
CLI	226
CLI command	262
help - CLI command	262
Helpall	
CLI command	262
Hexadecimal	226, 242
0xhhh form	226, 242
Hhhh form	226, 242
history - CLI command	263
hostname - CLI command	263

I

ICMP	
statistics	15
Icons	
Cog	140
IEC13	
cable	7
IEEE	
802.2	111
802.3	111
IFG	217
IGMP/MLD	
processing status	200
Importing	
PKCS#12 files	150
Inband management	231
gateway	229
gateway enabling	120



LAN requirements	231
overview	230
Route Add command	231
route addition	231
inband_vlan - CLI command	263
Indicators	
CN6000 Series	4
Power	7
initcfg - CLI command	265
injected Action	205
Installing	
CM7	133
CM7 on Linux	136
firmware	27
unpacking hardware	21
Interface(s)	
for CN Series	5
key distribution	200
RESTful	123
Internal Certification	165
inventory - CLI command	270
IP	
port statistics	15
ip - CLI command	271
IP addresses	
setting from the CLI	23
IP Rules	205
CLI command	274
deleting	103
maximum	102
specifying	102
table	101
iprules - CLI command	274
J	
Jflow traffic analyzer	114
Jitter	110



K

KDF	202
key derivation function	98
key provider	200
kdf - CLI command	276
KDK	
current key	172
file creation	155
generation	26
installation time	171
Key Derivation Key	26, 276
key distribution	171
keys	155
next key	172
kem - CLI command	277
Key Derivation Function	98, 202
Key Derivation Key	276
Key Provider	
model description	97
NTP or Counter based	41
selection KDF or KMIP	200
timing of changes	98, 278
Key servers	
KMIP	97, 99
Key synchronization	
TIM mode	105
Key(s)	
certification key size (PK Size)	193
certification type (PK Type)	193
distribution interface	200
group	44
Group	109
KID - Key Identifier	96
pairwise	44
update interval	209-211
update period	211



Keypad	2, 29
keypad - CLI command	277
keyprovider - CLI command	277
KeySecure	
adding servers	188
configuring with CM7	187
key provider	99
KID	
described	96
KMIP	
key provider	200
key server	97
key servers	99
key synchronization	105
with Auto population	108
kscfg - CLI command	278
kstier - CLI command	279

L

L3 encryption	
allowing for NAT	275
LAN	231
Latency	79, 110
Ethernet	110
of CN Series	110
with STP	79
Layer 4 checksum calculation	275
LCD	
backlight	5
display	2
Lexical diversity	
checking	117
Licenses	
slot allocation	303
Licensing screen	168
Lightning strikes	22
limitations	62



line - CLI command	280
Line (Point-point) Mode	199
Link Loss Forwarding	216
Alarm message	341
Link status	216
linkspeed - CLI command	281
List configuration	236
LLC	
header	111
LLM See Local Link Monitoring	216
Local activation	242
Local interface	
diagnostics	219
statistics	17-18
status	216
Local link monitoring	216
Location of encryptors	22
Locking	
access	177
front panel	177
USB port	177
Locmacs	
adding manually	86
CLI command	283
table	76
locmacs - CLI command	283
Logging	
OID utilization	177
Login	
explicit	141
Logout	
CLI command	284
logout - CLI command	284
Logs	323
Audit	325
based on OIDs	177



Event	324
long term from CM7	176
Long term logging	176
Longest Prefix Match	206, 274
LPM	
Longest Prefix Match	274
M	
MAC address(es)	
encryptor ports	209-211
management port	15
migration	77
remote peer	210, 212
unknown action	203
unknown Multicast action	203
Maintainer	122, 181
role and privileges	122
Manage	
screen	173
Management	
ethertypes of frames	200
gateway address	183
gateway encryptor	120
Inband	231
interfaces	15
IP address	183
network prefix	183
Man-in-the-middle	83, 89
Master key	
issues	239
Message(s)	
Alarm	341
Audit	327
SNMP Trap	344
System	334
MIB	115
mode - CLI command	285



Mode(s)	
Connection	43
cryptographic	42
encryptor operating	41
mode CLI command	285
Modem	16
Module	
management module details	178
Monitoring	
Alarms	124
certificates via RESTful interface	124
with SNMPv1/2	120
MPLS	
alternate ethertype	202
bypass shims (default disabled)	202
CLI command	285
labels	113
shims	113
mpls - CLI command	285
MTU	
Ethernet - maxumim	43
overflow prevention in CTR mode	200
preventing overflow	302
Multicast	244
auto discovery	75, 211
operation	109
Multi-slot encryptors	161
Mutation	
of ethertypes	58, 73, 93
N	
Naming encryptors	24
NAT	
allowing L3 encryption	275
encrypting Layer 3 traffic	205
Netflow traffic analyzer	114



Netmac	
adding manually	86
auto discovery	75
netmacs CLI command	286
netmacs - CLI command	286
Network	
inband_vlan management addresses	183
interfaces	76
management addresses	182
Network interface	
Diagnostics	220
statistics	19-20
status	216
NIST	
KDF approved 800-108	98
Non Activated Password	141
NTP	
date and time updates	179
format	179
key provider	41
Server	177
server as source of Date and time	25
Server count	323
use for KDK	99
ntpconf - CLI command	287
NTU	22
Null modem cable	16

O

OCSP	
CLI command	287
configuring servers	194
servers	194
ocsp - CLI command	287
Offset processing	205
OID	123
gEthSenderId	213



selection for logging	177
sysMgmtHostName	213
Operating environment	21
Operation mode	
Ethernet	41
Operational mode	41
Operator	122, 181
Optical LLF	216
Other - see Unlisted ethertype	258
OUI	112
Overheads	
TCP and UDP	41
TIM mode	41
overview - CLI command	288
P	
Pairwise keys	44
password - CLI command	288
Password(s)	
allowed characters	117
CLI command	288
enhanced mode	117
lexical diversity	116
Non Activated	141
PC - See Personal Computer	16
PCAP network analysis files	236
Peer encryptor	
remote MAC address	210, 212
PEM file	
import	192
saving CSR to	168
Performance	
Ethernet encryptors	110
Personal computer	
settings	16
PKCS#12	
creating on Configuration server	144



file creation	165
file deletion	156
importing/exporting files	150
Pluggable interfaces	5
Point-point (Line) mode	199
Policy	
based on peer MAC address	75
CLI command	292
Ethernet encryption	40, 90, 198
ethertype	57, 72, 92, 203
ethertype mutation	205
global	199
Layer 3/4 IP Rules	205
Line (point-point) mode	199
operational mode	199
Q-in-Q	92
Transport Independant Mode (TIM)	101
policy - CLI command	292
Ports	
configuring Traps	141
Remote CLI (22)	190
speed auto negotiation	217
trap listener	141
UDP (161)	233
Post-Login	181
Power supplies	
Alarms	7
CN6000 AC	8
CN6000 Series	8
CS10	7
Power-up	12
Pre-Login	181
PRNG psuodorandom number generator	98
profile - CLI command	295
prompt - CLI command	176, 296
protocol - CLI command	296



psu - CLI command	296
Public Path	141
PVST	78

Q

Q-in-Q policy	92
qkd - CLI command	297
QKD quantum key distribution	255
address setup	214
statistics	215
QoS quality of service	
in Line mode	109
layer 2 VLAN support	44
QRA quantum resistant algorithm	152
interoperability	152
key size	247
use with QKD	215
QSFP	
CLI command	298
qsfp - CLI command	298
Quantum	
Resistant Algorithms	152

R

Rate limiting	31
frame loss	32
need for traffic shaping	32
Real Time Clock	7, 24
Reboot	
CLI command	299
on mode change	45
Redhat	137
Redis	162
Redundant supply	7
Refresh rate	
Encryptor list	141
Network View	141



Release	
number for firmware	27
Remote ID	
peer encryptor MAC address	210, 212
Requirements	
for CM7 installation	134
rest - CLI command	300
Restart	
of encryptor	44
RESTful interface	123
Access with CM7	123
certificates for	250
examples	124
RFC1024	112
RFC1305	179
RFC5424	184
Roles	
Administrator	122
Maintainer	122
Operator	122
Supervisor	122
Routing	233
RTC	7
S	
Safety notices	iv, 241
SAP	
format	112
SAP SNAP format	112
Secure halt	13
indication	5
Secure Shell (SSH)	189
Security	
levels	160
physical	22
Sender ID	91, 100



Senetas	
ethertype	76, 110
Serial connections	7
Serial Number	193
Servers	
CRL	194
FTP/FTPS firmware upgrades	187
OCSP	194
Service VLAN	113
Session	
establishment Ethernet	76
multipoint MAC	76
timeout	141
Settings	
file (CM7)	140
hiding if not required	141
security levels	160
SFP	
CLI command	301
sfp - CLI command	301
Shim	
CLI command	302
CTR mode rate	200
GCM mode	43
insertion rate	43
preventing MTU overflow	302
shim - CLI command	302
SID - see Sender ID	91
Skipped sequence count	308
Slot	
CLI command	161
slot	
license allocation	303
slot - CLI command	303
snap - CLI command	304
SNAP observe PID	253



SNMP	184, 325
cancelling requests	227
changing trap listener port	141
enabling CM7 to receive traps	141
enabling SNMPv1	120
encryptor settings	184
Local encryptor management	227
rate limiting frame loss	32
security levels	160
SNMPv1 monitoring	120
trap configuration	184
Trap messages	344
Trap Preferences	326
traps	325
snmpcfg - CLI command	305
snmptraps - CLI command	305
SNMPv1	
enabling with CM7	184
SNMPv2	
trap messages	325
SNMPv3	227
Software	
Build	178
firmware description	178
Spanning Tree Protocol	78
auto-discovery required	245
configuring	81
monitoring	78
SSH	189
key pair creation	190
sshaux - CLI command	306
sshcli - CLI command	306
Stacked VLAN	113
Station ID	141
Statistics	
management	15



management port	217
stats - CLI command	307
Status	
local interface	216
network interface	216
STP	78
BPDU messages	202
monitoring	202
Supervisor	181
role	122
Support	
configuration sharing	173
SYN frames	206
Syslog	
CLI command	309
configuration using CM7	184
format	184
Server IP Address	179, 185
syslog - CLI command	309
sysMgmtHostName	213
System	
CM7 requirements	134
details display	177
encryptor information	177

T

Table(s)	
Ethertype	45
local and remote MAC clearing	45
locmac	76
MAC addresses	76
network MAC addresses	76
VLAN clearing	45
tacacs - CLI command	311
TACACS+	189
Tamper	
alarm	14



from front panel	6
TCP protocol	
overheads	41
Temperature	
of modules	217
Terminal server	16
This documents ID	i
Ticket Request Password	141
Tile	
management windows	141
TIM mode	
configuration	25
configuration via CLI	107
encryption policy	101
frame formats	107
KDK distribution	171
KDK generation	155
key synchronization	105
Time zones	
for encryptor	179
Timeouts	
discovery	141
timezone - CLI command	311
TLS	100, 107
algorithms	39
Traffic	
analysis	236
PCAP files	236
shaping	32
TRANSEC	62
Flow Control	64
Overview	62
with Rate limiting	64
transec	
CLI command	313
transec - CLI command	313



Transport frame	65
Traps	
enabling	325
handling	325
Troubleshooting	
Cable problem	240
Certificate expired	238
FIPS mode incompatibility	238
FLOW states	238
Master status	239
Tunnels	
CLI command	314
tunnels - CLI command	314
U	
UDP	15
UDP protocol	16
management statistics	15
overheads	41
Unicast	
addresses	58, 73
MAC connections	76
operation	109
Unlisted ethertype	
(O)ther type	258
Unlocking	
access	177
front panel	177
USB port	177
Unpacking encryptors	21
upgrade - CLI command	317
Upgrade(s)	
firmware	122
screen	221
usb - CLI command	317
USB port	
locking and unlocking	177



User definable features	
entropy pool	29
User Path - current	141
User(s)	
access	180
access attributes	117
account details	181
account management	122
CLI command	317
console access	181
logout	226
Name (short and long)	181
SNMP access	181
users - CLI command	317
UTC	312
Utilization	176

V

Validity	193
Version	
CLI command	318
TLS	39
version - CLI command	318
Virtual management	115, 234
VLAN	
bypassing multiple	293
CLI command	319
configuring ID (Pt-Pt mode)	60
customer tag, C-VLAN, CE-VLAN, C-TAG	113
enabling/disabling auto-discovery	240
encryptor settings	200
Group keys	109
header display	209-210
ID display	209
ID override	211
Q-in-Q	113
restarting connections	91



Service, S-VLAN, SP-VLAN, PE-VLAN, S-TAG	113
stacked tags	113
tags	112
vlan - CLI command	319
VPLS	
inband management	183

W

Warnings	
enabling display	141
Windows	
Refresh rate	141
Wireshark	
traffic analysis tool	236

X

X.509 certificates	
CA - certificate signing type	193
EN - data encryption type	193
OT - other (utility) type	193

